Regulating Cryptocurrencies in New Zealand

The Law Foundation NEW ZEALAND

September 2018

Associate Professor Alexandra Sims
Dr Kanchana Kariyawasam
Professor David Mayes

THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

BUSINESS SCHOOL

Griffith UNIVERSITY

Acknowledgements

The authors would like to acknowledge the support of the New Zealand Law Foundation, without which the project and resulting report would not have occurred. Thanks also to Chaowei Fan for providing input and valuable translation skills into the part on China's work on a central bank-issued cryptocurrency.

Alex[1] and Kanchana[2] would like to dedicate this report to their co-author Professor David Mayes,[3] who sadly passed away in November 2017 after a short illness.

[1] Associate Professor Alexandra Sims, Department of Commercial Law, Business School, the University of Auckland.
[2] Dr Kanchana Kariyawasam, Senior Lecturer, Griffith Business School, Griffith University.
[3] Professor David Mayes, BNZ Professor of Finance, Department of Finance and Accounting, Business School, the University of Auckland.

ISBN: 978-0-473-45925-3

Table of contents

Executive summary and recommendations

Cryptocurrencies, in particular bitcoin, have captured the public's attention. It is hard to find a person who has not heard about bitcoin, albeit blockchain, the technology that the creators of bitcoin devised, is still a mystery to most. (Blockchain is just one form of distributed ledger technology (DLT). For the sake of simplicity the term blockchain is used throughout this report.)

Prior to bitcoin, people who wanted to transfer value between themselves needed to do it face-to-face or rely on trusted third parties. Even transacting face-to-face often required the use of bank notes (cash) issued by central banks – and good luck trying to get someone in New Zealand to accept Moroccan dirham for a cup of coffee. Cryptocurrencies allow people to transfer value in seconds – if using a newer cryptocurrency than bitcoin – between themselves even if they are on opposite sides of the world without using third parties: something which conventional banking systems cannot do. Not only can value be transferred, but there are considerable cost savings: a blockchain is a shared tamper-proof ledger which means the parties do not need to reconcile their records.

Conventional payment systems have not caught up with the internet age. We take it for granted that we can send digital files, such as photographs and documents, across the world in seconds. Moreover, the use of cryptocurrencies goes well beyond mere transfers of value; it can transform how we transact. The provision of goods and services, including the transfer of legal title and the payment, can be done in one transaction. So compelling are the opportunities that blockchain technology allows that large corporations are already using cryptocurrencies in their operations to move value around the world and central banks are actively working on creating central bank-issued cryptocurrencies, which we refer to as CBDCs.

Fears of the dangers of technology are understandable, such as the ability for criminals to use cryptocurrencies to launder money and finance terror; however, any technology can be used for good and bad. If early humans had turned their backs on fire due to the very real risk of harm, none of us would be reading this report. Indeed, criminals are using the current banking and corporate/trusts systems more than cryptocurrencies.

While cryptocurrencies are tolerated in New Zealand, as they are in most countries, in practice they are difficult to obtain and use. Many New Zealand cryptocurrency exchanges, where people can purchase cryptocurrencies with New Zealand dollars (fiat currency), find it difficult to obtain bank accounts, and when they do, the exchanges' bank accounts are often closed down. Businesses find it extremely difficult to operate without bank accounts. In turn, consumers are potentially harmed if they purchase cryptocurrencies from overseas exchanges, which may not be subject to the same level of regulatory oversight as New Zealand exchanges. The risk increases if those cryptocurrencies are stored by the overseas exchanges.

Businesses that want to receive and pay in cryptocurrencies also find it difficult to obtain and keep bank accounts in New Zealand. As a result, businesses, and the resulting economic activity, migrate to those countries that are actively fostering their blockchain ecosystem. New Zealand has an opportunity to be a blockchain and financial technology (fintech) hub, which would fit well with New Zealand's perception as a nimble, agile and innovative country. However, for New Zealand to realise its potential, change is required.

Recommendations:

1. The New Zealand Government should continue to allow cryptocurrencies to be traded as well as used for the payment of goods and services within and outside New Zealand.
2. New Zealand-based cryptocurrency exchanges should be encouraged, and clear and detailed guidance provided as to their anti-money laundering/counter-the funding of terrorism (AML/CFT) obligations by both the Department of Internal Affairs (DIA) and the Financial Markets Authority (FMA). That is, follow Australia's example.

3. Greater advice and therefore protection should be provided to consumers on cryptocurrencies by the FMA, DIA and other organisations.
4. Cryptocurrency exchanges that comply with AML/CFT and other requirements must have access to bank accounts with New Zealand banks.
5. Merchants must be able to accept cryptocurrency payments by people or organisations for under NZD 100 or payments made through a New Zealand exchange (or an overseas exchange) that complies with AML/CFT requirements, without the merchants losing their bank accounts.
6. GST is removed from cryptocurrencies that are used for the payment of goods and services.
7. The Inland Revenue Department (IRD) clarifies other taxation rules around the use of cryptocurrencies.
8. The IRD should accept cryptocurrencies for the payment of taxes.
9. The Reserve Bank of New Zealand (RBNZ) should trial the creation and issuance of a New Zealand CBDC.
10. Although this point goes wider than merely cryptocurrencies, New Zealand should follow countries such as the United Kingdom (UK) and Australia, and create a regulatory sandbox and ensure that the regulators work alongside fintech companies.

> Virtual currencies[4] are in a different category [to digital payments in existing currencies, through Paypal, and other "e-money" providers such as Alipay in China, or M-Pesa in Kenya], because they provide their own unit of account and payment systems. These systems allow for peer-to-peer transactions without central clearinghouses, without central banks.
>
> For now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of fiat currencies and central banks. Why? Because they are too volatile, too risky, too energy intensive, and because the underlying technologies are not yet scalable. Many are too opaque for regulators; and some have been hacked.
>
> But many of these are technological challenges that could be addressed over time. Not so long ago, some experts argued that personal computers would never be adopted, and that tablets would only be used as expensive coffee trays. So I think it may not be wise to dismiss virtual currencies.[5]

1. Introduction

Many new technologies are treated with fear and suspicion. The first cars were limited to a speed of four miles per hour on public highways and two miles an hour in cities, towns and villages. A person was required to walk in front of the car carrying a red flag to warn riders and drivers of horses about the oncoming vehicle.[6] Lifts are another example. The first lifts were controlled by lift operators, who pushed buttons manually and opened and closed the doors. When operators were removed due to technological advancements, many people refused to enter lifts not staffed by them.[7] To overcome people's fear, first music and then a voice informing people that doors were closing and which floor they were arriving at were used. It is no wonder then, that cryptocurrencies, and the underlying technology, blockchain, are treated with fear and concern. For example, the banking system is used to launder billions of dollars a year[8] (for almost all laundered money passes through at least one bank)[9] and also to fund terrorism.[10] Nevertheless, the United States (US) Department of the Treasury Under Secretary, Sigal Mandelker, singled out bitcoin,[11] observing that "law enforcement authorities recently arrested a woman in New York who used Bitcoin to launder fraud proceeds before wiring the money to ISIS".[12] If one incident was sufficient to shut down an

---

[4] In this report the term "cryptocurrency" is used where possible in place of terms such as "virtual currency", "digital currency" or "e-currency" to avoid confusion and maintain consistency. In addition, while there are thousands of "cryptocurrencies" in truth almost all are tokens and are not designed as payment systems. Currently the main cryptocurrencies that are designed (or are used in practice) for payments are bitcoin, Bitcoin Cash, Dash, Ethereum, Litecoin, Monero, Ripple, Stellar Lumens, Tether, and ZCash.

[5] Christine Lagarde "Central Banking and Fintech: A Brave New World" (2018) Innovations 4 (at the time of the speech which the article reproduces, Lagarde was the Managing Director of the International Monetary Fund).

[6] The Locomotive Act 1865 (UK), ss 3(2) and 4.

[7] Steve Henn "Remembering When Driverless Elevators Drew Skepticism" (Podcast, 31 July 2015) Planet Money <https://www.npr.org/2015/07/31/427990392/remembering-when-driverless-elevators-drew-skepticism>.

[8] Max de Haldevang "The Top 50 Global Banks Allegedly Involved in a $21 billion Russian Money-laundering Scheme" *Quartz* (United States, 22 March 2017) <https://qz.com/938504/the-top-50-global-banks-allegedly-involved-in-the-20-8-billion-russian-laundromat-money-laundering-scheme/>.

[9] As the organisation Global Financial Integrity has observed, "[b]ecause laundering money almost always requires it to pass through one or more banks, the primary strategy against it is to require banks to perform certain checks and monitor transactions to make sure their accounts are not being used for money laundering." Global Financial Integrity "Money Laundering" <http://www.gfintegrity.org/issue/money-laundering/>.

[10] Issie Lapowsky "Banks Deploy AI to Cut off Terrorists' Funding" *Wired* (United States, 9 July 2017) <https://www.wired.com/story/quantaverse-ai-terrorist-funding/>.

[11] For the purposes of this report, the term "Bitcoin" will be used to refer to Bitcoin the technology and protocol, ie the Bitcoin blockchain, and "bitcoin" to the cryptocurrency itself though the dinstinction is not always clear-cut. Except, of course, when a source uses a different method of capitalisation, such as the quote later in this sentence. Both are sometimes abbreviated BTC.

[12] Sigal Mandelker "US Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference" (speech to the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference, New York, February 2018) <https://home.treasury.gov/news/press-release/sm0286>.

organisation, few banks, if any, would be in existence,[13] not to mention professional industries: accountants and lawyers can unwittingly play a part in money laundering.[14]

It is vital to remember that the use of a technology for both legitimate and criminal means is nothing new. Looking around again at mundane items, kitchen knives are a useful tool, but they can be lethal in the wrong person's hands. As the United Kingdom's (UK's) Chief Scientific Adviser observed in relation to blockchain:[15]

> As with most new technologies, the full extent of future uses and abuses is only visible dimly. And in the case of every new technology the question is not whether the technology is "in and of itself" a good thing or a bad thing. The questions are: what application of the technology? for what purpose? and applied in what way and with what safeguards?

Before Bitcoin[16] the ability to send and receive money was mediated by a bank or another financial institution. Payment providers such as PayPal and even newer ones like Android Pay and Apple Pay, still use conventional technologies and are reliant on banks and credit card companies to facilitate payments that use national currencies, or, as they are referred to in this report, fiat currencies. Even if one person hands another person New Zealand bank notes, those bank notes were supplied by the Reserve Bank of New Zealand (RBNZ). Bitcoin, and the many cryptocurrencies created in its wake,[17] challenge the current payments schemes, although as we shall see below what we consider to be money has evolved over time.[18] A person sending bitcoin to another person is in effect sending money[19] without the involvement of a bank, financial institution or any other centrally controlled institution. It makes no difference if the payer and recipient are standing next to each other or are on opposite sides of the world: the costs and the speed of the transaction are the same. As a payment mechanism, bitcoin is now comparatively slow and clunky, not to mention expensive, compared to newer cryptocurrencies such as Litecoin and Dash. The ability for people to use a plethora of alternative currencies is not new to New Zealand. Prior to 1934 British coins minted by the Royal Mint in London were the only legal tender coin in New Zealand, but bank notes were issued by individual banks. The bank notes might or might not be accepted by other banks, although mostly they were.[20]

The use of cryptocurrencies in combination with smart contracts has the potential to transform commerce as cryptocurrencies can do considerably more than current technology, which uses fiat currency. Take the example of smart contracts which can be used to programme how, when and to whom a payment in a cryptocurrency is made, as well as a range of other things as the following

---

[13] Nick McKenzie, Richard Baker and Georgina Mitchell "Australian banks are exposed to millions in money laundering" *Stuff* (New Zealand, online ed, 15 September 2017) <https://www.stuff.co.nz/business/world/96869035/australian-banks-are-exposed-to-millions-in-money-laundering>.

[14] New Zealand's AML/CFT legislation, the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009, was extended to cover lawyers and accountants from 1 July 2018. See also A Mitchell, P Sikka and H Willmott "Sweeping it Under the Carpet: The Role of Accountancy Firms in Money Laundering" (1998) 23 Accounting, Organizations and Society 569.

[15] United Kingdom Government Chief Scientific Adviser *Distributed Ledger Technology: Beyond Block Chain* (19 January 2016) <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain> at 7.

[16] Bitcoin was created by a person or persons known as Satoshi Nakamoto. A Whitepaper outlining blockchain technology and what was to become known as Bitcoin was released in October 2008: Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* (Whitepaper, 2008) <https://bitcoin.org/bitcoin.pdf>.

[17] On 21 April 2018 the website Coincap.io (https://coincap.io) listed 1262 different coins. These other cryptocurrencies are sometimes called alt coins. While some are designed for use on payment rails, most are not. For example, some are designed as tokens that are required to access and use certain systems, such as Sia and Golem Network Tokens, which are both decentralised storage systems. Some central banks have started to explore the possibility of creating their own cryptocurrencies, see Section 8 Central bank-issued cryptocurrencies below.

[18] See Section 3.1 A brief history of money below.

[19] The question of whether bitcoin is money is contentious.

[20] Te Ara, the Encyclopedia of New Zealand "Coins and Banknotes – Varied Coins and Banknotes, 1840s to 1930s" <https://teara.govt.nz/en/coins-and-banknotes/page-1>.

example demonstrates. A smart contract[21] can be used so that payment is made automatically when a shipment of New Zealand lamb arrives at a foreign port.[22] The smart contract can be programmed to allow title to the lamb to pass at the same time as the payment is made.[23] In addition, the smart money can allow the payment to be programmed even further. Instead of the current system, where money is paid to one party who then pays tax to the Inland Revenue Department (IRD), pays the farmer(s), pays the parties involved in shipping the lamb and so on, each party can be paid a pre-set percentage of the payment. The implications of real-time payments to all those connected with the supply chain are profound – and not just for the tax base. Furthermore, if an entity used a cryptocurrency for all of its income and expenditure then potentially it would not need to prepare tax returns. Such a system would require all payments and receipts to be coded with the relevant information and that information stored on the blockchain or in a place to which the IRD had access.

Smart contracts can also be programmed to prevent the spending of money beyond the purposes for which it was provided. For example, the UK Government has already trialled GovCoin for benefit payments. Albeit GovCoin has attracted its fair share of criticism,[24] if used it would go a long way towards reducing the costs of friction and fraud in welfare and other Government payments.

The ramifications of the ability to use blockchain to prevent wrongdoing and not simply to give people legal rights – which may not be of any use to them even if they could afford to go to court – will be transformative. That is, the law's response to wrongdoing does not always help the innocent party or victim. For example, if a driver fails to stop for a pedestrian on a pedestrian crossing and kills them a successful prosecution of the driver does not magically bring the victim back to life. It would be much more desirable to prevent the driver from running over the pedestrian in the first place. In the offline world it is difficult, or rather it is often not cost-effective, to prevent laws being broken. For the pedestrian example it would require bollards on either side of the pedestrian crossing to arise before the pedestrian started to cross. However, limitations are more easily imposed when computer code is used.[25]

Take, for example, a family trust that has a house as one of its assets. The trustee is the legal owner of the house, but owes duties to the beneficiaries. As the legal owner the trustee has the ability to sell the house. If the trustee sells the house to a third party who has no knowledge of the trust, the third party is entitled to keep the house and the beneficiaries cannot get it back. While the beneficiaries do have the right to sue the trustee, at best they can recover the proceeds of the sale, but if the trustee has absconded overseas with the money the beneficiaries' rights are to all intents and purposes worthless. If land titles are put on the blockchain,[26] it can be set up so that the land can only be sold if both the trustees and the beneficiaries assent to the transaction. That is, the code prevents the breaking of the law.

To be sure, a system of requiring the beneficiaries to agree to the sale of the house does not necessitate blockchain to implement it, but if such a system (which would require radical law change) was implemented using current technology it would not work because traditional written

---

[21] A smart contract is a computer program of the form: if X happens do Y. For this and other terms, see Glossary.

[22] Emily Cadman "Commonwealth Bank's cotton bale blockchain experiment could change trade forever" *The Sydney Morning Herald* (Australia, online ed, 24 October 2016) <https://www.smh.com.au/business/banking-and-finance/commonwealth-banks-cotton-bale-blockchain-experiment-could-change-trade-forever-20161024-gs8x4n.html>.

[23] Ibid.

[24] Robert Herian "Why a Blockchain Startup called Govcoin Wants to 'Disrupt' the UK's welfare state" *The Conversation* (Australia, 28 November 2017) <https://theconversation.com/why-a-blockchain-startup-called-govcoin-wants-to-disrupt-the-uks-welfare-state-88176>.

[25] See generally, Lawrence Lessig *Code: version 2.0* (2nd ed, Basic Books, New York, 2006).

[26] See Joon Ian Wong "Sweden's Blockchain-powered Land Registry is Inching Towards Reality" *Quartz* (United States, 3 April 2017) <https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/>.

signatures ("wet" signatures), can be forged relatively easily.[27] What is needed to protect the beneficiaries is for them to assent or "sign" using their digital identity.[28]

The importance of digital identity cannot be overstated, and it is not just required for blockchain applications. Current systems of identification do not work effectively and the costs they impose on organisations and people are immense. Blockchain is being used to provide digital identity solutions.[29] The World Economic Forum has recognised the urgency of being able to prove identity, how our current systems are inadequate and must change and also how blockchain can play a part.[30]

In addition, if the trust in the above example has been set up so that a beneficiary is not entitled to certain assets until reaching a certain age, and the assets have been tokenised, a smart contract can be used so that the assets cannot be released to the beneficiary until that age. Moreover, because the assets are controlled by the smart contract there is no need for human intervention to transfer the ownership and control of the assets; these procedures are performed automatically by the smart contract.

Given blockchain technology's advantages over existing technology, banks and other financial institutions including central banks are trialling its use for, among other things, payments.[31] In addition, some central banks are working on issuing their own cryptocurrencies,[32] with some already issued or about to be.[33] Klickex, a New Zealand remittance business (a money transfer operator (MTO)), in conjunction with IBM, is using the cryptocurrency Stellar Lumens for part of its transaction process.[34] Thus people sending money from New Zealand to the Pacific Islands are using a cryptocurrency without realising. More recently IBM has launched its IBM Blockchain World Wire, which allows cross-border payments between financial institutions to be settled in seconds not days.[35] The institutions can "agree to use a stable coin, central bank digital currency or other digital asset as the bridge asset between any two fiat currencies. The digital asset facilitates the trade and supplies important settlement instructions."[36]

Unknown to most people, the use of cryptocurrencies has been reasonably well embedded within the payments sector for a number of years as we have been employing cryptocurrency debit cards.[37]

---

[27] In which case the beneficiaries would again lose out if the trustee forged the signatures and the purchaser had no knowledge of the forgery.

[28] For work on digital identity that cannot be hacked see Patrick Gower "Kiwi Tech Company Centrality's radical Data Privacy Solution" *Newshub* (New Zealand, 23 April 2018) <http://www.newshub.co.nz/home/new-zealand/2018/04/kiwi-tech-company-centrality-s-radical-data-privacy-solution.html>.

[29] See, for example, Sovrin <https://sovrin.org/>; Civic <https://www.civic.com/>; Uport <https://www.uport.me/>; Sphere Identity <https://sphereidentity.com/>; and Single Source <https://www.mysinglesource.io/>.

[30] World Economic Forum *Digital Identity: On the Threshold of a Digital Identity* (Whitepaper, January 2018) <http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf>.

[31] "$10 payment paving the way for banking revolution" *Stuff* (New Zealand, online ed, 22 September 2016) <http://www.stuff.co.nz/business/money/84549159/10-payment-paving-the-way-for-banking-revolution>. This describes the transfer from one employee's account to another account in Canada that took 10 seconds to process as "one small transfer for National Australia Bank, one giant leap for banks worldwide".

[32] See Section 8 Central bank-issued cryptocurrencies below.

[33] Venezuela has released its Petro (<http://petrodollars.io/>), see Matt O'Brien "Venezuela's Cryptocurrency is One of the Worst Investments Ever" *Washington Post* (United States, online ed, 5 March 2017) <https://www.washingtonpost.com/news/wonk/wp/2018/03/05/venezuelas-cryptocurrency-is-one-of-the-worst-investments-ever/?noredirect=on&utm_term=.734d941a0624>. The Marshall Islands passed its Declaration and Issuance of the Sovereign Currency Act 2018 on 26 February 2018 (see <http://law.sov.global/law.pdf>) which will be legal tender in the Marshall Islands (along with the United States dollar) <https://www.sov.global/>.

[34] IBM "IBM Announces Major Blockchain Solution to Speed Global Payments" (Press release, 16 October 2017) <http://www-03.ibm.com/press/us/en/pressrelease/53290.wss>.

[35] IBM "IBM Blockchain World Wire" (2018) <https://www.ibm.com/blockchain/solutions/world-wire>.

[36] Ibid. For a discussion about stable coins, see Section 4.9.1 Fluctuations in price below.

[37] See, for example, TenX (<https://www.tenx.tech/>) and Bitpay (<https://bitpay.com/card/>). With others being developed, see, for example, Oscar Williams-Grut "A London Startup is Launching a Debit Card that lets you Spend Bitcoin

Users load cryptocurrency onto the cards through an app and can use them at any place that supports the cards, namely, any merchants that accept Visa or MasterCard. In addition, the cryptocurrency debit cards can be employed to withdraw fiat currencies from automated teller machines (ATMs). Merchants receive fiat currency rather than cryptocurrency, and will not know that cryptocurrencies are being used as they are simply accepting a credit card payment, even though both Visa and MasterCard appear to be having second thoughts about continuing to allow the use of such cards.[38]

Despite a flurry of activity in commercial and regulatory circles, cryptocurrencies are not new: their origins can be traced to 1982.[39] However, the use of the early cryptocurrencies was limited and did not gain traction. While Bitcoin can be seen as a development of those early cryptocurrencies, its decentralised structure and the blockchain technology or distributed ledger technology (DLT) that it created set it apart from its predecessors. Notwithstanding the remarkable technology that Bitcoin created, blockchain now looks relatively dated compared to new DLTs such as IOTA[40] and Hashgraph.[41] However, for the purposes of this report the term "blockchain" will be used as a general term to describe DLT.

Blockchain technology has been described as creating ledgers that:[42]

> … record transaction and ownership using pervasive, persistent, and permanent data structures replicated across numerous computers. The two principal technology components are public-key cryptography and "peer-to-peer" or shared data storage. The end result is a data source that is simultaneously logically "central" while technically "distributed" across the computers on the network. The network of computers using the ledger can consult a single authoritative and immutable ledger of all the data transactions from the origin ("genesis") of the data structure. Everyone has the same "view" of the same "data", though they may be retrieving the data from different physical sources.

Blockchain technology is a paradigm-shifting technology that could transform business and society beyond mere money.[43] Scott Morrison, when he was the Australian Treasurer, was reported as imploring companies and government departments to use reports[44] prepared for the Government

---

and Ethereum" *Business Insider Australia* (15 November 2017) <https://www.businessinsider.com.au/london-block-exchange-launches-prepaid-cryptocurrency-debit-card-2017-11?r=UK&IR=T>.

[38] See Annie Nova "Some Cryptocurrency-backed Debit Cards Dropped from Visa Network, Leaving Users Scrambling" *CNBC* (United States, 5 January 2018) <https://www.cnbc.com/2018/01/05/some-cryptocurrency-backed-cards-dropped-from-visa-network.html> and JP Buntinx "MasterCard Removes Cryptocurrency Debit Card Availability Outside EEA" *The Merkle* (12 October 2017) <https://themerkle.com/mastercard-joins-visa-in-removing-cryptocurrency-debit-card-availability-outside-of-the-eea/>.

[39] David Chaum "Blind Signatures for Untraceable Payments" in RL Rivest, A Sherman and D Chaum (eds) *Advances in Cryptology: Proceedings of Crypto 82* (Plenum Press, New York, 1983) at 199 and see Section 3.2 The evolution of cryptocurrencies below.

[40] IOTA, a blockchain designed for use by IOT (Internet of Things) devices and micro payments which uses a Tangle rather than a series of liner blocks. See Serguei Popov *The Tangle* (Whitepaper, Version 1.3, 1 October 2017) <https://iota.org/IOTA_Whitepaper.pdf>.

[41] Hashgraph is another new proposed system. See Leemon Baird *The Swirlds Hashgraph Consensus Algorigthm: Fair, Fast, Byzantine Fault Tolerance* (Whitepaper, 31 May 2016) <http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>.

[42] Michael Mainelli and Alistair Milne "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle" (Working Paper No. 2015-007, SWIFT Institute, 9 May 2016) at 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777404>.

[43] See Section 3.3 Cryptocurrencies after Bitcoin – not limited merely to payments below. And see James Eyers "Data 61 Reports Blockchain will Have a Profound Impact on the Economy" *The Australian Financial Review* (online ed, 7 June 2017) <http://www.afr.com/technology/data61-reports-blockchain-will-have-a-profound-impact-on-the-economy-20170605-gwktp9>.

[44] The Data 61 reports are: Data 61 *Distributed Ledgers: Scenarios for the Australian Economy over the Coming Decades* (May 2017) and Data 61 *Risks and Opportunities for Systems using Blockchain and Smart Contracts* (May 2017) – both available from <http://www.data61.csiro.au/en/Our-Work/Safety-and-security/Secure-Systems-and-Platforms/Blockchain>.

for "guidance on how they can accelerate their uptake of blockchain technology".[45] While this report focuses on cryptocurrencies, we also touch on aspects of the blockchain, including smart contracts that employ blockchain technology.[46]

Such is the potential of blockchain technology even within the banking and payments field that some governments and other institutions have seized upon it.[47] The Bank of Canada began trialling blockchain technology for its wholesale interbank payments settlement system in 2016. As Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, stated, "it's not surprising that central banks have developed a keen interest in FinTech and distributed ledger technology (DLT)."[48] The potential for use in capital markets has also been recognised, with estimates that "blockchain could save lenders up to $20 billion annually in settlement, regulatory, and cross-border payments costs."[49]

It is important to realise that while the first blockchain, the Bitcoin blockchain, was, and remains, decentralised, blockchain technology does not need to be decentralised. "Permissioned" blockchains, where people need to be granted access, can and are being used. That is, the blockchain's control is centralised, whether there is one party controlling it or a consortium. Linux's Hyperledger Fabric,[50] the platform that IBM[51] is using in a number of industries, is one example of a permissioned blockchain. Thus blockchain technology covers a wide range of different types of blockchains. Interestingly – and this is arguably the key to blockchain technology's rapid development – most blockchains run on open source software, including Hyperledger Fabric.[52]

As with any technology, blockchain has benefits and risks. Many of the benefits and risks flow from its nature as a decentralised ledger if a public blockchain is used. Decentralisation of authentication of data in the ledger means that the ledger's users do not need to trust a third party for security and verification of the information within the ledger.[53] Decentralisation means that changes to the blockchain which would be contrary to the interests of most users are rejected.[54] This makes blockchains resilient to attacks.[55] The system is also predictable because the software is self-executing and is not subject to discretionary decision making.[56] However, its decentralised nature is also the source of some of the risks. For example, if a person loses their private keys, they[57] lose their cryptocurrency.[58]

---

[45] See Eyers, above n 43.
[46] See Section 2.2 The value of blockchain technology beyond cryptocurrencies below.
[47] See, for example, Section 8 Central bank-issued cryptocurrencies (CBDCs) below.
[48] Carolyn Wilkins "Project Jasper: Lessons From Bank of Canada's First Blockchain Project" *Coindesk* (10 February 2017) <https://www.coindesk.com/project-jasper-lessons-bank-of-canada-blockchain-project/>.
[49] Greg Medcraft "The Future of Capital Markets in a Digital Economy" (Distinguished speaker series, Carnegie Mellon University, Adelaide Australia, Australian Securities and Investments Commission, September 2015) at 5 <http://download.asic.gov.au/media/3356655/keynote-address-future-of-capital-markets-20151709-final.pdf>.
[50] <https://www.hyperledger.org/projects/fabric>.
[51] <https://www.ibm.com/blockchain/hyperledger.html>.
[52] See Alexandra Sims "Why Blockchain Challenges Conventional Thinking about Intellectual Property" *The Conversation* (Australia, 27 February 2018) <https://theconversation.com/why-blockchain-challenges-conventional-thinking-about-intellectual-property-91469>.
[53] Pak Nian Lam and David Lee Kuo Chuen "Introduction to Bitcoin" in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 5 at 9; Adrian Blundell-Wignall "The Bitcoin Question: Currency versus Trust-less Transfer Technology" (Working Paper on Finance, Insurance and Private Pensions No. 37, OECD, 2014) at 15; and Pedro Franco *Understanding Bitcoin: Cryptography, Engineering, and Economics* (Wiley, 2015) at 169.
[54] Franco, above n 53, at 5.
[55] At 5–6.
[56] At 5.
[57] While is it is arguably grammatically correct to use "he or she" to denote a single person, such a construction does not take into account intersex, trans-sexual and genderqueer people. The gender-neutral "they" is therefore used in this report.
[58] See Section 4.9.2 Loss of private keys and passwords below, although no one else can use this "lost" currency.

Despite the shortcomings of current technology and current limited reach of cryptocurrencies, though, we should be wary of thinking that cryptocurrencies could not turn out to be a revolutionary change adopted around the world. For example, as we shall see, a number of central banks are working on creating their own central bank-issued cryptocurrencies (CBDCs).[59] Even the potential of Bitcoin took many years to manifest. The Whitepaper that proposed what became Bitcoin was released in 2008,[60] the first bitcoins were created[61] in 2009 and the first time bitcoin was used to purchase goods was May 2010.[62] Despite the slow start, bitcoin has gained in popularity and use, even though it is still a niche currency.

The current crop of cryptocurrencies and blockchain technology generally can be likened to the internet in its early days when it was comparatively slow and difficult to use. Even when the internet began to be used widely some people could not see the point of it:[63]

> Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms … Baloney. Do our computer pundits lack all common sense? The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works ... We're promised instant catalog shopping—just point and click for great deals. We'll order airline tickets over the network, make restaurant reservations and negotiate sales contracts … Even if there were a trustworthy way to send money over the Internet—which there isn't—the network is missing a most essential ingredient of capitalism: salespeople.

The internet has become such a part of everyday life and commerce that an airline which did not sell its tickets on the internet today would go out of business quickly. Now many people purchase goods and services online by entering their credit card details or through services such as PayPal. The ability to send money over the internet with relative safety was solved through the use of strong cryptography. And as we shall see, cryptocurrencies also use strong cryptography. Banks also permit their customers to send money directly over the internet through internet banking, which relies on cryptography and other safeguards. The assurance "The cheque is in the mail" is being replaced with "I have paid the money into your account".

Interestingly, one of the commonest criticisms of cryptocurrencies is that they will become worthless once quantum computing is perfected because they rely on cryptography. While this argument is valid, there will be larger problems to deal with if cryptography is rendered useless: many of our systems, including the traditional banking system and especially credit cards, rely on cryptography. Thus the threat from quantum computing is not limited to cryptocurrencies. Work is being undertaken on post-quantum cryptography.[64]

Another criticism that comes up in conversations repeatedly, especially from computer scientists and those in the IT industry, is that centralised databases work and have worked very well, so there is no need for decentralised databases. However, before the internet things worked well, too; you could send a letter to someone and they would normally receive it, notwithstanding that there was a wait. Now with email and other almost instantaneous forms of communication we know that there

---

[59] See Section 8 Central bank-issued cryptocurrencies (CBDCs) below. While CBDC is not the acronym of central bank-issue cryptocurrencies, that is the term that is commonly used. The "D" stands for "digital".

[60] Nakamoto, above n 16.

[61] The technical term for creating bitcoins is "mining". See Glossary.

[62] Paul Vigna and Michael J Casey *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order* (St Martin's Press, New York, 2015) at 79. Even then the bitcoin were not paid by the bitcoin owner to the merchant (who was selling pizza); rather, another person purchased the pizza using his credit card and the bitcoin owner transferred the bitcoin to the purchaser.

[63] Clifford Stoll "Why the Web Won't be Nirvana" *Newsweek* (United States, 26 February 1995) <http://europe.newsweek.com/clifford-stoll-why-web-wont-be-nirvana-185306?rm=eu>.

[64] Daniel J Bernstein and Tanja Lange "Post-quantum Cryptography" (2017) 549 Nature 188.

is no need to wait for days or even weeks to communicate with people, even if those people are on the other side of the world.

Banks and other financial institutions know how much money and time is being wasted with traditional systems. As the instigators of Corda, an open source permissioned blockchain developed by a number of large banks, set out in the abstract to a Whitepaper:[65]

> A distributed ledger made up of mutually distrusting nodes would allow for a single global database that records the state of deals and obligations between institutions and people. This would eliminate much of the manual, time consuming effort currently required to keep disparate ledgers synchronised with each other. It would also allow for greater levels of code sharing than presently used in the financial industry, reducing the cost of financial services for everyone.

Just as more of our lives and commerce takes place online, the nature of fiat currency has evolved. Cryptocurrencies are often described as digital[66] or virtual[67] currencies,[68] yet in truth in New Zealand and Australia almost all our money is digital; the part that is not digital is coins and bank notes (cash).[69] Thus for the purposes of this report, the term cryptocurrency and not digital currency will be used to refer to decentralised cryptocurrencies.

Predicting the future is impossible. The future of money is a contested space. A viable alternative to fiat currency seems to be appearing. As early as 2016 an article in the respected Journal of Banking Regulation analysed the ramifications of banks allowing their customers to use cryptocurrencies instead of fiat currencies.[70] Similarly work has been done on whether cryptocurrencies should be included in the portfolio of international reserves held by a central bank,[71] and numerous central banks are actively exploring creating their own CBDCs.

---

[65] Richard Gendal Brown, James Carlyle, Ian Grigg and Mike Hearn *Corda: An Introduction* (Whitepaper, August 2016) <https://docs.corda.net/_static/corda-introductory-whitepaper.pdf>.

[66] See, for example, Economics References Committee (Australian Senate References Committee) "Digital Currency—Game Changer or Bit Player" (August 2015) at [4.35]. <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report/>.

[67] See Matthew P Ponsford "A Comparative Analysis of Bitcoin and other decentralised virtual currencies: Legal Regulation in the People's Republic of China" (2015) 9 Hong Kong Journal of Legal Studies 29.

[68] Both digital and virtual currencies can, however, also be used to describe more than simply cryptocurrency. "The concept of VCs [virtual currencies] covers a wider array of 'currencies,' ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), to VCs backed by assets such as gold and 'cryptocurrencies' such as Bitcoin." Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko and Concepcion Verdugo-Yepes "Virtual Currencies and Beyond: Initial Considerations" (Staff Discussion Note, IMF, January 2016) at 7 <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>.

[69] Amber Wadsworth "What is Digital Currency?" (2018) 81(3) Bulletin 3 (April 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018apr81-03.pdf>. Also the Reserve Bank in 2016 in Amber Wadsworth "Disruption or distraction? How digitisation is changing New Zealand banks and core banking systems" (2016) 79 Bulletin 12 (May 2016) <http://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2016/2016may79-8.pdf> observed that in 2014 Payments New Zealand stated that New Zealand had the lowest value of bank notes per capita in the OECD (at that stage is was NZD 1,035 per capita, or 2.1 per cent of GDP). Australia was higher at NZD 2,799 per capita or 3.9 per cent of GDP but still well below the United States (NZD 4,269 per capita or 7.5 per cent of GDP) and Japan (NZD 7,827 per capita or 17.9 per cent of GDP): Payments New Zealand *What is Really Happening with Cash in New Zealand* (June 2014).

[70] Gareth W Peters, Ariane Chapelle and Efstathios Panayi "Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective" (2016) 17 Journal of Banking Regulation 239.

[71] Winston Moore and Jeremy Stephen "Should Cryptocurrencies be Included in the Portfolio of International reserves held by the Central Bank of Barbados" (Working Paper No. WP/15/16, Central Bank of Barbados, 13 November 2015) <http://www.centralbank.org.bb/Portals/0/Files/Working_Papers/2015/Should%20Cryptocurrencies%20be%20included%20in%20the%20Portfolio%20of%20International%20Reserves%20held%20by%20the%20Central%20Bank%20of%20Barbados.pdf>. The working paper did not rule out the possibility, but remarked at 21 that, given the volatility of bitcoin, if bitcoin was incorporated into the portfolio of foreign balances its share should be relatively small. Note, while the paper was included in the working papers the authors are academics and not employees of the Central Bank of Barbados. Working

Curiously, unlike some earlier attempts this century to create alternative currencies which were shut down by regulators,[72] only a handful of countries have attempted to ban bitcoin and the other cryptocurrencies.[73] In China, while no exchanges can operate, Chinese nationals can and do use exchanges based outside China.[74] There are two main reasons why bitcoin was not shut down early in its life. First, bitcoin's decentralisation means there is no one source (or person) to go after. Indeed, the creator or creators of Bitcoin were careful not to disclose their identity or identities, and used the pseudonym Satoshi Nakamoto.[75] Second, efforts were made not to publicise and draw unwanted attention to Bitcoin in its early days. For example, Satoshi Nakamoto is said to have asked Julian Assange not to use bitcoin to raise funding for WikiLeaks as "Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage."[76]

Not surprisingly, given the potential technological advances that blockchain offers, banks and other financial institutions including central banks are exploring using it to facilitate their operations. Trying, however, to bolt on new technology to existing systems with their legacy issues is painful and seldom achieves the same results as systems created from scratch. That is why businesses and industries born digital have advantages over their established counterparts.[77] For example, WeBank, the bank of WeChat,[78] in the space of just over two years was able to loan as much money as a Chinese city commercial bank's entire retail business.[79] In contrast to borrowers having to wade through paperwork with traditional banks, WeBank can approve loan applications in 0.3 seconds.[80] As the British Bankers' Association (BBA) has acknowledged:[81]

---

papers on the website are academic articles that are a work-in-progress. They are submitted by the author(s) and posted on the Central Bank of Barbados website for comments and suggestions.

[72] Reuben Grinberg "Bitcoin: An Innovative Alternative Digital Currency" (2012) 4 Hastings Science & Technology Law Journal 159, at 161.

[73] For example, Morocco (Sana Elouazi "Bye-Bye Bitcoin: Morocco Bans Cryptocurrencies" *Morocco World News* (21 November 2017) <https://www.moroccoworldnews.com/2017/11/234382/bitcoin-morocco-cryptocurrencies-economy/>); Bolivia (Belén Marty "Bolivia Not Revolutionary Enough to Tolerate Bitcoin" *Panam Post* (10 July 2014) <https://panampost.com/belen-marty/2014/06/19/bolivia-not-revolutionary-enough-to-tolerate-bitcoin/>); Kyrgyzstan (Pete Rizzo "Kyrgyzstan: Bitcoin Payments Violate State Law" *Coindesk* (4 August 2014) <https://www.coindesk.com/kyrgyzstan-bitcoin-payments-violate-state-law/>). In Bangladesh and Nepal it is not clear whether holding cryptocurrency is illegal or whether the trading of cryptocurrency is illegal: see eg Samuel Haig "Bangladesh Authorities on 'Hunt' for Bitcoin Traders" *Bitcoin.com* (20 February 2018) <https://news.bitcoin.com/bangladesh-authorities-hunt-bitcoin-traders/> and C Edward Kelso "Nepal Continues Crackdown, Two More Bitcoiners Arrested" *Bitcoin.com* (6 November 2017) <https://news.bitcoin.com/nepal-continues-crackdown-two-more-bitcoiners-arrested/>.

[74] Kenneth Rapoza "Cryptocurrency Exchanges Officially Dead in China" *Forbes* (United States, 2 November 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/?ss=markets#6ff36de32a83>.

[75] Nakamoto, above n 16.

[76] Nermin Hajdarbegovic "Assange: Bitcoin and WikiLeaks Helped Keep Each Other Alive" *Coindesk* (16 September 2014) <https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive/>.

[77] Alexei Dingli and Dylan Seychell *The New Digital Natives: Cutting the Chord* (Springer, 2015) at 13, citing B Stein and D Lipsher *The Value of Human Capital in the Digital Age* (Korn/Ferry Institute, 2013). And see Wadsworth "Disruption or Distraction?", above n 69, at 12 "Replacing or modernising a core banking system is not a straightforward process for any bank. Banks with larger and more complex existing core banking systems may find it relatively more expensive and technically difficult than those banks with relatively newer systems and fewer operations."

[78] For those unfamiliar with WeChat, see this video from *The New York Times*: <https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html>.

[79] Felix Yang "Wechat's Loan Platform is Already on-par with some of the Biggest Banks in China" *Kapron Asia* (7 September 2017) <https://www.kapronasia.com/china-banking-research-category/item/889-wechat-loan-blows-retail-banking-with-rmb100-billion-loans-in-two-years.html>.

[80] Ibid.

[81] British Bankers' Association *Digital Disruption: UK Banking Report* (March 2015) at 30 <https://www.bba.org.uk/news/reports/digital-disruption-uk-banking-report/#.WwXf0yC-mUk>.

> Lots of functions that currently reside in the core platform [of British banks] do not really need to be there. … Such complexity is the result of an accumulation within banks of thousands of minor software patches and variations, sometimes over decades. Systems have evolved, but not by design, and the outcome for banks has been the creation of enormous and intractable complexity.

With blockchain technology, it is not a matter of merely making existing processes and systems more efficient, albeit that would not be the worst outcome. Instead, cryptocurrencies let us do what was not possible before. For example, if a government funds a project, whether it is building a road or foreign aid, it becomes possible to see in real time exactly where the money was spent and what is was spent on.[82] Moreover the money could be programmed so that it can be paid only to specified organisations and people. Thus it is not simply a case of having an audit trail if things go wrong; instead, wrongdoing cannot occur because money cannot be transferred to the wrong organisations or people – code can be law.[83] These things simply cannot be done with traditional systems.

Despite cryptocurrencies' potential advantages in lower transaction costs, higher speed of transactions and other benefits, such as its decentralised and thus resilient network,[84] and despite their transforming what we once thought money could do, cryptocurrencies can pose risks for consumers. These risks are explored and explained in this report.[85] In addition, the pseudonymity of bitcoin also provides a potential opportunity for criminal exploitation as demonstrated clearly in the online Silk Road, which was used inter alia for purchasing drugs.[86] Tackling the opportunities for money laundering and other crimes is one of the major concerns for authorities. However, the use of cryptocurrencies by criminals is not unique; bank notes, too, are used for purchasing illegal goods and by criminals.[87] Cash is the vehicle of choice of many criminals because to all intents and purposes it cannot be tracked or traced by those determined to avoid the government's gaze. In contrast, with bitcoin the whole audit trail is laid bare for all to see. Similarly, claims that cryptocurrencies are being used for money laundering and terrorist financing are overstated. [88] The UK Treasury in 2017 assessed the money-laundering risk for cryptocurrencies as low.[89] Terrorist financing using cryptocurrencies was also assessed as a low risk.[90] In contrast, the UK Treasury noted that "the risk of criminals seeking to launder money through UK and overseas corporate structures is

---

[82] Enrique Aldaz-Carroll and Eduardo Aldaz-Carroll "Can Cryptocurrencies and Blockchain Help Fight Corruption?" *Brookings* (1 February 2018) <https://www.brookings.edu/blog/future-development/2018/02/01/can-cryptocurrencies-and-blockchain-help-fight-corruption/>.

[83] See generally, Lessig, above n 25.

[84] Peters, Chapelle and Panayi, above n 70, at 258.

[85] See, for example, Ponsford, above n 67, at 33. One of the dangers of cryptocurrencies is cited as being potential fraud where consumers are promised high rates of return on bitcoin investments.

[86] Curiously a compelling argument has been made that the Silk Road can be seen as reducing harm. As with most online selling platforms, vendors received reviews from purchasers. The reviews on Silk Road forced vendors to compete on price and quality of goods as well as to resolve disputes quickly; thus drug users were able to purchase better quality goods without some of the dangers inherent in purchasing face-to-face. See James Martin "Lost on the Silk Road: Online drug distribution and the 'cryptomarket'" (2014) 14 Criminology & Criminal Justice 351.

[87] Financial Intelligence Unit "National Money Laundering and Terrorism Financing Risk Assessment" 2018 <http://www.police.govt.nz/sites/default/files/publications/fiu-nra-2018.pdf> 8: in New Zealand "cash remains the dominant means of transacting for domestic drug crimes. Dealers in high value goods remain vulnerable to abuse to place cash proceeds as does casino gambling." And see generally, Kenneth S Rogoff *The Curse of Cash* (Princeton University Press, Princeton, 2016) and David Wolman *The End of Money: Counterfeiters, Preachers, Techies, Dreamers--and the Coming Cashless Society* (Da Capo Press, Boston, 2012).

[88] See, for example, Samantha Chang "Bitcoin Is Wrongly Linked To Mass Money-Laundering, Says Canadian Chief Scientist" *BTC Manager* (19 April 2018) <https://btcmanager.com/bitcoin-is-wrongly-linked-to-mass-money-laundering-says-canadian-chief-scientist/>.

[89] United Kingdom HM Treasury "National Risk Assessment of Money Laundering and Terrorist Financing" (October 2017) at [5.3] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf>.

[90] Ibid.

therefore assessed to be high".[91] New Zealand may be one such jurisdiction that is assisting the laundering of money due to its laws for New Zealand-registered companies: at the time of writing the companies' beneficial owners do not need to be declared.[92] It could be argued that the situation is not as bad in New Zealand as it is in the UK as the beneficial owners of a company in New Zealand do have to be declared as a matter of routine customer due diligence (CDD) if the company is accessing financial services from a New Zealand-based or New Zealand-regulated institution.[93] However, in practice the legislation and associated tools appear not to have had the desired effect of reducing money laundering through companies. The Government has acknowledged recently that:[94]

> The current tools to access beneficial ownership information have several shortcomings:
>
> a. Beneficial ownership information is often difficult or impossible to access.
>
> b. Where information is available, it cannot always be relied upon to be accurate.
>
> c. Some existing tools can tip off criminals.

So concerned is the Government that the laws and other tools (and thus practices of professionals and others in this area) are not fit for purpose that it has recently released the Discussion Paper "Increasing the Transparency of the Beneficial Ownership of New Zealand Companies and Limited Partnerships".[95]

Another risk that some governments perceive is that if cryptocurrency use becomes widespread they will lose their ability to control money supply and will also miss out on tax revenue.[96] Granted, there is some risk to the tax base, but a properly designed system, which we advocate for in this report, may assist rather than hinder the taxation authorities. Also, there is the practical point that stopping the use of cryptocurrencies is a Sisyphean task and doomed to fail.[97]

Given the potential impacts of cryptocurrencies, should they be used widely by consumers and businesses, it has been argued that "governments are going to do everything that they can to stop [cryptocurrencies] because [they] take away their control entirely".[98] This argument, however, has

---

[91] At [9.5].

[92] Interview with investigative journalist Nicky Hager (Alex Perrottet, Morning Report, RNZ: National, 19 April 2018) "The Daphne Project: Is NZ still a tax haven?" <https://www.radionz.co.nz/national/programmes/morningreport/audio/2018641323/daphne-project-is-nz-still-a-tax-haven>. The Government is aware of the problem and the Minister for Commerce and Consumer Affairs, Kris Faafoi, stated on 19 April 2018 that it was working to introduce legislation so that beneficial owners of New Zealand companies could be identified: Interview with Kris Faafoi, Minister of Commerce and Consumer Affairs (Susie Ferguson, Morning Report, RNZ: National , 20 April 2018, "Govt not Surprised at Daphne Project Revelations – Faafoi") <https://www.radionz.co.nz/national/programmes/morningreport/audio/2018641495/govt-not-surprised-at-daphne-project-revelations-faafoi>.

[93] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 11.

[94] Ministry of Business, Innovation and Employment "Increasing the Transparency of the Beneficial Ownership of New Zealand Companies and Limited Partnerships" (Discussion Document, June 2018) [54] and see generally [54–62] <http://www.mbie.govt.nz/info-services/business/business-law/supporting-the-integrity-of-the-corporate-governance-system/increasing-transparency-beneficial-ownership-nz-companies-and-ltd-partnerships/discussion-document.pdf>.

[95] Ibid.

[96] S Gruber "Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?" (2013) 32 Quinnipiac Law Review 135.

[97] For example, despite attempts in Bangladesh to ban trading in cryptocurrencies, cryptocurrency trading is rampant. See Haig, above n 73, who reports that an internet search of where to buy cryptocurrencies in Bangladesh returns a number of websites offering to sell cryptocurrencies in that country.

[98] Ian Apperley "How Bitcoins will be really disruptive" *The National Business Review* (New Zealand, online ed, 20 May 2016). See also Anais Carmona "The Bitcoin: The Currency of the Future, Fuel of Terror" in Misty Blowers (ed) *Evolution of Cyber Technologies and Operations to 2035* (Springer, 2015) at 132, "[t]here is a concerted effort by governments and banks around the world to destroy the Bitcoin and the cyber currency movement. There is no question that banking authorities in the United States, Europe and Australia view the growing cryptocurrency ecosystem as an emerging threat."

not yet been borne out. Both the New Zealand and Australian governments, in common with numerous others around the world, recognise that cryptocurrencies offer benefits as well as potential dangers,[99] and many are working on how they will treat cryptocurrencies.[100] In Australia, the initial reception to cryptocurrencies has been positive, with the Australian Senate Economics References Committee recognising that cryptocurrencies offered opportunities as well as risks[101] and that legislation required changes so that legitimate users were not penalised for utilising cryptocurrencies instead of fiat currency.[102] In the United States an unsuccessful attempt was made in January 2015 in New Hampshire to require the state treasurer to develop an implementation plan for the state to accept bitcoin as payment for taxes and fees and for that plan to be implemented.[103] More successful were the attempts in Switzerland; in the municipality of Chiasso taxes can be paid in bitcoin and in Zug council services can be paid for in bitcoin.[104]

Not all cryptocurrencies are the same and it can be misleading to treat them as one homogenous group.[105] This report does not go through all of the hundreds of cryptocurrencies, but it does look at some of them, in particular, bitcoin. Bitcoin is the most-used cryptocurrency, and at the time of writing has the highest market capitalisation[106] and according to one commentator is the cryptocurrency that best fulfils the functions of money.[107] Albeit bitcoin is not used widely and thus has not lived up to its original promise. One vital point to remember is that while bitcoin has certain features, not all cryptocurrencies share all those features; indeed it is technically possible to create cryptocurrencies that do not suffer from some of the current limitations of bitcoin and other cryptocurrencies. This report argues that some changes may be required to cryptocurrencies for them to be permitted to operate as a new payment system. Bitcoin may well be superseded by other distributed ledger technologies in the not-too-distant future.[108]

This report does not argue that cryptocurrencies should replace current established payment systems, but rather that cryptocurrencies provide an alternative, and, at times, complementary payment system, which for the reasons the report sets out, could be highly advantageous to individuals, organisations and wider society. Moreover, for New Zealand to harness the benefits of cryptocurrencies we recommend that the RBNZ should issue its own CBDC.

Initial coin offerings (ICOs) have not been looked at in detail in this report. While the regulation of ICOs is topical, their rise came after the start of the project on which the report is based. However, a

---

[99] Wadsworth "Disruption or distraction?", above n 69, at 16.

[100] Various taxation authorities around the world have issued guidance, or partial guidance, on how they will treat cryptocurrencies, including New Zealand: see Section 6.1.1 Tax treatment below.

[101] Economics References Committee, above n 66, at [3.1].

[102] At [4.35], where it was recommended to the Government that cryptocurrencies be treated as money for the purposes of GST.

[103] New Hampshire, House Bill 552 "Requiring the state treasurer to develop an implementation plan for the state to accept bitcoin as payment for taxes and fees" <https://legiscan.com/NH/bill/HB552/2015>.

[104] Livine Sanchez "Mass adoption: Chiasso, Switzerland to Accept Tax Payment in Bitcoin" *ZyCrypto* (10 September 2017) <https://zycrypto.com/chiasso-switzerland-accept-tax-bitcoin/>.

[105] Economics References Committee, above n 66, at [2.4–2.7], where no distinction is made between the different cryptocurrencies short of stating that there are a number and most of them "were inspired by, or explicitly modelled on, Bitcoin."

[106] On 2 May 2018 Bitcoin's market capitalisation was USD 163 billion <https://coinmarketcap.com/>.

[107] Saifedean Ammous "Can Cryptocurrencies Fulfil the Functions of Money?" (Working Paper No. 92, Columbia University Center on Capitalism and Society, August 2016) <http://capitalism.columbia.edu/files/ccs/workingpage/2016/ammous_cryptocurrencies_and_the_functions_of_money.pdf>.

[108] For example, IOTA, a blockchain designed for use by IOT (Internet of Things) devices and micro payments, which uses a Tangle rather than a series of linear blocks: see Popov, above n 40. Hashgraph is another new proposed system: see Baird, above n 41 and also the Glossary.

point needs to be made that jurisdictions such as Switzerland[109] and Singapore[110] are recognised as desirable places to launch an ICO for a global investor market. In addition, the lack of clarity around the taxation of proceeds of an ICO, including the treatment of utility and security coins, makes jurisdictions which have no or low tax a lot more attractive as a place to launch ICOs from.

An additional reason why few ICOs are being attempted in New Zealand is the difficulty that anyone trying to do an ICO from New Zealand will find in securing and then keeping a New Zealand bank account. Hence the report's recommendation of action to allow those dealing in cryptocurrencies to obtain and maintain a New Zealand bank account.

2. Introduction to blockchain technology

A general introduction to blockchain technology follows. For a more detailed, technical explanation of blockchain technology see Section 2.5 below.

Before looking at the actual technology, some general points need to be made. First blockchain is regarded as the next generation of internet as it allows for the transferring of value.[111] Indeed, attempts are being made to use blockchain to replace the current internet with a new decentralised internet.[112] Cryptocurrencies are just one of myriad examples of technology being built upon blockchain.[113]

Second, as discussed in the Introduction, blockchain is just one form of distributed ledger technology (DLT). Indeed, a number of projects are designing platforms that are not blockchains: they still use the idea of a decentralised ledger but are designed to overcome the limitation of blockchain technology.[114] Third, there is a fundamental difference between the public blockchains and permissioned ones. Blockchains such as Bitcoin and Ethereum are public. This means that anyone is able to look at the transactions on the blockchain, download a copy of the blockchain and also perform work to secure the blockchain (often called mining). By contrast, in permissioned blockchains, as the name suggests, people need to be granted access to the blockchain. Prominent examples of permissioned blockchains include Hyperledger Fabric,[115] Corda,[116] and Azure.[117] A good analogy is to liken permissioned blockchains to intranets and public blockchains to the internet.[118] With intranets, companies control who has access and who sees what. With public blockchains there is no such control. Most of the work that is occurring, for example, on central bank-issued cryptocurrencies (see Section 8 Central bank-issued cryptocurrencies (CBDCs) below) is using

---

[109] Ralph Atkins "Switzerland Embraces Cryptocurrency Culture" *Financial Times* (UK, online ed, 25 January 2018) <https://www.ft.com/content/c2098ef6-ff84-11e7-9650-9c0ad2d7c5b5>.

[110] Coco Liu "Forget China: Hong Kong, Singapore are New Kids on the Blockchain" *South China Morning Post* (online ed, 23 April 2018) <https://www.scmp.com/week-asia/business/article/2142682/forget-china-hong-kong-singapore-are-new-kids-blockchain>.

[111] See, for example, Muneeb Ali "Trust-to-Trust Design of a New Internet" (PhD Thesis, Princeton University, 2017) <ftp://ftp.cs.princeton.edu/techreports/2017/003.pdf> and Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff "Internet of Things, Blockchain and Shared Economy Applications" (2016) 98 Procedia Computer Science 461.

[112] Tim Simonite "The Decentralized Internet is Here, with Some Glitches" *Wired* (United States, 3 May 2018) <https://www.wired.com/story/the-decentralized-internet-is-here-with-some-glitches/> and see Muneeb Ali, Ryan Shea, Jude Nelson and Michael J Freedman *Blockstack: A New Decentralized Internet* (Whitepaper, 16 May 2017) <https://pdfs.semanticscholar.org/606b/2c57cfed7328dedf88556ac657e9e1608311.pdf>.

[113] See, for example, "Banking Is Only The Beginning: 42 Big Industries Blockchain Could Transform" (21 June 2018) CB Insights <https://www.cbinsights.com/research/industries-disrupted-blockchain/?utm_source=CB+Insights+Newsletter&utm_campaign=dd4b870866-ThursNL_06_21_2018&utm_medium=email&utm_term=0_9dc0513989-dd4b870866-89762513>.

[114] See above nn 40–41.

[115] See <https://www.hyperledger.org/projects/fabric>.

[116] See <https://www.corda.net/>.

[117] See <https://azure.microsoft.com/en-us/solutions/blockchain/>.

[118] Thomas Mueller "Public or Permissioned Chains – What's the Best Option for Enterprises" (25 May 2017) Medium <https://medium.com/contractus/public-or-permissioned-chains-whats-the-best-option-for-enterprises-5dcf38a6d263>.

permissioned blockchains. However, things are not quite so simple. It is possible to have a permissioned version of a public blockchain: for example, Enterprise Ethereum Alliance lets enterprises run a version of the Ethereum blockchain customised to its requirements.[119] In addition, for some applications of blockchain, such as land registries, it is likely that blockchains will be hybrids: they will have features of both public and permissioned blockchains. For example, if land titles are put on the blockchain it would be desirable for there to be a registrar who places the land title on the blockchain in the first place and who can also transfer ownership to another party – for example, if a person becomes bankrupt.[120]

Permissioned blockchains enjoy certain advantages over current public blockchains. For instance, they can process many more transactions at a much higher speed than under the current technology.[121] But with advantages come disadvantages. The primary disadvantage of permissioned blockchains is that they are not as secure as public blockchains because the fewer the nodes running the system the greater the ability to hack a majority of the nodes, or the likelihood that the nodes will be combined and achieve control of the blockchain.[122]

2.1 General introduction to blockchain technology and public key cryptography

A blockchain uses public key cryptography to create a ledger that records information which, in a properly functioning blockchain, is immutable and is replicated across many computers.[123] The result is a digital record of transactions on a distributed network, thus called a distributed ledger. To reprise an earlier explanation: "Everyone has the same 'view' of the same 'data', though they may be retrieving the data from different physical sources."[124] The ledger's accuracy is confirmed by reconciling each record against all copies in existence. Transactions are grouped into blocks, and as each is verified, a new block is added to the chain of previous transactions. The time taken for verification of each block depends on the blockchain being used. For example, Bitcoin takes an average of 10 minutes for a block to be verified; in contrast, Ethereum blocks are verified about every 14 seconds.[125] As the blocks are added the blockchain is updated instantaneously on every computer that holds the ledger and is online. Thus everyone who has a copy of the up-to-date ledger will have an accurate record of the entire history of the relevant transactions.[126] The rationale for this technology is to promote efficiency and transparency across a decentralised network, omitting the need for a third-party intermediary to manage transactions. In addition, unlike many other databases, people do not have to have an entire copy of the ledger to be able to check transactions; they can do so through websites such as https://blockchain.info/.

---

[119] See <https://entethalliance.org/>.

[120] See generally, J Michael Graglia and Christopher Mellon "Blockchain and Property in 2018: At the End of the Beginning" (2018) 12 Innovations 90.

[121] Hyperledger Fabric can process more than 3,500 transactions per second: Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, ManishSethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco and Jason Yellick "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" arXiv:1801.10228 (17 April 2018) <https://arxiv.org/abs/1801.10228v1>. In contrast currently Ethereum has an estimated capacity of 20 transactions per second: Jim Manning "The Raiden Network Could Allow Instant Transactions in Ethereum" *Eth News* (5 November 2016) <https://www.ethnews.com/the-raiden-network-could-allow-instant-transactions-in-ethereum>.

[122] Duncan Jones "How to Secure 'Permissioned Blockchains'" (28 February 2018) Dark Reading <https://www.darkreading.com/endpoint/how-to-secure-permissioned-blockchains-/a/d-id/1331129>.

[123] Mainelli and Milne, above n 42, at 3.

[124] Ibid.

[125] Antony Lewis "A Gentle Introduction to Ethereum" (2 October 2016) Bits on Blocks <https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/>.

[126] Gavin Smith, Valeska Bloch, Simun Soljo and David Rountree *Blockchain Reaction: Understanding the Opportunities and Navigating the Legal Frameworks of Distributed Ledger Technology and Blockchain* (Whitepaper, Allens, 2016) <https://www.allens.com.au/general/forms/pdf/blockchainreport.pdf>.

Blockchain allows for fast transactions at low costs without third-party intermediaries.[127] For merchants, the irreversibility of transactions is also an advantage. Merchants accepting cryptocurrencies, unlike credit card payments, are not exposed to the risk of charge-backs.[128] Moreover, consumers are arguably better protected than when they use credit cards. When consumers pay by credit card they hand over information, such as the credit card number, expiry date and CCV number, that can be used by the receiver or anyone else who obtains that information to make additional purchases. Credit card information can be likened to the key to the door of a house: whoever has a copy of the key can enter the house as they wish until the lock is changed. Granted, with a credit card if the key is used fraudulently the "home owner" will be recompensed by the credit card company, but it is often the merchants who were victims of the fraud who bear the cost. Contrast the situation with cryptocurrencies: while the owner will hand over one key (the public key) to make or receive a payment, that key will not open the door. The door can only be opened if the owner discloses their private key, which they do not need to do to make or receive payment. Nevertheless, for convenience sake some people do disclose their private keys to third parties.[129]

The public key can also be explained by likening it to a bank account number. Merely being in possession of a bank account number, such as by reading the account number which a business includes on its invoices, does not let the possessor withdraw the money from the account. In this analogy, the possession of a public key only allows them to pay money into that account. For a person to withdraw money from the account they need the password (and possibly other information) of the bank account holder; that password is therefore more akin to the private key. Unlike a bank account number, however, if a person knows the public key that person can see all the transactions ever made to and from that public key as well as the current balance it controls.

Some people are quite rightly worried about the lack of privacy afforded by public keys. For example, if you were paid in bitcoin and in turn paid your landlord in bitcoin, the landlord would be able to find out how much you were paid, and to raise the rent if you had a pay increase.[130]

---

[127] Lam and Kuo Chuen, above n 53, at 22–23.

[128] At 23. A charge-back occurs where a payment made to a merchant is reversed because the transaction was fraudulent. Thus even if the merchant was innocent and had no idea that the credit card was being used fraudulently the merchant bears the loss from the fraudulent use.

[129] Private keys are sometimes disclosed to cryptocurrency exchanges. The advantage for the consumer is that they can use a password to access their cryptocurrency and if they forget their password the exchange will reset it. But providing the cryptocurrency exchange with the private key leaves the consumer susceptible to the exchange being hacked or losing the cryptocurrency in other ways.

[130] In practice landlords have been known to raise rents when they realise that their tenants are receiving more income. When student allowances were raised in New Zealand in 2018 some landlords put up the rent: see Henry Cooke "Student Allowance Boost Blamed for Rent Spikes" *Stuff* (New Zealand, online ed, 11 January 2018) <https://www.stuff.co.nz/national/politics/100485600/student-allowance-boost-blamed-for-rent-spikes>.

2.2 The value of blockchain technology beyond cryptocurrencies

Like one of the authors of this report, some people believe that blockchain has the potential to be as transformative as the internet,[131] if not more.[132] Albeit not all commentators believe that blockchain's effects will go beyond cryptocurrencies:[133]

> After eight years and millions of users, it is safe to say his [Satoshi Nakamoto's] design has succeeded in producing digital cash, and, unsurprisingly, nothing else. This digital cash can have commercial and digital applications, but it is not meaningful to discuss blockchain technology as a technological innovation in its own right with applications in various fields.

Views like this one are in the minority. As Jeremy Wilson, Barclays' Vice Chairman, says, speaking for the majority, "[blockchain] will change not just finance, but the lives of everyone".[134] The UK's Financial Conduct Authority (FCA) released its discussion paper on DLT in April 2017.[135] (The UK Government has chosen to use the term "distributed ledger technology" rather than "blockchain".) The FCA's discussion paper noted that the 24 months prior to April 2017 had seen industry efforts to investigate DLT, and it was not until the second half of 2017 and into 2018 that actual use cases would begin to appear.[136] Indeed, in January 2016 the UK Government's Chief Scientific Adviser, Sir Mark Walport, released a major report stating that DLT could transform how public services are delivered and boost productivity.[137] In a second report, this time by the UK House of Lords,[138] blockchain was identified as potentially assisting the Government in many areas including:

- border control, customs, trade and immigration;
- national security, criminal investigations, police and public safety;
- taxation and benefits payments;
- health assurance, patient record management, drug safety and treatment accountability;
- food standards and safety, traceability and accountability;
- privacy, cybersecurity and counter-fraud; and
- public procurement, contracting, payments, visibility of spending and asset traceability.

Banking payments and transactions have been touted as one of the most promising uses for blockchain technology. Blockchain technology may allow banks and other financial institutions to improve their transactional efficiency by minimising the high transfer costs usually associated with financial exchanges, especially cross-border payments. For a start it removes the need to use foreign exchange. Conversion is only needed, after the event, if the holder wants another currency for some

---

[131] Daniel Lanyon "New Research Reveals the IT Crowd are Expecting Huge Change from Blockchain Technology" *Alt Fi* (23 April 2018) <http://www.altfi.com/article/4334_blockchain-will-be-as-transformative-as-the-internet>.

[132] See generally, Michael J Casey and Paul Vigna *The Truth Machine: The Blockchain and the Future of Everything* (Harper Collins, 2018); Vigna and Casey *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order*, above n 62; Dan Tapscott and Alex Tapscott *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World* (Penguin Random House, 2016) and Alex Sims "Forget Bitcoin, Blockchain Technology is Much Bigger" *Stuff* (New Zealand, online ed, 17 December 2017) <https://www.stuff.co.nz/business/opinion-analysis/99905784/forget-bitcoin-blockchain-technology-is-much-bigger>.

[133] Saifedean Ammous "Blockchain Technology: What is it Good for?" (Working Paper No. 91, Columbia University Center on Capitalism and Society, 8 August 2016) at 5. <http://capitalism.columbia.edu/files/ccs/workingpage/2016/ammous_blockchain_technology_.pdf>.

[134] Lynsey Barber "Is Blockchain a 'New Operating System for the Planet'? Barclays Vice Chairman Jeremy Wilson Thinks so" *CityAM* (25 January 2017) <http://www.cityam.com/257805/blockchain-new-operating-system-planet-barclays-vice>.

[135] Financial Conduct Authority "Discussion Paper on Distributed Ledger Technology" DP17/3 (April 2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>.

[136] Ibid.

[137] United Kingdom Government Chief Scientific Adviser, above n 15.

[138] United Kingdom House of Lords "Distributed Ledger Technologies for Public Good: Leadership, Collaboration and Innovation" (November 2017) <http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf>.

reason. Blockchain technology offers a solution where transactions can be approved more quickly and accurately without multiple intermediaries.

The potential value of blockchain technology is significant in the financial sector because it offers the opportunity for financial institutions to trade and transfer digital assets in minutes, even seconds, rather than days. For example, it could transform the record-keeping and transfer procedures associated with securities transactions. Currently, the clearing and settlement process in Australia is slow (requiring two business days to settle – three until quite recently) and involves intermediaries.[139] Blockchain technology has the potential to allow for quicker settlement and improved integration with other systems, lowering costs to all parties involved. In December 2017 the Australian Securities Exchange (ASX) announced that after two years of trials it would replace its registry, settlement and clearing system with blockchain technology.[140] At the same time, blockchain's accuracy may also assist with records of ownership, and hence could be used by custodians.[141] That said, other systems can and are being used to achieve near-real-time settlement systems without resorting to blockchain.[142]

Blockchain technology has been projected to provide USD 11–12 billion in global cost savings from cash securities by cutting settlement times and reconciliation costs. Another prediction is that the technology is capable of reducing the global banking industry's operating costs by USD 20 billion a year.[143] In Australia, ASX's advisors have estimated that the use of blockchain for equities post trade could result in annual savings of AUD 4–5 billion for end users.[144] These figures show that the potential saving is the subject of some debate. Another estimate is that "banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance" will be reduced by between USD 15 and 20 billion by 2020.[145]

But blockchain has moved beyond mere promises. The ASX has not simply recognised blockchain's potential, it has already started building a system using blockchain to replace its Clearing House Electronic Sub-register System (Chess).[146] ASX is the first exchange that has made such a move. In doing so it has surprised at least one participant in the industry, albeit the same participant stated that "when the technology becomes available you have to embrace it".[147] IBM, in conjunction with ANZ and Westpac, has developed a blockchain solution for bank guarantees for commercial property leases.[148] Bank guarantees for commercial leases in Australia use a paper-based system that is extremely inefficient. A trial using blockchain was successful and demonstrated that blockchain could

---

[139] ASX "How Settlement Works" <https://www.asx.com.au/services/settlement/asx-settlement/how-settlement-works.htm>.

[140] "Australia's ASX Selects Blockchain to Cut Costs" *Reuters* (7 December 2017) <https://www.reuters.com/article/us-asx-blockchain/australias-asx-selects-blockchain-to-cut-costs-idUSKBN1E037R>.

[141] Nick Ayton "Global Custody Is About to Face Its Nemesis: Blockchain" *Innovation Enterprise* (15 August 2017) <https://channels.theinnovationenterprise.com/articles/global-custody-is-about-to-face-its-nemesis-blockchain>.

[142] Euroclear "Streamlined Real-time Settlement Euroclear UK & Ireland's CREST system" <https://www.euroclear.com/dam/PDFs/Settlement/EUI/MA2740-CREST-settlement.pdf>.

[143] Smith, Bloch, Soljo and Rountree, above n 126.

[144] Goldman Sachs *Profiles in Innovation Putting Theory into Practice* (24 May 2016) <https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf>.

[145] See also Santander InnoVentures, Oliver Wyman and Anthemis Group *The Fintech 2.0 Paper: Rebooting Financial Services* (2016) <https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf>. See further Mainelli and Milne, above n 42.

[146] "ASX to Use Blockchain to Handle Share Transactions" *The Sydney Morning Herald* (Australia, online ed, 7 December 2017) <https://www.smh.com.au/business/banking-and-finance/update-1-australias-asx-selects-blockchain-to-cut-costs-20171207-p4yxhe.html>.

[147] Ibid.

[148] Chris Pash "ANZ and Westpac just successfully used blockchain on commercial property deals" *Business Insider Australia* (10 July 2017) <https://www.businessinsider.com.au/anz-and-westpac-just-successfully-used-blockchain-on-commercial-property-deals-2017-7> and Hari Janakiraman, Rodolf Salem and Chris T'en "Why bank guarantees need blockchain", Blue Notes, ANZ (11 July 2017) <https://bluenotes.anz.com/posts/2017/07/why-bank-guarantees-need-blockchain>.

move the manual paper-based model into the digital era and lift efficiency for all parties involved.[149] ANZ has recently also released details of its proof of concept using blockchain technology for insurance. This allows both insurance companies and brokers to see the same information at the same time, and removes the need for information to be re-entered (incurring the inevitable mistakes), with reconciliation between the different parties' databases all looking at the one source of information.[150]

Due to its versatility, blockchain technology also has the potential to operate in many fields. Indeed, it is hard to see an industry that it could not be applied to. For example, the possibility of an energy blockchain has been raised.[151] Sony has started to develop blockchain technology in educational infrastructure to make programs and data damage- and tamper-proof.[152] The accuracy and sophistication associated with blockchain technology makes its application to record keeping promising, not only in relation to government records but for the protection of intellectual property rights.

2.2.1 Smart contracts

More recently, Ethereum (the rival blockchain and cryptocurrency to Bitcoin) has allowed for the programming of smart contracts – self-executing contracts – which may be able to be used for simple, highly repeatable transactions such as conveyancing and insurance. Smart contracts may eventually lead to the demise of drafting and exchanging paper contracts, albeit the replacement of all written contracts by smart contracts is a long way off. Following Ethereum's lead, a number of other platforms that allow smart contracts to be deployed have also been developed.[153]

The term "smart contracts" is, however, a misnomer. Not all smart contracts are contracts:[154] for example, a smart contract can be used so that a car would only open and start for the owner of the car.[155] Nor are they necessarily smart: mistakes in coding can have disastrous consequences.[156] Smart contracts are simply self-executing computer programs: If X occurs then do Y. For example, Alice could buy a car online from Bob.[157] The smart contract can be coded so that Bob will receive the money only after the car passes an emission test and it has been delivered. The shipping agent and the emission-testing agent verify the car has been delivered and the car has passed the test, and the money is then

---

[149] ANZ, Westpac and IBM *Distributed Ledger Technology and Bank Guarantees for Commercial Property Leasing* (Whitepaper, July 2017) <https://bluenotes.anz.com/content/dam/bluenotes/documents/whitepaper%20_bank_guarantees_dlt_poc.pdf>.

[150] ANZ *Distributed Ledger Technology for Reconciliation between Insurance Companies and Brokers* (Whitepaper, April 2018) <https://www.anz.co.nz/resources/f/d/fd397495-8c57-41e0-b9b6-9c51b410a8b8/Distributed-Ledger-Technology.pdf?MOD=AJPERES>.

[151] Stephen Lacey "The Energy blockchain: How Bitcoin Could be a Catalyst for the Distributed Grid" *GreenTech Media* (26 February 2016) <https://www.greentechmedia.com/articles/read/the-energy-Blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid>.

[152] Luke Parker "Sony Launches Blockchain-based Educational Infrastructure Project" (23 February 2016) Brave New Coin <http://bravenewcoin.com/news/sony-launches-Blockchain-based-educational-infrastructure-project/?utm_source=BNC+Newsletter&utm_campaign=89eb421dd5-BNC_Weekly_News_Highlights_26_Feb_2016&utm_medium=email&utm_term=0_83439a8472-89eb421dd5-245125889>.

[153] The blockchains which allow the use of smart contracts include: EOS <https://eos.io/>; NEO <https://neo.org/>; NEM <https://nem.io/>; Lisk <https://lisk.io/>; NXT <https://nxtplatform.org/>; Qtum <https://qtum.org/en/>; RootStock <https://www.rsk.co/> and Tezos <https://www.tezos.com/>.

[154] Max Raskin "The Law and Legality of Smart Contracts" (2017) 1 Georgia Law Technology Review 305.

[155] Nick Szabo "The Idea of Smart Contracts" (1997) Nick Szabo's Papers and Concise Tutorials <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html>.

[156] The spectacular downfall of The DAO, which contained software errors, demonstrates how smart contracts can be dangerous. See, for example, Quinn DuPont "Experiments in Algorithmic Governance: A History and Ethnography of 'The DAO', a failed Decentralized Autonomous Organization" in Malcolm Campbell-Verduyn (ed) *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance* (Routledge, 2018).

[157] This example has been taken from Marten Nelson "What is Programmable Money?" *Payments Journal* (23 March 2017) <http://paymentsjournal.com/What-Is-Programmable-Money/?/>.

transferred to Alice. One of the strengths of using a smart contact is that Alice will be required to pay the money "to the smart contract", but the smart contract pays out only to Bob when the shipping agent and the tester agree the conditions have been met. If, for example, the car fails the emission test the smart contract will have been coded so that the money is returned to Alice.

To be sure, the Alice and Bob example looks similar to a third party holding the money in escrow, which is a common commercial practice. But a traditional escrow arrangement requires a third party to be paid to hold the funds and receive notification from one or more people that conditions have been met before the amount is paid out. Also, the parties to the agreement run the risk of the third party unlawfully taking the money or becoming insolvent. With a smart contract there is no risky third party to contend with. However, there remains a potential risk with the use of oracles (agents that find and verify things that happen in the real world) because the information they provide may be compromised. For example, a farmer may have insurance for low rainfall, with the information being taken from a variety of websites. Those websites may be hacked and thus the information may be incorrect.[158] Certainly, it would be hard to design a system that is 100 per cent accurate (indeed, it is hard to think of any existing system outside blockchain that is 100 per cent accurate), so dispute resolution is a key part of the blockchain ecosystem and a number of projects are in fact working on providing dispute resolution.[159]

Smart contracts are being used or are planned to be used in a wide range of situations. The secure storing and retrieval of patient health data,[160] clinical trials,[161] auditing,[162] sale and purchase of land,[163] decentralised autonomous organisations[164] and electronic voting (for local government, central government and even companies and other organisations)[165] are just some of the developing and potential applications of blockchain technology.[166] Moreover, health and safety could be

[158] Delphi "The Oracle Problem" (15 July 2017) Medium <https://medium.com/@DelphiSystems/the-oracle-problem-856ccbdbd14f>.

[159] See, for example, Kleros <https://kleros.io/> and Jury.Online <https://jury.online/> and see Aragon <https://aragon.one/>.

[160] See, for example, Proof Work <https://proof.work>.

[161] Timothy Nugent, David Upton and Mihai Cimpoesu "Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts" (20 October 2016) Version 1 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5357027/>.

[162] Chartered Professional Accountants of Canada and the American Institute of CPAs "Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession" (2017) <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf>.

[163] Shefali Anand "A Pioneer in Real Estate Blockchain Emerges in Europe" *Wall Street Journal* (United States, online ed, 6 March 2018) <https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601?mod=searchresults&page=1&pos=3> reporting that Sweden is preparing to conduct its first blockchain property transaction after two years of testing.

[164] Ellie Rennie and Jason Potts "The DAO: A Radical Experiment that could be the Future of Decentralised Governance" *The Conversation* (Australia, 11 May 2016) <https://theconversation.com/the-dao-a-radical-experiment-that-could-be-the-future-of-decentralised-governance-59082>; Vitalik Buterin "Bootstrapping A Decentralized Autonomous Corporation: Part I" *Bitcoin Magazine* (19 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/>; Vitalik Buterin "Bootstrapping An Autonomous Decentralized Corporation, Part 2: Interacting With the World" *Bitcoin Magazine* (21 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-an-autonomous-decentralized-corporation-part-2-interacting-with-the-world-1379808279/> and
Vitalik Buterin "Bootstrapping a Decentralized Autonomous Corporation, Part 3: Identity Corp" *Bitcoin Magazine* (24 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-3-identity-corp-1380073003/>.

[165] See, for example, <https://horizonstate.com/>; <https://polys.me/> and John Biggs "Sierra Leone just ran the first blockchain-based election" *TechCrunch* (15 March 2018) <https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/>.

[166] Kurt Fanning and David P Centers "Blockchain and Its Coming Impact on Financial Services" (2016) 27(5) Journal of Corporate Accounting & Finance 53, at 57; Aaron Wright and Primavera De Filippi "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015) <https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2580664> at 10–17; Lewis Cohen and David Contreiras Tyler and Pamela Buxton "Blockchain's Three Capital Markets Innovations Explained"

revolutionised through the use of smart contracts.[167] For example, an employer may only want a machine to be operated by people who have had the requisite training. A biometric lock could be placed on the machine (for example, both fingerprints and facial recognition). Only approved persons could then use the machine.[168] Granted, that technology exists and an argument can be made that no blockchain is required. However, it would be possible for skilled people to hack into a system based on such existing technology, override the electronic codes and let unauthorised people operate the machine. With blockchain, the smart contract could not be changed by the hacker. Also, the smart contract could be set up so that new training certificates for people are uploaded automatically to the smart contract, which would save on administrative time and cost. Moreover, it would mean that the employer and others could see instantly those people who are authorised to operate the machine – which is not necessarily the easiest thing to do with current systems. When employees cease to be employed their authorisation is cut automatically. The smart contract could also be programmed to book training for people whose certificates are about to expire.

Insurance is an obvious example where smart contracts can and are being deployed, for example, flight insurance for delayed and cancelled flights that enables 100 per cent automated insurance.[169] The smart contract can be connected to global air traffic databases that monitor flights, so that if the insured flight is delayed by over two hours compensation is paid automatically. Similarly, smart contracts can be set up for life insurance policies so that when a death certificate is issued the payment is made automatically.[170]

While smart contracts can reduce costs significantly by eliminating the need to produce invoices and people can be paid in real time, there are, however, limitations.[171] For example, often contracts are breached, yet the breach is minor, such as a payment to a landlord being made one hour late. The innocent party will not normally want to take the steps it is entitled to under the contract, like evicting the tenants. Likewise the innocent party in a smart contract would most likely not want the consequences of the breach to be triggered immediately after the payment was missed: for instance, freezing the locks on the doors and so preventing the tenants entering the property.[172] One way around this is to programme the smart contract to send an alert to the innocent party advising them that payment has not occurred and letting them decide whether to allow the smart contract to run as programmed – in this case freezing the door locks.

One common concern in smart contracts is who bears liability if a mistake is made in the code; for example, if money paid into the smart contract is now frozen and neither party can recover the money. However, traditional legal doctrines cover such situations, which include negligence, mistake and unjust enrichment. To be sure, if the parties to the smart contract are pseudonymous or anonymous there will be difficulties in ascertaining their identity, but most people in commerce will want to use

(2016) 35(26) International Financial Law Review; and Pierre Noizat "Blockchain Electronic Vote" in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 453. See also Melanie Swan *Blockchain: Blueprint for a New Economy* (O'Reilly, 2015).

[167] Alexandra Sims "How Smart Contracts Could Radically Transform Health and Safety" *The National Business Review* (New Zealand, online ed, 24 February 2017).

[168] Arthur Falls "BHP, Tracking the Most Valuable Rock on Earth" (Podcast, 18 October 2016) The Ether Review <https://etherreview.info/tagged/podcast>.

[169] Samburaj Das "AXA Uses the Public Ethereum Blockchain for Flight Delay Insurance" *Cryptocoins News* (22 September 2017) <https://www.cryptocoinsnews.com/axa-uses-ethereum-blockchain-flight-delay-insurance/>.

[170] Srinivasa Siriyanna "Blockchain Smart Contracts in Insurance" (4 January 2017) Infosys <http://www.infosysblogs.com/blockchain/2017/01/blockchain_smart_contracts_in_.html>.

[171] See generally, Eliza Mik "Smart Contracts: Terminology, Technical Limitations and Real World Complexity" (2017) 9 Law, Innovation and Technology 269 and Kevin D Werbach and Nicolas Cornell "Contracts Ex Machina" (2017) 67 Duke Law Journal 313.

[172] This scenario would use smart locks. See Cat Johnson "4 Revolutionary Smart Locks that Decentralise and Automate Asset Sharing" *Shareable* (1 December 2015) <https://www.shareable.net/blog/4-revolutionary-smart-locks-that-decentralize-and-automate-asset-sharing>.

their real names.[173] If people choose to deal with parties who are pseudonymous or anonymous that is the risk they take. Indeed, many projects are working on digital identity as it is key to being able to use blockchain to its full extent.[174] As highlighted above, the issue of dispute resolution is another key aspect of blockchain and a number of blockchain platforms are being built specifically for resolving disputes.[175]

2.3 How banks and other financial institutions are using/exploring blockchain technology

A number of financial institutions have started trialling the feasibility of blockchain technology. However, it is interesting to note that observers such as Michael Mainelli (Emeritus Professor of Commerce at Gresham College in the UK) and Leda Glyptis (a director of Sapient Global Marketing, a technology marketing and consulting company) describe this move as motivated by fear. In Mainelli's words, "banks are on the cusp of change, but sadly what is driving them into this space is fear".[176] Glyptis agrees: "in the past year we have seen the industry move from panic and disbelief to realisation that the technology is real and very powerful".[177]

Mainelli and Glyptis also note that the limits of blockchain technology are still unknown (and its scope still unclear), and warn that financial institutions should not take too narrow a view of the uses to which blockchain can be put in financial services.[178]

2.3.1 New Zealand and Australia

In Australia, financial institutions have also become drawn to blockchain technology because of its perceived ability to increase profits. The technology has the ability not only to enhance efficiency over existing systems (such as the ASX investigating whether blockchain could be used to replace its settlement and clearing systems),[179] but to replace human workers when it comes to transaction verification.[180]

Australian financial institutions are supportive of the technology for efficiency maximisation. Commonwealth Bank, NAB, Macquarie Bank and Westpac, along with 30 of the world's largest banks, have been part of a blockchain project that will permit banks to send information to each other.[181] The former Governor of the Reserve Bank of Australia (RBA), Glenn Stevens, is also supportive of Bitcoin and blockchain technology, drawing parallels with Uber and Airbnb.[182] Stevens emphasises that conducting business using new technology does not necessarily make it any riskier than doing it in old-world models.[183] Financial institutions, however, are more concerned with the emergence of

---

[173] A key part of blockchain is creating digital identities for people, organisations and things which are a lot more secure than the current identification forms that are used.
[174] The projects include: Sovrin <https://sovrin.org/>; Civic <https://www.civic.com/>; Uport <https://www.uport.me/>; and Single Source <https://www.mysinglesource.io/>. And see World Economic Forum, above n 30.
[175] See above n 159.
[176] Helen Thompson "Imagine the Trust: the Role of Blockchain in Financial Services" *Coindesk* (27 February 2016) <https://www.coindesk.com/imagining-the-role-of-blockchain-in-financial-services/>.
[177] Ibid.
[178] Ibid.
[179] Jessica Sier "ASX Working on Industrial Strength Blockchain Platform" *The Sydney Morning Herald* (Australia, online ed, 28 September 2016) <http://www.smh.com.au/business/markets/asx-working-on-industrial-strength-Blockchain-platform-20160927-grp9gu.html>.
[180] Sarah Murray "Blockchain can Create Financial Sector Jobs as well as Kill them" *Financial Times* (UK, online ed, 7 September 2016) <https://www.ft.com/content/3a9ef8d8-33d5-11e6-bda0-04585c31b153>.
[181] Jessica Sier "CBA Joins Global Banks in Project to Explore Bitcoin Model" *The Australian Financial Review* (online ed, 16 September 2015) <http://www.afr.com/technology/cba-joins-global-banks-in-bitcoin-research-20150916-gjo40b>.
[182] Paul Smith "RBA Governor Glenn Stevens Backs Blockchain and Tech Disruptors" *The Australian Financial Review* (online ed, 16 December 2015) <http://www.afr.com/technology/rba-governor-glenn-stevens-backs-Blockchain-and-tech-disruptors-20151215-glnsnm#ixzz4SbQw5ON3>.
[183] Ibid.

bitcoin and its decentralised and pseudonymous nature, rather than blockchain technology, because of compliance issues with anti-money laundering (AML) and counter-terrorism financing laws (CFT).[184]

2.3.1.1 Views from Westpac

Michael Southwell, Director of Payments – Global Transaction Services at Westpac, has identified several key issues in assessing the potential, applicability and capability of blockchain technology as regards Westpac:[185]

> *If the solution requires a distributed or centralised ledger* – much of the focus on crypto currencies and Blockchain is the distributed nature of the ledger. However, in many cases a ledger does not need to be distributed (it would be more efficient to keep it centralised, as most ledgers today are). De-centralised ledgers are more resilient, but resiliency often isn't necessarily the most important attribute.
>
> *If the solution operates in a trustless environment; or if a strong degree of trust is already established between participants* – this comes down to determining whether or not the readers and writers to the ledger are trusted. For example, with Bitcoin there is no trusted counterparty, which then requires a lot of time and effort from the de-centralised network to figure out how to reduce or eliminate fraud. Whereas with a permissioned ledger, participants would know who the counterparty is and have trust, making processing more efficient.
>
> *If there is any economic advantage adding information on Blockchain* – determining how the technology would be more efficient than existing solutions, or produce a greater economic incentive than other solutions in the market. This last consideration can have the biggest influence on applicability of potential solutions, because if there is no additional money to be saved or made, there is very little reason for participants to change their behaviour.

Southwell also noted that it was unclear whether today's generation of cryptocurrencies such as bitcoin would be sustainable in the long term:[186]

> Crypto currencies like Bitcoin can be seen as a commodity because they're mined, you have to consider the cost of production and remaining Bitcoin "reserves" into the price. At the same time, they can also be seen as a fiat currency, as they don't have any intrinsic asset backing them. There's no gold standard sitting behind Bitcoin, for example.
>
> So, when you look at it from that perspective, you have the volatility of the commodities market and the cost of producing the commodity on one hand; while on the other hand you have the volatility of a currency that's not really tied to a defined monetary policy or central bank.

Nevertheless, Westpac has been investigating how blockchain technology can benefit its customers, forming an internal think tank and hosting a Blockchain Design Challenge.[187]

2.3.1.2 Views from ANZ

Nick Groves, Executive Manager, Group Strategy at ANZ, has stated that ANZ recognises blockchain as an exciting trend and that the bank's foray into blockchain capability revolved around two considerations: how it could meet the quality requirements of banks and the potential uses that could

---

[184] Jessica Sier, above n 181. This report predominantly uses the abbreviation CFT, standing for Counter Funding Terrorism, rather than CTF, which stands for Counter Terrorism Funding. As below at 746, somewhat confusingly Australia (and some other countries) use the term "AML/CTF"; in New Zealand the term "AML/CFT" is used.

[185] Michael Southwell "Assessing Blockchain Capabilities at Westpac" (paper presented to the Blockchain Summit, Melbourne, 2016) at 45 <https://www.linkedin.com/pulse/preparing-blockchain-innovation-australias-major-banks-jared-haube/>.

[186] Ibid.

[187] At 45.

be made of it.[188] ANZ has taken a lead role in two projects: SWIFT GPII, a global payments innovation initiative, and the Linux Foundation's Hyper Ledger Project, an open source project aimed at advancing blockchain technology for transaction recording and verification. Groves noted that ANZ was less interested in Bitcoin as an open public system designed to facilitate pseudonymous participants because it was not designed with banks in mind. Banks do not operate in open networks, but in networks of known and registered participants. ANZ's focus was therefore on permissioned blockchain technology, and in 2016 it was reviewing its capability from a back-end (internal) perspective (rather than the front-end customer-facing perspective), as ANZ sees the back-end area as a place where the technology can be examined and tested safely.[189]

2.3.2 Internationally

Banks have been exploring the potential uses of blockchain technology for a number of years. The following table contains a list of global banks and their investments in the technology at 18 August 2015.[190]

Fidor Bank	Fidor was the first major bank to experiment with cryptocurrency and blockchain. It partnered with Kraken, a cryptocurrency exchange (in October 2013) to provide a digital currency exchange in the EU and with Bitcoin Deutschland GmbH in Germany. This was followed by a partnership with Ripple Labs to use its payment protocol to provide customers money transfer services in multiple currencies at a lower cost (May 2014). In February 2015, it partnered with bitcoin.de, a peer-to-peer bitcoin trading platform.
LHV Bank	Expressed it was working on a new project with blockchain technology (June 2014). Developed Cuber Wallet, an app based on Colored Coins blockchain technology (June 2015). Partnered with Coinbase (September 2014) and CoinFloor (July 2015). It is also experimenting with digital security.
CBW Bank, Cross River Bank	Announced partnership with Ripple Labs (September 2014). Working on building a risk-management system, and also to provide low-cost cross-border payment transactions.
Rabobank	Experimenting with bitcoin, blockchain and Ripple payments network.
ABN Amro	Investigating blockchain technology for banking purposes.
ING Bank	Researching Blockchain with the aim to improve the speed of transactions.
Goldman Sachs	Participated as a lead investor with USD 50m funding for Bitcoin startup Circle Internet Financial Ltd (April 2015).
BBVA Ventures	Released a research report in July 2015 stating interest in blockchain technology. Participated in a USD 75m Series C funding for Coinbase (January 2015).
Santander	Claims to have 20–25 use cases for blockchain and that around £12 billion could be saved in bank infrastructure by switching to the blockchain concept. Set up team Crypto 2.0 to research the use of blockchain in banking with a specific focus on international payments and smart contracts (June 2015).

[188] Nick Groves "Exploring Bank-grade Blockchain Technology at ANZ" (presented to the Blockchain Summit, Melbourne, June 2016) at 78.
[189] Ibid 78.
[190] Amit Goel "Bank-Wise Analysis of Blockchain Activity" *Medici* (18 August 2015) <https://gomedici.com/bank-wise-analysis-of-blockchain-activity/>. Table is adapted from list in the article.

Westpac	Partnered with Ripple and is pilot testing a proof of concept with its staff for making low-value cross-border payments (June 2015). Through its investments in venture capital fund Reinventure, it participated in Series C funding of AUD 75m in Coinbase (January 2015).
UBS	Has a research lab in London focused on blockchain. UBS CIO Oliver Bussmann also provides one-on-one mentoring to fintech start-ups based out of London in the areas of blockchain and social media analytics. The firm is experimenting in the areas of payments, trading and settlement, and smart bonds (April 2015).
BNY Mellon	Created own currency called BK Coins as a corporate recognition programme that can be redeemed for gifts and other rewards (April 2015).
Barclays Bank	Ran a 90-day accelerator programme with Safello (Bitcoin Exchange), Atlas Card (Bitcoin debit cards creator) and Blocktree (blockchain for the insurance industry) in March 2015. In June 2015, signed a deal with Safello to work on proof of concepts for testing banking services on blockchain.
Commonwealth Bank	Partnered with Ripple Labs to implement blockchain ledger system for payment settlements between its subsidiaries (May 2015).
USAA Bank	Created a research team to study uses of bitcoin (May 2015).
ANZ Bank	Partnered with Ripple to explore potential use cases of blockchain (June 2015).
BNP Paribas	Experimenting with making transactions faster by using blockchain (July 2015).
Société Générale	Planning to equip employees with bitcoin, blockchain and cryptocurrency expertise (July 2015).
Citibank	Set up three separate systems within Citi that deploy blockchain-based distributed technologies. It developed an equivalent to bitcoin called Citicoin, which is being used internally to understand the digital currency trading system better. Blockchain is one of five domains that Citi is exploring to digitise payments and transactions with a specific focus on cross-border capacity (July 2015).

In the intervening years many banks around the world have begun work on blockchain, with Japan's MUFG, its largest bank, set to release its MUFG coin in 2018.[191] Initially, however, the banks formed consortiums to investigate the use of blockchain and payments.

2.3.2.1 The Utility Settlement Coin Project

Four of the largest banks in the world[192] formed the Utility Settlement Coin Project to investigate facilitating monetary transactions though blockchain technology.[193] Subsequently other large banks such as Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC and State Street also

[191] Mathew Tompkins "Japan's Largest Financial Group to Launch Own Virtual Currency" *Bitcoinist* (16 January 2018) <http://bitcoinist.com/japans-largest-financial-group-launch-virtual-currency/>.
[192] Swiss Bank UBS, BNY Mellon, Deutsche Bank and Santander. In addition there is the broker ICAP and the technology company Clearmatics: see Jemima Kelly "UBS Leads Team of Banks Working on Blockchain Settlement system" *Reuters* (24 August 2016) <http://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147>.
[193] Ibid.

joined.[194] Swiss Bank UBS initiated the project in September 2015 when it created an innovation lab to explore the viability of using blockchain technology within the finance sector.[195] UBS published a Whitepaper *Building the Trust Engine* in 2016.[196] Among other things, UBS identified that it would be advantageous for the finance sector to explore the possibility of making use of blockchain technology given that it is "a potentially transformative technology that will leave as deep a mark on our world over the next twenty years as the internet has over the last twenty".[197]

Although individual banks have previously initiated similar investigations, the Utility Settlement Coin Project is the first joint project involving major players in the finance industry.[198] The commercial launch of the technology was expected to occur in early 2018, albeit restricted to low-risk transactions.[199] Between 2019 and 2021 it is envisaged that a full roll-out of the service will take place.[200]

Utility Settlement Coins, unlike bitcoin, are a digital form of existing prominent fiat currencies such as the Euro and the US dollar.[201] The value of Utility Settlement Coins will be at parity with the fiat currencies.[202] Axel Lehmann, the CEO of UBS, argues that the fact Utility Settlement Coins are linked to fiat currencies will ensure widespread adoption within the finance sector.[203] The project has as its imperative the streamlining of transactions by authenticating transactions electronically.[204] Costs the banks currently incur in facilitating transactions are expected to reduce by approximately USD 65 to 80 billion per annum.[205] Thus for example, Julia Faura, Head of Research and Development at Santander, stresses that the large office spaces retained by banks primarily exist for the purposes of processing and authenticating interbank transactions using traditional methods.[206] Although banks were concerned initially about blockchain technology being used for fraudulent purposes, they have now begun to explore the technology to determine the extent to which it can reduce their expenditure.[207] According to Lehmann, it is expected that bank staff now employed to process transactions via traditional methods would instead be diverted to focus on "service, needs and relationships".[208]

Banks have realised that if blockchain technology is used for banking transactions it could reduce the time required to process transactions. When using traditional methods, these can take several days,[209]

---

[194] "Six Big Banks Join Blockchain Digital Cash Settlement Project" *Reuters* (31 August 2017) <https://www.reuters.com/article/us-blockchain-banks/six-big-banks-join-blockchain-digital-cash-settlement-project-idUSKCN1BB0UA>.

[195] Yolanda Redrup "UBS Invests Big in Blockchain Future" *The Australian Financial Review* (online ed, 3 October 2016) <http://www.afr.com/technology/ubs-invests-big-in-blockchain-future-20160926-groidr>.

[196] Alex Batlin, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka and Shane Williams *Building the Trust Engine* (Whitepaper, UBS, 2016) <https://www.ubs.com/microsites/blockchain-report/en/home.html?hootPostID=6d427ec622fb4f862bcab7bb4a960870> at 10.

[197] At 5.

[198] Kelly, above n 192.

[199] Martin Arnold "Big Banks Plan to Coin New Digital Currency" *Financial Times* (UK, online ed, 24 August 2016) <https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c>.

[200] Ibid.

[201] Kelly, above n 192.

[202] Tim Worstall "UBS and Other Banks Are Not Creating A New Digital Currency - It's Blockchain Settlement Not Money" *Forbes* (United States, 24 August 2016) <http://www.forbes.com/sites/timworstall/2016/08/24/ubs-and-other-banks-are-not-creating-a-new-digital-currency-its-blockchain-settlement-not-money/2/#f0790d146304>.

[203] Redrup, above n 195.

[204] Arnold, above n 199 and Kelly, above n 192.

[205] Arnold, above n 199 and Kelly, above n 192.

[206] Ibid.

[207] Ibid.

[208] Redrup, above n 195.

[209] Kelly, above n 192.

if not weeks.[210] Instead, as explained by Tim Worstall, Fellow of the Adam Smith Institute of London, settlement will occur instantaneously and in real time.[211] In particular, it is possible that blockchain technology may pose a threat to the viability of longstanding international transfer services such as SWIFT.[212] SWIFT (the Society for Worldwide Interbank Financial Telecommunication) was developed as a means to facilitate communication between banks located in 15 countries, which has now expanded to more than 200 countries.[213] Among other things, SWIFT provides a service allowing people to make payments between banks in different countries.[214] Not only is there a fee associated with these transactions,[215] but even standard orders can take up to 10 days to process.[216] The length of time for cross-border transactions is a common cause of complaint.[217] Not surprisingly, SWIFT has trialled the use of blockchain, and with positive results,[218] albeit the technology is not yet sufficiently advanced to roll out across its system.[219]

UBS also identified that blockchain technology creates many benefits in terms of data integrity. To take one example, data loss will not occur when one computer system crashes because this data will be stored on the other computer systems with access to the blockchain.[220] Furthermore, there is the possibility that the blockchain could be viewed in real time by regulators, thereby enabling anomalies in data to be addressed before the further integrity of the data is prejudiced.[221] In highlighting this latter benefit, UBS has observed that regulators:[222]

> … would be able to spot anomalies as they arise, and calculate systemic risk on-the-fly. This would allow them to install "circuit breakers" to "cool off" the system before catastrophe hits. They would be able to do the same with individual institutions in danger of failing, quickly cordoning them off from the rest of the system to avoid contagion. Such capabilities would allow regulators to move from a cure-based approach to one of prevention, making for a much safer financial system.

The argument has been made that security of data will be maintained because, unlike Bitcoin, Utility Settlement Coin will be run on a permissioned blockchain, and thus only trusted parties with

---

[210] "How Long do International Bank Transfers Take?" (2 August 2017) Fexco <https://fexco.com/fexco/news/how-long-international-bank-transfers-take/>: "All too often, funds are delayed in the international banking system due to incorrect account details preventing funds from being applied to the beneficiary account. This can potentially delay a transfer by weeks due to the recall and re-sending of funds with amended correct details."

[211] Worstall, above n 202.

[212] Peter Sayer "5 Enterprise-related Things you can do with Blockchain Technology Today" *PC World* (online ed, 12 December 2016) <http://www.pcworld.co.nz/article/611448/5-enterprise-related-things-can-do-blockchain-technology-today/>.

[213] "SWIFT history" Society for Worldwide Interbank Financial Telecommunication (2017) <https://www.swift.com/about-us/history>.

[214] "All about SWIFT Payments" (2017) Nationwide <http://www.nationwide.co.uk/support/payments-and-transfers/specialist-payments/swift-payments>.

[215] Ibid.

[216] SWIFT "Emergency and high priority customer requests" Society for Worldwide Interbank Financial Telecommunication 2017 <https://www.swift.com/myswift/ordering/order-products-services/emergency#Emergencyhandling>.

[217] David Wilson "Why Electronic Banking Transactions Can Take so Much Time" *The Sydney Morning Herald* (Australia, online ed, 21 August 2014) <http://www.smh.com.au/money/planning/why-electronic-banking-transactions-can-take-so-much-time-20140821-106v32.html>.

[218] SWIFT "SWIFT tests show blockchain has potential for global liquidity optimisation" Society for Worldwide Interbank Financial Telecommunication (13 October 2017) <https://www.swift.com/news-events/press-releases/swift-tests-show-blockchain-has-potential-for-global-liquidity-optimisation>. Swift's trial was done using IBM's Hyperledger Fabric.

[219] Martin Arnold "Swift says Blockchain not Ready for Mainstream Use" *Financial Times* (UK, online ed, 9 March 2018) <https://www.ft.com/content/966f5694-22c6-11e8-ae48-60d3531b7d11>.

[220] Batlin, Jaffrey, Murphy, Przewloka and Williams, above n 196, at 24.

[221] At 10.

[222] At 24.

permission will be able to access the information on the blockchain.[223] However, one of the many advances of public blockchains is that information can be kept secret from all but the contracting parties. For instance, by using zero knowledge proofs (zk-SNARK),[224] the cryptocurrency Zcash prevents others accessing the information. Likewise, the cryptocurrency Monero employs another cryptographic tool, ring signatures.[225]

Notwithstanding banks' extensive trials of blockchain, they have continued to express reservations as to whether the technology can fulfil their business needs, including meeting their regulatory obligations.[226] In light of these concerns, Suresh Kumar, CIO of BNY Mellon, has said that minimum regulatory standards would need to be adopted to ensure that the use of blockchain technology can continue to expand.[227] In addition, UBS has stated that "to build a large, open source system which can be shared by all will require common rules. The existing financial infrastructure has these to a great extent, but in the blockchain world, which works differently, these rules will have to be written anew."[228] The Utility Settlement Coin Project is currently addressing this concern by liaising with regulators to ensure a "regulation compliant, robust and efficient structure" for the release of the Utility Settlement Coin.[229] According to UBS, financial institutions have also been keen to work together to develop this regulatory framework.[230]

In terms of the regulatory framework that it is necessary to develop, UBS has made it clear that there needs to be a standardisation of the language used within financial blockchain systems to ensure efficient communication between the various components.[231] In doing so, UBS has drawn comparisons with standard formats on the internet, such as JavaScript and PDF documents, which it notes have improved the user friendliness of the World Wide Web.[232]

2.3.2.2 The Global Payments Steering Group

The Global Payments Steering Group (GPSG) consists of a number of banks including Merrill Lynch, Santander, Unicredit, Westpac Banking Corporation, Bank of America and the Royal Bank of Canada.[233] Other banks and payment service providers have also joined.[234] The Steering Group aims to develop a mechanism for instant payments to be made internationally using blockchain technology.[235] As at

---

[223] David Wigan "Blockchain will make Dodd Frank Obsolete, Bankers Say" *International Financing Review Asia* (online ed, 15 September 2015) <http://www.ifrasia.com/blockchain-will-make-dodd-frank-obsolete-bankers-say/21216014.fullarticle>.

[224] Zero knowledge proofs are akin to magic: they allow one party (the prover) to prove to someone else (the verifier) that a statement is correct without having to reveal what the statement actually is.

[225] Ring signatures allow one person in a group of people to sign a transaction. It is impossible to work out who among the group signed the transaction, thus providing anonymity to the signer. See "Monero: Ring Signatures" (11 June 2017) <https://www.youtube.com/watch?v=zHN_B_H_fCs>.

[226] Kelly, above n 192.

[227] Tsubasa Suruga "Asian Fintechs are in Infancy with Much Potential, says BNY Mellon CIO" *Nikkei Asian Review* (online ed, 14 November 2016) <http://asia.nikkei.com/Business/Trends/Asian-fintechs-are-in-infancy-with-much-potential-says-BNY-Mellon-CIO>.

[228] Batlin, Jaffrey, Murphy, Przewloka and Williams, above n 196, at 34.

[229] Tanya Andreasyan "Deutsche Bank Pledges Commitment to GTB and Digital" *Banking Technology* (7 October 2016) <http://www.bankingtech.com/602201/deutsche-bank-pledges-commitment-to-gtb-and-digital/>.

[230] Batlin, Jaffrey, Murphy, Przewloka and Williams, above n 196, at 37.

[231] At 35–36.

[232] At 36.

[233] Marcus Treacher "Announcing Ripple's Global Payments Steering Group" (23 September 2016) Ripple <https://ripple.com/insights/announcing-ripples-global-payments-steering-group/>.

[234] MUFG, BBVA, SEB, Akbank, Axis Bank, YES BANK, SBI Remit, Cambridge Global Payments, Star One Credit Union and eZforex.com. David Paterson "Ten More Financial Institutions Join Ripple's Global Payments Network" (26 April 2017) Ripple <https://ripple.com/ripple_press/ten-financial-institutions-join-ripples-global-payments-network/>.

[235] Treacher, above n 233.

23 September 2016 the GPSG was the only international alliance with "defined rules and governance".[236] In particular, GPSG seeks to better facilitate high-volume, low-value transactions.[237]

Ripple will provide the technology facilitating these payments.[238] Ripple is an existing provider of blockchain technology for the transfer of money and has offices in Australia, Europe and the US.[239]

2.3 R3 – Corda

R3 is a company founded in 2014 that is leading a consortium of some of the largest financial institutions. The consortium developed Corda,[240] an open source distributed ledger platform.[241] The consortium has had its problems, with Goldman Sachs and Banco Santander withdrawing in November 2016.[242] Corda[243] is operational with banks and others prototyping trade finance applications.[244] Indeed, Corda has extended well beyond banks and financial institutions and is now an open source blockchain platform designed for business use that rivals Hyperledger Fabric and Ethereum blockchains.[245] For example, Project Jasper,[246] the Bank of Canada's project to use blockchain within its interbank payments settlement system, trialled both Corda and a permissioned version of Ethereum.[247] Singapore's equivalent of Project Jasper, Project Ubin,[248] in turn trialled Corda, Hyperledger Fabric and another open source platform, Quorum.[249]

2.4 Arguments against the use of blockchain technology

As this section shows, a number of arguments have been made against the use of blockchain technology, including equating it to Skynet, the sentient autonomous computer system in the *Terminator* films and franchise that attempts to destroy humanity.[250] However, many of the arguments miss the point. Some developers have warned against governments using the technology in applications such as property title systems on the basis that once commenced, a blockchain algorithm would be unable to respond to court orders in ways other than it had initially been

---

[236] Ibid.
[237] Ibid.
[238] "Santander Joins Forces with Other Banks Create a Steering Group to Develop Instant International Transfers" Santander (23 September 2016) <http://www.santander.com/csgs/Satellite/CFWCSancomQP01/es_ES/Corporativo/Sala-de-comunicacion/Santander-Noticias/2016/09/23/Santander-y-otros-bancos-lanzan-un-comite-para-impulsar-las-transferencias-internacionales-instantaneas.html?leng=en_GB>.
[239] Ripple "Overview" <https://ripple.com/company/>.
[240] See <https://www.corda.net/>.
[241] Brown, Carlyle, Grigg and Hearn, above n 65.
[242] Robert Hackett "Why Goldman Sachs and Santander Are Bailing on R3's Blockchain Group" *Fortune* (United States, online ed, 21 November 2016) <http://fortune.com/2016/11/21/goldman-sachs-r3-blockchain-consortium/>.
[243] <https://www.corda.net/>.
[244] "R3 and TradeIX Develop Open Account Trade Finance DLT Business Network" (26 September 2017) R3 <https://www.r3.com/blog/2017/09/26/r3-and-tradeix-develop-open-account-trade-finance-dlt-business-network/>.
[245] Martin Valenta and Philipp Sandner "Comparison of Ethereum, Hyperledger Fabric and Corda" (Working Paper, FSBC (Frankfurt School Blockchain Center), 17 June 2017) <http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf".
[246] See Payments Canada, Bank of Canada and R3 *Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement* (Whitepaper, September 2017) <https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf>. See also James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack and Wade McMahon "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?" (2017) Financial Systems Review 1 <https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf>.
[247] At 1.
[248] Monetary Authority of Singapore *Project Ubin: SGD on Distributed Ledger* (2016) <http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf>.
[249] <https://www.jpmorgan.com/global/Quorum>. Quorum was created by JP Morgan and is an enterprise (permissioned) version of Ethereum.
[250] Morgen E Peck "The Blockchain has a Dark Side" (2016) 53(6) IEEE (Institute of Electrical and Electronic Engineers) Spectrum 12 <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7473136> at 13.

programmed to.[251] However, property title systems would likely be run on a hybrid ledger so that changes could be made.[252] For example, if a court declared a person bankrupt the ownership of the land could be removed from that person. Thus we expect not all blockchains will be fully decentralised. Rather, there will be a mix of decentralised, permissioned and other types of blockchains.

Another concern is that because blockchain technology is designed so that all transactions are permanent and irreversible, cancelling or adjusting inadvertent transactions (a common occurrence easily rectified at present by financial institutions) would not be possible.[253] The Depository Trust & Clearing Corporation questions how current blockchain platforms can evolve to support, cancel or reverse transactions.[254] However, there is now little difference in some respects between blockchain technology and bank payment systems. In New Zealand and Australia, once payments are finalised – as little as two hours – those transactions cannot be reversed. The agreement of the counterparty, the bank to whom the money has been paid, is required to initiate a matching transaction. In other words, if the party who has received the mistaken payment does not agree to return the payment, the only way to recover that payment would be to go to court.[255]

Decentralised blockchain applications and their so-called anonymous nature make them difficult for governments to control and regulate.[256] The potential diminishment of government control has its advantages and disadvantages. Anonymity allows dissenting views to be voiced without fear of repercussions and can lead to positive social change, which is particularly important in oppressive regimes. On the other hand, there are occasions when law enforcement authorities legitimately would need to engage in surveillance of their citizens and others.[257] Indeed, Vlad Zamfir, one of the creators of Ethereum, has urged blockchain developers to be wary of harmful applications of the technology, such as employing them to evade restrictions on hate speech or defamation.[258] Cryptocurrencies can be an attractive tool for persons seeking to avoid tax and to fund illicit activities or launder their proceeds.[259] The potential for cryptocurrencies to be used for bribery and corruption has also been noted.[260] Cryptocurrencies are further used to buy and sell illegal drugs, as well as malware bots and spying tools.[261] Terrorist groups such as ISIS have also turned their attention to cryptocurrencies to fund their activities.[262] However, as we have also noted, cash is used for many criminal and terrorist endeavours, so much so in fact that calls have been made for cash to be removed.[263]

---

[251] Ibid.

[252] See, for example, Graglia and Mellon, above n 120.

[253] Depository Trust & Clearing Corporation *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-trade Landscape* (Whitepaper, January 2016) at 8. <http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology>.

[254] At 89.

[255] New Zealand Banking Ombudsman Scheme "Mistaken Payments" <https://bankomb.org.nz/guides-and-cases/quick-guides/payment-systems/mistaken-payments/>.

[256] Wright and De Filippi, above n 166, at 19–20.

[257] At 22.

[258] Peck, above n 250, at 13.

[259] Wright and De Filippi, above n 166, at 21–22.

[260] Kim-Kwang Raymond Choo "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks" in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 283, at 301–302.

[261] Angela SM Irwin and George Milad "The Use of Crypto-currencies in Funding Violent Jihad" (2016) 19 Journal of Money Laundering Control 407, at 411.

[262] At 410.

[263] See, for example, Rogoff, above n 87.

One significant consequence of the lack of any central authority controlling cryptocurrencies is that users will be left without recourse to their funds should their private keys be lost or stolen.[264] However, cryptocurrency exchanges can store consumers' keys.

From an economic standpoint, the proliferation of decentralised cryptocurrencies could mean that governments lose control of monetary policy as a means of ensuring sustainable economic growth.[265] But cryptocurrencies are not widely used, and there is a sufficiently large window of time to accommodate their use. Alternatively, as will be seen later, governments are exploring issuing their own cryptocurrencies to provide a viable alternative to decentralised cryptocurrencies.[266]

Ammous identifies five main drawbacks to blockchain technology itself.[267] However, each drawback is overstated and can be overcome. First, in relation to permissioned blockchains, recording details in the blockchain of every transaction ever made by every member of the network is unnecessary and increases costs for no benefit. The benefit of blockchain technology is that it can be used to create a full audit trail; thus the recording of every transaction is a feature not a bug. However, it may be desirable not to overload a blockchain with transactions, and considerable work is being done on off-chain transactions so that not all transactions are recorded on the blockchain;[268] a case in point is Bitcoin's lightning network.[269]

Second, it is true that blockchain technologies have difficulties with scaling and face issues of feasibility the larger the network becomes. However, the most cost-effective way to handle a large numbers of transactions would be to centralise in one node, which would then defeat the purpose of decentralisation. A significant amount of work is in fact being done on scaling. Just as the early internet evolved from being slow and clunky, so blockchain technology will evolve. Indeed, there is already a blockchain that can process considerably more transactions per second than Visa.[270] The lightning network is just one of the methods that is being worked upon with Bitcoin to help with scaling.

In addition, it is unlikely for there to be one blockchain; separate blockchains will probably continue to co-exist. However, what is necessary if blockchain technology is to be more than a niche use is to make the blockchains interoperable so that they can communicate with each other.[271] A number of projects are working on interoperability.[272] Interoperability will let blockchains be smaller and enable transactions to be moved between them. In addition it is possible and often desirable to pair blockchain with legacy IT systems.[273] Albeit as observed already, trying to bolt on new technology to

---

[264] Lam and Kuo Chuen, above n 53, at 23.

[265] Wright and De Filippi, above n 166.

[266] See Section 8 Central bank-issued cryptocurrencies (CBDC) below.

[267] Ammous "Blockchain Technology: What is it Good for?", above n 133, at 4–5.

[268] Off-chain transactions can occur when a series of transactions take place between parties which are not all recorded on the blockchain, instead all the transactions are totalled and offset against each other with one transaction being recorded on the blockchain.

[269] Joseph Poon and Thaddeus Drja *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* (Whitepaper, Version 0.5.9.1, 20 November 2015) <https://www.weusecoins.com/assets/pdf/library/Lightning%20Network%20Whitepaper.pdf>.

[270] Rebecca Campbell "University of Sydney's Red Belly Blockchain Scales 660,000 Transactions/Sec; 11.5x of Visa, 94,000x of Bitcoin" *Cryptocoins News* (26 October 2017) <https://www.cryptocoinsnews.com/university-sydneys-red-belly-blockchain-scales-660000-transactionssec/>.

[271] Shaan Ray "Blockchain Interoperability" (16 June 2018) Medium <https://towardsdatascience.com/blockchain-interoperability-33a1a55fe718>. For a more technical discussion see Vitalik Buterin "Chain Interoperability" (9 September 2016) <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>

[272] See, for example, Polkadot <https://polkadot.io>; Cosmos <https://cosmos.network/>; Aion Network <https://aion.network/>; Ark <https://ark.io/> and Block Collider <(https://www.blockcollider.org/>.

[273] IDG Connect "Blockchain: What are the implementation challenges?" (22 March 2018) <https://www.idgconnect.com/blog-abstract/29865/blockchain-what-implementation-challenges>.

existing systems with their legacy issues is painful and seldom achieves the same results as systems created from scratch. Thus, businesses and industries born digital have advantages over their established counterparts.[274]

Third in addressing Ammous's five asserted drawbacks, there is the issue of whether blockchain technology is truly "immutable".[275] Both the Bitcoin blockchain and the Ethereum blockchain have been altered to remedy significant issues.[276] While some may see the ability to make changes to a blockchain as a major problem, in the interest of perfecting an as-yet-imperfect system the ability to make changes at least in exceptional circumstances can be seen as a feature not a bug.

Fourth, the security of blockchain databases is dependent on the expenditure of processing power and large amounts of electricity by friendly nodes when using proof-of-work.[277] However, considerable research and development is also being undertaken to avoid the use of large amounts of electricity, and not all blockchains use proof-of-work.

Fifth, difficulties with regulation are identified by Ammous as a drawback to the technology. It is not uncommon, though, for regulators to struggle with new technology. To abandon a technology because of initial difficulties over regulating would mean that many technologies we take for granted, including the internet, and now Uber, would have been given away early with a resulting loss to society.[278] Even respected institutions such as PayPal were once novel and had a lot of regulatory hurdles to overcome.[279] Finally, Swan also identifies other limitations such as throughput limitations, latency, size and bandwidth issues, wasted resources and poor usability of developer Application Programming Interfaces (APIs) as the current technological limitations to blockchain.[280]

Another potential drawback with blockchain technology is the right to be forgotten under the EU's General Data Protection Regulation (GDPR).[281] New Zealand companies must comply with the GDPR when they hold information about EU citizens.[282] However, some blockchain platforms are already compliant because they do not store personally identifiable information (PII) on the blockchain itself.[283]

2.5 The mechanics of blockchain technology

Blockchain technology represents transformative potential for the peer-to-peer economy. By combining peer-to-peer networks, cryptographic algorithms, distributed data storage and decentralised consensus mechanisms, it provides a way for people to agree on a particular state of affairs and record that agreement in a secure and verifiable manner. The key technological

---

[274] See above nn 77–81 and accompanying text.
[275] See, for example, Angela Walch "The Path of the Blockchain Lexicon (and the Law)" (2017) 36 Review of Banking and Financial Law 713, at 735–745.
[276] At 738–739.
[277] See Section 2.5.3.1 Proof-of-work below.
[278] For example, so ubiquitous is Uber now that Auckland Transport (AT) incorporates both traditional taxis and Uber into its public transport app to assist AT passengers with the first and last mile of their journey. (The first and last mile are the distance that people must travel to get to or from a bus or train stop.)
[279] See generally, Eric M Jackson *The PayPal Wars: Battles with eBay, the Media, the Mafia, and the Rest of the Planet Earth* (World Ahead Publishing, 2004).
[280] Swan, above n 166 cited in Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park and Kari Smolander "Where Is Current Research on Blockchain Technology?—A Systematic Review" (2016) 11(1) PLoS ONE 1, at 3–4.
[281] General Data Protection Regulation (GDPR) EU 2016/679, art 17.
[282] Bianca Mueller "GDPR Compliance in Four Steps" (2017) 913 *Law Talk* (New Zealand, 1 December 2017) <https://www.lawsociety.org.nz/practice-resources/practice-areas/privacy/gdpr-compliance-in-four-steps.>
[283] Henry Hirsh "GDPR: The Blockchain Iceberg" (12 June 2018) SingleSource <https://www.mysinglesource.io/blog/gdpr-the-blockchain-iceberg> and see Sovrin <https://sovrin.org/> and Lucas Mearian "Will blockchain run afoul of GDPR? (Yes and no)" *Computer World* (7 May 2018) <https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html>.

developments critical to the creation of the blockchain and cryptocurrencies are outlined in the following sections.

2.5.1 Hash functions

A hash function is an algorithm that transforms data of arbitrary size into a fixed size. Essentially, data is run through a computer program and a long string of numbers is created.[284] For example, the hash of the abstract for the Bitcoin Whitepaper is: 5551D438496B1A2E28ED7A3B3535CC74FD009EFBF704AD39D9F2FE952B333F11. Say the abstract was changed by altering the full stop after "double-spending" to a comma and the letter following the former full stop to a lower case. That would result in this new (and clearly different) hash: 0C658066924068BB28BEE9825305712DCBE8C8B67F6230ECDC2F4985A1989586. In other words it is easy to ascertain if a document is the one recorded on the blockchain. All that needs to be done is to run the hashing algorithm over the document or image or any file that a person is claiming to be the one recorded on the blockchain. Because the amount of information does not produce a longer hash – a 1,000-page book will produce the same length hash as the letter "a" – hash functions allow information to be stored more efficiently and thus on a smaller blockchain. Note also a critical characteristic of a secure cryptographic hash function, namely that it is one-way. That is, while a document can be checked to see if it is the same document, the document cannot be reconstructed from the hash.

On permissioned blockchains, full documents can be stored rather than hashes, because the number of people and organisations using them will be fewer than on public blockchains. Public blockchains would become too large too quickly if full documents were stored on them. The ability to store full documents on permissioned blockchains currently gives permissioned blockchains an advantage over public blockchains.

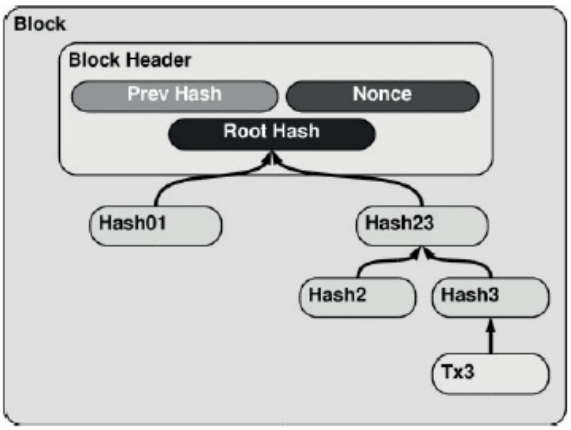
2.5.2 Time-stamping and Merkle trees

Blockchains use digital time stamps to prove that certain information existed at a particular time. They are similar to the traditional physical time stamps employed by companies to record the date and time letters are received or sent out, or the time stamp on digital photos to indicate when a picture was taken. But rather than using a postmark or a rubber stamp to keep track of physical documents, digital time stamps keep track of the creation and modification of blockchains. The important difference is that traditional time stamps can be forged. Alternatively, a person may forget to apply a traditional time stamp; with blockchain the time stamp is applied automatically each time – without the time stamp the transaction cannot be entered onto the blockchain.

For cryptocurrencies, time stamps are used to verify that transactions occurred. Time stamps are vital because cryptocurrencies, while encrypted and decentralised, act as a transparent accounting system in which every transaction is recorded. On a technical level, the information included in the digital time stamp is the hash value (rather than the actual input data itself). This is to ensure that the actual information to be time-stamped (ie the input data) remains private. To secure digital time stamps, a Merkle tree is often used. A Merkle tree is a data structure in which the time-stamped fixed hash values (derived from the initial input data) are grouped into a smaller number of hash values, with the latter being grouped again into a still smaller number of hash values. This process is repeated until there is one central hash value at the top (known as the root of the Merkle tree). Given the complex branches stemming from a Merkle tree, deciphering the data structure (to recover the initial data input) is computationally extremely difficult and prevents attackers from stealing information. On the other hand, Merkle trees provide an efficient method for users to verify transactions, as they would only need to verify that the transaction was included in the tree to prove that it took place.

[284] See, for example, <https://passwordsgenerator.net/sha256-hash-generator/>.

Merkle trees allow older transactions to be discarded without breaking the block's hash by keeping the root only. This is illustrated in the diagram below where the block header contains the hash of the previous block in the blockchain, the root of the Merkle tree of the transactions and the nonce (a random number used only once).[285]



2.5.3 Consensus mechanisms

As explained below, Satoshi Nakamoto's Bitcoin blockchain[286] was not the first attempt to create electronic cash,[287] nor was the technology behind Bitcoin breathtakingly new. Bitcoin used pre-existing technology, such as public key infrastructure.[288] Nakamoto combined existing technology with incentives to incentivise people to host copies of the blockchain and perform work such as ensuring that fraudulent transactions do not occur. Nakamoto's genius was to create a system that operated without the assistance or even the oversight of a central entity. To ensure that only correct transactions are processed the network must reach a consensus. Cryptocurrencies (and blockchains in general) use a variety of ways to achieve consensus. The main consensus mechanisms are set out below.

2.5.3.1 Proof-of-work

Inevitably, blockchains will be the target of attacks. The reason is attackers wish to access the data structure so that they can engage in a fraudulent transaction. This results in two different transactions trying to use the same funds. Other attackers wish to access the data structure for the sake of excluding users from the network or simply inconveniencing them (for example by draining a user's computational resources or slowing down the transaction confirmation rate). Blockchains like Bitcoin protect their network by using the proof-of-work (PoW) concept to secure the distributed database.

The concept of PoW problems was first introduced in the early 1990s by Cynthia Dwork and Moni Naor.[289] The PoW concept is a method in which access to a blockchain can only occur if a specific

---

[285] Source: Franco, above n 53, at 118.
[286] Nakamoto, above n 16.
[287] See Section 3.2 The evolution of cryptocurrencies below.
[288] Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman "New Directions in Cryptography" (1976) IEEE Transactions on Informational Theory 644; proof-of-work was invented in 1993 by Cynthia Dwork and Moni Naor "Pricing via Processing or Combatting Junk Mail" *Proceedings of Crypto 1992, Lecture Notes in Computer Science 740* (Springer, 1993) 139 to combat spam; Ralph Merkle invented Merkle Trees in 1982, US Patent 4309569A "Method of Providing Digital Signatures" (5 January 1982).
[289] Cynthia Dwork and Moni Naor, ibid.

computationally hard or computer memory-hard problem is solved.[290] It acts as a deterrent to attackers because of the complexity and time required to solve the problem. PoWs are utilised as a majority-voting mechanism to enforce the ledger's integrity and achieve global consensus.

Blockchains using PoW are susceptible to 51 per cent attacks. A 51 per cent attack occurs when an individual owns more than 50 per cent of the computational power of the network or a group of people who control more than 50 per cent of the computational power combine. Recently a number of the smaller PoW coins including Litecoin have been subject to 51 per cent attacks.[291]

2.5.3.2 Proof-of-stake

PoW was the predominant design for cryptocurrencies. There have, however, quite rightly been concerns over the large amounts of electricity required to run the Bitcoin blockchain. With computational and energy usage in mind, the proof-of-stake (PoS) concept was developed as an alternative way to secure cryptocurrencies. PoS was first used in the cryptocurrency Peercoin. PoS has now been adopted by other cryptocurrencies including NavCoin, NuShares/NuBits, ShadowCash and BlackCoin. Ethereum looks likely to move to PoS.[292] Unlike PoW, where transaction validation and the creation of new blocks can only occur if a complex puzzle is solved, PoS chooses who can create the next block based on the extent of ownership of the network/currency. PoS requires the user to demonstrate ownership of a certain number of tokens. It has been touted as a future replacement for the PoW concept because the latter is wasteful. As Buterin observes:[293]

> Six hundred trillion … computations are being performed by the Bitcoin network every second, and ultimately these computations have no practical or scientific value; their only purpose is to solve proof-of-work problems that are deliberately made to be hard so that malicious attackers cannot easily pretend to be millions of nodes and overpower the network.

Buterin's view is understandable as computations take a lot of time and power to perform the work. This in turn leads to higher electricity usage. As John Quiggin noted in October 2015, the early days of Bitcoin only required an ordinary computer to process the computations.[294] Now special purpose machines are optimised to run continuously through night and day. The result is that 10,000–12,000 kWh in electricity (the average annual consumption of a US household) could only generate four bitcoins, which at the time of that writing were worth a little under USD 1,000.[295] The price of bitcoin, however, has risen since Quiggin's comments and four bitcoins are now (writing in 2018) worth around USD 26,684.[296] In addition, there is also a widely held belief that PoS transactions are less vulnerable to 51 per cent attacks. It has been argued that the probability of a 51 per cent attack

---

[290] For Satoshi Nakamoto's explanation of proof-of-work see Nakamoto, above n 16, at 3.

[291] "Litecoin Cash Allegedly the Latest Small-Cap Altcoin to Suffer 51 Percent Attack" *CCN* (8 June 2018) <https://www.ccn.com/litecoin-cash-latest-small-cap-altcoin-to-suffer-51-percent-attack/>. See also Husam Abboud "The Realistic Lucrative Case of Ethereum Classic attack — Today" (22 May 2018) Medium <https://medium.com/@HusamABBOUD/the-realistic-lucrative-case-of-ethereum-classic-attack-with-1mm-today-8fa0430a7c25> and Husam Abboud "H/Rindex: The Hashing Power and Robustness Index, Computational Power-weighted Benchmark for Global Blockchain and Crypto Market" (1 October 2017) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3136635>.

[292] Lewis Gray "Proof of Stake Is Coming, and Will Be a Game Changer" *CCN* (7 February 2018) <https://www.ccn.com/proof-stake-coming-will-game-changer/>.

[293] Vitalik Buterin "What Proof of Stake is and Why it Matters" *Bitcoin Magazine* (26 August 2013) <https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/>.

[294] John Quiggin "Bitcoins are a Waste of Energy – Literally" *ABC News* (Australia, 6 October 2015) <http://www.abc.net.au/news/2015-10-06/quiggin-bitcoins-are-a-waste-of-energy/6827940>.

[295] Ibid.

[296] Coinmarketcap.com on 26 August 2018 Bitcoin was trading at USD 6,671 per bitcoin.

is lower in a PoS system because it would be more expensive to buy 50 per cent of the currency rather than 50 per cent of the computational power.[297]

2.5.3.3 Alternative consensus mechanisms

As a way to utilise the advantages of both PoW and PoS, some cryptocurrencies such as Peercoin use elements from both concepts.

While PoS does not involve extensive energy usage, it is arguably unfair as people require large amounts of coins to participate in mining, and it has the tendency to concentrate resources. As an alternative, the cryptocurrency and blockchain platform NEM uses proof-of-importance.[298] Whereas PoS depends on the number of coins staked, thus privileging those with large holdings, proof-of-importance looks at the public key's network activity. This includes not only the number of coins, but also, for instance, the reputation and the number of transactions made to and from the public key.

In the case of delegated proof-of-stake (DPoS), coin owners elect nodes that can have ability to secure the network; those people are called Witnesses. DPoS avoids the large computing and electricity cost involved in PoW, and also keeps the Witnesses working hard and honestly because if they act in a way that others do not like they can have their Witness status removed and thus the ability to earn revenue.

Finally, there is leased proof-of-stake (LPoS). With ordinary PoS a large number of coins are required to validate a block of transactions. Thus many coin owners are not able to participate in validation. LPoS holders to lease balances to a node and receive rewards in proportion to the node that has leased the coins.

3. Cryptocurrencies

Before looking at cryptocurrencies it is useful to survey the trajectory of how money and our notion of it has transformed over the millennia.

3.1 A brief history of money

Money has not always underpinned society. When humans lived in small hunter-gatherer groups there was no need for money. Successful hunters brought the carcasses back to the group, where they were distributed to all of the group members. Also shared were the spoils of women's foraging – nuts, fruit and other edible plant-based foods – as well as small animals they had killed. It is thought that such reciprocal and communal arrangements worked well within the small groups, with young, old and infirm members receiving their share. However, when groups started to come into contact with other groups, and as they increased in size, changes and adaptations were required and bartering came to the fore.[299] For example, if one group had access to honey and the other to livestock it made sense to exchange those goods.

Bartering is limited: it requires two people to have things they are willing to trade at the same time for what the other happens to have, such as dried fish for salt. Among other hitches, bartering does not work so well if people want to trade items not thought to be of equal value; the owner of a pig would not want to trade it for one chicken. The issues compound if someone has perishable and fragile produce. To overcome bartering's limitations people began to use objects to symbolise value.

---

[297] "Proof of Work vs Proof of Stake – Explained!" *Monetha* (3 January 2018) <https://blog.monetha.io/proof-work-vs-proof-stake-explained/>.

[298] NEM "Proof of Importance (POI)" <https://nem.io/xem/harvesting-and-poi/#proof-of-importance>.

[299] Whether the origins of money in fact lie in bartering is much contested. However, it is not necessary for the purposes of this article to go through the debate of whether bartering led to the creation of money. See eg Frederic L Pryor "The Origins of Money" (1977) 9(3) Journal of Money, Credit and Banking, 391, at 395396. Pryor argues that money was not necessary to solve problems associated with bartering: for example, that extending credit could have sufficed.

Those objects included: shells,[300] beads,[301] salt,[302] rice,[303] bars of metal,[304] animal skins,[305] cloth,[306] tea,[307] silk,[308] tobacco[309] and a myriad of other things.

A standard definition of money states that it functions as a unit of account, medium of exchange and a durable store of value.[310] Not all of the objects listed above meet the requirements perfectly. For instance, as a medium of exchange, bars of metal can be difficult to transport, and as a store of value food and skins are subject to spoiling. Nonetheless, in their times and locations of use they were accepted as money. As Quiggin observes, "everyone, except an economist, knows what 'money' means, and even an economist can describe it in the course of a chapter or so, but it is impossible to define with rigid outlines".[311] Moreover, some objects actually enjoyed advantages over what we later consider money such as coins; it was impossible to counterfeit or forge shells. Indeed, one Chinese emperor, despairing of counterfeit metal coins, abolished the whole monetary system and returned to shells as the official currency.[312]

Most of these objects had practical uses. For instance, salt of course preserved other goods and metal could be turned into manifold items including tools and weapons, which in turn could be used as symbols of value. In truth such objects were more akin to commodities.[313] Shells and beads, while not so useful, could still have ornamental use[314] and were deemed to possess supernatural powers.[315]

Not all such objects were of use, though.[316] On the tiny island of Yap in the Pacific Ocean, enormous limestone slabs were quarried from distant islands, carved into discs and carried to Yap.[317] The size and weight of the stones, some heavier than a car, rendered them virtually impossible to move once positioned on the island. Yet, despite their lack of portability, the stones served as a store of value – they could be used for a daughter's dowry or if a crop failed they could be traded for food. The bigger stones often remained in the same place but simply changed ownership.[318] Such was the value ascribed to these discs that, according to oral tradition, one disc was lost overboard in a storm

---

[300] Tortoise and cowry shells were used in China: see Arthur Robert Burns *Money and Monetary Policy in Early Times* (K Paul, Trench, Trubner & Company, New York, 1927) at 3–5. See also in relation to cowry shells, Jan Hogendorn and Marion Johnson *The Shell Money of the Slave Trade* (Cambridge University Press, Cambridge, 2003).

[301] See A Hingston Quiggin *A Survey of Primitive Money: The Beginning of Money* (Barnes & Noble, New York, 1970) at 36–44.

[302] At 220, salt was used in China as a medium of exchange.

[303] D Sherman *Rice, Rupees, and Ritual: Economy and Society Among the Samosir Batak of Sumatra* (Stanford University Press, 1990) at 3 noting that in Sumatra goods were traded for rice and it was not until later than goods were traded for money.

[304] Percy Gardner "The Origin of Money" (1897) 11(3) The Classical Review 172.

[305] Quiggin, above n 301, at 308: in what is now the United States beaver and moose skins were used.

[306] At 51 noting that cloth was used extensively in Africa despite it not being as specialised as iron making, but in the pre-industrial age cloth production was time-consuming work.

[307] At 220.

[308] At 220.

[309] Murray N Rothbard *A History of Money and Banking in the United States: The Colonial Era to World War II* (Ludwig Von Mises Institute, Auburn, Alabama, 2002) at 48.

[310] Aaron Kumar and Christie Smith "Crypto-currencies – An introduction to not-so-funny moneys" (November 2017) Reserve Bank of New Zealand Analytical Notes at 20 <https://www.rbnz.govt.nz/-</media/ReserveBank/Files/Publications/Analytical%20notes/2017/an2017-07.pdf>.

[311] Quiggin, above n 301, at 1 quoted in Felix Martin *Money: The Unauthorised Biography* (Alfred A Knopf, New York, 2014) at 3.

[312] Quiggin, above n 301, at 25–26.

[313] Paul Einzig *Primitive Money in its Ethnological, Historical, and Economic Aspects* (2nd ed, Pergamon Press, 1966) at 312.

[314] Quiggin, above n 301, at 25 (shells).

[315] At 36.

[316] Einzig, above n 313, at 312.

[317] See generally, Jacob Goldstein and David Kestenbaum "The Island of Stone Money" (Podcast, 10 December 2010) Planet Money <http://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money>.

[318] Quiggin, above n 301, at 146.

yet was still regarded as property that a person owned and the ownership transferred from person to person over the years.[319] While the stones could be argued to be abstract units, they made a very large store of value and could not be divided into smaller units.[320]

In China tools and weapons were utilised as a medium of exchange. Later, for convenience smaller replicas cast in bronze were used.[321] The drawback with the smaller versions was that handling could result in injuries when they were retrieved from pouches and bags, and their irregular size still made them cumbersome to use. Round objects were safer and easier to handle, so flat disks of metal began to be used. The flat disks gave way to coins. The first officially minted coins were from Lydia, now part of western Turkey. But coins have their own limitations. They can be bulky and expensive to make, are able to be counterfeited, and may be difficult to transport in large quantities.

Recognising the limitations of metallic or coin money, the Chinese invented paper currency.[322] As with a number of technologies, Europe lagged behind China, and paper money did not start to circulate there until many centuries later.[323] While it is widely accepted that the first type of paper money in Europe was bills of exchange,[324] research shows that other forms of preceded those.[325] Bills of exchange, promissory notes and other forms of paper money allowed the bearer to take them to the issuer and exchange them for coins. Crucially, this early money was not state-backed; that is, there was no government that stood behind the money. On the other hand, states in the US issued state-backed paper money, beginning in Massachusetts in 1690.[326] In the early 19th century there were hundreds of different banks, each issuing their own paper notes.[327] It was not until 1913 that the US's official currency came into being.[328] Similarly in New Zealand, banks issued their own notes and it was not until 1934, when the RBNZ was established, that it became the sole supplier of New Zealand bank notes.[329] Furthermore, between 1857 and 1881, due to a shortage of British coins (which were the only legal tender coins in New Zealand at the time), merchants issued their own low-value bank notes and bronze and copper tokens to be used as small change.[330] While the tokens were not official currency the Government did nothing to prevent their use even though the tokens could be used only for redemption for goods at the issuing trader's store.[331] Tokens only ceased to be used in 1881 when the British Government announced that it could supply New Zealand with sufficient coins.[332]

---

[319] At 146 and Goldstein and Kestenbaum, above n 317.

[320] For a discussion about how the Yap stone money was used more recently, including the fact that smaller stones were used as well as large ones, see Einzig, above n 313, at 3640.

[321] Quiggin, above n 301, at 230–231.

[322] Francis T Lui "Cagan's Hypothesis and the First Nationwide Inflation of Paper Money in World History" (1983) 91 Journal of Political Economy 1067, at 1068, noting that paper money was invented in China in the Northern Song dynasty (AD 960-1126).

[323] Not quite on point, but see J Keith Horsefield "The Beginnings of Paper Money in England" (1977) 6 Journal of European Economic History 17.

[324] Claire Jones "The History of Paper Money" *Financial Times* (UK, online ed, 11 September 2013) <https://www.ft.com/content/f11c6126-1a39-11e3-93e8-00144feab7de>.

[325] See generally, R D Richards "The Evolution of Paper Money in England" (1927) 41 The Quarterly Journal of Economics 361 and Abbott Payson Usher "The Origin of the Bill of Exchange" (1914) 22 Journal of Political Economy 566.

[326] Rothbard, above n 309, at 51. However, as Rothbard explains, the promise of Massachusetts to redeem the notes was quickly forgotten.

[327] For a discussion about how paper money evolved in the United States see William Watts Folwell "Evolution of Paper Money in United States" (1924) 8(7) Minnesota Law Review 561.

[328] In the United States the Government only acquired a monopoly over the issuing of notes in 1913 and the notes were only made legal tender in 1933: see Angela Redish "Anchors Aweigh: The Transition from Commodity Money to Fiat Money in Western Economies" (1993)(4) Canadian Journal of Economics 777, at 782.

[329] Te Ara, above n 20.

[330] Te Ara, ibid.

[331] Te Ara, ibid.

[332] Te Ara, ibid.

Linking paper money to something perceived to have value such as gold was a feature of many fiat currencies. A number of countries including the US, the UK, Australia and New Zealand used the gold standard. The gold standard was a monetary system where a country's currency was fixed to the price of gold and the country held reserves of gold to back that currency. Thus it was possible to take a bank note issued by the Bank of England (BoE) to the BoE and for it to pay out the value of that note in gold. The gold standard, however, no longer applies and paper notes cannot be exchanged for gold. Bank notes have become fiat currency: "money without intrinsic value that is used as money because of government decree".[333]

Bank notes now comprise only a small amount of New Zealand's fiat currency; most fiat currency can be described as digital money.[334] For example, most New Zealand employees are no longer paid wages in paper notes (cash). Wages are now routinely paid straight into bank accounts. In turn payments are made through debit cards, credit cards[335] and through internet banking.

Even more recently mobile payment systems such as Apple Pay have been coming into use. Thus goods and services are increasingly being acquired without the need to touch and transfer physical cash. In a number of countries, including New Zealand, power cuts mean that businesses struggle to operate as many people have no cash on them.[336] However, there are alternatives to a fixed point of sale machine that must be connected to power. It has been possible for a number of years to accept credit card payments through a card reader attached to a mobile phone: all that is required then is an internet connection.[337] Alternatively customers can scan quick response (better known as QR) codes to make payments. The disadvantage, as with Apple Pay, is that both the merchant and customer must run the same system. Contrast cryptocurrencies, where if the customer has a mobile wallet capable of scanning QR codes (which most do), all that is needed is for the merchant to be able to accept the same cryptocurrency as the customer wishes to pay.

Thus money, or rather what we use as a unit of account, medium of exchange and a durable store of value, and how we transfer it between people and organisations, has evolved over millennia.[338] The point often overlooked is that "a public money system is of comparatively late origin while the device of legal tender is a still more recent invention".[339] Cryptocurrencies can be seen as a natural extension of this development.

---

[333] N Gregory Mankiw *Principles of Macroeconomics* (7th ed, Cengage Learning, Australia, 2017) at 220.

[334] Money in commercial bank accounts is described as "fixed conventional digital currency". In February 2016 notes and cash amounted to only 4 per cent of broad money balances in the United Kingdom. Broad money balances are the "notes and coin held by the non-bank public plus sight and time deposits held by households, private non-financial corporations and non-intermediary other financial corporations." John Barrdear and Michael Kumhof "The Macroeconomics of Central Bank Issues: Digital Currencies" (Staff Working Paper No. 605, Bank of England, 2016) at 4–5 <http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>.

[335] Credit cards are problematic for merchants. Credit card companies' fees can be prohibitively expensive for small businesses: see Eloise Gibson "Credit cards costing small businesses $100 a week" *Stuff* (New Zealand, online ed, 17 July 2015) <http://www.stuff.co.nz/business/money/70217405/credit-cards-costing-small-businesses-100-a-week>. In addition, there are charge-backs where if a payment is disputed successfully – for example, if a card is used fraudulently – the transaction is reversed and the merchant loses that money. See generally, Fumiko Hayashi, Zach Markiewicz and Richard J Sullivan "Chargebacks: Another Payment Card Acceptance Cost for Merchants" (Working Paper No. 16-01, Federal Reserve Bank of Kansas City, 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2720386>.

[336] Chloe Winter "Storm Cuts Power to Cellphone Towers, Makes Life Hard for Retailers in Auckland" *Stuff* (New Zealand, online ed, 11 April 2018) <https://www.stuff.co.nz/business/103005351/Storm-cuts-power-cellphone-towers-makes-life-hard-for-retailers-in-Auckland>.

[337] Adam Turner "3 Ways to Accept Credit Card Payments" (29 May 2015) MYOB <https://www.myob.com/nz/blog/3-alternatives-to-eftpos-terminal/>.

[338] Bank notes are not always a medium of exchange, nor are they a durable store of value: see, for example, Alex Sims "Money and its Myths" *Newsroom* (New Zealand, 4 July 2018) <https://www.newsroom.co.nz/@future-learning/2018/07/03/137959/the-myths-surrounding-money>.

[339] Herman Oliphant "The Theory of Money in the Law of Commercial Instruments" (1920) 29 Yale Law Journal 606, at 616, cited by Ali Khan "The Evolution of Money: A Story of Constitutional Nullification" (1999) 67 University of Cincinnati Law

Suspicion of the new has deep roots in the history of money and currency. Einzig observes that the metallist school of economics confined its definition of money to "metallic money and treated paper money as a freak development or an emergency measure".[340] Paper money was not accepted into the fold of currencies until the end of the 19th century.[341] Thus it should come as no surprise that cryptocurrencies are treated with suspicion by many. For example, it is curious that lack of any intrinsic value is a criticism levelled against cryptocurrencies.[342] Both fiat and cryptocurrencies are without intrinsic value, the difference being that fiat currency is used because of governmental decree, whereas cryptocurrencies are used because others are willing to accept them in return for goods and services.[343] Zimbabwe, for example, stands as a recent and unfortunate example of fiat currency not being backed by anything. The last note printed by Zimbabwe before it managed to bring its hyperinflation under control was $1,000,000,000,000,000 (one hundred trillion), worth only about USD 0.40.[344] Ironically, bitcoin was and is being used as a currency in Zimbabwe,[345] because the US dollar, also in circulation, was being rationed by the banks.[346]

3.2 The evolution of cryptocurrencies

The beginning of the evolution of cryptocurrencies is often attributed to a paper published by cryptographer David Chaum in 1982.[347] Chaum proposed a digital payment system based on blind signatures[348] that would be untraceable. The system involved the use of serial numbers signed by a bank blindly as tokens. These tokens could then be exchanged and redeemed from the signing bank. Notably, this system did not protect merchants against "double spending", the problem of a rogue buyer giving the same token to two different merchants. To avoid accepting as payment a token already given to another merchant, a merchant would have to successfully redeem the token before accepting it. The system could therefore only work online, where tokens could quickly be verified with the signing bank.[349]

Chaum continued to work on improving his proposal and in 1990 published a paper proposing a system called eCash, a refinement of his earlier system.[350] Like his earlier proposal, eCash involved the use of blind signatures but it featured a built-in protection against double spending. The protection was based in the type of data involved in the token. Unlike Chaum's earlier approach, this data was not simply a random serial number but also contained hidden information about the user.

Review 393, at 396–397. There is significant confusion about what is meant by legal tender. For an explanation of legal tender in New Zealand and its practical effect see Nick McBride "Payments and the Concept of Legal Tender" (2015) 78(6) (September 2015) <https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2015/rbb2015-78-00-01>. As McBride explains, while section 27 of the Reserve Bank of New Zealand Act 1989 provides that New Zealand bank notes and coins are legal tender, the Act does not say what legal tender actually is.

[340] Einzig, above n 313, at 312.

[341] Ibid.

[342] Bank for International Settlements, Committee on Payments and Market Infrastructures *Digital Currencies* (November 2015) <http://www.bis.org/cpmi/publ/d137.pdf> at 1.

[343] Indeed, paper currency has its limitations. So nearly the whole of India discovered on 8 November 2016 when overnight the most valuable notes were no longer accepted by merchants: SP "Why India Scrapped its Two Biggest Bank Notes" *The Economist* (UK, online ed, 14 November 2016) <http://www.economist.com/blogs/economist-explains/2016/11/economist-explains-6>.

[344] Dominic Frisby "Zimbabwe's Trillion-dollar Note: From Worthless Paper to Hot Investment" *The Guardian* (UK, online ed, 14 May 2016) <https://www.theguardian.com/money/2016/may/14/zimbabwe-trillion-dollar-note-hyerinflation-investment>.

[345] James Titcomb "How Bitcoin has Become Zimbabwe's Crisis Currency" *The Telegraph* (UK, online ed, 17 November 2017) <https://www.telegraph.co.uk/technology/2017/11/20/bitcoin-has-become-zimbabwes-crisis-currency/>.

[346] Gavin du Venage "Zimbabwe's Embrace of Bitcoin Poses Problems" *The National* (United Arab Emirates, online ed, 18 October 2017) <https://www.thenational.ae/business/zimbabwe-s-embrace-of-bitcoin-poses-problems-1.668430>.

[347] Chaum "Blind Signatures for Untraceable Payments", above n 39.

[348] See generally Franco, above n 53, at 71–72.

[349] At 162–163.

[350] David Chaum, Amos Fiat and Moni Naor "Untraceable Electronic Cash" in S Goldwasser (ed) *Advances in Cryptology: Proceedings of Crypto 88* (Springer-Verlag, 1990) 319.

The format of the information was such that a single merchant receiving a token could not access the information about the user, but two merchants receiving the same token could combine their tokens to access the information. Users therefore had a disincentive to double spend because this would sacrifice their anonymity. The eCash system did not, however, prevent users from double spending altogether.[351] The eCash proposal was realised through DigiCash, a company founded by Chaum in 1990.[352] DigiCash is said to have been the first commercially operating cryptocurrency.[353] DigiCash went bankrupt in 1998.[354]

A further development significant to the evolution of cryptocurrencies was the invention of Hashcash by Adam Back in 1997.[355] Hashcash was originally invented as a method of reducing email spam, but has since been used in cryptocurrencies such as bitcoin as a PoW system: a cryptographic puzzle that is difficult to solve but simple to verify.[356] In 2004, Hal Finney published an improvement on the Hashcash system which allowed PoWs to be exchanged without having to be regenerated.[357]

In 1998, two further currency systems were proposed, Nick Szabo's bit gold[358] and Wei Dai's b-money.[359] Both of these proposals involved solving PoW problems to create money. Unlike Chaum's eCash, these proposed currencies employed distributed transaction ledgers and did not rely on a trusted central server. Servers would communicate with each other to maintain a shared database of transactions. Inconsistences between the servers' reports on the contents of the database would be resolved by majority rule. A problem with this type of system, known as the Byzantine Generals' Problem, was described as early as 1982.[360] How could the information from servers be trusted? With conflicts in the database resolved by majority rule, the system would be vulnerable to attackers taking control of 51 per cent of the computational power of the servers to make changes to the database. Neither bit gold nor b-money was ever implemented, but the proposals were nevertheless important precursors to the development of Bitcoin and blockchain technology.[361] Solving the Byzantine Generals' Problem was one of Bitcoin's major achievements.[362]

A further currency system was proposed by Tomas Sander and Amnon Ta-Shma in 1999.[363] Notably, this system used Merkle trees[364] to store a list of valid coins. Updates to the Merkle tree were to be publicly broadcast, making the system auditable. Sander and Ta-Shma's proposal contemplated the existence of a bank that updated the Merkle tree, but Franco notes that this was not a necessary feature of the system; this function could be decentralised.[365] The system was also to be fully anonymous. Like bit gold and b-money, the system was never implemented.

---

[351] Franco, above n 53, at 163.
[352] Marius-Cristian Frunza *Solving Modern Crime in Financial Markets* (Elsevier, 2015) at 40.
[353] Lam and Kuo Chuen, above n 53, at 8.
[354] Julie Pitta "Requiem for a Bright Idea" *Forbes* (United States, online ed, 1 November 1999) <http://www.forbes.com/forbes/1999/1101/6411390a.html>.
[355] Adam Back "Hash Cash Postage Stamp Implementation" (28 March 1997) <http://www.hashcash.org/papers/announce.txt>.
[356] Franco, above n 53, at 164.
[357] Hal Finney "RPOW – Reusable Proofs of Work" (15 August 2004) <http://marc.info/?l=cypherpunks&m=109259877510186&w=2> cited in Franco, above n 53, at 167.
[358] Nick Szabo "Bit Gold" (27 December 2008) Unenumerated <http://unenumerated.blogspot.co.nz/2005/12/bit-gold.html>.
[359] Wei Dai "bmoney" (1998) <http://www.weidai.com/bmoney.txt>.
[360] Leslie Lamport, Robert Shostak and Marshall Pease "The Byzantine Generals Problem" (1982) 4 ACM Transactions on Programming Languages and Systems 382. See the Glossary for the Byzantine Generals Problem.
[361] Franco, above n 53, at 165 and see Alex B "The Mining Delusion" (25 April 2017) Medium <https://medium.com/@bergealex4/the-mining-delusion-96e021b6f899>.
[362] Ibid.
[363] Tomas Sander and Amnon Ta-Shma "Auditable, Anonymous Electronic Cash" in Wiener M (eds) *Advances in Cryptology — CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666* (Springer, Berlin, Heidelberg,1999) 555.
[364] For Merkle trees see 2.5.2 Time-stamping and Merkle trees above and see generally Franco, above n 53, at 117–120.
[365] Franco, above n 53, at 167.

Meanwhile, investor demand for gold-backed currencies led to the creation of a number of digital gold currencies in the early 2000s, including iGolder, gBullion and e-Gold. Most of the companies running these currencies were shut down by the US Government for regulatory breaches.[366] A digital currency called Liberty Reserve was launched to fill the void left by the dismantling of e-Gold. But Liberty Reserve was also shut down by US authorities in 2013 and a number of its directors were convicted of conspiring to operate an unlicensed money transmitting business involving the transmission of funds derived from criminal activity.[367]

In 2008, Bitcoin was created by a person or persons operating under the pseudonym of Satoshi Nakamoto. A Whitepaper explaining the Bitcoin system was published on 31 October 2008 under that name.[368] The genesis block initiating Bitcoin's blockchain was created on 3 January 2009 and the system was launched publicly on 11 January 2009 through an announcement to a cryptography mailing list. Bitcoin was the first cryptocurrency that did not require a trusted third party as an intermediary.[369] Like bit gold and b-money, bitcoin dealt with the double-spending problem using a PoW system.[370] Furthermore, bitcoin's blockchain system dealt with the Byzantine Generals' Problem by providing incentives for nodes to be honest. Essentially, even if an attacker gained control of 51 per cent of the computational power in the network, it would be more profitable for them to use this computational power to generate new coins legitimately than to attempt to defraud others by stealing back payments.[371] The blockchain is regarded as bitcoin's key innovation as a cryptocurrency.[372]

Bitcoin has been the most successful cryptocurrency. As at 26 August 2018 it was estimated to have a market cap of USD 111 billion.[373] Its launch has also spawned a number of similar cryptocurrencies sometimes known as alternative coins or "altcoins", some based on modified versions of Bitcoin's source code.[374] The low entry costs associated with establishing a cryptocurrency are cited as one of the reasons for the proliferation of these altcoins.[375] Now there are well over 5,000 ERC-20 tokens alone.[376]

The question, of course, is whether cryptocurrencies can function as money. Ammous has shown that of the five main cryptocurrencies, which are broadly representative of the different types of cryptocurrencies, bitcoin could serve as money.[377] Although, as we shall see, there are currently limitations to a widespread adoption of bitcoin.[378] At this point it must be noted that there is much hype about cryptocurrencies, which has the potential to catch out policy makers and others, including investors and consumers. Unless Ammous is playing a double bluff, his work on cryptocurrencies is more credible than most as he is not a cheer leader for blockchain technology. In

---

366 Frunza, above n 352, at 40 and 55–56; Lam and Kuo Chuen, above n 53, at 9.
367 Frunza, above n 352, at 56–57.
368 Nakamoto, above n 16.
369 Jerry Brito and Andrea Castillo *Bitcoin: A Primer for Policymakers* (Mercatus Center, 2013) at 3.
370 Nakamoto, above n 16, at section 4.
371 At section 6.
372 Preston Miller "The Cryptocurrency Enigma" in John Sammons (ed) *Digital Forensics* (Syngress, 2015) 1, at 5; Blundell-Wignall, above n 53, at 8.
373 *Crypto-Currency Market Capitalizations* <https://coinmarketcap.com/>.
374 Franco, above n 53, at 171.
375 At 178; Blundell-Wignall, above n 53, at 11.
376 Pascal Thellmann "There Are Currently Over 5300 ERC-20 Tokens - What Are They All For?" *Cointelegraph* (18 August 2017) <https://cointelegraph.com/news/there-are-currently-over-5300-erc-20-tokens-what-are-they-all-for>.
377 Ammous "Can Cryptocurrencies Fulfil the Functions of Money?", above n 107.
378 As the Governor of the Reserve Bank of Australia has noted, "[t]he number of payments that can currently be handled [by Bitcoin] is very low, there are governance problems, the transaction cost involved in making a payment with Bitcoin is very high and the estimates of the electricity used in the process of mining the coins are staggering." Philip Lowe "An eAUD?" (address to the 2017 Australian Payment Summit, Sydney, Australia, December 2017) <https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html>.

another article entitled "Blockchain Technology: What is it good for?", Ammous is clear that he does not think that blockchain technology has wide application outside cryptocurrencies.[379]

Notwithstanding that Bitcoin was designed as a "peer-to-peer electronic cash system",[380] some cryptocurrencies have become far more than simply an electronic payment system, as discussed in Section 3.3 below.

While cryptocurrencies began to be developed in the 1990s, it was not until Bitcoin was launched in 2009 that they started to gain traction. Bitcoin spurred the creation of many cryptocurrencies, including Freicoin (February 2011), Namecoin (April 2011), Litecoin (October 2011), Peercoin (August 2012), Primecoin (July 2013), Dogecoin (December 2013) and Auroracoin (February 2014).[381] Now there are over a thousand cryptocurrencies,[382] more than the number of fiat currencies.[383] However, most are not designed to be used as payments.[384]

The global financial crisis (GFC) in 2008 is cited as a factor influencing the renewed development of cryptocurrencies.[385] The GFC led to a loss of trust in traditional financial intermediaries, trading platforms and payment systems.[386] Indeed, Bitcoin's genesis block, the first block in the Bitcoin blockchain, contains the statement "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."[387] There was a similar loss of trust in traditional fiat currencies.[388] Nick Szabo, for example, the proponent of bit gold, in 2008 lamented the dependence on trusted third parties and problems of inflation associated with fiat currencies.[389] Concerns about trust also extended to protection of customer privacy by third-party institutions.[390] This loss of trust led to heightened interest in alternative currencies. Bitcoin offered a number of advantages for persons lacking trust in traditional currencies: for example, it was not controlled by a government, or indeed any central authority.[391] This resolved issues around the need for a trusted third party.[392] However, despite Bitcoin's advantages, its initial uptake was slow. It took more than one year for the first bitcoin to be

[379] Ammous "Blockchain Technology: What is it Good for?", above n 133.
[380] Nakamoto, above n 16.
[381] Alexandru Pirjan, Dana-Mihaela Petrosanu, Mihnea Huth and Mihaela Negoita "Research Issues Regarding the Bitcoin and Alternative Coins Digital Currencies" (2015) Journal of Information Systems and Operations Management 1, at 5–9.
[382] See Crypto-Currency Market Capitalizations <https://coinmarketcap.com/>.
[383] Peters, Chapelle and Panayi, above n 70, at 240, reports that there were 467 fiat currencies exchange traded in US dollars as at August 2014.
[384] For example, TravelbyBit has an interactive map to help people find merchants that accept cryptocurrency across Australia. It states: "Selected merchants accept a combination of Bitcoin, NEM, Bitcoin Cash, Litecoin, Ethereum, and Dash" <https://www.travelbybit.com/merchants>. Thus while many tokens can be traded on cryptocurrency exchanges, the number of cryptocurrencies that are currently accepted by merchants is limited.
[385] Bitcoin's first block includes the text of a newspaper article published on the same day the block was made, "The Times 03/Jan/2009 Chancellor on brink of second bailout of banks": Bill Maurer, Taylor C Nelms and Lana Swartz "When Perhaps the Real Problem is Money Itself!: The Practical Materiality of Bitcoin" (2013) 23 Social Semiotics 261, at 275 quoting Joshua Davis "The Crypto-currency" *The New Yorker* (United States, online ed, 10 October 2011) <https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>.
[386] Chris Richter, Sascha Kraus and Ricarda B Bouncken "Virtual Currencies Like Bitcoin As A Paradigm Shift In The Field Of Transactions" (2005) 14 International Business & Economics Research Journal 575, at 575; Frunza, above n 352, at 45; Lam and Kuo Chuen, above n 53, at 9; Blundell-Wignall, above n 53, at 7.
[387] Robleh Ali, John Barrdear, Roger Clews and James Southgate "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Bank of England Quarterly Bulletin Q3 262, at 267.
[388] Grinberg, above n 72, at 172–173; Szabo, "Bit Gold", above n 358 and Lam and Kuo Chuen, above n 53, at 10.
[389] Szabo, "Bit Gold", above n 358. See also Nick Szabo "Trusted Third Parties Are Security Holes" (2001) <https://web.archive.org/web/20160309161628/http://szabo.best.vwh.net/ttps.html> and Richter, Kraus and Bouncken, above n 386, at 580.
[390] Nakamoto, above n 16, at section 10.
[391] Frunza, above n 352, at 45; Grinberg, above n 72, at 174; Richter, Kraus and Bouncken, above n 386, at 575.
[392] Lam and Kuo Chuen, above n 53, at 9; Blundell-Wignall, above n 53, at 169.

used to purchase goods in May 2010, and even then it cost 10,000 bitcoins to purchase pizzas worth USD 41.[393]

Satoshi Nakamoto, the pseudonymous creator of Bitcoin, identifies reliance on trust as a transaction risk associated with traditional payment systems.[394] The traditional non-reversibility of transactions requires financial institutions to price the costs of mediating disputes and pass those on to their customers.[395] Furthermore, Nakamoto points to the possibility in traditional payment systems to make reversible payments as creating higher transaction costs for the system as a whole as well as causing merchants to demand more information from their customers "than they would otherwise need".[396] Nakamoto's Bitcoin system reduces costs for transacting parties by letting them transact directly with each other without the need for a trusted third party.[397]

Related to the issue of trust is the issue of privacy. While all bitcoin transactions are announced publicly, the original intent was that parties maintain their privacy by keeping their public keys anonymous.[398] However, it is hard to be truly anonymous if the same public key is used for a series of transactions. Thus "pseudonymous" is a better term than anonymous. Some commentators struggle to understand the difference between anonymity and pseudonymity. Indeed, these mistaken commentators have argued that the high degree of anonymity associated with cryptocurrencies is the main driving force for the increased proliferation of these currencies.[399] Blundell-Wignall draws a link between the anonymity of cryptocurrencies and the demand for anonymous payment methods for illegal activities such as money laundering, terrorist financing, tax evasion and circumvention of financial regulations.[400] Yet, in truth, frustration with the traditional banking system is a large reason why cryptocurrencies have gained a foothold. As one person observed in an interview, "the last time I had to wire money out of my bank account, I had to go into the office, meet with a manager, fill out a bunch of paperwork, pay them like $20 and wait seven to 10 days".[401] Alternatively, had bitcoin been used the money could have been sent directly without requiring a bank's authorisation and, at the time, for a fraction of the cost and time.

Lam and Kuo Chuen identify a number of socioeconomic forces driving the demand for alternative currencies generally.[402] In addition to concerns about traditional banking systems and fiat currencies and the reduced transaction costs of cryptocurrencies discussed above, they list technological improvements driven by reduced barriers to entry and network effects, localism (concern for promoting local commerce), environmentalism, financial freedom (such as the ability to bypass capital controls), and the opportunity for speculative investment[403] as further factors influencing the development of alternative currencies.[404]

---

[393] Vigna and Casey *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order*, above n 62, at 79. Even then the bitcoin were not paid by the bitcoin owner to the merchant. Rather, another person purchased the pizza using his credit card and the bitcoin owner transferred the bitcoin to the purchaser.
[394] Nakamoto, above n 16 at 1.
[395] Ibid.
[396] Ibid.
[397] Ibid, see also Brito and Castillo, above n 369, at 10–12; Simon Barber, Xavier Boyen, Elaine Shi and Ersin Uzon "Bitter to Better — How to Make Bitcoin a Better Currency" (2012) 7397 Lecture Notes in Computer Science 399, at 401. See also Lam and Kuo Chuen, above n 53, at 8 and Richter, Kraus and Bouncken, above n 386, at 580.
[398] Nakamoto, above n 16, at 6.
[399] Blundell-Wignall, above n 53, at 7.
[400] Ibid.
[401] Steven Porter "Decentralize Clearinghouses: Regulators take Notice" (2016) <http://news.medill.northwestern.edu/chicago/Blockchain-could-decentralize-clearinghouses-regulators-take-notice/>.
[402] Lam and Kuo Chuen, above n 53, at 7–8. "Alternative currencies" is used in this context to capture all non-fiat currencies, not only digital non-fiat currencies.
[403] See also Brito and Castillo, above n 369, at 17–18.
[404] Lam and Kuo Chuen, above n 53, at 7–8.

Bitcoin and other cryptocurrencies' limited supply is attractive to some.[405] Fiat currency can and is created by central and retail banks, which devalues the fiat currency over time. Cryptocurrencies such as bitcoin contain a limited supply, which potentially allows the currency to hold its value.[406] It is for this reason that the People's Bank of China (China's central bank) suggested in January 2016 that it would like to launch its own cryptocurrency to cut the costs of circulating traditional paper money and boost policymakers' control of money supply.[407]

Finally, the development of cryptocurrencies is driven by the growing number of businesses and individuals who are willing to switch to them. While some businesses, such as PayPal, Dell, Lamborghini and Virgin Galactic, publicly declared that they accepted bitcoin,[408] the uptake was not high. However, this changed in some jurisdictions, for example when merchants in Japan gained the ability to accept payment in bitcoin at their point of sale machines.[409]

3.3 Cryptocurrencies after Bitcoin – not limited merely to payments

Notwithstanding that Bitcoin was developed as a "peer-to-peer electronic cash system",[410] relatively early on people began to realise that Bitcoin could be used for more than simply payments. A Whitepaper which proposed coloured coins was released in December 2012.[411] Bitcoin transactions contain space where information can be placed in addition to the time, public keys of the sender and receiver and the amount transacted. It was realised that the additional space could be used to store information such as the owner of certain property, including stocks, bonds, physical property and smart property.[412] With smart property the ownership of physical assets like a car would be represented as a token and the car could only be operated by the owner of the token.[413] For example, the owner's smart phone could have a near field communication (NFC) chip[414] that would only be activated when they unlocked their smart phone and the car doors and ignition would work only if it detected the activation of the NFC chip. Interestingly the idea of smart contracts was proposed in 1997 by Nick Szabo,[415] but the technology took many years to allow for the implementation of the idea. Almost more interestingly with the coloured coins[416] it was proposed that once, say, a company stock was issued and recorded on the Bitcoin blockchain, that "platform would easily allow sending Bitcoin dividends to shareholders, and allow shareholders to cryptographically vote".[417]

The idea of using Bitcoin for more than mere transfer of value was seized upon by Vitalik Buterin, a young Russian-born Canadian who released a Whitepaper in December 2013, "Ethereum

[405] Bitcoin is limited to 21 million coins.
[406] Al Moldof "Bitcoin developments: The Advance of Digital Currency" (2016) 31(4) Internal Auditing 38, at 41.
[407] Chen Aizhu "China's Central Bank Plans to Launch its own Digital Currencies" *Reuters Business News* (United States, online ed, 20 January 2016) <http://www.reuters.com/article/us-china-currency-digital-idUSKCN0UY1JT>.
[408] Chris Rose "The Evolution of Digital Currencies: Bitcoin, a Cryptocurrency Causing a Monetary Revolution" (2015) 14(4) International Business and Economics Research Journal 617, at 618.
[409] Kevin Helms "Rollout of 260,000+ Bitcoin-Accepting Stores in Japan Begins" *Bitcoin.com* (4 July 2017) <https://news.bitcoin.com/rollout-of-260000-bitcoin-accepting-stores-in-japan-begins/>.
[410] Nakamoto, above n 16.
[411] Meni Rosenfeld *Overview of Colored Coins* (Whitepaper, 4 December 2012) <https://bitcoil.co.il/BitcoinX.pdf>.
[412] Ibid
[413] Ibid.
[414] A NFC chip is a "near field communication chip" which allows two devices to communicate with each other. The devices containing the chip need to be close to each other, within 4 centimetres. NFC chips are used commonly. For example, they are inside contactless credit cards and are used for Android Pay, Apple Pay and Google Pay and so on.
[415] Szabo "The Idea of Smart Contracts", above n 155.
[416] The coloured protocol was built on top of the Bitcoin blockchain. It aimed to facilitate the trading of assets beyond bitcoin such as financial instruments, gold, or property using Bitcoin's underlying payment infrastructure.
[417] Rosenfeld, above n 411, at 1.

Whitepaper: A next-generation smart contract and decentralized application platform".[418] If Bitcoin was 1.0, Ethereum was 2.0. The introduction to the Ethereum Whitepaper included the following:[419]

> Commonly cited applications include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungible assets such as domain names ("Namecoin") as well as more advanced applications such as decentralized exchange, financial derivatives, peer-to-peer gambling and on-blockchain identity and reputation systems. Another important area of inquiry is "smart contracts" - systems which automatically move digital assets according to arbitrary pre-specified rules. For example, one might have a treasury contract of the form "A can withdraw up to X currency units per day, B can withdraw up to Y per day, A and B together can withdraw anything, and A can shut off B's ability to withdraw". The logical extension of this is decentralized autonomous organizations (DAOs) - long-term smart contracts that contain the assets and encode the bylaws of an entire organization. What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

While some cryptocurrencies, coloured coins aside, are designed for payments and thus as currencies, other cryptocurrencies are designed differently, albeit as the following shows there can often be overlap.

3.3.1 Utility tokens

Utility tokens are used within a blockchain itself and are often described as utility coins because they allow the holder to do something on the network.[420] For example, the decentralised file storage system Sia uses Siacoin: people can pay Siacoin for storing files on others' computers and those people in turn receive the Siacoin. Aragon tokens will be used by people who want their disputes heard by a decentralised court and can also be used to pay arbitrators who act as judges in disputes.[421] Utility tokens do more than simply allow people to access and use a blockchain: for instance, some can also be used by the holders to govern the blockchain, something that is planned to occur on Aragon.

While ether is certainly used as a currency, it is also part utility coin as some ether ("gas") is required to execute smart contracts on the Ethereum blockchain.[422] Thus if Bob and Alice create a smart contract for the sale of Bob's car to Alice so that Alice's payment to Bob goes through once certain conditions are satisfied,[423] then each transaction requires the payment of ether.[424] The transactions would be: Alice's payment of the purchase price to the smart contract; the shipping agent's

---

[418] Vitalik Buterin *Ethereum White Paper: A Next-generation Smart Contract and Decentralized Application Platform* (Whitepaper, December 2013) <https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>.

[419] At 1.

[420] Edmund Hillary Fellowship *New Zealand: Unlocking Blockchain's Potential: Recommendations on Regulation and Policy*"(December 2017) at 10 <https://static1.squarespace.com/static/57cd3bd059cc6804d1884b86/t/5a39dbbd419202030eebdc18/1513741249608/NZ+Unlocking+Blockchains+Potential+-+Dec+2017.pdf>.

[421] <https://aragon.one/network/> and see Luis Cuende and Jorge Izquierd *Aragon Network: A Decentralised Infrastructure for Value Exchange* (Whitepaper, Version 1.1, 20 April 2017) <https://bravenewcoin.com/assets/Whitepapers/Aragon-Whitepaper.pdf>.

[422] Thus "ether" refers to the cryptocurrency and "Ethereum" to its blockchain. For this and further explanations see the Glossary.

[423] See n 157 above and accompanying text.

[424] See generally, Danny Ryan "Costs of a Real World Ethereum Contract" *Hackernoon* (11 August 2017) <https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214>.

confirmation that the car had been delivered; the emission-testing agent's verification that the car had passed the test; the passing of ownership from Bob to Alice; and the payment to Bob.

3.3.2 Asset tokens

Asset tokens allow the tokenisation of property, so that the ownership/title to property such as a car in the example above is placed on the blockchain. Asset tokens make it is easy not only to see who the owner of an asset is, but also to transfer the ownership of that asset. Currently people buying goods second-hand take a risk because if they purchase goods from someone who is not the legal owner, the legal owner is entitled to claim those goods, despite the purchaser being the innocent party. The ownership of assets can also be split. Thus there may be 1,000 tokens for one house which multiple people could own.[425]

Car ownership in particular poses problems in New Zealand: the "registered owner" of a car is not necessarily the legal owner. The registered owner is the person who is entitled to possession of the car and is responsible for ensuring that it is safe to drive as well as for any licensing or traffic infringement fees.[426] Thus a person who purchases a car privately from the registered owner in the belief they now become the owner of the car may find themselves losing the vehicle. Alternatively, through a quirk of the Personal Property Securities Act 1999 (NZ), a person who leases a car to another can lose ownership of it if the lessee becomes the registered owner and obtains a loan and the lender registers a security interest over the car.[427]

3.3.3 Security tokens

New Zealand does not have the same security laws as other countries such as the US. The test in New Zealand as to what constitutes a regulated investment security (called a "financial product"[428] in New Zealand) is not exactly the same as in other countries, though it does include similar basic elements. Financial products fall into four categories: debt securities, equity securities, managed investment products and derivatives.[429] In addition, the Financial Markets Authority (FMA) has a designation power[430] and takes a substance-over-form approach, so it is possible that some cryptocurrencies will fall within the existing definition of a financial product – most likely because they are "managed investment products". Even if a cryptocurrency does not fall within any of the four baskets of financial product,[431] it may nevertheless come within the broader definition of a "security" and so be potentially subject to the FMA's designation power. That power means the FMA can declare a token that falls outside the four categories to be a financial product within one of the four.[432] However, that power cannot be exercised retrospectively[433] and requires the FMA to follow a consultation process first.[434]

---

[425] Omri Barzilay "Will Blockchain Ignite Fractional Ownership Market For Homes?" *Forbes* (United States, 7 August 2017) <https://www.forbes.com/sites/omribarzilay/2017/08/07/will-blockchain-ignite-fractional-ownership-market-for-homes/#1c29885b3370>. And see <https://atlant.io/>.

[426] New Zealand Transport Agency "Your Responsibilities as the Registered Person" <https://www.nzta.govt.nz/vehicles/how-the-motor-vehicle-register-affects-you/your-responsibilities-as-the-registered-person/>.

[427] Matthew Theunissen "Car Hire Business to Pay Heavy Price for Client's Alleged Fraud" *The New Zealand Herald* (online ed, 19 November 2017) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11944268>.

[428] Financial Markets Conduct Act 2013, s 7. Section 8 defines the different types of financial products.

[429] At s 7. Section 8 defines the different types.

[430] At s 562.

[431] At s 7: debt securities, equity securities, managed investment products and derivatives.

[432] At s 562.

[433] At s 564.

[434] At s 563(1)(d).

3.4 How cryptocurrencies work

This section looks at how cryptocurrencies work from a payments system point of view and not as a registration system for assets, or at their use in smart contracts or other uses. Traditionally, and as is currently the practice with fiat currency, the central bank is responsible for validating transactions and holds a central ledger that records the funds of each bank. In turn banks keep ledgers containing entries of their customers' money. In contrast, the records for cryptocurrencies are held by hundreds or thousands of computers on a distributed ledger. Each computer has its own identical copy of the blockchain. There is no central authority such as a central bank to validate transactions.

Within the constraints above, this section provides an overview of how cryptocurrencies work, their features, the differences between them and why the differences are important. On 21 April 2018 the website coincap.io listed 1,262 different coins,[435] and there will be more. Some are based on Bitcoin's source code, with modifications,[436] while others have been created from scratch,[437] albeit most are ERC-20 tokens.[438] Cryptocurrencies differ from each other in many ways, including how they are created and distributed; whether there is a fixed limit on the number of coins or tokens available; whether "pre-mining" has occurred; whether PoW or PoS is used; the rate of rewards for miners and whether it changes; whether transaction fees are charged; and whether the cryptocurrency has demurrage (a concept explained at Section 3.4.5 below).

Each cryptocurrency has its own blockchain. As the name suggests, the blockchain comprises a series of blocks chained together. The Bitcoin blockchain in effect records how many, for example, bitcoins or parts of a bitcoin a person owns. The names of people or organisations are not used; rather the bitcoin is linked to a public key, and the person who controls that public key controls the bitcoin. (Just as dollars are divisible, so too are cryptocurrencies, only more so: instead of, for instance, being divisible down to one cent, bitcoin is divisible down to one-hundredth-of-a-million of one bitcoin.)

Just as a person who has $1,000 in a New Zealand bank account does not physically hold that $1,000, the owner of a bitcoin does not physically hold the bitcoin. While in theory the bank account holder can go to the bank or ATM and withdraw that money in bank notes, if every person attempted to convert their bank accounts to bank notes there would be a run on the banks and New Zealand would be plunged into crisis – most of the money in New Zealand is digital and not in the form of notes. One of the key distinctions between cryptocurrencies and fiat currencies when the latter are held in bank accounts is that the money in the bank account no longer belongs to the bank account holder.[439] The money is now the bank's and the relationship is one of creditor (bank account holder) and debtor (bank).[440]

Unlike in the case of a bank account, where the money is held under a person or entity's name, cryptocurrencies are ascribed to a private key, and whoever possesses that private key can be seen as "owning" the cryptocurrency, and cannot be prevented from spending that money. Contrast the bank account, where the bank can prevent the release of money as the money no longer belongs to the account holder. The disadvantage of cryptocurrencies is therefore that if a person loses or forgets their private key they lose access to their cryptocurrencies.[441] The legal status of issues

---

[435] <https://coincap.io.>.

[436] Franco, above n 53, at 171.

[437] For example, XEM, which is the coin used on the NEM Blockchain.

[438] Token that complies with a list of rules that an Ethereum token has to implement. Once the rules are met the token can be used on the Ethereum ecosystem. Most ICOs have used ERC-20 tokens, with many then going on to create their own blockchains: EOS is one such example.

[439] *Foley v Hill* (1848) 2 HLC 28, 9 ER 1002.

[440] See, for example, Kelvin FK Low and Ernie GS Teo "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9 Law, Innovation and Technology 235 and Tatiana Cutts and David Goldstone "Bitcoin Ownership and its Impact on Fungibility" *Coindesk* (14 June 2015) <www.coindesk.com/bitcoin-ownership-impact-fungibility/>.

[441] See Section 4.9.2 Loss of private keys and passwords below.

surrounding the ownership of cryptocurrencies is beyond the scope of this report, but it does raise serious questions.[442]

If money is digital, how do you stop the same money being spent twice (or even an infinite number of times)? The genius of the blockchain is that it solves the double-spend conundrum (a person being able to spend the same money twice) without the need for a trusted central entity or other third parties.[443]

Once a block is created and is joined to the preceding block, that block is replicated on all the computers that host the blockchain. The records of transactions contained within each block are immutable once a certain number of blocks have been added; with Bitcoin that is normally regarded as six blocks. If a person wishes to spend their bitcoin they need to submit their private key and the blockchain is checked to see whether the public key that corresponds with the private key holds that amount of bitcoin. So long as the majority of nodes (computers that hold the blockchain ledger) show that the public key does hold that bitcoin, the bitcoin the person wants to transfer will be transferred and the transaction will be recorded on the blockchain. The public key to which the person sent the bitcoin will now be recorded as the owner of that particular bitcoin transaction.

To keep the cryptocurrency blockchains running and the checking and verification done, some form of payment or reward is normally required. The form of payment of reward is looked at below. Not all blockchains require payment or rewards to be made: for example, IOTA has an elegant solution and requires anyone who wishes to make a transaction to validate other transactions.[444]

3.4.1 Creation and distribution of coins

There is significant variation in the way that cryptocurrencies are created and distributed. This section looks at the main differences between the cryptocurrencies.

3.4.1.1 Pre-mining of coins

Pre-mining occurs where a portion or even the whole of the total possible monetary supply of a currency is created prior to the currency being launched. Invented in Iceland, Auroracoin is an example, since 50 per cent of Auroracoin was pre-mined, with the remaining 50 per cent available to be mined in the same manner as bitcoin. The residents of Iceland received the 50 per cent share of pre-mined Auroracoins.[445] Bitcoin, in contrast, had no pre-mining.

3.4.1.2 Limited or unlimited supply of cryptocurrency

Another feature of some cryptocurrencies is that the new coins are created when they are released to the miners. Some cryptocurrencies are limited in the total coins that can ever be released. Bitcoin, for instance, has a limit of 21 million coins. When no new bitcoins are available for miners, increasingly higher transaction fees may be required.[446] Another cryptocurrency that has a limited supply is Litecoin.[447]

At first glance it might appear good that cryptocurrencies have a natural limit because new coins cannot be created at will, unlike fiat currency; however, it has been argued that a limited supply

---

[442] Someone can hand over their private key to another for that person to deal with the cryptocurrency on their behalf. That person, of course, does not become the owner of the cryptocurrency.
[443] Gerald P Dwyer "The Economics of Bitcoin and Similar Private Digital Currencies" (2015) 17 Journal of Financial Stability 81, at 82.
[444] Popov, above n 40.
[445] Franco, above n 53, at 175.
[446] Barrdear and Kumhof, above n 334, at 7 <http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>.
[447] Litecoin's limit is 84 million coins.

means that such cryptocurrencies are deflationary in nature,[448] which would limit their ability to be units of account and thus limit their use as money.[449]

3.4.2 Proof-of-work versus proof-of-stake (consensus)

3.4.2.1 Proof-of-work

Proof-of-work (PoW) has been described in Section 2.5.3.1 above. In short, PoW means that considerable computing power must be used to hash – that is, form – each block. The computing power is used to solve a complex mathematical puzzle. When a block is successfully hashed, this is considered PoW. While the solving of the puzzle is difficult and expensive as it takes large amounts of electricity, it is easy for others to verify.

Bitcoin uses a PoW function for distribution.[450] Among the cryptocurrencies which use PoW functions for distribution, there are also variations in the function used. Bitcoin, Namecoin, Peercoin and a number of other cryptocurrencies use the secure hash algorithm SHA-256.[451] Litecoin and Dogecoin use scrypt, another popular cryptographic function.[452] Primecoin uses a PoW function that searches for chains of prime numbers, which has the added benefit of assisting academics researching the nature and distribution of prime numbers.[453]

3.4.2.2 Proof-of-stake

Some cryptocurrencies use PoS instead of PoW, including ShadowCash, Nxt, BlackCoin and NavCoin. PoS, unlike PoW, does not depend on computational work for the creation of new coins.[454] Rather, new coins are awarded to existing currency holders in proportion to their holdings. Some PoS awards take into account not only the value of coins held but also the time since these funds were last spent.[455]

While PoW is technically more secure than PoS, the computing power required for PoW is sizeable: one of the criticisms of Bitcoin is the large amounts of electricity needed to run it due largely to the PoW requirement.[456] O'Dwyer and Malone estimate that in early 2014 the total electricity costs of maintaining the Bitcoin network roughly equalled the electricity consumption of Ireland.[457] Considerably more electricity is used now. Because of the power demands of PoW, work is being done on Ethereum, one of the most prominent blockchains, to move from PoW to a hybrid PoW/PoS system.[458] Some cryptocurrencies, such as Peercoin, already operate a hybrid PoW/PoS system.[459]

---

[448] Barber, Boyen, Shi and Uzon, above n 397, at 404.
[449] "Money from nothing: Chronic Deflation may keep Bitcoin from Displacing its Fiat Rivals" *The Economist* (UK, online ed, 15 March 2014) <https://www.economist.com/news/finance-and-economics/21599053-chronic-deflation-may-keep-bitcoin-displacing-its-fiat-rivals-money>.
[450] Nakamoto, above n 16, at 5.
[451] See further CoinGecko <https://www.coingecko.com/en?hashing_algorithm=SHA-256>.
[452] See further CoinGecko <https://www.coingecko.com/en?hashing_algorithm=Scrypt>.
[453] Franco, above n 53, at 175–176.
[454] At 234–236.
[455] At 234.
[456] Quiggin "Bitcoins are a Waste of Energy – Literally", above 294.
[457] Karl J O'Dwyer and David Malone "Bitcoin Mining and Its Energy Footprint" (2014) Proceedings of Irish Signals and Systems Conference 280 <https://ieeexplore.ieee.org/document/6912770/> cited by Barrdear and Kumhof, above n 334, at 6. <http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>.
[458] See Vitalik Buterin and Virgil Griffith "Casper the Friendly Finality Gadget" (15 November 2017) <https://arxiv.org/abs/1710.09437> and see Timothy MaCallum "First Impressions of Ethereum's Casper — Proof of Stake (PoS)" (5 January 2018) Medium (5 January 2018) <https://medium.com/cybermiles/first-impressions-of-ethereums-casper-proof-of-stake-pos-5ce752e4edd9>.
[459] Franco, above n 53, at 173.

3.4.2.3 Other forms of consensus

As noted above in Section 2.5.3.3, other consensus methods are also being used.

3.4.3 Block generation speeds

A critical aspect of cryptocurrencies is how quickly blocks are created. Blocks in the Bitcoin blockchain are generated on average every 10 minutes. The relatively slow block generation speed poses problems. For example, it is possible for someone to double spend bitcoin during that time – a chink in Bitcoin's armour against double spending. For higher-value transactions merchants and others receiving payment should not release goods until the transaction has been confirmed by six blocks, which will take around 60 minutes.

Blocks in the blockchain of other currencies are generated at different rates. Dogecoin blocks are generated every minute, Ethereum blocks every 14 to 15 seconds. The advantage of fast block generation speeds is faster transaction times.[460] However, while high block generation speeds benefit merchants by letting them confirm transactions quickly, they can result in reduced security for the cryptocurrency.[461] Ethereum incorporates an additional protocol known as the GHOST protocol to counteract the reduced security associated with its faster generation.[462] Other blockchains boast still quicker times than Ethereum – for example, Steem has a block time of three seconds.[463]

3.4.4 Rate of change of rewards

Whether the reward for mining changes and, if so, the rate at which the reward changes, is a further feature that differs between cryptocurrencies. The reward for finding a block for Bitcoin halves every 210,000 blocks, approximately every four years, and is called the halving. This decreasing function is the origin of the limit of 21 million bitcoins that can possibly be generated.[464] It is expected that the last bitcoin will be mined in 2040.

The PoS block reward for Peercoin grows at one per cent per year. In the long run, this means that the inflation of the currency will occur at one per cent per year, less the value of the currency lost in destroyed transaction fees.[465]

The rewards for the cryptocurrency Ethereum do not change.[466] This means the rate of inflation of the currency is a decreasing function, trending towards zero per cent per year as the rate at which new coins are mined becomes a smaller and smaller proportion of the total number of coins in existence. Dogecoin is similar in this regard.[467]

3.4.5 Transaction fees

For cryptocurrencies where miners are rewarded with cryptocurrency when they create a block successfully, there may be no need to charge transaction fees if the block reward is sufficient to

---

[460] "Why is Ethereum Different to Bitcoin?" (6 September 2016) CryptoCompare <https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin/>.
[461] Vitalik Buterin "Toward a 12-second Block Time" (11 July 2014) Ethereum Blog <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/>.
[462] "What is the GHOST protocol for Ethereum?" (29 February 2016) CryptoCompare <https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/>.
[463] <https://steem.io/>, see Priyab Satoshi "Steem (STEEM) — Blockchain-based Social Media Platform" (20 August 2017) Medium <https://medium.com/crypt-bytes-tech/steem-steem-blockchain-based-social-media-platform-889f7f3c3245>.
[464] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker and Stefan Savage "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" (paper presented to ACM SIGCOMM Internet Measurement Conference, Barcelona, Spain, 2013) at 128 <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>.
[465] Franco, above n 53, at 174.
[466] "Why is Ethereum different to Bitcoin?", above n 460.
[467] Franco, above n 53, at 174.

compensate miners for their work. However, falling block rewards may force transaction fees to rise.[468]

With bitcoin, transaction fees are optional and variable.[469] While bitcoin transaction fees were initially zero and then very low, [470] they rose to high levels,[471] but have since fallen,[472] albeit there are other cryptocurrencies with considerably cheaper fees. The greater the fee attached to a transaction, the faster the transaction will be processed.[473] The fee is an incentive for a particular miner to process the transaction. Some other currencies deal with fees differently. With Peercoin, for example, transaction fees are fixed at 0.01 PPC (the Peercoin currency symbol) per transaction. Unlike with bitcoin, the transaction fee for Peercoin is not received by the party processing the transaction; the fee is destroyed.[474]

At first Bitcoin was able to operate on no or low transaction fees because of the reward of cryptocurrency for successful miners: the block reward.[475] There is concern that as the returns provided by mining decrease (or even disappear once the 21 million bitcoin have been mined) mining transaction fees will need to rise.[476] Not only is the number of bitcoins limited to 21 million, the reward that successful miners receive for completing a block halves every four years. It has been argued that cryptocurrencies will have higher costs and will only be able to compete with centralised systems if the number of miners falls.[477] Reducing the number of miners runs contrary to the original design of Bitcoin and exposes the system to greater risks.[478] However, with the increase in the price of bitcoin that has occurred in the past, the block halving becomes irrelevant. At the last halving in 2016, when the block reward reduced from 25 to 12.5 bitcoins,[479] one bitcoin was worth around USD 660. As of 26 August 2018, bitcoin sits at USD 6,671. To be sure, bitcoin prices have dropped dramatically a number of times and there is an argument that people will stop mining if the price of bitcoin falls. But this argument shows a lack of understanding of how bitcoin works. The difficulty is adjusted. If fewer people are mining the difficulty level drops, thus drawing new miners in. In contrast, if more people begin to mine the difficulty increases.[480]

Alternatively new blockchains have devised methods so that transaction fees are not payable.[481]

---

[468] Mark Carney "The Future of Money" (speech to the inaugural Scottish Economics Conference, Edinburgh University, Scotland, March 2018) at 8 <https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418>.

[469] "Transaction Fees" (last modified 22 November 2016) bitcoinwiki <https://en.bitcoin.it/wiki/Transaction_fees>.

[470] The transaction fees of most cryptocurrencies are extremely low, often well below 0.05% of the transaction's value: Barrdear and Kumhof, above n 334, at 7.

[471] At one stage bitcoin fees were USD 20 per transaction: see Kai Sedgwick "Bitcoin Fees have Become Infeasible" *Bitcoin.com* (17 December 2017) <https://news.bitcoin.com/bitcoin-fees-have-become-infeasible/>.

[472] On 27 July 2018 the fee was USD 0.15 per transaction to have the transaction mined on the next block (10 minutes), USD 0.15 to have it mined within three blocks (30 minutes) or, for those prepared to wait, USD 0.04 to be mined within the next six blocks (one hour). For a website that shows fees in real time see <https://bitcoinfees.info/>.

[473] Justin O'Connell "The Quick Death of the Zero-Fee Bitcoin Transaction" *Crypto Coins News* (21 May 2016) <https://www.cryptocoinsnews.com/death-zero-fee-bitcoin-transaction/>.

[474] Franco, above n 53, at 174. The purpose of destroying the fee is to prevent inflation by deflating the money supply.

[475] See Kerem Kaskaloglu "Near Zero Bitcoin Transaction Fees Cannot Last Forever" (paper presented to the International Conference on Digital Security and Forensics (DigitalSec2014), Czech Republic, June 2014) <http://sdiwc.net/digital-library/near-zero-bitcoin-transaction-fees-cannot-last-forever.html>.

[476] See Ali, Barrdear, Clews and Southgate, above n 387, at 281.

[477] Ibid.

[478] Ibid.

[479] Aaron van Wirdum "How Bitcoin's Second Halving Came and Went, and Not Much Happened" *Bitcoin Magazine* (18 July 2016) <https://bitcoinmagazine.com/articles/how-bitcoin-s-second-halving-came-and-went-and-not-much-happened-1468856719/>.

[480] P Buninx "What is the Mining Difficulty?" *The Merkle* (14 April 2017) <https://themerkle.com/what-is-the-mining-difficulty/>.

[481] IOTA and EOS.

3.4.5 Demurrage

In the context of cryptocurrencies, demurrage is tax on holding units of a currency,[482] and it is designed to make people spend money, not hoard it.[483] Freicoin uses demurrage. A fraction of each transaction is levied in proportion to the time since the coin was last used. This essentially operates as a negative interest rate on currency holders. Freicoin's demurrage fee is approximately five per cent per year.[484] Freicoin has not proved popular though. On 13 April 2018 it was worth only USD 0.0047.[485]

4. Arguments against cryptocurrencies

Many arguments have been made against the use of cryptocurrencies. This section examines those arguments and explains why some are ill-founded. For those drawbacks that remain live issues, many can be solved, whether by changes to technology underlying cryptocurrencies, regulation or a combination of both. Specific potential risks for consumers are addressed in Section 4.9.

4.1 Cryptocurrencies are not money

The argument is often made that cryptocurrencies are not money and therefore not a currency.[486] Much work has been done to determine whether cryptocurrencies meet the definition of money.[487] In some cases internationally, cryptocurrencies have been held by the courts to be a currency and thus money;[488] however, equally they have been treated as commodities[489] and there are arguments that some cryptocurrencies may be securities.[490] For example, William Hinman from the (US) Securities and Exchange Commission recently noted that:[491]

> Promoters … to raise money to develop networks on which digital assets will operate, often sell the tokens or coins rather than sell shares, issue notes or obtain bank financing. But, in many cases, the economic substance is the same as a conventional securities offering. Funds are raised with the expectation that the promoters will build their system and investors can earn a return on the instrument – usually by selling their tokens in the secondary market once the promoters create something of value with the proceeds and the value of the digital enterprise increases.

Hinman also noted that even if the digital asset had started out as a security it would not necessarily remain a security for all time: for example, if the "digital asset is sold only to be used to purchase a good or service available through the network on which it was created."[492]

The debate over the classification of cryptocurrencies as currency or not is, however, largely redundant. If governments through their respective legislatures declare cryptocurrencies, or some of

---

[482] Swan, above n 166, at 75.
[483] Franco, above n 53, at 177.
[484] <http://freico.in/about/>.
[485] <https://Coincap.io>.
[486] See, for example, David Yermack "Is Bitcoin a Real Currency? An Economic Appraisal" in David KC Lee (ed) The Handbook of Digital Currency (Elsevier, 2015) 31 and Mazin Sidahmed "Bitcoin 'Not Real Money' says Miami Judge in Closely Watched Ruling" *The Guardian* (UK, online ed, 26 July 2017) <https://www.theguardian.com/technology/2016/jul/26/bitcoin-not-real-money-miami-judge>.
[487] See eg Dong He et al, above n 68, at 1017.
[488] *US v Murgio*, No 15-cr-769 (AJN) (Southern District of New York, 12 January 2017).
[489] *Commodity Futures Trading Commission v McDonnell*, 6 March 2018 Memorandum & Order (Eastern District of New York).
[490] Peter Valkenburgh *Framework for Securities Regulation of Cryptocurrencies Version 1* (Coin Center Report, January 2016) <https://coincenter.org/wp-content/uploads/2016/01/SECFramework2.5.pdf>.
[491] Willam Hinman "Digital Asset Transactions: When Howey Met Gary (Plastic)" (paper presented to Yahoo Finance All Market Summit, San Francisco, United States, June 2018) <https://www.sec.gov/news/speech/speech-hinman-061418#_ftn3>.
[492] Ibid. Hinman gives only a qualified "yes" in the situation.

them, to be money, they will be money. If businesses in New Zealand accept cryptocurrencies as payment for goods and services, the average person will believe that they are akin to money, as has occurred in Japan where merchants have the ability to accept bitcoin at their point of sale machines.[493] Furthermore, to not recognise that cryptocurrencies are money can bring unintended consequences. For example, Australian tax law treated bitcoin transactions, and thus other cryptocurrency transactions, as a form of barter and as such Goods and Services Tax (GST) was chargeable when people purchased bitcoin and then used it to buy goods or services. Consumers who converted Australian dollars to bitcoin lost one-eleventh in each transaction.[494] The Australian Senate Economics References Committee in its report "Digital currency – game changer or bit player" acknowledged the disparity of treatment between Australian dollars and cryptocurrencies and recommended to the Government that cryptocurrencies be treated as money for the purposes of GST. [495] The New Zealand IRD did not state until April 2017 how it would treat cryptocurrencies.[496] Prior to that it had been reported that the IRD would treat cryptocurrencies the same as foreign currencies.[497] The IRD has since provided some guidance on cryptocurrencies.[498]

Indeed, the IRD, in an Issues Paper released in June 2018, sought information on how to treat the payment of cryptocurrencies by employers to their employees as part of their employees' remuneration.[499] This question is not hypothetical, as the IRD notes "[i]t is becoming more common for employees (particularly those working in cryptocurrency-related industries) to receive regular remuneration in cryptocurrency."[500] The question is whether cryptocurrencies can be regarded as salary or wages for the purposes of the Income Tax Act 2007 or are they caught under fringe benefit tax (FBT). While salary and wages are normally thought of as requiring the payment of money and cryptocurrencies are not currently thought of as money, section 6 of the Interpretation Act 1999 provides that old legislation must be interpreted as applying to modern circumstances.[501] In addition, PAYE covers non-monetary benefits, for example, employer-provided accommodation.[502] On that basis the IRD has tentatively suggested that the regular payments to employees of cryptocurrencies are able to come within the concepts of salary and wages.[503]

An argument levelled against cryptocurrencies related to the classification question is that people primarily utilise them as a speculative investment rather than as a currency,[504] and also that the other primary uses are by criminals, or in cross-border payments or gambling.[505] However, the

---

[493] Helms, above n 409.
[494] Economics References Committee, above n 66, at [4.9].
[495] At [4.35]. The Australian Treasury released the Discussion Paper "GST Treatment of Digital Currency" (May 2016) <http://www.treasury.gov.au/~/media/Treasury/Consultations%20and%20Reviews/Consultations/2016/GST%20treatment%20of%20digital%20currency/Key%20Documents/PDF/GST_treatment_of_digital_currency.ashx>, in which it proposed either treating cryptocurrencies as money for the purposes of GST or making their purchase GST exempt.
[496] There were calls relatively early on for clarity in New Zealand over the treatment of cryptocurrencies for tax purposes. See Frances Mazzanti "Bitcoins and other Digital currencies – emerging tax treatment" Johnston Associates South (21 August 2014) <https://jacalsouthisland.nz/bitcoins-and-other-digital-currencies-emerging-tax-treatment/>.
[497] Gareth Vaughan "IRD says Bitcoin should be Treated in the Same Manners as Foreign Currencies for Tax Purposes" *Interest.co.nz* (New Zealand, 23 July 2014) <http://www.interest.co.nz/personal-finance/71048/ird-says-bitcoin-should-be-treated-same-manner-foreign-currencies-tax>.
[498] Inland Revenue Department "Questions & Answers: Cryptocurrency and tax" <http://www.ird.govt.nz/income-tax-individual/cryptocurrency-qa.html> and see Section 6.1.1 Tax treatment below.
[499] Inland Revenue Department "No. 11: Whether Reumeration Paid to an Employee in Cryptocurrency is Subject to PAYE or FBT" Issues Paper (20 June 2018) <https://www.ird.govt.nz/resources/9/b/9be098bb-7db4-40b6-84c3-0bbb0b5b8885/irruip11.pdf>.
[500] At 4.
[501] At 13
[502] At 12 and 18 and see Income Tax Act CE 1(1)(bb).
[503] At 18.
[504] Yermack, above n 486 and Kumar and Smith, above n 310, at 28.
[505] Kumar and Smith, above n 310, at 28.

greater the adoption and use of cryptocurrency, the more of a broad-use currency they will become. Indeed, the sources relied upon to show that usage is for speculation, criminal activities, cross-border payments and gambling dated from 2013 and 2014,[506] when there were few ways available to actually use bitcoin. In regard to use by criminals, the UK Treasury assessed cryptocurrencies as a low risk.[507] The current banking system is too easy for criminals to use to launder money[508] so there is no need for criminals to change from something that works for them.[509]

4.2 Cryptocurrencies are anonymous and only criminals and terrorists will want to use them

Some equate bitcoin with criminal activity because of its use on the Dark Web such as the so-called Silk Road, where it was used to purchase drugs, weapons and other illegal goods.[510] Yet the demise of the Silk Road did nothing to affect bitcoin, although bitcoin has yet to shake unfortunate reputational damage.[511] Others claim that bitcoin is ideally suited for use by terrorists.[512] Nevertheless, bitcoin was not the necessary ingredient that allowed people to purchase illicit and harmful goods or fund terror; bank notes have long been the payment instrument of choice for criminals. As observed already, the UK Treasury has rated cryptocurrencies as low risk for the funding of terrorists' activities.[513] Indeed, so mindful of the ability of bank notes to facilitate illegal activity have some central banks been that they have withdrawn high-denomination notes, or are planning to remove such notes from circulation.[514] The risk of counterfeit bank notes is a concern, to the point that it is common for shops in the UK to refuse to accept £50 notes.[515]

Any technology can be used for good and bad.[516] Gift cards are used to launder large amounts of money;[517] so too are self-published books on Amazon.[518] However, just as not all gift cards and self-

---

[506] Ibid citing F Glaser, K Zimmermann, M Haferkorn, MC Weber and M Siering "Bitcoin – Asset or Currency? Revealing Users' Hidden Intentions" (paper presented in Proceedings of the European Conference on Information Systems (ECIS), Tel Aviv, Israel 2014) <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1131&context=ecis2014> and "All about Bitcoin" Global Macro Research Top of Mind 21, Goldman Sachs (11 March 2014) <https://www.coursehero.com/file/15396844/GoldmanSachs-Bit-Coin/>.

[507] United Kingdom HM Treasury "National Risk Assessment of Money Laundering and Terrorist Financing", above n 89, at [5.3].

[508] McKenzie, Baker and Mitchell, above n 13.

[509] Pamela Williams "How Criminal Gangs Ran Rings Around Commonwealth Bank Culture" *The Australian* (online ed, 14 September 2017) <https://www.theaustralian.com.au/news/inquirer/austrac-uncovers-unreported-money-laundering-at-commonwealth-bank/news-story/66e21b2a59faf2cf3fad10acc013be8c> and see Australian Prudential Regulation Authority "Prudential Inquiry into the Commonwealth Bank of Australia (CBA) Final Report" (April 2018) <http://www.apra.gov.au/AboutAPRA/Documents/CBA-Prudential-Inquiry_Final-Report_30042018.pdf>.

[510] Zoe Gross "The Dark Side of the Coin: Bitcoin and Crime" *FinFeed* (5 September 2017) <https://finfeed.com/features/dark-side-coin-bitcoin-crime/>.

[511] Marco Santori "Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise" *Coindesk* (5 May 2017) <https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/>.

[512] Carmona, above n 98, at 127–135, arguing that Bitcoin is ideally suited for use by terrorists.

[513] Richard Henderson, global security strategist at data security firm Absolute, quoted by Jack Marx "Will Crime be the End of Bitcoin?" *CEO Magazine* (online ed, May 2017) <https://www.theceomagazine.com/business/will-crime-be-the-end-of-bitcoin>.

[514] Anirban Nag and Vrishti Beniwal "India's Scramble to Switch 23 Billion Banknotes: QuickTake Q&A" *Bloomberg* (United States, 15 November 2016) <https://www.bloomberg.com/news/articles/2016-11-15/india-s-scramble-to-switch-23-billion-banknotes-quicktake-q-a>.

[515] Lee Boyce "Are Shops Allowed to Refuse £50 Notes Even though they are Legal Tender - and Will We Get New Polymer Ones to Beat Fakes?" *This is Money* (UK, 1 August 2017) <http://www.thisismoney.co.uk/money/experts/article-4749554/Can-shops-legally-refuse-50-html>

[516] United Kingdom Government Chief Scientific Adviser, above n 15, at 7.

[517] Lauren Gensler "The Idiot's Guide to Laundering $9 Million" *Forbes* (United States, 11 January 2017) <https://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering/#de4b56814496>.

[518] Aarron Pressman "How an Amazon Self-Published Book May Be the Latest Money Laundering Scam" *Fortune* (United States, 11 February 2018) <http://fortune.com/2018/02/22/money-laundering-books-amazon/>.

published books are a means to launder money, not all holders of cryptocurrency are using it to launder money or engage in other forms of criminal activity. As a security consultant observes, "getting rid of Bitcoin to stop ransomware would be like the US Government getting rid of $100 bills to try to stop drug dealers from laundering their dirty money".

To be sure, demands for payment in bitcoin have been made in ransomware attacks, but such attacks existed well before Bitcoin was invented: Bitcoin did not create ransom attacks; in fact, Western Union and PayPal were commonly used.[519] A recent study shows that the amounts of bitcoin received by criminals using ransom were considerably lower than people would expect. [520] The study estimated the lower bound direct financial aspect of ransomware between 2013 and mid-2017 was nearly USD 13 million.[521]

Behind a large part of people's fear of criminals wanting to use bitcoin and other cryptocurrencies is the fact that cryptocurrencies can deliberately obscure users' identity. However, it is inaccurate to say that bitcoin and similar cryptocurrencies allow for anonymous transactions; rather they allow pseudonymous transactions. It is possible for a skilled computer scientist to work out who is sending or receiving bitcoin. For example, investigators were able to catch a former US Secret Service agent who extorted bitcoin during an investigation into the Silk Road.[522] Despite that, privacy coins such as ZCash and Monero[523] can be used to hide not only the participants, but also the value of the transactions; it may well be that Monero begins to be used for ransomware attacks rather than bitcoin.[524]

Given that transactions are recorded on the blockchain,[525] a criminal would be unwise to use bitcoin and similar cryptocurrencies, because once the criminal's public key is known all the transactions to and from that address can be seen. If a criminal is caught with drugs and cash they can be charged with one crime, but if they are caught selling drugs using bitcoin then in effect their books have been discovered and the authorities now have their criminal history.[526]

4.3 Cryptocurrencies cannot scale

A common criticism of bitcoin in particular is that it is too slow and is therefore unsuited as a currency as it cannot scale to facilitate large numbers of payments. For example, the Governor of the Reserve Bank of Australia (RBA) said in December 2017:[527]

---

[519] Danny Palmer "How Bitcoin Helped Fuel an Explosion in Ransomware Attacks" *ZDNet* (22 August 2016) <https://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/>.
[520] Masarah Paquet-Clouston, Bernhard Haslhofer and Benoit Dupont "Ransomware Payments in the Bitcoin Ecosystem" (paper presented to 17th Annual Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, April 2018) <https://arxiv.org/pdf/1804.04080.pdf>.
[521] Ibid.
[522] "Silk Road: US agent jailed over bitcoin theft" *BBC News* (UK, 8 December 2015) <http://www.bbc.com/news/technology-35038971>.
[523] See nn 224–225 above.
[524] Danny Palmer "Ransomware: Why the Crooks are Ditching Bitcoin and Where they are Going Next" *ZDNe*t (15 February 2018) <https://www.zdnet.com/article/ransomware-why-the-crooks-are-ditching-bitcoin-and-where-they-are-going-next/>.
[525] With the lightning network and similar networks not all transactions will necessarily be recorded on the blockchain itself.
[526] John Bohannon "Why Criminals Can't Hide Behind Bitcoin" *Science* (United States, 9 March 2016) <https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>.
[527] Philip Lowe "An eAUD?" (speech to the 2017 Australian Payment Summit, Sydney, Australia, December 2017) <https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html>.

> [t]he number of payments that can currently be handled [by Bitcoin] is very low, there are governance problems, the transaction cost involved in making a payment with Bitcoin is very high and the estimates of the electricity used in the process of mining the coins are staggering.

Certainly, even with Bitcoin's lightning network, it is unlikely to be able to compete even with the Visa and MasterCard networks. However, bitcoin was just the first cryptocurrency. To judge cryptocurrencies by bitcoin would be akin to dismissing powered flight because the first aeroplanes by Richard Pearse and the Wright brothers were clumsy. The technology is still maturing, and is barely one decade old, yet in tests Red Belly Blockchain has shown that it can process payments considerably faster than Visa's network.[528]

4.4 Bitcoin's code cannot be altered

Arguments have been made that Bitcoin's code cannot be altered. However, while it took a long time, Bitcoin's code was altered in August 2017 in an attempt to reduce transaction fees. Indeed, the inability of Bitcoin to be changed easily is viewed by many as one of its strengths and sees it treated by some as digital gold rather than a global payments vehicle.[529]

4.5 Some cryptocurrencies can be changed arbitrarily

In contrast to the extreme difficulty of changing Bitcoin's software, other cryptocurrencies arguably suffer from the ability to be changed too easily.[530] If software can be changed at will this will damage the cryptocurrency's credibility and dampen the uptake.

4.6 Financial instability

If people and organisations turn away from using banks to make payments, the banks and other financial institutions could experience a decline in profits. While some would rejoice at falling bank profits,[531] the RBNZ has sounded a warning:[532]

> Stress test results reveal that the profitability of New Zealand banks provides a buffer against losses in downturn scenarios where a large number of creditors default on their loans. Lower profitability results in a smaller buffer against potential losses caused by an economic downturn, and also reduces access to international capital markets as the cost of funds increases in proportion to the riskiness of the bank.

The RBNZ's warning was not directed solely at cryptocurrencies, but rather at various disrupters; cryptocurrencies were just one, another being peer-to-peer lending programmes.[533] The RBNZ noted that the soundness of the financial system was a concern, for if more competitors entered the banking sector this would reduce the number of "systemically important banking entities" and "may alleviate the 'too-big-to-fail' risk".[534] The RBNZ did, however, go on to acknowledge that:[535]

> In a more hypothetical long term scenario, banks may be challenged to change the fundamental model of banking in order to meet the demands of Millennials as they progress through life…. digital

---

[528] <http://redbellyblockchain.io/> and see Campbell, above n 270.
[529] Luke Parker "For Bitcoin, is Being a Store of Value More Important Than a Payment System?" *Coindesk* (17 November 2017) <https://bravenewcoin.com/news/for-bitcoin-is-being-a-store-of-value-more-important-than-a-payment-system/>.
[530] See Ammous "Can Cryptocurrencies Fulfil the Functions of Money?", above n 107.
[531] Richard Meadows "Q&A: Are Australian banks really rorting New Zealanders?" *Stuff* (New Zealand, 3 November 2016) <http://www.stuff.co.nz/business/money/73626116/Q-A-Are-Australian-banks-really-rorting-New-Zealanders>.
[532] Wadsworth "Disruption or distraction?", above n 69, at 12.
[533] Ibid.
[534] At 14.
[535] At 12.

> disruptors are more likely to have a stronger relationship with younger customers (or Millennials) which could pose a considerable threat to the business models of incumbent banks.

The RBNZ was clear that it in the medium to long term the digital disruption to the banking sector may improve the financial system's efficiency.[536]

Decentralised cryptocurrencies are at most a long-term threat to retail banks. More immediate threats are open banking[537] as well as competition from tech giants. In the UK it has been estimated that banks in that country face a loss of 10 to 20 per cent of their banking business due to open banking.[538] Chinese tech giant Tencent, which owns WeChat, started a bank, WeBank, in China in May 2015. Barely more than two years later it was already loaning the same amount as an average Chinese city commercial bank.[539] New Zealand banks would struggle with approving loans in the 0.3 seconds it takes WeBank to process and approve a loan.[540]

The elephant in the room, however, is what will happen when central banks start to issue their own CBDCs.[541] For example, if people are able to have bank accounts with the central bank there would be no need to have an account with a retail bank to receive salaries and to make payments. People and organisations could just have an account with their central bank.[542] The former Australian Securities and Investments Commission (ASIC) chairman, Greg Medcraft, has predicted that traditional bank accounts may be obsolete within a decade.[543]

4.7 Central banks' loss of ability to control money supply

Attempts to control what can be used as money can backfire. Amply demonstrating that is the relatively recent debacle in India that followed the removal of the most valuable notes, 500 rupee (USD 7.50) and 1,000 rupee (USD 12.50) from circulation.[544] Overnight, after a surprise announcement by the Prime Minister on 8 November 2016,[545] the large denomination notes that accounted for 86 per cent of the Indian currency were no longer usable to purchase goods or services.[546] Non-cash payment methods were still available, such as cheques, debit or credit cards and electronic transfers. The aim was to reduce the black-market economy, loss of taxes to the

---

[536] At 16.

[537] Calls have been made for the New Zealand Government to follow Europe, the UK and now Australia and mandate open banking. See Laura Littlewood, Toby Sharpe and Kerry Beaumont "How open is New Zealand to Open Banking?" (20 February 2018) Bell Gully <https://www.bellgully.com/publications/how-open-is-new-zealand-to-open-banking>. The New Zealand Government has been briefed by Payments NZ on what it is doing in relation to facilitating open banking in New Zealand: see Jenée Tibshraeny "What the NZ Retail Payments Industry is Doing to Facilitate Open Banking and Reduce Merchant Fees to Keep the Government Happy and Avoid Regulation*" Interest.co.nz* (New Zealand, 18 April 2017) <https://www.interest.co.nz/business/93246/what-nz-retail-payments-industry-doing-facilitate-open-banking-and-reduce%C2%A0merchant>.

[538] Stanford Swinton and Eduardo Roma "Coping with the Challenge of Open Banking" (7 February 2018) Bain Brief <http://www.bain.com/publications/articles/coping-with-the-challenge-of-open-banking.aspx>.

[539] Yang, above n 79.

[540] Ibid.

[541] See Section 8 Central bank-issued cryptocurrencies (CBDCs) below.

[542] James Eyers "ASIC's Greg Medcraft says traditional bank accounts may be obsolete in a decade" *The Australian Financial Review* (online ed, 3 September 2017) <http://www.afr.com/business/banking-and-finance/financial-services/asics-greg-medcraft-says-traditional-bank-accounts-could-be-obsolete-in-a-decade-20170902-gy9k9o> and "Bitcoin is Not the Answer to Central Bank Worries" *The Economic Times* (India, online ed, 11 May 2016) <https://economictimes.indiatimes.com/news/international/business/bitcoin-is-not-the-answer-to-central-bank-worries/articleshow/52215383.cms>.

[543] Ibid.

[544] Nag and Beniwal, above n 514, albeit new 500 and 2,000 notes were to be issued replacing the old notes. The USD values were at the time the notes were removed from circulation.

[545] Press Information Bureau, Government of India "Text of Prime Minister's address to the Nation" (Press release, 8 November 2016) <http://pib.nic.in/newsite/erelease.aspx?relid=153404>.

[546] Nag and Beniwal, above n 514.

Government and endemic corruption, and to nudge the cash-dominated country towards digital money.[547] People were required to exchange their notes for smaller denominations; however, the mechanics of the note exchange process were not thought through. Only 4,000 rupees could be exchanged at banks at a time, so people could not trade all their high-denomination notes at once.[548] Moreover, the lack of small-denomination notes limited how much people could withdraw.[549] Seemingly every person in India, including those who had travelled there, was affected,[550] with people queueing each day for hours to exchange money or even to withdraw money from ATMs.[551] More than one month later the queues remained and the economy suffered.[552] After all the upheaval and cost to the economy, it has been argued that the move would not work anyway as the black money hoarders would be able to hire people to exchange the notes on their behalf.[553]

4.8 Governments become unable to collect taxes

Another argument against cryptocurrencies is that governments would be unable to tax any profits made on their use.[554] But avoidance of tax is not confined to cryptocurrencies: cash payments are particularly problematic.[555] If cryptocurrencies were banned then the IRD would receive very little tax. If cryptocurrencies continue to be tolerated, the IRD is much more likely to receive tax, especially if another of this report's recommendations is also adopted: that the IRD accept tax payments for cryptocurrency profits. Moreover, a further recommendation notes that if New Zealand cryptocurrency exchanges are encouraged even more tax would be paid as people are more likely to use those exchanges to store their cryptocurrencies – the IRD would be able to access the information from those exchanges.

4.9 Potential risks to consumers

Cryptocurrencies are often portrayed as risky for consumers. As ASIC warns, "if you decide to trade or use virtual currencies you are taking on a lot of risk with no recourse if things go wrong".[556] The

---

[547] Ibid.

[548] Pragati Kapoor "Exchange of Old Rs 500, Rs 1,000 Notes Worth Rs 4,000 Allowed Only Once Till RBI Review" *The Economic Times* (India, online ed, 11 November 2016) <http://economictimes.indiatimes.com/wealth/personal-finance-news/exchange-of-old-rs-500-rs-1000-notes-worth-rs-4000-allowed-only-once-till-rbi-review/articleshow/55369778.cms>.

[549] Weeks after the announcement people were limited to withdrawing 2,500 rupees per day. Savings account holders could withdraw up to 24,000 per week from banks, and current account holders could withdraw up to 50,000 rupees a week, provided the account had been in operation for at least three months. "Exchange of Rs 500 and Rs 1,000 notes ends; can be deposited till Dec 30" *Hindustan Times* (India, online ed, 24 November 2016) <https://www.hindustantimes.com/india-news/exchange-of-currency-stopped-use-of-old-notes-for-utility-bills-extended-till-dec-15/story-S9eIPUPtMnrsuMZ2FCXpkJ.html>.

[550] The mother of one of the authors went to India for a holiday at the time the bank notes were withdrawn from circulation. While credit card payments were not affected, many businesses did not accept credit cards which was an inconvenience.

[551] SP, above n 343.

[552] James Bennett "India's Currency Recall: Concerns Mount as Cash shortage continues" *ABC* (12 December 2016) <http://www.abc.net.au/news/2016-12-12/india's-currency-recall:-is-it-working-who-is-responsible/8111072>. Also Bennett notes that it appears that the money returned will exceed the amount that the Government was expecting to recover, meaning that either people with illicit cash have managed to launder their cash, or that the problem was not as large as the Government claimed.

[553] SP, above n 343.

[554] Jen Wieczner "Bitcoin Investors Aren't Paying Their Cryptocurrency Taxes" *Fortune* (United States, 13 February 2018) <http://fortune.com/2018/02/13/bitcoin-cryptocurrency-tax-taxes/>.

[555] Susan Edmunds "Cash Payments will Always Leave a Trail Inland Revenue Says" *Stuff* (New Zealand, online ed, 21 December 2017) <https://www.stuff.co.nz/business/100078541/cash-payments-will-always-leave-a-trail-inland-revenue-says>.

[556] MoneySmart Virtual currencies (Australian Consumer & Investment Commission) <https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies.>

FMA in New Zealand also has warned consumers.[557] To be sure, there are risks for consumers:[558] this section addresses the risks and explains how they can be mitigated. In addition, it must be borne in mind that fiat currency is not risk-free for consumers. For example, while consumers with money in bank accounts in some countries are offered some protection through government-provided deposit insurance,[559] New Zealand consumers enjoy no such protection,[560] and so no safeguard against the loss of their money if a bank were to be unable to pay its debts. In contrast, in Australia, under the Financial Claims Scheme (FCS), deposits up to $250,000 in Authorised Deposit-taking Institutions (ADIs), which include banks, building societies and credit unions,[561] are guaranteed.[562]

4.9.1 Fluctuations in price

Historic fluctuations in price, and inherent price volatility are often cited as a key reason why bitcoin and other cryptocurrencies are unsuitable for use by consumers and others.[563] Bitcoin has experienced sudden price fluctuations, not to mention an explosive rise in value of around 5,000 per cent since its launch.[564] For instance, the first few weeks of June 2011 saw bitcoin increase from around USD 0.80 to over USD 30.[565] While at the time of writing and for the preceding few years bitcoin has no longer increased or decreased by a factor of over 30 in a short space of time, it is nonetheless volatile. In the intervening years it surged to USD 979 in November 2013.[566] In December 2013 the exchange rate fell to USD 600, rebounded to USD 1,000 and then dropped to the USD 500 range. The price continued to fluctuate, going back above USD 1,000 in January 2014, then kept falling with the low point in the USD 200–300 range in March 2015. Between March 2015 and January 2017, the price rose and in early January 2017 exceeded USD 1,000. The fluctuations are arguably linked to events.[567] The doubling of bitcoin from January 2016 to January 2017 was attributed to Chinese investors wanting to move money offshore, Venezuela's economic problems and India attempting to remove black money from circulation.[568] The end of 2017 saw prices spike at USD 19,343, again swiftly followed by a plunge to USD 6,914 at the beginning of February 2018.[569] On 26 August 2018 bitcoin was trading at USD 6,671.[570]

Despite the price volatility, it is possible for merchants to accept cryptocurrencies in some parts of the world without taking the risk of price fluctuations. To do so, a merchant can use a payment processing gateway that converts the cryptocurrency into fiat currency automatically so that the merchant does not touch the cryptocurrency.[571] Indeed, it is widely accepted that stability of value is desirable and a number of cryptocurrencies had been or are being designed to have stable prices –

---

[557] Financial Markets Authority "Cryptocurrencies" <https://fma.govt.nz/investors/ways-to-invest/cryptocurrencies/>.
[558] For a useful guide on different cryptocurrencies and their features, including whether they are scams, see Nate Murray "100 Cryptocurrencies Described in Four Words or Less" *TechCrunch* (United States, 20 November 2017) <https://techcrunch.com/2017/11/19/100-cryptocurrencies-described-in-4-words-or-less/>.
[559] Ponsford, above n 67, at 33–34.
[560] Geof Mortlock "How Safe are your Deposits if a Bank Fails" *Stuff* (New Zealand, online ed, 8 April 2016) <http://www.stuff.co.nz/business/opinion-analysis/78727017/How-safe-are-your-deposits-if-a-bank-fails>.
[561] For a list of ADIs covered under the FCS see <https://www.fcs.gov.au/which-adis-are-covered>.
[562] The Financial Claims Scheme is set out in the Banking Act 1959 (Cth) Division 2AA and the limits on payment in the Banking Regulation 2016 (Cth), cl 11.
[563] Ponsford, above n 67, at 33–34.
[564] Ali, Barrdear, Clews and Southgate, above n 387, at 267.
[565] Maurer, Nelms and Swartz, above n 385 at n 31.
[566] <https://www.coindesk.com/price/>.
[567] For a graph detailing the price of bitcoin and events see <https://99bitcoins.com/price-chart-history/>.
[568] Ana Swanson "Why Bitcoin Just had an Amazing Year" *Washington Post* (United States, online ed, 3 January 2017) <https://www.washingtonpost.com/news/wonk/wp/2017/01/03/why-bitcoin-just-had-an-amazing-year/?utm_term=.6ba4a8feecce>.
[569] See <https://www.coindesk.com/price/>
[570] <coinmarketcap.com>.
[571] See, for example, <https://coingate.com/accept-bitcoin>.

namely "stable coins".[572] The most successful stable coin so far is the aptly named Tether, which is meant to be backed one-to-one with US dollars;[573] however, there is growing doubt about whether this is actually the case and the US Commodity Futures Trading Commission is investigating whether Tether has its reported 2.3 billion US dollars in reserve.[574] One of benefits of CBDCs is that most will be stable coins because many will be pegged to, and some backed by, fiat currency.[575]

4.9.2 Loss of private keys and passwords

One of the most significant current problems with cryptocurrencies is the management of private keys. Cryptocurrencies are normally stored in a virtual "wallet", namely a computer program that contains the owner's private key, or a paper wallet where both the public and private key are printed on paper. So-called cold storage,[576] such as a wallet containing cryptocurrencies on a computer that is not connected to the internet, is reasonably safe, but for the risk of the hard drive failing, or being stolen or thrown away accidentally.[577] There are also hardware wallets such as Trezor, which stores the private key and keeps it protected by a PIN.

In a paper wallet, the public address and private key are written down on paper.[578] Yet, while this is arguably safer than storage on a computer, there is still the risk of loss, whether through losing the piece of paper, another person finding the piece of paper or destruction of the paper. Mobile wallets are accessible via an app on a smart phone,[579] so if someone hacks into a computer (including a smart phone) it is sometimes possible for them to gain access to the cryptocurrencies. Another way is to memorise the private key (called brain wallet), but that runs the real risk of forgetting it, not to mention preventing the person's heirs from inheriting the assets.

A person can lose private keys in a range of ways. For example, they may set up a mobile wallet on their smart phone. If they do not keep a record of their private key (or their 12 or 24-word mnemonic phrase) and later lose their phone, delete the app, or swap to a new phone, they will lose the cryptocurrency. Even if they do keep a record, that record may be lost or someone may find the record and use that to download a copy of the app and transfer the cryptocurrency out of the mobile wallet. Thus, if the computer is compromised or fails, the cryptocurrency can be stolen, and unless the private key is recorded elsewhere, the owner effectively loses the cryptocurrency.

Contrast the case where someone forgets their internet banking password, or the PIN to their debit card: they can contact their bank, and upon providing proof of identity they will be granted access to their funds. Because of the problem of private key management, some people get third parties such

---

[572] Sherman Lee "Explaining Stable Coins, The Holy Grail of Cryptocurrency" *Forbes* (United States, 12 March 2018) <https://www.forbes.com/sites/shermanlee/2018/03/12/explaining-stable-coins-the-holy-grail-of-crytpocurrency/#202584374fc6>.

[573] <https://tether.to/>.

[574] Matthew Leising "U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether" *Bloomberg* (United States, 31 January 2018) <https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc>.

[575] Ben SC Fung and Hanna Halaburda "Central Bank Digital Currencies: A Framework for Assessing Why and How" (Staff Discussion Paper 2016-22, Bank of Canada, November 2016) at 12. <http://www.bankofcanada.ca/wp-content/uploads/2016/11/sdp2016-22.pdf "Central Bank Digital Currencies: A Framework for Assessing Why and How">.

[576] Cold storage refers to keeping a reserve of cryptocurrency including all the private-key data offline. As the cryptocurrency is stored off-line it is not susceptible to attack via a hacker getting into the network.

[577] Andreas M Antonopoulos *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media, Sebastopol, California 2014) at 106 and see Aatif Sullyman "Man Who 'Threw Away' Bitcoin Haul Now Worth over $80 million Wants to Dig Up Landfill Site" *Independent* (UK, online ed, 4 December 2017) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html>.

[578] See Antonopoulos, above n 577, at 106.

[579] Mobile wallets include Bread and Jaxx.

as exchanges to in effect hold their keys. Third parties, however, are more liable to be attacked by hackers, and such hacks have occurred.[580]

As with the scaling issue,[581] key management is accepted as being a significant issue[582] and is being worked upon.[583] In the meantime people are using a variety of means to secure their private keys. In the US, technological entrepreneurs the Winklevoss twins have cut their private keys into parts and put those parts in bank accounts through safe deposit boxes.[584]

4.9.3 Security

Concerns have been expressed over the security of cryptocurrencies.[585] However, it must be noted that the distributed nature of decentralised systems should also mean that they are more resilient to systemic operational risk.[586] A further risk common to both centralised and decentralised payment systems is the risk of fraud, which manifests itself in different ways for each system.[587] The current banking system is vulnerable, and numerous banks have been compromised from time to time with large amounts of money stolen,[588] albeit the banks have compensated their clients, as has one exchange.[589] This is because if a bank's computer system is compromised because of a security breach,[590] provided not all the money in the bank is stolen, they will get the money back.[591] The loss of cryptocurrencies through hacking exchanges is due to practices of the exchange, not necessarily to do with cryptocurrencies per se. For example, if cryptocurrencies are held in cold storage, which many exchanges do, it would be extremely difficult for those cryptocurrencies to be stolen. Moreover, newer cryptocurrencies such as XEM have the ability to set up a "multi-sig" wallet so that a number of users have to approve a transaction, which would again thwart a hacker from making off with any of the cryptocurrency.[592]

Because Bitcoin is decentralised, there is no entity to compensate bitcoin holders if their bitcoin is stolen through a hack of the blockchain. The question then becomes, can the bitcoin blockchain be hacked and bitcoins "stolen". At the time of writing the Bitcoin protocol has not been hacked. The

---

[580] Daniel Shane "$530 Million Cryptocurrency Heist may be Biggest Ever" *CNNTech* (29 January 2018) <http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html>.
[581] See Section 4.3 Cryptocurrencies cannot scale above.
[582] Shayan Eskandari, David Barrera, Elizabeth Stobert and Jeremy Clark "A First Look at the Usability of Bitcoin Key Management" (paper presented to NDSS Workshop on Usable Security (USEC) 2015, San Diego, United States, February 2015) <https://arxiv.org/abs/1802.04351> and Ouriel Ohayon "The Sad State of Cryptocurrency Custody" *Techcrunch* (2 February 2018) <https://techcrunch.com/2018/02/01/the-sad-state-of-crypto-custody/>.
[583] See, for example, "Shamrock: Self-contained High Assurance Micro Crypto and Key-management Processor" MIT Technology Licensing Office <https://tlo.mit.edu/technologies/shamrock-self-contained-high-assurance-micro-crypto-and-key-management-processor>.
[584] Kif Leswing "The Winklevoss Twins cut up the Key to their $1.3 Billion Bitcoin Fortune and Keep Each Piece in Different Bank Vaults" *Business Insider Australia* (20 December 2017) <https://www.businessinsider.com.au/winklevoss-twins-cut-up-key-to-protect-their-bitcoin-fortune-2017-12?r=US&IR=T>.
[585] Financial Markets Authority "Cryptocurrencies", above n 557.
[586] See further Ali, Barrdear, Clews and Southgate, above n 387, at 270–271.
[587] Ibid.
[588] "Spanish police arrest suspected mastermind of $1 billion bank hacks" *Reuters* (27 March 2018) <https://in.reuters.com/article/cyber-banks-spain/spanish-police-arrest-suspected-mastermind-of-1-billion-bank-hacks-idINKBN1H21GX>.
[589] Rachel Koning Beals "Hacked Japanese Cryptocurrency Exchange Coincheck Refunds Customers" *Marketwatch* (13 March 2018) <https://www.marketwatch.com/story/hacked-japanese-cryptocurrency-exchange-coincheck-refunds-customers-2018-03-13>.
[590] "Spanish police arrest suspected mastermind of $1 billion bank hacks", above n 588.
[591] New Zealand Bankers' Association "The Code of Banking Practice" at 8.1.3 <http://www.nzba.org.nz/consumer-information/code-banking-practice/code-of-banking-practice/>.
[592] "Coincheck Hacking and What it says About NEM" (4 February 2018) Medium <https://medium.com/nemofficial/coincheck-hacking-and-what-it-says-about-nem-b4f3a7b00534>.

hacks that have occurred have been at exchanges that controlled the private keys of the cryptocurrencies' owners. Theft has occurred when people have placed their bitcoins in exchanges and other organisations that deal in cryptocurrencies and those entities have been hacked. The best-known example is the Japan-based Mt Gox, where hackers allegedly made off with more than USD 500,000 worth of bitcoin,[593] although subsequently is transpired that the loss may have been a case of embezzlement.[594] An analogy can be made with credit cards. If a person's Visa credit card details are stolen and misused we do not say that Visa's system has been hacked, but rather that the card has been misused. The difference is that normally the credit card company will reimburse the credit card holder for fraudulent use of the card.

The fact that Bitcoin's blockchain has not been hacked, however, does not render cryptocurrencies risk-free for consumers and others who own them, as the loss of private keys and hacking of exchanges demonstrates. Another weakness in the Bitcoin protocol arises where a mining pool (group of bitcoin miners) could control more than 50 per cent of the network's computing power – the 51 per cent attack. A pool or an entity could abuse its power to reverse transactions, double spend bitcoin and prevent other miners from mining otherwise valid blocks.

Should quantum computing eventuate, cryptography will no longer work and the Bitcoin protocol will fail. However, if quantum computing does occur it will not merely threaten cryptocurrencies. Quantum computing would mean that credit cards could no longer be used securely online since that involves public key cryptography. The Bitcoin protocol, as with all other technology that operates public key cryptography, will have to adapt to meet the demands of quantum computing.[595]

Banks are under threat from tech firms and open banking,[596] and indeed will be under even further threat when central banks begin to issue their own cryptocurrencies.[597] To protect profits it makes sense for banks to offer services to their customers in the form of holding their customers' private keys and thus their cryptocurrency. Work has been done already on the benefits and risk of banks allowing their customers to use cryptocurrencies.[598]

4.9.4 Non-reversibility of transactions

One reason why some merchants prefer payment in cryptocurrency is that not only are its processing fees often lower than the current payment systems, but there will be no charge-backs. On the other hand, if you transfer cryptocurrency to the wrong address, unless the person receiving it returns it to you, there is nothing that you can do; you will have lost that cryptocurrency. However, in New Zealand[599] and in Australia mistaken payments are not reversible.[600]

---

[593] Nikolei Kaplanov "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation" (2012) 25 Loyola Consumer Law Review 111, at 124. The value of the stolen bitcoin has increased dramatically since that time.
[594] Samuel Gibbs "Head of Mt Gox Bitcoin Exchange on Trial for Embezzlement and Loss of Millions" *The Guardian* (UK, online ed, 11 July 2017) <https://www.theguardian.com/technology/2017/jul/11/gox-bitcoin-exchange-mark-karpeles-on-trial-japan-embezzlement-loss-of-millions>.
[595] Work is already underway on post-quantum cryptography: see Bernstein and Lange, above n 64.
[596] See generally nn 533–535 and accompanying text.
[597] Charles Brett "Central Bank Cryptocurrency to Upset the Bank Applecart?" *Enterprise Times* (UK, 8 January 2018) <https://www.enterprisetimes.co.uk/2018/01/08/central-bank-cryptocurrency-to-upset-the-bank-applecart/>.
[598] See Peters, Chapelle and Panayi, above n 70.
[599] New Zealand Banking Ombudsman Scheme "Mistaken Payments", above n 255.
[600] Clancy Yeates "Real Time Payments Overhaul Coming in 2017" *The Sydney Morning Herald* (Australia, online ed, 27 December 2017) <http://www.smh.com.au/business/banking-and-finance/real-time-payments-overhaul-coming-in-2017-20161206-gt50sv.html>.

4.9.5 Cryptocurrencies are unregulated

The RBNZ observes that:[601]

> … disruptors that participate in a payment system in New Zealand are subject to the Reserve Bank's information gathering powers under Part 5B of the Reserve Bank of New Zealand Act (1989). However, there are currently no coordinated prudential regulations of "disruptor" entrants to the banking system that address the risk that a systemic failure of these entities could pose for the financial system.

Banks and other financial institutions pride themselves on the legal protections afforded to consumers. Laws, however, are effective only to the extent that they are followed and enforced. The presence of strong laws on paper does not mean much to consumers if those laws are flouted, or worse, not enforced when breaches occur.[602] Financial advisers in New Zealand are regulated heavily,[603] yet that does not stop financial advisers stealing investors' money.[604] Moreover, it is possible to set some cryptocurrencies up in such a way that those who are holding the cryptocurrencies on behalf of others cannot spend those cryptocurrencies; in other words, the financial institution and the customer would both have to sign the transaction to transfer the cryptocurrency to a third party.[605] Be that as it may, cryptocurrency exchanges that hold people's cryptocurrency could be regulated, and we argue should be. The question then becomes, how should they be regulated? This is explored in Section 9.

5. Limitations of the current payment systems and how cryptocurrencies could solve them

This section looks generally at the weaknesses of payment systems for consumers, noting that the extent of the weaknesses varies between different markets.[606] Many of the limitations can be ascribed to a lack of competition in the payment sector. An analogy to telecommunications can be made. In New Zealand, as in Australia, there was one telecommunication company.[607] Installing

---

[601] Amber Wadsworth "Disruption or distraction?", above n 69, at 16.

[602] See, for example, Alexandra Sims and Louise Mara "Unfair Online Contract Terms in New Zealand: Evaluating the Effect of Regulatory Change (2014) 24 Competition & Consumer Law Journal 128. There the introduction of an unfair contract terms law made little difference to the contracts of businesses as all continued to use unfair contract terms, albeit there was a 10 per cent reduction in the number of unfair contract terms used in the contracts studied.

[603] See, for example, Financial Service Providers (Registration and Dispute Resolution) Act 2008.

[604] See, for example, "Financial Adviser Accused of Stealing $3m" *The New Zealand Herald* (online ed, 5 September 2013) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11120011>; Financial Markets Authority "David Ross Sentenced for New Zealand's Largest Ever Ponzi" (15 November 2013) <https://fma.govt.nz/news-and-resources/media-releases/david-ross-sentenced-for-new-zealands-largest-ever-ponzi/>; and Ben Bathgate "Jailed Financial Adviser Stole $1m From Elderly Clients" *Stuff* (New Zealand, online ed, 19 June 2015) <https://www.stuff.co.nz/business/money/69536687/jailed-financial-adviser-stole-1m-from-elderly-clients>. In addition, one of the requirements of becoming an Authorised Financial Adviser (AFA) is to pass a closed book multi-choice exam that demonstrates understanding of the legislative framework (see Code Committee "Code of Professional Conduct for Authorised Financial Advisers" (December 2016) <https://fma.govt.nz/assets/Code-of-Professional-Conduct-for-AFAs/Code-of-Professional-Conduct-for-AFAs.pdf>, Code Standard 15 and <https://skills.org.nz/careers-and-courses/business/financial-services/authorised-financial-advisers/>.) The exam is more difficult than standard multi-choice tests as part of it uses multi-select questions and more than 70 per cent has to be achieved in each of the sections. Despite this, one of the authors of this report a number of years ago was able to pass the exam easily despite not having experience as a financial adviser and minimal preparation.

[605] Thomas Kerin "The Year of Multisig: How is it Doing So Far?" *Coindesk* (17 May 2014) <https://www.coindesk.com/year-multisig-so-far/>.

[606] Keith Horowitz, Ashwin Shirvaikar and Donald Fandetti *US Digital Banking: Could The Bitcoin Blockchain Disrupt Payments?* (Citi Research, 30 June 2016) <https://ir.citi.com/onWP8PeDTFCEOpVtHBNtpVSgNCDKcVVUBdHotDbLJ%2BjXmVXuVE8aY3W2hNxoAfPWNcuytXi1ocM%3D> at 18.

[607] In New Zealand, Telecom. In Australia, Telstra.

telephone lines could take many weeks if not months, and toll calls were prohibitively expensive. Now phone (and more importantly internet) connections are considerably faster and cheaper. Competition is good for consumers.

5.1 High transaction costs

A common complaint from merchants is the fees they must pay when accepting credit cards.[608] The costs for international bank transfers are high.[609] International transfers of money generally involve fees to payment service providers, which act as intermediaries. In the first quarter of 2016, Citi Research found that the average fee to send USD 200 internationally through a bank was approximately 11 per cent (USD 22) and that banks routinely charge USD 35–40 for wire transfers. The fee is usually fixed: sending larger amounts is in effect cheaper than small amounts. Furthermore, international transfers may also be subject to additional fees from other banks as the money makes its way to its destination, including additional lifting fees, foreign exchange fees and taxes.[610] For large amounts, the foreign exchange fees become significant. Account-to-account transfers within the same bank are subject to fewer and lower fees, but Citi Research found that even the same-bank account-to-account international transfers were subject to an average of six per cent in fees.[611] Thus the use of fiat currency can be more expensive than is commonly thought, entailing significant indirect costs that are not always visible to consumers.[612]

Citi Research in 2016 also identified licensing, consumer protection requirements, customer on-boarding know your customer (KYC) requirements, and anti-money laundering (AML) monitoring requirements as additional sources of friction that increase the costs of bank transfers.[613] However, we are not advocating that all transfers of cryptocurrencies be free from KYC and AML requirements in New Zealand. Indeed, cryptocurrency exchanges need to comply with KYC and AML requirements, and this report also recommends that merchants that accept more than NZD 100 in a cryptocurrency transaction only be allowed to do so if the transaction is made through a New Zealand-based cryptocurrency exchange or an exchange based overseas (including a wallet provided by that exchange) that is subject to similar AML/KYC requirements, such as Coinbase in the US and Australian and Japanese exchanges. The reason for this recommendation is that companies wishing to accept payments in cryptocurrency run the real risk of losing their bank account if they accept cryptocurrency payments. Requiring payments over $100 in value to go through accredited exchanges would enable New Zealand businesses to accept payments without the risk of having their bank account closed (being “debanked”). Albeit it could still be seen as unfair to merchants since businesses can accept considerably higher sums from their customers if those payments are made in cash.

Centralised/intermediated services are expensive because credit risk, liquidity risk and operational risk must be priced into the system.[614] Credit and liquidity risks are addressed through prudential regulation requirements for banks, such as capital adequacy ratios. While these regulatory requirements serve important policy goals, such as ensuring the stability of the banking system and the economy as a whole, they are also a cost, which reduces the efficiency of the system. Ensuring initial compliance with these requirements presents a significant barrier to entry, which dissuades

---

608 Rob Stock “Merchant Anger Rising at Growing Cost of ‘Interchange' on Credit and Debit Cards” *Stuff* (New Zealand, online ed, 2 November 2015) <http://www.stuff.co.nz/business/73515906/Merchant-anger-rising-at-growing-cost-of-interchange-on-credit-and-debit-cards>.

609 Bank for International Settlements *Digital Currencies*, above n 342, at 9; Zoe Thomas “Why Bitcoin could be the Key to Banking’s Future” (2014) International Financial Law Review.

610 Horowitz, Shirvaikar and Fandetti, above n 606, at 19.

611 Ibid.

612 Brett King, *Breaking Banks: The Innovators, Rogues and Strategists Rebooting Banking* (Wiley, 2014) 122.

613 Horowitz, Shirvaikar and Fandetti, above n 606, at 28–29.

614 Ali, Barrdear, Clews and Southgate, above n 387, at 270.

new firms from entering the market to provide banking services. The reduced competition is another inefficiency of the banking system. Decentralised systems, such as cryptocurrencies, remove credit risks relating to intermediaries as the use of intermediaries is eliminated,[615] and they therefore do not entail the associated costs of protecting against such risks. On the other hand, intermediaries can offset so that the absolute amounts that have to be exchanged fall. Decentralised operations may have to operate using gross amounts, which may be more expensive. In addition, with cryptocurrencies the credit risk of the counterparty remains.

Cost has been identified as an area in which cryptocurrencies might have a competitive advantage, providing the ability to transfer money internationally more cheaply than through traditional banking methods.[616] The Bank for International Settlements (BIS) argues, however, that cryptocurrencies do not necessarily involve lesser fees, and that the transaction costs for international transactions of cryptocurrencies are not always transparent.[617] Cross-border transactions of digital currencies may involve conversion fees from fiat currencies to cryptocurrencies and back again but their major advantage will be for people who do not want to convert because they can use the same currency in both the origin and destination countries.

Citi Research found that Bitcoin-based systems are unlikely to compete with traditional banking and MTOs in providing remittance services "within a reasonable time-frame".[618] One of the reasons for Citi Research's conclusion is that at the time of its research bitcoin did not provide cheaper costs for remitting funds than other options available in most remittance corridors.[619] While bitcoin did have a low base cost for a transfer, at the time only USD 0.06 for the median transaction size, there are a number of other costs for consumers seeking to use the technology for remitting funds across borders.

First, to use bitcoin, fiat currency must first be exchanged at a bitcoin exchange. It is also likely that the recipient of the remittance will want to exchange the remitted bitcoins to the fiat currency of their country. This is called the "on-ramp" and "off-ramp" of bitcoin transactions.[620] Both of these exchange transactions will involve fees from the exchanges used. Fees may also arise that relate to bank transfers, card network charges and occasionally taxes.[621] Second, the costs of exchanging fiat currency for bitcoin and vice versa may be significant in countries where the exchange markets lack liquidity. Third, there will still be a need for some physical infrastructure, which will entail distribution costs. Citi Research conclude that TransferWise, an MTO operating in competition with Western Union and MoneyGram, is simply cheaper than bitcoin, for the most part,[622] although Citi Research question whether TransferWise's business model is sustainable in the long run.[623] Notwithstanding Citi Research's arguments, there are a number of remittance businesses competing with the traditional banks and MTOs.[624]

---

[615] At 271.
[616] Mustafa Ally, Michael Gardiner and Michael Lane "The Potential Impact of Digital Currencies on the Australian Economy" (paper presented to Australasian Conference on Information Systems, Adelaide, 2015) at [5.1].
[617] Bank for International Settlements *Digital Currencies*, above n 342, at 9.
[618] Horowitz, Shirvaikar and Fandetti, above n 606, at 32.
[619] At 39–41.
[620] At 33.
[621] At 40.
[622] At 41.
[623] At 23.
[624] Casey Hynes "Meet The Cryptocurrency Startups Targeting The $26 Billion Remittance Industry In The Philippines" *Forbes* (United States, 15 September 2017) <https://www.forbes.com/sites/chynes/2017/09/15/meet-the-cryptocurrency-startups-targeting-the-26-billion-remittance-industry-in-the-philippines/#3df86f505510>.

5.2 Slow transaction times

A second weakness of the banking system is its processing speed for transactions.[625] This can be between one and five days for international transfers. Faster international transfers are provided by MTOs, which offer options for transfers that are effective within minutes or within one day. BIS argues that a number of innovations have been developed for traditional banking systems to improve payment speeds, such as real-time gross settlement systems and faster retail payment systems.[626]

For cryptocurrencies, the speed of the transaction itself is no longer if the two parties are based in different countries than if they are based in the same country.[627] However, Citi Research note that while bitcoin transactions themselves can be settled in less than an hour, the whole remittance process can be substantially longer if, as is sometimes the case, the remitted funds need to be converted to the recipient's local currency, particularly in low-liquidity exchange markets.[628] There is an additional layer of complexity where the recipient of the remittance not only requires the money to be converted to fiat currency, but also requires the money in physical cash. In developing countries, where many people do not have access to banking, this may be difficult.

The Australian Senate observes that "Australians already have many different payment systems including EFTPOS, interbank transfers, PayPal and international transfer via SWIFT. In this context, digital currencies, such as Bitcoin, do not offer much more additional capability".[629] However, as we shall see, just in transaction times alone there are significant advantages with cryptocurrencies. Merchants who accept EFTPOS do not receive the money instantly.[630] Indeed, EFTPOS payments are limited for a number of reasons. First, the parties need to be physically proximate to allow the card owner to run the EFTPOS card through the merchant's machine. Second, EFTPOS payments are dependent on the receiver having a machine; they cannot be made by consumers to consumers. Third, the amount that can be spent in any one transaction is limited.[631] But they are attractive to merchants because the merchants do not pay additional fees for accepting EFTPOS, unlike when accepting debit cards and credit cards.[632] Debit cards remove the first limitation as they can be used over the internet, and if paid through PayPal can be used to pay another consumer as long as both consumers have a PayPal account, albeit payments through PayPal can take days, depending on the type of transaction.[633]

In the past if a person in New Zealand wanted to pay someone whose account was with a different bank by internet banking, the recipient would not receive the money until the next day at the earliest.[634] This has now changed[635] and interbank payments can take as little as an hour, provided

---

[625] Horowitz, Shirvaikar and Fandetti, above n 606, at 20.
[626] Bank for International Settlements *Digital Currencies*, above n 342, at 10.
[627] Ibid.
[628] Horowitz, Shirvaikar and Fandetti, above n 606, at 41.
[629] Economics References Committee, above n 66, at [3.8].
[630] <https://eftpos.co.nz/mobile-faqs>.
[631] Each bank has slightly differently limits. For example, Kiwibank's limit is $2,500 per day for ATM withdrawals and $5,000 for purchases, whereas ASB's ATM withdrawal limit is $2,000 per day and its purchase limit is the same as Kiwibank's.
[632] Rob Stock "Merchant Anger Rising at Growing Cost of 'Interchange' on Credit and Debit Cards" *Stuff* (New Zealand, online ed, 2 November 2015) <https://www.stuff.co.nz/business/73515906/Merchant-anger-rising-at-growing-cost-of-interchange-on-credit-and-debit-cards>.
[633] "How Long Does it Take to Get my Money Using PayPal Invoicing" <https://www.paypal.com/us/selfhelp/article/How-long-does-it-take-to-get-my-money-using-PayPal-Invoicing-FAQ3140>.
[634] Susan Edmunds "Banks Implement New, Faster Payment Processing Systems" *Stuff* (New Zealand, online ed, 11 November 2016) <http://www.stuff.co.nz/business/86300659/Banks-implement-new-faster-payment-processing-systems>.
[635] Ibid.

the transaction occurs during a business day.[636] Internet banking, therefore, is slow compared with the cryptocurrency payments. Indeed, one of the most common complaints made to New Zealand's Banking Ombudsman is over recipients not receiving money until the next business day.[637]

SWIFT is commonly used to send money from a bank account in one country to a bank account in another. The transaction times vary, with banks estimating that it normally takes between one and four working days;[638] however, for some countries, such as India and Pakistan, it could be as long as three weeks.[639] The extreme delay is because bank drafts are sent by post between the countries.[640] In fact, in May 2018 Kiwibank was advising its customers that if they wanted to cash a foreign cheque or a bank draft they would first have to go to a Kiwibank and deposit it in their bank account. If the cheque or bank draft was from Australia and worth NZD 15,000 or less the funds would normally be available after 20 business days. If it was from anywhere else it would take 30 business days.[641] In contrast, if a person in the UK wants to send bitcoin to a person in New Zealand the bitcoin will be available for use within an hour or so, and the lag is only minutes for some other cryptocurrencies.

5.3 Significant cost of credit card fraud

In 2016 global credit card fraud was estimated at USD 21.84 billion, with the figure projected to rise substantially in successive years.[642] While individuals do not pay for the cost of credit card fraud directly,[643] the losses incurred by card issuers and merchants result in customers paying higher credit card fees and interest, and increased prices for goods and services.

Most New Zealand consumers purchasing goods online from traders based overseas use credit cards or debit cards, as there is no direct simple way of paying.

5.4 The unbanked and under-banked

A large proportion of people in the world are unable to access the banking system. Approximately 2.5 billion people are "unbanked" because they cannot afford the costs banks charge, do not meet the requirements for opening an account, or because banks are simply not available in the area in which they live.[644] Many more people are described as "under-banked". Bitcoin is said to present an opportunity to provide access to payment services for many of these people. While the number of

---

[636] Westpac states: "If you are expecting funds from another bank, these will appear shortly after the bank sends the payment to Westpac between 9:15am and 11:30pm on business days. (Some banks do not yet send payments to Westpac during the day and these payments will be visible in your account approximately 2am the following morning on business days)." "How long does it take you to process payments?" <http://westpac.custhelp.com/app/answers/detail/a_id/871/~/how-long-does-it-take-you-to-process-payments%3F>.

[637] Edmunds "Banks Implement New, Faster Payment Processing Systems", above n 634.

[638] Westpac says 1–3 days: <https://www.westpac.co.nz/business/international-business/international-payments/>.

[639] Kiwibank "International Payments" <https://www.westpac.co.nz/business/international-business/international-payments/>.

[640] Ibid.

[641] Kiwibank "Depositing foreign cheques or bank drafts" <https://www.kiwibank.co.nz/business-banking/international/receiving-money-from-overseas/depositing-foreign-cheque-or-bank-drafts/>.

[642] "The Nilson Report" (October 2016) <https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf> at 6.

[643] Card issuers absorbed 62% of the losses and merchants the remaining 38%: see "Global Card Fraud Losses Reach $16.31 Billion — Will Exceed $35 Billion in 2020 According to The Nilson Report" *Business Wire* (4 August 2015) <http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VcJZlvlVhBc>.

[644] Ally, Gardiner and Lane, above n 616, at [5.1].

people unable to obtain banking services is not large in New Zealand,[645] it is a significant problem internationally. It has been estimated that only 69 per cent of adults globally have a bank account.[646]

5.5 Identity theft

The Department of Internal Affairs (DIA) estimates that in New Zealand alone identity crimes, which include creating false identities, can cost the economy over $200 million.[647] Identity is one of the many areas which in which blockchain technology is being used.[648] Indeed it has been argued that:[649]

> Blockchains, possibly even Bitcoin, might be the first successful implementations of identities made for an online world. They will make it possible for us to build an online reputation and maintain all the perks that come with it, such as trust and credit, while making it difficult to have these identities stolen due to the advantages of asymmetric encryption and transparent ledgers.
>
> It will be a great advantage, and possibly even a deciding factor, if these identities are not maintained by a single entity, but rather kept by a decentralized system such as Bitcoin.
>
> It remains unanswered how such an online identity system will integrate with our legal systems, but it can help to make many things possible that Bitcoin cannot, such as credit, which in return allows for recurring payments and a shift of risk away from the consumer.

Not surprisingly, work is underway in New Zealand with a mix of companies and the New Zealand Government on using blockchain to provide New Zealanders with a digital identity.[650]

5.6 Slow rate of innovation

The British Bankers' Association (BBA) identifies the general complexity of the banking system as a challenge for banks in responding to digital disruption:[651]

> Lots of functions that currently reside in the core platform [of British banks] do not really need to be there. … Such complexity is the result of an accumulation within banks of thousands of minor software patches and variations, sometimes over decades. Systems have evolved, but not by design, and the outcome for banks has been the creation of enormous and intractable complexity.

"Core complexity" slows innovation, reduces agility and security, increases risk and costs, and damages trust. The BBA also identified friction in banks' digital services (that is, sub-optimal usability of these services) as a challenge for banks responding to digital changes:[652]

> The propensity of UK consumers to buy products and services online is increasing, and banks' digital services must be as seamless and frictionless as possible. However, research

---

[645] Andrew Van der Werff, Jeanne M Hogarth and Nathanael D Peach "A Cross-Country Analysis of Unbanked Within the OECD" (2013) 59 Consumer Interests Annual 1, at 6. The authors note that New Zealand, lying in the high 90 per cent range, had the third-highest percentage of people with accounts at formal financial institutions in the OECD.
[646] Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar and Jake Hess *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution* (World Bank, 2018) at 17 <http://globalfindex.worldbank.org/>.
[647] The Department of Internal Affairs "Identity Theft – What Is Identity Theft? <https://www.dia.govt.nz/Identity---What-is-identity-theft>.
[648] Amit Goel "12 Companies Leveraging Blockchain for Identification and Authentication" *Medici* (28 March 2016) <https://gomedici.com/12-companies-leveraging-blockchain-for-identification-and-authentication/> and see Sarah Perez "Civic Launches a Free Service that Aims to Stop Identity Theft Before it Happens" *Techcrunch* (20 July 2016) <https://techcrunch.com/2016/07/19/civic-launches-a-free-service-that-aims-to-stop-identity-theft-before-it-happens/>.
[649] Arthur Baxter "Blockchain – unchaining the world from fraud?" (14 April 2016) The Paypers <http://www.thepaypers.com/expert-opinion/blockchain-unchaining-the-world-from-fraud-/763845>.
[650] Gower, above n 28.
[651] British Bankers' Association, above n 81.
[652] At 21–22.

> shows that banks still have some way to go to deliver the experiences that customers are looking for.
>
> Consumers have a growing appetite for simple, easy-to-use, friction free payments that are consistently supported across channels. They have already embraced the newly reinvented, streamlined and seamless digital experiences provided by technology players like Apple, Amazon, Facebook, Google and PayPal, and they expect similar experiences from the payment services offered by their banks.

For a discussion of further issues with the customer experience provided by banks, see *Breaking Banks* by Brett King.[653]

5.7 Fragile banking system

While securities are not strictly part of payment systems, the global financial crisis is said to have been caused by the sub-prime mortgage crisis in the US.[654] Institutions were unable to see what the underlying securities were. If that information had been on a blockchain it would have been easier to assess the risk as regulators could be given a "regulator node" so they can see into the blockchain in real time[655] or, if an institution did fall over because regulators and auditors were not doing their jobs, the damage could be mitigated quickly, as J Christopher Giancarlo, a Commissioner at the US Commodity Futures Trading Commission, notes:[656]

> Had Lehman still failed, records powered by DLT and held by trading counterparties (and available to regulators) would have accurately shown Lehman's open positions across asset classes.
>
> Imagine if, instead of requiring countless legal actions spanning eight years, we could have known all of Lehman's exposures within minutes of its bankruptcy filing. Accelerated settlement of open positions and accounts could have taken weeks, not years.

5.8 Money laundering

Money laundering is a large issue for banks and other financial institutions. The Financial Action Task Force has set up the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation[657] that countries, including New Zealand, must comply with. New Zealand's relevant legislation is the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

Despite strong laws in New Zealand and around the world, banks are seemingly the vehicle of choice for money-laundering. For example, in 2017 it was reported that "[g]aping holes in the anti-money laundering systems of Australia's big banks are being exploited by crime groups to wash up to $5 million in drug cash a day, according to confidential briefings by federal and state policing agencies."[658] Australian banks are not alone. The RBNZ in 2017 assessed retail banks as being at a high inherent risk of money laundering.[659]

---

653 Brett King *Breaking Banks: The Innovators, Rogues and Strategists Rebooting Banking* (Wiley, 2014) in particular 239–250.

654 Mainelli and Milne, above n 42, at 9.

655 J Christopher Giancarlo "LabCFTC: Engaging Innovators in Digital Financial Markets" (address to the New York FinTech Innovation Lab, New York, United States, May 2017) <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-23>.

656 Ibid.

657 Financial Action Task Force "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (February 2012) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>.

658 McKenzie, Baker and Mitchell, above n 13.

659 Reserve Bank of New Zealand "Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)" <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/SRA-

The UK Treasury in its 2017 "National Risk Assessment of Money Laundering and Terrorist Financing"[660] noted that the UK's Financial Conduct Authority (FCA) had said that "most" UK banks recognise the importance of strong money laundering law and that the UK Treasury's first report[661] on the subject:[662]

> … highlighted the most common issues in terms of banks' compliance as inadequate governance structures, inadequate risk assessment process, poor IT systems, poor management of transaction alerts, poor identification of source of funds, and poor management of foreign PEPs [politically exposed persons] and correspondent banks.

Despite the historical deficiencies in the UK banking system, the UK Treasury found that the vulnerabilities persisted.[663] The common issues that remained were:[664]

> … weaknesses in governance, and longstanding and significant underinvestment in resourcing. This underinvestment may affect the infrastructure underpinning firms' controls, such as transaction monitoring IT systems that are not kept up to date. Managing complex legacy systems remains a challenge for a number of firms, but the FCA is seeing continuing improvements.

Not surprisingly given its comments, the UK Treasury found that retail banks remained at high risk of money laundering.[665] In contrast, the same report assessed the money-laundering risk for cryptocurrencies as low.[666] Thus assertions from regulators such as "[m]oney laundering is a common financial crime in the crypto-currency domain due to pseudonymity and a lack of regulation" are difficult to justify.[667] In a similar vein the Financial Intelligence Unit (FIU) of the New Zealand Police in a report was concerned that cryptocurrencies were being used for money laundering and the financing of terror.[668] The FIU were unable to supply any concrete evidence for the financing of terror.[669] In regards to potential money laundering and the purchase of illicit goods the FIU provided three case studies.[670] If the abuse of a technology by criminals was a reason to prevent its use in New Zealand, the banking system would be closed and cash abolished. Indeed, in Annex 1 of the FIU's report, the examples of "The three internationally accepted phases for the money laundering process" do not involve cryptocurrencies, but rather work through cash being placed into a bank account, from where that money is transferred to other bank accounts, and international travel tickets are purchased and cancelled so that a reimbursement cheque of now clean money (minus the cancellation fees) is issued.[671]

In a more recent report by the FIU many vulnerabilities were found in international wire transfers, alternative payment methods, new technology, gatekeeper professional services including formation

---

2017.pdf?la=en> 4. See also Financial Intelligence Unit "National Money Laundering and Terrorism Financing Risk Assessment", above n 87, at 24.

[660] United Kingdom HM Treasury "National Risk Assessment of Money Laundering and Terrorist Financing", above n 89.

[661] United Kingdom HM Treasury "UK National Risk Assessment of Money Laundering and Terrorist Financing" (October 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf>.

[662] United Kingdom HM Treasury "National Risk Assessment of Money Laundering and Terrorist Financing", above n 89, at [4.27–4.28].

[663] At [4.28].

[664] At [4.27–4.29].

[665] At [4.4].

[666] At [5.3].

[667] Kumar and Smith, above n 310, at 28.

[668] Financial Intelligence Unit "Quarterly Typology Report: First Quarter (Q1) FY 2016-2017 – Cryptocurrency" (December 2016) <http://www.police.govt.nz/sites/default/files/publications/fiu-qtr-q1-2016-17-cryptocurrency.pdf>.

[669] At 12. Only the following article was referred to: Irwin and Milad, above n 261.

[670] At 16–18.

[671] At 20.

of companies, trusts and charities, cash, businesses and high value goods.[672] Cryptocurrencies have been placed into the "new technology" area, albeit the FIU noted that the risk "may not be as high as other countries due to lower uptake of high risk services and high levels of scrutiny from the traditional financial sector."[673]

It does not come as a surprise that the UK Treasury assessed cryptocurrencies as being of low risk for money launders. Cryptocurrencies can in fact be more traceable and less susceptible to money laundering, and indeed they have been described as "a criminal's worst nightmare".[674] Why, if you were a criminal, would you move to using cryptocurrencies when the banking system works well for your nefarious activities?

6. Current (and proposed) treatment of cryptocurrencies excluding the United States

Many countries have no direct regulation of cryptocurrencies,[675] and as the UK Government stated in 2014, "the advent of cryptocurrencies such as Bitcoin is a new and evolving area and determining their legal and regulatory status is ongoing".[676] However, the uncertainty about cryptocurrencies does not mean jurisdictions do not recognise them in certain contexts, particularly when it comes to taxation issues and AML/CFT regulation.

Some of the following is historical; but in some countries the position before regulatory changes makes for interesting reading, as it shows how regulators have grappled with cryptocurrencies. In addition, some jurisdictions are mentioned due to their treatment of ICOs, albeit ICOs are not the focus of this report.

6.1 New Zealand

New Zealand was late in grappling with cryptocurrencies. In July 2014 Geoff Bascand, Deputy Governor of the RBNZ, when speaking on behalf of the RBNZ, considered that cryptocurrencies were unlikely to replace cash in the near future.[677] This was and still is true. However, things can change quickly. Three years ago China used cash for most transactions; now, thanks to Alipay and WeChat, mobile phones are used for almost everything.[678] The RBNZ's view that cryptocurrencies such as bitcoin were speculative investment commodities rather than transactional payment instruments[679] has not been borne out, as people are using cryptocurrencies to effect payments, albeit in New Zealand the use remains low.[680] Also, because the value of using cryptocurrencies to make payments lies more with making cross-border payments from New Zealand to foreign countries the RBNZ's data is unlikely to account for such payments. In 2014 the RBNZ was monitoring trends relating to cryptocurrencies in New Zealand and overseas, but at that stage had not actively considered the

---

[672] Financial Intelligence Unit, above n 81, at 7–8.
[673] At 8.
[674] Will Yakowicx "Startups Helping the FBI Catch Bitcoin Criminals" *Inc* (9 January 2018) <https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html>. And see Mike Orcutt "Criminals Thought Bitcoin was the Perfect Hiding Place, but they Thought Wrong" *MIT Technology Review* (11 September 2017) <https://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong/>.
[675] In this report the term "cryptocurrency" is used where possible in place of terms such as "virtual currency", "digital currency" or "e-currency" to avoid confusion and maintain consistency.
[676] United Kingdom Government "Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies" (2014) <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies>.
[677] Geoff Bascand, Deputy Governor of the Reserve Bank of New Zealand "The Evolution of New Zealand's Currency" (speech given to Royal Numismatic Society, Wellington, New Zealand, July 2014) <http://rbnz.govt.nz/research-and-publications/speeches/2014/speech2014-07-05>.
[678] Nikki Mandow "China's Alipay to Join NZ's Eftpos Network" *Newsroom* (New Zealand, 14 March 2018) <https://www.newsroom.co.nz/2018/03/14/96629/alibaba-coming-to-an-eftpos-terminal-near-you>.
[679] Bascand, above n 677.
[680] See, for example, Living Room of Satoshi in Australia that allows people to pay bills with cryptocurrencies, <https://www.livingroomofsatoshi.com/graphs>.

implications of cryptocurrency regulation.[681] In 2018 the RBNZ released work on the implications of New Zealand issuing its own central bank-issued cryptocurrency.[682]

New Zealand has not, at the time of writing, passed specific legislation regulating cryptocurrencies. The lack of specific regulation, however, does not mean that cryptocurrencies are not subject to regulation. Regulators have applied existing laws to cryptocurrencies, albeit the lateness of official guidance about how the regulators would view them within existing legal frameworks has caused some confusion and uncertainty.

6.1.1 Tax treatment

In July 2014 a reputable news source quoted an IRD spokesperson as saying that cryptocurrencies should be treated in the same way as foreign currencies for tax purposes:[683]

> Generally if someone sells goods or services in exchange for bitcoin, then the market value of the goods or services received in exchange is liable for tax. People should treat an alternative "currency" dollar, such as bitcoin as they would a foreign dollar from a tax perspective, as transactions are assessable and deductible for income tax purposes to the same extent as other cash or credit transactions.

In January 2018 the same news source reported that IRD's advice had been altered, and that the IRD would be releasing guidance stating it would be treated in the same or a similar way as buying and selling gold.[684] In April 2018 the IRD released its guidance.[685] The IRD's guidance made it clear that it was not treating cryptocurrency as foreign (fiat) currency, but rather cryptocurrencies were being treated as property.[686] If a person purchased cryptocurrency for the purpose of disposal (selling or exchanging it, for example, to exchange it for another cryptocurrency) then proceeds are taxable. This means that not only is any profit taxable, but also that losses can be claimed. The IRD has not provided guidance on GST, but is working on the issue, and it is likely that the view taken that cryptocurrency is property means that technically GST is payable on all purchases and sales of cryptocurrency in New Zealand. It appears as though legislation is required to remove GST from cryptocurrency payments, as occurred in Australia.[687]

Currently the uncertainty over GST in New Zealand presents a significant barrier to exchanges providing services to New Zealanders and to local merchants accepting cryptocurrencies for payment (in combination with the banks' reluctance to provide bank accounts or to then keep them open). If GST is charged when businesses accept cryptocurrencies as payment for goods and services double taxation will occur. This will prevent cryptocurrencies from functioning as currency, which distorts the market. Moreover the charging of GST places New Zealand exchanges at a distinct disadvantage to offshore exchanges, which are exempt from New Zealand GST. It also unwittingly exposes New Zealand consumers to potentially more risk when dealing with offshore exchanges that may not be as well regulated and run as New Zealand ones. The Government has been mindful in

---

[681] Bascand, above n 677.

[682] Amber Wadsworth "Decrypting the Role of Distributed Ledger Technology in Payments Processes" (2018) 81(5) Bulletin 3 (May 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018may81-05.pdf>; Amber Wadsworth "The Pros and Cons of Issuing a Central Bank Digital Currency" (2018) 81(7) Bulletin 3 (June 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018jun81-07.pdf>; Wadsworth "What is Digital Currency?", above n 69 and see Geoff Bascand "In Search of Gold: Exploring Central Bank Digital Currency" (speech to Payments NZ Conference, Auckland, New Zealand, June 2018).

[683] Vaughan, above n 497.

[684] Jenée Tibshraeny "The IRD Says People Should Consider Money Made Selling Cryptocurrencies Bought with the Intention of Resale as Taxable, Until it Releases Specific Guidance on the Matter" *Interest.co.nz* (New Zealand, 11 January 2018) <https://www.interest.co.nz/personal-finance/91564/ird-says-people-should-consider-money-made-selling-cryptocurrencies-bought>.

[685] Inland Revenue "Questions & Answers: Cryptocurrency and tax", above n 498.

[686] Ibid.

[687] See below, Section 6.2.1 Tax treatment.

other areas to ensure that New Zealand businesses are able to operate on a level playing field with their overseas counterparts when it comes to GST. For example, in 2017 GST became chargeable for offshore digital service providers such as Netflix.[688] And, in response to urgent calls by businesses for GST to be charged for goods and services on goods purchased overseas,[689] the Government has said it plans to charge GST on all purchases from overseas retailers.[690] One question is whether GST should be removed for all cryptocurrencies. In Australia while cryptocurrencies (albeit called "digital currencies"), such as bitcoin, Ethereum, Litecoin, Dash, Monero, ZCash, Ripple and YbCoin are excluded from GST,[691] not all cryptocurrencies are treated this way. Currencies that are backed by another currency, presumably a cryptocurrency such as Tether, are not cryptocurrencies for GST purposes and thus GST is payable.[692] It is curious that Australia has taken such a stance. The purpose of having a currency backed by another currency is to create what is called a stable coin that does not fluctuate widely in price and is designed not to appreciate more than the currency which backs it. Stable coins are designed purely for use as a currency, so to charge GST on transactions using those coins makes no sense, especially when cryptocurrencies such as bitcoin and Ethereum do not attract GST.

In addition, cryptocurrencies that allow people to do something on a network, commonly called utility coins, are not GST exempt.[693] The Australian Taxation Office (ATO) provides the following useful example of a fictitious cryptocurrency that would not be GST exempt:[694]

> Hybrid Co is developing a new digital currency, NewCoin. It is designed to be the exclusive payment method for DistStore distributed file storage network, and it is also intended to be freely used outside this network.
>
> The file storage network will rely on third party participants buying and selling file storage services, and setting their own prices in NewCoin.
>
> Under the terms of issue of the Initial Coin Offering (ICO) arranged by Hybrid Co, all NewCoins contain a permanent right to a specified amount of file storage that will be supplied by Hybrid Co. The purpose is to ensure that any prospective DistStore users have confidence in being able to acquire file storage with their NewCoins, even if there are not enough providers that offer file storage on DistStore at [a] certain time.
>
> NewCoins would not be [crypto]currency for GST purposes as they carry an entitlement to file storage in addition to them being able to be used as payment on DistStore.

At the very least New Zealand needs to enact legislation which follows Australia's and remove GST on cryptocurrencies that are being used as currencies, but New Zealand should not follow Australia and exclude those cryptocurrencies that are backed by other currencies, especially fiat currencies.

In addition there is a lack of clarity on how businesses are to treat the receipt of cryptocurrencies (and fiat currency) they receive through ICOs, for example, whether a business can defer the recognition of income to later years. The IRD advises that businesses wishing to do an ICO should

---

[688] Taxation (Residential Land Withholding Tax, GST on Online Services, and Student Loans) Act 2016 and see Holly Ryan "'Netflix' Tax to Take Effect from Tomorrow" *The New Zealand Herald* (online ed, 30 September 2016) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11720057>.

[689] See, for example, Madison Reidy "NZ Businesses Want GST Law Change as International Online Retailers Pocket Government Millions" *Stuff* (New Zealand, online ed, 6 July 2017) <https://www.stuff.co.nz/business/94400111/nz-businesses-want-gst-law-change-as-international-online-retailers-pocket-government-millions>.

[690] Hon Stuart Nash and Hon Meka Whaitiri "GST Loophole Closed to Offshore Companies" (Press release, 1 May 2018) <http://taxpolicy.ird.govt.nz/news/2018-05-01-gst-imported-low-value-goods-proposals-launched>.

[691] Australian Taxation Office "GST and Digital Currency" <https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency/>.

[692] Ibid.

[693] Ibid.

[694] Ibid.

applying for a binding ruling.[695] While not every ICO is the same, it would be useful for the IRD to provide guidance on commonly structured ICOs.

6.1.2 AML/CFT

Although this report focuses on the use of cryptocurrencies for payments, some more mention will be made of the DIA (Department of Internal Affairs) and the FMA (Financial Markets Authority). The DIA is New Zealand's supervisor for money exchangers for AML/CFT purposes,[696] and it regards cryptocurrency exchanges to be money changers.[697] Nothing is ever simple, however. There are a range of different cryptocurrencies and if an exchange allows trading of what the FMA regards as financial products then they may also be under the supervision of the FMA and be required to obtain a licence to operate.[698]

6.1.3 Financial regulation and consumer protection

The FMA issued a warning in October 2017 that "cryptocurrencies are digital tokens you can buy through an online exchange or through Initial Coin Offers (ICOs). Many online exchanges are unregulated, so it's important to understand the risks before you invest."[699]

In regards to the regulation of ICOs, in October 2017 the FMA released its guidance on ICOs, stating that depending on the token involved they can be either debt securities, equity securities, managed investment products or derivatives.[700] The FMA is continuing to work on its guidance.[701] Fortunately the FMA has given an indication of what form that guidance is likely to take.[702] There is no indication that the FMA is seeking law changes, in contrast to the IRD.

6.2 Australia

Australia was mindful early that regulation of cryptocurrencies may be desirable. In October 2014 the Australian Senate referred the matter of cryptocurrencies to the Economics References Committee (ERC) for inquiry.[703] The inquiry's aim was to "examine how best to define digital currency within the regulatory frameworks in order to support innovation and the needs of the growing Australian digital currency industry".[704] The ERC, after analysing the submissions of relevant stakeholders and interested parties, made four recommendations:

(1) Cryptocurrencies be treated as money for GST purposes. To achieve this, the ERC recommended that the Australian Government, in consultation with states and territories, amend the definition of money in the A New Tax System (Goods and Services Tax) Act 1999 (Cth) and include cryptocurrency in the financial supply definition in A New Tax System (Goods and Services Tax) Regulations 1999 (Cth);[705]

---

[695] Inland Revenue "Questions & Answers: Cryptocurrency and tax", above n 498.
[696] New Zealand Department of Internal Affairs "List of Reporting Entities" <https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-List-of-Reporting-Entities?OpenDocument>.
[697] The document DIA "Currency Exchange / Money Changing" (April 2014) has been provided by the DIA to New Zealand businesses wishing to set up cryptocurrency exchanges in New Zealand (on file with authors).
[698] Financial Markets Authority "Market operators: Who needs to comply" <https://fma.govt.nz/compliance/role/market-operators/who-needs-to-comply-2/>.
[699] Financial Markets Authority "Cryptocurrencies", above n 557.
[700] Financial Markets Authority "Initial Coin Offers" <https://fma.govt.nz/compliance/cryptocurrencies/initial-coin-offers/>.
[701] The FMA in its Annual Corporate Plan 2018/19 states that as part of its activities and milestones for 2018/19 it will be "[r]eviewing and issuing guidance on new products and services when required, eg guidance for ICOs": Financial Markets Authority "Annual Corporate Plan 2018/19" at 21 <https://fma.govt.nz/assets/FMAs-role/180808-FMA-Annual-Corporate-Plan-2018-19.pdf>.
[702] Andrew Dentice "More Certainty for NZ Blockchain Industry as Regulator Continues Proactive Approach" Hudson Gavin Martin (19 April 2017) <http://whatshappeningnow.hgmlegal.com/post/102eudg/more-certainty-for-nz-blockchain-industry-as-regulator-continues-proactive-approa>.
[703] Economics References Committee, above n 66, at [1.1].
[704] At [1.3].
[705] At [4.35].

(2) The appropriate tax treatment of cryptocurrencies, especially income tax and fringe benefit tax, be included for consideration in the taxation Whitepaper process;[706]
(3) The Australian Government consider developing a Digital Economy Taskforce to obtain information about uses, opportunities and risks associated with cryptocurrencies. The proposed taskforce will enable regulators such as the Reserve Bank of Australia and ASIC to determine when cryptocurrency businesses may require regulation. The ERC supported continued self-regulation development in the meantime;[707] and
(4) AML/CTF regulations be applied to cryptocurrency exchanges.[708]

6.2.1 Tax treatment

As noted above by the ERC, transactions involving cryptocurrencies were treated as barter arrangements in Australia, similar to the position in Canada.[709] Cryptocurrencies are not considered money, foreign currency or a financial supply of goods and services, although they are considered an asset for capital gains tax purposes.[710] Transactions involving cryptocurrencies therefore had similar tax consequences to barter arrangements.[711] In August 2014 the ATO (Australian Tax Office) released a number of rulings on how bitcoin should be treated for tax purposes.[712] The rulings, finalised in December 2014, were:

> Capital Gains Tax (CGT): if cryptocurrencies are used for investment purposes, they are subject to CGT upon disposal as if they were shares or similar.[713] Cryptocurrencies used for personal everyday transactions, where the cost of the cryptocurrency is under A$10,000, are not subject to CGT.[714]
>
> Goods and Services Tax (GST): GST applies to individuals' purchases of cryptocurrencies and to businesses who sell or buy cryptocurrencies in the same way as other goods or services.[715]

---

[706] At [4.45].
[707] At [5.64].
[708] At [6.37].
[709] At [2.8] and [2.13].
[710] Australian Government "Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin" (18 December 2014) <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>.
[711] Ibid and Taxation Ruling No. IT 2668 "Income Tax: Barter and Countertrade Transactions" (13 February 1992) <http://law.ato.gov.au/atolaw/view.htm?docid=ITR/IT2668/NAT/ATO/00001>.
[712] Economics References Committee, above n 66, at [2.8]; Taxation Determination TD 2014/25 "Income Tax: Is Bitcoin a 'Foreign Currency' for the Purposes of Division 775 of the Income Tax Assessment Act 1997?" <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201425/NAT/ATO/00001>; Taxation Determination TD 2014/26 "Income Tax: is Bitcoin a 'CGT Asset' for the Purposes of Subsection 108-5(1) of the Income Tax Assessment Act 1997?" <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201426/NAT/ATO/00001>; Taxation Determination TD 2014/27 "Income Tax: Is Bitcoin Trading Stock for the Purposes of Subsection 70-10(1) of the Income Tax Assessment Act 1997?" <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201427/NAT/ATO/00001>; Taxation Determination TD 2014/28 "Fringe Benefits Tax: is the Provision of Bitcoin by an Employer to an Employee in Respect of their Employment a Property Fringe Benefit for the Purposes of Subsection 136(1) of the Fringe Benefits Tax Assessment Act 1986?" <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201428/NAT/ATO/00001>; and Goods and Services Tax Ruling GSTR 2014/3 "Goods and services tax: the GST implications of transactions involving bitcoin" <http://law.ato.gov.au/atolaw/view.htm?DocID=GST/GSTR20143/NAT/ATO/00001>.
[713] Taxation Determination TD 2014/26, ibid.
[714] Australian Government "Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin", above n 710 and Taxation Determination TD 2014/26, above n 712.
<http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201426/NAT/ATO/00001> at 17.
[715] Australian Government "Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin", above n 710; and Goods and Services Tax Ruling GSTR 2014/3 Goods and services tax: the GST implications of transactions involving bitcoin <http://law.ato.gov.au/atolaw/view.htm?DocID=GST/GSTR20143/NAT/ATO/00001> above n 702, at 7.

> Income Tax (IT): Businesses which operate a cryptocurrency exchange, buy and sell cryptocurrency or mine cryptocurrency pay IT on their profits.[716] If a business is paid in cryptocurrency the amount must be included in their income in Australian dollars and is assessable income.[717]
>
> Fringe Benefits Tax (FBT): If an employee is paid in cryptocurrency and has a valid salary sacrifice agreement then it is subject to FBT.[718] If not, the normal PAYG [pay as you go] rules apply as with any other wages or salary.[719]

The ERC recommended that cryptocurrencies be treated as money for GST purposes, but there was disagreement among submitters as to whether cryptocurrencies should be treated in the same way as foreign currencies for income tax, FBT and CGT.[720] Some argued there was scope within the existing legislation to define cryptocurrencies as foreign currencies instead of commodities, and disagreed with the ATO's interpretation of the then tax law.[721] The Tax Institute claimed that currency and money are defined broadly enough in the existing tax law to include bitcoin[722] (the Income Tax Assessment Act 1997 (Cth) defines foreign currency as "currency other than Australian currency"),[723] and that if cryptocurrencies were adopted by foreign countries as legal tender, then such cryptocurrencies would automatically fall within the definition of foreign currency for tax and GST purposes and as money for FBT purposes.[724]

Submitters also raised concerns about the ATO ruling that cryptocurrencies be treated as property for FBT purposes and in the paying of salaries and wages.[725] The Bitcoin Foundation and Bitcoin Association of Australia observed that there are a number of international businesses that pay their employees in bitcoin, and that Australia subjecting such payments to FBT would be a barrier for Australian businesses in attracting "global talent".[726] The Tax Institute proposed that salary and wages paid in cryptocurrency should not be a fringe benefit for FBT purposes.[727] In addition, Taxpayers Australia raised concerns about the application of the FBT regime to cryptocurrencies, stating that "'further consideration of the degree of integration into the PAYG withholding system, the superannuation and other employment tax obligation regimes will need to be made in respect of digital currencies".[728]

Some submitters argued that the definition of currency for both income tax and GST purposes should be changed to include cryptocurrencies.[729] For example, the Australian Digital Currency Commerce Association, a group that represents the cryptocurrency industry in Australia, noted that if cryptocurrencies are classified in the same way as foreign currency in Australian tax law it will ensure the use of cryptocurrencies alongside fiat currencies as a method of payment is "not rendered obsolete before it has had a chance to enter the mainstream payment system and be

---

[716] Taxation Determination TD 2014/27 "Income Tax: Is Bitcoin Trading Stock for the Purposes of Subsection 70-10(1) of the Income Tax Assessment Act 1997?", above n 702, at 13.
[717] Australian Government "Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin", above n 710.
[718] Economics References Committee, above n 66, at [2.10]; and Taxation Determination TD 2014/28 "Fringe Benefits Tax", above n 702, at 1.
[719] Australian Government "Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin", above n 710.
[720] Economics References Committee, above n 66, at [4.35–4.36].
[721] At [4.37].
[722] Ibid.
[723] Income Tax Assessment Act 1997 (Cth), s 995.1.
[724] Economics References Committee, above n 66, at [4.37].
[725] At [4.38].
[726] Ibid.
[727] Ibid.
[728] Ibid.
[729] At [4.39–4.40].

tested by the market".[730] Likewise, it was argued to that to solve the problem, a new concept of "digital currency" should be introduced and included within the concepts of money.[731]

In contrast, the Tax and Transfer Policy Institute disagreed with the view that cryptocurrencies should be treated as foreign currencies for income tax, FBT and CGT purposes. It was of the view that characterising cryptocurrencies as foreign currencies would not likely be beneficial to users for tax purposes, and that doing so would actually add "unnecessary complexity, with no gain for the ATO and digital currency users".[732] It considered that because foreign currency is usually treated as a capital asset for CGT and income tax purposes, classifying cryptocurrency as foreign currency would not make significant difference to its tax treatment for CGT and income tax because disposing of foreign currency and disposing of a commodity have broadly similar consequences.[733] The Tax and Transfer Policy Institute did not recognise a clear policy basis for classifying cryptocurrencies as money for income tax purposes at the time of their submission, instead recommending that further research and analysis be undertaken before amending income tax law in regard to cryptocurrencies.[734]

Another view was that while the Australian Treasury was monitoring cryptocurrencies, the cryptocurrency industry was in its infancy, and it was too soon to be making changes to tax law to accommodate the cryptocurrency industry.[735] The ERC concluded that further research was needed before cryptocurrencies are regarded as foreign currency for income tax and FBT,[736] and recommended including the issue in the taxation Whitepaper process.[737]

The Australian Parliament accepted the call for the removal of GST on the purchase and sale of digital currencies and GST was lifted retrospectively effective from 1 July 2017.[738] The ATO has issued guidance that it sees bitcoin as neither money nor foreign currency, but rather, in line with New Zealand, considers it property and thus an asset for CGT.[739]

6.2.2 Anti-money laundering and counter-terrorism financing

At the time of the ERC inquiry, cryptocurrencies were not covered under section 5 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), despite the Act covering "e-currency", which is very narrowly defined in section 5 as: [740]

> … an internet-based, electronic means of exchange that is:
>
> (a) known as any of the following:
>
> (i) e-currency;
>
> (ii) e-money;
>
> (iii) digital currency;
>
> (iv) a name specified in the AML/CTF Rules; and
>
> (b) backed either directly or indirectly by:

[730] Economics References Committee, above n 66, at [4.39].
[731] At [4.40].
[732] At [4.41].
[733] At [4.41].
[734] At [4.42].
[735] At [4.43].
[736] At [4.44].
[737] At [4.45].
[738] Section 9-10(4) of A New Tax System (Goods and Services Tax) Act 1999 (Cth) was amended by No 118 of 2017 from "However, a supply does not include a supply of money unless the money is provided as consideration for a supply that is a supply of money" to "However, supply does not include: (a) a supply of money unless the money is provided as consideration for a supply that is a supply of money or digital currency; or (b) a supply of digital currency unless the digital currency is provided as consideration for a supply that is a supply of digital currency or money."
[739] Australian Taxation Office "Tax treatment of cryptocurrencies" <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>.
[740] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 5.

(i) precious metal; or
(ii) bullion; or
(iii) a thing of a kind prescribed by the AML/CTF Rules; and
(iv) not issued by or under the authority of a government body;
(c) and includes anything that, under the regulations, is taken to be e-currency for the purposes of this Act.

Businesses that dealt in cryptocurrencies were concerned about the absence of cryptocurrencies in the Act: they argued this restricted their access to banking services because Australian banks refused to provide service on the grounds that cryptocurrency businesses "pose an unacceptable risk to the banks' business and reputation".[741] While cryptocurrency transactions could be monitored at the on-ramp and off-ramp stages, for example in transactions between foreign accounts and Australian accounts for the sale or purchase of cryptocurrencies,[742] for the large part they were unregulated with regard to AML/CFT.

The Australian Government heeded the calls for greater regulation, particularly as regulation would be seen as Australia complying with the FATF's suggestions of targeting exchanges.[743] In April 2016 the Australian Government released its "Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations".[744] Following consultation[745] Australia amended its AML/CTF law and from 3 April 2018 cryptocurrency exchanges became subject to AML/CTF[746] obligations.[747] The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) was amended[748] with the definition of digital currency inserted. Digital currency was defined in section 5 as meaning:

(a) a digital representation of value that:
  (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
  (ii) is not issued by or under the authority of a government body; and
  (iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and
  (iv) is generally available to members of the public without any restriction on its use as consideration; or
(b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;

but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of this Act.

[741] Economics References Committee, above n 66, at [6.7].
[742] At [2.29].
[743] Financial Action Task Force "Guidance for a Risk-Based Approach: Virtual Currencies" (June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> 14.
[744] Attorney-General's Department "Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations" (2016) <https://www.homeaffairs.gov.au/consultations/Documents/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>.
[745] Attorney-General's Department "Regulating Digital Currencies under Australia's AML/CTF regime – Consultation Paper" (December 2016).
[746] Somewhat confusingly Australia (and some other countries) use the term "AML/CTF", whereas in New Zealand the term "AML/CFT" is used.
[747] Australian Transaction Reports and Analysis Centre "Digital Currency Exchange Providers: Register Online with AUSTRAC" (3 April 2018) <http://www.austrac.gov.au/news/digital-currency-exchange-providers-register-online-austrac>. The Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth) amended the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth) s 5 now has inserted a definition of digital currency and in s 4 inserted that "Providers of registrable digital currency exchange services must be registered with the AUSTRAC CEO."
[748] Amended by the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017 (Cth).

In Australia, cryptocurrency exchanges must now be registered with Australian Transaction Reports and Analysis Centre (AUSTRAC) and are required to:[749]

- have and maintain an AML/CTF programme to identify, mitigate and manage money laundering and terrorism financing risks;
- identify and verify their customers' identities;
- report to AUSTRAC suspicious matters and transactions involving physical currency $10,000 or more;
- keep certain records for seven years.

6.2.3 Financial regulation and consumer protection

At the time of the ERC's report cryptocurrencies did not fall under the Payment Systems (Regulation) Act 1998 (Cth), which is regulated by the Reserve Bank of Australia (RBA), and were not considered a financial product under the Corporations Act 2001 (Cth) or the Australian Securities and Investments Commission Act 2001 (Cth).[750] However, some facilities associated with cryptocurrencies may fall within the definition of financial products.[751] ASIC, in its submission to the ERC inquiry, considered a wide range of facilities associated with cryptocurrencies and came to the conclusion that the following are financial products:[752]

- Contracts for the sale or purchase of cryptocurrencies where there is a delay between agreement on price and delivery of the cryptocurrency are derivatives and therefore are a financial product.[753] Consequently the financial services and financial markets regimes apply in the normal way.[754]
- The use of cryptocurrencies incorporated into products provided by licensed financial services providers. For example, derivatives offered over cryptocurrencies because they allow for speculation over the price of cryptocurrencies; and arrangements that allow merchants to receive payment in cryptocurrencies because such arrangements may be non-cash payment facilities.[755]
- Facilities that allow the purchase of goods or services to be paid for in cryptocurrencies even if the merchant does not accept cryptocurrencies as payment. Such facilities act as intermediaries by transferring the cryptocurrency payment to real currency which is then transferred to the merchant. The intermediary provides a non-cash payment facility and as such may require an Australian Financial Services licence.[756]

In September 2017 ASIC issued guidance for ICOs. As with New Zealand's FMA, how ICOs will be regulated depends on the tokens that are issued.[757]

In 2015 the RBA announced it would undertake a review of the existing legislation to assess whether it could accommodate cryptocurrencies and other alternatives, [758] but as yet no result has been

---

[749] Australian Transaction Reports and Analysis Centre "Digital Currency Exchange Providers: Register Online with AUSTRAC", above n 737; and see Anti-Money Laundering and Counter-Terrorism Financing (Digital Currency Exchange Register) Policy Principles 2018.
[750] Economics References Committee, above n 66, at [2.14–2.16].
[751] Australian Securities and Investments Commission *Submission 44* (December 2014) at 11 <http://www.aph.gov.au/DocumentStore.ashx?id=4b6d105f-3e0a-4d52-aaab-1f35842ed5f1&subId=302297>.
[752] At [54–70].
[753] At [61].
[754] At [62].
[755] At [67].
[756] At [68].
[757] Australian Securities and Investments Commission "17-325MR ASIC Provides Guidance for Initial Coin Offerings" (28 September 2017) <http://asic.gov.au/about-asic/media-centre/find-a-media-release/2017-releases/17-325mr-asic-provides-guidance-for-initial-coin-offerings/>. For the actual guidance see Australian Securities and Investments Commission "Initial coin offerings: INFO 225" < https://www.asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/>.
[758] Stan Higgins "Australian Government to Review Bitcoin Regulation Powers" *CoinDesk* (20 October 2015) <http://www.coindesk.com/australian-government-to-review-bitcoin-regulation-powers/>; and Economics References Committee, above n 66, at [2.15].

released. Indeed, in a speech to the House of Representatives Standing Committee on Tax and Revenue in October 2017 the RBA stated that:[759]

> We note that Committee members have expressed interest in digital currencies or cryptocurrencies. This, and the broader area of distributed ledger technology, is a topic that the Bank has been monitoring closely over recent years.
>
> There have been substantial increases in the prices of cryptocurrencies like bitcoin and ether over the past year. Most of this seems to relate to speculative demand and in particular the use of digital currencies as the means of participation in Initial Coin Offerings. The use of bitcoin and other digital currencies as an actual method of payment remains relatively limited in Australia, as elsewhere. From the Bank's payments policy mandate, digital currencies do not currently appear to raise any pressing regulatory issues.
>
> Cryptocurrencies can serve as a means of payment in the illicit economy. Accordingly, their use may have some implications for tax authorities and they raise more significant issues for authorities tasked with crime prevention and detection. The distributed and cross-border nature of digital currencies like bitcoin means that regulation of the core protocols of these systems is unlikely to be effective. Authorities have therefore tended to focus on the "on-ramps" and "off-ramps" – that is the links to the traditional payments system. In some jurisdictions, central banks and other authorities have taken action in relation to digital currency exchanges, such as the measures undertaken by the People's Bank of China earlier this year.
>
> While the longer-term prospects for private digital currencies are unclear, the Bank has previously noted that the distributed ledger and blockchain technologies underlying them have potential for widespread use in the financial sector and many other parts of the economy. The greatest potential is likely to be in sectors where workflows involve lots of different parties with no trusted central entity, and where current practices are quite inefficient. Some frequently suggested financial sector use cases include correspondent banking and remittances, as well as trade financing.

ASIC has advised consumers about the risks involved with cryptocurrencies on its webpage, MoneySmart, stating firmly that "if you decide to trade or use virtual currencies you are taking on a lot of risk with no recourse if things go wrong".[760] In addition, general consumer protection provisions contained in the Competition and Consumer Act 2010 (Cth), administered by the Australian Competition and Consumer Commission (ACCC), apply to cryptocurrencies, so there is a certain degree of protection.[761] For example, the Act states that service providers must not make false or misleading representations[762] or engage in unconscionable conduct.[763]

6.3 United Kingdom

Her Majesty's Revenue and Customs (HMRC) has stated that "for businesses which accept payment for goods or services in bitcoin there is no change to when revenue is recognised or how taxable profits are calculated".[764] Therefore, the UK Government accepts that people in the UK hold cryptocurrencies as investments and also that cryptocurrencies are being accepted by UK merchants for goods and services.

---

[759] Tony Richards and David Emery, Reserve Bank of Australia "Opening Statement to the Inquiry into Taxpayer Engagement with the Tax System" (speech to House of Representatives Standing Committee on Tax and Revenue, Canberra, October 2017) <https://www.rba.gov.au/speeches/2017/sp-so-2017-10-27.html>.

[760] Australian Securities and Investments Commission "Virtual Currencies" (8 September 2016) MoneySmart <https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies>.

[761] Economics References Committee, above n 66, at [2.21].

[762] Competition and Consumer Act 2010 (Cth), Sch 2, s 18.

[763] Competition and Consumer Act 2010 (Cth), Sch 2, s 20.

[764] See United Kingdom Government "Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies", above n 676.

6.3.1 Tax treatment

Corporation tax (CT): cryptocurrencies are subject to the general rules of foreign exchange and loan relationships and profits or losses on exchange movements are taxable.[765] The UK Government has not considered it necessary to entertain bespoke rules for cryptocurrencies because if there is an exchange rate between cryptocurrencies and the functional currency then movements between the two are reported in the company's profit and loss accounts and are taxable under normal CT rules.[766]

Income tax: profits and losses on cryptocurrency transactions must be reported in a non-incorporated company's accounts and are taxable under normal income tax rules.[767]

Chargeable gains including CT and CGT: profits or losses on currency contracts that are not covered by trading profits or loan relationship tax rules are normally taxable as a chargeable gain or allowable as a loss under CT or CGT.[768] Gains and losses on cryptocurrencies are covered by CGT for individuals and for CT if they accrue to a company.[769] Notwithstanding the guidance, tax was not seen as a particular issue until the latter part of 2017 and the beginning of 2018 as the price of many cryptocurrencies rose rapidly.[770]

Value Added Tax (VAT): VAT is an EU tax and as such the tax treatment of cryptocurrencies in the UK must be consistent with the tax treatment that may be implemented across the EU.[771] HMRC has outlined provisional VAT liabilities for supplies of cryptocurrencies; further development of the VAT liabilities outlined below is dependent on the development of regulatory and EU VAT provisions (albeit with Brexit the UK may not have to continue to follow EU VAT law):[772]

- Bitcoin mining does not constitute an economic activity for VAT purposes because there is "an insufficient link between any services provided and any consideration received".[773] Therefore, any bitcoin received by miners for bitcoin mining activity is generally outside the scope of VAT liability.[774]
- Miners and others who perform certain specific bitcoin transactions are exempt from VAT on charges they make on the transactions under the Value Added Tax Act 1994, which exempts "the issue, transfer or receipt of, or any dealing with, money, any security for money or any note or order for the payment of money".[775] Charges made "over and above the value of the Bitcoin" on the performance of related intermediary services, such as arranging bitcoin transactions, that meet conditions outlined in VATFIN7200[776] are also exempt from VAT.[777]

---

[765] Ibid.
[766] Ibid.
[767] Ibid.
[768] Ibid.
[769] Ibid.
[770] See, for example, David Dawkins "Bitcoin warning: Cryptocurrency Profits to be TAXED" *Express* (UK, online ed, 27 December 2017) <https://www.express.co.uk/finance/city/897066/HMRC-Bitcoin-warning-Cryptocurrency-profits-to-be-TAXED> and Andrew Goldstone and Helen Cox "Do You Need to Declare your Cryptocurrency to HMRC?" Mishcon de Reya (12 January 2018) <https://www.mishcon.com/news/briefings/do-you-need-to-declare-your-cryptocurrency-to-hmrc>.
[771] United Kingdom Government "VAT Finance Manual: VATFIN2330" (8 April 2016) <https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin2330>.
[772] Ibid.
[773] Ibid.
[774] Ibid.
[775] Value Added Tax Act 1994, Item 5, Sch 9, Gp 5.
[776] A supplier of an exempt intermediary service under VATFIN7200 is one who: "brings together a person seeking a financial service with a person providing a financial service; acts as intermediary between the parties in the contract; and undertakes work to prepare the contract for provision of financial services – whether the contract is completed or not." United Kingdom Government "VAT Notice 701/49: Finance" (30 January 2013) <https://www.gov.uk/government/publications/vat-notice-70149-finance/vat-notice-70149-finance#intermediaries>; and United Kingdom Government "VAT Finance Manual: VATFIN7200" (8 April 2016) <https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin7200>.
[777] Value Added Tax Act 1994, Item 5, Sch 9, Gp 5.

- No VAT will be due on the value of bitcoin itself in transactions where it is exchanged for goods or services.[778]
- In all instances where cryptocurrencies are exchanged for goods or services, VAT will be due in the normal way on the sterling value of the cryptocurrency at the time the transaction takes place.[779]

In formulating provisional VAT liabilities for cryptocurrencies, HMRC took into account *Skatteverket v David Hedqvist*[780] decided by the Court of Justice of the European Union, which considered whether bitcoin exchange transactions constituted a supply for VAT purposes and if so, whether they would be exempt. The Court, referring to *Commissioners of Customs and Excise v First National Bank of Chicago*,[781] ruled that bitcoin exchange transactions do constitute a supply of services effected for consideration and that exchange of traditional currencies for cryptocurrencies are financial transactions that fall within the exemption under Article 135(1)(e) of the VAT Directive.[782]

In March 2014 the UK Government made it clear that the tax treatment of cryptocurrencies was limited solely to tax purposes and was no indication of the treatment of cryptocurrencies for "regulatory or other purposes".[783]

6.3.2 Anti-money laundering and counter-terrorism financing

In March 2015 the UK Government recognised that cryptocurrencies were attractive to both illegal and legitimate users alike due to their unique features, and stated its intention to apply AML regulation to cryptocurrency exchanges to "support innovation and prevent criminal use".[784] The Government committed itself to a full consultation on a proposed regulatory approach in the next Parliament. In response to a written question to the Chancellor of the Exchequer as to "what steps his Department is taking to regulate (a) bitcoin and (b) other crypto-currencies", the answer was:[785]

> The UK government is currently negotiating amendments to the 4th Anti-Money Laundering Directive that will bring virtual currency exchange platforms and custodian wallet providers into Anti-Money Laundering and Counter-Terrorist Financing regulation, which will result in these firms' activities being overseen by national competent authorities for these areas. The government supports the intention behind these amendments. We expect these negotiations to conclude at EU level in late 2017/early 2018.

A Briefing Paper on "The Sanctions and Anti-Money Laundering Bill 2017-19" was released,[786] and it was noted that the Treasury planned to regulate cryptocurrencies so that they meet AML/CTF legislation.[787] As part of this, traders would be required to disclose their identities.[788] The Government also considered the risks users of cryptocurrencies are exposed to and stated its intention to work with the British Standards Institution and the cryptocurrency industry to create a

---

[778] United Kingdom Government "VAT Finance Manual: VATFIN2330", above n 771.
[779] United Kingdom Government "Revenue and Customs Brief 9 (2014): Bitcoin and other Cryptocurrencies", above n 676.
[780] Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECR I-498.
[781] Case C-172/96 *Commissioners of Customs and Excise v First National Bank of Chicago* [1998] ECR I-4387.
[782] Council Directive 2006/112/EC on the common system of value added tax [2006] OJ L 347; United Kingdom Government "VAT Finance Manual: VATFIN2330", above n 771.
[783] United Kingdom Government "Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies", above n 676.
[784] United Kingdom HM Treasury "Digital Currencies: Response to the Call for Information" (March 2015) at [4.2] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> cited in Natalie Chapman "Defining the Regulatory Landscape of Virtual Currencies in New Zealand**"** (LLB (Hons) Dissertation, University of Auckland, 2016) at 28; and see United Kingdom HM Treasury "Digital Currencies: Response to the Call for Information" (March 2015) at [1.5].
[785] United Kingdom Parliament "Cryptocurrencies: Regulation: Written question – 110111" (27 October 2017).
[786] Ben Smith "The Sanctions and Anti-Money Laundering Bill 2017-19" (15 February 2018) House of Commons Library, Briefing Paper.
[787] Julia Kollewe "Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears" *The Guardian* (UK, online ed, 4 December 2017) <https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity>.
[788] Ibid.

framework for best practice standards for consumer protection – one that would address the identified risks but avoid imposing a "disproportionate regulatory burden on the industry".[789] The Sanctions and Anti-Money Laundering Act 2018 received Royal Assent on 23 May 2018, but at the time of writing it has yet to come into force. Part 2 of the Act allows the UK Government to make regulations to enable or facilitate the detection, investigation or prevention of money laundering and financing of terrorism.

6.4 Canada

As with New Zealand and Australia, the Canadian Government was concerned about the risks posed to consumers due to cybertheft, bankruptcy of a digital currency exchange or volatility in the price of digital currencies.[790]

6.4.1 Tax treatment

Canadian regulatory authorities such as the Canada Revenue Agency and the Bank of Canada do not consider that cryptocurrencies are "money" or "currency" for Canadian tax purposes.[791] Therefore, the use of cryptocurrencies in purchasing or selling goods or services is considered a barter transaction, where "two persons agree to a reciprocal exchange of goods or services and carry out that exchange usually without using money".[792] Cryptocurrencies are considered property, not currency, for tax purposes and the normal tax rules relating to property apply.[793]

The income tax implications mean that barter transactions need to be reported in Canadian dollars where the person is a business or where the amount must be brought into income, and the amount is equal to the amount a person would have charged in an arm's length transaction.[794] For GST or Harmonized Sales Tax where applicable, the amount payable is determined by the market value of the cryptocurrency at the time of the transaction.[795]

If a taxpayer has a cryptocurrency mining business, their income for the year will be determined by their inventory at the end of the year.[796] If cryptocurrency is given as a gift, the eligible amount for tax purposes is determined by the fair market value of the cryptocurrency, which is a question of fact.[797] The Canadian Government also recognises that cryptocurrencies can be bought and sold as a

---

[789] United Kingdom HM Treasury "Digital Currencies: Response to the Call for Information", above n 784 at [4.5] and United Kingdom HM Treasury "Budget 2015" (March 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/416330/47881_Budget_2015_Web_Accessible.pdf> at [2.215].

[790] Standing Committee on Banking, Trade and Commerce (Canada) *Digital Currency: You Can't Flip this Coin!* (June 2015) <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rms/12jun15/home-e.htm>.

[791] Canada Revenue Agency Document No. 2013-0514701I7 "Bitcoins" (23 December 2013) <http://www.canadiantaxlitigation.com/wp-content/uploads/2014/01/2013-0514701I7.txt>; Olivier Fournier and John J Lennard "Rebooting Money: The Canadian Tax Treatment of Bitcoin and Other Cryptocurrencies" (paper presented to Canadian Tax Foundation, 2014 Conference) at 11:2 <https://dwpv.com/~/media/Files/PDF_EN/2015/2015-10-09-Annual-Conference-Report-Bitcoin.ashx>; and Christopher Payne "IRS: Bitcoin Not a Currency for Tax Purposes" Dentons (4 April 2014) <http://www.canadiantaxlitigation.com/irs-bitcoin-not-a-currency-for-tax-purposes>.

[792] Income Tax Interpretation Bulletin IT-490 "Barter Transactions" (5 July 1982) <http://www.cra-arc.gc.ca/E/pub/tp/it490/it490-e.html> at [3].

[793] Canada Revenue Agency Document No. 2013-0514701I7 "Bitcoins", above n 791.

[794] Income Tax Interpretation Bulletin IT-490 "Barter Transactions", above n 792.

[795] Financial Consumer Agency of Canada "Digital Currency" <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html> and see Timothy Fitzsimmons "Bitcoin: More Guidance from the CRA" Dentons (22 January 2014) <http://www.canadiantaxlitigation.com/bitcoins-more-guidance-from-the-cra>.

[796] Income Tax Act 1985, s 10(1); Income Tax Regulations (CRC, c 945), Part XVIII and Fitzsimmons, ibid.

[797] Katie Robinson "Tax Issues Relating to Bitcoins" (23 December 2013) <http://www.canadiantaxlitigation.com/wp-content/uploads/2014/01/2013-0514701I7.txt>.

commodity so gains or losses could be taxable income or capital for the user of the cryptocurrency and taxed accordingly.[798]

6.4.2 Anti-money laundering and counter-terrorism financing

In June 2015 the Canadian Standing Senate Committee on Banking, Trade and Commerce published a report on its inquiry into the treatment of cryptocurrencies.[799] A number of recommendations were made, including:

- The government should exercise a regulatory "light touch" to avoid stifling new cryptocurrencies and their technologies, and should create an environment that "fosters innovation" for cryptocurrencies;[800]
- Cryptocurrency exchanges should be required to conform to the same requirements as Money Services Businesses (MSBs);[801]
- The government should work with other countries on an "ongoing and active basis" to formulate worldwide guidelines for cryptocurrencies;[802] and
- The government should assess the appropriateness of the cryptocurrency regulatory environment in the next three years.[803]

Canada's regulatory position on cryptocurrencies is focused on exchanges, which the Standing Senate Committee described as the "on and off ramps of the digital currency system".[804] Curiously, the Standing Senate Committee on Banking, Trade and Commerce Report was published well after Parliament had passed a Bill[805] that was designed to amend Canada's AML/CFT legislation.[806]

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act[807] was amended in 2014 to specifically include persons or entities dealing in the business of cryptocurrencies (referred to as virtual currencies) as defined by the regulations.[808] However, while proposed regulations were published in the Canada Gazette in July 2015[809] they have yet to come into force.[810] The proposed regulations cover businesses, such as cryptocurrency exchanges like MSBs, but do not cover individuals or businesses that use cryptocurrencies for buying or selling goods or services.[811] The proposed regulations will require a cryptocurrency business to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), report certain suspicious transactions and certain clients, keep records and ensure a compliance regime is followed.[812] The

---

[798] Canada Revenue Agency "What you should Know about Digital Currency" (3 December 2014) <http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html>.
[799] Standing Committee on Banking, Trade and Commerce (Canada), above n 790.
[800] At 13.
[801] At 14.
[802] At 15.
[803] At 17.
[804] At 9.
[805] An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures ("Bill C-31").
[806] Proceeds of Crime (Money Laundering) and Terrorist Financing Act SC 2000, c 17 ("PCMLTFA").
[807] Ibid.
[808] The Economic Action Plan 2014 Act, No. 1. s 244.7(4)(a)(iv) and (b)(iv).
[809] "Regulations Amending Certain Regulations Made under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2015" 149(27) Canada Gazette <http://gazette.gc.ca/rp-pr/p1/2015/2015-07-04/html/reg2-eng.php>.
[810] Corin Faife "Canada Is Gearing Up to Regulate Cryptocurrency" *Motherboard* (21 March 2018) <https://motherboard.vice.com/en_us/article/d358zk/canada-is-gearing-up-to-regulate-cryptocurrency-parliament-hearing>; and Financial Transactions and Reports Analysis Centre of Canada "Money services businesses (MSBs)" (29 February 2016) <http://www.fintrac-canafe.gc.ca/msb-esm/intro-eng.asp>.
[811] Financial Transactions and Reports Analysis Centre of Canada "FINTRAC Advisory Regarding Money Services Businesses Dealing in Virtual Currency" (30 July 2014) <http://www.fintrac-canafe.gc.ca/new-neuf/avs/2014-07-30-eng.asp>.
[812] Financial Transactions and Reports Analysis Centre of Canada "Your Money Services Business in Canada: What you Need to Know" (29 February 2016) <http://www.fintrac-canafe.gc.ca/publications/brochure/2012-06/1-eng.asp>.

regulations will apply to any cryptocurrency business that provides services to persons or entities within Canada, whether the business is domestic or international.[813] In addition, banks in Canada are prohibited from providing financial services to any MSB, and therefore any cryptocurrency exchange, that is not registered with FINTRAC.[814]

On 7 February 2018 the Canadian Department of Finance released a consultation document "Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime".[815]

6.5 Estonia

Estonia's treatment of cryptocurrencies was complicated, and in some instances contradictory. In 2014, the central bank of Estonia warned consumers to stay away from cryptocurrencies, stating they could be little more than a "Ponzi scheme".[816] As Mihkel Nommela, head of the Estonian central bank's payment and settlement systems department, noted: "all risks are assumed by the user, who has no one to turn to for help".[817] However, just two months later, the Tax and Customs Board of Estonia declared that cryptocurrencies could be treated as alternative payment means and be subject to CGT and VAT.[818] Bitcoin specifically, however, was not viewed as any type of security or e-currency by Estonian financial regulators or tax authorities.[819]

In contrast, the largest independent bank in Estonia, LHV Pank (LHV), was the first bank in the world to experiment with programmable money.[820] LHV engaged a "virtual currency expert" to help develop products and services for cryptocurrencies.[821] As a result, LHV established a subsidiary, Cuber Technologies, which is focused on Bitcoin-based digital securities.[822] There are two arms to Cuber Technologies: Cuber Securities, which issues bank certificates of deposits recorded in Bitcoin blockchain technology but denominated in euros;[823] and Cuber Wallet, which allows smart phone users to make payments in both cryptocurrencies and fiat currencies digitally.[824] While Cuber and Cuber Wallet are in experimental stages, LHV and its partner in development, Chromaway, are urging regulators to "embrace block chain technology and adapt, rather than run scared from it".[825]

Estonia has also implemented several initiatives that utilise blockchain technology, such as e-residency, which aims to attract foreigners to Estonia by allowing them to run a business, open accounts in Estonian banks and use digital signatures to sign documents.[826] E-residents receive an ID card similar to Estonian residents.[827] The creators of e-residency intend to use blockchain technology

---

[813] Victoria van Eyk "What Canada's New Regulations Mean for Bitcoin Businesses" *CoinDesk* (24 June 2014) <http://www.coindesk.com/canadas-new-regulations-mean-bitcoin-businesses/>.
[814] Ponsford, above n 67, at 43.
[815] Department of Finance (Canada) "Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" (7 February 2018) <https://www.fin.gc.ca/activty/consult/amlatfr-rpcfa-eng.pdf>.
[816] Ott Ummelas and Milda Seputyte "Bitcoin 'Ponzi' Concern Sparks Warning From Estonia Bank" *Bloomberg* (United States, 1 February 2014) <https://www.bloomberg.com/news/articles/2014-01-30/bitcoin-ponzi-scheme-worry-sparks-estonia-central-bank-caution>.
[817] Ibid.
[818] Peter Roudik "Estonia: Rules on Taxation of Bitcoin" (18 April 2014) <http://www.loc.gov/law/foreign-news/article/estonia-rules-on-taxation-of-bitcoin/>; and "How legal is Bitcoin and Crypto Currencies?" *CryptoCompare* (18 November 2016) <https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies/>.
[819] Roudik, ibid and "How legal is Bitcoin and Crypto Currencies?", ibid.
[820] United Kingdom Government Chief Scientific Adviser, above n 15, at 81.
[821] Jonathan Millet "Estonian Bank LHV Brings Aboard Virtual Currency Expert" *NewsBTC* (13 June 2014) <http://www.newsbtc.com/2014/06/13/estonian-bank-lhv-brings-aboard-virtual-currency-expert/>.
[822] United Kingdom Government Chief Scientific Adviser, above n 15, at 81.
[823] Ibid and see "CUBER – LHV Bank started public use of blockchain technology by issuing securities" (8 June 2015) Cuber <http://www.cuber.ee/en_US/news/>.
[824] United Kingdom Government Chief Scientific Adviser, above n 15, at 81; and Cuber, above n 823.
[825] United Kingdom Government Chief Scientific Adviser, above n 15, at 82.
[826] Ilya Lopatin "Blockchain and Bitcoin in Estonia: How the Industry Is Shaping the Country's Future" *Forklog* (7 February 2017) <http://forklog.net/blockchain-and-bitcoin-in-estonia-how-the-industry-is-shaping-the-countrys-future/>.
[827] Ibid.

in the project.[828] Estonia is also planning to use blockchain technology in e-health and e-voting projects.[829] However, despite its eagerness to embrace blockchain technology in some regards, Estonia treats bitcoin and similar cryptocurrencies using blockchain technology quite differently.[830]

6.5.1 Tax treatment

Income generated from cryptocurrencies is subject to CGT and VAT.[831] In 2014, Estonia made a submission[832] to the European Court of Justice to give its opinion on the VAT treatment of bitcoin in the case of *Skatteverket v David Hedqvist,*[833] stating that cryptocurrency transactions should be subject to VAT on their full amount and do not fall under the exemptions in Article 135 of the VAT Directive.[834] Estonia's reasoning was that cryptocurrencies are not recognised as financial instruments, therefore transactions involving cryptocurrencies do not constitute financial services and so are not exempt from VAT or social security contribution requirements.[835] The European Court of Justice ruled that cryptocurrencies should be treated as foreign currencies.[836] As the ruling is issued by a highest-resort court, it should be mandatory for all member states, yet it remains unclear how cryptocurrencies are taxed in Estonia.[837]

6.5.2 Anti-money laundering and counter-terrorism financing

In April 2014 the Estonian Supreme Court found that bitcoin trading is an economic activity and is therefore subject to AML/CFT regulation and public oversight.[838] In *Otto Albert de Voogd*, a Bitcoin entrepreneur who was operating a bitcoin exchange called BTC.ee, was shut down by Estonian law enforcement authorities.[839] The Money Laundering and Terrorist Financing Prevention Act 2007 requires that persons who offer bitcoin exchange services (referred to as "alternative means of payment") must, if the value of transactions by a customer in a month in aggregate exceeds €1,000, identify and verify the identity of the customer on establishment of a business relationship and carrying out a transaction "while being present at the same place as the customer,"[840] and must also identify all parties to individual transactions.[841]

---

[828] Ibid.
[829] Ibid.
[830] Ibid.
[831] Roudik, above n 818.
[832] The untranslated submission can be found at <https://www.scribd.com/document/249854692/Estonia-Submits-Opinion-on-Bitcoin-Tax-at-European-Court-of-Justice?ad_group=&campaign=Skimbit%2C+Ltd.&content=10079&irgwc=1&keyword=ft500noi&medium=affiliate&source=impactradius>.
[833] *Skatteverket v David Hedqvist*, above n 780.
[834] Council Directive 2006/112/EC on the common system of value added tax [2006] OJ L 347; United Kingdom Government "VAT Finance Manual: VATFIN2330", above n 771.
[835] Roudik, above n 818.
[836] "Estonia Seeks Cryptocurrency Clarification" *Forklog* (1 December 2015) <http://forklog.net/estonia-seeks-cryptocurrency-clarification/>.
[837] Ibid.
[838] Administrative Chamber of the Supreme Court Ruling No 3-3-1-75-15 (11 April 2016); Politsei-ja Piirivalveamet "The Supreme Court finds that bitcoin trading is an economic activity" (14 April 2016) <https://www.politsei.ee/en/uudised/uudis.dot?id=558348&order=date2+desc&currentPage=1&searchquery=bitcoin>; and Gautham "Bad News for Otto De Voogd as Supreme Court Regulates Bitcoin in Estonia" *NEWSBTC* (11 April 2016) <http://www.newsbtc.com/2016/04/11/otto-de-voogd-bitcoin-estonia-case/>.
[839] Gautham, ibid.
[840] Money Laundering and Terrorist Financing Prevention Act 2007 § 15(8)(2).
[841] Ibid.

The judgment was respected by the Estonian Cryptocurrency Association, but it disagreed with applying existing AML/CFT, with board member Asse Sauga stating, after recognising the need for AML/CFT regulation:[842]

> Today, we are of the opinion that the general money-laundering regulation in force in Estonia is clearly contrary to innovation and new technologies, and it must be reviewed and updated. We sincerely hope that this will be dealt with as priority.

Estonia is making progress towards change, with its first major bitcoin and blockchain conference being held in Tallinn in March 2017.[843]

Now the position for cryptocurrency exchanges is clear in Estonia under the Money Laundering and Terrorist Financing Prevention Act 2007. Operating a cryptocurrency exchange requires an operating licence issued by the Estonian Financial Intelligence Unit, as does being a cryptocurrency wallet provider.[844]

6.6 Japan

Japan is attempting to position itself as the leading cryptocurrency and blockchain jurisdiction.[845] On April 2017 bitcoin and other cryptocurrencies were recognised as legal methods of payment,[846] albeit causing issues for how to account for them.[847] On 1 July 2017 Japan's consumption tax was revised and bitcoin and other cryptocurrency transactions had the formerly levied eight per cent consumption tax removed.[848]

6.6.1 Tax treatment

Japan treats the taxation of cryptocurrencies interestingly as it treats it as miscellaneous income, and not the same as income made from stocks or foreign currencies.[849] The tax payable depends on taxpayer's income and ranges from 15 to 55 per cent.[850] If the taxpayer received no income and the profits on cryptocurrency were less than ¥200,000 (about USD 1,857), no tax is payable.[851]

6.6.2 Anti-money laundering and counter-terrorism financing

Japan amended its Payment Services Act, with effect from 1 April 2017, so that cryptocurrency exchanges required registration with the Financial Services Agency as a virtual currency exchange service provider.[852] At the end of March 2018, 16 applicants were registered with a further 16 still

---

[842] Aivar Pau "Supreme Court Subjects Bitcoins Trade to Money Laundering Rules" *Postimees* (Estonia, 12 April 2016) <http://news.postimees.ee/3652435/supreme-court-subjects-bitcoins-trade-to-money-laundering-rules>.
[843] Lopatin, above n 826.
[844] Money Laundering and Terrorist Financing Prevention Act § 70. See also KRM Advisor "Starting a cryptocurrency company in Estonia" <https://www.estoniancompanyregistration.com/cryptocurrency-company/>.
[845] Kai Sedgwick "Japan Teaches Western Governments a Lesson in Cryptocurrency Regulation" *Bitcoin.com* (13 November 2017) <https://news.bitcoin.com/japan-teaches-western-governments-lesson-cryptocurrency-regulation/>.
[846] Garrett Keirns "Japan's Bitcoin Law Goes Into Effect Tomorrow" *Coindesk* (31 March 2017) <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/>.
[847] "Virtual Money Poses Accounting Dilemma for Japan's Early Adopters" *Nikkei Asian Review* (29 March 2018) <https://asia.nikkei.com/Business/Trends/Virtual-money-poses-accounting-dilemma-for-Japan-s-early-adopters>.
[848] Kevin Helms "Revised Tax in Effect From Today In Japan, Giving Residents 'Access to Global Markets'" *Bitcoin.com* (1 July 2017) <https://news.bitcoin.com/revised-tax-on-bitcoin-in-japan-in-effect-from-today-giving-residents-access-to-global-markets/>.
[849] Yuko Takeo and Maiko Takahashi "Crypto Investors Face Tax of Up to 55% in Japan" *Bloomberg Technology* (United States, 9 February 2018) <https://www.bloomberg.com/news/articles/2018-02-08/crypto-investors-in-japan-face-tax-of-up-to-55-on-their-takings>.
[850] "Japan And Tax On Cryptocurrency – Part 1" Tyton <https://www.tytoncapital.com/investment-advice-japan/japan-and-tax-on-cryptocurrency-bitcoin/>.
[851] Ibid.
[852] Financial Services Agency "Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider" <https://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf>.

being examined.[853] Fortunately, the Financial Services Agency has provided requirements that must be met in English.[854] The requirements are not as complicated as New York's BitLicense,[855] and the applicant must meet three requirements to gain registration. It must:

(a) Be a Japanese joint-stock company (Kabushiki Kaisha), unless the applicant is categorised as a Foreign Virtual Currency Exchange Service Provider. To be a Foreign Virtual Currency Exchange Service Provider the provider must engage in virtual currency exchange services in its home jurisdiction that has an appropriate registration status that is equivalent to that in the Payment Services Act, it must have a local office in Japan and the representative of the local office must have Japanese residency.
(b) Have a minimum capital of ¥10 million (around USD 93,000) and positive net assets.
(c) Have systems that comply with the Payment Services Act.

Complying with the Payment Services Act includes:[856] segregating customers' money from its own by putting it into a separate bank account or a trust; segregating virtual currencies from its own so that its customers' virtual currency is identifiable immediately; providing the account balance daily and correcting any mistakes within five working days; auditing the segregation of money and virtual currencies at least once a year; the exchange notifying the customer that their virtual currencies are not considered Japanese currency or foreign currency and that there is a risk of loss due to price fluctuations. The exchange must follow KYC procedures in accordance with the Law for Prevention of Transfer of Criminal Proceeds Act 2007.

Importantly the Financial Services Agency is policing the law, and in March 2018 ordered two exchanges to suspend operations for a month as well as issuing business improvement orders to five other exchanges.[857] The Japanese regulations and the Financial Services Agency's proactive work in the area have been met with approval.[858] As the *Financial Times* has observed, "entrepreneurs do not often welcome regulation. For Japanese cryptocurrency start-ups, however, a framework put in place by the country's financial authorities has been a boon".[859]

Interestingly, the regulations appear to be working as Japanese cryptocurrency exchanges reported 669 cases of suspected money laundering between April and December 2017.[860] (This is a drop in the bucket compared to the 400,043 cases reported by Japanese financial institutions in 2017.) [861]

---

[853] "More Japanese cryptocurrency exchanges to close" *Nikkei* (29 March 2018) <https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close>; see also Financial Services Agency "Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider", above n 852.

[854] See Financial Services Agency "Grounds for Refusing Registration, and Relevant Statutes and Regulations Pertaining to Viewpoints in Registration-Screening" <https://www.fsa.go.jp/en/news/2017/20170930-1/01.pdf> and Financial Services Agency "Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider", above n 852.

[855] See Section 7.2.6 New York below.

[856] See Masahiko Ishida, Edward Mears and Ryutaro Takeda "Japan Regulatory Update on Virtual Currency Business" (29 December 2017) DLA Piper <https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/> and Naoya Ariyoshi, Susumu Tanizawa and Hideki Katagiri "Japan: The Essential Points Of The Amendments To The Regulation On Virtual Currency Exchange Services" *Mondaq* (21 January 2017) <http://www.mondaq.com/x/554128/Financial+Services/The+Essential+Points+Of+The+Amendments+To+The+Regulation+On+Virtual+Currency+Exchange+Services>.

[857]Jake Adelstein "Japan Shuts Down Two Cryptocurrency Exchanges But It May Be Good News For The Industry" *Forbes* (United States, 8 March 2018) <https://www.forbes.com/sites/adelsteinjake/2018/03/08/japan-shuts-down-two-cryptocurrency-exchanges-but-it-may-be-good-news-for-the-industry/#2da9e360359d>.

[858] Koji Higashi "I was so Wrong about the Cryptocurrency Regulation in Japan" (27 November 2017) Medium <https://medium.com/@coin_and_peace/i-was-so-wrong-about-the-cryptocurrency-regulation-in-japan-66ab17671095> and Jake Adelstein, ibid.

[859] Emiko Terazono "Bitcoin gets Official Blessing in Japan" *Financial Times* (UK, online ed, 18 October 2017) <https://www.ft.com/content/b8360e86-aceb-11e7-aab9-abaa44b1e130>.

[860] "NPA Cryptocurrency Tips Point to 669 Suspected Money-laundering Cases from April to December" *Japan Times* (online ed, 22 February 2018) <https://www.japantimes.co.jp/news/2018/02/22/business/npa-cryptocurrency-tips-point-669-suspected-money-laundering-cases-april-december/#.WwXi9CC-mUk>.

[861] Ibid.

7. United States

The position in the US is complicated. The US dollar is the only legal tender,[862] albeit the US Treasury treats cryptocurrencies as money for the purposes of AML/CFT and as property for federal tax purposes.[863] In August 2013 a US District Court held that bitcoin is a "form of money" for the purposes of the Securities Act 1993.[864] In addition, some states have issued their own cryptocurrency regulations, including New York,[865] California,[866] Connecticut,[867] New Hampshire,[868] Wyoming[869] and in the case of Texas, guidance.[870] Overall, the US has focused on fitting cryptocurrencies into existing regulations instead of formulating new cryptocurrency-specific regulation.

7.1 Tax treatment

In May 2013 the US Government Accountability Office recommended the Internal Revenue Service (IRS) issue informal guidance on the taxation of cryptocurrency transactions.[871] Formal guidance was issued in March 2014.[872] For federal tax purposes, convertible cryptocurrencies are treated as property and subject to the same taxation rules that apply to other property.[873] Convertible cryptocurrencies are those that have an equivalent value in real currency, or which can act as a substitute for real currency, such as bitcoin.[874] The existing tax principles do not apply to cryptocurrencies that are not convertible, although the Treasury Department and the IRS recognise that cryptocurrencies that are not convertible should be addressed in future guidance and have sought comments from the public in this regard.[875] Where "cryptocurrency" is referred to in the federal tax implications below it means convertible cryptocurrencies.

The implications of applying existing federal tax rules to convertible cryptocurrencies include:

- For federal tax purposes, cryptocurrencies are not currencies that can generate foreign currency gains or losses.[876]
- If a taxpayer receives cryptocurrency as payment for goods or services, they must include the fair market value of the cryptocurrency in US dollars at the date the cryptocurrency was received in their

---

[862] 31 USC § 5103.
[863] Russ Marshall "Bitcoin: Where Two Worlds Collide" (2015) 27 Bond Law Review 89 at 101.
[864] *Securities and Exchange Commission v Shavers* (Case no 4:13 – CV 416, Eastern District of Texas).
[865] 23 NYCRR Part 200 (New York's Virtual Currency Regulation) <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.
[866] 2014 CA Assembly Bill AB-129 <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB129>.
[867] Edward V Murphy, M Maureen Murphy and Michael V Seitzinger *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (Congressional Research Service, 13 October 2013) <https://fas.org/sgp/crs/misc/R43339.pdf>.
[868] NH HB436 Regular session 2017 <http://gencourt.state.nh.us/bill_status/billText.aspx?sy=2017&id=638&txtFormat=html>.
[869] See Section 7.2.4 Wyoming below.
[870] Texas Department of Banking "Supervisory Memorandum – 1037" (3 April 2014) <http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf>.
[871] Howard Wiener, Jonathan Zelnik, Israel Tarshish and Michael Rodgers "Chomping at the Bit: U.S Federal Income Taxation of Bitcoin Transactions" (2014) 73(4) Tax Notes International 352 <https://kpmg-us-inst.adobecqms.net/content/dam/kpmg/taxwatch/pdf/2014/012714-bitcoin-transactions.pdf> at 358; and United States Government Accountability Office *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks* (May 2013) <http://www.gao.gov/assets/660/654620.pdf>.
[872] Internal Revenue Service "IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply" (25 March 2014) <https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance>.
[873] Ibid.
[874] Internal Revenue Service "Notice 2014-21" (25 March 2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> at section 2.
[875] At section 3.
[876] At section 4.

gross income calculations.[877] If the fair market value of property exchanged for cryptocurrency exceeds the fair market value of the cryptocurrency at the time it is received the taxpayer has a taxable gain. Conversely, if the fair market value of the property is less than the fair market value of the cryptocurrency received, the taxpayer has a loss, which may be deductible.[878] Whether a gain or loss is capital gain or loss or an ordinary gain or loss depends on whether the cryptocurrency is a capital asset (such as stocks, bonds or investment property) or not (for example, if cryptocurrency is held as inventory) in the hands of the taxpayer and is taxed accordingly.[879]

- Taxpayers who mine cryptocurrencies, such as bitcoin miners, must include the fair value of the cryptocurrency in US dollars in their gross income as at the date the cryptocurrency was received.[880]
- Cryptocurrency received by an independent contractor for services performed constitutes self-employment income and is subject to self-employment tax on the fair value of the cryptocurrency in US dollars at the date it is received.[881]
- Cryptocurrency paid to an employee by an employer as remuneration constitutes wages and is subject to federal income tax withholding on the fair value of the cryptocurrency in US dollars at the date of payment.[882]
- Payments made in cryptocurrencies to a US non-exempt recipient where the fair value of the cryptocurrency is $600 or more are subject to the same information reporting requirements as any other payment made in property. Such payments could include rent, wages or annuities.[883]
- In general, a person who makes a payment in cryptocurrency to an independent contractor for services performed where the fair value of the cryptocurrency is $600 or more in a taxable year is required to file an information return with the IRS.[884]
- Payments made using cryptocurrency are subject to backup withholding to the same extent as other payments made in property.[885]
- In general, a third party who contracts to settle payments on behalf of unrelated merchants and their customers (a third-party settlement organisation) must include payments made in cryptocurrencies at their fair value in US dollars at the date of payment in aggregation with payments made in real currencies when determining the total amount they are required to report to the IRS.[886]

7.2 Anti-money laundering and counter-terrorism financing

In March 2013 the Financial Crimes Enforcement Network (FinCEN) issued guidance to clarify the application of the Bank Secrecy Act to all users of cryptocurrencies.[887] While users of convertible cryptocurrencies who use the cryptocurrency to purchase goods or services are not MSBs and are not subject to MSB registration, administrators or exchange operators are subject to MSB registration.[888] Exchange operators are those "persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies".[889] Cryptocurrency administrators are those who engage in businesses which issue, or put into circulation, and have the authority to redeem, or withdraw from circulation, cryptocurrencies.[890]

---

[877] Ibid.
[878] Ibid 4.
[879] Ibid 4.
[880] Ibid 4.
[881] Ibid 4.
[882] Ibid.
[883] Ibid.
[884] Ibid.
[885] Ibid.
[886] Ibid.
[887] Department of the Treasury Financial Crimes Enforcement Network "FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>. FinCEN regulations refer to "virtual currency" or "e-currency" but "cryptocurrency" is used in this report instead for consistency.
[888] At 1.
[889] Ibid.
[890] Ibid.

FinCEN reviewed various activities involving cryptocurrencies and made recommendations on how administrators and exchangers should be regulated in three scenarios: brokers and dealers of e-currencies and e-precious metals; centralised convertible cryptocurrencies; and decentralised convertible cryptocurrencies.[891] Recommended regulatory treatment under each of the three scenarios is outlined below.

Brokers or dealers of e-currencies and e-precious metals typically distribute digital certificates of ownership of e-currencies and e-precious metals electronically, with the certificate of ownership being the currency.[892] Depending on the business model, a broker or dealer could be either an administrator or an exchanger if they engage in money transmission (which is where they exchange money between a customer and third party not part of the e-currency or e-precious metals transaction).[893] The treatment of money transmitters does not vary based on whether the currency is real or a cryptocurrency, so the normal rules applicable to money transmitters apply to brokers or dealers of e-currencies and e-precious metals.[894] However, if the broker or dealer accepts and transmits funds solely for the purchase or sale of real currency or commodities for a customer they are not acting as a money transmitter under the regulations.[895]

Centralised convertible cryptocurrencies are those which have a centralised repository, such as Perfect Money or Liberty Reserve (which was shut down by the US Government for money laundering).[896] Administrators of centralised repositories are money transmitters insofar as they allow transfer of value from one location to another or between persons, whether the value is denominated in real currency or convertible cryptocurrency.[897] Exchangers that (or who) access the convertible cryptocurrency services provided by administrators to accept or transmit the convertible cryptocurrency as intermediaries are also money transmitters.[898]

FinCEN recognises that exchanger activity may take two forms. First, where the exchanger acts as a seller of the convertible cryptocurrency, accepting real currency or equivalent from a purchaser, and transfers the value of that real currency to the purchaser's convertible cryptocurrency account with an administrator. Sending "value that substitutes for currency" to another location or person may constitute money transmission under FinCEN regulations.[899]

Second, where the exchanger privately credits a user with an amount of the exchanger's own convertible cryptocurrency held by the administrator of the repository in return for fiat currency or equivalent. The exchanger then transfers internally credited value to third parties at the user's direction. This activity is a non-transparent de facto sale of cryptocurrency and constitutes transmission to another person (the third party to which transmissions are made), thus further constituting money transmission on the part of the exchanger.[900]

Decentralised convertible cryptocurrencies are those which have no central repository and no single administrator and which can be obtained by persons through their own effort (such as through

---

[891] At 3.
[892] Ibid.
[893] Ibid.
[894] At 4.
[895] See generally Department of the Treasury Financial Crimes Enforcement Network "FIN-2008-G008: Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities" (10 September 2008) <https://www.fincen.gov/sites/default/files/guidance/fin-2008-g008.pdf>.
[896] "New York's Final 'BitLicense' Rule: Overview and Changes from July 2014 Proposal" (5 June 2015) <https://www.davispolk.com/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf> at 10.
[897] Department of the Treasury Financial Crimes Enforcement Network "FIN-2013-G001", above n 887, at 4.
[898] Ibid.
[899] 31 CFR § 1010.100(ff)(5)(i)(A).
[900] Department of the Treasury Financial Crimes Enforcement Network "FIN-2013-G001", above n 887, at 5.

computing or manufacturing),[901] for example, bitcoin, Litecoin and other altcoins based on the Bitcoin protocol.[902] A person who creates their own convertible cryptocurrency and uses it to purchase goods or services is not a money transmitter and therefore not subject to FinCEN regulation.[903] However, a person who creates their own convertible cryptocurrency and sells it to another person for real currency or equivalent is a money transmitter because they are transferring the cryptocurrency from one location to another.[904] In addition, if a person accepts decentralised convertible cryptocurrency from one person and transmits it to another person as part of acceptance and transfer or currency, funds or other value that substitutes for currency, they are an exchanger and a money transmitter.[905]

Cryptocurrency miners who use their mined cryptocurrency to purchase goods and services are not subject to FinCEN regulation, but miners who sell their mined cryptocurrency for fiat currency or equivalent are classed as money transmitters and are subject to FinCEN regulation.[906] The FinCEN regulation imposes registration, reporting and record-keeping requirements on MSBs in general under the Bank Secrecy Act and the relevant users of cryptocurrencies must comply as well.[907]

7.2 State regulation of cryptocurrencies

A number of US states have taken steps to introduce regulatory frameworks for cryptocurrencies, most notably California, Connecticut and New York,[908] and more recently Wyoming. Texas and New Hampshire have also been active. This section examines activities in these jurisdictions. Of all the states, New York has the most comprehensive regulation of cryptocurrencies, and for the sake of completeness the requirements of New York's regulation are gone through in some detail. However, the stringent demands of New York's regulation appear to have had the effect of stifling cryptocurrency use rather than fostering it.[909] For example, New York's BitLicense has been in operation since 2015 and at May 2018 only four companies had managed to obtain a licence.[910] In contrast, Japan,[911] which had brought in its regulation less than one year ago, had already granted 16 licences.[912]

7.2.1 California

In 2014 California signed Assembly Bill No. 129 into law, repealing section 107 of its Corporations Code,[913] which limited companies from putting into circulation "the lawful money of the United States" only,[914] opening the door for cryptocurrencies to be used for purchasing goods and services

[901] Ibid.
[902] "New York's Final 'BitLicense' Rule: Overview and Changes from July 2014 Proposal**",** above n 896, at 10.
[903] Department of the Treasury Financial Crimes Enforcement Network "FIN-2013-G001", above n 887, at 5.
[904] Ibid.
[905] Ibid.
[906] Marshall, above n 863, at 101.
[907] Department of the Treasury Financial Crimes Enforcement Network "Money Laundering Prevention: A Money Services Business Guide" <https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf>.
[908] Murphy, Murphy and Seitzinger, above n 867, at 14.
[909] "New York's Bitcoin Hub Dreams Fade with Licensing Backlog" *CNBC* (United States, 31 October 2016) <http://www.cnbc.com/2016/10/31/new-york-bitcoin-hub-dreams-fade-with-licensing-backlog.html>; and see Stan Higgins "New York Lawmakers Open to Revisiting the BitLicense" *Coindesk* (23 February 2018) <https://www.coindesk.com/bitcoin-crypto-ny-lawmaker-pledges-make-bitlicense-something-works/>.
[910] Jen Wieczner "Inside New York's BitLicense Bottleneck: An 'Absolute Failure'" *Fortune* (United States, 25 May 2018) <http://fortune.com/2018/05/25/bitcoin-cryptocurrency-new-york-bitlicense/>.
[911] See Section 6.6 Japan above.
[912] Wieczner, above n 910.
[913] CA Corp Code § 107 (through 2013 Leg Sess).
[914] 2014 CA Assembly Bill AB-129 <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB129>.

legally.[915] The California Department of Business Oversight (CDBO) has considered the regulation of cryptocurrency businesses.[916] In April 2014 the CDBO issued an advisory explaining cryptocurrencies and warning consumers about the risks involved in exchanging or investing in cryptocurrencies, urging consumers to assess the risks thoroughly before investing.[917] In January 2015 the CDBO Commissioner, Jan Lyn Owen, issued a press release confirming the state's position on cryptocurrency regulation after Coinbase Exchange, a platform for bitcoin trading, reported erroneously that it had been granted regulatory approval by the State of California.[918] The press release stated the CDBO "has not decided whether to regulate virtual currency transactions, or the businesses that arrange such transactions, under the state's Money Transmission Act".[919] It further warned consumers that Coinbase Exchange was not regulated or licensed by the State.[920]

Given much criticism of BitLicense, it appears changes will be made to it, with a Bill likely to be introduced "very soon" as of October 2016.[921] In February 2018 a Bill was submitted to establish a sandbox.[922]

7.2.2 Connecticut

On 19 June 2015 Connecticut amended the Connecticut Money Transmission Act (CMTA), requiring all virtual currency businesses to be licensed to operate in Connecticut.[923] The amendments subject virtual currency businesses to requirements imposed on MSBs and include additional standards imposed on cryptocurrency businesses.[924] A virtual currency business is defined as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology".[925] Cryptocurrency that cannot be converted into fiat currency used exclusively as part of consumer rewards programmes and cryptocurrency used solely for online gaming are not covered by the definition.[926] The amendments specifically imposed on cryptocurrency businesses[927] are:

(a) In applications for initial or renewal or current licenses under sections 36a-595 to 36a-612 of the CMTA, money transmission businesses must state whether the type of business they conduct will include the transmission of cryptocurrencies;[928]

---

[915] John Weru Maina "AB 129 – California Legally Approves the Use of Bitcoin" *CCN* (5 January 2015) <https://www.cryptocoinsnews.com/ab-129-california-legally-approves-use-bitcoin/>.
[916] Murphy, Murphy and Seitzinger, above n 867, at 16.
[917] California Department of Business Oversight "What You Should Know About Virtual Currencies" (April 2014) <http://www.dbo.ca.gov/Consumers/Advisories/Virtual_Currencies_0414.pdf>.
[918] John Southurst "Coinbase Secures Approval to Launch Regulated US Bitcoin Exchange" *Coindesk* (25 January 2015) <http://www.coindesk.com/coinbase-secures-approval-launch-regulated-us-bitcoin-exchange/>; and California Department of Business Oversight "DBO Commissioner Owen Clarifies Coinbase Exchange's Regulatory Status in California" (Press release, 27 January 2015) <http://www.dbo.ca.gov/Press/press_releases/2015/Statement_on_Coinbase_Exchange_Regulatory_Status_01-27-15.pdf>.
[919] California Department of Business Oversight, above n 917.
[920] Ibid.
[921] Higgins "New York Lawmakers Open to Revisiting the BitLicense", above n 909.
[922] Assembly Bill A9899A "AN ACT to amend the financial services law, in relation to creating a regulatory sandbox program; to amend the banking law, in relation to safeguarding financial technology products and services and prohibiting licensing fees for such products and services; and providing for the repeal of such provisions upon expiration thereof", sponsored by Ron Kim.
[923] Murphy, Murphy and Seitzinger, above n 867, at 16; and Connecticut House Act (2015 Regular Session – HB 6800) <https://www.cga.ct.gov/2015/act/pa/2015PA-00053-R00HB-06800-PA.htm>.
[924] Murphy, Murphy and Seitzinger, above n 867, at 16.
[925] Conn Gen Stat § 36a-596(14).
[926] Murphy, Murphy and Seitzinger, above n 867, at 16–17.
[927] The legislation refers to "virtual currency businesses"; however, "cryptocurrency businesses" will be used for consistency.
[928] Conn Gen Stat § 36a-598(6)(a).

(b) The Commissioner may, at their discretion, deny a license to a money transmission business that may engage in transmission of monetary value in the form of cryptocurrencies if the Commissioner considers the applicant's business model may present undue risk of financial loss to consumers;[929]
(c) The Commissioner may, at their discretion, impose additional requirements or restrictions on the license of cryptocurrency businesses, including the amount of surety bond required by section 36a-602;[930]
(d) The surety bond required to be held by cryptocurrency businesses shall be calculated by the Commissioner reasonably, in order to address the current and prospective volatility of cryptocurrency markets.[931] For applicants that do not engage in the transmission of monetary value in the form of cryptocurrencies, surety bonds are set at specific amounts, dependent on the average weekly amount of transactions the applicant business deals with.[932]

7.2.3 New Hampshire

On 1 January 2016 New Hampshire's Licensing of Money Transmitters statute was amended to include cryptocurrency businesses.[933] "Convertible virtual currency" was added to the definition of "Monetary value"[934] and is defined as:[935]

> a digital representation of value that:
> (a) Can be a medium of exchange, a unit of account, and/or a store of value;
> (b) Has an equivalent value in real currency or acts as a substitute for real currency;
> (c) May be centralized or decentralized; and
> (d) Can be exchanged for currency or other convertible virtual currency.

The addition of convertible virtual currency into the Licensing of Money Transmitters statute means that cryptocurrency businesses that are money transmitters are subject to the same rules as other money transmitters; however, no provisions specific to cryptocurrency businesses are found in the statute.

In January 2015 a Bill[936] was introduced proposing to allow New Hampshire residents to pay taxes in bitcoin;[937] however, a subcommittee recommended it be voted "inexpedient to legislate" due to concerns about the exchange rate risks involved with the volatile cryptocurrency market.[938] While the Bill was defeated, state representative Eric Schleien stated that he would work with the legislators who voted for the Bill and introduce a similar one in the future.[939]

In June 2016 a commission to study whether cryptocurrency regulation was necessary in New Hampshire was established.[940] On 12 January 2017 House Bill 436 was filed.[941] It proposed to exempt businesses that use cryptocurrencies from registering as money transmitters, even those businesses

---

[929] Conn Gen Stat § 36a-600(7)(c).
[930] Conn Gen Stat § 36a-600(7)(d).
[931] Conn Gen Stat § 36a-602(8)(a).
[932] Conn Gen Stat § 36a-602(8)(a).
[933] Luke Parker "New Hampshire Money Transmitter Rule Change will Include Bitcoin Businesses" (8 December 2015) Brave New Coin <http://bravenewcoin.com/news/new-hampshire-money-transmitter-rule-change-will-include-bitcoin-businesses/>.
[934] NH Rev Stat § 399-G:1(XV) (2015).
[935] Ibid.
[936] NH HB552-FN Regular session 2015 <http://gencourt.state.nh.us/bill_status/billText.aspx?id=62&txtFormat=html&sy=2016>.
[937] Stan Higgins "New Hampshire Legislators Kill Bitcoin Tax Bill" *Coindesk* (21 January 2016) <http://www.coindesk.com/new-hampshire-legislators-vote-down-bitcoin-tax-bill/>.
[938] Ibid.
[939] Ibid.
[940] NH HB552-FN Regular session 2015 <http://www.gencourt.state.nh.us/rsa/html/xxxvi/399-g/399-g-mrg.htm>.
[941] NH HB436 Regular session 2017 <http://gencourt.state.nh.us/bill_status/billText.aspx?sy=2017&id=638&txtFormat=html>.

that maintain control of virtual currency on behalf of others[942] and which conduct business "using transactions conducted in whole or in part in virtual currency".[943] The Bill was passed on 7 June and came into effect on 1 August 2017.[944]

7.2.4 Wyoming

In March 2018 five Bills dealing with cryptocurrencies and blockchain, either directly or by laying the groundwork for their use, were passed in an attempt to lure blockchain businesses to Wyoming, or at least be registered there. This approach is similar to Delaware's successful move to convince people to register their corporations in Delaware, as most corporations registered in that state are not located there.[945] It has been argued that Wyoming's move paid dividends even before the Governor of Wyoming had signed off four of the five Bills: "a US version of Switzerland's 'Crypto Valley' will hopefully soon spring up in Wyoming, if early indications of interest pan out. Dozens of small software companies have already formed Wyoming entities and some of these have already leased office space – 20,000 square feet and counting".[946]

The term "virtual currency" is used rather than cryptocurrency. Virtual currency is defined as meaning "any type of digital representation of value that:

(a) Is used as a medium of exchange, unit of account or store of value; and
(b) Is not recognised as legal tender by the United States government".[947]

The five Acts are:[948]

- HB 19[949] exempts virtual currency used within Wyoming from money transmitter laws and regulations, subject to providing "specified verification authority" to the Wyoming Secretary of State and the Wyoming Banking Commissioner. Specified verification authority entails representations and undertakings of the issuer of utility tokens to confirm beneficial ownership of virtual currency, as well as steps taken to prevent fraudulent duplication of those virtual currencies by unaffiliated third parties. Wyoming companies and trusts are able to conduct commerce with other Wyoming companies and trusts without being subject to money transmitter laws.
- HB 70[950] provides that a person who develops, sells or facilitates the exchange of an open blockchain token (a utility token) is not subject to specified securities and money transmission laws, subject to providing "specified verification authority" to the Wyoming Secretary of State and the Wyoming Banking Commissioner. Utility tokens issued for non-investment purposes will generally be exempt from registration requirements under Wyoming's securities laws.

---

[942] Ibid.
[943] Ibid.
[944] Sterlin Lujan "New Hampshire's Bill to Deregulate Bitcoin Effective Next Week" *Bitcoin.com* (25 July 2017) https://news.bitcoin.com/new-hampshires-pro-bitcoin-bill-effective-next-week/.
[945] Tyler Lindholm and Caitlin Long "A Haven for Blockchain: The Case for Wyoming" *Coindesk* (27 January 2018) <https://www.coindesk.com/haven-blockchain-case-wyoming/>.
[946] Caitlin Long "Wyoming's Blockchain Bills: A Very Personal Labor of Love" (9 March 2018) <https://caitlin-long.com/2018/03/09/wyomings-blockchain-bills-a-very-personal-labor-of-love/>.
[947] Bill HB19 "AN ACT relating to trade and commerce; amending the Wyoming Money Transmitter Act to provide an exemption for virtual currency; and providing for an effective date."
[948] Robert V Cornish Jr "Wyoming Enacts Trailblazing Blockchain and Cryptocurrency Legislation" Wilson Elser (12 March 2018) <https://www.wilsonelser.com/news_and_insights/insights/3090-wyoming_enacts_trailblazing_blockchain_and>.
[949] HB 19 Wyoming Money Transmitter Act-virtual currency exemption, "AN ACT relating to trade and commerce; amending the Wyoming Money Transmitter Act to provide an exemption for virtual currency; and providing for an effective date."
[950] HB 70 Open blockchain tokens-exemptions. "AN ACT relating to securities; providing that a person who develops, sells or facilitates the exchange of an open blockchain token is not subject to specified securities and money transmission laws; providing specified verification authority to the secretary of state and banking commissioner; making conforming amendments; and providing for an effective date."

- SF 111[951] provides that virtual currency is not subject to taxation as "property" in Wyoming. (In addition, Wyoming does not impose income tax on its residents.)
- HB 101[952] provides for the maintenance of corporate records of Wyoming entities via blockchain so long as electronic keys, network signatures and digital receipts are used. Lists of shareholders, nominee shareholders and attendant voting matters are intended to be encompassed through this legislation, thus paving the way for the development of transfer agencies and exchanges within Wyoming.
- HB 126[953] modifies Wyoming's corporate code to permit the formation of series limited liabilities companies (LLCs). Series LLCs often are used by hedge funds and private equity funds to create insulated "cells" within a corporate structure to limit liabilities of the parent LLC. This corporate structure is used frequently in the blockchain space as well. The aim is to promote Wyoming as a jurisdiction of choice for securities formation and to compete with Delaware and Nevada for corporate registration revenue.

7.2.5 Texas

On 3 April 2013 the Texas Department of Banking (TDB) issued Supervisory Memorandum 1037, Regulatory Treatment of Virtual Currencies under the Texas Money Services Act, which expressed the TDB's interpretation of the Texas Money Services Act[954] in relation to cryptocurrencies.[955] The Memorandum did not introduce new regulatory treatment of cryptocurrencies, but instead sought to establish treatment of cryptocurrencies under existing regulations.[956] The Memorandum only concerns licensing issues for decentralised cryptocurrencies and does not offer guidance on centralised cryptocurrencies because "factors distinguishing the various centralized virtual currencies are usually complicated and nuanced" and should be individually analysed by the TDB.[957]

The TDB in its analysis, determined that exchanging cryptocurrency for fiat currency is not a currency exchange under the Texas Finance Code[958] because the Code defines currency as being "the coin and paper money of the US or any country that is designated as legal tender and circulates and is customarily used and accepted as a medium of exchange in the country of issuance",[959] and cryptocurrencies do not meet this definition. Thus, businesses that exchange cryptocurrency for fiat currency in Texas are not required to have a currency exchange licence.[960] Cryptocurrencies are not considered money or monetary value under the Money Services Act because "'money' or 'monetary value' means currency or a claim that can be converted into currency through a financial institution, electronic payments network, or other formal or informal payment system".[961] Cryptocurrency is not

[951] SF 111 Property taxation-digital currencies "AN ACT relating to property taxation; exempting virtual currencies from property taxation; and providing for an effective date."
[952] HB 101 Electronic corporate records "AN ACT relating to the Wyoming Business Corporations Act; authorizing corporations to use electronic networks or databases for the creation or maintenance of corporate records; authorizing the use of a data address to identify a corporation's shareholder; authorizing corporations to accept shareholder votes if signed by a network signature that corresponds to a data address; specifying requirements for use of electronic networks or databases; requiring the secretary of state to review its rules for consistency with this act; and providing for an effective date."
[953] HB 126, Limited liability companies-series "AN ACT relating to limited liability companies; authorizing limited liability companies to establish series of members, managers, transferable interests or assets as specified; specifying powers; providing for limitations on liabilities; providing for management, termination and dissolution; authorizing distributions to members; imposing a requirement on foreign limited liability companies that establish series; requiring rulemaking; and providing for effective dates."
[954] Texas Finance Code Ch 151 (2005).
[955] Texas Department of Banking "Supervisory Memorandum – 1037", above n 870.
[956] At 3.
[957] At 2.
[958] Texas Finance Code Ch 151 § 155.501 (2005).
[959] At §151.501(b)(1) (2005).
[960] Texas Department of Banking "Supervisory Memorandum – 1037", above n 870, at 2.
[961] Texas Finance Code Ch 151 §151.301(b)(3).

currency as stated above, nor is it a claim that must be honoured, therefore the Money Services Act does not apply.[962]

Because cryptocurrency is not considered currency or money, transactions where only cryptocurrencies are involved do not constitute money transmission in Texas.[963] The TDB, however, recognised that where fiat currency is involved, money transmission may occur, and provided guidance on some common cryptocurrency transactions accordingly:[964]

(1) Exchange of cryptocurrency for fiat currency or vice versa is essentially a sale of goods and is not money transmission.
(2) Exchange of one cryptocurrency for another is not money transmission.
(3) Transfer of cryptocurrency alone is not money transmission because even if there is a promise to make it available at a later date, it is not considered money or monetary value. This means that intermediaries and entities who hold cryptocurrency on behalf of others are not money transmitters in that regard.
(4) Cryptocurrency exchangers that exchange cryptocurrency for fiat currency are generally money transmitters because they receive one party's fiat currency in exchange for a promise to make it available to the other party.
(5) Cryptocurrency ATMs where fiat currency is exchanged for cryptocurrency, are usually money transmitters because they act as an intermediary between a buyer and seller (the cryptocurrency bought is generally connected to an established exchange site). However, if there is not a third party involved and the machine only acts as a seller for its operator, not an intermediary, there is no money transmission.

Cryptocurrency businesses that act as money transmitters must comply with the applicable licensing provisions of Finance Code Chapter 151 and of Title 7, Texas Administrative Code, Chapter 33.[965] The TDB highlighted several issues that should be considered in complying with the licensing provisions:[966]

(1) Because a cryptocurrency business that is a money transmitter conducts business on the internet it must comply with the minimum net worth of $500,000,[967] which can be increased to $1,000,000 if necessary.[968]
(2) Cryptocurrency assets cannot be included in calculations for permissible investments allowed under the Texas Finance Code.[969]
(3) Money transmitters that handle cryptocurrencies must demonstrate that cryptocurrency held by them is secure by submitting a third party security audit of their computer systems.[970]

More recently, with the rise of ICOs, the Texas Securities Commissioner has taken the view that certain tokens are securities and requires them to be registered under the Texas Securities Act and State Securities Board Rules and Regulations, and also for companies and exchanges selling them to be registered to sell securities in Texas.[971] Texas has embraced cryptocurrencies and as part of that has been active in attempting to shut down cryptocurrency exchanges, cryptocurrency "banks" and others that have harmed, or have the potential to harm, consumers.[972] For example, the state took

---

[962] Texas Department of Banking "Supervisory Memorandum – 1037", above n 870, at 3.
[963] Ibid.
[964] Ibid.
[965] At 4.
[966] At 4–5.
[967] Texas Finance Code Ch 151 §151.307(a).
[968] At §151.307(b).
[969] At §151.309.
[970] At §151.203(a)(3).
[971] Texas State Securities Board "$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales" (4 January 2018) <https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales>.
[972] Texas Department of Banking "Texas Department of Banking Commissioner Issues Cease & Desist Order Relating to AriseBank" (26 January 2018) <https://www.dob.texas.gov/public/uploads/files/news/press-releases/2018/01-26-18bpr.pdf>; Texas State Securities Board "Emergency Cease and Desist Letter – In the Matter of

action when an organisation claimed its bitcoin mining platform "consistently provides returns of up to 150% per year".[973] Texas' active enforcement has been heralded by many in the cryptocurrency community as beneficial: it is targeting those people and entities that are seen as acting fraudulently, and in turn allowing those with "good" business practices to flourish.[974]

7.2.6 New York

New York was the first state to implement regulation specific to cryptocurrencies.[975] In June 2015 Benjamin Lawsky, Superintendent of Financial Services, announced the final framework for BitLicense – a comprehensive framework for the regulation of firms dealing in cryptocurrencies,[976] administered by the New York State Department of Financial Services (NYSDFS).[977] The BitLicense framework contains rules concerning consumer protection, AML compliance and cybersecurity tailored for cryptocurrency firms.[978] The framework was the third and final framework introduced as a result of a regulatory enquiry by the NYSDFS that began in 2013.[979] The BitLicense framework requires every person who engages in Virtual Currency Business Activity to obtain a BitLicense.[980]

Virtual Currency Business Activity is defined as the conduct of any one of the following involving New York or a New York resident:[981]

(1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;
(2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
(3) buying and selling Virtual Currency as a customer business;
(4) performing Exchange Services as a customer business; or
(5) controlling, administering, or issuing a Virtual Currency.
The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.

The BitLicense framework prohibits any person who engages in any of the above Virtual Currency Business Activities from operating without a BitLicense, with the exception of persons chartered under New York banking law and approved by the superintendent to engage in Virtual Currency Business Activity; and consumers and merchants who use cryptocurrencies to buy or sell goods or for investment purposes.[982] Moreover, the definition of Virtual Currency Business Activity means that even if a business is out of state it must apply for a BitLicense if it meets the above criteria and

Bitconnect" (Press release, 4 January 2018) <https://www.ssb.texas.gov/sites/default/files/BitConnect_ENF-18-CDO-1754.pdf>; Texas State Securities Board "In the Matter of Estrada Trucking, Inc [et al]" (5 April 2018) <https://www.ssb.texas.gov/sites/default/files/ENF-18-CDO-1761.pdf>.

[973] Texas State Securities Board "Bitcoin Promoter USI-Tech Hit with Emergency Order" (Press release, 20 December 2017) <https://www.ssb.texas.gov/news-publications/bitcoin-promoter-usi-tech-hit-emergency-order>.

[974] "The Wild West Embraces Cryptocurrencies: Texas, Wyoming and Washington" *Crypto Insider* (30 January 2018) <https://cryptoinsider.21mil.com/the-wild-west-embraces-cryptocurrencies/>.

[975] Trust in Digital Life *Blockchain: Perspectives on Research, Technology & Policy* (17 June 2016) <https://trustindigitallife.eu/wp-content/uploads/2016/07/TDL_Blockchain_v1.1-_Pages.pdf>.

[976] The BitLicense framework refers to "virtual currency" but in this report "cryptocurrency" is used where possible.

[977] Benjamin M Lawsky, Superintendent of Financial Services "NYDFS Announces Final BitLicense Framework for Regulating Digital Currency Firms" (speech to BITS Emerging Payments Forum, Washington DC, June 2015) <https://media.scmagazine.com/documents/127/speech_-_june_3,_2015__nydfs_a_31558.pdf>.

[978] Ibid.

[979] Ibid.

[980] 23 NYCRR Part 200, above n 865, at § 200.3(a).

[981] At § 200.2(q).

[982] At § 200.3(c)(1)–(2).

involves New York or a New York resident.[983] However, state-chartered banks may be able to operate as virtual currency exchanges without a licence if approved by the NYSDFS.[984]

To obtain a licence, applicants must submit detailed information about their intended business and its directors and demonstrate that it will be compliant with the regulations upon licensing.[985] A BitLicense will only be granted if the superintendent is satisfied that the applicant will conduct business "honestly, fairly, equitably, carefully, and efficiently … in a manner commanding the confidence and trust of the community".[986]

The requirements of the BitLicense regulation are summarised below. While the summary goes into some detail, it provides an example of regulation that has had the effect of driving companies out of New York.[987]

7.2.6.1 Capital requirements

Licensees are required to maintain an amount of capital in a form as required by the superintendent at all times, which the superintendent determines is sufficient to ensure the financial integrity of the licensee and its operations, based on the risks specific to each licensee.[988] Factors in determining an appropriate amount and form of capital required include:[989]

(1) the composition of the licensee's assets;
(2) the composition of the licensee's liabilities;
(3) the actual and expected volumes of the licensee's Virtual Currency Business Activities;
(4) whether the licensee is licensed or regulated under Financial Services Law, Banking Law, Insurance Law or any other laws as provider of financial services, and the good standing of the licensee in such capacity;
(5) the amount of leverage used by the licensee;
(6) the liquidity of the licensee;
(7) financial protection provided through trust accounts or bonds by the licensee to its customers;
(8) the types of entities the licensee services; and
(9) the types of products or services offered by the licensee.

The required capital can be held in cash, cryptocurrency or high-quality, highly liquid investment assets.[990]

7.2.6.2 Custody and protection of customer assets

Licensees must maintain a surety bond or trust account for the benefit of their customers in US dollars and in such form as the superintendent considers acceptable for protection of the licensee's customers.[991] If the licensee maintains a trust, the trust must be maintained with a qualified custodian.[992] Licensees who store, hold or maintain cryptocurrency on behalf of other persons must hold cryptocurrency of the same type and amount owed to those other persons.[993] Licensees are

---

[983] New York State Department of Financial Services "BitLicense Frequently Asked Questions" <http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm>.
[984] Murphy, Murphy and Seitzinger, above n 867, at 15.
[985] 23 NYCRR Part 200, above n 865, at § 200.4(b).
[986] At § 200.6.
[987] Daniel Roberts "Behind the 'Exodus' of Bitcoin Startups from New York" *Fortune* (United States, 14 August 2015) <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/> and Wieczner, above n 910.
[988] 23 NYCRR Part 200, above n 865, at § 200.8(a).
[989] At § 200.8(a)(1)–(9).
[990] At § 200.8(b).
[991] At § 200.9(a).
[992] At § 200.9(a). A Qualified custodian is defined in § 200.2(n) as "a bank, trust company, national bank, savings bank, savings and loan association, federal savings association, credit union, or federal credit union in the State of New York, subject to the prior approval of the superintendent."
[993] At § 200.9(b).

prohibited from selling, transferring, assigning, lending, hypothecating, pledging or otherwise unencumbering or using assets, including cryptocurrencies held on behalf of another person, except at the direction of that other person.[994]

7.2.6.3 Material change to business

Licensees must obtain the superintendent's prior approval of any plan that would introduce or materially change a product or service offered or activities undertaken that would involve New York or a New York resident.[995] A change or introduction is material if it would raise legal or regulatory concerns; safety and soundness, or operational concerns; or it would make the product or service offered or activity undertaken materially different from what was on the BitLicense application.[996] Before implementing a material change the licensee must submit a written application describing the change in detail and the effect it would have on the licensee's business, among any other information required by the superintendent.[997]

7.2.6.4 Change of control and mergers and acquisitions

Licensees require prior approval from the superintendent if they want to take any action that will result in a change of control.[998] A written application for change of control must be made containing detailed information about the applicant and all directors, principal officers, principal stockholders and any other relevant person.[999] The superintendent will consider the motives and capabilities of the person wanting to gain control and also the public interest, among other factors.[1000]

Mergers or acquisitions of all or a substantial part of the licensee must not be undertaken without prior approval of the superintendent.[1001] The application to go ahead with a merger or acquisition must include details of the proposed business plan, the entities to be merged and the terms and conditions of the merger or acquisition.[1002] The superintendent will again take public interest into consideration among other factors.[1003]

7.2.6.5 Books and records

The licensee must keep all books and records associated with its Virtual Currency Business Activity in a condition that the superintendent can examine for a period of at least seven years.[1004] The books and records of the licensee include:[1005]

(1) Details of every transaction, including the amount, precise time of transaction, payment instructions, total amount of fees charged and received by the Licensee, and names, account numbers and physical

---

[994] At § 200.9(c).
[995] At § 200.10(a).
[996] At § 200.10(b)(1)(3).
[997] At § 200.10(c).
[998] At § 200.11(a). Control is defined in § 200.11(a)(2) as meaning "the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Licensee whether through the ownership of stock of such Licensee, the stock of any Person that possesses such power, or otherwise. Control shall be presumed to exist if a Person, directly or indirectly, owns, controls, or holds with power to vote ten per cent or more of the voting stock of a Licensee or of any Person that owns, controls, or holds with power to vote ten per cent or more of the voting stock of such Licensee. No Person shall be deemed to control another Person solely by reason of his being an officer or director of such other Person."
[999] At § 200.11(a)(1).
[1000] At § 200.11(a)(5).
[1001] At § 200.11(b).
[1002] At § 200.11(b)(1).
[1003] At § 200.11(b)(3).
[1004] At § 200.12(a).
[1005] At § 200.12(a)(1)(9).

addresses of the parties to the transaction that are customers of the Licensee and of third parties where possible;
(2) A general ledger of accounts;
(3) Bank statements and reconciliation records;
(4) All statements and valuations provided to or sent to customers and counterparties;
(5) Records or minutes of board meetings;
(6) Records which demonstrate compliance with applicable state and federal AML laws, including customer identification and verification documents, records that link customers to their accounts and records of all compliance breaches;
(7) Documents and communications regarding customer complaint investigations, resolution of transaction errors or any documentation relating to possible violation of laws, rules or regulations;
(8) All other records relating to the above; and
(9) All records not included in the above that the superintendent may require.

Licensees are required to provide the NYSDFS immediate access to all documents and records maintained by the licensee and its affiliates upon request, wherever such information is located.[1006]

Finally, the licensee must keep records of non-completed, outstanding or inactive cryptocurrency accounts and transactions for five years.[1007] After five years of being inactive, cryptocurrency accounts are deemed to be abandoned property under the Abandoned Property Law.[1008]

7.2.6.6 Examinations

The superintendent can examine licensees if it thinks necessary, and every two years is required to determine whether the licensee is complying with the BitLicense regulation and any other relevant matters, especially those matters that would affect the licensee's Virtual Currency Business Activity.[1009] The licensee must allow the superintendent or an affiliate to carry out the examination and must assist the superintendent's examination of the licensee's books, records, accounts, documents and other information at all times.[1010]

7.2.6.7 Reports and financial disclosures

Licensees are required to prepare financial reports the same as any similar business that does not engage in Virtual Currency Business Activity,[1011] with the additional requirement of notifying the superintendent in writing of any proposed change to the licensee's method of calculating the value of cryptocurrency in fiat currency that differs from the method(s) submitted to the NYSDFS in their licence application.[1012]

7.2.6.8 Anti-money laundering

Licensees must undertake an initial risk assessment of the legal, compliance, financial and reputational risks associated with their activities, services, customers, geographic location and counterparties, and design an AML programme based upon that risk assessment.[1013] Additional risk assessments should be carried out annually and the AML programme adjusted as required.[1014] The AML programme must meet minimum requirements and must:[1015]

[1006] At § 200.12(b).
[1007] At § 200.12(c).
[1008] At § 200.12(c); and NY Abandoned Property Law § 501 (2015).
[1009] At § 200.13(a)(1)–(5).
[1010] At § 200.13(b).
[1011] At § 200.14(a)–(c) and 200.14(e)–(f).
[1012] At § 200.14(d).
[1013] At § 200.15(b).
[1014] At § 200.15(b).
[1015] At § 200.15(c)(1)–(4).

(1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable AML rules and regulations;
(2) provide for independent testing for compliance with and effectiveness of the AML program at least annually, the findings of which must be reported to the superintendent;
(3) designate qualified individual(s) to monitor compliance with the AML program; and
(4) provide ongoing training to ensure individuals understand and can comply with AML requirements.

The board of directors or governing body must approve an AML policy to be included in the AML programme.[1016]

As part of its AML programme, each licensee is required to fulfil the following reporting and record-keeping requirements:[1017]

(1) Keep records of cryptocurrency transactions, involving the payment, receipt, exchange, conversion, purchase, sale, transfer, or transmission of cryptocurrency;
(2) Report cryptocurrency-to-cryptocurrency transactions that are not covered by federal currency transaction reporting requirements to the NYSDFS within 24 hours where the amount transacted by one person in aggregate exceeds US $10,000 in one day; and
(3) Monitor cryptocurrency transactions that may be suspicious and may signify money laundering, tax evasion, or other illegal or criminal activity and report suspicious transactions.

Licensees are prohibited from structuring transactions in a way to evade reporting requirements[1018] and are prohibited from engaging in, facilitating or knowingly allowing a transaction involving cryptocurrency that would disguise the identity of a customer or counterparty.[1019] The licensee does not, however, have to make the identity of parties involved available to the public, nor the fact or nature of cryptocurrency transactions.[1020]

As part of the AML programme, each licensee must maintain a customer identification programme,[1021] incorporating the following elements:

(1) Identification and verification of account holders: when a customer opens an account the Licensee must verify the customer's identity, maintain records of the verification, and check customers against the Specially Designated Nationals (SDNs) list maintained by the Office of Foreign Asset Control (OFAC), which is part of the US Treasury Department. If a customer is high risk due to factors such as high volume accounts or accounts which have been reported for suspicious activity, the Licensee must use enhanced due diligence;[1022]
(2) Enhanced due diligence for accounts involving foreign entities: Licensees who maintain accounts for foreign entities must have in place enhanced due diligence policies, procedures and controls to assess the risk of foreign entity accounts based on the nature, type and purpose of the foreign business and its activity and the anti-money laundering and supervisory regime of the foreign jurisdiction in order to detect money laundering;[1023]
(3) Prohibition on accounts with foreign shell entities: Licensees are prohibited from having any type of relationship in their cryptocurrency business with entities that do not have a physical presence in any country;[1024] and
(4) Identification required for large transactions: Licensees must verify the identity of any customer who initiates a transaction worth US $3,000 or more.[1025]

[1016] At § 200.15(d).
[1017] At § 200.15(e)(1)–(3).
[1018] At § 200.15(f).
[1019] At § 200.15(g).
[1020] At § 200.15(g).
[1021] At § 200.15(h).
[1022] At § 200.15(h)(1).
[1023] At § 200.15(h)(2).
[1024] At § 200.15(h)(3).
[1025] At § 200.15(h)(4).

Licensees must be able to demonstrate that their AML programmes are compliant with applicable regulations issued by OFAC[1026] and have policies and procedures in place to prevent transactions that violate federal or state laws, rules or regulations.[1027]

Individuals who are responsible for the day-to-day operation of the AML programme must fulfil at least the following requirements:[1028]

(1) Monitor changes in AML laws and update the AML program accordingly;
(2) Maintain all records required under AML section;
(3) Review all reports that need to be filed;
(4) Escalate matters concerning AML where appropriate;
(5) Report periodically to the board of directors or governing body of the Licensee; and
(6) Ensure training requirements are complied with.

7.2.6.9 Cybersecurity programme

The BitLicense regulation requires licensees to maintain effective cybersecurity programmes to protect their systems and the data stored on those systems from unauthorised access, tampering or use.[1029] The cybersecurity programmes must be designed to perform five core functions:[1030]

(1) Identify information stored on licensees' systems, sensitivity of the information, how it can be accessed and by whom it can be accessed;
(2) Protect the licensees' electronic systems and data stored on those systems from unauthorised access, use or malicious acts;
(3) Detect Cyber Security Events such as intrusions into the system, data breaches and unauthorised access;
(4) Respond to any detected Cyber Security Events and mitigate negative effects; and
(5) Recover from Cyber Security Events to restore normal operations and services.

Licensees are required to have a written cybersecurity policy that sets out the licensee's policies and procedures for protecting its electronic systems and customer and counterparty data. The policy must be reviewed by the licensee's board of directors or governing body at least annually and must address 13 key areas:[1031]

(1) information security;
(2) data governance and classification;
(3) access controls;
(4) business continuity and disaster recovery planning and resources;
(5) capacity and performance planning;
(6) systems operations and availability concerns;
(7) systems and network security;
(8) systems and application development and quality assurance;
(9) physical security and environmental controls;
(10) customer data privacy;
(11) vendor and third-party service provider management;
(12) monitoring and implementing changes to core protocols not directly controlled by the Licensee, as applicable; and
(13) incident response.

[1026] At § 200.15(i).
[1027] At § 200.15(j).
[1028] At § 200.15(k)(1)–(6).
[1029] At § 200.16(a).
[1030] At § 200.16(a)(1)–(5).
[1031] At § 200.16(b)(1)–(13).

In addition, there are further requirements, such as the requirement to have a Chief Information Security Officer,[1032] the requirement to report at least annually on the functionality and integrity of the licensee's electronic systems,[1033] auditing requirements,[1034] the requirement to have an application security programme which is reviewed at least annually[1035] and the requirement to employ and provide regular training for cybersecurity personnel.[1036]

7.2.6.10 Business continuity and disaster recovery

Licensees must implement a business continuity and disaster recovery (BCDR) plan to ensure their services and other business activities remain available and functional in the case of an emergency.[1037] A copy of the current BCDR plan must be distributed to all relevant employees,[1038] who must be trained in their roles and responsibilities in implementing it.[1039] In addition, licensees must notify the superintendent of any emergency or disruption that may affect the licensee's ability to comply with regulatory requirements, or that may have a significant adverse effect on the market, the licensee or its counterparties,[1040] and the licensee must have the BCDR plan independently tested, and revised if required, at least annually.[1041]

7.2.6.11 Advertising and marketing

Licensees must include that they are "licensed to engage in Virtual Currency Business Activity by the New York State Department of Financial Services" in any advertising and marketing material advertised in New York or to New York residents,[1042] and comply with any disclosure requirements under federal and state laws, rules and regulations.[1043] Licensees also need to retain copies of any advertising material for seven years for examination by the superintendent should the superintendent wish to do so, and must retain hard copies of the material where applicable.[1044] Not surprisingly, licensees, or any other persons acting on their behalf, must not make false, misleading, or deceptive representations or omissions either directly or by implication.[1045]

7.2.6.12 Consumer protection

The consumer protection requirements of BitLicense regulation require the licensee to make initial and per-transaction disclosures to their customers and impose acknowledgement requirements on the licensee.[1046]

7.2.6.13 Initial disclosure

In establishing a relationship with a customer, and prior to entering into an initial transaction, the licensed business must disclose all material risks associated with its products, services and activities, as well as cryptocurrencies generally.[1047] The risks that must be disclosed include, at a minimum:[1048]

[1032] At § 200.16(c).
[1033] At § 200.16(d).
[1034] At § 200.16(e).
[1035] At § 200.16(f).
[1036] At § 200.16(g)(1)–(3).
[1037] At § 200.17(a).
[1038] At § 200.17(b).
[1039] At § 200.17(c).
[1040] At § 200.17(d).
[1041] At § 200.17(e).
[1042] At § 200.18(a).
[1043] At § 200.18(c).
[1044] At § 200.18(b).
[1045] At § 200.18(d).
[1046] "New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal**"**, above n 896, at 27.
[1047] 23 NYCRR Part 200, above n 865, at § 200.19(a).
[1048] At § 200.19(a)(1)–(10).

(1) Cryptocurrencies are not legal tender and are not protected by the Federal Deposit Insurance Corporation or Securities Investor Protection Corporation;
(2) Any regulatory changes that may adversely affect cryptocurrencies;
(3) That transactions made with cryptocurrencies may not be reversible, meaning losses caused by fraud or errors may not be recoverable;
(4) The date that cryptocurrency transactions are deemed to be made is the date they are recorded on a public ledger, which may not be the same date the customer initiates the transaction;
(5) The value of cryptocurrencies can fluctuate depending on what market participants determine they are worth (through exchange rates etc) and that the value of a particular cryptocurrency may be lost completely if the market for it disappears;
(6) If a person accepts cryptocurrency as payment at present, there is no guarantee they will continue to do so in the future;
(7) A significant loss on cryptocurrency can occur in a very short time due to market fluctuations;
(8) There is an increased risk of fraud or cyberattack due to the nature of cryptocurrencies;
(9) If the Licensee has technical difficulties, customers' ability to access their cryptocurrency may be affected; and
(10) If a customer has a bond or trust account with the Licensee business, the amount in that account may not be enough to cover any losses the customer incurs.

The licensee must also disclose general terms and conditions associated with the relationship, such as:[1049]

(1) The customer's liability for unauthorised cryptocurrency transactions;
(2) The customer's ability to stop cryptocurrency payments already authorised and the procedure for doing so;
(3) The Licensee's rights regarding disclosure of information about the customer's account to third parties;
(4) The customer's right to periodic account statements and valuations;
(5) The customer's right to receive a receipt or other evidence of each transaction;
(6) The customer's right to receive prior notice of any change in Licensee's policies; and
(7) Other disclosures that are normally given in the opening of a customer account.

7.2.6.14 Pre-transaction disclosure

Prior to a cryptocurrency transaction taking place, licensees must disclose to their customers in writing the amount of the transaction; fees and other charges payable by the customer and the applicable exchange rate; the type and nature of the cryptocurrency transaction; a warning that the transaction may not be undone once executed, if applicable; and such other disclosures that are normally given in transactions of this nature.[1050]

7.2.6.15 Acknowledgement requirement

The licensee must ensure that the customer acknowledges the receipt of all disclosures required above.[1051]

7.2.6.16 Receipts

Following each transaction, the licensee must provide to the customer a receipt containing the licensee's contact details, including the phone number the licensee has established to answer questions and deal with complaints, the details of the transaction, the liability of the licensee for delayed delivery or non-delivery, the licensee's refund policy, and any other information the

[1049] At § 200.19(b)(1)–(7).
[1050] At § 200.19(c)(1)–(5).
[1051] At § 200.19(d).

superintendent may require.[1052] The licensee must make the receipt available to NYSDFS if requested.[1053]

7.2.6.17 Anti-fraud

It is prohibited for licensees to engage in fraudulent activity.[1054] Licensees are required to take action to prevent fraud and must have a written anti-fraud policy, which includes at a minimum identification and assessment of risk areas related to fraud, procedures and controls to guard against identified risks, an allocation of responsibility for risk-management, and procedures for periodic evaluation and revision of the anti-fraud policy.[1055]

7.2.6.18 Complaints

Each licensee must have written policies to deal with complaints and publish details about how to make a complaint, including contact details, in a "clear and conspicuous manner".[1056] If there is a change in the licensee's complaint policies or procedures they must report the change to the superintendent within seven days.[1057]

8. Central bank-issued cryptocurrencies (CBDCs)

A number of central banks have begun work on the impact of central bank-issued cryptocurrencies (abbreviated here as CBDCs, standing for central bank-issued digital currencies),[1058] and some have even released their own. As Tony Richards, Head of Payments Policy at the RBA observes, Bitcoin has "served to stimulate interest in the potential offered by distributed ledgers, extending to the possibility of central bank-issued digital currencies".[1059] Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, states that "it's not surprising that central banks have developed a keen interest in fintech and distributed ledger technology (DLT)".[1060] Indeed, China began work on a possible CBDC in 2014.[1061] The Bank of England raised the possibility of a CBDC in 2015.[1062] Central banks that are not mentioned later in this report, but have indicated that they are prepared to look, or have started

[1052] At § 200.19(e)(1)–(7).
[1053] At § 200.19(e).
[1054] At § 200.19(g).
[1055] At § 200.19(g)(1)–(4).
[1056] At § 200.20(b).
[1057] At § 200.20(c).
[1058] This report uses the abbreviation CBDC instead of CBIC as CBDC is the commonest term. For an overview of the potential for blockchain for central banks see, Jürgen Bott and Udo Milkau "Central Bank Money and Blockchain: A Payments Perspective" (2017) 11(2) Journal of Payments Strategy & Systems 145.
[1059] Tony Richards "The Ongoing Evolution of the Australian Payments System" (speech to Payments Innovation 2016 Conference, Sydney, February 2016) <http://www.rba.gov.au/speeches/2016/sp-so-2016-02-23.html>.
[1060] Wilkins, above n 48.
[1061] Stan Higgins "China's Central Bank Discusses Digital Currency Launch" *Coindesk* (20 January 2016) <https://www.coindesk.com/peoples-bank-of-china-discusses-plans-to-issue-digital-currency/>.
[1062] Bank of England "Digital Currencies" <https://www.bankofengland.co.uk/research/digital-currencies> referring to Bank of England "One Bank Research Agenda" (February 2015) at 6 <https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120>.

looking, into CBDCs include China,[1063] India[1064] and Russia.[1065] New Zealand has dipped a very tentative toe into the water as regards entertaining the potential use of blockchain, or DLT to be more accurate, by central banks.[1066]

While it may appear extraordinary that central banks are actively exploring and trialling a technology that is not yet a decade old and represents a seismic shift in monetary policy, it has been argued that they may have no option but to embrace the new technology:[1067]

> Given the rapid pace of innovations in payments technology and the proliferation of virtual currencies such as bitcoin and ethereum, it might not be prudent for central banks to be passive in their approach to CBDC. If the central bank does not produce any form of digital currency, there is a risk that it loses monetary control, with greater potential for severe economic downturns. With this in mind, central banks are moving expeditiously when they consider the adoption of CBDC.

The actual mechanics of how a CBDC blockchain would be run are beyond the scope of this report, but work from the Bank of England shows that while the central bank would issue the CBDC for security of the system, a decentralised system is preferable to a centralised one:[1068]

> From a macroeconomic perspective, the use of distributed ledgers is not strictly required for the operation of a CBDC system, but we contend that it would be necessary as a practical matter, in order to ensure the resiliency of a system that would clearly be of critical importance to the financial stability of the economy. There are several ways in which such a decentralised system could be implemented. A central bank could maintain all of the copies of the ledger itself, several public institutions could maintain copies for each other, or private sector agents could be involved in collaboration with the central bank.

Again, the question that some will raise is: why are central banks so interested in CBDCs? Indeed, BIS warned recently that "the introduction of a CBDC in one jurisdiction could adversely affect others. Central banks that have introduced or are seeking to introduce a CBDC should consider cross-border issues where relevant".[1069] One reason for the interest nevertheless is that cryptocurrencies and CBDCs "provide a more efficient means for exchanging value globally".[1070] Already IBM, banks and other financial institutions are using cryptocurrencies because there are no viable CBDCs available. For example, IBM's Global Financial Transaction Network, built on Hyperledger Fabric, is using Stellar

---

[1063] Fan Yikei "On Digital Currencies, Central Banks Should Lead" *Bloomberg* (United States, 2 September 2016) <https://www.bloomberg.com/view/articles/2016-09-01/on-digital-currencies-central-banks-should-lead> and Zhang Yuzhe and Han Wei "PBOC Set to be First to Issue Digital Bills" *Caixin* (26 January 2017) <https://www.caixinglobal.com/2017-01-26/101049103.html>.

[1064] Institute for Development and Research in Banking Technology *Applications of Blockchain Technology to Banking and Financial Sector in India* (Whitepaper, January 2017) at 26 <http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf>: "we feel that [blockchain technology] has matured enough and there is sufficient awareness among the stakeholders which makes this an appropriate time for initiating suitable efforts towards digitizing the Indian Rupee through [blockchain technology]." The Institute was established by the Reserve Bank of India and R Gandhi, the Deputy Governor of the Reserve Bank of India and the Chairman of the Institute, wrote the Whitepaper's foreword.

[1065] Kevin Helms "Russia's Central Bank Pushes for National Cryptocurrency" *Bitcoin.com* (6 October 2017) <https://news.bitcoin.com/russias-central-bank-pushes-for-national-cryptocurrency/>.

[1066] Amber Wadsworth "Decrypting the Role of Distributed Ledger Technology in Payments Processes", above n 682 and Amber Wadsworth "The Pros and Cons of Issuing a Central Bank Digital Currency", above n 682.

[1067] Michael Bordo and Andrew Levin "Central Bank Digital Currency and the Future of Monetary Policy" (23 September 2017) Vox <https://voxeu.org/article/benefits-central-bank-digital-currency>.

[1068] Barrdear and Kumhof, above n 334, at 7–8.

[1069] Bank for International Settlements *Central Bank Digital Currencies* (March 2018) at 2 <https://www.bis.org/cpmi/publ/d174.pdf>.

[1070] Kaspar Korjus "We're Planning to Launch Estcoin — and that's only the Start" (19 December 2017) Medium <https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790>. Korjus is the Managing Director of e-Residency in Estonia (e-Residency is an Estonian government department): <https://e-resident.gov.ee/>.

Lumens, a cryptocurrency,[1071] but a CBDC is viewed as an alternative.[1072] Also, if cryptocurrencies increased in use this would affect monetary policy and the ability of central banks to be the lenders of last resort.[1073] In addition, if one of the large cryptocurrencies failed, potentially a large number of users could suffer significant financial loss.[1074] Furthermore, CBDCs would be stable coins, and if issued by reputable countries would be stable in price, as the central bank's monetary policy would maintain the stability of its CBDC[1075] just as it currently maintains the value of its fiat currency.

There is a second reason why CBDCs are so attractive for some central banks and governments, and in this report we argue it is the main reason. Quite simply, to quote Governor of the Bank of England Mark Carney, CBDCs will be "transformative"[1076] – albeit they will need to be properly designed – as blockchain can:[1077]

- Increase the efficiency of managing data;
- Improve resilience by eliminating central points of failure, as multiple parties will share replicated data and functionality;
- Enhance transparency (and auditability) through the creation of instant, permanent and immutable records of transactions; and
- Expand the use of straight-through processes, including with "smart contracts" that on receipt of new information, automatically update and if appropriate, pay.

These properties mean distributed ledger technology could transform everything from how people manage their interactions with public agencies, including their tax and medical records, through to how businesses manage their supply chains.

The CBDCs that have been thought about or issued take a variety of forms. The main distinction is between wholesale and retail CBDCs.[1078] However, as Carney observed, for a CBDC to be transformative it would have to be retail rather than wholesale.[1079]

Before looking at those two main types of CBDCs, wholesale and retail, there is the question of anonymity. It has been argued that it is unlikely for central banks to issue a CBDC that is truly decentralised and allows users to remain anonymous.[1080] Rather it is likely that the current features of financial privacy would be retained; that is, the system would be private, transaction details would be known only to the parties of the transaction, but infrastructure operators would need to be able to identify them and law enforcement would also be able to view the transactions of particular parties in appropriate circumstances.[1081] However, as shown below, Sweden is contemplating an anonymous CBDC, albeit for small sums. Indeed, currently an anonymous currency is used frequently around the world: cash. Although as Bech and Garratt explain, the anonymous nature of cash is most likely due

[1071] IBM "IBM Announces Major Blockchain Solution to Speed Global Payments", above n 30.
[1072] IBM "IBM Blockchain: Global Financial Transaction Network" August 2017 (PowerPoint slides, on file with author).
[1073] Fung and Halaburda, above n 575, at 3.
[1074] At 4.
[1075] At 12.
[1076] Carney, above n 468, at 12.
[1077] Ibid.
[1078] Morten Bech and Rodney Garratt "Central Bank Cryptocurrencies" (2017) BIS (Bank for International Settlements) Quarterly Review 55 <https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf>.
[1079] "To be truly transformative a general purpose CBDC would open access to individuals and firms": Carney, above n 468, at 12.
[1080] Aleksander Berentsen and Fabian Schar "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies" (2018) 100 Federal Reserve Bank of St Louis Review 97 <https://files.stlouisfed.org/files/htdocs/publications/review/2018/04/16/the-case-for-central-bank-electronic-money-and-the-non-case-for-central-bank-cryptocurrencies.pdf>.
[1081] Simon Scorer "Beyond Blockchain: What are the Technology Requirements for a Central Bank Digital Currency?" (13 September 2017) Bank Underground <https://bankunderground.co.uk/2017/09/13/beyond-blockchain-what-are-the-technology-requirements-for-a-central-bank-digital-currency/>.

to historical happenstance rather than intent.[1082] Now technology in the form of a CBDC allows for a conscious decision to be made.[1083]

8.1 Wholesale central bank-issued cryptocurrency

A wholesale CBDC is a cryptocurrency that is used between banks and other financial institutions. Both Canada and Singapore have been exploring and trialling a wholesale CBDC using permissioned blockchains. Canada's Project Jasper is a collaborative research initiative by governmental agency Payments Canada, the Bank of Canada, financial innovation consortium R3 and a number of Canadian financial institutions.[1084] One aspect of Project Jasper allows approved retail banks to pledge cash collateral into an account at the central bank, which is converted to a CAD-coin and transferred to the participant's account.[1085] The participants can exchange the CAD-coin between themselves and can redeem the CAD-coin for cash collateral, with the central bank in turn destroying that amount of CAD-coin. In truth, however, the CAD-coin is not strictly speaking a CBDC, but rather a tool for using DLT for wholesale interbank settlement. Likewise Singapore's Project Ubin[1086] is an Interbank Real-Time Gross Settlement System, again not strictly speaking a CBDC.

A better term for Canada's and Singapore's projects would be a proto-CBDC. Proto-CBDCs would not realise the transformational power alluded to by the Governor of the Bank of England for that economy.[1087]

8.2 Retail central bank-issued cryptocurrencies

A retail CBDC is a currency that businesses and people can use to transact. There are three broad types of retail CBDCs. As the name implies, all are issued by the central bank, which either runs the system to secure the CBDC or uses decentralised nodes to secure the CBDC system.[1088] In the first type a person or entity would need a bank account with the central bank to receive and spend the CBDC. In the second, retail banks could deal with the CBDC, so people would continue to have bank accounts with retail banks. With the final type, the CBDC does not require the user to have an account with the central bank, and instead the CBDC can be transferred between any parties that choose to accept it, similar to cryptocurrencies such as bitcoin and Ethereum. (As long as the rules on the particular CBDC allow it to be traded freely, for example, it is possible to provide that the CBDC can be held by people who have met certain requirements. We will see this below with the Marshall Islands.)

[1082] Bech and Garratt, above n 1078, at 65.

[1083] Ibid.

[1084] Payments Canada, Bank of Canada and R3, above n 246. See also Chapman, Garratt, Hendry, McCormack and McMahon, above n 246.

[1085] Laura Shin "Canada Has Been Experimenting with a Digital Fiat Currency Called CAD-COIN" *Forbes* (United States, 16 June 2016) <https://www.forbes.com/sites/laurashin/2016/06/16/canada-has-been-experimenting-with-a-digital-fiat-currency-called-cad-coin/#4b1985fe46a4>.

[1086] Monetary Authority of Singapore, above n 248; Monetary Authority of Singapore and the Association of Banks in Singapore *Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies* (November 2017) <http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20Phase%202%20Reimagining%20RTGS.pdf>.

[1087] See Carney, above n 468 and accompanying text.

[1088] For a proposal for a CBDC that is secured by decentralised authorities see George Danezis and Sarah Meiklejohn "Centrally Banked Cryptocurrencies" (paper presented to 23rd Annual Network and Distributed System Security Symposium, NDSS, San Diego, California, United States, 2016) <http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf>.

8.2.1 Accounts need to be held with the central bank

8.2.1.1 Sweden

Sweden has tentatively suggested two types of e-krona.[1089] One would be a register-based e-krona where the balance would be stored in a central database. By contrast, the value-based e-krona would be more akin to cash and would be stored locally in an app or on a card. The value-based e-krona would be used for low-value payments.

The register-based e-krona would not therefore have the utility of decentralised cryptocurrencies as both the sender and receiver must have an account at the central bank. The advantage of the value-based e-krona is that while it would not be as freely tradable as bitcoin, it could allow for people using cards to remain anonymous[1090] as with cash (if a card was used that did not need to be registered) and also enable those without bank accounts to pay for goods and services.

8.2.1.2 United Kingdom

The Bank of England has been working on CBDCs. The work done so far suggests that a CBDC would work alongside existing retail bank offerings and have positive effects since it would require the retail banks to improve their offerings:[1091]

> … [a] CBDC would be economically equivalent to the establishment of an online-only, reserve-backed, narrow bank alongside the existing commercial banking system and, as such, would represent an expansion of competition in the market for deposit accounts. This should again lead to a more rapid adoption of innovative technologies and account offerings.

Unlike under the Swedish proposal, where accounts would be held with the central bank, the CBDC would continue to be held on deposit at retail banks.[1092]

Notwithstanding the Bank of England's work on a possible CBDC, "given current technological shortcomings in distributed ledger technologies and the risks with offering central bank accounts for all, a true, widely available reliable CBDC does not appear to be a near-term prospect".[1093]

8.2.2 Retail banks able to deal in the CBDC

8.2.2.1 China

China's central bank, the People's Bank of China (PBoC), suggested in January 2016 that it would like to launch its own CBDC to cut the costs of circulating traditional paper money and boost policymakers' control of money supply.[1094] This was confirmed in an article in January 2018 by Yifei Fan, the bank's Deputy Governor.[1095] Mr Fan indicated that the short-term focus of any CBDC would be to replace "M0" currency (bank notes and coins). As it stands, M0 currency suffers from being: costly to operate as it requires printing, storing, circulating as well as costs when notes are withdrawn from circulation; inconvenient; susceptible to forgery; and commonly used for money laundering. In contrast, M1 and M2 currency has already been largely digitised in China and so it would be a waste of resources to "re-digitise". In the same vein, Mr Fan announced at the 2018

[1089] Sveriges Riksbank *The Riksbank's e-krona Project, Report 1* (September 2017) <http://archive.riksbank.se/Documents/Rapporter/E-krona/2017/rapport_ekrona_170920_eng.pdf> at 5.
[1090] At 19.
[1091] Barrdear and Kumhof, above n 334, at 11.
[1092] At 7.
[1093] Carney, above n 463, at 12.
[1094] Aizhu, above n 407 and see Yifei Fan "Considerations concerning the Central Bank's Digital Currency" (2018) <http://www.yicai.com/news/5395409.html> (translated by Chaowei Fan).
[1095] Yifei Fan "Considerations concerning the Central Bank's Digital Currency" (2018) <http://www.yicai.com/news/5395409.html> (translated by Chaowei Fan).

National Currency Gold and Silver Bureau teleconference, that one of the key priorities in 2018 is to further promote the research on, and development of, a CBDC.[1096] It is clear from these developments that China's central bank is taking the idea of a CBDC seriously. In addition, the impact that digital payment platforms have on China is undeniable, with WeChat Pay boasting over 938 million monthly active users in Q1 2017.[1097]

In October 2017, the Tsinghua University National Institute of Financial Research published a report titled "The Exploration of the Legal Digital Currency in China",[1098] setting out the history and the progress China has made in investigating a digitised Renminbi cryptocurrency.[1099] The report discussed various fundamental elements that would be required in a State-backed cryptocurrency. In particular, the report recognised the need for a balance between anonymity of use (to protect citizens' legal rights over private property) and safeguarding social order (allowing the State to trace transactions to stop or prevent criminal activity).[1100] To achieve this balance, the report suggested among other design features that:[1101]

- the CBDC must have strong integration between the central bank and retail banks;
- the central bank should make full use of blockchain (for bookkeeping and registration) and big data; and
- there needs to be active participation of third party institutions and end consumers within the digital currency ecosystem.

At its core, the Chinese CBDC would operate in a similar fashion to how paper legal tender works currently. The PoBC would issue money to commercial banks who in turn provide deposit, withdrawal and other related financial services to the public.[1102] Mr Fan has confirmed the PoBC's preference is to adopt this "two-tiered" approach between the central bank and commercial banks to deploy the State-backed cryptocurrency. [1103]

The report also envisions that three "centres" will be set up to support and operate the CBDC framework:

- Certification centre – responsible for the PoBC's management of the CBDC institutions and user identities;
- Registration centre – responsible for recording transactions and registering the corresponding ownership of the CBDC; and
- Big data analysis centre – responsible for the analysis of customer transactions to avoid risks and prevent illegal activities. Data from transactions can also assist in providing insight required for monetary policy and financial stability analysis.

From the end users' perspective, transactions will be conducted by way of mobile applications, making it easy to send to, and receive from, other users and merchants.

8.2.3 No bank account required

As staff members of the Central Bank of Malaysia have noted, there are two potential modalities for CBDCs: one where individuals and organisations hold accounts with the central bank or through retail

---

[1096] The People's Bank of China (2018) <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3509038/index.html> (translated by Chaowei Fan).
[1097] Tencent, RDCY and Ipsos "2017 Mobile Payment Usage in China Report" (2017) <https://www.ipsos.com/sites/default/files/ct/publication/documents/2017-08/Mobile_payments_in_China-2017.pdf>.
[1098] Jin Liu "The Exploration of the Legal Digital Currency in China" (2017) <www.pbcsf.tsinghua.edu.cn/Upload/file/20171026/20171026143301_6961.pdf> (translated by Chaowei Fan).
[1099] At [1.2].
[1100] At [2.1].
[1101] See Figure 2.1.
[1102] At [2.2].
[1103] Qian Yao "Technical considerations of the Central Bank's digital currency" (2018) <http://www.yicai.com/news/5404436.html> (translated by Chaowei Fan).

banks, and one where the CBDC would circulate between individuals without the involvement of central banks or retail banks.[1104]

8.2.3.1 Venezuela

Venezuela has released the Petro as a CBDC,[1105] albeit one that will hopefully not be copied by any other country.[1106] The Petro is pegged to the price of one barrel of Venezuelan oil,[1107] but such is international suspicion of the Venezuelan Government that its price at the time of writing in late August 2018 was only USD 0.02.[1108] The Government used an ICO to launch the Petro. In contrast to other CBDCs, the Petro can only be purchased with euros, US dollars, bitcoin or ether, which means that Venezuelan citizens cannot purchase it using bolívars, the Venezuelan fiat currency. It has been reported recently that the Venezuelan President Nicolás Maduro has ordered Venezuelan banks to use the Petro as a unit of account, thus banks must reflect all financial information in both bolívars and Petros.[1109]

While at first glance the Petro runs counter to the argument that no country would release a CBDC that would allow its users to remain anonymous,[1110] it is simply an attempt by the Venezuelan Government to attract money from overseas, albeit it is now legal tender in Venezuela.[1111]

8.2.3.2 Marshall Islands

The Marshall Islands passed its Declaration and Issuance of the Sovereign Currency Act 2018 on 26 February 2018.[1112] This allows for the creation of the Sovereign, or SOV.[1113] SOVs will be legal tender in the Marshall Islands, along with the US dollar.[1114] An ICO will be used to issue the token[1115] and as part of the process Marshall Islands citizens will be given a number of SOVs for free – an "airdrop". The SOV has been capped at 24 million tokens (divisible into 100 sub-units)[1116] and it is not redeemable.[1117] For the Marshall Islands the SOV is seen as an assertion of national sovereignty: the Minister-in-Assistance to the President of the Marshall Islands states, "As a country, we reserve the right to issue a currency in whatever form it is, whether in digital or fiat form" and adds that CBDCs are "the way of the future".[1118]

While people wanting to buy and sell SOVs will not need an account with the Bank of Marshall Islands (which is not a central bank but a commercial bank majority-owned by the Government), to obtain

---

[1104] Nurjannah Ahmat and Sabrina Bashir "Central Bank Digital Currency: A Monetary Policy Perspective" Staff Insights (September 2017) at 4 <http://www.bnm.gov.my/index.php?ch=en_publication&pg=en_staffinsight&ac=45&bb=file>.
[1105] <http://petrodollars.io/>. For the Whitepaper see *Petro* (Whitepaper, 30 January 2018) <https://d158ejkbvy3pxw.cloudfront.net/wp-poricontent/uploads/2018/01/Whitepaper_Petro_en.pdf.>
[1106] Jack Karsten and Darrell M West "Venezuela's 'Petro' Undermines other Cryptocurrencies – and International Sanctions" *Brookings* (9 March 2018) <https://www.brookings.edu/blog/techtank/2018/03/09/venezuelas-petro-undermines-other-cryptocurrencies-and-international-sanctions/> and O'Brien, above n 33.
[1107] Ibid.
[1108] <https://coincap.io> as at 23 April 2018 – or to be more precise $0.02322213.
[1109] "Venezuela orders banks to adopt cryptocurrency" *France24* (28 August 2018) <https://www.france24.com/en/20180828-venezuela-orders-banks-adopt-cryptocurrency>.
[1110] Berentsen and Schar, above n 1080, at 103–104.
[1111] Adam James "Venezuela Decrees Petro 'Cryptocurrency' as Legal Tender" *Bitcoinist* (14 April 2018) <http://bitcoinist.com/venezuela-decree-accept-petro-legal-tender/>.
[1112] <https://www.sov.global/read-the-law>.
[1113] Interestingly the Act's text is in effect the Sov coin's Whitepaper.
[1114] Declaration and Issuance of the Sovereign Currency Act 2018 s 104(1) and (3).
[1115] At s 104(4).
[1116] At s 105(2).
[1117] At s 104(5).
[1118] Gertrude Chavez-Dreyfuss "Marshall Islands to Issue own Sovereign Cryptocurrency" *Reuters* (1 March 2018) <https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD>.

SOVs they will have to "apply to a pre-selected, reputable KYC company, using government-issued identification".[1119] The users' identity and transactions will not be made public. The ability to transact without requiring a bank account with the Marshall Islands Government, as the Marshall Islands has no central bank, would appeal to some. The requirement that SOVs only be held and thus used by people and organisations approved by reputable third parties following appropriate KYC requirements, crucially entailing government-issued identification, would put the risk of money laundering and other criminal activity on a par with the traditional banking system, as it would be possible to use artificial intelligence to monitor and detect suspicious transactions.[1120]

Interestingly, tax evasion could also be targeted. The Marshall Islands is a member of the Global Forum on Transparency and Exchange of Information for Tax Purposes, as is New Zealand. As part of the OECD's Common Reporting Standard the participating countries are required to exchange information about citizens of foreign tax residents with the country for which they are a tax resident, such as account balances, income and payment information.[1121]

8.3 Ecuador, Tunisia and Dubai

Ecuador has been said to have released a CBDC,[1122] largely in an attempt to roll back dollarisation there.[1123] However, Ecuador's digital money did not use a blockchain and was more akin to the M-Pesa,[1124] which was first launched in Kenya and Tanzania. By all accounts it has not worked out well and is being closed down as a failed experiment.[1125]

Tunisia has also been announced as launching a CBDC, in late 2016;[1126] however, the Chairman and CEO of Tunisia Post, which facilitates the payments in Tunisia,[1127] made it clear on 21 March 2017 that experiments were still being undertaken to put a currency on a blockchain. In May 2017 it was announced that a Bitdinar mobile wallet was being developed.[1128]

[1119] Declaration and Issuance of the Sovereign Currency Act 2018 s 104(3) and see <https://www.sov.global/yokwe>.
[1120] For the use of AI to detect suspicious transactions see TJ Horan, Frank Holzenthal, and Scott Zoldi *Advancing AML Compliance with Artificial Intelligence* (FICO, 2017) <http://www.fico.com/en/node/8140?file=12318>.
[1121] Inland Revenue Department "Guidance on the Common Reporting Standard for Automatic Exchange of Information" (June 2017) <http://www.ird.govt.nz/resources/c/e/ce0dd7f2-3e73-4103-833a-1d6dea19b37d/crs-guidance-final.pdf>.
[1122] Everett Rosenfeld "Ecuador Becomes the First Country to Roll out its own Digital Cash" *CNBC* (United States, 6 February 2015) <https://www.cnbc.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html>.
[1123] Ecuador's legal tender is the US dollar. Ecuador did have its own fiat currency, sucres, but it slowly lost value to such a degree that Ecuadorians began to use US dollars and the sucre was eventually replaced as legal tender by the US dollar in 2000. See generally Larry White "Defending Dollarization in Ecuador" *Alt-M* (4 December 2014) <https://www.alt-m.org/2014/12/04/defending-dollarization-in-ecuador/>.
[1124] Giorgio Milki "The Case for National Digital Currencies" *Kapron Asia* (14 December 2017) <https://www.kapronasia.com/blockchain-research-menu-item/item/914-a-growing-number-of-countries-are-creating-their-own-digital-currencies.html> and Taylor Nelms "'Ecuador Bans Bitcoin'! A Monetary Mix Up" (20 October 2015) King's Review <http://kingsreview.co.uk/articles/ecuador-bans-bitcoin-a-monetary-mix-up/>.
[1125] Evelyn Tapia "ECB Will Stop Opening New Electronic Money Accounts" *El Comercio* (Peru, 29 December 2017) <http://www.elcomercio.com/actualidad/bce-cuentas-dineroelectronico-banca-reactivacion.html> and Larry White "The World's First Central Bank Electronic Money Has Come – And Gone: Ecuador, 2014-2018" *Alt-M* (29 March 2018) <https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/>.
[1126] "Tunisia is the First Country to put National Currency on Blockchain" *FT Reporter* (29 November 2016) <http://ftreporter.com/tunisia-is-the-first-country-to-put-national-currency-on-blockchain/>.
[1127] Moez Chakchouk "Blockchain in Tunisia: From Experimentations to a Challenging Commercial Launch (slides from ITU Workshop on "Security Aspects of Blockchain" Geneva, Switzerland, 21 March 2017) <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/S3_2.%20ITU-BlockchainWS-21032017.pdf>.
[1128] Oussema Settala "Bitdinar: The Mobile Wallet" (12 May 2017) Medium <https://medium.com/vink-io/bitdinar-the-mobile-wallet-9e6e867cbdb>.

Dubai is reported as having launched its CBDC, emCash, in October 2017, but there are few details of how it will work or works in practice.[1129]

8.4 Estonia – a different approach

Estonia has floated the concept of the estcoin,[1130] which is not surprising given Estonia's embrace of the digital economy and its mindset.[1131] The proposed estcoins would be "crypto tokens" – such terminology is important because as part of the European Union Estonia's currency is limited to the euro. Crucially Estonia has realised the power of cryptocurrencies and that CBDCs are not simply limited to being a payment mechanism.

Estonia has proposed not one, but three types of tokens. First a "community estcoin", which would not be backed; indeed an ICO would be used to raise money for Estonia. To work round the euro problem, the tokens would only be held by Estonian e-residents and businesses that offer services to the e-residents including accountants, banking and virtual offices. E-residents could earn the community estcoin if they, for example, "drive web traffic to e-Residency, successfully sign up a new e-resident, post a tender within our community that provides work to another e-resident or Estonian company, or spend time providing useful advice to other e-residents."[1132]

The second coin is the "identity estcoin". Identity is a significant issue. Financial institutions spend significant amounts on KYC,[1133] not to mention the time and inconvenience for customers: it is not uncommon to spend over an hour in New Zealand proving identity when setting up a bank account. Estonians and e-residents would be issued with a number of tokens that are attached to their digital identity and could purchase more if required. The identity estcoin would also enable the e-residents to prove who they were for individual transactions. The identity estcoin would not be intended to make a profit; rather, revenue raised from identity tokens would be used to maintain the network. Given that the identity coins are not tradable as they are unique to each person, they are not a traditional currency. However, they would use the blockchain and also provide the benefit of greater transparency, and may even go as far as helping ensure order, as the Estonian Police and Border Guard Board could be granted the ability to revoke the tokens if e-residents had broken laws.

The final coin, the "euro estcoin", would be pegged to the euro. Similar to the way tokens work within video games or online worlds, the euro estcoin would be used between e-residents with the intent of encouraging business between e-residents. Unlike the community estcoin, e-residents would purchase the euro estcoin with fiat currency and when desired sell the euro estcoin back to the Estonian Government at the exchange rate of one estcoin to one euro.

8.5 Potential issues with retail central bank-issued cryptocurrencies

Security is a concern, albeit, as work at the Bank of England has suggested, a decentralised CBDC system may be more secure than a centralised system.[1134] One way to mitigate against security fears would be to issue a relatively small amount to circulate in parallel with the existing fiat currency to

---

[1129] Suparna Dutt D'Cunha "Dubai Sets Its Sights on Becoming the World's First Blockchain-Powered Government" *Forbes* (United States, 18 December 2017) <https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#3ce9fa6c454b>.

[1130] Korjus, above n 1070.

[1131] See, generally, Nathan Heller "Estonia, the Digital Republic" *The New Yorker* (United States, online ed, 18 December 2017) <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>. As the article says "The Estonian government is so eager to take on big problems that many ambitious techies leave the private sector to join it."

[1132] Korjus, above n 1070.

[1133] See generally, Thomson Reuters *Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points* (26 October 2017) <https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html>.

[1134] See above n 1068 and accompanying text.

trial the security and other features of the CBDC. In New Zealand, the sum of NZD 50 million has been mooted.[1135]

Of more concern is the financial stability risk that BIS has identified. There may be a flight away from retail banks and other institutions to what is seen as a more secure financial institution, that is, the central bank.[1136] Such a risk would become more pronounced in times of stress, and the presence of a CBDC could allow for "digital runs" towards the central bank on a scale never seen before, especially if there was no deposit insurance scheme or the scheme was limited.[1137] One way of enticing people and organisations to keep deposits with retail banks would be if no interest was payable on the CBDC, albeit that with central banks offering very low interest rates in many countries, and even negative interest rates,[1138] the lure of interest may not be sufficient to prevent people fleeing to a central bank's CBDC. However, even CBDCs may not be as attractive as cryptocurrencies given quantitative easing and other factors. As a novelist and journalist has already perceptively observed:[1139]

> Imagine a secure international cryptocurrency whose steady value was not subjected to deliberate, systematic decay, whose supply was strictly limited, whose coin was universally accepted, and whose production was beyond the control of the state. Even if the investment couldn't be expected to appreciate in the slightest, I'd put my every last farthing in such a currency in a heartbeat.

Thus central banks must make their CBDCs attractive for people to both store their wealth and transact.[1140]

9. Recommendations and conclusion

There is currently no standard international treatment of cryptocurrencies. New Zealand is not alone in using existing laws and attempting to clarify where cryptocurrencies sit legally. Some other jurisdictions have been proactive and have regulated, some with the intent of fostering the industry, such as in Japan, while still others, like China, have attempted to prevent the use of cryptocurrencies. What is clear is that numerous central banks are exploring the creation of CBDCs.

9.1 Discontinue with hands-off approach

The heading, "discontinue with the hands-off approach", is potentially misleading as it is wrong to say that New Zealand has no regulation of cryptocurrencies. New Zealand cryptocurrency exchanges are subject to AML/CFT requirements.[1141] The term "hands-off" is being used to mean that the supervisors and the Government in general are standing back when banks are arguably overstepping the mark and closing exchanges' bank accounts and making it difficult for businesses to accept cryptocurrencies as payment. Even the Financial Intelligence Unit has observed that the use of cryptocurrencies in New Zealand may not be as high as other countries because of the "high levels of scrutiny from the traditional financial sector."[1142]

[1135] Grant Anderson "Why New Zealand Could Become a Cryptocurrency Leader" *Acuity* (1 December 2016) <https://www.acuitymag.com/opinion/why-new-zealand-could-become-a-cryptocurrency-leader>.
[1136] Bank for International Settlements *Central Bank Digital Currencies*, above n 1059, at 16.
[1137] At 16.
[1138] Jana Randow and Simon Kennedy "Negative Interest Rates" *Bloomberg* (United States, 22 March 2017) <https://www.bloomberg.com/quicktake/negative-interest-rates>.
[1139] Lionel Shriver "Why Cryptocurrency is the Answer" *The Spectator* (UK, online ed, 6 January 2018) <https://www.spectator.co.uk/2018/01/why-cryptocurrencies-are-the-answer/>.
[1140] Jesús Fernández-Villaverde "On the Economics of Currency Competition" Vox (03 August 2017) <https://voxeu.org/article/competition-between-government-money-and-cryptocurrencies>.
[1141] Exchanges will be operating a value transfer service and under s 5 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008 they will be deemed to be providing a financial service and thus subject to the requirements of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. See Financial Markets Authority "Cryptocurrency Services" <https://fma.govt.nz/compliance/cryptocurrencies/cryptocurrency-services/>.
[1142] Financial Intelligence Unit "National Money Laundering and Terrorism Financing Risk Assessment", above n 87, at 8.

The regulation of exchanges and the imposition of AML/CFT requirements on them should be continued as it is the most practical and cost-effective approach,[1143] and it is impracticable to regulate the sender or receiver of cryptocurrency.[1144] The (intergovermental) Financial Action Task Force (FATF) recommends the targeting of exchanges in terms of AML/CFT and not users of those exchanges.[1145] What is needed, however, is clear and accessible guidance to those wanting to operate cryptocurrency exchanges. When verbal inquiries are made to Government departments, different answers are given, even when dealing with the same department. The same level of information and consistency that is afforded to other industries needs to be given. For example, the Ministry of Justice, whichwrote New Zealand's AML/CFT legislation, could follow its own example of the excellent webpage that it has for lawyers[1146] and accountants[1147] for AML/CFT and produce a similar one for cryptocurrency exchanges.

In an ideal world if the FMA considers certain tokens should not be available on New Zealand cryptocurrency exchanges it would state what those tokens are. In practice, though, it would be impracticable for the FMA to review every token in a timely fashion. Also the alternative approach of a "ruling service" where exchanges could request rulings to be made would be cumbersome, time consuming and expensive. A more practical and reasonable approach would be for the FMA to provide more detailed guidance including case studies to help exchanges and their advisers reach their own view as to when a particular token is a "financial product".

The compelling argument against continuing with the current hands-off approach in New Zealand (and Australia) is that cryptocurrencies occupy a grey area that banks are wary of, with serious consequences for businesses. New Zealand businesses that trade or otherwise deal in cryptocurrencies have lost their banking services,[1148] as has occurred in Australia.[1149] To be sure, there are some high-profile success stories in New Zealand, such as Centrality[1150] and MyCryptoSaver (formerly called MyBitcoinSaver);[1151] however, they are the exception rather than the rule. In addition, MyCryptoSaver managed to secure a stable bank account only after two previous bank accounts with different banks had been closed down and the businesses had to suspend operations for weeks while banking arrangements were sorted out.

Kiwibank's Digital Advisor, Peter Fletcher-Dobson, has been reported as accepting that it is hard for cryptocurrency exchanges in New Zealand to establish themselves: "New Zealand banks have opted to take a conservative, risk-averse approach to cryptocurrencies. Whereas countries like Japan and

---

[1143] Danton Bryans "Bitcoin and Money Laundering: Mining for an Effective Solution" 2014 Indiana Law Journal 441, at 471–472.

[1144] At 469–470.

[1145] Financial Action Task Force "Guidance for a Risk-Based Approach: Virtual Currencies", above n 743, at 14.

[1146] Ministry of Justice "Lawyers and AML/CFT" <https://www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/info-for-businesses/lawyers-accountants/>.

[1147] Ibid.

[1148] Holly Ryan "Bank Closes Cryptopia Account" *The New Zealand Herald* (online ed, 31 January 2018) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11985380>; Jenée Tibshraeny "Founder of the World's Second Largest Digital Currency Urges Regulators to get Banks to Stop Blanket De-risking; RBNZ 'Generally Comfortable' with Banks' Approaches to Cryptocurrency" *Interest.co.nz* (New Zealand, 12 May 2017) <https://www.interest.co.nz/business/87670/founder-worlds-second-largest-digital-currency-urges-regulators-get-banks-stop>; Jamie Redman "New Zealand Exchange Bitnz Shuts Down Due to 'Banking Hostility'" *Bitcoin.com* (14 February 2018) <https://news.bitcoin.com/new-zealand-exchange-bitnz-shuts-down-banking-hostility/>; and "NZ Bitcoin ATM Shut Down" *The New Zealand Herald* (online ed, 29 July 2014) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11300912>.

[1149] Paul Smith "ACCC Investigating Banks' Closure of Bitcoin Companies' Accounts" *The Australian Financial Review* (online ed, 19 October 2015) <http://www.afr.com/technology/big-banks-cut-off-accounts-of-bitcoin-companies-in-battle-for-the-future-of-payments-20150921-gjr7hu>.

[1150] <https://www.centrality.ai/> and see Gower, above n 28.

[1151] <https://mycryptosaver.com/>.

China have been much more willing to experiment."[1152] As Fletcher-Dobson identifies, the issue appears to be that there is "no true digital identity solution that bridges crypto and fiat financial systems".[1153] One solution that people are working on including in New Zealand is to create digital identities; that way money could be tied to a person or an organisation.[1154]

In Australia the reason given by banks for the removal of banking services is that the banks were concerned that they would not comply with their AML/CTF obligations.[1155] Granted, banks are exploring ways to use the blockchain in their businesses and are investing in blockchain development heavily, but that is not the same as nimble innovation-driven start-ups. The ACCC was sufficiently concerned with the banks' actions that it investigated whether banks were colluding to block potential competitors.[1156]

The pattern of bank accounts being denied or closed down by those dealing with cryptocurrencies or wishing to is widespread. The UK's FCA was clear that denial of access to banking services was of considerable concern to it and was a real issue for businesses.[1157] The FCA only became aware of the true extent of the obstacle that legitimate businesses faced when it became actively involved in the development and promotion of the businesses through its sandpit. This makes the FCA's concerns particularly instructive:[1158]

> We are aware that in recent years some banks have been withdrawing or failing to offer banking services to some types of customers. We are concerned that denying certain customers bank accounts on a wholesale basis causes significant barriers to entry and could lead to poor competition in certain markets. This is commonly referred to as "de-risking".
>
> The drivers behind these practices are many and complex. This is, at least in part, driven by banks' perception of greater money laundering and terrorist financing risks posed by certain types of customers, but also appears to come from other factors including strategic business decisions, the profitability of certain relationships, credit risk assessments, and overall compliance costs. Research has found that some banks are closing accounts for certain companies (for example money transmission services), and that de-risking seems to affect small businesses more than large ones.
>
> We have witnessed the denial of banking services first-hand across a number of firms in the first two cohorts of the sandbox. Difficulties have been particularly pronounced for firms wishing to leverage DLT, become payment institutions, or become electronic money institutions. We are concerned by what appear to be blanket refusals for certain kinds of applicant firms. There are also apparent inconsistencies within individual banks regarding how they apply their assessment criteria in approving access to banking services.
>
> We recognise that this is not an issue faced solely by firms in the sandbox. However, this process has given us closer insight into the difficulties faced by firms in this area. Some firms have been unable to conduct their tests as initially planned as a result. If certain firms cannot secure bank accounts it is possible that they will be unable to meet our conditions for authorisation and would therefore be unable to enter the market, even to test in the sandbox.
>
> We work to ensure that the UK financial system is a hostile environment for money launderers. However, we are clear that effective money laundering risk management need not result in wholesale

---

[1152] Richard MacManus "Bitcoin Startups Stalled by Banks" *Newsroom* (New Zealand, 28 June 2017) <https://www.newsroom.co.nz/2017/06/18/34731/bitcoin-startups-stalled-by-banks>.
[1153] Ibid.
[1154] Goel "12 Companies Leveraging Blockchain for Identification and Authentication", above n 648 and see Gower, above n 28.
[1155] Smith, above n 1149.
[1156] Ibid.
[1157] Financial Conduct Authority "Regulatory Sandbox Lessons Learned Report" (October 2017) at [5.2–5.6] <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>.
[1158] Ibid.

> de-risking, and are aware of the risks this may pose to innovation and competition and intend to continue our focus on this issue.

It has been observed that the banks' conduct in the UK has the effect of thwarting "the UK's ambition to be a global hub for the fast-growing fintech sector".[1159]

The question is how to address the banks' concern over meeting their AML/CFT requirements. Allowing that the banks do have legitimate concerns over meeting their AML/CFT obligations,[1160] the problem nevertheless is that this is not the first time that banks in New Zealand have claimed that AML/CFT requirements have required them to remove banking facilities from potential competitors, as the following example with remittances demonstrates.

Migrants and immigrants often send money from New Zealand and Australia to their home countries, particularly to the Pacific Islands, through remittances. The World Bank in 2015 estimated that globally some USD 582 billion was sent in remittances. A number of businesses offer international money transfer services, more commonly described as money remitters or MTOs. The cost of remittances is high. In September 2014 the global average cost of sending USD 200 was 8.91 per cent, with the rate even higher in New Zealand at 9.23.[1161] Remitting money to the Pacific Islands is higher still: Samoa at 9.49 per cent, Tonga at 10.61 per cent and Vanuatu at 12.09.[1162]

Notwithstanding the cost of remittances, MTOs are important as they provide a convenient specialised financial service to which a number of people would not otherwise have access.[1163] As the New Zealand Treasury has noted, many people in the Pacific who live outside main urban areas have limited access to banking services, and MTOs are often the only viable way to transfer money.[1164] Despite the importance of MTOs in the Pacific, in recent years MTOs have been in effect closed down by New Zealand and Australian banks as they have had their banking services in New Zealand and Australia either limited or removed completely.[1165] The banks' explanation for removing services to MTOs was that they were required to adhere to their obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (NZ), and Australia's equivalent, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).[1166] Yet, while it may have been that some MTOs were acting inappropriately, it is difficult to see that the whole sector was not following the law. Indeed, the RBNZ was sufficiently concerned with blanket service removal to release a statement expressing concern over the banks' behaviour:[1167]

> … the AML/CFT Act doesn't require banks to take a broad-brush approach, closing existing accounts or refusing to open new accounts for an entire category of customers such as money remitters. Nor does the AML/CFT Act prohibit banks from providing services to any customers unless the banks are unable

---

[1159] Martin Arnold "Cryptocurrencies Companies Forced to Bank outside UK" *Financial Times* (UK, online ed, 23 October 2017) <https://www.ft.com/content/3853358e-b508-11e7-a398-73d59db9e399>.

[1160] Australian Transaction Reports and Analysis Centre "AUSTRAC and CBA Agree $700m Penalty" (4 June 2018) <http://www.austrac.gov.au/media/media-releases/austrac-and-cba-agree-700m-penalty>, which reported that AUSTRAC and the Commonwealth Bank of Australia reached a AUD 700 million penalty to resolve Federal Court proceedings relating to serious breaches of AML/CTF laws.

[1161] Reserve Bank of New Zealand "Statement about Banks Closing Accounts of Money Remitters" (28 January 2015) <http://www.rbnz.govt.nz/news/2015/01/statement-about-banks-closing-accounts-of-money-remitters> at 4.

[1162] Ibid.

[1163] Ibid.

[1164] New Zealand Treasury *Treasury Report: Update on Remittances to the Pacific* (T2015/34, 12 March 2015) <http://www.treasury.govt.nz/downloads/pdfs/oia/oia-20150421.pdf> at 5.

[1165] Ken C Ooi and Ross P Buckley "Pacific Injustice and Instability: Bank account Closures of Australian Money Transfer Operators" (2014) 25 Journal of Banking and Finance Law and Practice 243, 245 and Reserve Bank of New Zealand "Statement about Banks Closing Accounts of Money Remitters", above n 1161.

[1166] Ooi and Buckley, ibid, and Reserve Bank of New Zealand "Statement about Banks Closing Accounts of Money Remitters" ibid.

[1167] Reserve Bank of New Zealand "Statement about Banks Closing Accounts of Money Remitters", ibid.

> to conduct customer due diligence on those customers. Although the AML/CFT Act requires banks to have adequate and effective procedures in place to manage and mitigate money laundering and terrorism financing risks posed by their customers, that obligation does not require banks to cease to provide services to an entire category of customers.

It appears, however, that some banks withdrew MTOs' access not because of the AML/CFT, but rather under commercial pressure by US banks: the international remittances often went via US-based correspondent banks, and the latter were concerned with US law, which is arguably even stricter than New Zealand's.[1168]

In response to the closure of MTOs, many New Zealand banks stepped into the breach. For example, ANZ offers a type of remittance service for remittances that use internet banking to send money to bank accounts in Samoa, Vanuatu and Tonga.[1169] Although the New Zealand Treasury could not measure the actual impact on prices of the reduced MTO competition, it believed "that fundamental market behaviour and recent studies of other markets support a view that the closure of MTOs is contributing to an increase in remittance costs to the Pacific".[1170] The Treasury expressed particular concern on the limited access to banking services outside main Pacific Island cities, which can leave MTOs the sole viable means of transfer.[1171] Fortunately MTOs have been able to reinsert themselves and offer substantially cheaper services than the banks.[1172]

By parallel reasoning, if cryptocurrency exchanges are simply dealing with people with New Zealand bank accounts, and customers are making and receiving payments from New Zealand bank accounts, there is no justification for removing an exchange's own transactional bank accounts. The only justification would be if an exchange's conduct was shown to be a potential breach of the AML/CFT requirements, for example, if the exchange was purchasing cryptocurrencies from sources which could be engaged in money laundering or terrorism financing. Thus if an exchange is purchasing from exchanges overseas, such as Coinbase, which have rigorous identity verification processes it would be difficult to find concerns in relationship to New Zealand AML/CFT requirements.

9.2 Recommendations

The following sets out the report's recommendations with brief explanations of each.

9.2.1 Recommendation 1 – The New Zealand Government should continue to allow cryptocurrencies to be traded as well as used for the payment of goods and services within and outside New Zealand.

Given that most countries have not attempted to ban cryptocurrencies, and they are being used by at least one large corporation in New Zealand, New Zealand should continue to allow them both to be traded as well as for the payment of goods and services within and outside New Zealand. Any effort to ban the use of cryptocurrencies is unlikely to work and would put New Zealand businesses at a distinct advantage to businesses in more progressive and fintech-friendly countries such as Japan, Australia and the UK. Also, as the use of cryptocurrencies grows and other countries begin to

---

[1168] New Zealand Treasury, above n 1164, at 6–7.
[1169] Pattrick Smellie "How Anti-money-laundering Measures can Hurt Migrant Workers" *Listener* (online ed, 22 July 2016) <http://www.noted.co.nz/money/investment/how-anti-money-laundering-measures-can-hurt-migrant-workers/>.
[1170] New Zealand Treasury above n 1164, at 5; World Bank *Report on the Remittance Agenda of the G20* (2014) <http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1400093105293/GPFI_Remittances_Report_Final072014.pdf>.
[1171] New Zealand Treasury above n 1164, at 5.
[1172] On 25 April 2018, the cost of sending USD 200 from Samoa to New Zealand ranged from $5.51 with Klickex, an MTO, to $45.91 with ASB. Both took 3–5 days. See <https://www.sendmoneypacific.org/>.

issue CBDCs, currency competition will be beneficial to New Zealand's economy, since it has been argued that:[1173]

> … the threat of competition from private monies imposes market discipline on any government that issues currency. If a central bank, for example, does not provide a sufficiently "good" money, then it will have difficulties in implementing allocations. This may be the best feature of cryptocurrencies. In a world in which we can switch to Bitcoin or Ethereum, central banks need to provide, paraphrasing Adam Smith, a tolerable administration of money. Currency competition may have a large upside for human welfare after all.

9.2.2 Recommendation 2 – New Zealand-based cryptocurrency exchanges should be encouraged and clear guidance provided as to their AML/CFT obligations by both the DIA and the FMA (that is, follow Australia's example).

It is generally safer for individuals and businesses to deal with cryptocurrency exchanges based in New Zealand than ones based overseas. Arguably Japan and now Australia have clearly stated the requirements for cryptocurrency exchanges in terms of AML/CFT, and they have not created a bespoke regulation as occurred in New York with BitLicense. New Zealand regulators, principally the DIA, do not need to amend their laws for cryptocurrency exchanges; rather, they need to provide more guidance on what those laws are specifically for cryptocurrency exchanges. Australia serves as a good example.[1174]

9.2.3 Recommendation 3 – Greater advice and therefore protection should be provided to consumers on cryptocurrencies by the FMA, DIA and other organisations.

Despite regulators and others preferring that people not purchase cryptocurrencies, some people will. It is preferable that those who do buy cryptocurrencies do so in ways where risk is reduced. To that end it is preferable that New Zealanders purchase cryptocurrencies from New Zealand exchanges rather than ones based overseas, which may not be regulated.

Somewhat surprisingly as the supervisor for exchanges, the DIA has no information for consumers and businesses wishing to purchase and use cryptocurrencies. The FMA does have some useful information, although it could be improved.[1175] In particular we recommend that on the FMA's page "Cryptocurrencies":[1176]

a. The statement "Many online exchanges are unregulated", while true, could be clarified so that it reads "many online exchanges that are based outside New Zealand …". While later on the page it does specifically state that "Many overseas cryptocurrency exchanges are unregulated", this does not undo the effect of the initial statement.
b. Under the subsection beginning "Make sure any New Zealand exchange you use" the page states to check that the exchange is registered on the Financial Service Providers Register (FSPR). It would be useful for a link to the register (<https://fsp-register.companiesoffice.govt.nz/>) to be provided.
c. The advice to make sure such an exchange "holds your New Zealand dollars in a trust account" is interesting. How can a consumer check whether their New Zealand dollars are held in a trust account?

[1173] Fernández-Villaverde, above n 1140.
[1174] See, for example, Australian Transaction Reports and Analysis Centre "Enrolment and Registration" <http://www.austrac.gov.au/businesses/enrolment-and-registration/enrolment-and-registration>; Australian Transaction Reports and Analysis Centre "Are you a Digital Currency Exchange Provider?" (24 January 2018) <http://www.austrac.gov.au/news/are-you-digital-currency-exchange-provider>; and the extremely useful Australian Transaction Reports and Analysis Centre "Chapter 5B - Digital currency exchange registration requirements" <http://www.austrac.gov.au/chapter-5-dce-registration-requirements>.
[1175] Financial Markets Authority "Cryptocurrencies", above n 557.
[1176] Ibid.

> Even if an exchange states that customers' money is being held in a trust account how can the customer verify that this is in fact occurring?[1177]

Another change would also be beneficial. The website for the Insurance & Financial Services Ombudsman[1178] could be improved to help consumers. For example, the searching function for participants of the scheme appears to work only for registered company names and not the name under which they trade. For example, entering the name of the exchange "Dasset" produced no results. However, when the word "digital" was typed in a box came up with "Digital Asset Exchange Limited" and on clicking further it states "Trading as Dasset" and provides a link to Dasset's website.

9.2.4 Recommendation 4 – Cryptocurrency exchanges and blockchain businesses that comply with AML/CFT and other requirements must have access to bank accounts with New Zealand banks.

Blockchain businesses and in particular cryptocurrency exchanges experience difficulties in securing and keeping transactional bank accounts, and this is a significant impediment for those businesses. However, some New Zealand-based blockchain companies and even cryptocurrency exchanges do have bank accounts with large New Zealand banks. This shows that it is possible for banks to provide such services and still meet their AML/CFT obligations. It would greatly aid both the blockchain and banking industries for the banks to share at all levels the experience gained in onboarding exchanges and other blockchain businesses.

RBNZ needs to give the banks a clear signal that if the current practice of debanking without good cause continues then it will consider regulation. However, while the ability of a regulator to prosecute may look good on paper, in reality regulators do not investigate every complaint, much less prosecute every alleged infraction. Likewise, granting rights to those wishing to set up cryptocurrency exchanges or those cryptocurrency exchanges that have bank accounts looks good in theory but in practice does little, and most exchanges and blockchain businesses lack the resources to litigate against a bank.[1179] One possibility is for the Banking Code of Practice to be amended so that contrary to the current situation, where banks can close bank accounts for any reason,[1180] if the business is a cryptocurrency exchange the bank must show good reason for any closure. Similarly the opening of a bank account could not be refused for arbitrary reasons. Alternatively, either the Government banker, Westpac, or else Kiwibank could be required to provide bank accounts for cryptocurrency exchanges and others dealing with cryptocurrencies, thus becoming a banker of last resort.

One way to provide more comfort to banks in terms of their AML/CFT requirements is to follow Japan and Australia's lead in simplified regulation of exchanges. Note: if that move was made it would require the same speed of processing applications as is offered in Japan.[1181] Current New Zealand exchanges should be permitted to operate while their applications are processed.

9.2.5 Recommendation 5 – Merchants must be able to accept cryptocurrency payments by people or organisations for under NZD 100 or payments made through a New Zealand exchange (or

---

[1177] One of blockchain's promises is that it will allow people to verify that assets are being held, and where.
[1178] <https://www.ifso.nz/>.
[1179] Albeit there is the occasional exception as one Israeli cryptocurrency has gone to court to attempt (so far successfully) to keep its bank account: "Israeli Supreme Court Forbids Bank Account Closure of Crypto Exchange" *Trustnodes* (27 February 2018) <https://www.trustnodes.com/2018/02/27/israeli-supreme-court-forbids-bank-account-closure-crypto-exchange>.
[1180] New Zealand Bankers Association "Banking Code of Practice" at [9] "Either you or we may end any banking relationship at any time…" <http://www.nzba.org.nz/consumer-information/code-banking-practice/code-of-banking-practice/3-products-and-services/>; and see Banking Ombudsman Scheme "Closing Accounts" <https://bankomb.org.nz/guides-and-cases/quick-guides/bank-accounts/closing-accounts/>.
[1181] As noted above at n 909–910 and accompanying text, New York's BitLicence has not worked, as the processing of applications has taken years.

an overseas exchange) that complies with AML/CFT requirements, without the merchants losing their bank accounts.

Another change required is to ensure that merchants are able to accept cryptocurrencies from their customers and in turn to use those cryptocurrencies, whether to convert to fiat or to purchase goods or services. The banks have made it clear to a number of merchants that if they wish to accept cryptocurrencies from their customers they will lose their bank accounts. Granted, the concerns are based on AML/CFT fears, yet the same banks allow those merchants to accept cash from their customers.

One way to break the impasse is to stop banks from preventing merchants accepting cryptocurrency payments made through cryptocurrency exchanges or wallets that are registered in New Zealand, or ones registered overseas that meet the same or similar standards. Examples would be those registered in Australia and Japan, as well as those registered in the US, such as Coinbase. The cryptocurrency exchanges would take care of the AML/CFT requirements.[1182] Also, once digital identity has been sorted out, people could use their digital identity to sign transactions,[1183] a system that would be less open to abuse and money-laundering concerns than is currently the situation with cash.

9.2.6 Recommendation 6 – GST is removed from cryptocurrencies that are used for the payment of goods and services.

There remains considerable uncertainty over the taxation of cryptocurrencies in New Zealand in respect to GST. Businesses wishing to accept payments in cryptocurrencies for goods and services are potentially subject to GST. So too are New Zealand exchanges that provide exchange services to New Zealand customers. This double taxation cannot be justified, even less so when Australia changed its GST on cryptocurrencies to remove GST from certain cryptocurrencies, such as such as bitcoin, Ethereum, Litecoin, Dash, Monero, ZCash, Ripple, and YbCoin.[1184] Not all of the Australian changes should be adopted, however. Stable coins, cryptocurrencies that are backed by other currencies and assets, including fiat and other cryptocurrencies, are not GST excluded in Australia. The purpose of such stable coins is entirely for use as currencies and they should also be excluded from GST in New Zealand.

9.2.7 Recommendation 7 – The IRD clarifies other taxation rules around the use of cryptocurrencies.

The treatment of income for ICOs needs clarification. Ideally income received through ICOs should, in appropriate circumstances, be able to be deferred to subsequent years.

9.2.8 Recommendation 8 – The IRD should accept cryptocurrencies for the payment of taxes.

Requiring the IRD to accept cryptocurrencies as payment for taxes on income gained on the trading cryptocurencies should have the effect of collecting more tax. For, paying tax in cryptocurrency is arguably psychologically easier than paying in fiat currency. It would also ensure that there are exchanges in New Zealand so that the IRD can use those exchanges, thus driving further economic activity in New Zealand and not offshore. In addition, for New Zealand to be seen as a progressive

---

[1182] Omri Marian "A Conceptual Framework for the Regulation of Cryptocurrencies" (2015) 82 University of Chicago Law Review 53, at 58.
[1183] At 62.
[1184] Australian Taxation Office "GST and Digital Currency" <https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency/>.

country the IRD should also allow the payment of cryptocurrencies for all taxes.

9.2.9 Recommendation 9 – The RBNZ should trial the creation and issuance of a New Zealand CBDC.

In one comment the RBNZ's paper on cryptocurrencies hinted itself rather cryptically at work on a CBDC:[1185]

> work is currently under-way to assess the future demand for New Zealand fiat currency and to consider whether it would be feasible for the Reserve Bank to replace the physical currency that currently circulates with a digital alternative. Over time, analysis associated with this project will filter through into the public domain.

While subsequent work and announcements have shown that the RBNZ has no immediate plans to trial a CBDC,[1186] when the RBNZ does issue a CBDC it should be backed one-to-one by the New Zealand dollar.[1187] The CBDC would be a retail CBDC. The question, of course, is would the retail banks handle the CBDC, or could holders simply have a bank account with the RBNZ? Requiring holders of a New Zealand CBDC to have a bank account with either a New Zealand retail bank or the RBNZ would greatly reduce the utility of a New Zealand CBDC for cross-border payments.

9.2.10 Recommendation 10 – Although wider than cryptocurrencies, New Zealand should follow countries such as the UK and Australia, and create a regulatory sandbox to ensure that the regulators work alongside fintech companies. While one government department could be the primary sponsor, it would be advantageous for it to be a cross-agency initiative. That way the regulators can see first-hand the successes and roadblocks that fintech companies are experiencing.

New Zealand needs to ensure that it is not left behind other countries. As Kiwibank's Digital Advisor, Peter Fletcher-Dobson, has been reported as saying, "New Zealand needs to get a move on, otherwise we'll miss out on the massive opportunity presented by cryptocurrencies" and "regulatory sandboxes should potentially be created".[1188]

10. Conclusion

Cryptocurrencies are a challenge to conventional thinking, but as this report has shown, the genie is out of the bottle and many, including central banks, are well aware of the transformative potential that blockchain promises. Indeed, the use of blockchain for the store and movement of value extends well beyond mere payments. The question is how best to embrace the opportunities that technology provides and reduce the disadvantages. While it is extremely unlikely that bitcoin or another cryptocurrency, or even a CBDC, will be the sole world currency, we may be seeing a return to the past with a proliferation of alternative currencies that people can choose to use. Prior to 1934 New Zealand was awash with different currencies.

Large international corporations such as IBM are resorting to cryptocurrencies to move value around the world because fiat currencies are not fit for purpose. Central banks have realised that DLT offers compelling advantages over existing technology and many are actively working on issuing their own CBDCs. New Zealand needs to join these international moves and work on the introduction of a CBDC, even if it is initially for a relatively small amount. New Zealand prides itself on being innovative, nimble and agile. For New Zealand not to issue a CBDC would be to forgo some of the

---

[1185] Kumar and Smith, above n 310, at 28.
[1186] See Amber Wadsworth "Decrypting the Role of Distributed Ledger Technology in Payments Processes", above n 682; Amber Wadsworth "The Pros and Cons of Issuing a Central Bank Digital Currency", above n 682; Wadsworth "What is Digital Currency?", above n 69 and Bascand "In Search of Gold: Exploring Central Bank Digital Currency", above n 682.
[1187] Anderson, above n 1135.
[1188] MacManus, above n 1152.

benefits cryptocurrencies and blockchain offer to the New Zealand economy, and would hamper the ability of New Zealand businesses to compete internationally.

Finally, New Zealand's current largely hands-off treatment of businesses attempting to deal in cryptocurrencies is not only harming those businesses or potential businesses; it is also detracting from the country's ability to fully embrace the opportunities that fintech provides. Without changes, New Zealand risks losing its reputation as an innovative, agile and nimble country.

Abbreviations

ACCC Australian Competition and Consumer Commission
ADI Authorised Deposit-taking Institution (Australia)
AI Artificial Intelligence
AML Anti-Money Laundering
AML/CFT Anti-Money Laundering/Counter Financing Terrorism (equivalent to AML/CTF)
AML/CTF Anti-Money Laundering/Counter Terrorism Funding
ASIC Australian Securities and Investment Commission
API Application Programming Interface
ASX Australian Securities Exchange
ATM Automated Teller Machine
ATO Australian Taxation Office
AUD Australian Dollar
AUSTRAC Australian Transaction Reports and Analysis Centre
BBA British Bankers' Association
BCDR Business Continuity and Disaster Recovery
BIS Bank for International Settlements
BoE Bank of England
BPI Bitcoin Price Index
BTC Bitcoin
CBDC Central Bank Digital Currency (the standard abbreviation for central bank-issued cryptocurrency, though also sometimes referred to in other sources as CBIC)
CDBO California Department of Business Oversight
CDD Customer Due Diligence
CFT Counter Financing Terrorism
CFTC Commodities Futures Trading Commission (US)
CGT Capital Gains Tax
Chess Clearing House Electronic Sub-register System (Australia)
CRA Canada Revenue Agency
CT Corporation Tax
CTF Counter Terrorism Funding
DAC Decentralised Autonomous Corporation
DAO Decentralised Autonomous Organisation
DDoS Distributed Denial of Service
DIA Department of Internal Affairs (New Zealand)
DLT Distributed Ledger Technology
ERC Economics References Committee (Australia)
ETH Ether
ETF Exchange Traded Fund
EU European Union
EVM Ethereum Virtual Machine
FATF Financial Action Task Force
FBI Federal Bureau of Investigation (US)
FBT Fringe Benefit Tax
FCA Financial Conduct Authority (UK)
FCS Financial Claims Scheme (Australia)
FinCEN Financial Crimes Enforcement Network (US)
FINTRAC Financial Transactions and Reports Analysis Centre of Canada
FIU Financial Intelligence Unit (New Zealand)
FMA Financial Markets Authority (New Zealand)
FTC Federal Trade Commission (US)
GPSG Global Payments Steering Group
GST Goods and Services Tax
HMRC Her Majesty's Revenue and Customs (UK)
HTTP Hyper-Text Transfer Protocol

ICO Initial Coin Offering
IMF International Monetary Fund
IP Internet Protocol
IPFS Interplanetary File System
IRD Inland Revenue Department (New Zealand)
IRS Internal Revenue Service (US)
KYC Know Your Customer
LLC Limited Liability Company
MSB Money Services Business
MTO Money Transfer Operator
NAB National Australia Bank
NFC Near Field Communication
NYSDFS New York State Department of Financial Services
NZD New Zealand Dollar
OFAC Office of Foreign Asset Control (US)
P2P Peer-to-peer
PAYG Pay As You go (Australia)
PBOC People's Bank of China
PII Personally Identifiable Information
PIN Personal Identification Number
PKI Public Key Infrastructure
PoS Proof-of-Stake
PoW Proof-of-Work
PPC Peercoin
PPP Purchasing Power Parity
QR (code) Quick Response (code)
RBA Reserve Bank of Australia
RBNZ Reserve Bank of New Zealand
SAR Suspicious Activity Report
SEC Securities and Exchange Commission (US)
SMS Short Message Service
Spv Simplified Payment Verification
SWIFT Society for Worldwide Interbank Financial Telecommunication
TCO Transnational Criminal Organization
TCP/IP Transmission Control Protocol/Internet Protocol
TDB Texas Department of Banking
TGE Token Generation Event
USD United States Dollars
VAT Value Added Tax

Glossary

51 per cent attack: more than half the computing power on a **blockchain** is controlled by a single **miner** or group of miners. That amount of power theoretically makes them the authority on the network and gives them power to (1) interfere with issuing and confirming transactions, (2) double spend bitcoin or (3) prevent other miners from mining valid blocks.

Address: an address is used to send and receive transactions. It contains a string of alphanumeric characters, but can also be represented as a quick response code (**QR code**) that can be scanned. An address is also the **public key** in the pair of keys used by **cryptocurrency** holders to digitally sign transactions.

Airdrop: method of distributing **cryptocurrency** among a population, first attempted with **Auroracoin** in early 2014. More recently airdrops have been used to distribute cryptocurrency to people who hold certain **wallets** such as MyEtherWallet. Airdrops are a good way of getting **coins** out to a wide range of people and creating a network effect.

Altcoin: collective name for **cryptocurrencies** other than **bitcoin** – but the instances of its use are decreasing.

Anti-Money Laundering (AML): a set of procedures, required by laws or regulations, designed to stop the practice of **money laundering** (the converting of profits gained through illegal actions into legitimate assets). The procedures require considerable monitoring and reporting of suspicious activities.

API (Application Programming Interface): set of requirements that dictate how two pieces of software talk to each other. APIs are used commonly in **open banking**.

Application-Specific Integrated Circuit (ASIC chip): silicon chip specifically designed to do a single task. In the case of Bitcoin, ASIC chips are designed for **mining** (solving a very difficult mathematical problem).

ASIC: Australian Securities and Investment Commission.

ASIC chip: see **Application-Specific Integrated Circuit**.

ASIC miner: piece of equipment containing an **ASIC chip**, configured to mine for **bitcoin** as well as other **coins** such as Litecoin.

Asymmetric key algorithm: algorithm used to generate **public keys** and **private keys**.

Atomic swap: ability to swap two **cryptocurrencies**, for example, **bitcoin** and **Litecoin**, without needing to go through an **exchange**. The technology is at an early stage. Over time it will enable smaller blockchain**s** as information/transactions can pass between **chains**.

Auroracoin: altcoin designed for Iceland. Auroracoin aimed to restrict the movement of the currency outside of the country (capital flight).

AUSTRAC: Australian Transaction Reports and Analysis Centre.

Autonomous agent: software entity that carries out a set of tasks autonomously on an owner's behalf.

Bank Secrecy Act (BSA): initially adopted in 1970 in the US, established the basic framework for **anti-money laundering** obligations imposed on financial institutions. Among other things, it authorises the Secretary of the Treasury to issue regulations requiring financial institutions (including broker-dealers) to keep records and file reports on financial transactions that may be useful in investigations and prosecution of **money laundering** and other financial crimes.

Bit: sub-unit of a bitcoin – 1,000,000 bits is equal to one bitcoin; equivalent to one microbitcoin (**uBTC**).

Bitcoin (symbol BTC or ₿**):** first of the **cryptocurrencies** to use **blockchain** technology and at the time of writing (in 2018) the cryptocurrency with the highest market capitalisation as well as the most frequently used. Bitcoin is a system of digital cash (specifically a **decentralised cryptocurrency**) which allows peer-to-peer value transfer over the internet with no reliance on third parties. It is built on a new invention, a blockchain, which is a form of **decentralised ledger**. Bitcoin is essentially cash for the internet.

When used as “bitcoin”, ie in lower case, bitcoin refers to the cryptocurrency that is digitally traded between users. “Bitcoin”, capitalised, refers to both the open source software used to create the cryptocurrency and the **Peer-to-Peer (P2P)** network formed as a result.

Bitcoin ATM: automated teller machine that enables a person to exchange **bitcoin** and cash. Many Bitcoin ATMs are one-directional, meaning customers can buy bitcoins, but cannot sell them (or vice versa). A bi-directional machine does both.

Bitcoin Cash (BCH): cryptocurrency created on 1 August 2017 when the Bitcoin **blockchain** was **forked**.

Bitcoin Gold (BTG): cryptocurrency created on 24 October 2017 when the Bitcoin **blockchain** was **forked**.

BlackCoin: **altcoin** which uses a **proof-of-stake (Pos) consensus** mechanism.

Block: group of transactions recorded cryptographically on the **blockchain** that contains and confirms data. Blocks are linked together in a linear sequence to form a blockchain.

Block halving: when the **block reward** for miners is halved; thus the payoff for mining blocks reduces over time until the finite amount of **cryptocurrencies** has been mined. (Applies only to those cryptocurrencies such as **bitcoin** that have a finite supply.)

Block header: contains information about a **block**, such as the **hash** of the previous **block header**, its version number, the current target, a **time stamp**, and a **nonce**.

Block height: a **block's** location in the **blockchain**, with blocks "higher" up being more recent.

Block reward: cryptocurrency awarded to a **miner** for solving a **block**.

Block time: the average length of time it takes to create a **block**. In **Bitcoin** the block time is around 10 minutes; in **Ethereum** it is around 14 seconds.

Blockchain: in terms of **cryptocurrencies**, the ledger of all transactions.

Blockchain identity: set of cryptographically verifiable interactions sharing the property that they were all created by the same person.

Botnets: group of two or more computers and/or mobile devices that are controlled and/or updated remotely for an illegal purpose. Botnets can be used to perform **denial-of-service (DOS)** attacks**,** send spam email, and host illegal content; they may aid in most other types of online criminal behaviour.

Brain wallet: wallet which uses a long string of words to secure its **coins**. This "passphrase" can be memorised, allowing the wallet owner to spend bitcoin by simply remembering the passphrase.

BTC: symbol used for **bitcoin**.

Byzantine Generals' Problem: metaphor for a problem in consensus making when communication channels cannot be trusted. Two generals for the Byzantine Empire, who are on opposite sides of an enemy city, want to attack it. To increase the chances of success, the generals need to agree to strike at the same time. They use a messenger to communicate with each other to decide the time of attack. The only way for the messenger to get between camps is to go through the enemy city. The problem is that neither general can trust the information as it may have been tampered with, so "ATTACK AT 1pm" might be changed to "ATTACK AT 6pm". **Bitcoin** solved the problem by adding some nonsense code at the end of each message (for example, "tu78jaIl0967"), called a **nonce**. Thus the message would be "ATTACK AT 1pm tu78jaIl0967. The generals have already agreed that the **hash** of the message including the nonce must create a number than begins with at least ten zeros: if it does not then the message has been tampered with. The general who is broadcasting the message spent hours running their computer trying a series of random nonces until finding one where the message and the nonce created a hash that began with ten zeros. All the receiving general needs to do is to hash the message received and if it starts with at least ten zeros then the message has not been tampered with.

CAD coin: experimental **CBDC** trialled in Canada.

Capital controls: local measures such as transaction taxes, limits or prohibitions that a government can use to regulate flows from capital markets into and out of the country.

CBDC: central bank-issued cryptocurrency (referred to in some sources as central bank-issued digital currency, hence the initials). A **cryptocurrency** that has been issued by a government.

Central bank: national authority that conducts monetary policy and inter alia regulates **retail banks** that operate within that country. New Zealand's central bank is the Reserve Bank of New Zealand (RBNZ).

Chains: shorthand name for a **blockchain**. See also **off-chain** and **on-chain**.

Charge-back: credit card payment made to a merchant that is reversed because the transaction was fraudulent.

Client: piece of software that transforms a computer into a **node** in the **Bitcoin** network. Clients help in the generation of **private keys**, security, and payment. Clients can be full, light or mobile. Full clients store the entire **blockchain** whilst light or mobile clients only store parts of it.

Cloud: type of computing that relies on shared computing resources rather than storing that information and computer programs on local servers or personal devices. The services are delivered and used over the internet.

Cloud hashing: system whereby people can rent computer power from someone in the **cloud** to **mine bitcoin** or other cryptocurrencies. Cloud hashing is also the generic name for a business which offers this service (also called **cloud mining**).

Cloud mining: see **cloud hashing**.

Coin: informal term that refers to a **cryptocurrency** that can be used as a means of payment, for example, **bitcoin**, **Ether**, **Monero**, **Zcash**, **Dash** and so on.

Coinbase: **exchange** based in the United States.

Cold storage: offline storage of a **cryptocurrency**. Cold storage provides a high level of security: cryptocurrency stored off-line is not susceptible to attack via a hacker getting into the network. Cryptocurrency **exchanges** normally should hold most of their clients' cryptocurrency in cold storage.

Collective mining: see **mining pool**.

Coloured coins: the coloured coins protocol is a project built on top of the **Bitcoin blockchain**. It aims to facilitate the trading of assets beyond bitcoin such as financial instruments, gold, or property using Bitcoin's underlying payment infrastructure. Coloured coins are used to tie ownership to a real world asset, for example, the ownership of a car. There is no need for a whole bitcoin to be used; a few **satoshi** would be sufficient.

Computational infeasibility: A process is computationally infeasible if it would take an impracticably long time for someone to hack, for example, millions of years.

Confirmation: act of **hashing** a transaction successfully into a **block** and confirming its validity. For **Bitcoin** a single confirmation takes around 10 minutes to complete, which is the average length of time for a block to be hashed. However, some transactions because of their sensitivity or size may require multiple confirmations, meaning that more blocks must be hashed and added to the **blockchain** after the transaction's block has been hashed. Each time another block is added to the **blockchain** after the transaction's block, the transaction is confirmed again.

Consensus: agreement among a network as to the state of the network.

Consensus mechanism: process where participants in the network decide whether a transaction is valid. Common consensus mechanisms are **proof-of-work** and **proof-of-stake**. Others include **proof-of-importance**, **delegated proof-of-stake** and **leased proof-of-stake**.

Corda: a **permissioned blockchain** that is **open source**.

Cosigner: an additional person or entity that has partial control over a **wallet**.

Cryptocurrency: a **digital currency** which uses encryption to regulate the generation of its units and also to verify the transfer of its units. Cryptocurrency operates independently from **central banks**, unless it is a **CBDC**.

Cryptoeconomics: emerging field which has no set definition. It can be seen as studying the protocols that govern the production, distribution and consumption of goods and services in a decentralised digital economy. It draws from many different disciplines, most notably economics.

Cryptography: mathematical codes and ciphers that can be used to conceal information and are employed to verify and secure **cryptocurrency** transactions.

CSRNG: abbreviation for "Cryptographically Secure Random Number Generator", used in **private key** generation for **wallets**.

DAO (Decentralised Autonomous Organisation, and not to be confused with The DAO below): organisation run through rules encoded as computer programs called **smart contracts**. The **cryptocurrency DASH** is run as a DAO. **Bitcoin** can be seen as a very early and primitive form of DAO. DAOs form part of the emergent field of **institutional cryptoeconomics**. Decisions about governance are hard-coded at the outset.

Darkweb: part of the internet that is accessible by using the **Tor** browser. Users of the Darkweb are anonymous, unless they voluntarily disclose who they are. The Darkweb is used by some people in repressive countries who would not be able to communcate on the internet for fear of being identified. Parts of the Darkweb are also used for illegal activity such as illegal **peer-to-peer** file sharing and the purchase of drugs and other illegal goods.

Dash: cryptocurrency designed specifically for payments.

Debanking: closing of a customer's bank account by the bank without asking the customer.

Debit card: similar to a credit card as it can be used anywhere that accepts credit cards, including with online merchants. But unlike with a credit card, where you can borrow money, the user of a debit card is limited to

the amount they have loaded on the card. Thus a debit card is similar to an **eftpos card**, but with the advantage of being usable for online purchases. Merchants prefer to accept eftpos cards as these incur no additional charges when receiving payment, whereas debit cards do.

Decentralised: there is no one person or group of people controlling a **blockchain**, but rather varying levels of decentralisation. **Bitcoin** is quite decentralised; indeed, that is one reason why making changes is hard. Other blockchains are not so decentralised – for example, **Ethereum**.

Decentralised Application (Dapp): computer program run by many people which either uses or creates a decentralised network sitting on a **blockchain** for some specific purpose, for example, connecting buyers and sellers in a marketplace, creating a digital identity and online file storage and so on. Currently there are a limited number of Dapps, but that will change over time.

Decentralised Autonomous Corporation (DAC): a **DAO** whose purpose is to run more like a company rather than a collection of individuals combining for a project**.**

Decentralised exchange: **exchange** for **cryptocurrencies** where the exchange does not keep or handle the cryptocurrency. Instead **smart contracts** are used so that the people wishing to trade **coins** trade directly. **EtherDelta** is one example.

Deep Web: parts of the internet that cannot be accessed using ordinary search engines and include organisations' intranets and other websites that are protected by passwords. Some parts of the Deep Web are used for criminal activity and these are called the **Darkweb**.

Delegated proof-of-stake (DPoS): **coin/token** owners can elect a list of **nodes** that can have ability to secure the network; the people so delegated are called **Witnesses**. DPoS avoids the large computing and electricity cost involved in **proof-of-work.** It also keeps the Witnesses working hard and honestly because if they act in a way others do not like they can have their Witness status removed.

Denial of service (DoS): cyberattack in which the attackers attempt to make a server or a network unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet by sending excessive messages to the server or network.

Derisking: closure of bank accounts and other financial services due to concerns of AML/CFT.

Deterministic wallet: see **HD wallet**.

Difficulty: the amount of computing power needed to mine a **cryptocurrency** using **proof-of-work** fluctuates over time depending on the computing power on the network. If the price of a cryptocurrency such as **bitcoin** rises more people will start to **mine** it and the "difficulty" in this technical sense will increase. If the computing power decreases, for example, the price of bitcoin falls and miners stop mining because it is uneconomic, the difficulty decreases to encourage more computing power to re-enter the network.

Digital currency: often used to refer to **cryptocurrency**, especially in the term **CBDC** for central bank-issued digital currency, but more accurately used to describe all **fiat currency** other than cash.

Digital signature: technique that binds a person/entity to their digital data. This process can be used to attach to an electronic message a digital code that is unique to the "signer" of the message.

Distributed ledger: database that has no central administrator or centralised data storage. Instead the ledger is shared across a network of multiple sites, geographies or institutions. A **blockchain** is one form of a distributed ledger.

Dogecoin: cryptocurrency which started as a joke in response to **Bitcoin**. It has better features than some of the earlier cryptocurrencies: for example, Dogecoin's **block** confirmation time is just under a minute, compared to 2.5 minutes on **Litecoin** and 10 minutes with **Bitcoin**. Unlike the currency bitcoin, there is no maximum amount to be issued.

Double spending: attempting to spend **cryptocurrencies** twice. For example, Jane may attempt to send Felix 0.1 **bitcoin** from a **wallet** that holds only 0.12 bitcoin, but then also try to send Bob 0.1 bitcoin: that is, Jane is attempting to spend the 0.1 bitcoin twice. Both transactions go into the **mempool**. If the transaction to Felix is picked up in the next **block** and the one to Bob is not, Felix will receive the bitcoin and Bob will not. For, when the transaction to Bob is picked up the **nodes** will see that Jane no longer owns the bitcoin. However, if both transactions are picked up for the same block the transaction that gets verified first will go into the block. Occasionally, due to the size of the network, two blocks can be mined at the same time, one containing the transaction to Felix and the other the transaction for Bob. In effect there are now two chains and the **miners** have to choose which to mine. In this process one chain will win and the blocks on the other chain will be discarded, so either Felix or Bob will lose out. Because of this possibility of blocks being discarded, if a person

wants to accept bitcoin in a transaction it is sensible to wait until six blocks have been confirmed. After six block confirmations (for Bitcoin, a minimum of one hour) people can be confident about the payment. For small purchases such as a cup of coffee, waiting an hour is not feasible, but for larger purchases it is prudent. Bitcoin's relatively slow block confirmations are a major reason many do not see it as being a viable payments system. Although the **lightning network** has been designed to attempt to allow Bitcoin to operate as a payments system.

Dust transactions: transactions so small that they are considered "spam" by the network. They are not relayed, to stop people accidentally or deliberately clogging the **blockchain**.

Eftpos card: method of making payments without needing to carry cash. Eftpos can only be used in stores or at ATMs. Money is taken directly from the user's bank account. Sometimes confused with **debit card**. Increasingly New Zealand banks are issuing debit cards instead of eftpos cards.

Electronic payment systems: means of transferring money among parties to facilitate e-commerce and operate using **fiat currency** or **cryptocurrency**.

Elliptic Curve Digital Signature Algorithm (ECDSA): used to sign many transactions in the **Bitcoin**, **Ethereum** and other **blockchains**.

E-money: fiat currency that has been digitised. Thus money in a bank account is e-money, but cash (paper notes) is not.

Encryption: a method of masking data using **cryptography** to prevent unauthorised visibility during transfer or storage.

EOS: cryptocurrency that will be able to be used to run **smart contracts** (once it is operational), similar to **Ethereum** but more advanced. Unlike Ethereum it will not charge **transaction fees**. If Bitcoin was version 1.0 of **blockchain**, and Ethereum 2.0, then if it lives up to its promise, EOS will be 3.0.

ERC-20 token: **token** that complies with a list of rules that an **Ethereum** token has to implement. Once the rules are met the token can be used on the **Ethereum ecosystem**. Most **ICOs** have used ERC-20 tokens, with many then going on to create their own **blockchains**. **EOS** is one example.

Escrow: act or state of holding funds or assets in a third-party account until the details of the trade can be acknowledged and approved by the two principal parties. Reduces the risk of the payer or payee committing fraud. **Smart contracts** can also serve as an alternative to a third party holding the funds – which saves reliance on trusting a third party and the associated higher transaction costs. If a smart contract is used the funds will be paid out automatically by the smart contract once the conditions have been met.

ETF (Exchange-Traded Fund): investment funds traded on stock markets that track the price index of an underlying asset. **Bitcoin** ETFs have been proposed in the US.

ETH: call sign for the **Ethereum coin**.

Ether: a **cryptocurrency**. Ether (**ETH**) is the internal network currency for the **Ethereum blockchain,** which is a **token** or **coin** used on the Ethereum network, also sometimes called an **altcoin**.

EtherDelta: an example of a **decentralised exchange**.

Ethereum: a public **blockchain**-based distributed computing platform, which **smart contracts** are being written on. Ethereum provides a decentralised virtual machine, the **Ethereum Virtual Machine** (**EVM**). The native **token** for Ethereum is **Ether**.

Ethereum Classic: chain created as a result of a **hard fork** on the **Ethereum blockchain** following **The DAO** hack.

Ethereum Virtual Machine (**EVM**): attempt at making a decentralised world computer using **Ethereum**.

Exchange: central place for exchanging and/or storing **cryptocurrencies**. Some exchanges will only exchange **fiat currency** for **bitcoin** and sometimes a few other cryptocurrencies, such as **ether**. Other exchanges trade between a wide range of cryptocurrencies. Many exchanges are run by organisations and often they hold the **private keys,** which makes them attractive targets for hackers. If all that is sought is an exchange of cryptocurrencies, some services do not require the user to provide their private keys. Those services include Shapeshift and Changelly. Increasingly **decentralised exchanges** are being set up which use **smart contracts** to provide a market place where people can transact without revealing their private keys or knowing who they are transacting with. However, decentralised exchanges are often difficult to use.

Fee: see **transaction fee**.

Fiat currency: government-issued currency such as the New Zealand dollar, Australian dollar, US dollar, Chinese yuan and so on.

FinCEN (Financial Crimes Enforcement Network): a bureau of the United States Treasury Department dedicated to combating financial crime and **money laundering** and maintaining national security.

Fork: split in the **blockchain** producing two different blockchains upon which **miners** can work. Forks can occur if software updates are incompatible or if developers decide that changes must be made to the programming of a blockchain. The term can also describe a separate **cryptocurrency** which has been split from the main blockchain, such as Namecoin being a "fork" of **Bitcoin**. Both **Bitcoin Cash** and **Bitcoin Gold** were **hard forks** of Bitcoin. **Ethereum Classic** is a fork of **Ethereum**. When Bitcoin and **Ethereum** were forked to create respectively Bitcoin Cash, Bitcoin Gold and Ethereum Classic all those people holding Bitcoin or Ethereum received the same quantity of the new cryptocurrency as they held of Bitcoin (for Bitcoin Cash and Bitcoin Gold) and Ether (for Ethereum Classic).

Frictionless: a payment system is "frictionless" when there are zero transaction costs or other restraints on trading. **Atomic swaps** are frictionless.

Gas: internal pricing for running a transaction or contract in **Ethereum**. The term "gas" is simply the ether cost you have to pay to get your Ethereum message or transaction executed.

Genesis block: the first **block** in a **blockchain**.

GitHub: website where developers post **open source** software and other material. Having access to the software allows others to collaborate on improving it, copying it (since it is open source) and also for others to assess whether the project is viable.

GPU (Graphics Processing Unit): specialised processor originally designed for the high graphics requirements of computer games. **GPU**s are also used to **mine cryptocurrency** since they outperform CPUs. **ASIC miners** have superseded GPUs.

Hard fork: see **fork**.

Hardware wallet: wallet which stores a person's **public key** and **private key** offline on hardware devices, such as a **Trezor**. Hardware wallets are protected by a PIN so even if a person finds a hardware wallet they cannot spend the **cryptocurrency** unless they know the PIN.

Hash: mathematical process that takes a variable amount of data and produces a shorter, fixed-length output which is a long series of letters and numbers. A hashing function has two important characteristics. First, it is mathematically difficult to work out what the original input was by looking at the output. Second, even the slightest change to the input will produce an entirely different output. If even a full stop in a document was changed to a comma the hash will be different, instantly showing that the document has been changed. Whole documents are not normally stored on public **blockchains** because of their size and concerns about making the blockchain too large; instead, a hash of a document is stored. The documents themselves are often stored on **IPFS**. With **permissioned blockchains**, where storage is less of a problem, whole documents are often stored.

Hash function: a hash function takes an arbitrary input such as a string of integers (a key) and outputs a value of a pre-specified length (a **hash**). **Bitcoin** uses a cryptographic hash function to secure the network.

Hashgraph: a form of **distributed ledger**.

Hashrate: the number of **hashes** that can be performed by a **miner** in a given period of time.

HD wallet: wallet based on a system of deriving multiple keys from a single starting point known as a seed. This seed is all that is needed to restore a wallet if it is lost and can allow the creation of public **addresses** without the knowledge of the **private key**.

Hierarchical Deterministic wallet: see **HD wallet**.

Hot wallet: a **wallet** that is connected in some way to the internet, eg a software wallet on a laptop or an app on a mobile phone.

Hybrid wallet: cryptocurrency storage and maintenance system that is a combination of a **software wallet** (stored on the user home computer) and a **web wallet** (stored on a third-party server).

Hyperledger Fabric: open source distributed ledger platform hosted by the Linux Foundation. Currently IBM is a large user of Hyperledger Fabric and is utilising it to create permissioned blockchains for clients. There are a range of other Hyperledger platforms such as Hyperledger Burrow, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Cello, Hyperledger Composer, Hyperledger Explorer and Hyperledger Indy.

ICO (Initial Coin Offering): method of crowdfunding. People pay, normally in **ether** or **bitcoin**, and receive **tokens** in return. A **Whitepaper** is normally released that contains details of the project, how much money is being sought, and whether there is a maximum or minimum amount to be raised. If a minimum amount is to be raised and that sum is not reached the money pledged will be returned. While some ICOs have been designed in an attempt to circumvent securities and other regulations, other ICOs do attempt to meet the legal requirements, though these are often unclear. It is common for ICOs not to be available for residents of certain countries, including the United States, China and even New Zealand. ICOs are also now being called **TGEs** (Token Generation Events).

Inputs: reference to an output of a previous transaction. Inputs to an **address** are added up, and this amount determines the amount a **wallet** can spend.

Institutional cryptoeconomics: an emerging theory that can be seen as a subset of New Institutional Economics.

Internet of Things (IoT): network of physical devices that are connected to the internet and have the ability to record, receive and send data. Covers internet-connected cars, light bulbs, fridges, clothes, pedometers and everything in between.

IOTA: a **distributed ledger** that uses a tangle rather than a **blockchain**. Principally designed to be used for **IoT** devices, but its applications can be a lot broader. It does not rely on the normal **consensus mechanisms** such as **proof-of-work** or **proof-of-stake.** Rather, to make a transaction the person has to validate two other unrelated transactions. IOTA is claimed to be resistant to **quantum computers**. Transactions on IOTA are free.

Interplanetary File System (IPFS): an **open source** protocol and network designed to create a **peer-to-peer** method of storing and sharing information in a distributed file system. Unlike on the internet, material cannot be removed and/or changed. Its proponents argue that in time it could replace the internet.

IPFS: see **Interplanetary File System.**

Know Your Customer (KYC): guidelines stated or implied by regulatory bodies that require financial institutions to know and identify their clients to a certain degree in an attempt to prevent **money laundering** and the financing of terrorism.

KYC: see **Know Your Customer**

Laundry: for **cryptocurrencies** the process of combining funds from various users and redistributing them, making tracing the cryptocurrency back to their original source very difficult by mixing their "taint". (Laundry is also known as a **mixing service**).

Leased proof-of-stake (LPoS): with **proof-of-stake** a large number of **coins** are required to validate a **block** of transactions. Thus many coin owners are not able to participate in validation. LPoS allows holders to lease balances to a **node** and receive rewards in proportion with the node that has leased the coins.

Light client: see **Spv client**.

Lightning network: attempt to make the **Bitcoin blockchain** faster and cheaper for transactions by conducting transactions **off-chain** (see https://lightning.network/).

Litecoin: a particular **altcoin** designed for payments. Litecoin can handle a higher volume of transactions than its counterpart **Bitcoin** as it has an average **block time** of 2.5 minutes, rather than Bitcoin's 10 minutes.

Lock time: a time or **block height** before which a transaction cannot be added to a **block**.

Longest chain: it is possible for two miners to create **blocks** around the same time which creates two different **blockchains** in the network: blockchain A and blockchain B. (For the sake of explanation we will call those two blocks "aa" and "bb".) **Miners** will work on both blockchain A and B, so blocks aa and bb. The first miner to find a block for either blockchain A or blockchain B will resolve the conflict and the miners will now work off that blockchain. If the new block was bb and therefore mined on blockchain B, blockchain A (and block aa) will be invalid and the block reward for aa will go to the miner of bb. The transactions contained in aa are no longer in the longest chain (aa is now an **orphan block**) and are returned to the **mempool**.

Main chain: see **longest chain**.

Mainnet: main **Bitcoin** network and its **blockchain**. The term is mostly used in comparison to **testnet,** an alternative Bitcoin blockchain being used purely for testing purposes.

Malware: computer software that facilitates illicit activities such as data exfiltration, denial-of-service attacks, fraud, and spam dissemination.

mBTC: millibitcoin, 0.001 of a **bitcoin**

Mempool: memory pool or **transaction pool**, files with data about transactions that are not included into a **block** as they are unconfirmed. When there are a lot of transactions the mempool grows and transaction times can lengthen. People then often raise the **transaction fees** they are willing to pay to ensure their transactions get through: **miners** prefer to take transactions with higher fees as they are more profitable.

Merkle tree (Hash tree): a full binary tree of a **hash** values. It is a data structure that is used to verify any kind of data stored, handled and transferred in and between computers.

Miner: computer software that adds new transactions to **blocks**, broadcasts that block and collects the **block reward**.

Miner's fee: see **transaction fee**.

Mining: the act of securing the network by solving cryptographic problems using computing hardware to verify transactions and it is how new **bitcoins** (and some other **cryptocurrencies**) are created. The allusion is to gold mining. Although **Bitcoin** creators do not seek or strike literal gold, the process requires exertion and it slowly releases new bitcoin to the network as successful miners are rewarded with a **block reward**.

Mining pool: miners share their computer processing power over a network, and split the **block reward** according to the amount of work they contributed to the probability of finding a **block**. Sometimes called collective mining.

Mintage cap: the maximum number of **coins** that can be mined for a specific **cryptocurrency**. For example, bitcoin's mintage cap is 21 million coins.

Mixer: person who provides a **mixing service**.

Mixing service: service that mixes **public key addresses** to further anonymise **cryptocurrency** transactions. A mixing service (also known as a **tumbler**) helps preserve privacy and anonymity because it attempts to prevent people from tracing a particular **bitcoin** to an individual. It also has the potential to be used for **money laundering**. (A mixing service is also known as a **laundry.**)

Mobile wallet: a **software wallet** that allows the user to store **cryptocurrencies** on their mobile devices, often on their smart phone. Many mobile wallets allow users to pay in bricks-and-mortar stores by scanning a **QR code** or using "tap to pay". Some websites also provide QR codes which can be scanned for payment.

Monero: privacy coin where the identity of the parties to the transaction and the amount of the transaction are hidden from others through the use of **ring signatures**.

Money laundering: process of concealing the origin of money, which typically occurs in three major stages: (a) placement, which is the initial point of entry for funds derived from criminal activities; (b) layering, which is the creation of complex networks of transactions that attempt to obscure the link between the initial entry point and the end of the laundering cycle; and (c) integration, which is the return of funds to the legitimate economy for later extraction. In other words, money gained through criminal means can be made to look as though it came from legitimate sources.

Money Services Business (MSB): defined by the United States Department of the Treasury as a business that issues, sells, or redeems money orders or traveller's checks, provides cheque-cashing services, is a currency dealer or foreign exchange dealer, or provides money transfer services. MSBs must register with the Internal Revenue Service (IRS) within 180 days of beginning operation and must renew their registration every two years.

Mt Gox: Bitcoin exchange located in Japan. Launched in July 2010, by 2013 it was handling more than 70 per cent of Bitcoin transactions.

Mt Gox hack: in February 2014 **Mt Gox's** computer systems were hacked and hundreds of thousands of **bitcoins** were stolen.

Multi-sig (or multi-signature): requires more than one person (or device) to sign a transaction and in so doing increases security.

Mutual ledger: term occasionally used to describe a **distributed ledger**.

Namecoin: an **altcoin** based on **Bitcoin's** code and employing the same **proof-of-work** algorithm. Namecoin was designed to provide an alternative to the traditional domain name systems (DNS).

NAVCoin: first **altcoin** to be fully anonymous.

NEM: a **blockchain** that allows the use of **smart contracts**. NEM's **consensus mechanism** is **proof-of-importance**. NEM's **coin** is **XEM**.

Neo: cryptocurrency from China that is the Chinese equivalent of **Ethereum**. **NFC chip (Near Field Communication chip)**: allows two devices to communicate with each other. The devices containing the chip need to be within 4 centimetres of each other. NFC chips are used commonly, for example, inside contactless credit cards and for Android Pay, Apple Pay and Google Pay and so on.

Node: network participant which (or who) runs a full copy of **blockchain**. Some nodes on the **Bitcoin blockchain** are **miners**, while others are not.

Nonce: meaningless value in a **block** which can be adjusted in order to try to satisfy the **difficulty** of **proof-of-work**.

Novacoin: a type of **altcoin**.

NuBits: decentralised open source **altcoin** launched in 2014. NuBit coins are not **mined**, but rather issued by the project's shareholders, whose primary goal is to maintain a one-to-one NuBit peg to the US dollar.

Off-chain: refers to transactions that are not recorded on the **blockchain**. For example, it is possible for a series of transactions to occur between parties which are not all recorded on the blockchain, and instead all the transactions are totalled and offset against each other with just one transaction being recorded on the blockchain. For example, take Mark who buys coffee and food from a café most days a week and wants to make these purchases with **bitcoin**. Instead of paying by bitcoin whenever he visits the café and incurring **transaction fees** each time, it would help Mark if Sarah, the café owner, used the **lightning network**. A payment channel would then be set up between Sarah and Mark. All the transactions would be added up and at an agreed date Sarah would be paid the total owing by Mark in one transaction. Off-chain can also be used when disputes and governance decisions are not handled by **smart contracts**.

Offline storage: see **cold storage**.

Off-ramp: reference to a place, often an **exchange**, where **cryptocurrency** can be converted into **fiat currency**.

On-chain: refers to transactions that are recorded on the **blockchain**. For governance, when disputes or parts of disputes are handled via **smart contracts**.

OneGram: stable coin backed by gold.

Online wallet: see **web wallet**.

On-ramp: references a place, often an **exchange,** where **fiat currency** can be used to purchase **cryptocurrency**.

Open banking: banks share customer data using **APIs** (Application Interface Platforms) with third parties securely and in real time. For example, instead of Bob having to employ a credit card or purchase credits to use a car sharing scheme, the car sharing company could take the money directly from Bob's account, with Bob being able to see his current bank account balance. Through open banking customers get an accurate view of their finances and can also compare offerings between suppliers.

Open source: software that is not proprietary; that is, software that other people can contribute to and also copy and adapt if they so wish. Open source software is often published on **Github**.

Oracle: an agent that finds and verifies events which occur in the real world and transmits that information to a **blockchain** to be used for a **smart contract**. Oracles can be particular devices, for example, an **IoT** device placed in a shipping container that is used to measure temperature and location. If the wifi signal from the IoT device is picked up at an agreed location like a foreign port, and the temperature has remained within the range set out in the smart contract, the **cryptocurrency** payment that the smart contract is holding is released to the party or parties specified in the smart contract. Alternatively the oracle can take information from other sources. For example, if two people bet on the outcome of a rugby test, the information about the final score can be taken from a combination of different websites. There can also be a combination of a device and information collected from other sources. For instance, if an insurance contract for a farmer is specified to pay out in the event of low rainfall somewhere, the information can be taken from specified websites and also from an IoT device on the property designed to measure rainfall.

Orphan block: block which is not part of the **main chain** or **longest chain**. Orphan blocks occur when two **miners** produce blocks at similar times: a decision is made which block to keep, and the orphaned block is not incorporated into the main chain. Orphan blocks can also be created when an attacker attempts to reverse transactions.

Paper wallet: a sheet of paper that contains **cryptocurrency wallet** information such as a **public address** and the corresponding **private key**.

Payment processor: a company appointed by a merchant to handle transactions from various channels.

Peercoin: a type of **altcoin**. At one stage Peercoin was the third-most valuable **cryptocurrency** after **Bitcoin** and **Litecoin**.

Peer-to-peer (P2P): decentralised interactions between at least two parties in a highly interconnected network.

Permissioned blockchain: closed **blockchain** where the access of each participant is well defined and restricted to the roles the participants play. Blockchains used within a consortium of organisations will normally use permissioned blockchains. The best-known are **Hyperledger Fabric** and **Corda**. Some **public blockchains**, such as **Ethereum** and **NEM** offer permissioned versions as well.

Permissionless blockchain: on a permissionless blockchain anybody can download a copy of the **blockchain** (and/or view it) and make transactions on it. **Bitcoin** and **Ethereum** are the two best-known examples.

Personally Identifiable Information (PII): data that could potentially identify a specific individual.

Pool: a collection of **mining** clients who mine a **block** collectively and split the reward. **Mining pools** are a useful way to increase probability of successfully mining a block as the difficulty increases.

Post-blockchain distributed ledger: newer **distributed ledgers** that do not use a **blockchain**, ie they do not use a linear set of **blocks**. Examples include **Hashgraph** and **IOTA**.

Post-quantum cryptography: cryptography that cannot be compromised by **quantum computers**.

Pre-mining: mining of a **cryptocurrency** by its developers or founders before release.

Primecoin: an **altcoin**.

Privacy coin: coins such as **Zcash** and **Monero** which keep the sender and receiver anonymous and also hide what the transaction was for.

Private blockchain: term often used to describe a **permissioned blockchain**.

Private key: alphanumeric string kept secret by the user and designed to sign a digital communication when hashed with a public key. Maintaining the secrecy of private keys is vital because whoever has the private key can spend the **cryptocurrency**.

Proof-of-burn: a form of distributed **consensus mechanism** and an alternative to **proof-of-work** and **proof-of-stake**. Proof-of-burn involves destroying **coins**. Proof-of-burn employs the idea of eliminating – metaphorically "burning" – coins to reduce the need for powerful computational resources when mining. Proof-of-burn has numerous advantages over both proof-of-work and proof-of-stake. For example (a) energy consumption is very low; (b) there is no need to invest in powerful computing hardware; and (c) burnt coins cannot be stolen.

Proof-of-importance: a **consensus mechanism** used in **NEM**. In **proof-of-stake** the key thing is the number of **coins** that are staked, thus privileging those with large holdings. Proof-of-importance looks instead at the **public key**'s network activity. This includes not only the number of coins, but also, for instance, the reputation and the number of transactions made to and from the public key.

Proof-of-stake (PoS): consensus mechanism that is an alternative to **proof-of-work**. People "stake" **coins** by locking up their coins within the network, that is, they put coins into an account. People who have staked their coins are chosen at random to validate **blocks**.

Proof-of-work (PoW): form of **consensus mechanism**. To validate and therefore mine a **block** a hard computational maths problem must be solved. While the problem is difficult to solve it is easy for others to check that the solution is correct. The first **miner** to solve the maths problem receives the **block reward**. **Bitcoin** uses proof-of-work but this comes in for heavy criticism because, with the price of bitcoin so high, a lot of miners are attempting to mine the blocks. To keep the 10-minute average **block time** the **difficulty** of the maths problem increases but this requires more powerful computers and more electricity to run them.

Pseudonymous: bearing or using a fictitious name. Most **cryptocurrency** transactions are similar to writing under a pseudonym since the person's name is not used as part of the transaction. However, if a user's **public key** is linked to their identity, all the transactions to and from the public key will be linked to this identity. Take the case where a person is paid their wages in a cryptocurrency and they use the same **wallet** to pay their rent. Both the employer and the landlord, if they so wished, could view all the transactions that person made using that wallet. The landlord could then see the person's wages coming in and when the person received a pay rise could raise the rent. To avoid the release of such information a **HD wallet** can be used.

Public blockchain: blockchain that anyone can view and access without asking. Examples include **Bitcoin** and **Ethereum**. A public blockchain is different to a **permissioned blockchain,** where permission must be granted for viewing and access.

Public key: publicly known alphanumeric string which is hashed with another, privately held string to sign a digital communication. With **Bitcoin**, the public key is a bitcoin **address**.

Public key encryption: a cryptographic system that uses two different keys: a **private key** and a **public key**. A public key is used to encrypt the data, and can be given to anyone. A private key that is known only to one party in an exchange of information is used to decrypt it.

QR code (Quick Response code): a type of bar code that can be read both horizontally and vertically, as long as the person reading it is connected to the internet and has a QR reader. This allows large amounts of information to be encoded.

Quantum computers: computers that use **quantum computing**.

Quantum computing: extraordinarily powerful computers based on quantum physics. Quantum computing is still in its early days. Once the technology matures, it would be able to break current **cryptography** easily. As **cryptocurrencies**, **CBDCs** and **distributed ledgers** rely on cryptography they will potentially be useless when quantum computing develops. However, it is not just distributed ledger technology that will be affected; many of our systems – credit cards, online banking and more – rely on cryptography. Considerable work is going into **post-quantum cryptography,** which would be able to withstand quantum computing. **IOTA**, a cryptocurrency, is said to be safe from quantum computing.

Red Belly Blockchain: blockchain developed at the University of Sydney in conjunction with Data 61 which in tests has processed 600,000 transactions per second – an order of magnitude faster than the networks of Visa and MasterCard combined.

Regulatory sandbox: see **sandbox**.

Regulatory sandpit: see **sandbox**.

Remittance: funds are sent from a domestic financial institution to another institution abroad, often a migrant's country of origin.

Retail bank: bank that people and all manner of organisations have bank accounts with – for example, in New Zealand, ASB, Westpac and so on. The contrast is to the **central bank**. However, when **CBDCs** start to be issued, depending on how the CBDC is set up, people may be able to have bank accounts directly with the central bank.

Ring signature: used in **Monero** to allow one person in a group to sign a transaction. It is impossible to work out who among the group signed the transaction, thus providing anonymity to the signer. **Monero** is a **privacy coin**.

Ripple: payment network that can be used to transfer any currency (including ad hoc currencies created by users). The network consists of payment **nodes** and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships. Ripple is sometimes referred to as a **cryptocurrency**, but as it is controlled centrally by Ripple Labs it is hard to see that it is a **decentralised** and therefore a cryptocurrency.

Sandbox (or sandpit): a set of rules that allows innovators to test their products/business models in live environments without following some or all legal requirements and also normally works closely with the relevant regulators. A number of jurisdictions have sandboxes including Singapore, Australia, Holland, Canada, Hong Kong, United Arab Emirates and the UK. New Zealand does not, at the time of this report, have a sandbox.

Sandpit: see **sandbox**.

Satoshi: smallest subdivision of a **bitcoin** currently available (0.00000001 **BTC**) – which is one-hundredth-of-a-million of one bitcoin.

Scale: ability or inability of a platform to handle a large number of transactions. A common criticism of **public blockchains** such as **Bitcoin** and **Ethereum** is that they cannot scale: for example, Ethereum can only process around 20 transactions per second compared to well over 20,000 for Visa. Bitcoin is slower still at seven per second, and even that figure may be on the high side. Various attempts are being made to scale both Bitcoin and Ethereum. Attempts include **sharding**, **state channels**, and the **lightning network**. Newer blockchains have much higher **transaction rates**, with at least one, **Red Belly Blockchain**, being able to process many times more than Visa in testing, at over 600,000 per second.

Scamcoin: an **altcoin** produced expressly for making money for the founder.

Scrypt: popular cryptographic function (see CoinGecko <https://www.coingecko.com/en?hashing_algorithm=Scrypt>).

Security coin (or security token): there is no settled definition of a security coin. (Security is not meant in the sense of a "secure" coin, rather it is meant to refer to tradable financial assets, with many people attempting to argue that their coin is not a security coin.) What is clear, however, is that a **token** such as **Bitcoin** will not be a **security token**. Considered perhaps most inclusively, security coins would be tokens that grant the owner any one of the following: (a) an ownership asset in a legal entity; (b) an equity interest; (c) a share of profits, losses, assets and/or liabilities; (d) status as a creditor or lender; (e) a claim in a bankruptcy or liquidation as an equity interest holder or creditor; (f) a repayment obligation to the holder from the system or the legal entity issuer of the token; or (g) ability to convert the token at a later date to an instrument with investment interests (see <http://7marketingmedia.com/blog/2017/11/6/blockchain-is-my-ico-a-security-or-utility-coin>).

Security token: see **security coin**.

Seed phrase: list of words that store the information needed to recover a **wallet**.

SHA-256: the cryptographic function used as the basis for **Bitcoin's** and some other **cryptocurrencies' proof-of-work** system. See <https://www.coingecko.com/en?hashing_algorithm=SHA-256>.

ShadowCash: anonymous **coin** used within a **blockchain**-based software platform developed by the Shadow Project.

Sharding: process of splitting up a **blockchain** so that **nodes** do not have to process all the transactions, designed to help blockchains **scale**.

Sia: **decentralised** storage system run on the Sia **blockchain**. Users pay in **Siacoin** to store their files on others' computers and those people storing the files are paid in Siacoin.

Siacoin: coin used on the **Sia blockchain** to pay and be paid for **decentralised** file storage.

Silk Road: online marketplace that traded **bitcoins** for illicit goods, primarily drugs. Silk Road was shut down in early October 2013.

Simplified Payment Verification (Spv): way to confirm **bitcoin** payments without having to download the full **blockchain** of every recorded transaction.

Smart contract: computer protocols that facilitate, verify or enforce the execution of a computer program. Not a particularly good name as a smart contract is not necessarily smart and is not always a contract. Can be used to effect payment. For example, Eva and Gina could agree that Eva will send Gina a container of wool. Gina promises to pay Eva $50,000 for when the container reaches a pre-specified overseas port. The container is fitted with an **IoT** device and a smart contract is written so that once the IoT device is picked up by wifi at the port the $50,000 is sent automatically to Eva. To start the smart contract Gina must send the $50,000 (in a **cryptocurrency**) to the smart contract. The smart contract holds it in **escrow** and once the IoT device is picked up at the port it releases the money to Eva. The smart contract should be coded so that if the wool does not arrive at the port, for example, it gets lost during transportation, the cryptocurrency is returned to Gina. Smart contracts can be used in a wide variety of settings: for example, when decisions are made about changes to the code and how the blockchain is to be run (governance) the mechanism for making the changes can be contained in the smart contracts. For instance, voting power may be set at one token, one vote. For certain types of decisions a smart contract could require 40 per cent of token holders to vote on the matter and of those 40 per cent, 60 per cent would have to vote in favour. Because a smart contract is used, if the requirements have been met the change is made automatically.

Soft fork: see **fork**.

Software wallet: computer program that stores **tokens** on a PC or laptop.

Spv client: a client that downloads only a small part of the **blockchain**. This allows users of low-power or low-storage hardware like smart phones and laptops to maintain almost the same guarantee of security by sometimes selectively downloading small parts of the state without needing to spend megabytes of bandwidth and gigabytes of storage on full blockchain validation and maintenance. (Also called **light client.)**

Stable coin: coin designed so that its price does not fluctuate wildly. Such coins can be backed by **fiat currencies**, such as **Tether**, or by gold, such as **OneGram**, or by a combination of other means, incuding a mix of **cryptocurrencies**. **CBDCs** when they are issued by certain countries would be seen as being stable coins and therefore desirable for use in commerce.

Stale block: block successfully processed by a **miner** or **mining pool** but not included in the current best **blockchain**. A stale block is created when more than one miner discovers and solves the same block. As the

block has already been solved it does not offer miners any reward for further work on it. Experienced miners know to skip stale blocks.

State channel: used on **Ethereum** to create a two-way pathway between two users to set up a channel. The channels are **off-chain** and private. The transactions are signed by each party with their **private key**. Once the channel closes the transaction history is loaded on the **blockchain**. Imagine Deb and Ewen have a state channel and both start with 100 **ethers**. Deb then sends Ewen five lots of six ethers and Ewen sends Deb two lots of five ethers. When the blockchain is updated it will show Deb with 80 ethers and Ewen with 120 ethers, but only one transaction (of 20 ethers from Deb to Ewen) is recorded. Using a state channel has the advantage of speeding up the transaction times of the payments and also reducing the number of transactions recorded **on-chain**.

Stellar Lumens: cryptocurrency designed for cross-border payments.

Suspicious Activity Report (SAR): form that must be filed when a financial institution identifies or suspects criminal activity.

Testnet: alternative **blockchain** to the **mainnet** and is used for testing by developers and also for people who want to use a blockchain without losing any money. Testnet **coins** are separate and distinct from the actual coins on the mainnet and are not supposed to have any value.

Tether: stable coin that is backed one-to-one with the US dollar. (There are concerns that the company behind Tether, Tether Limited, does not hold sufficient US dollars to back each tether that it has issued.)

TGE (Token Generation Event): term starting to be used instead of **ICO**.

The DAO: This is not to be confused with **DAOs** (see above). The DAO was an entity set up in May 2016 that raised over USD 150 million in **ether**. The intent was to use that money for funding projects. Anyone with a project could put forward their idea and DAO **token** holders could vote. Successful projects would be funded and token holders would receive a share of any profits from that project. Before any projects were funded a bug in The DAO's code enabled a person to drain a large amount of ether to an account. A decision was made by the ether token holders to prevent the money being taken and a **hard fork** occurred. Essentially the hard fork rolled back the Ethereum **blockchain** until just before the first ether from The DAO was removed. The **hard fork** was controversial and some people continued to mine the chain containing the old tokens, now called **Ethereum Classic**. All holders of ether tokens at the time of the hard fork were given the same number of Ethereum Classic tokens.

The Onion Router (Tor): anonymous routing protocol, used to conceal its users' identities and online activites from surveillance. Onion routing encrypts and then randomly bounces communications through a network of relays run by volunteers around the world.

Time stamp: more accurately, a digital time stamp. Generally refers to the digital date and time information that is attached to digital data. It serves as proof that a piece of data existed at a certain point in time. The time stamp of a **block**, for example, shows when it was mined. On the **blockchain**, it is an identifier which stamps and verifies a specific transaction that has taken place. Time stamps (and time signatures) can verify documents, copyrights, contracts or any other digital transaction that occurs on a blockchain.

Token: used interchangeably with the term **coin**.

Token economy: used interchangeably with **cryptoeconomics**.

Transaction block: A group of transactions which are hashed (solved or verified) and then added to the **blockchain**.

Transaction fee: fee imposed on some transactions sent across blockchain networks and collected by the **miner** of a **block**. This is to encourage miners to add the transaction to a block in a timely fashion. Also called **miner's fee** or simply **fee**. Not all **cryptocurrencies** charge a fee: see, for example, **Hashgraph** and **IOTA**.

Transaction pool: see **mempool**.

Trezor: a type of **hardware wallet**. **Tumbler:** see **mixing service**.

uBTC: microbitcoin, 0.000001 of one **bitcoin**; equivalent to one **bit**.

Unbanked: unbanked customers have no banking services with traditional regulated financial institutions.

Underbanked: underbanked customers have one or more bank accounts, but need to conduct many of their financial transactions with alternative service providers and still use cash for many transactions.

Unique identity: a set of cryptographically verifiable interactions sharing the property that they were all created by the same person, but with the added constraint that one person cannot have multiple unique identities.

Utility coin: see **utility token**.

Utility token: sometimes called **utility coin**. **Token** that will be able, or is able, to be used on a **blockchain** platform. For example, the **Sia** blockchain is a **decentralised** storage platform. Siacoins are used to purchase data storage and people who host data from other people on their computers are paid in Siacoin.

Virgin bitcoin: a **bitcoin** received as a reward for mining a block. Thus, it has never been spent before.

Virgin coin: an **altcoin** or a **bitcoin** received as a **block reward**. Thus, it has never been spent before.

Virtual currency: cryptocurrencies are sometimes called virtual currencies; indeed, that is the term used in English translations of Japan's cryptocurrency legislation. Virtual currencies are technically broader than cryptocurrencies as virtual currencies are digital representations that can be traded, and cover things that are used within gaming platforms such as Linden dollars (in Second Life) and World of Warcraft gold. Other forms are M-Pesa and loyalty schemes such as Air New Zealand Airpoints.

Virtual Private Network (VPN): method used to add security and privacy to private and public networks, like wifi hotspots and the internet. VPNs are often used by corporations to protect sensitive data.

Wallet: method of storing **tokens** for later use. A wallet holds the **private key** and **public key**.

Web wallet: stores the user's **private keys** online. However, there can be security issues as the user's keys are stored on a third party's server, which may be hacked. The main advantage of web wallets is that they are easily accessible from anywhere in the world. Also called **online wallet**.

Whitepaper: document setting out a **blockchain** project or an improvement on an existing one. It may be for a blockchain that has not yet been developed, one that is in its early days of development or even for a fully functioning and operational blockchain. The seminal Whitepaper is the Whitepaper for what became Bitcoin (Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) <https://bitcoin.org/bitcoin.pdf>). A Whitepaper should allow technical experts to assess the viability and accuracy of the project, but it is often also used as a marketing tool. For example, Whitepapers are used for **ICOs.** The term has slipped a little and some governments and organisations are releasing reports on **blockchain** activities and calling them Whitepapers.

Witnesses: see **delegated proof-of-stake**.

XEM: the **token** of the **NEM** blockchain.

YBCoin: a **token** from China designed to be a currency. It has a 60-second **block time** and uses a combination of **proof-of-stake** and **proof-of-work**.

Zcash: privacy coin, although sender and receiver can choose for transactions and **addresses** to be publicly viewable if desired.

Zcoin: the implementation of the **Zero coin** protocol. Unlike **Bitcoin**, ZCoin reportedy obfuscates all data related to both senders and recipients.

Zero-confirmation transactions: transaction whereby a merchant agrees the sale of a product or service in return for a **cryptocurrency** transaction, before the transmission of the cryptocurrency has been confirmed and added to the **blockchain**. There is a risk to this because the person purchasing the good or service could be trying to **double spend**, or the **mempool** could be so large that the transaction times out.

Zero coin: privacy coin, an anonymous protocol designed to keep the identities of users secret. The protocol is to be used in **Zcoin**, another **altcoin**.

Zero knowledge proofs: used in **Zcash,** these are akin to magic as they allow one party (the prover) to prove to someone else (the verifier) that a statement is correct without having to reveal what the statement actually is.

Bibliography

Cases

New Zealand

R v Robinson [2015] NZHC 2641.

R v Turnock [2016] NZHC 1364.

Rest of the world

Administrative Chamber of the Supreme Court Ruling No 3-3-1-75-15 (11 April 2016).

Case C-172/96 *Commissioners of Customs and Excise v First National Bank of Chicago* [1998] ECR I-4387.

Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECR I-498.

Commodity Futures Trading Commission v McDonnell (6 March 2018, Memorandum & Order (Eastern District of New York)).

Foley v Hill (1848) 2 HLC 28, 9 ER 1002.

Securities and Exchange Commission v Shavers (Case no 4:13 – CV 416, Eastern District of Texas).

US v Murgio, No 15-cr-769 (AJN) (SDNY, 12 January 2017).

Legislation

Australia

A New Tax System (Goods and Services Tax) Act 1999 (Cth)

A New Tax System (Goods and Services Tax) Regulations 1999 (Cth)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth).

Anti-Money Laundering and Counter-Terrorism Financing (Digital Currency Exchange Register) Policy Principles 2018.

Banking Act 1959 (Cth).

Banking Regulation 2016 (Cth).

Competition and Consumer Act 2010 (Cth).

Banking Act 1959 (Cth).

Canada

An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures ("Bill C-31").

Income Tax Act RSC 1985.

Income Tax Regulations (CRC, c 945).

Proceeds of Crime (Money Laundering) and Terrorist Financing Act SC 2000 c 17 ("PCMLTFA").

The Economic Action Plan 2014 Act.

Estonia

Money Laundering and Terrorist Financing Prevention Act 2007.

European Union

Council Directive 2006/112/EC on the common system of value added tax [2006] OJ L 347.

General Data Protection Regulation (GDPR) EU 2016/679.

Japan

Law for Prevention of Transfer of Criminal Proceeds Act 2007.

Marshall Islands

Declaration and Issuance of the Sovereign Currency Act 2018.

New Zealand

Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

Financial Markets Conduct Act 2013.

Financial Service Providers (Registration and Dispute Resolution) Act 2008.

Income Tax Act 2007.

Reserve Bank of New Zealand Act 1989.

Taxation (Residential Land Withholding Tax, GST on Online Services, and Student Loans) Act 2016.

United Kingdom

Sanctions and Anti-Money Laundering Act 2018.

The Locomotive Act 1865.

Value Added Tax Act 1994.

United States

23 NYCRR Part 200 (New York's Virtual Currency Regulation) <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.

31 CFR § 1010.

2014 CA Assembly Bill AB-129 <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB129>.

Assembly Bill A9899A.

CA Corp Code § 107 (through 2013 Leg Sess).

Conn Gen Stat § 36a.

Connecticut House Act (2015 Regular Session – HB 6800) <https://www.cga.ct.gov/2015/act/pa/2015PA-00053-R00HB-06800-PA.htm>.

HB 19 Wyoming Money Transmitter Act-virtual currency exemption, "AN ACT relating to trade and commerce; amending the Wyoming Money Transmitter Act to provide an exemption for virtual currency; and providing for an effective date."

New Hampshire House Bill 552 "Requiring the state treasurer to develop an implementation plan for the state to accept bitcoin as payment for taxes and fees" <https://legiscan.com/NH/bill/HB552/2015>.

NH HB436 Regular session 2017 <http://gencourt.state.nh.us/bill_status/billText.aspx?sy=2017&id=638&txtFormat=html>.

NH Rev Stat § 399-G:1(VII) (2015).

NH Rev Stat § 399-G:1(XV) (2015).

NY Abandoned Property Law § 501 (2015).

Texas Finance Code Ch 151 (2005).

Books and chapters in books

Andreas M Antonopoulos *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media, Sebastopol, California, 2014).

Arthur Robert Burns *Money and Monetary Policy in Early Times* (K Paul, Trench, Trubner & Company, New York, 1927).

Anais Carmona "The Bitcoin: The Currency of the Future, Fuel of Terror" in Misty Blowers (ed) *Evolution of Cyber Technologies and Operations to 2035,* vol 63 of *Advances in Information Security* (Springer, 2015) 127.

Michael J Casey and Paul Vigna *The Truth Machine: The Blockchain and the Future of Everything* (Harper Collins, 2018).

David Chaum "Blind Signatures for Untraceable Payments" in RL Rivest, A Sherman and D Chaum (eds) *Advances in Cryptology: Proceedings of Crypto 82* (Plenum Press, New York, 1983) 199.

David Chaum, Amos Fiat and Moni Naor "Untraceable Electronic Cash" in S Goldwasser (ed) *Advances in Cryptology: Proceedings of Crypto 88* (Springer-Verlag, New York, 1990) 319.

Kim-Kwang Raymond Choo "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks" in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 283.

Alexei Dingli and Dylan Seychell *The New Digital Natives: Cutting the Chord* (Springer, Berlin, Heidelberg, 2015).

Quinn DuPont “Experiments in Algorithmic Governance: A history and ethnography of ‘The DAO’, a failed Decentralized Autonomous Organization” in Malcolm Campbell-Verduyn (ed) *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance* (Routledge, 2018).

Paul Einzig *Primitive Money in its Ethnological, Historical, and Economic Aspects* (2nd ed, Pergamon Press, Oxford, 1966).

Pedro Franco *Understanding Bitcoin: Cryptography, engineering, and economics* (Wiley, 2015).

Marius-Cristian Frunza *Solving Modern Crime in Financial Markets* (Elsevier, 2015).

A Hingston Quiggin *A Survey of Primitive Money: The Beginning of Money* (Barnes & Noble, New York, 1970).

Jan Hogendorn and Marion Johnson *The Shell Money of the Slave Trade* (Cambridge University Press, Cambridge, 2003).

Eric M Jackson *The PayPal Wars: Battles with eBay, the Media, the Mafia, and the Rest of the Planet Earth* (World Ahead Publishing, 2004).

Brett King *Breaking Banks: The Innovators, Rogues and Strategists Rebooting Banking* (Wiley, 2014).

Pak Nian Lam and David Lee Kuo Chuen “Introduction to Bitcoin” in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 5.

Lawrence Lessig *Code: version 2.0* (2nd ed, Basic Books, New York, 2006).

N Gregory Mankiw *Principles of Macroeconomics* (7th ed, Cengage Learning, Australia, 2017).

Felix Martin *Money: The Unauthorised Biography* (Alfred A Knopf, New York, 2014).

Preston Miller “The Cryptocurrency Enigma” in John Sammons (ed) *Digital Forensics* (Syngress, 2015) 1.

Mwelwa C Musambachime *Wealth from the Rocks: Mining and Smelting of Metals in Pre-Colonial Zambia* (Xlibris, 2016).

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, Princeton, 2016).

Pierre Noizat “Blockchain Electronic Vote” in David Lee Kuo Chuen (ed) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Elsevier, 2015) 453.

Kenneth S Rogoff *The Curse of Cash* (Princeton University Press, Princeton, 2016).

Murray N Rothbard *A History of Money and Banking in the United States: The Colonial Era to World War II* (Ludwig Von Mises Institute, Auburn, Alabama, 2002).

Tomas Sander and Amnon Ta-Shma “Auditable, Anonymous Electronic Cash” in Michael Weiner (ed) *Advances in Cryptology — CRYPTO’ 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666* (Springer, Berlin, Heidelberg, 1999) 555.

D George Sherman *Rice, Rupees, and Ritual: Economy and Society Among the Samosir Batak of Sumatra* (Stanford University Press, 1990).

Melanie Swan *Blockchain: Blueprint for a New Economy* (O’Reilly Media, Sebastopol, California, 2015).

Dan Tapscott and Alex Tapscott *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World* (Penguin Random House, 2016).

Jan van Dijk *The Network Society* (3rd ed, Sage, 2012) 144.

Paul Vigna and Michael J Casey *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order* (St Martin’s Press, New York, 2015).

David Wolman *The End of Money: Counterfeiters, Preachers, Techies, Dreamers--and the Coming Cashless Society* (Da Capo Press, Boston, 2012).

David Yermack “Is Bitcoin a Real Currency? An Economic Appraisal” in David KC Lee (ed) *The Handbook of Digital Currency* (Elsevier, 2015).

Journal articles

Robleh Ali, John Barrdear, Roger Clews and James Southgate “Innovations in Payment Technologies and the Emergence of Digital Currencies” (2014) Q3 Bank of England Quarterly Bulletin 262.

Morten Bech and Rodney Garratt “Central Bank Cryptocurrencies” (2017) BIS (Bank for International Settlements) Quarterly Review 55.

Aleksander Berentsen and Fabian Schar “The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies” (2018) 100 Federal Reserve Bank of St Louis Review 97.

Daniel J Bernstein and Tanja Lange “Post-quantum cryptography” (2017) 549 Nature 188.

Jürgen Bott and Udo Milkau “Central Bank Money and Blockchain: A Payments Perspective” (2017) 11(2) Journal of Payments Strategy & Systems 145.

Danton Bryans “Bitcoin and Money Laundering: Mining for an Effective Solution” 2014 Indiana Law Journal 441.

James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack and Wade McMahon “Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?” (2017) Financial Systems Review 1.

Lewis Rinaudo Cohen, David Contreiras Tyler and Pamela Buxton “Blockchain’s Three Capital Markets Innovations Explained” (2016) 35(26) International Financial Law Review 9.

Whitfield Diffie and Martin Hellman “New Directions in Cryptography” (1976) IEEE (Institute of Electrical and Electronics Engineers) Transactions on Informational Theory 644.

Cynthia Dwork and Moni Naor “Pricing via Processing or Combatting Junk Mail” *Proceedings of Crypto 1992, Lecture Notes in Computer Science 740* (Springer, 1993) 139.

Gerald P Dwyer “The Economics of Bitcoin and Similar Private Digital Currencies” (2015) 17 Journal of Financial Stability 81.

Kurt Fanning and David P Centers “Blockchain and Its Coming Impact on Financial Services” (2016) 27(5) Journal of Corporate Accounting and Finance 53.

Percy Gardner “The Origin of Money” (1897) 11(3) The Classical Review 172.

J Michael Graglia and Christopher Mellon “Blockchain and Property in 2018: At the End of the Beginning” (2018) 12 Innovations 90.

Reuben Grinberg “Bitcoin: An Innovative Alternative Digital Currency” (2012) 4 Hastings Science & Technology Law Journal 159.

S Gruber “Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?” (2013) 32 Quinnipiac Law Review 135.

Eric Holmquist “Bitcoin and the Coming Revolution in Financial Transactions” (2014) 97(3) Risk Management Association Journal 22.

J Keith Horsefield “The Beginnings of Paper Money in England” (1977) 6 Journal of European Economic History 17.

Steve Huckle, Rituparna Bhattacharya, Martin White and Natalia Beloff “Internet of Things, Blockchain and Shared Economy Applications” (2016) 98 Procedia Computer Science 461.

Angela SM Irwin and George Milad “The Use of Crypto-currencies in Funding Violent Jihad” (2016) 19 Journal of Money Laundering Control 407.

Nikolei Kaplanov “Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation” (2012) 25 Loyola Consumer Law Review 111.

Ali Khan “The Evolution of Money: A Story of Constitutional Nullification” (1999) 67 University of Cincinnati Law Review 393.

Christine Lagarde “Central Banking and Fintech: A Brave New World” (2018) Innovations 4.

Leslie Lamport, Robert Shostak and Marshall Pease “The Byzantine Generals Problem” (1982) 4 ACM (Association for Computing Machinery) Transactions on Programming Languages and Systems 382.

Kelvin FK Low and Ernie GS Teo “Bitcoins and Other Cryptocurrencies as Property?” (2017) 9 Law, Innovation and Technology 235.

Francis T Lui “Cagan's Hypothesis and the First Nationwide Inflation of Paper Money in World History” (1983) 91 Journal of Political Economy 1067.

Omri Marian “A Conceptual Framework for the Regulation of Cryptocurrencies” (2015) 82 University of Chicago Law Review 53.

Russ Marshall “Bitcoin: Where Two Worlds Collide” (2015) 27 Bond Law Review 89.

James Martin “Lost on the Silk Road: Online Drug Distribution and the ‘Cryptomarket’” (2014) 14 Criminology & Criminal Justice 351.

Bill Maurer, Taylor C Nelms and Lana Swartz “When Perhaps the Real Problem is Money Itself!: The Practical Materiality of Bitcoin” (2013) 23(2) Social Semiotics 261.

Nick McBride “Payments and the Concept of Legal Tender” (2015) 78(6) (September 2015) <https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2015/rbb2015-78-00-01>.

Eliza Mik “Smart Contracts: Terminology, Technical Limitations and Real World Complexity” (2017) 9 Law, Innovation and Technology 269.

A Mitchell, P Sikka and H Willmott “Sweeping it Under the Carpet: The Role of Accountancy Firms in Money Laundering” (1998) 23 Accounting, Organizations and Society 569.

Al Moldof “Bitcoin Developments: The Advance of Digital Currency” (2016) 31(4) Internal Auditing 38.

Karl J O’Dwyer and David Malone “Bitcoin Mining and Its Energy Footprint” (2014) Proceedings of Irish Signals and Systems Conference 280 <https://ieeexplore.ieee.org/document/6912770/>.

Herman Oliphant “The Theory of Money in the Law of Commercial Instruments” (1920) 29 Yale Law Journal 606.

Ken C Ooi and Ross P Buckley “Pacific Injustice and Instability: Bank Account Closures of Australian Money Transfer Operators” (2014) 25 Journal of Banking and Finance Law and Practice 243.

Louise Parsons “Bitcoin protection and regulatory challenges” (2016) 27 Journal of Banking and Finance Law and Practice 184.

Morgen E Peck “The Blockchain has a Dark Side” (2016) 53(6) IEEE (Institute of Electrical and Electronic Engineers) Spectrum 12.

Gareth W Peters, Ariane Chapelle and Efstathios Panayi “Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective” (2016) 17 Journal of Banking Regulation 239.

Alexandru Pîrjan, Dana-Mihaela Petroşanu, Mihnea Huth and Mihaela Negoiță “Research Issues Regarding the Bitcoin and Alternative Coins Digital Currencies” (2015) Journal of Information Systems and Operations Management 1.

Matthew P Ponsford “A Comparative Analysis of Bitcoin and other decentralised virtual currencies: Legal Regulation in the People’s Republic of China” (2015) 9 Hong Kong Journal of Legal Studies 29.

Frederic L Pryor “The Origins of Money” (1977) 9(3) Journal of Money, Credit and Banking 391.

Max Raskin “The Law and Legality of Smart Contracts” (2017) 1 Georgetown Law Technology Review 305.

Angela Redish “Anchors Aweigh: The Transition from Commodity Money to Fiat Money in Western Economies” (1993) 26(4) Canadian Journal of Economics 777.

RD Richards “The Evolution of Paper Money in England” (1927) 41(3) The Quarterly Journal of Economics 361.

Chris Richter, Sascha Kraus and Ricarda B Bouncken “Virtual Currencies Like Bitcoin as a Paradigm Shift in the Field Of Transactions” (2005) 14(4) International Business & Economics Research Journal 575.

Chris Rose “The Evolution of Digital Currencies: Bitcoin, a Cryptocurrency Causing a Monetary Revolution” (2015) 14(4) International Business and Economics Research Journal 617.

David Rountree “Champing at the Bitcoin: Bitcoin, Regulators and the Law” (2013) 32(4) Communications Law Bulletin 5.

Alexandra Sims and Louise Mara “Unfair Online Contract Terms in New Zealand: Evaluating the Effect of Regulatory Change” (2016) 24(2) Competition and Consumer Law Journal 128.

Zoe Thomas “Why Bitcoin could be the key to banking’s future” (2014) 33(5) International Financial Law Review.

Abbott Payson Usher “The Origin of the Bill of Exchange” (1914) 22 Journal of Political Economy 566.

Andrew Van der Werff, Jeanne M Hogarth and Nathanael D Peach “A Cross-Country Analysis of Unbanked Within the OECD” (2013) 59 Consumer Interests Annual 1.

Amber Wadsworth “Decrypting the Role of Distributed Ledger Technology in Payments Processes” (2018) 81(5) Bulletin 3 (May 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018may81-05.pdf>.

Amber Wadsworth “Disruption or Distraction? How Digitisation is Changing New Zealand Banks and Core Banking Systems (2016) 79(8) Bulletin 3 (May 2016) <http://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2016/2016may79-8.pdf>.

Amber Wadsworth “The Pros and Cons of Issuing a Central Bank Digital Currency” (2018) 81(7) Bulletin 3 (June 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018jun81-07.pdf>.

Amber Wadsworth “What is Digital Currency?” (2018) 81(3) Bulletin 3 (April 2018) <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2018/2018apr81-03.pdf>.

Angela Walch “The Path of the Blockchain Lexicon (and the Law)” (2017) 36 Review of Banking and Financial Law 713.

William Watts Folwell “Evolution of Paper Money in United States” (1924) 8(7) Minnesota Law Review 561.

Kevin D Werbach and Nicolas Cornell “Contracts Ex Machina” (2017) 67 Duke Law Journal 313.

Howard Wiener, Jonathan Zelnik, Israel Tarshish and Michael Rodgers “Chomping at the Bit: U.S. Federal Income Taxation of Bitcoin Transactions” (2014) 73(4) Tax Notes International 352.

Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park and Kari Smolander “Where Is Current Research on Blockchain Technology?—A Systematic Review” (2016) 11(10) PLoS ONE 1.

Conference papers

Mustafa Ally, Michael Gardiner and Michael Lane “The Potential Impact of Digital Currencies on the Australian Economy” (paper presented to Australasian Conference on Information Systems, Adelaide, 2015).

Moez Chakchouk “Blockchain in Tunisia: From Experimentations to a Challenging Commercial Launch (slides from ITU Workshop on “Security Aspects of Blockchain” Geneva, Switzerland, 21 March 2017) <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/S3_2.%20ITU-BlockchainWS-21032017.pdf>.

George Danezis and Sarah Meiklejohn “Centrally Banked Cryptocurrencies” (paper presented to 23rd Annual Network and Distributed System Security Symposium, NDSS, San Diego, California, United States, February 2016) <http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf>.

Shayan Eskandari, David Barrera, Elizabeth Stobert and Jeremy Clark “A First Look at the Usability of Bitcoin Key Management” (paper presented to NDSS Workshop on Usable Security (USEC) 2015, San Diego, February 2015) <https://arxiv.org/abs/1802.04351>

Olivier Fournier and John J Lennard “Rebooting Money: The Canadian Tax Treatment of Bitcoin and Other Cryptocurrencies” (paper presented to Canadian Tax Foundation, 2014 Conference, held in Toronto, Canada) <https://dwpv.com/~/media/Files/PDF_EN/2015/2015-10-09-Annual-Conference-Report-Bitcoin.ashx>.

F Glaser, K Zimmermann, M Haferkorn, MC Weber and M Siering “Bitcoin – Asset or Currency? Revealing Users’ Hidden Intentions” in Proceedings of the European Conference on Information Systems (ECIS), Tel Aviv, Israel (2014) <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1131&context=ecis2014>.

Nick Groves “Exploring bank-grade Blockchain technology at ANZ” (paper presented to Blockchain Summit, Melbourne, June 2016).

Kerem Kaskaloglu “Near Zero Bitcoin Transaction Fees Cannot Last Forever” (paper presented to the International Conference on Digital Security and Forensics (DigitalSec2014), Czech Republic, June 2014) <http://sdiwc.net/digital-library/near-zero-bitcoin-transaction-fees-cannot-last-forever.html>.

Benjamin M Lawsky, Superintendent of Financial Services “NYDFS Announces Final BitLicense Framework for Regulating Digital Currency Firms” (paper presented to BITS Emerging Payments Forum, Washington DC, June 2015) <https://media.scmagazine.com/documents/127/speech_-_june_3,_2015__nydfs_a_31558.pdf>.

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker and Stefan Savage “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names” (paper presented to the ACM SIGCOMM Internet Measurement Conference, Barcelona, Spain, 2013) <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>.

Masarah Paquet-Clouston, Bernhard Haslhofer and Benoit Dupont “Ransomware Payments in the Bitcoin Ecosystem” (paper presented to 17th Annual Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, April 2018) <https://arxiv.org/pdf/1804.04080.pdf>.

Louise Parsons “Bitcoin – Sending Money Home” (paper presented to Banking and Financial Services Law Association (BFSLA) Conference, Queenstown, New Zealand, 2016) <http://bfsla.org/wp-content/uploads/papers/2016/3A%20-%20Louise%20Parsons.pdf>.

Michael Southwell “Assessing Blockchain capabilities at Westpac” (paper presented to Blockchain Summit, Melbourne, June 2016).

Whitepapers

Muneeb Ali, Ryan Shea, Jude Nelson and Michael J Freedman *Blockstack: A New Decentralized Internet* (Whitepaper, 16 May 2017) <https://pdfs.semanticscholar.org/606b/2c57cfed7328dedf88556ac657e9e1608311.pdf>.

ANZ *Distributed Ledger Technology for Reconciliation between Insurance Companies and Brokers* (Whitepaper, April 2018) <https://www.anz.co.nz/resources/f/d/fd397495-8c57-41e0-b9b6-9c51b410a8b8/Distributed-Ledger-Technology.pdf?MOD=AJPERES>.

ANZ, Westpac and IBM *Distributed Ledger Technology and Bank Guarantees for Commercial Property Leasing* (Whitepaper, July 2017) <https://bluenotes.anz.com/content/dam/bluenotes/documents/whitepaper%20_bank_guarantees_dlt_poc.pdf>.

Leemon Baird *The Swirlds Hashgraph Consensus Algorigthm: Fair, Fast, Byzantine Fault Tolerance* (Whitepaper, 31 May 2016) <http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>.

Alex Batlin, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka and Shane Williams *Building the Trust Engine* (UBS, Whitepaper, 2016) <https://www.ubs.com/microsites/blockchain-report/en/home.html?hootPostID=6d427ec622fb4f862bcab7bb4a960870>.

Richard Gendal Brown, James Carlyle, Ian Grigg and Mike Hearn *Corda: An Introduction* (Whitepaper, August 2016) <https://docs.corda.net/_static/corda-introductory-whitepaper.pdf>.

Vitalik Buterin *Ethereum White Paper: A next-generation smart contract and decentralized application platform* (Whitepaper, December 2013) <https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>.

Tyler Crain, Vincent Gramoli, Mikel Larrea and Michel Raynal *(Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains* (Whitepaper, 5 May 2017) <https://www.researchgate.net/publication/313642430_LeaderRandomizationSignature-free_Byzantine_Consensus_for_Consortium_Blockchains>.

Luis Cuende and Jorge Izquierdo *Aragon Network: A Decentralised Infrastructure for Value Exchange* (Whitepaper, Version 1.1, 20 April 2017) <https://bravenewcoin.com/assets/Whitepapers/Aragon-Whitepaper.pdf>.

Depository Trust & Clearing Corporation *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-trade Landscape* (Whitepaper, January 2016) <http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology>.

Institute for Development and Research in Banking Technology *Applications of Blockchain Technology to Banking and Financial Sector in India*, (Whitepaper, January 2017) <http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf>

Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* (Whitepaper, 2008) <https://bitcoin.org/bitcoin.pdf>.

Payments Canada, Bank of Canada and R3 *Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement* (Whitepaper, September 2017) <https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf>.

Joseph Poon and Thaddeus Drja *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* (Whitepaper, Version 0.5.9.1, 20 November 2015) <https://www.weusecoins.com/assets/pdf/library/Lightning%20Network%20Whitepaper.pdf>.

Serguei Popov *The Tangle* (Whitepaper, Version 1.3, 1 October 2017) <https://iota.org/IOTA_Whitepaper.pdf>.

Meni Rosenfeld *Overview of Colored Coins* (Whitepaper, 4 December 2012) <https://bitcoil.co.il/BitcoinX.pdf>.

Gavin Smith, Valeska Bloch, Simun Soljo and David Rountree *Blockchain Reaction: Understanding the Opportunities and Navigating the Legal Frameworks of Distributed Ledger Technology and Blockchain* (Allens, Whitepaper, 2016) <https://www.allens.com.au/general/forms/pdf/blockchainreport.pdf>.

World Economic Forum *Digital Identity: On the Threshold of a Digital Identity* (Whitepaper, January 2018) <http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf>.

Working papers

Saifedean Ammous “Blockchain Technology: What is it Good for?” (Working Paper No. 91, Columbia University Center on Capitalism and Society, 8 August 2016) <http://capitalism.columbia.edu/files/ccs/workingpage/2016/ammous_blockchain_technology_.pdf>.

Saifedean Ammous “Can Cryptocurrencies Fulfil the Functions of Money?” (Working Paper No. 92, Columbia University Center on Capitalism and Society, August 2016) <http://capitalism.columbia.edu/files/ccs/workingpage/2016/ammous_cryptocurrencies_and_the_functions_of_money.pdf>.

John Barrdear and Michael Kumhof “The Macroeconomics of Central Bank Issues Digital Currencies” (Staff Working Paper No. 605, Bank of England, July 2016) <http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>.

Adrian Blundell-Wignall “The Bitcoin Question: Currency versus Trust-less Transfer Technology” (Working Paper on Finance, Insurance and Private Pensions No. 37, OECD, 2014) <https://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf>.

Christian Catalini and Joshua S Gans “Some Simple Economics of the Blockchain” (Working Paper No. 2874598, Rotman School of Management and Sloan Research Paper No. 5191-16, MIT, 21 September 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598>.

Ben SC Fung and Hanna Halaburda “Central Bank Digital Currencies: A Framework for Assessing Why and How” (Staff Discussion Paper 2016-22, Bank of Canada, November 2016) <http://www.bankofcanada.ca/wp-content/uploads/2016/11/sdp2016-22.pdf “Central Bank Digital Currencies: A Framework for Assessing Why and How”>.

Fumiko Hayashi, Zach Markiewicz and Richard Sullivan “Chargebacks: Another Payment Card Acceptance Cost for Merchants” (Working paper No. 16-01, Federal Reserve Bank of Kansas City, January 2016) <https://www.kansascityfed.org/publications/research/rwp/articles/2016/chargebacks-payment-card-cost-merchants>.

Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko and Concepcion Verdugo-Yepes “Virtual Currencies and Beyond: Initial Considerations” (Staff Discussion Note, IMF, January 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>.

Michael Mainelli and Alistair Milne “The Impact and Potential of Blockchain on the Securities Transaction Lifecycle” (Working Paper No. 2015-007, SWIFT Institute, 9 May 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777404>.

Winston Moore and Jeremy Stephen “Should Cryptocurrencies be Included in the Portfolio of International reserves held by the Central Bank of Barbados” (Working Paper No. WP/15/16, Central Bank of Barbados, 13 November 2015) <http://www.centralbank.org.bb/Portals/0/Files/Working_Papers/2015/Should%20Cryptocurrencies%20be%20included%20in%20the%20Portfolio%20of%20International%20Reserves%20held%20by%20the%20Central%20Bank%20of%20Barbados.pdf>.

Martin Valenta and Philipp Sandner “Comparison of Ethereum, Hyperledger Fabric and Corda” (Working Paper, FSBC (Frankfurt School Blockchain Center), 17 June 2017) <http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf>.

Parliamentary and government materials

Australia

Attorney-General’s Department, Australian Government “Regulating digital currencies under Australia’s AML/CTF regime – Consultation Paper” (December 2016).

Attorney-General’s Department, Australian Government “Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations” (2016) <https://www.homeaffairs.gov.au/consultations/Documents/report-on-the-statutory-review-of-the-anti-money-laundering.pdf >.

Australian Prudential Regulation Authority “Prudential Inquiry into the Commonwealth Bank of Australia (CBA) Final Report” (April 2018) <http://www.apra.gov.au/AboutAPRA/Documents/CBA-Prudential-Inquiry_Final-Report_30042018.pdf>.

Australian Securities and Investments Commission “17-325MR ASIC Provides Guidance for Initial Coin Offerings” (28 September 2017) <http://asic.gov.au/about-asic/media-centre/find-a-media-release/2017-releases/17-325mr-asic-provides-guidance-for-initial-coin-offerings/>.

Australian Securities and Investments Commission “Initial coin offerings: INFO 225” <https://www.asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/>.

Australian Taxation Office - Goods and Services Tax Ruling GSTR 2014/3 “Goods and services tax: the GST implications of transactions involving bitcoin” <http://law.ato.gov.au/atolaw/view.htm?DocID=GST/GSTR20143/NAT/ATO/00001>.

Australian Taxation Office - Taxation Determination TD 2014/25 “Income Tax: Is Bitcoin a 'Foreign Currency' for the Purposes of Division 775 of the Income Tax Assessment Act 1997?” <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201425/NAT/ATO/00001>.

Australian Taxation Office - Taxation Determination TD 2014/26 “Income Tax: is Bitcoin a 'CGT Asset' for the Purposes of Subsection 108-5(1) of the Income Tax Assessment Act 1997?” <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201426/NAT/ATO/00001>.

Australian Taxation Office - Taxation Determination TD 2014/27 “Income Tax: Is Bitcoin Trading Stock for the Purposes of Subsection 70-10(1) of the Income Tax Assessment Act 1997?” <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201427/NAT/ATO/00001>.

Australian Taxation Office - Taxation Determination TD 2014/28 “Fringe Benefits Tax: is the Provision of Bitcoin by an Employer to an Employee in Respect of their Employment a Property Fringe Benefit for the Purposes of Subsection 136(1) of the Fringe Benefits Tax Assessment Act 1986?” <http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201428/NAT/ATO/00001>.

Australian Taxation Office - Taxation Ruling No. IT 2668 “Income tax: barter and countertrade transactions” (13 February 1992) <http://law.ato.gov.au/atolaw/view.htm?docid=ITR/IT2668/NAT/ATO/00001>.

Australian Taxation Office “Tax Treatment of Crypto-currencies in Australia – Specifically Bitcoin” (18 December 2014) <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>.

Australian Transaction Reports and Analysis Centre “Are you a digital currency exchange provider?” (24 January 2018) <http://www.austrac.gov.au/news/are-you-digital-currency-exchange-provider>.

Australian Transaction Reports and Analysis Centre “Chapter 5B - Digital currency exchange registration requirements” <http://www.austrac.gov.au/chapter-5-dce-registration-requirements>.

Australian Transaction Reports and Analysis Centre “Digital currency exchange providers: register online with AUSTRAC” (3 April 2018) <http://www.austrac.gov.au/news/digital-currency-exchange-providers-register-online-austrac>.

Australian Transaction Reports and Analysis Centre “Enrolment and registration” <http://www.austrac.gov.au/businesses/enrolment-and-registration/enrolment-and-registration>.

Australian Treasury “GST Treatment of Digital Currency” (Discussion Paper, May 2016) <http://www.treasury.gov.au/~/media/Treasury/Consultations%20and%20Reviews/Consultations/2016/GST%20treatment%20of%20digital%20currency/Key%20Documents/PDF/GST_treatment_of_digital_currency.ashx>.

Economics References Committee (Australian Senate References Committee) “Digital Currency—Game Changer or Bit Player” (August 2015) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report/>.

Canada

Canada Revenue Agency Document No. 2013-0514701I7 “Bitcoins” (23 December 2013) <http://www.canadiantaxlitigation.com/wp-content/uploads/2014/01/2013-0514701I7.txt>.

Department of Finance “Reviewing Canada’s Anti-Money Laundering and Anti-Terrorist Financing Regime” (7 February 2018) <https://www.fin.gc.ca/activty/consult/amlatfr-rpcfa-eng.pdf>.

Financial Consumer Agency of Canada “Digital Currency” <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>.

Income Tax Interpretation Bulletin IT-490 “Barter Transactions” (5 July 1982) <http://www.cra-arc.gc.ca/E/pub/tp/it490/it490-e.html>.

"Regulations Amending Certain Regulations Made under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2015" 149(27) Canada Gazette (4 July 2015) <http://gazette.gc.ca/rp-pr/p1/2015/2015-07-04/html/reg2-eng.php>.

Japan

Financial Services Agency "Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider" <https://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf>.

Financial Services Agency "Grounds for Refusing Registration, and Relevant Statutes and Regulations Pertaining to Viewpoints in Registration-Screening" <https://www.fsa.go.jp/en/news/2017/20170930-1/01.pdf>.

New Zealand

Code Committee "Code of Professional Conduct for Authorised Financial Advisers" (December 2016) <https://fma.govt.nz/assets/Code-of-Professional-Conduct-for-AFAs/Code-of-Professional-Conduct-for-AFAs.pdf>.

Department of Internal Affairs "Currency Exchange / Money Changing" (April 2014).

Department of Internal Affairs "List of Reporting Entities" <https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-List-of-Reporting-Entities?OpenDocument>.

Financial Intelligence Unit "National Money Laundering and Terrorism Financing Risk Assessment" (2018) <http://www.police.govt.nz/sites/default/files/publications/fiu-nra-2018.pdf>.

Financial Intelligence Unit "Quarterly Typology Report: First Quarter (Q1) FY 2016-2017 – Cryptocurrency" (December 2016) <http://www.police.govt.nz/sites/default/files/publications/fiu-qtr-q1-2016-17-cryptocurrency.pdf>.

Financial Markets Authority "Cryptocurrencies" <https://fma.govt.nz/investors/ways-to-invest/cryptocurrencies/>.

Financial Markets Authority "Cryptocurrency Services" <https://fma.govt.nz/compliance/cryptocurrencies/cryptocurrency-services/>.

Financial Markets Authority "Initial Coin Offers" <https://fma.govt.nz/compliance/cryptocurrencies/initial-coin-offers/>.

Financial Markets Authority "Market Operators: Who Needs to Comply" <https://fma.govt.nz/compliance/role/market-operators/who-needs-to-comply-2/>.

Inland Revenue Department "Guidance on the Common Reporting Standard for Automatic Exchange of Information" (June 2017) <http://www.ird.govt.nz/resources/c/e/ce0dd7f2-3e73-4103-833a-1d6dea19b37d/crs-guidance-final.pdf>.

Inland Revenue Department "Questions & Answers: Cryptocurrency and Tax" <http://www.ird.govt.nz/income-tax-individual/cryptocurrency-qa.html>.

Inland Revenue Department "No. 11: Whether Reumeration Paid to an Employee in Cryptocurrency is Subject to PAYE or FBT" (Issues Paper, 20 June 2018) <https://www.ird.govt.nz/resources/9/b/9be098bb-7db4-40b6-84c3-0bbb0b5b8885/irruip11.pdf>.

Ministry of Business, Innovation and Employment "Increasing the Transparency of the Beneficial Ownership of New Zealand Companies and Limited Partnerships" (Discussion Document, June 2018) <http://www.mbie.govt.nz/info-services/business/business-law/supporting-the-integrity-of-the-corporate-governance-system/increasing-transparency-beneficial-ownership-nz-companies-and-ltd-partnerships/discussion-document.pdf>.

Ministry of Business, Innovation and Employment "Retail Payment Systems in New Zealand" (Issues Paper, October 2016) <http://www.mbie.govt.nz/info-services/business/competition-policy/retail-payment-systems/retail-payment-systems-issues-paper.pdf>.

United Kingdom

Bank of England "Digital Currencies" <https://www.bankofengland.co.uk/research/digital-currencies>.

Bank of England "One Bank Research Agenda" (February 2015) <https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120>.

Financial Conduct Authority “Discussion Paper on distributed ledger technology” DP17/3 (April 2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>.

Financial Conduct Authority “Regulatory Sandbox Lessons Learned Report” (October 2017) <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>.

House of Lords “Distributed Ledger Technologies for Public Good: Leadership, Collaboration and Innovation” (November 2017) <http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf>.

United Kingdom Government “Revenue and Customs Brief 9 (2014): Bitcoin and other Cryptocurrencies” (2014) <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies>.

United Kingdom Government “VAT Finance Manual: VATFIN2330” (8 April 2016) <https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin2330>.

United Kingdom Government “VAT Finance Manual: VATFIN7200” (8 April 2016) <https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin7200>.

United Kingdom Government “VAT Notice 701/49: Finance (30 January 2013) <https://www.gov.uk/government/publications/vat-notice-70149-finance/vat-notice-70149-finance#intermediaries>.

United Kingdom HM Treasury “Digital Currencies: Response to the Call for Information” (March 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf>.

United Kingdom HM Treasury “National Risk Assessment of Money Laundering and Terrorist Financing” (October 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf>.

United Kingdom HM Treasury “UK National Risk Assessment of Money Laundering and Terrorist Financing” (October 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf>.

United Kingdom Parliament “Cryptocurrencies: Regulation: Written question – 110111” (27 October 2017).

United States

Department of the Treasury Financial Crimes Enforcement Network “FIN-2008-G008: Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities” (10 September 2008) <https://www.fincen.gov/sites/default/files/guidance/fin-2008-g008.pdf>.

Department of the Treasury Financial Crimes Enforcement Network “FIN-2013-G001: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (18 March 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

Internal Revenue Service “Notice 2014-21” (25 March 2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

Texas Department of Banking “Supervisory Memorandum – 1037” (3 April 2014) <http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf>.

Texas Department of Banking “Texas Department of Banking Commissioner Issues Cease & Desist Order Relating to AriseBank” (26 January 2018) <https://www.dob.texas.gov/public/uploads/files/news/press-releases/2018/01-26-18bpr.pdf>.

Texas State Securities Board “$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales” (4 January 2018) <https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales>.

Texas State Securities Board “Bitcoin Promoter USI-Tech Hit With Emergency Order” (Press release, 20 December 2017) <https://www.ssb.texas.gov/news-publications/bitcoin-promoter-usi-tech-hit-emergency-order>.

Texas State Securities Board “Emergency Cease and Desist Letter – In the Matter of Bitconnect” (Press release, 4 January 2018) <https://www.ssb.texas.gov/sites/default/files/BitConnect_ENF-18-CDO-1754.pdf>.

Texas State Securities Board “In the Matter of Estrada Trucking, Inc [et al]” (5 April 2018) <https://www.ssb.texas.gov/sites/default/files/ENF-18-CDO-1761.pdf>.

Reports

Australian Government *Financial System Inquiry* (2014) <http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf>.

Australian Securities and Investments Commission *Submission 44* (December 2014) <http://www.aph.gov.au/DocumentStore.ashx?id=4b6d105f-3e0a-4d52-aaab-1f35842ed5f1&subId=302297>.

Australian Transaction Reports and Analysis Centre *Typologies and Case Studies Report* (2012) <http://www.austrac.gov.au/files/typ_rprt12_full.pdf>.

Bank of Canada *Decentralized E-Money (Bitcoin)* (2014) <http://www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf>.

Bank for International Settlements *Central Bank Digital Currencies* (March 2018) <https://www.bis.org/cpmi/publ/d174.pdf>.

Bank for International Settlements, Committee on Payments and Market Infrastructures *Digital Currencies* (November 2015) <http://www.bis.org/cpmi/publ/d137.pdf>.

British Bankers' Association *Digital Disruption: UK Banking Report* (24 March 2015) <https://www.bba.org.uk/news/reports/digital-disruption-uk-banking-report/#.WwXf0yC-mUk>.

Jerry Brito and Andrea Castillo *Bitcoin: A Primer for Policymakers* (Mercatus Center, 2013) <https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf>.

Data 61 *Distributed Ledgers: Scenarios for the Australian Economy over the Coming Decades* (May 2017) <http://www.data61.csiro.au/en/Our-Work/Safety-and-security/Secure-Systems-and-Platforms/Blockchain>.

Data 61 *Risks and Opportunities for Systems using Blockchain and Smart Contracts* (May 2017) <http://www.data61.csiro.au/en/Our-Work/Safety-and-security/Secure-Systems-and-Platforms/Blockchain>.

Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar and Jake Hess *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution* (World Bank, 2018) <http://globalfindex.worldbank.org/>.

Edmund Hillary Fellowship *New Zealand: Unlocking Blockchain's Potential: Recommendations on Regulation and Policy* (December 2017) <https://static1.squarespace.com/static/57cd3bd059cc6804d1884b86/t/5a39dbbd419202030eebdc18/1513741249608/NZ+Unlocking+Blockchains+Potential+-+Dec+2017.pdf>.

European Central Bank *Virtual Currency Schemes* (2012) <http://www.ecb.europa.eu/pub/pdf/other/virtualcurren- cyschemes201210en.pdf>.

Goldman Sachs *Profiles in Innovation: Blockchain: Putting Theory into Practice* (24 May 2016) <https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf>.

TJ Horan, Frank Holzenthal and Scott Zoldi *Advancing AML Compliance with Artificial Intelligence* (FICO, 2017) <http://www.fico.com/en/node/8140?file=12318>.

Keith Horowitz, Ashwin Shirvaikar and Donald Fandetti *US Digital Banking: Could The Bitcoin Blockchain Disrupt Payments?* (Citi Research, 30 June 2016) <https://ir.citi.com/onWP8PeDTFCEOpVtHBNtpVSgNCDKcVVUBdHotDbLJ%2BjXmVXuVE8aY3W2hNxoAfPWNcuytXi1ocM%3D>.

Monetary Authority of Singapore *Project Ubin: SGD on Distributed Ledger* (2016) <http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf>.

Monetary Authority of Singapore and the Association of Banks in Singapore *Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies* (November 2017) <http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20Phase%202%20Reimagining%20RTGS.pdf>.

Edward V Murphy, M Maureen Murphy and Michael V Seitzinger *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (Congressional Research Service, 13 October 2013) <https://fas.org/sgp/crs/misc/R43339.pdf>.

New Zealand Treasury *Treasury Report: Update on Remittances to the Pacific* (T2015/34, 12 March 2015) <http://www.treasury.govt.nz/downloads/pdfs/oia/oia-20150421.pdf>.

Payments New Zealand (2014) *What is* Really *Happening with Cash in New Zealand* (June 2014).

Santander InnoVentures, Oliver Wyman and Anthemis Group *The Fintech 2.0 Paper: Rebooting Financial Services* (2016) <https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf>.

Standing Committee on Banking, Trade and Commerce (Canada) *Digital Currency: You Can't Flip this Coin!* <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rms/12jun15/home-e.htm>.

Becky Stein and Drew Lipsher *The Value of Human Capital in the Digital Age* (Korn/Ferry Institute, 1 August 2013).

Sveriges Riksbank *The Riksbank's e-krona Project, Report 1* (September 2017) <http://archive.riksbank.se/Documents/Rapporter/E-krona/2017/rapport_ekrona_170920_eng.pdf>.

Thomson Reuters *Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points* (26 October 2017) <https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html>.

Trust in Digital Life *Blockchain: Perspectives on Research, Technology & Policy* (17 June 2016) <https://trustindigitallife.eu/wp-content/uploads/2016/07/TDL_Blockchain_v1.1-_Pages.pdf>.

United Kingdom Government Chief Scientific Advisor *Distributed Ledger Technology: Beyond Block Chain* (December 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>.

United States Government Accountability Office *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks* (May 2013) <http://www.gao.gov/assets/660/654620.pdf>.

Peter Valkenburgh *Framework for Securities Regulation of Cryptocurrencies Version 1* (Coin Center Report, January 2016) <https://coincenter.org/wp-content/uploads/2016/01/SECFramework2.5.pdf>.

World Bank *Report on the Remittance Agenda of the G20* (2014) <http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1400093105293/GPFI_Remittances_Report_Final072014.pdf>.

Dissertations and theses

Muneeb Ali "Trust-to-Trust Design of a New Internet" (PhD Thesis, Princeton University, 2017) <ftp://ftp.cs.princeton.edu/techreports/2017/003.pdf>.

Natalie Chapman "Defining the Regulatory Landscape of Virtual Currencies in New Zealand" (LLB (Hons) Dissertation, University of Auckland, 2016).

Newspaper and magazine articles

"$10 Payment Paving the Way for Banking Revolution" *Stuff* (New Zealand, online ed, 22 September 2016) <http://www.stuff.co.nz/business/money/84549159/10-payment-paving-the-way-for-banking-revolution>.

"ASX to Use Blockchain to Handle Share Transactions" *The Sydney Morning Herald* (Australia, 7 December 2017) <https://www.smh.com.au/business/banking-and-finance/update-1-australias-asx-selects-blockchain-to-cut-costs-20171207-p4yxhe.html>.

"Australia's ASX Selects Blockchain to Cut Costs" *Reuters* (7 December 2017) <https://www.reuters.com/article/us-asx-blockchain/australias-asx-selects-blockchain-to-cut-costs-idUSKBN1E037R>.

"Bitcoin is Not the Answer to Central Bank Worries" *The Economic Times* (India, 11 May 2016) <https://economictimes.indiatimes.com/news/international/business/bitcoin-is-not-the-answer-to-central-bank-worries/articleshow/52215383.cms>.

"Estonia Seeks Cryptocurrency Clarification" *ForkLog* (online ed, 1 December 2015) <http://forklog.net/estonia-seeks-cryptocurrency-clarification/>.

"Exchange of Rs 500 and Rs 1,000 notes ends; can be deposited till Dec 30" *Hindustan Times* (India, 24 November 2016) <https://www.hindustantimes.com/india-news/exchange-of-currency-stopped-use-of-old-notes-for-utility-bills-extended-till-dec-15/story-S9eIPUPtMnrsuMZ2FCXpkJ.html>.

"Financial Adviser Accused of Stealing $3m" *The New Zealand Herald* (5 September 2013) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11120011 >.

"Global Card Fraud Losses Reach $16.31 Billion — Will Exceed $35 Billion in 2020 According to The Nilson Report" *Business Wire* (4 August 2015)

<http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VcJZlvlVhBc>.

"Israeli Supreme Court Forbids Bank Account Closure of Crypto Exchange" *Trustnodes* (27 February 2018) <https://www.trustnodes.com/2018/02/27/israeli-supreme-court-forbids-bank-account-closure-crypto-exchange>.

"Litecoin Cash Allegedly the Latest Small-Cap Altcoin to Suffer 51 Percent Attack" *CCN* (8 June 2018) <https://www.ccn.com/litecoin-cash-latest-small-cap-altcoin-to-suffer-51-percent-attack/>.

"Money from Nothing: Chronic Deflation may keep Bitcoin from Displacing its Fiat Rivals" *The Economist* (UK, online ed, 15 March 2014) <https://www.economist.com/news/finance-and-economics/21599053-chronic-deflation-may-keep-bitcoin-displacing-its-fiat-rivals-money>.

"More Japanese cryptocurrency exchanges to close" *Nikkei* (29 March 2018) <https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close>.

"New York's Bitcoin Hub Dreams Fade with Licensing Backlog" *CNBC* (United States, 31 October 2016) <http://www.cnbc.com/2016/10/31/new-york-bitcoin-hub-dreams-fade-with-licensing-backlog.html>.

"NPA Cryptocurrency Tips Point to 669 Suspected Money-laundering Cases from April to December" *The Japan Times* (online ed, 22 February 2018) <https://www.japantimes.co.jp/news/2018/02/22/business/npa-cryptocurrency-tips-point-669-suspected-money-laundering-cases-april-december/#.WwXi9CC-mUk>.

"NZ Bitcoin ATM Shut Down" *The New Zealand Herald* (online ed, 29 July 2014) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11300912>.

"Proof of Work vs Proof of Stake – Explained!" *Monetha* (3 January 2018) <https://blog.monetha.io/proof-work-vs-proof-stake-explained/>.

"Silk Road: US agent jailed over bitcoin theft" *BBC News* (UK, online ed, 8 December 2015) <http://www.bbc.com/news/technology-35038971>.

"Six Big Banks Join Blockchain Digital Cash Settlement Project" *Reuters* (31 August 2017) <https://www.reuters.com/article/us-blockchain-banks/six-big-banks-join-blockchain-digital-cash-settlement-project-idUSKCN1BB0UA>.

"Spanish police arrest suspected mastermind of $1 billion bank hacks" *Reuters* (27 March 2018) <https://in.reuters.com/article/cyber-banks-spain/spanish-police-arrest-suspected-mastermind-of-1-billion-bank-hacks-idINKBN1H21GX>.

"The Wild West Embraces Cryptocurrencies: Texas, Wyoming and Washington" *Crypto Insider* (30 January 2018) <https://cryptoinsider.21mil.com/the-wild-west-embraces-cryptocurrencies/>.

"Tunisia is the First Country to put National Currency on Blockchain" *FT Reporter* (29 November 2016) <http://ftreporter.com/tunisia-is-the-first-country-to-put-national-currency-on-blockchain/>.

"Venezuela orders banks to adopt cryptocurrency" *France24* (28 August 2018) <https://www.france24.com/en/20180828-venezuela-orders-banks-adopt-cryptocurrency>.

"Virtual Money Poses Accounting Dilemma for Japan's Early Adopters" *Nikkei Asian Review* (29 March 2018) <https://asia.nikkei.com/Business/Trends/Virtual-money-poses-accounting-dilemma-for-Japan-s-early-adopters>.

Jake Adelstein "Japan Shuts Down Two Cryptocurrency Exchanges But It May Be Good News For The Industry" *Forbes* (United States, 8 March 2018) <https://www.forbes.com/sites/adelsteinjake/2018/03/08/japan-shuts-down-two-cryptocurrency-exchanges-but-it-may-be-good-news-for-the-industry/#2da9e360359d>.

Chen Aizhu "China's Central Bank Plans to Launch its own Digital Currencies" *Reuters Business News* (United States, online ed, 20 January 2016) <http://www.reuters.com/article/us-china-currency-digital-idUSKCN0UY1JT>.

Shefali Anand "A Pioneer in Real Estate Blockchain Emerges in Europe" *Wall Street Journal* (United States, online ed, 6 March 2018) <https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601?mod=searchresults&page=1&pos=3>.

Grant Anderson "Why New Zealand Could Become a Cryptocurrency Leader" *Acuity* (1 December 2016) <https://www.acuitymag.com/opinion/why-new-zealand-could-become-a-cryptocurrency-leader>.

Tanya Andreasyan "Deutsche Bank Pledges Commitment to GTB and Digital" *Banking Technology* (online ed, 7 October 2016) <http://www.bankingtech.com/602201/deutsche-bank-pledges-commitment-to-gtb-and-digital/>.

Ian Apperley “How Bitcoins will be really disruptive” *The National Business Review* (New Zealand, online ed, 20 May 2016) <https://www.nbr.co.nz/article/how-bitcoins-will-be-really-disruptive-189194>.

Naoya Ariyoshi, Susumu Tanizawa and Hideki Katagiri “Japan: The Essential Points Of The Amendments To The Regulation On Virtual Currency Exchange Services” *Mondaq* (21 January 2017) <http://www.mondaq.com/x/554128/Financial+Services/The+Essential+Points+Of+The+Amendments+To+The+Regulation+On+Virtual+Currency+Exchange+Services>

Martin Arnold “Big Banks Plan to Coin New Digital Currency” *Financial Times* (UK, online ed, 24 August 2016) <https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c>.

Martin Arnold “Cryptocurrencies Companies Forced to Bank Outside UK” *Financial Times* (UK, online ed, 23 October 2017) <https://www.ft.com/content/3853358e-b508-11e7-a398-73d59db9e399>.

Ralph Atkins “Switzerland Embraces Cryptocurrency Culture” *Financial Times* (UK, online ed, 25 January 2018) <https://www.ft.com/content/c2098ef6-ff84-11e7-9650-9c0ad2d7c5b5>.

Nick Ayton “Global Custody Is About to Face Its Nemesis: Blockchain” *Innovation Enterprise* (15 August 2017) <https://channels.theinnovationenterprise.com/articles/global-custody-is-about-to-face-its-nemesis-blockchain>.

Lynsey Barber “Is Blockchain a ‘New Operating System for the Planet’? Barclays Vice Chairman Jeremy Wilson Thinks so” *CityAM* (25 January 2017) <http://www.cityam.com/257805/blockchain-new-operating-system-planet-barclays-vice>.

Omri Barzilay “Will Blockchain Ignite Fractional Ownership Market For Homes?” *Forbes* (7 August 2017) <https://www.forbes.com/sites/omribarzilay/2017/08/07/will-blockchain-ignite-fractional-ownership-market-for-homes/#1c29885b3370>.

Ben Bathgate “Jailed Financial Adviser Stole $1m From Elderly Clients” *Stuff* (New Zealand, online ed, 19 June 2015) <https://www.stuff.co.nz/business/money/69536687/jailed-financial-adviser-stole-1m-from-elderly-clients>.

James Bennett “India's Currency Recall: Concerns Mount as Cash shortage continues” *ABC* (Australia, 12 December 2016) <http://www.abc.net.au/news/2016-12-12/india's-currency-recall:-is-it-working-who-is-responsible/8111072>.

John Biggs “Sierra Leone just ran the first blockchain-based election” *TechCrunch* (United States, 15 March 2018) <https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/>.

John Bohannon “Why Criminals can’t Hide behind Bitcoin” *Science* (9 March 2016) <http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>.

Lee Boyce “Are Shops Allowed to Refuse £50 Notes even though they are Legal Tender – and will we get new Polymer ones to Beat Fakes?” *This is Money* (UK, 1 August 2017) <http://www.thisismoney.co.uk/money/experts/article-4749554/Can-shops-legally-refuse-50-notes.html>.

Charles Brett “Central Bank Cryptocurrency to Upset the Bank Applecart?” *Enterprise Times* (UK, 8 January 2018) <https://www.enterprisetimes.co.uk/2018/01/08/central-bank-cryptocurrency-to-upset-the-bank-applecart/>.

JP Buntinx “MasterCard Removes Cryptocurrency Debit Card Availability Outside EEA” *The Merkle* (12 October 2017) <https://themerkle.com/mastercard-joins-visa-in-removing-cryptocurrency-debit-card-availability-outside-of-the-eea/>.

JP Buntinx “What is the Mining Difficulty?” *The Merkle* (14 April 2017) <https://themerkle.com/what-is-the-mining-difficulty/>.

Vitalik Buterin “Bootstrapping A Decentralized Autonomous Corporation: Part I” *Bitcoin Magazine* (19 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/>.

Vitalik Buterin “Bootstrapping An Autonomous Decentralized Corporation, Part 2: Interacting With the World” *Bitcoin Magazine* (21 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-an-autonomous-decentralized-corporation-part-2-interacting-with-the-world-1379808279/>.

Vitalik Buterin “Bootstrapping a Decentralized Autonomous Corporation, Part 3: Identity Corp” *Bitcoin Magazine* (24 September 2013) <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-3-identity-corp-1380073003/>.

Vitalik Buterin “What Proof of Stake is and Why it Matters” *Bitcoin Magazine* (26 August 2013)

<https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/>.

Emily Cadman "Commonwealth Bank's Cotton Bale Blockchain Experiment could Change Trade Forever" *The Sydney Morning Herald* (Australia, online ed, 24 October 2016) <https://www.smh.com.au/business/banking-and-finance/commonwealth-banks-cotton-bale-blockchain-experiment-could-change-trade-forever-20161024-gs8x4n.html>.

Rebecca Campbell "University of Sydney's Red Belly Blockchain Scales 660,000 Transactions/Sec; 11.5x of Visa, 94,000x of Bitcoin" *Cryptocoins News* (26 October 2017) <https://www.cryptocoinsnews.com/university-sydneys-red-belly-blockchain-scales-660000-transactionssec/>.

Samantha Chang "Bitcoin Is Wrongly Linked To Mass Money-Laundering, Says Canadian Chief Scientist" *BTC Manager* (19 April 2018) <https://btcmanager.com/bitcoin-is-wrongly-linked-to-mass-money-laundering-says-canadian-chief-scientist/>.

Gertrude Chavez-Dreyfuss "Marshall Islands to Issue own Sovereign Cryptocurrency" *Reuters* (1 March 2018) <https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD>.

Henry Cooke "Student Allowance Boost Blamed for Rent Spikes" *Stuff* (New Zealand, online ed, 11 January 2018) <https://www.stuff.co.nz/national/politics/100485600/student-allowance-boost-blamed-for-rent-spikes/>.

Tatiana Cutts and David Goldstone "Bitcoin Ownership and its Impact on Fungibility" *CoinDesk* (14 June 2015) <www.coindesk.com/bitcoin-ownership-impact-fungibility/>.

Samburaj Das "AXA Uses the Public Ethereum Blockchain for Flight Delay Insurance" *Cryptocoins News* (22 September 2017) <https://www.cryptocoinsnews.com/axa-uses-ethereum-blockchain-flight-delay-insurance/>.

Joshua Davis "The Crypto-Currency: Bitcoin and its mysterious inventor" *The New Yorker* (United States, online ed, 10 October 2011) <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>.

David Dawkins "Bitcoin warning: Cryptocurrency profits to be TAXED" *Express* (UK, online ed, 27 December 2017) <https://www.express.co.uk/finance/city/897066/HMRC-Bitcoin-warning-Cryptocurrency-profits-to-be-TAXED>.

Gavin du Venage "Zimbabwe's Embrace of Bitcoin Poses Problems" *The National* (United Arab Erimates, online ed, 18 October 2017) <https://www.thenational.ae/business/zimbabwe-s-embrace-of-bitcoin-poses-problems-1.668430>.

Suparna Dutt D'Cunha "Dubai Sets Its Sights on Becoming the World's First Blockchain-Powered Government" *Forbes* (United States, 18 December 2017) <https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#3ce9fa6c454b>.

Susan Edmunds "Banks Implement New, Faster Payment Processing Systems" *Stuff* (New Zealand, online ed, 11 November 2016) <http://www.stuff.co.nz/business/86300659/Banks-implement-new-faster-payment-processing-systems>.

Susan Edmunds "Cash Payments will Always Leave a Trail Inland Revenue Says" *Stuff* (New Zealand, online ed, 21 December 2017) <https://www.stuff.co.nz/business/100078541/cash-payments-will-always-leave-a-trail-inland-revenue-says>.

Sana Elouazi "Bye-Bye Bitcoin: Morocco Bans Cryptocurrencies" *Morocco World News* (21 November 2017) <https://www.moroccoworldnews.com/2017/11/234382/bitcoin-morocco-cryptocurrencies-economy/>.

James Eyers "ASIC's Greg Medcraft says traditional bank accounts may be obsolete in a decade" *The Australian Financial Review* (online ed, 3 September 2017) <http://www.afr.com/business/banking-and-finance/financial-services/asics-greg-medcraft-says-traditional-bank-accounts-could-be-obsolete-in-a-decade-20170902-gy9k9o>.

James Eyers "Data 61 Reports Blockchain will Have a Profound Impact on the Economy" *The Australian Financial Review* (online ed, 7 June 2017) <http://www.afr.com/technology/data61-reports-blockchain-will-have-a-profound-impact-on-the-economy-20170605-gwktp9>.

Corin Faife "Canada Is Gearing Up to Regulate Cryptocurrency" *Motherboard* (21 March 2018) <https://motherboard.vice.com/en_us/article/d358zk/canada-is-gearing-up-to-regulate-cryptocurrency-parliament-hearing>.

Jesús Fernández-Villaverde “On the Economics of Currency Competition” *Vox* (3 August 2017) <https://voxeu.org/article/competition-between-government-money-and-cryptocurrencies>.

Dominic Frisby “Zimbabwe’s Trillion-dollar Note: From Worthless Paper to Hot Investment” *The Guardian* (UK, online ed, 14 May 2016) <https://www.theguardian.com/money/2016/may/14/zimbabwe-trillion-dollar-note-hyerinflation-investment>.

Gautham “Bad News for Otto De Voogd as Supreme Court Regulates Bitcoin in Estonia” *NewsBTC* (11 April 2016) <http://www.newsbtc.com/2016/04/11/otto-de-voogd-bitcoin-estonia-case/>.

Lauren Gensler “The Idiot's Guide To Laundering $9 Million” *Forbes* (United States, 11 January 2017) <https://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering/#de4b56814496>.

J Christopher Giancarlo “With Blockchain, Regulators should First do no Harm” *Financial Times* (UK, online ed, 12 April 2016) <https://www.ft.com/content/8090cc80-fff6-11e5-99cb-83242733f755>.

Samuel Gibbs “Head of Mt Gox Bitcoin Exchange on Trial for Embezzlement and Loss of Millions” *The Guardian* (UK, online ed, 11 July 2017) <https://www.theguardian.com/technology/2017/jul/11/gox-bitcoin-exchange-mark-karpeles-on-trial-japan-embezzlement-loss-of-millions>.

Eloise Gibson “Credit cards costing small businesses $100 a week” *Stuff* (New Zealand, online ed, 17 July 2015) <http://www.stuff.co.nz/business/money/70217405/credit-cards-costing-small-businesses-100-a-week>.

Amit Goel “12 Companies Leveraging Blockchain for Identification and Authentication” *Medici* (28 March 2016) < https://gomedici.com/12-companies-leveraging-blockchain-for-identification-and-authentication/>.

Amit Goel “Bank-Wise Analysis of Blockchain Activity” *Medici* (18 August 2015) <https://gomedici.com/bank-wise-analysis-of-blockchain-activity/>.

Patrick Gower “Kiwi Tech Company Centrality’s radical Data Privacy Solution” *Newshub* (New Zealand, 23 April 2018) <http://www.newshub.co.nz/home/new-zealand/2018/04/kiwi-tech-company-centrality-s-radical-data-privacy-solution.html>.

Lewis Gray “Proof of Stake Is Coming, and Will Be a Game Changer” *CCN* (7 February 2018) <https://www.ccn.com/proof-stake-coming-will-game-changer/>.

Zoe Gross “The Dark Side of the Coin: Bitcoin and Crime” *FinFeed* (5 September 2017) <https://finfeed.com/features/dark-side-coin-bitcoin-crime/>.

Robert Hackett “Why Goldman Sachs and Santander Are Bailing on R3's Blockchain Group” *Fortune* (United States, online ed, 21 November 2016) <http://fortune.com/2016/11/21/goldman-sachs-r3-blockchain-consortium/>.

Max de Haldevang “The top 50 global banks allegedly involved in a $21 billion Russian money-laundering scheme” *Quartz* (United States, 22 March 2017) <https://qz.com/938504/the-top-50-global-banks-allegedly-involved-in-the-20-8-billion-russian-laundromat-money-laundering-scheme/>.

Kevin Helms “Rollout of 260,000+ Bitcoin-Accepting Stores in Japan Begins” *Bitcoin.com* (4 July 2017) <https://news.bitcoin.com/rollout-of-260000-bitcoin-accepting-stores-in-japan-begins/>.

Kevin Helms “Russia’s Central Bank Pushes for National Cryptocurrency” *Bitcoin.com* (6 October 2017) <https://news.bitcoin.com/russias-central-bank-pushes-for-national-cryptocurrency/>.

Cat Johnson “4 Revolutionary Smart Locks that Decentralise and Automate Asset Sharing” *Shareable* (1 December 2015) <https://www.shareable.net/blog/4-revolutionary-smart-locks-that-decentralize-and-automate-asset-sharing>.

Samuel Haig “Bangladesh Authorities on ‘Hunt’ for Bitcoin Traders” *Bitcoin.com* (20 February 2018) <https://news.bitcoin.com/bangladesh-authorities-hunt-bitcoin-traders/>.

Nermin Hajdarbegovic “Assange: Bitcoin and WikiLeaks Helped Keep Each Other Alive” *Coindesk* (16 September 2014) <https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive/>.

Nathan Heller “Estonia, the Digital Republic” *The New Yorker* (United States, online ed, 18 December 2017) <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>.

Robert Herian “Why a Blockchain Startup called Govcoin Wants to ‘Disrupt’ the UK’s welfare state” *The Conversation* (28 November 2017) <https://theconversation.com/why-a-blockchain-startup-called-govcoin-wants-to-disrupt-the-uks-welfare-state-88176>.

John Herrman “The Return of the Techno-Moral Panic” *New York Times* (United States, 5 December 2017) <https://www.nytimes.com/2017/12/05/magazine/the-return-of-the-techno-moral-panic.html>.

Stan Higgins “Australian Government to Review Bitcoin Regulation Powers” *Coindesk* (20 October 2015) <http://www.coindesk.com/australian-government-to-review-bitcoin-regulation-powers/>.

Stan Higgins “China's Central Bank Discusses Digital Currency Launch” *Coindesk* (20 January 2016) <https://www.coindesk.com/peoples-bank-of-china-discusses-plans-to-issue-digital-currency/>.

Stan Higgins “New Hampshire Legislators Kill Bitcoin Tax Bill” *Coindesk* (21 January 2016) <http://www.coindesk.com/new-hampshire-legislators-vote-down-bitcoin-tax-bill/>.

Stan Higgins “New York Lawmakers Open to Revisiting the Bitlicense” *Coindesk* (23 February 2018) <https://www.coindesk.com/bitcoin-crypto-ny-lawmaker-pledges-make-bitlicense-something-works/>.

Casey Hynes “Meet The Cryptocurrency Startups Targeting The $26 Billion Remittance Industry In The Philippines” *Forbes* (United States, 15 September 2017) <https://www.forbes.com/sites/chynes/2017/09/15/meet-the-cryptocurrency-startups-targeting-the-26-billion-remittance-industry-in-the-philippines/#3df86f505510>.

Adam James “Venezuela Decrees Petro ‘Cryptocurrency’ as Legal Tender” *Bitcoinist* (14 April 2018) <http://bitcoinist.com/venezuela-decree-accept-petro-legal-tender/>.

Claire Jones “The History of Paper Money” *Financial Times* (UK, online ed, 11 September 2013) <https://www.ft.com/content/f11c6126-1a39-11e3-93e8-00144feab7de>.

Pragati Kapoor “Exchange of old Rs 500, Rs 1,000 notes worth Rs 4,000 allowed only once till RBI review” *The Economic Times* (India, online ed, 11 November 2016) <http://economictimes.indiatimes.com/wealth/personal-finance-news/exchange-of-old-rs-500-rs-1000-notes-worth-rs-4000-allowed-only-once-till-rbi-review/articleshow/55369778.cms>.

Jack Karsten and Darrell M West “Venezuela’s ‘Petro’ Undermines other Cryptocurrencies – and International Sanctions” *Brookings* (United States, 9 March 2018) <https://www.brookings.edu/blog/techtank/2018/03/09/venezuelas-petro-undermines-other-cryptocurrencies-and-international-sanctions/>.

Garrett Keirns “Japan's Bitcoin Law Goes Into Effect Tomorrow” *Coindesk* (31 March 2017) <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/>.

Jemima Kelly “UBS Leads Team of Banks Working on Blockchain Settlement system” *Reuters* (24 August 2016) <http://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147>.

Thomas Kerin “The Year of Multisig: How is it Doing So Far?” *Coindesk* (17 May 2014) <https://www.coindesk.com/year-multisig-so-far/>.

C Edward Kelso “Nepal Continues Crackdown, Two More Bitcoiners Arrested” *Bitcoin.com* (6 November 2017) <https://news.bitcoin.com/nepal-continues-crackdown-two-more-bitcoiners-arrested/>.

Julia Kollewe “Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears” *The Guardian* (UK, online ed, 4 December 2017) <https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity>.

Rachel Koning Beals “Hacked Japanese Cryptocurrency Exchange Coincheck Refunds Customers” *Marketwatch* (13 March 2018) <https://www.marketwatch.com/story/hacked-japanese-cryptocurrency-exchange-coincheck-refunds-customers-2018-03-13>.

Stephen Lacey “The Energy blockchain: How Bitcoin Could be a Catalyst for the Distributed Grid” *GreenTech Media* (26 February 2016) <https://www.greentechmedia.com/articles/read/the-energy-Blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid>.

Daniel Lanyon “New Research Reveals the IT Crowd are Expecting Huge Change from Blockchain Technology” *Alt Fi* (23 April 2018) <http://www.altfi.com/article/4334_blockchain-will-be-as-transformative-as-the-internet>.

Issie Lapowsky “Banks Deploy AI to Cut off Terrorists’ Funding” *Wired* (9 July 2017) <https://www.wired.com/story/quantaverse-ai-terrorist-funding/>.

Sherman Lee “Explaining Stable Coins, The Holy Grail of Cryptocurrency” *Forbes* (United States, 12 March 2018) <https://www.forbes.com/sites/shermanlee/2018/03/12/explaining-stable-coins-the-holy-grail-of-crytpocurrency/#202584374fc6>.

Matthew Leising “U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether” *Bloomberg* (United States, 31 January 2018) <https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc>.

Kif Leswing "The Winklevoss Twins Cut up the Key to their $1.3 Billion Bitcoin Fortune and Keep Each Piece in Different Bank Vaults" *Business Insider Australia* (20 December 2017) <https://www.businessinsider.com.au/winklevoss-twins-cut-up-key-to-protect-their-bitcoin-fortune-2017-12?r=US&IR=T>.

Tyler Lindholm and Caitlin Long "A Haven for Blockchain: The Case for Wyoming" *CoinDesk* (27 January 2018) <https://www.coindesk.com/haven-blockchain-case-wyoming/>.

Coco Liu "Forget China: Hong Kong, Singapore are New Kids on the Blockchain" *South China Morning Post* (23 April 2018) <https://www.scmp.com/week-asia/business/article/2142682/forget-china-hong-kong-singapore-are-new-kids-blockchain>.

Ilya Lopatin "Blockchain and Bitcoin in Estonia: How the Industry Is Shaping the Country's Future" *ForkLog* (7 February 2017) <http://forklog.net/blockchain-and-bitcoin-in-estonia-how-the-industry-is-shaping-the-countrys-future/>.

Sterlin Lujan "New Hampshire's Bill to Deregulate Bitcoin Effective Next Week" *Bitcoin.com* (25 July 2017) <https://news.bitcoin.com/new-hampshires-pro-bitcoin-bill-effective-next-week/>.

Richard MacManus "Bitcoin Startups Stalled by Banks" *Newsroom* (New Zealand, 28 June 2017) <https://www.newsroom.co.nz/2017/06/18/34731/bitcoin-startups-stalled-by-banks>.

Nikki Mandow "China's Alipay to join NZ's Eftpos network" *Newsroom* (New Zealand, 14 March 2018) <https://www.newsroom.co.nz/2018/03/14/96629/alibaba-coming-to-an-eftpos-terminal-near-you>.

Jim Manning "The Raiden Network Could Allow Instant Transactions in Ethereum" *Eth News* (5 November 2016) <https://www.ethnews.com/the-raiden-network-could-allow-instant-transactions-in-ethereum>.

Belén Marty "Bolivia Not Revolutionary Enough to Tolerate Bitcoin" *Panam Post* (10 July 2014) <https://panampost.com/belen-marty/2014/06/19/bolivia-not-revolutionary-enough-to-tolerate-bitcoin/>.

Jack Marx "Will Crime be the End of Bitcoin?" *CEO Magazine* (online ed, May 2017) <https://www.theceomagazine.com/business/will-crime-be-the-end-of-bitcoin>.

Nick McKenzie, Richard Baker and Georgina Mitchell "Australian Banks are Exposed to Millions in Money Laundering" *Stuff* (New Zealand, online ed, 15 September 2017) <https://www.stuff.co.nz/business/world/96869035/australian-banks-are-exposed-to-millions-in-money-laundering>.

Richard Meadows "Q&A: Are Australian banks really rorting New Zealanders?" *Stuff* (New Zealand, online ed, 3 November 2016) <http://www.stuff.co.nz/business/money/73626116/Q-A-Are-Australian-banks-really-rorting-New-Zealanders>.

Lucas Mearian "Will blockchain run afoul of GDPR? (Yes and no)" *Computer World* (online ed, 7 May 2018) <https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html>.

Giorgio Milki "The Case for National Digital Currencies" *Kapron Asia* (14 December 2017) <https://www.kapronasia.com/blockchain-research-menu-item/item/914-a-growing-number-of-countries-are-creating-their-own-digital-currencies.html>.

Jonathan Millet "Estonian Bank LHV Brings Aboard Virtual Currency Expert" *NewsBTC* (13 June 2014) <http://www.newsbtc.com/2014/06/13/estonian-bank-lhv-brings-aboard-virtual-currency-expert/>.

Geof Mortlock "How Safe are your Deposits if a Bank Fails?" *Stuff* (New Zealand, online ed, 8 April 2016) <http://www.stuff.co.nz/business/opinion-analysis/78727017/How-safe-are-your-deposits-if-a-bank-fails>.

Bianca Mueller "GDPR Compliance in Four Steps" (2017) 913 *Law Talk* (New Zealand, 1 December 2017) <https://www.lawsociety.org.nz/practice-resources/practice-areas/privacy/gdpr-compliance-in-four-steps>.

Nate Murray "100 Cryptocurrencies Described in Four Words or Less" *TechCrunch* (United States, 20 November 2017) <https://techcrunch.com/2017/11/19/100-cryptocurrencies-described-in-4-words-or-less/>.

Sarah Murray "Blockchain can Create Financial Sector Jobs as well as Kill them" *Financial Times* (UK, online ed, 7 September 2016) <https://www.ft.com/content/3a9ef8d8-33d5-11e6-bda0-04585c31b153>.

Anirban Nag and Vrishti Beniwal "India's Scramble to Switch 23 Billion Banknotes: QuickTake Q&A" *Bloomberg* (United States, 15 November 2016) <https://www.bloomberg.com/news/articles/2016-11-15/india-s-scramble-to-switch-23-billion-banknotes-quicktake-q-a>.

Marten Nelson "What is Programmable Money?" *Payments Journal* (23 March 2017) <http://paymentsjournal.com/What-Is-Programmable-Money/?/>.

Annie Nova “Some Cryptocurrency-backed Debit Cards Dropped from Visa Network, Leaving Users Scrambling” *CNBC* (United States, 5 January 2018) <https://www.cnbc.com/2018/01/05/some-cryptocurrency-backed-cards-dropped-from-visa-network.html>.

Matt O’Brien “Venezuela’s Cryptocurrency is One of the Worst Investments Ever” *Washington Post* (United States, 5 March 2017) <https://www.washingtonpost.com/news/wonk/wp/2018/03/05/venezuelas-cryptocurrency-is-one-of-the-worst-investments-ever/?noredirect=on&utm_term=.734d941a0624>.

Justin O’Connell “Is a Lack of Regulation Stifling Bitcoin Growth?” *CCN* (23 July 2017) <https://www.cryptocoinsnews.com/lack-regulation-stifling-bitcoin-growth/>.

Justin O’Connell “The Quick Death of the Zero-Fee Bitcoin Transaction” *Crypto Coins News* (21 May 2016) <https://www.cryptocoinsnews.com/death-zero-fee-bitcoin-transaction/>.

Ouriel Ohayon “The Sad State of Cryptocurrency Custody” *TechCrunch* (United States, 2 February 2018) <https://techcrunch.com/2018/02/01/the-sad-state-of-crypto-custody/>.

Mike Orcutt “Criminals Thought Bitcoin was the Perfect Hiding Place, but They Thought Wrong” *The MIT Technology Review* (United States, 11 September 2017) <https://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong/>.

SP “Why India scrapped its two biggest bank notes” *The Economist* (UK online ed, 14 November 2016) <http://www.economist.com/blogs/economist-explains/2016/11/economist-explains-6>.

Danny Palmer “How Bitcoin Helped Fuel an Explosion in Ransomware Attacks” *ZDNet* (22 August 2016) <https://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/>.

Danny Palmer “Ransomware: Why the Crooks are Ditching Bitcoin and Where they are Going Next” *ZDNet* (15 February 2018) <https://www.zdnet.com/article/ransomware-why-the-crooks-are-ditching-bitcoin-and-where-they-are-going-next/>.

Luke Parker “For Bitcoin, is Being a Store of Value More Important Than a Payment System?” *Coindesk* (17 November 2017) <https://bravenewcoin.com/news/for-bitcoin-is-being-a-store-of-value-more-important-than-a-payment-system/>.

Chris Pash “ANZ and Westpac just successfully used blockchain on commercial property deals” *Business Insider Australia* (10 July 2017) <https://www.businessinsider.com.au/anz-and-westpac-just-successfully-used-blockchain-on-commercial-property-deals-2017-7>.

Aivar Pau “Supreme Court subjects Bitcoins trade to money laundering rules” *Postimees* (Estonia, online ed, 12 April 2016) <http://news.postimees.ee/3652435/supreme-court-subjects-bitcoins-trade-to-money-laundering-rules>.

Sarah Perez “Civic Launches a Free Service that Aims to Stop Identity Theft Before it Happens” *TechCrunch* (United States, 20 July 2016) <https://techcrunch.com/2016/07/19/civic-launches-a-free-service-that-aims-to-stop-identity-theft-before-it-happens/>.

Julie Pitta “Requiem for a Bright Idea” *Forbes* (United States, online ed, 1 November 1999) <http://www.forbes.com/forbes/1999/1101/6411390a.html>.

Aarron Pressman “How an Amazon Self-Published Book May Be the Latest Money Laundering Scam” *Fortune* (United States, 11 February 2018) <http://fortune.com/2018/02/22/money-laundering-books-amazon/>.

John Quiggin “Bitcoins are a Waste of Energy – Literally” *ABC News* (Australia, 6 October 2015) <http://www.abc.net.au/news/2015-10-06/quiggin-bitcoins-are-a-waste-of-energy/6827940>.

Kenneth Rapoza “Cryptocurrency Exchanges Officially Dead in China” *Forbes* (United States, 2 November 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/?ss=markets#6ff36de32a83>.

Jamie Redman “New Zealand Exchange Bitnz Shuts Down Due to ‘Banking Hostility’” *Bitcoin.com* (14 February 2018) <https://news.bitcoin.com/new-zealand-exchange-bitnz-shuts-down-banking-hostility/>.

Yolanda Redrup “UBS invests big in blockchain future” *The Australian Financial Review* (online ed, 3 October 2016) <http://www.afr.com/technology/ubs-invests-big-in-blockchain-future-20160926-groidr>.

Madison Reidy “NZ Businesses Want GST Law Change as International Online Retailers Pocket Government Millions” *Stuff* (New Zealand, online ed, 6 July 2017) <https://www.stuff.co.nz/business/94400111/nz-businesses-want-gst-law-change-as-international-online-retailers-pocket-government-millions>.

Ellie Rennie and Jason Potts “The DAO: A Radical Experiment that could be the Future of Decentralised Governance” *The Conversation* (Australia, 11 May 2016) <https://theconversation.com/the-dao-a-radical-experiment-that-could-be-the-future-of-decentralised-governance-59082>.

Pete Rizzo “Kyrgyzstan: Bitcoin Payments Violate State Law” *Coindesk* (4 August 2014) <https://www.coindesk.com/kyrgyzstan-bitcoin-payments-violate-state-law/>.

Daniel Roberts “Behind the ‘Exodus’ of Bitcoin Startups from New York” *Fortune* (14 August 2015) <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>.

Everett Rosenfeld “Ecuador Becomes the First Country to Roll out its own Digital Cash” *CNBC* (United States, 6 February 2015) <https://www.cnbc.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html>.

Holly Ryan “Bank closes Cryptopia account” *The New Zealand Herald* (online ed, 31 January 2018) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11985380>.

Holly Ryan “‘Netflix’ Tax to Take Effect from Tomorrow” *The New Zealand Herald* (online ed, 30 September 2016) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11720057>.

Livine Sanchez “Mass adoption: Chiasso, Switzerland to Accept Tax Payment in Bitcoin” *ZyCrypto* (10 September 2017) <https://zycrypto.com/chiasso-switzerland-accept-tax-bitcoin/>.

Marco Santori “Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise” *Coindesk* (5 May 2017) <https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/>.

Peter Sayer “5 Enterprise-related Things you can do with Blockchain Technology Today” *PCWorld* (online ed, 12 December 2016) <http://www.pcworld.co.nz/article/611448/5-enterprise-related-things-can-do-blockchain-technology-today/>.

Kai Sedgwick “Bitcoin fees have become infeasible” *Bitcoin.com* (17 December 2017) <https://news.bitcoin.com/bitcoin-fees-have-become-infeasible/>.

Daniel Shane $530 Million Cryptocurrency Heist may be Biggest Ever” *CNNTech* (United States, 29 January 2018) <http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html>.

Laura Shin “Canada Has Been Experimenting with a Digital Fiat Currency Called CAD-COIN” *Forbes* (United States, 16 June 2016) <https://www.forbes.com/sites/laurashin/2016/06/16/canada-has-been-experimenting-with-a-digital-fiat-currency-called-cad-coin/#4b1985fe46a4>.

Lionel Shriver “Why Cryptocurrency is the Answer” *The Spectator* (UK, 6 January 2018) <https://www.spectator.co.uk/2018/01/why-cryptocurrencies-are-the-answer/>.

Mazin Sidahmed “Bitcoin 'Not Real Money' says Miami Judge in Closely Watched Ruling” *The Guardian* (UK, online ed, 26 July 2017) <https://www.theguardian.com/technology/2016/jul/26/bitcoin-not-real-money-miami-judge>.

Jessica Sier “ASX working on industrial strength blockchain platform” *The Sydney Morning Herald* (Australia, online ed, 28 September 2016) <http://www.smh.com.au/business/markets/asx-working-on-industrial-strength-Blockchain-platform-20160927-grp9gu.html>.

Jessica Sier “CBA joins global banks in project to explore bitcoin model” *The Australian Financial Review* (online ed, 16 September 2015) <http://www.afr.com/technology/cba-joins-global-banks-in-bitcoin-research-20150916-gjo40b>.

Tim Simonite “The Decentralized Internet is Here, with Some Glitches” *Wired* (3 May 2018) <https://www.wired.com/story/the-decentralized-internet-is-here-with-some-glitches/>.

Alex Sims “Forget Bitcoin, Blockchain Technology is Much Bigger” *Stuff* (New Zealand, 17 December 2017) <https://www.stuff.co.nz/business/opinion-analysis/99905784/forget-bitcoin-blockchain-technology-is-much-bigger>.

Alex Sims “Money and its Myths” *Newsroom* (New Zealand, 4 July 2018) <https://www.newsroom.co.nz/@future-learning/2018/07/03/137959/the-myths-surrounding-money>.

Alexandra Sims “How smart contracts could radically transform health and safety” *The National Business Review* (New Zealand, 24 February 2017).

Alexandra Sims “Why Blockchain Challenges Conventional Thinking about Intellectual Property” *The Conversation* (Australia, 27 February 2018) <https://theconversation.com/why-blockchain-challenges-conventional-thinking-about-intellectual-property-91469>.

Pattrick Smellie “How Anti-money-laundering Measures can Hurt Migrant Workers” *Listener* (New Zealand, online ed, 22 July 2016) <http://www.noted.co.nz/money/investment/how-anti-money-laundering-measures-can-hurt-migrant-workers/>.

Paul Smith “ACCC Clears Australian Banks of Colluding to Block Bitcoin Competition” *The Australian Financial Review* (15 February 2016) <http://www.afr.com/technology/accc-clears-australian-banks-of-colluding-to-block-bitcoin-competition-20160205-gmmxmc>.

Paul Smith “ACCC Investigating Banks’ Closure of Bitcoin Companies’ Accounts” *The Australian Financial Review* (online ed, 19 October 2015) <http://www.afr.com/technology/big-banks-cut-off-accounts-of-bitcoin-companies-in-battle-for-the-future-of-payments-20150921-gjr7hu>.

Paul Smith “RBA Governor Glenn Stevens backs blockchain and tech disruptors” *The Australian Financial Review* (online ed, 16 December 2015) <http://www.afr.com/technology/rba-governor-glenn-stevens-backs-Blockchain-and-tech-disruptors-20151215-glnsnm#ixzz4SbQw5ON3>.

John Southurst “Coinbase Secures Approval to Launch Regulated US Bitcoin Exchange” *CoinDesk* (25 January 2015) <http://www.coindesk.com/coinbase-secures-approval-launch-regulated-us-bitcoin-exchange/>.

Rob Stock “Merchant Anger Rising at Growing Cost of ‘Interchange' on Credit and Debit Cards” *Stuff* (New Zealand, online ed, 2 November 2015) <http://www.stuff.co.nz/business/73515906/Merchant-anger-rising-at-growing-cost-of-interchange-on-credit-and-debit-cards>.

Clifford Stoll “Why the Web Won’t be Nirvana” *Newsweek* (United States, online ed, 27 February 2017) <http://europe.newsweek.com/clifford-stoll-why-web-wont-be-nirvana-185306?rm=eu>.

Tsubasa Suruga “Asian fintechs are in infancy with much potential, says BNY Mellon CIO” *Nikkei Asian Review* (online ed, 14 November 2016) <http://asia.nikkei.com/Business/Trends/Asian-fintechs-are-in-infancy-with-much-potential-says-BNY-Mellon-CIO>.

Ana Swanson “Why Bitcoin just had an Amazing Year” *Washington Post* (United States, online ed, 3 January 2017) <https://www.washingtonpost.com/news/wonk/wp/2017/01/03/why-bitcoin-just-had-an-amazing-year/?utm_term=.6ba4a8feecce>.

Yuko Takeo and Maiko Takahashi “Crypto Investors Face Tax of Up to 55% in Japan” *Bloomberg Technology* (United States, 9 February 2018) <https://www.bloomberg.com/news/articles/2018-02-08/crypto-investors-in-japan-face-tax-of-up-to-55-on-their-takings>.

Evelyn Tapia “ECB Will Stop Opening New Electronic Money Accounts” *El Comercio* (Peru, 29 December 2017) <http://www.elcomercio.com/actualidad/bce-cuentas-dineroelectronico-banca-reactivacion.html>.

Emiko Terazono “Bitcoin gets Official Blessing in Japan” *Financial Times* (UK, online ed, 18 October 2017) <https://www.ft.com/content/b8360e86-aceb-11e7-aab9-abaa44b1e130>.

Pascal Thellmann “There Are Currently Over 5300 ERC-20 Tokens – What Are They All For?” *Cointelegraph* (18 August 2017) <https://cointelegraph.com/news/there-are-currently-over-5300-erc-20-tokens-what-are-they-all-for>.

Matthew Theunissen “Car hire business to pay heavy price for client's alleged fraud” *The New Zealand Herald* (online ed, 19 November 2017) <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11944268>.

Helen Thompson “Imagine the Trust: the Role of Blockchain in Financial Services” *Coindesk* (27 February 2016) <https://www.coindesk.com/imagining-the-role-of-blockchain-in-financial-services/>.

Jenée Tibshraeny “Founder of the World's Second Largest Digital Currency Urges Regulators to get Banks to Stop Blanket De-risking; RBNZ ‘Generally Comfortable’ with Banks’ Approaches to Cryptocurrency” *Interest.co.nz* (New Zealand, 12 May 2017) <https://www.interest.co.nz/business/87670/founder-worlds-second-largest-digital-currency-urges-regulators-get-banks-stop>.

Jenée Tibshraeny “What the NZ Retail Payments Industry is Doing to Facilitate Open Banking and Reduce Merchant Fees to Keep the Government Happy and Avoid Regulation” *Interest.co.nz* (New Zealand, 18 April 2017) <https://www.interest.co.nz/business/93246/what-nz-retail-payments-industry-doing-facilitate-open-banking-and-reduce%C2%A0merchant>.

Jenée Tibshraeny “The IRD says People Should Consider Money made Selling Cryptocurrencies Bought with the Intention of Resale as Taxable, until it Releases Specific Guidance on the Matter” *Interest.co.nz* (New Zealand, 11 January 2018) <https://www.interest.co.nz/personal-finance/91564/ird-says-people-should-consider-money-made-selling-cryptocurrencies-bought>.

James Titcomb “How Bitcoin has become Zimbabwe's Crisis Currency” *The Telegraph* (UK, online ed, 17 November 2017) <https://www.telegraph.co.uk/technology/2017/11/20/bitcoin-has-become-zimbabwes-crisis-currency/>.

Mathew Tompkins “Japans Largest Financial Group to Launch Own Virtual Currency” *Bitcoinist* (16 January 2018) <http://bitcoinist.com/japans-largest-financial-group-launch-virtual-currency/>.

Ott Ummelas and Milda Seputyte “Bitcoin ‘Ponzi’ Concern Sparks Warning From Estonia Bank” *Bloomberg* (1 February 2014) <https://www.bloomberg.com/news/articles/2014-01-30/bitcoin-ponzi-scheme-worry-sparks-estonia-central-bank-caution>.

Victoria van Eyk “What Canada's New Regulations Mean for Bitcoin Businesses” *CoinDesk* (24 June 2014) <http://www.coindesk.com/canadas-new-regulations-mean-bitcoin-businesses/>.

Gareth Vaughan “IRD says Bitcoin should be Treated in the same manner as Foreign Currencies for Tax Purposes” *Interest.co.nz* (New Zealand, 23 July 2014) <http://www.interest.co.nz/personal-finance/71048/ird-says-bitcoin-should-be-treated-same-manner-foreign-currencies-tax>.

John Weru Maina “AB 129 – California Legally Approves the Use of Bitcoin” *CryptoCoinsNews* (online ed, 5 January 2015) <https://www.cryptocoinsnews.com/ab-129-california-legally-approves-use-bitcoin/>.

Larry White “Defending Dollarization in Ecuador” *Alt-M* (4 December 2014) <https://www.alt-m.org/2014/12/04/defending-dollarization-in-ecuador/>.

Larry White “The World's First Central Bank Electronic Money Has Come – And Gone: Ecuador, 2014-2018” *Alt-M* (29 March 2018) <https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/>.

Jen Wieczner “Bitcoin Investors Aren't Paying Their Cryptocurrency Taxes” *Fortune* (United States, 13 February 2018) <http://fortune.com/2018/02/13/bitcoin-cryptocurrency-tax-taxes/>.

Jen Wieczner “Inside New York's BitLicense Bottleneck: An 'Absolute Failure’” *Fortune* (United States, 25 May 2018) <http://fortune.com/2018/05/25/bitcoin-cryptocurrency-new-york-bitlicense/>.

David Wigan “Blockchain will make Dodd Frank Obsolete, Bankers Say” *International Financing Review Asia* (online ed, 15 September 2015) <http://www.ifrasia.com/blockchain-will-make-dodd-frank-obsolete-bankers-say/21216014.fullarticle>.

Carolyn Wilkins “Project Jasper: Lessons From Bank of Canada's First Blockchain Project” *Coindesk* (10 February 2017) <https://www.coindesk.com/project-jasper-lessons-bank-of-canada-blockchain-project/>.

Pamela Williams “How Criminal Gangs Ran Rings Around Commonwealth Bank Culture” *The Australian* (14 September 2017) <https://www.theaustralian.com.au/news/inquirer/austrac-uncovers-unreported-money-laundering-at-commonwealth-bank/news-story/66e21b2a59faf2cf3fad10acc013be8c>.

Oscar Williams-Grut “A London Startup is Launching a Debit Card that Lets you Spend Bitcoin and Ethereum” *Business Insider Australia* (15 November 2017) <https://www.businessinsider.com.au/london-block-exchange-launches-prepaid-cryptocurrency-debit-card-2017-11?r=UK&IR=T>.

David Wilson “Why Electronic Banking Transactions Can Take so Much Time” *The Sydney Morning Herald* (Australia, online ed, 21 August 2014) <http://www.smh.com.au/money/planning/why-electronic-banking-transactions-can-take-so-much-time-20140821-106v32.html>.

Chloe Winter “Storm Cuts Power to Cellphone Towers, Makes Life Hard for Retailers in Auckland” *Stuff* (New Zealand, online ed, 11 April 2018) <https://www.stuff.co.nz/business/103005351/Storm-cuts-power-cellphone-towers-makes-life-hard-for-retailers-in-Auckland>.

Joon Ian Wong “Sweden’s Blockchain-powered Land Registry is Inching Towards Reality” *Quartz* (United States, 3 April 2017) <https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/>.

Tim Worstall “UBS and Other Banks Are Not Creating A New Digital Currency - It's Blockchain Settlement Not Money” *Forbes* (United States, online ed, 24 August 2016) <http://www.forbes.com/sites/timworstall/2016/08/24/ubs-and-other-banks-are-not-creating-a-new-digital-currency-its-blockchain-settlement-not-money/2/#f0790d146304>.

Will Yakowicx "Startups Helping the FBI Catch Bitcoin Criminals" *Inc* (9 January 2018) <https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html>.

Felix Yang "Wechat's Loan Platform is Already On-par with some of the Biggest Banks in China" *Kapron Asia* (7 September 2017) <https://www.kapronasia.com/china-banking-research-category/item/889-wechat-loan-blows-retail-banking-with-rmb100-billion-loans-in-two-years.html>.

Clancy Yeates "Real time payments overhaul coming in 2017" *The Sydney Morning Herald* (online ed, 27 December 2017) <http://www.smh.com.au/business/banking-and-finance/real-time-payments-overhaul-coming-in-2017-20161206-gt50sv.html>.

Fan Yikei "On Digital Currencies, Central Banks Should Lead" *Bloomberg* (United States, 2 September 2016) <https://www.bloomberg.com/view/articles/2016-09-01/on-digital-currencies-central-banks-should-lead>

Zhang Yuzhe and Han Wei "PBOC Set to be First to Issue Digital Bills" *Caixin* (China, 26 January 2017) <https://www.caixinglobal.com/2017-01-26/101049103.html>.

Patents

Ralph Merkle, US Patent 4309569A, "Method of Providing Digital Signatures" (5 January 1982).

Internet resources

"All about Bitcoin" (11 March 2014) Global Macro Research Top of Mind 21, Goldman Sachs <https://www.coursehero.com/file/15396844/GoldmanSachs-Bit-Coin/>.

"All about SWIFT payments" (2017) Nationwide <http://www.nationwide.co.uk/support/payments-and-transfers/specialist-payments/swift-payments>.

"Banking Is Only The Beginning: 42 Big Industries Blockchain Could Transform" (21 June 2018) CB Insights <https://www.cbinsights.com/research/industries-disrupted-blockchain/?utm_source=CB+Insights+Newsletter&utm_campaign=dd4b870866-ThursNL_06_21_2018&utm_medium=email&utm_term=0_9dc0513989-dd4b870866-89762513>.

"Bitcoin Price Chart with Historic Events" 99 Bitcoins <https://99bitcoins.com/price-chart-history/>.

"Blockchain: Is My ICO an Security of Utility Coin" (6 November 2017 <http://7marketingmedia.com/blog/2017/11/6/blockchain-is-my-ico-a-security-or-utility-coin.>

"Coincheck Hacking and what it says about NEM" (4 February 2018) Medium <https://medium.com/nemofficial/coincheck-hacking-and-what-it-says-about-nem-b4f3a7b00534>.

"Crypto-Currency Market Capitalizations" (2017) CoinMarketCap <https://coinmarketcap.com/>.

"CUBER – LHV Bank started public use of blockchain technology by issuing securities" (8 June 2015) Cuber <http://www.cuber.ee/en_US/news/>.

"History of bitcoin" (last modified 13 February 2017) Wikipedia <https://en.wikipedia.org/wiki/History_of_bitcoin>.

"How Legal is Bitcoin and Crypto Currencies?" (18 November 2016) CryptoCompare <https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies/>.

"How Long do International Bank Transfers Take?" (2 August 2017) Fexco <https://fexco.com/fexco/news/how-long-international-bank-transfers-take/>

"How long does it take to get my money using PayPal Invoicing?" PayPal <https://www.paypal.com/us/selfhelp/article/How-long-does-it-take-to-get-my-money-using-PayPal-Invoicing-FAQ3140>.

"Japan And Tax On Cryptocurrency – Part 1" Tyton <https://www.tytoncapital.com/investment-advice-japan/japan-and-tax-on-cryptocurrency-bitcoin/>.

"New York's Final 'BitLicense' Rule: Overview and Changes from July 2014 Proposal**"** (5 June 2015) Davis Polk <https://www.davispolk.com/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf>.

"R3 and TradeIX Devlop Open Account Trade Finance DLT Business Network" (26 September 2017) R3 <https://www.r3.com/blog/2017/09/26/r3-and-tradeix-develop-open-account-trade-finance-dlt-business-network/>.

"Santander Joins Forces with Other Banks Create a Steering Group to Develop Instant International Transfers" (23 September 2016) Santander <http://www.santander.com/csgs/Satellite/CFWCSancomQP01/es_ES/Corporativo/Sala-de-

comunicacion/Santander-Noticias/2016/09/23/Santander-y-otros-bancos-lanzan-un-comite-para-impulsar-las-transferencias-internacionales-instantaneas.html?leng=en_GB>.

"Shamrock: Self-contained High Assurance Micro Crypto and Key-management Processor" MIT Technology Licensing Office <https://tlo.mit.edu/technologies/shamrock-self-contained-high-assurance-micro-crypto-and-key-management-processor>.

"Streamlined Real-time Settlement Euroclear UK & Ireland's CREST system" Euroclear <https://www.euroclear.com/dam/PDFs/Settlement/EUI/MA2740-CREST-settlement.pdf>.

"The Nilson Report" (October 2016) <https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf>.

"Transaction fees" (22 November 2016) bitcoinwiki <https://en.bitcoin.it/wiki/Transaction_fees>.

"What is the GHOST protocol for Ethereum?" (29 February 2016) CryptoCompare <https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/>.

"Why is Ethereum different to Bitcoin?" (6 September 2016) CryptoCompare <https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin/>.

Husam Abboud "The Realistic Lucrative Case of Ethereum Classic attack — Today" (22 May 2018) Medium <https://medium.com/@HusamABBOUD/the-realistic-lucrative-case-of-ethereum-classic-attack-with-1mm-today-8fa0430a7c25>.

Husam Abboud "H/Rindex: The Hashing Power and Robustness Index, Computational Power-weighted Benchmark for Global Blockchain and Crypto Market" (1 October 2017) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3136635>.

Nurjannah Ahmat and Sabrina Bashir "Central Bank Digital Currency: A Monetary Policy Perspective" (September 2017) Staff Insights <http://www.bnm.gov.my/index.php?ch=en_publication&pg=en_staffinsight&ac=45&bb=file>.

Enrique Aldaz-Carroll and Eduardo Aldaz-Carroll "Can cryptocurrencies and Blockchain help Fight Corruption?" (1 February 2018) Brookings <https://www.brookings.edu/blog/future-development/2018/02/01/can-cryptocurrencies-and-blockchain-help-fight-corruption/>.

Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, ManishSethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco and Jason Yellick "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" 17 April 2018, v 2) <arXiv:1801.10228, 17 April 2018 <https://arxiv.org/abs/1801.10228v1>.

ASX "How Settlement Works" <https://www.asx.com.au/services/settlement/asx-settlement/how-settlement-works.htm>.

Australian Securities and Investments Commission "Virtual Currencies" (8 September 2016) MoneySmart <https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies>.

Australian Securities and Investment Commission "AUSTRAC and CBA Agree $700m Penalty" (4 June 2018) <http://www.austrac.gov.au/media/media-releases/austrac-and-cba-agree-700m-penalty>.

Australian Taxation Office "GST and Digital Currency" <https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency/>.

Alex B "The Mining Delusion" (25 April 2017) Medium <https://medium.com/@bergealex4/the-mining-delusion-96e021b6f899>.

Adam Back "Hash Cash Postage Implementation" (28 March 1997) <http://www.hashcash.org/papers/announce.txt>.

Arthur Baxter "Blockchain – unchaining the world from fraud?" (14 April 2016) The Paypers <http://www.thepaypers.com/expert-opinion/blockchain-unchaining-the-world-from-fraud-/763845>.

Michael Bordo and Andrew Levin "Central Bank Digital Currency and the Future of Monetary Policy" (23 September 2017) Vox <https://voxeu.org/article/benefits-central-bank-digital-currency>.

Vitalik Buterin and Virgil Griffith "Casper the Friendly Finality Gadget" (15 November 2017) <https://arxiv.org/abs/1710.09437>.

Vitalik Buterin "Chain Interoperability" (9 September 2016) <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>.

Vitalik Buterin “Toward a 12-second Block Time” (11 July 2014) Ethereum Blog <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/>.

California Department of Business Oversight “DBO Commissioner Owen Clarifies Coinbase Exchange’s Regulatory Status in California” (Press release, 27 January 2015) <http://www.dbo.ca.gov/Press/press_releases/2015/Statement_on_Coinbase_Exchange_Regulatory_Status_01-27-15.pdf>.

California Department of Business Oversight “What You Should Know About Virtual Currencies” (April 2014) <http://www.dbo.ca.gov/Consumers/Advisories/Virtual_Currencies_0414.pdf>.

Canada Revenue Agency “What you should Know about Digital Currency” (3 December 2014) <http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html>.

Christian Catalini “How Blockchain Technology Will Impact the Digital Economy” (24 April 2017) <https://www.law.ox.ac.uk/business-law-blog/blog/2017/04/how-blockchain-technology-will-impact-digital-economy>.

Chartered Professional Accountants of Canada and the American Institute of CPAs “Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession” (2017) <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf>.

CoinGecko <https://www.coingecko.com/en?hashing_algorithm=SHA-256>.

CoinGecko <https://www.coingecko.com/en?hashing_algorithm=Scrypt>.

Robert V Cornish Jr “Wyoming Enacts Trailblazing Blockchain and Cryptocurrency Legislation” (12 March 2018) Wilson Elser <https://www.wilsonelser.com/news_and_insights/insights/3090-wyoming_enacts_trailblazing_blockchain_and>.

Deloitte “Bitcoin 101: Back to Basics” <https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/bitcoin-101-back-to-basics.htm>.

Delphi “The Oracle Problem” (15 July 2017) Medium <https://medium.com/@DelphiSystems/the-oracle-problem-856ccbdbd14f>.

Andrew Dentice “More Certainty for NZ Blockchain Industry as Regulator Continues Proactive Approach” (19 April 2017) Hudson Gavin Martin <http://whatshappeningnow.hgmlegal.com/post/102eudg/more-certainty-for-nz-blockchain-industry-as-regulator-continues-proactive-approa>.

Department of the Treasury Financial Crimes Enforcement Network “Money Laundering Prevention: A Money Services Business Guide” <https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf>.

Yifei Fan “Considerations concerning the Central Bank’s Digital Currency” (2018) <http://www.yicai.com/news/5395409.html> (translated by Chaowei Fan).

Financial Transactions and Reports Analysis Centre of Canada “FINTRAC Advisory regarding Money Services Businesses dealing in virtual currency” (30 July 2014) <http://www.fintrac-canafe.gc.ca/new-neuf/avs/2014-07-30-eng.asp>.

Financial Markets Authority “David Ross Sentenced for New Zealand’s Largest Ever Ponzi” (15 November 2013) <https://fma.govt.nz/news-and-resources/media-releases/david-ross-sentenced-for-new-zealands-largest-ever-ponzi/>.

Financial Markets Authority “Annual Corporate Plan 2018/19” <https://fma.govt.nz/assets/FMAs-role/180808-FMA-Annual-Corporate-Plan-2018-19.pdf>.

Financial Action Task Force “Guidance for a Risk-Based Approach: Virtual Currencies” (June 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

Financial Action Task Force “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation” (February 2012) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>.

Financial Transactions and Reports Analysis Centre of Canada “Money services businesses (MSBs)” (29 February 2016) <http://www.fintrac-canafe.gc.ca/msb-esm/intro-eng.asp>.

Financial Transactions and Reports Analysis Centre of Canada “Your Money Services Business in Canada: What you Need to Know” (29 February 2016) <http://www.fintrac-canafe.gc.ca/publications/brochure/2012-06/1-eng.asp>.

Hal Finney “RPOW - Reusable Proofs of Work” (15 August 2004) <http://marc.info/?l=cypherpunks&m=109259877510186&w=2>.

Timothy Fitzsimmons “Bitcoin: More Guidance from the CRA” (22 January 2014) Dentons <http://www.canadiantaxlitigation.com/bitcoins-more-guidance-from-the-cra>.

Global Financial Integrity “Money Laundering” <http://www.gfintegrity.org/issue/money-laundering/>.

Andrew Goldstone and Helen Cox “Do you need to Declare your Cryptocurrency to HMRC?” (12 January 2018) Mishcon de Reya <https://www.mishcon.com/news/briefings/do-you-need-to-declare-your-cryptocurrency-to-hmrc>.

Koji Higashi “I was so Wrong about the Cryptocurrency Regulation in Japan” (27 November 2017) Medium <https://medium.com/@coin_and_peace/i-was-so-wrong-about-the-cryptocurrency-regulation-in-japan-66ab17671095>

Henry Hirsh “GDPR: The Blockchain Iceberg” (12 June 2018) Singlesource <https://www.mysinglesource.io/blog/gdpr-the-blockchain-iceberg>.

IBM “IBM Announces Major Blockchain Solution to Speed Global Payments” (Press release, 16 October 2017) <http://www-03.ibm.com/press/us/en/pressrelease/53290.wss>.

IBM “IBM Blockchain World Wire” (2018) <https://www.ibm.com/blockchain/solutions/world-wire>.

IDG Connect “Blockchain: What are the implementation challenges?” (22 March 2018) <https://www.idgconnect.com/blog-abstract/29865/blockchain-what-implementation-challenges>.

Internal Revenue Service “General Rules for Property Transactions Apply” (25 March 2014) <https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance>.

Internal Revenue Service “IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply” (25 March 2014) <https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance>.

Masahiko Ishida, Edward Mears and Ryutaro Takeda “Japan Regulatory Update on Virtual Currency Business” (29 December 2017) DLA Piper <https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/>.

Hari Janakiraman, Rodolf Salem and Chris T’en “Why Bank Guarantees need Blockchain” (11 July 2017) Blue Notes, ANZ <https://bluenotes.anz.com/posts/2017/07/why-bank-guarantees-need-blockchain>.

Duncan Jones “How to Secure ‘Permissioned Blockchains’” (28 February 2018) Dark Reading <https://www.darkreading.com/endpoint/how-to-secure-permissioned-blockchains-/a/d-id/1331129>.

Kiwibank “Depositing foreign cheques or bank drafts” <https://www.kiwibank.co.nz/business-banking/international/receiving-money-from-overseas/depositing-foreign-cheque-or-bank-drafts/>

Kiwibank “International Payments” <https://www.westpac.co.nz/business/international-business/international-payments/>.

Kaspar Korjus “We’re Planning to Launch Estcoin — and that’s only the Start” (19 December 2017) <https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790>.

KRM Advisor “Starting a cryptocurrency company in Estonia” <https://www.estoniancompanyregistration.com/cryptocurrency-company/>.

Aaron Kumar and Christie Smith “Crypto-currencies – An Introduction to Not-so-funny Moneys” (November 2017) Reserve Bank of New Zealand Analytical Notes <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Analytical%20notes/2017/an2017-07.pdf>.

Antony Lewis “A Gentle Introduction to Ethereum” (2 October 2016) Bits on Blocks <https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/>.

Laura Littlewood, Toby Sharpe and Kerry Beaumont “How Open is New Zealand to Open Banking?” (20 February 2018) Bell Gully <https://www.bellgully.com/publications/how-open-is-new-zealand-to-open-banking>.

Jin Liu “The Exploration of the Legal Digital Currency in China” (2017) <www.pbcsf.tsinghua.edu.cn/Upload/file/20171026/20171026143301_6961.pdf> translated by Chaowei Fan.

Caitlin Long “Wyoming’s Blockchain Bills: A Very Personal Labor of Love” (9 March 2018) <https://caitlin-long.com/2018/03/09/wyomings-blockchain-bills-a-very-personal-labor-of-love/>.

Frances Mazzanti “Bitcoins and other digital currencies – emerging tax treatment” (21 August 2014) Johnston Associates South <https://jacalsouthisland.nz/bitcoins-and-other-digital-currencies-emerging-tax-treatment/>.

Timothy McCallum “First impressions of Ethereum’s Casper — Proof of Stake (PoS)” (5 January 2018) Medium <https://medium.com/cybermiles/first-impressions-of-ethereums-casper-proof-of-stake-pos-5ce752e4edd9>.

Thomas Mueller “Public or Permissioned Chains – What’s the Best Option for Enterprises” (25 May 2017 Medium <https://medium.com/contractus/public-or-permissioned-chains-whats-the-best-option-for-enterprises-5dcf38a6d263>.

Hon Stuart Nash and Hon Meka Whaitiri “GST Loophold Closed to Offshore Companies” (Press release, 1 May 2018) <http://taxpolicy.ird.govt.nz/news/2018-05-01-gst-imported-low-value-goods-proposals-launched>.

Taylor Nelms “‘Ecuador Bans Bitcoin’! A Monetary Mix Up” (20 October 2015) King’s Review <http://kingsreview.co.uk/articles/ecuador-bans-bitcoin-a-monetary-mix-up/>.

New York State Department of Financial Services “BitLicense Frequently Asked Questions” <http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm>.

New Zealand Bankers’ Association “The Code of Banking Practice” <http://www.nzba.org.nz/consumer-information/code-banking-practice/code-of-banking-practice/>.

New Zealand Banking Ombudsman Scheme “Closing Accounts” <https://bankomb.org.nz/guides-and-cases/quick-guides/bank-accounts/closing-accounts/>.

New Zealand Banking Ombudsman Scheme “Mistaken Payments” <https://bankomb.org.nz/guides-and-cases/quick-guides/payment-systems/mistaken-payments/>.

New Zealand Department of Internal Affairs “Identity Theft – What Is Identity Theft? <https://www.dia.govt.nz/Identity---What-is-identity-theft>.

New Zealand Transport Agency “Your responsibilities as the Registered Person” <https://www.nzta.govt.nz/vehicles/how-the-motor-vehicle-register-affects-you/your-responsibilities-as-the-registered-person/>.

Timothy Nugent, David Upton and Mihai Cimpoesu “Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts” (20 October 2016) Version 1 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5357027/>.

Luke Parker “New Hampshire Money Transmitter Rule Change will Include Bitcoin Businesses” (8 December 2015) Brave New Coin <http://bravenewcoin.com/news/new-hampshire-money-transmitter-rule-change-will-include-bitcoin-businesses/>.

Luke Parker “Sony Launches Blockchain-based Educational Infrastructure Project” (23 February 2016) Brave New Coin <http://bravenewcoin.com/news/sony-launches-Blockchain-based-educational-infrastructure-project/?utm_source=BNC+Newsletter&utm_campaign=89eb421dd5-BNC_Weekly_News_Highlights_26_Feb_2016&utm_medium=email&utm_term=0_83439a8472-89eb421dd5-245125889>.

David Paterson “Ten More Financial Institutions Join Ripple’s Global Payments Network” (26 April 2017) Ripple <https://ripple.com/ripple_press/ten-financial-institutions-join-ripples-global-payments-network/>.

Christopher Payne “IRS: Bitcoin Not a Currency for Tax Purposes” (4 April 2014) Dentons <http://www.canadiantaxlitigation.com/irs-bitcoin-not-a-currency-for-tax-purposes>.

Politsei-ja Piirivalveamet “The Supreme Court Finds that Bitcoin Trading is an Economic Activity” (14 April 2016) <https://www.politsei.ee/en/uudised/uudis.dot?id=558348&order=date2+desc&currentPage=1&searchquery=bitcoin>.

Steven Porter “Decentralize Clearinghouses: Regulators Take Notice” (26 February 2016) Medill Reports Chicago <http://news.medill.northwestern.edu/chicago/Blockchain-could-decentralize-clearinghouses-regulators-take-notice/>.

Press Information Bureau, Government of India “Text of Prime Minister’s address to the Nation” (Press release, 8 November 2016) <http://pib.nic.in/newsite/erelease.aspx?relid=153404>.

Shaan Ray “Blockchain Interoperability” (16 June 2018) Medium <https://towardsdatascience.com/blockchain-interoperability-33a1a55fe718>.

Reserve Bank of New Zealand "Statement about Banks Closing Accounts of Money Remitters" (28 January 2015) <http://www.rbnz.govt.nz/news/2015/01/statement-about-banks-closing-accounts-of-money-remitters>.

Ripple "Overview" <https://ripple.com/company/>.

Katie Robinson "Tax Issues Relating to Bitcoins" (23 December 2013) <http://www.canadiantaxlitigation.com/wp-content/uploads/2014/01/2013-0514701I7.txt>.

Peter Roudik "Estonia: Rules on Taxation of Bitcoin" (18 April 2014) Library of Congress <http://www.loc.gov/law/foreign-news/article/estonia-rules-on-taxation-of-bitcoin/>.

Danny Ryan "Costs of a Real World Ethereum Contract" (11 August 2017) Hackernoon <https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214>.

Priyab Satoshi "Steem (STEEM) — Blockchain-based Social Media Platform" (20 August 2017) Medium <https://medium.com/crypt-bytes-tech/steem-steem-blockchain-based-social-media-platform-889f7f3c3245>.

Simon Scorer "Beyond Blockchain: What are the Technology Requirements for a Central Bank Digital Currency?" (13 September 2017) Bank Underground <https://bankunderground.co.uk/2017/09/13/beyond-blockchain-what-are-the-technology-requirements-for-a-central-bank-digital-currency/>.

Oussema Settala "Bitdinar: The Mobile Wallet" (12 May 2017) Medium <https://medium.com/vink-io/bitdinar-the-mobile-wallet-9e6e867cbdb>.

Srinivasa Siriyanna "Blockchain Smart Contracts in Insurance" (4 January 2017) Infosys <http://www.infosysblogs.com/blockchain/2017/01/blockchain_smart_contracts_in_.html>.

Ben Smith "The Sanctions and Anti-Money Laundering Bill 2017-19" (15 February 2018) House of Commons Library, Briefing Paper <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8232>.

Stanford Swinton and Eduardo Roma "Coping with the Challenge of Open Banking" (7 February 2018) Bain Brief <http://www.bain.com/publications/articles/coping-with-the-challenge-of-open-banking.aspx>.

SWIFT "Emergency and high priority customer requests" (2017) Society for Worldwide Interbank Financial Telecommunication <https://www.swift.com/myswift/ordering/order-products-services/emergency#Emergencyhandling>.

SWIFT "SWIFT history" (2017) Society for Worldwide Interbank Financial Telecommunication <https://www.swift.com/about-us/history>.

SWIFT "SWIFT tests show blockchain has potential for global liquidity optimisation" (13 October 2017) <https://www.swift.com/news-events/press-releases/swift-tests-show-blockchain-has-potential-for-global-liquidity-optimisation>.

Nick Szabo "Bit Gold" (27 December 2008) Unenumerated <http://unenumerated.blogspot.co.nz/2005/12/bit-gold.html>.

Nick Szabo "The Idea of Smart Contracts" (1997) Nick Szabo's Papers and Concise Tutorials <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html>.

Nick Szabo "Trusted Third Parties Are Security Holes" (2001) Nick Szabo's Papers and Concise Tutorials <https://web.archive.org/web/20160309161628/http://szabo.best.vwh.net/ttps.html>.

Te Ara, the Encyclopedia of New Zealand "Coins and Banknotes – Varied Coins and Banknotes, 1840s to 1930s" <https://teara.govt.nz/en/coins-and-banknotes/page-1>.

Tencent, RDCY and Ipsos "2017 Mobile Payment Usage in China Report" (2017) <https://www.ipsos.com/sites/default/files/ct/publication/documents/2017-08/Mobile_payments_in_China-2017.pdf>.

Texas State Securities Board, "$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales" (4 January 2018) <https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales>.

The People's Bank of China (2018) <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3509038/index.html> (translated by Chaowei Fan).

Marcus Treacher "Announcing Ripple's Global Payments Steering Group" (23 September 2016) Ripple <https://ripple.com/insights/announcing-ripples-global-payments-steering-group/>.

Adam Turner "3 Ways to Accept Credit Card Payments" (29 May 2015) MYOB <https://www.myob.com/nz/blog/3-alternatives-to-eftpos-terminal/>.

Westpac New Zealand "How Long does it take you to Process Payments?" <http://westpac.custhelp.com/app/answers/detail/a_id/871/~/how-long-does-it-take-you-to-process-payments%3F>.

Westpac New Zealand "International payments" <https://www.westpac.co.nz/business/international-business/international-payments/>.

Aaron Wright and Primavera De Filippi "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (20 March 2015) SSRN <https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2580664>.

Qian Yao "Technical Considerations of the Central Bank's Digital Currency" (2018) <http://www.yicai.com/news/5404436.html> (translated by Chaowei Fan).

Interviews / Podcasts

Arthur Falls "BHP, Tracking the Most Valuable Rock on Earth" (Podcast, 18 October 2016) The Ether Review <https://etherreview.info/tagged/podcast>.

Jacob Goldstein and David Kestenbaum "The Island of Stone Money" (Podcast, 10 December 2010) Planet Money <http://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money>.

Steve Henn "Remembering When Driverless Elevators Drew Skepticism" (Podcast, 31 July 2015) Planet Money <https://www.npr.org/2015/07/31/427990392/remembering-when-driverless-elevators-drew-skepticism>.

Interview with investigative journalist Nicky Hager (Alex Perrottet, Morning Report, RNZ: National, 19 April 2018, "The Daphne Project: Is NZ still a tax haven?") <https://www.radionz.co.nz/national/programmes/morningreport/audio/2018641323/daphne-project-is-nz-still-a-tax-haven>.

Interview with Kris Faafoi, Minister of Commerce and Consumer Affairs (Susie Ferguson, Morning Report, RNZ: National, 20 April 2018, "Govt not Surprised at Daphne Project Revelations – Faafoi") <https://www.radionz.co.nz/national/programmes/morningreport/audio/2018641495/govt-not-surprised-at-daphne-project-revelations-faafoi>.

Speeches

Geoff Bascand, Deputy Governor of the Reserve Bank of New Zealand "In Search of Gold: Exploring Central Bank Digital Currency" (speech at Payments NZ Conference, Auckland, New Zealand, June 2018).

Geoff Bascand, Deputy Governor of the Reserve Bank of New Zealand "The Evolution of New Zealand's Currency" (speech to Royal Numismatic Society, Wellington, New Zealand, July 2014) <http://rbnz.govt.nz/research-and-publications/speeches/2014/speech2014-07-05>.

Mark Carney, Governor of the Bank of England "The Future of Money" (speech to the Inaugural Scottish Economics Conference, Edinburgh University, Scotland, March 2018) <https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418>.

J Christopher Giancarlo, Acting Chairman of US Commodities Futures Commission "LabCFTC: Engaging Innovators in Digital Financial Markets" (New York FinTech Innovation Lab, New York, United States, 17 May 2017) <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-23>.

Willam Hinman, Director of Division of Corporation Finance, United States Securities and Exchange Commission "Digital Asset Transactions: When Howey Met Gary (Plastic)" (Yahoo Finance All Market Summit, San Francisco, 19 June 2018) <https://www.sec.gov/news/speech/speech-hinman-061418#_ftn3>.

Philip Lowe, Governor of the Reserve Bank of Australia "An eAUD?" (2017 Australian Payment Summit, Sydney, Australia, 13 December 2017) <https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html>.

Sigal Mandelker "U.S. Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference" (speech to the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference, New York, February 2018) <https://home.treasury.gov/news/press-release/sm0286>.

Greg Medcraft "The future of Capital Markets in a Digital Economy" (Distinguished speaker series, Carnegie Mellon University, Adelaide, Australia, Australian Securities and Investments Commission, September 2015) <http://download.asic.gov.au/media/3356655/keynote-address-future-of-capital-markets-20151709-final.pdf>.

Tony Richards, Head of Payments Policy Department, Reserve Bank of Australia "The Ongoing Evolution of the Australian Payments System" (Speech to Payments Innovation 2016 Conference, Sydney, 23 February 2016)

<http://www.rba.gov.au/speeches/2016/sp-so-2016-02-23.html> and <http://webcasting.boardroom.media/broadcast/56cba0fb19eabcfb07389309>.

Tony Richards "The Ongoing Evolution of the Australian Payments System" (speech to Payments Innovation 2016 Conference, Sydney, February 2016) <http://www.rba.gov.au/speeches/2016/sp-so-2016-02-23.html>.

Tony Richards and David Emery, Reserve Bank of Australia "Opening Statement to the Inquiry into Taxpayer Engagement with the Tax System" (speech to House of Representatives Standing Committee on Tax and Revenue, Canberra, October 2017) <https://www.rba.gov.au/speeches/2017/sp-so-2017-10-27.html>.

Other resources

<https://aion.network/>.

<https://aragon.one/>.

<https://ark.io/>.

<https://atlant.io/>.

<https://azure.microsoft.com/en-us/solutions/blockchain/>.

<https://bitcoinfees.info/>.

<https://www.blockcollider.org/>.

<https://www.civic.com>.

<https://coincap.io.>.

<https://www.coindesk.com/price/>.

<https://www.corda.net/>.

<https://cosmos.network/>.

<https://eftpos.co.nz/mobile-faqs>.

<https://eos.io/>.

<https://entethalliance.org/>.

<http://freico.in/about/>.

<https://www.hyperledger.org/projects/fabric>.

<https://www.jpmorgan.com/global/Quorum>.

<https://jury.online/>.

<https://kleros.io/>.

<https://lisk.io/>.

<https://www.livingroomofsatoshi.com/graphs>.

<https://qtum.org/en/>.

<https://nem.io/>.

<https://neo.org/>.

<https://www.mysinglesource.io/>.

<https://nxtplatform.org/>.

<https://passwordsgenerator.net/sha256-hash-generator/>.

<http://petrodollars.io/>.

<https://polkadot.io>.

<https://proof.work>.

<http://redbellyblockchain.io/>.

<https://www.rsk.co/>

<http://www.sendmoneypacific.org>.

https://skills.org.nz/careers-and-courses/business/financial-services/authorised-financial-advisers/>.

<https://www.sov.global/>.

<https://sovrin.org/>.

<https://sphereidentity.com/>

<https://steem.io/>.
<https://tether.to/>.
<https://www.tezos.com/>.
<https://www.uport.me/>.
<http://www.weidai.com/bmoney.txt>.