WHO SHOULD REGULATE BITCOIN?

Challenges and opportunities for blockchain technology in Australia.

Executive Summary

- Bitcoin is a cryptographically-secured internet-based digital currency, or cryptocurrency, that is a leading application of blockchains, or Distributed Ledger Technology (DLT).

- Bitcoin, along with DLT, was invented in 2008, and has since emerged as not only a new form of digital money but as a new, albeit still experimental, payments technology.

- There is growing concern in Australia and around the world over the regulatory implications and challenges surrounding the development and use of this promising new technology.

- Drawing on economic theories of technological change and economic theories of regulation, this report argues that while specialist regulatory agencies should certainly be paying attention to this developing new technology, and actively engaged in learning opportunities wherever possible (such as monitoring industry self-regulation and regulatory sandboxes) it would be premature at this early stage for specialist agencies to regulate the new technology.

- The Reserve Bank of Australia does not have, nor should it have, the technical capabilities in code development or platform design. Indeed the Payments System Board was never well-placed within the Reserve Bank of Australia because of the very different specialisations.

- Instead, specialist regulators should focus attention on particular products or services as they emerge.

- Cryptocurrencies and distributed ledger technologies are a still developing general purpose technology platform with considerable entrepreneurial uncertainty about its use cases, business models, and new capabilities native to the technology, such as smart contracts and distributed autonomous organizations.

- There is a risk that efforts to control the technology as it exists now will impede future blockchain technology innovation and the growth of nascent industries.

- These exciting developments in cryptocurrency as a new technology for payments, and DLT as a general purpose technology, provides another reason why the *Payment Systems (Regulation) Act 1998* should be repealed, and Payment Systems regulation moved to a specialist regulator.

Contents

About the authors

Professor Jason Potts is Professor of Economics in the School of Economics, Finance and Marketing at RMIT University, an Australian Research Council Future Fellow, and also an Adjunct Fellow at the Institute of Public Affairs. He has written five books and over 70 articles on the theory of economic evolution. His work focuses on how entrepreneurship and innovation drive economic growth and development. Jason has published in academic journals such as *Journal of Economic Behavior and Organisation*, *Journal of Institutional Economics*, and *Economic Affairs*.

Dr Trent MacDonald is research fellow in the School of Economics, Finance and Marketing at RMIT University and coordinator of *Melbourne Crypto*, a multidisciplinary, multi-institute research network for 'blockchain studies'. He has worked in the areas of creative city policy, cultural economics, digital inclusion, and the economics of entrepreneurship and innovation. In 2015 Trent won the Don Lavoie Memorial Award from the *Society for the Development of Austrian Economics*.

1. The technology

Bitcoin is an innovative peer-to-peer payment network and a new kind of money—often referred to as a digital currency or cryptocurrency—that offers fast peer-to-peer transactions, global payments, and low processing fees.[1] It uses cryptography to control the creation and transfer of money, and was intended as an electronic payment system that allows two parties to transact directly with each other over the internet without requiring a trusted third-party intermediary.[2]

Bitcoin was invented in 2008 by the pseudonymous Satoshi Nakamoto with the publication of the paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' and was introduced in 2009 as open source software. The project remained largely within the province of a small community of computer scientists and tech-minded activists before reaching mainstream attention following a dramatic price spike (and concomitant uptake in adoption) in late 2013. Today there are hundreds of similar digital currencies, with an aggregate market capitalisation of over $13 billion USD; of which $11 billion USD is dedicated to Bitcoin, exceeding the next largest capitalisation of Ethereum ($860 million USD) by about 13 times.[3]

As the first digital currency,[4] Bitcoin enjoys beneficial network effects that have contributed to its dominance over other digital currencies.[5] For the same reasons, Bitcoin itself has not yet achieved widespread acceptance compared to incumbent fiat currencies.[6] There has, however, been growing venture capital investment in Bitcoin companies, totalling almost $1.4 billion USD from 2012 to 2016.[7] It remains to be seen whether the ongoing entrepreneurial process will be capable of setting in motion a spontaneous monetary switch—or for that matter, whether the range of non-financial applications of the technology will succeed in their respective domains—or whether instead incumbent institutions will maintain their own dominance.[8] Nonetheless, governments and regulators worldwide are carefully considering the implications and challenges presented by the emergence of digital currencies, and Australia is no exception.

[1] https://bitcoin.org/en/.

[2] Satoshi Nakamoto, 'Bitcoin: A peer-to peer electronic cash system', https://bitcoin.org/bitcoin.pdf (accessed 1 November 2015).

[3] Market capitalization comparisons made as at 1 November 2016. See "Crypto-Currency Market Capitalizations", accessed 1 November 2016, https://coinmarketcap.com/.

[4] Robleh A., Barrdear, Clews, R. and Southgate, J. (2014). The economics of digital currencies. *Quarterly Bulletin*, Bank of England, 54(3), 277- http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf (accessed 1 November 2015).

[5] White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, *35*, 383-402.

[6] Luther, W. J. (2015). Cryptocurrencies, network effects, and switching costs. *Contemporary Economic Policy*, 34(3), 553-571.

[7] Total reported venture capital in Bitcoin companies was $2 million in 2012, $95 million in 2013, $350 million in 2014, and $550 million in 2015, and $375 million as of September 2016, summing to a little under $1.4 billion in overall investment. See "Bitcoin Venture Capital Investments," *CoinDesk*, accessed 1 November 2016, http://www.coindesk.com/bitcoin-venture-capital/.

[8] Nair, M. and Cachanosky, N. (2016). Entrepreneurship and Bitcoin: Breaking the network Effect. *Review of Austrian Economics*, Forthcoming. Available online: http://link.springer.com/article/10.1007/s11138-016-0348-x.

Digital currencies and Bitcoin

The distinction between digital currencies, such as Bitcoin, and fiat currencies, such as the Australian dollar:

> Digital currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the digital currency.
>
> Digital currency is distinguished from fiat currency, which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country.
>
> It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.[9]

More specifically, Bitcoin is the world's first completely decentralised, convertible digital currency:

> Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.
>
> Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet.
>
> Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 but the open-source nature of Bitcoin mean that its protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software.[10]

[9] FATF, *Virtual Currencies—Key Definitions and Potential AML/CFT Risks*, 2014, p. 4. http://www.fatfgafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-amlcft-risk.html; see also Attorney General's Department, *Submission 42*, p. 5.

[10] https://bitcoin.org/en/faq#what-is-bitcoin.

Bitcoin currency units can be obtained in exchange for products, services, or other currencies, or in a process called 'mining', in which network participants that provide computing power to verify and record payments into the public ledger are rewarded with transaction fees and newly-minted bitcoins:

> Users send and receive bitcoins using wallet software on a personal computer, mobile device, or a web application. When a Bitcoin user makes a purchase, the payment triggers a broadcast of the financial transaction to the Bitcoin network. The Bitcoin transaction is a digitally signed message transferring the ownership of bitcoins from one "Bitcoin address" to another. For the transaction to take effect it must be recorded in a public ledger or public transaction database called the blockchain. Approximately every ten minutes a bundle of transactions, called a "block", is added to the blockchain. The incentive for this accounting process, known as "mining", carries a reward of 25 bitcoins per block added to the block chain. This 25 bitcoins reward maintains the integrity of the Bitcoin system by allowing the computers that confirm transactions to also mint new bitcoins in the process. Bitcoin payment processing fees are optional, and generally substantially lower than those of credit cards or money transfers.[11]

Blockchains and distributed ledgers

The Bitcoin *blockchain*—the public ledger of transactions, in chronological order, and shared between all users—is a novel solution to the double-spend problem previously plaguing digital currency and e-money. Before Bitcoin, a centralised third party had to issue and reconcile digital cash transactions to prevent electronic cash from being spent multiple times (i.e., because digital assets can be copied). The blockchain is what enables the digital currency to be used in a decentralised payment system, and can therefore be seen as the main technical innovation behind Bitcoin.

Confusion often surrounds the term 'blockchain technology' as it can be used in different ways: to refer to the Bitcoin blockchain, or that of another digital currency, or some other non-financial application such as a platform for smart contracts. A blockchain is a "mathematically-secured, chronological, and decentralised consensus ledger, or database, whether maintained by internet interaction, peer-to-peer network, or otherwise."[12] Most generally, a blockchain is a *distributed ledger*, that is, a list of transactions that is shared among a number of computers, rather than being stored on a central server.[13]

> A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within the network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or seconds.[14]

[11] https://bitcoin.org/en/how-it-works.

[12] Vermont (US, Legislative Code) Rule of Evidence 902 §1913 (2016).

[13] Lewis, A. (2015). A Gentle Introduction To Blockchain Technology, *Brave New Coin*. Available online: http://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf.

[14] Walport, M. (2016). Distributed Ledger Technology: Beyond Blockchain. *UK Government Office for Science, Tech. Rep,19.*

More specifically, a blockchain is a particular type of distributed ledger (i.e., a cryptographically-secured one), while distributed ledger is a particular type of database (i.e., one maintained on a distributed network of computers). It may therefore seem trivial to point out that distributed ledgers and blockchains stand to compete with, and potential replace, ledgers. But the implication of this is much greater and follows from the fact that modern economies and societies are, ultimately, built upon ledgers:

> A ledger is a way of producing consensus about the facts that are necessary for commerce to function. Ledgers are the basic transactional recording technology at the heart of all modern economies. Moreover, the institutional and organisational outline of a modern economy is to a significant degree a consequence of those ledgers needing to be centralised (i.e., in government, in layers of bureaucracy, in large corporations, and so on). This is why blockchain technology—while still new and experimental—is appropriately described as both a general-purpose technology and a disruptive technology.[15]

Smart contracts and distributed autonomous organisations

A smart contract is a computer protocol that facilitates, verifies, or enforces the performance of a contract. In this way, conventional contractual clauses may be made partially or fully self-executing or self-enforcing (or both). Pioneer of the concept, Nick Szabo, explained how smart contracts might improve traditional contract law:

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions, minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.[16]

The second largest digital currency by market capitalisation, Ether, is a cryptographic token used to execute smart contracts on the decentralised applications platform Ethereum.[17] Smart contract applications run on a customised Ethereum blockchain "exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[18] One such class of decentralised applications are known as Distributed Autonomous Organisations (DAOs), which are self-executing organisations that are governed by smart contract-encoded rules, and maintained on a blockchain.[19]

[15] Davidson, S., De Filippi, P. and Potts, J. (2016). Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. Available online: https://ssrn.com/abstract=2811995. On general-purpose technologies see Bresnahan and Trajtenberg (1995), Lipsey et al. (2005). On disruptive technology see Christianson (1997). See also Buterin (2015), Wiles (2015), Tapscott (2016).

[16] Szabo, N. (1994). The idea of smart contracts. Available online: http://szabo.best.vwh.net/smart_contracts_idea.html.

[17] Ether market capitalisation of approximately $860 million USD as at 1 November 2016. See "Crypto-Currency Market Capitalizations", accessed 1 November 2016, https://coinmarketcap.com/. Ethereum was originally crowdfunded via an ether pre-sale in August 2014, raising approximately $18 million USD.

[18] https://www.ethereum.org/. Ethereum was initially described in a white paper by co-founder Vitalik Buterin: https://github.com/ethereum/wiki/wiki/White-Paper.

[19] Buterin (2014a), Wood (2014a).

Thus the vision of Ethereum, while not yet fully realised, can be seen to culminate the above-mentioned shift in foundation of modern economies, from centralised (traditional) ledgers to distributed (blockchain) ledgers, and from centralised institutions to distributed institutions. Which is to say smart contracts and distributed autonomous organisations have the potential to distinguish blockchain as a disruptive, general-purpose *institutional* technology. Indeed, this is implied in Ethereum co-founder Vitalik Buterin's definition and vision of the value of blockchain:

> A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publically visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.
>
> Blockchains are not about bringing to the world any one particular ruleset, they're about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They're Lego Mindstorms for building economic and social institutions.[20]

The emergence of a new general-purpose technology

General-purpose technologies (GPTs) are technologies that pervade entire economies and which have the potential to drastically disrupt incumbent institutions and economic structures. A GPT can be defined as such according to four criteria: (1) it is a single, recognisable generic technology; that (2) initially has much scope for improvement but comes to be widely used across the economy; (3) has many different uses; and (4) creates many spillover effects.[21]

While GPTs can only properly be identified retrospectively, distributed ledger blockchain technology is increasingly understood as a potential new general-purpose technology for a broad range of economic activities that rely on consensus of a database of transactions or records. To call blockchains a new general-purpose technology puts them in the same class of technological trajectories as electricity, transistors, computers, and the Internet. Just as smart phones and mobile media are the 'next generation' from personal computers, blockchains have been represented as the next generation of the Internet.[22] So perhaps the technological impact of blockchains will be similarly large, disruptive and widespread: eventually comparable to computers or the Internet.

> We should think about the blockchain as another class of thing like the Internet—a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money;

[20] Buterin, V. (2015) 'Visions Part I: The value of blockchain technology'. https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/.

[21] Lipsey, R. G., Carlaw, K. I., & Bekar, C. T. (2005). *Economic transformations: General purpose technologies and long-term economic growth*. OUP Oxford.

[22] Tapscott, D. and Tapscott, A., 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.

hard assets (physical property, homes, cars); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.).[23]

Blockchains are the technology that underpins digital currencies, but there is a much greater range of applications to any situation involving public records requiring consensus, that are still in nascent stages of exploration and discovery. That is, while the underlying *technical* invention of blockchain has been available since 2009, many applicable *entrepreneurial* opportunities remain unknown and undeveloped.[24] This entrepreneurial process—of discovering the entire constellation of potential opportunities for a technology—is what drives phases of economic growth and productivity.[25]

For blockchain to transform into a GPT it must not only come to be pervasive, but also generate sustained improvements in performance and productivity, and have complementarities with other technologies and sectors.[26] The evolution of blockchain technology has undergone three phases of development:

(1) currency—typified by Bitcoin, digital currencies, and related applications (e.g. currency transfer, remittance, digital payment systems);
(2) contracts—economic, market, and financial applications more extensive than simple cash transactions (e.g. stocks, bonds, futures, loans, mortgages, titles, smart property, smart contracts);
(3) governance—applications beyond currency, finance, and markets (e.g. government, health, science, literary, culture, art).[27]

The more bullish promoters of the technology believe that distributed ledgers could be used to encode, confirm, and transfer almost *all* forms of property:

- Financial: stock, private equity, bonds, derivatives, mutual funds, pensions, crowdfunding
- Public records: land and property titles, vehicle registries, business licences, passports, voter IDs, marriage certificates, death certificates
- Private records: contracts, bets, signatures, wills, trusts, escrows
- Attestation: proof of insurance, proof of ownership, notarised documents
- Physical asset keys: home, hotel rooms, rental cars, car keys, Internet of things
- Intangibles: patents, trademarks, copyrights, reservations, domain names[28]

[23] Swan, M., 2015. *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.".
[24] Allen, D. W. E. (2016). Discovering and developing the blockchain cryptoeconomy. Available online: https://ssrn.com/abstract=2815255.
[25] Helpman & Trajtenberg (1994).
[26] Bresnahan & Trajtenberg (1995).
[27] Swan, M., 2015. *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.".
[28] Swan, M., 2015. *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.".

A cursory examination of the emerging ecosystem of real-world applications of distributed ledgers and blockchain technology confirms that it is certainly a *potential* GPT:

- Coloured Coins: marking or 'colouring' bitcoins in order to represent digital and physical assets on top of the Bitcoin network[29]

- OmniLayer: software layer built on top of the Bitcoin blockchain for creating and trading custom digital assets and currencies[30]

- Counterparty: platform for users to construct self-executing applications and smart contracts using the Bitcoin blockchain[31]

- BitShares: decentralised crypto-equity share exchange[32]

- Ripple: real-time gross settlement system, currency exchange, and remittance network that supports tokens representing fiat currency, cryptocurrency, commodity or other units of value[33]

- Ethereum: distributed computing platform that supports decentralised applications, smart contracts, and distributed autonomous organisations[34]

- OpenBazaar: open source protocol for e-commerce transactions in a fully decentralised peer-to-peer marketplace[35]

- NameCoin: cryptocurrency that acts as an secure, censorship-resistant, decentralised Domain Name System (DNS)[36]

- Ascribe: decentralised platform for managing proof of ownership/provenance of digital content[37]

- MaidSafe: decentralised networking platform for hosting websites and that supports messaging, apps, email, social networks, data storage, video conferencing[38]

- Bitmessage: decentralised, encrypted, peer-to-peer, communications protocol[39]

- Twister: decentralised peer-to-peer microblogging platform (a censorship-proof distributed Twitter clone) based on both BitTorrent and Bitcoin-like protocols[40]

[29] http://coloredcoins.org/.

[30] http://www.omnilayer.org/.

[31] https://counterparty.io/.

[32] https://bitshares.org/.

[33] https://ripple.com/.

[34] https://www.ethereum.org/.

[35] https://openbazaar.org/.

[36] https://namecoin.org/.

[37] https://www.ascribe.io/.

[38] https://maidsafe.net/.

[39] https://bitmessage.org/.

[40] http://twister.net.co/.

- Storj: platform, cryptocurrency, and suite of decentralised applications that support decentralised cloud storage[41]
- LaZooz: decentralised transportation platform for utilising vehicles' unused space (i.e., ride-sharing)[42]
- Arcade City: Ethereum-based cryptocurrency to facilitate peer-to-peer ride-sharing transactions[43]
- Backfeed: Ethereum-based platform for distributed applications that enable collaborative creation and distribution of value[44]
- Augur: Ethereum-based decentralised prediction market, for trading virtual shares in the outcome of real-world events[45]

It is unavoidable that in the beginning of their technological trajectory general-purpose technologies face radically high uncertainty over what their future valuable applications will be.[46] It does seem reasonable, however, to diagnose blockchain as a generic technology with scope for improvement, many different use cases, and positive externalities among applications. Whether it comes to be widely used across the economy and can be regarded as a GPT will depend on benefits materialising, which also depends on the regulatory environment blockchain entrepreneurs find themselves in. Because it is always *ex ante* unclear as to the entire constellation of potential opportunities stemming from a given technological innovation (even a specific one), the early stages of transformation of general-purpose technologies are particularly conducive to the economic problems of entrepreneurial discovery; which include among them an acute sensitivity and vulnerability to overregulation. At this point in time, the productivity improvements from distributed ledgers blockchain technology are yet to be realised (or even clearly defined), drawing another parallel to previous GPTs such as Information Technology.

Potential risks and concerns for regulators

In addition to the potential benefits of Bitcoin and blockchain, there are some potential risks and concerns to consider for both users and regulators alike. These include price volatility, prudential concerns, security breaches, criminal uses such as illicit trade, money laundering, tax evasion, and terrorist financing, and even the prospect of less effective fiscal or monetary policy. From the outset it should be noted than many of these potential concerns are the same as those facing traditional cash.

After an initial largely dormant period, Bitcoin encountered its first significant price adjustment in April 2013, followed by another major spike in October 2013. There have been a number of similar price adjustments since then, generally resembling the pattern of a speculative bubble: overoptimistic media

[41] https://storj.io/.

[42] http://lazooz.net/.

[43] https://arcade.city/.

[44] http://backfeed.cc/.

[45] https://www.augur.net/.

[46] Bresnahan & Trajtenberg (1995); Helpman (1998); Lipsey et al. (2005).

coverage, entry of novice investors, exuberant price increases leading to overvaluation, and a subsequent downward price adjustment or 'crash'.

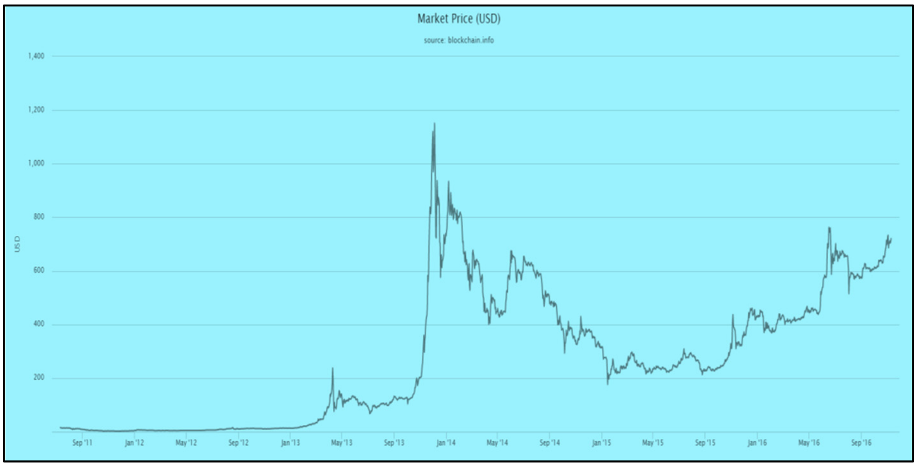

FIG x. Bitcoin market price (USD), Sep 2011 – Sep 2016

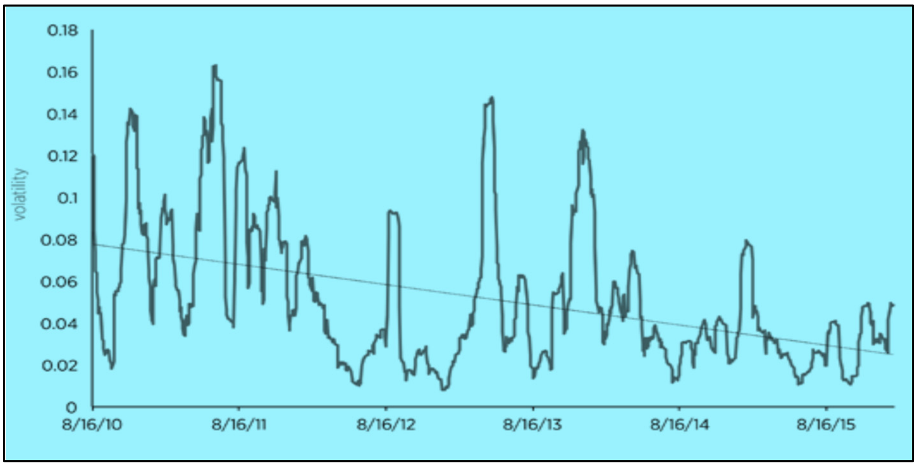

FIG x. Bitcoin price volatility (S.D. of 30-day returns USD), Aug 2010 – Aug 2015

This apparent price volatility[47] has engendered scepticism over the long-term viability of the digital currency, as it undermines its use as a store of value and unit of account. Yet, price volatility is less of a problem for its other primary use as a medium of exchange.[48] Indeed, entrepreneurial solutions, such as *CoinJar*[49], have already been developed to allow merchants and consumers to convert seamlessly between currencies, and thereby support Bitcoin's medium-of-exchange function. This is a likely explanation for why price volatility has not dampened the uptake and acceptance of Bitcoin among merchants. Moreover, price fluctuations have actually *decreased* over time, suggesting that the initial bouts of volatility served to stress test the digital currency, as users have developed more realistic expectations of its function and

[47] In fact, volatility, measured as the standard deviation of daily returns for the preceding 30-day window, appears to be *decreasing* over time. See FIG. x. Dotted line represents linear trend line. Source: Jerry Brito and Andrea Castillo, Bitcoin: A Primer for Policymakers, p. 33.

[48] Jerry Brito, "Why Bitcoin's Valuation Doesn't Really Matter," *Technology Liberation Front*, April 5, 2013, http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/.

[49] www.coinjar.com.au.

value, and as entrepreneurs have developed solutions to counteract volatility, such as derivatives and swaps markets.[50]

The threat of security breaches is another concern. While the Bitcoin *protocol* is virtually unhackable, and has to this date proven secure, the same cannot be said of bitcoin *currency units*. Bitcoin wallet software that is used to secure currency units can be hacked if a wallet holder or the provider financial institution engages in poor security management practices—just like traditional bank accounts. That is, if people do no protect their private keys their digital currency can be stolen, or if people misplace or delete them, so too have they lost their digital money—just like with traditional money. Moreover, if the cryptographic tools that underwrite the security of Bitcoin are found to be vulnerable to hacking attempts, then many more industries and technologies beside Bitcoin will likewise be vulnerable—including traditional financial institutions.

While the Bitcoin protocol itself is secure, inevitably some third party intermediaries that hold or convert the digital currency, such as wallet providers and currency exchanges, are not. Examples range from the negligent to the outright fraudulent. In December 2014 the widely trusted *Blockchain.info* service was exposed of security vulnerabilities by a 'white hat' hacker (a Good Samaritan that later returned the stolen funds) and promptly strengthened its security measures. In November 2013 the first and largest bitcoin exchange Mt. Gox, then managing around 70 percent of Bitcoin transactions, began delaying customer withdrawal requests and in February 2014 filed for bankruptcy, citing an 850,000 BTC ($473 million USD) hack.[51] As of 2016 over 24,000 Mt. Gox customers have made claims for reimbursement, with a mere $90 million USD of the digital currency in holding.[52] In other cases, exchanges have responded to incidents responsibly and reimbursed the full value of customers' hacked accounts.

Bitcoin services today take proactive measures to demonstrate the integrity of their business, and alleviate security or prudential concerns of prospective customers: for example, Coinbase[53] prominently publicises its account security insurance policies, while Kraken[54] undertakes third-party audits of its bitcoin reserves. Through an entrepreneurial process, the industry has solved many of the problems with digital currency, through efforts to assure customers their obligations will be met, or indeed through innovations that allow individuals to control their bitcoin holdings directly. Until this point, security and prudential concerns have been addressed though entrepreneurship and innovation, not regulation.

[50] Professional, regulated bitcoin derivatives and swaps markets are emerging around the world; examples include *TeraExchange* in the US (teraexchange.com), *Crypto Facilities* in the UK (cryptofacilities.com), and *BitMEX* in HK (bitmex.com).

[51] Paul Vigna, "5 Things about Mt. Gox's Crisis," *Wall Street Journal*, February 25, 2014, http://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/.

[52] Jon Russell, "Mt. Gox Customers Can Now File Claims for Their Lost Bitcoins," *TechCrunch*, April 22, 2015, http://techcrunch.com/2015/04/22/mt-gox-claims/.

[53] Nermin Hajdarbegovic, "Coinbase Names Aon as Its Bitcoin Insurance Broker," *CoinDesk*, August 28, 2014, http://www.coindesk.com/coinbase-names-aon-bitcoin-insurance-broker/.

[54] Nermin Hajdarbegovic, "Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit," *CoinDesk*, March 24, 2014, http://www.coindesk.com/krakens-audit-proves-holds-100-bitcoins-reserve/.

Related to security, is the issue of irreversibility of transactions on blockchains and the difficulty in repairing bugs in a protocol's code. An example of this can be found in *The DAO*, a distributed autonomous organisation for venture capital funding that was created on the Etheruem smart contract platform. *The DAO* received $160 million USD in crowdfunding upon its launch in June 2016 and promptly suffered a $50 million USD hack that exploited security vulnerabilities in its code. Bug fixes would be trivial to implement in a centralised code, but corrections to a distributed autonomous organisation are incredibly difficult to make once the system is in use. For *The DAO* this would have required a moratorium on its operation so that new code could be written, and agreement by participants to migrate funds to the new system. Stakeholders in *The DAO* could not reach such an agreement—some believed the hack was in fact a legitimate use of funds, given the poorly written code. In July 2016, after much debate, the decision was made by the encompassing Ethereum community to effectively exercise its higher-level authority to veto *The DAO*. The Ethereum blockchain on which *The DAO* existed was 'hard forked' so that a second version of the blockchain (dated prior to the hack and with updated code) came into existence, and virtually all the diverted funds were restored to their original contracts in the new blockchain. This is a notorious and somewhat ambiguous example of the potential perils of blockchain smart contract—both as a warning to what can go wrong when a new technology is tested in an unregulated environment *and* as an exemplar of the self-regulating potential of blockchains, i.e., an entrepreneurial private governance solution to public harm.

Another concern of policy makers and regulators relates to the pseudonymity of digital currencies and associated applications built by blockchain technologies. Indeed, *just like with traditional money*, pseudonymity generally does confer an ability on criminals to engage in money laundering and illicit trade—more particularly, it has facilitated the rapid expansion of online drug markets. The most illustrious example of this is the deep web black market, or cryptomarket, known as *Silk Road*. The pseudonymous character of Bitcoin (along with the anonymising networking software *Tor*) enables vendors and consumers to openly defy prohibition and participate in a vast transnational digital marketplace of illicit goods and services. *Silk Road* was eventually shut down by authorities following the arrest of its founder Ross Ulbricht in late 2013, but studies have estimated a monthly transaction volume of approximately $1.2 million USD during its February 2011 to October 2013 operation.[55]

Moreover, due to the open-source nature of the underlying technologies, the *Silk Road* prototype has been replicated many times (including its reincarnation *Silk Road 2*) and today there are dozens of competing marketplaces, making the overall cryptoeconomy much more robust than even the heyday of the original *Silk Road*. A survey of the 35 largest cryptomarkets found that between 2013 and 2015 total sales volumes fluctuated between $100 million USD and $180 million USD, even despite major setbacks like

[55] Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* (Carnegie Mellon CyLab Technical Report CMU-CyLab-12-018, July 30, 2012, revised November 28, 2012), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf. Alternative citation: Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). ACM: https://arxiv.org/pdf/1207.7139.pdf.

thefts, scams, takedowns, and arrests during the period.[56] The next generation of cryptomarkets, such as *OpenBazaar*, not only transact in digital currencies but also employ related technologies in their very marketplace infrastructure, meaning they are increasingly difficult for authorities to suppress or takedown.[57]

While it is clear that a number of harms can be associated with cryptomarket-enabled illicit trade, from a regulation policy perspective the more relevant question is a comparative institutional one. In the context of illicit drug trade, do cryptomarkets present a more or less harmful alternative to conventional drug distribution mechanisms?[58] It is apparent that for consumers the benefits of cryptomarkets outweigh the harms: despite asymmetric information problems and the threat of fraud, reputation acts as a sufficient self-enforcement mechanism to support transactions, users are able to avoid the risk of physical violence in physical street-based drug markets, and competition has increased the choice, quality, safety, and value of products and services.[59] Furthermore, when forming public policy, it is important to appreciate that illicit trade using digital currency, though not negligible, is still meager relative to the size of both the black market and digital currency economies.[60]

Likewise, the concern that digital currencies might be used to launder money or finance terrorism is rather more theoretical than empirical at this time. Digital currencies could indeed be used for these activities, but due to the fact that most are pseudonymous at best—because they provide public records of all transactions—the risk of laundering money or financing terrorism with digital currency is much higher than is commonly appreciated. Transaction records will always be public and accessible by law enforcement, meaning that if a connection between Bitcoin addresses and identities can be established, criminals would actually be more easily prosecuted than if they had transacted in traditional cash.

Moreover, several bitcoin exchanges have voluntarily complied with anti-money laundering and counter-terrorist financing (AML/CTF) and 'know your customer' (KYC) record-keeping and reporting requirements. Making such requirements mandatory and comprehensive would thus make digital currency even less attractive for these activities, but care should be given not to overregulate as this could serve only to inhibit legitimate business without a concomitant disincentive to criminal activities. In a sense the genie is already out of the bottle, as drug dealers, money launderers, and terrorists have the option of bypassing

[56] Ibid. For more detail, *The Economist* has extracted data from around 360,000 sales between December 2013 and July 2015 on the tree largest cryptomarkets (Agora, Evolution and Silk Road 2): http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete. See also, the September 2016 special issue of the International Journal of Drug Policy on drug cryptomarkets http://www.ijdp.org/issue/S0955-3959%2816%29X0012-6.

[57] OpenBazaar fashions itself as a decentralised network for peer-to-peer commerce online with no fees and no restrictions, in opposition to centralised incumbents e.g. Silk Road and Amazon: https://openbazaar.org/.

[58] Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer.

[59] Hardy, R. A., & Norgaard, J. R. (2015). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, 1-25. See also Martin (2014) and International Journal of Drug Policy, September 2016.

[60] Jerry Brito, "*National Review* Gets Bitcoin Very Wrong," *Technology Liberation Front*, June 20, 2013, http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/.

exchanges by purchasing digital currency units directly from individual holders. The challenge for policy makers and regulators is to develop oversights that satisfy their concern for criminality without overburdening legitimate activities and discouraging the benefits of digital currency.

2. The regulatory framework

Regulation is ubiquitous in our economies and societies. Governments, and their many agencies, use regulations to implement laws and legislation and achieve their policy objectives. Essentially they are standards or instructions that attempt to delimit what individuals and organisations are permitted or prohibited from doing. Regulation defines the boundaries of economic activity by attempting to modify or limit, but not outlaw.

The simplest economic approach to regulation is cost-benefit analysis. Social benefits are provided when the legal and regulatory framework establishes and enforces property rights and addresses market failures in a way that is comparatively efficient. Social costs are imposed when regulations undermine economic efficiency by diverting resources from otherwise productive private sector activity. According to this framework, regulation should happen when the net social benefit is greater with than without regulation. Yet in practice this seemingly simple cost-benefit calculus is problematic, due to the enormous difficulty in measuring the social costs and benefits of alternative regulatory policy approaches.

Why regulate and why not regulate?

The regulator's task is even more difficult when new technologies such as digital currencies and blockchains are the subject of analysis. The regulatory framework must ensure that it manages any risks that might arise from technological change without stifling innovation. For blockchain, the costs of overregulation could be even greater given its potential status as a general-purpose technology. The regulatory stance taken on a fledgling GPT may seem appropriate at a current moment (i.e., if it passes a net-beneficial cost-benefit calculus) only to be revealed in hindsight to have been over-burdensome. Put another way, the benefits associated with ameliorating the risks and concerns of consumers, policymakers, and regulators *today* could pale in comparison to the foregone benefits that would have otherwise eventuated *tomorrow*, if not for the regulation. Because blockchain is a potential-GPT, extra care should be taken not to sacrifice a dynamically efficient regulatory response (generally more permissive) for a statically efficient (and generally more restrictive) innovation-regulation trade-off.

The structure and shape of the new economies and opportunities afforded by blockchain technology—and the improvements in performance, productivity, and economic growth that come with them—remain shrouded in uncertainty. The only way to discover this information is through entrepreneurial endeavour in markets. There is a very real likelihood that excessive regulation on early-phase entrepreneurial firms, and particular on those engaged with new technologies such as Bitcoin and blockchain, places a significant burden upon innovative practices and structures. What is needed in Australia is a permissionless innovation approach: where entrepreneurs are left free to test, trial and experiment with these technologies. The Productivity Commission recently reached a comparable conclusion about the role of government in the face of potentially disruptive technological change:

> The pace of change has implications for how governments undertake regulatory functions. Some regulations and regulatory approaches are explicitly preventing the development and efficient

> adoption of technologies. In principle, governments should adopt a 'wait and see' approach to new business models and products rather than reacting quickly to regulate what may be unrealised risks.[61]

The permissionless innovation, 'wait and see' regulatory approach would represent a change of practice in Australia; the economy is heavily burdened by regulatory controls.[62] The Australian government has a long and poor history of stifling innovation through regulation. Examples of benign technological innovations that were delayed by excessive regulation in Australia include FM radio and pay television, and more recently somewhat more contested innovations in the sharing economy AirBnB and Uber have had to cope with substantial regulatory uncertainty.[63]

The arguments *for* regulation are well known; counter-arguments *against* regulation, less so. The "public interest" theory of regulation acknowledges that markets are generally efficient at allocating scarce resources to their best uses, but suggests that government intervention may improve (maximise) social welfare, and thereby serve the public interest, by correcting for market failures (e.g. externality, public good, monopoly, or asymmetric information). Yet many regulations—such as those that inhibited FM radio, pay television, and ridesharing—do not correspond to identifiable market failures.

Countervailing views of regulation comes from the Chicago and Public Choice schools of economics, and generally caution that regulation is susceptible to being introduced and implemented so that it furthers the private interest of individuals and organisations rather than the public interest of the community. The "capture theory" of regulation is that politicians and regulators end up being 'acquired' by special interests, usually the organisations they are intended to regulate. The result is that new regulations benefit incumbent market players by presenting barriers to entry for new competitors. Along similar lines, George Stilgler's "Economic Theory of regulation" states that the effect of regulation is akin to wealth transfer, and that it is likely to be biased toward benefiting small well-organised interest groups with strong preferences at the expense of large interest groups with weak preferences. Public choice theory identifies 'rent-seeking' with the economic waste involved in privately interested regulation; and argues that because regulators cannot always predict the consequences of their interventions they may unintentionally produce even worse outcomes than the market failure status quo (i.e., "government failure" or "regulator failure").

Because blockchain is a disruptive, general-purpose technology it is likely to exert pressures on several less efficient incumbent competitors and industries. This gale of creative destruction is set to initiate a "process of industrial mutation that incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one." In the face of this disruptive

[61] Productivity Commission. (2016). Digital Disruption: What Do Governments Need To Do? Available online: http://www.pc.gov.au/research/completed/digital-disruption.

[62] Berg, C. (2008). The Growth of Australia's Regulatory State: Ideology, accountability and the mega-regulators. *Institute of Public Affairs, Australia*. Available online: http://ipa.org.au/publications/980/the-growth-of-australia's-regulatory-state-ideology-accountability-and-the-mega-regulators.

[63] Allen, D., & Berg, C. (2014). The sharing economy. How over-regulation could destroy an economic revolution. *Institute of Public Affairs, Australia*. Available online: http://www.ipa.org.au/publications/2312/the-sharing-economy-how-over-regulation-could-destroy-an-economic-revolution/pg/2.

potential there is a significant threat that regulations will be used to protect private, rather than the public, interest. If regulations impose onerous costs on early-phase entrepreneurship they will effectively erect entry barriers around incumbent industries and the gale of creative destruction will be but a breeze. To encourage the growth of the nascent industries surrounding digital currency and blockchain, regulators should encourage bottom-up, organic, self-regulating institutions prior to introducing top-down government control. The huge potential benefits will only come to fruition if entrepreneurs are able to experiment, expand, and evolve in a flexible environment without unnecessary or onerous regulation.

Regulatory challenges

Current law and regulation does not easily apply to technologies like Bitcoin, because it "does not exactly fit existing statutory definitions of currency or other financial instruments or institutions, making it difficult to know which laws apply and how."[64] Digital currencies and other innovations based on blockchain technology can look like an electronic payments system, a currency, and a commodity, among other things. This situation is reminiscent of the regulatory uncertainty that has accompanied other new technologies, especially new GPTs.

While digital currencies and blockchain technology have generated a great deal of innovation and experimentation, they also raise significant regulatory and policy challenges. These stem from three sources: decentralisation, globalisation, and uncertainty. The first is the decentralised, open-source, and unregulated nature of the underlying blockchain protocol. The second is the digital, and therefore global, nature of the innovation in general and the emerging industries in particular. The third is the uncertain nature of innovation and transformation of general-purpose technologies

It is practically impossible to regulate blockchain *technology* itself, though it is of course possible to regulate the organisations that use the technology, once they bring products and services to markets within the physical jurisdiction of Australian regulators. One cannot regulate the technology of 'the wheel', but one can regulate businesses that use cars and trucks (i.e., the idea of the wheel) to do business. Bitcoin expert Andreas Antonopoulos made this point when he told the Australian Senate Inquiry into Digital Currency "regulation of the protocol itself is not really possible at this time."[65] Blockchain technology developer Ripple Labs also noted "as pure technologies, these protocols cannot themselves be regulated. However, the entities that make use of the protocols to buy, sell, or exchange those virtual or fiat currencies can be subject to regulation."[66] PayPal further elaborated:

> While the currency itself should not be regulated, and transactions by individual users without the assistance of intermediaries should not be regulated, companies that provide a financial service for digital currency transmission, for issuance or sale of digital currency, or for exchange with other currencies such as the Australian Dollar, should be regulated in a manner similar to the existing regulations that apply to other payment services. Those regulations, however, should be adapted to

[64] Brito and Castillo, Bitcoin: Primer for Policymakers.

[65] Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, p. 5.

[66] Ripple Labs, *Submission 21*, p. 3.

> recognise the specific details of how different digital currencies work, particularly 'decentralised' digital currencies that are not controlled by a specific issuer.[67]

Digital currency and blockchain technology is developing within a digital, and therefore global, innovation system. This means that the threat of global innovation arbitrage—the seeking out of different jurisdictions with more favourable and certain regulatory rules—presents another challenge to regulators. Policymakers may need to adopt a commitment to "permissionless innovation" instead of the "precautionary principle" (i.e., constrain innovation until its potential harms are well understood) approach to innovation-regulation. Permissionless innovation advocates implementing bottom-up self-regulation as the default policy mechanism, in which:

> experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if they develop at all, can be addressed later.[68]

Indeed, ASIC has intimated that regulatory arbitrage challenges their ability to subsume digital currency within the financial services regulatory regime. If compliance costs were too burdensome for digital currency trading platforms it would encourage them to move offshore:[69]

> The difficulty in regulating the trading platforms like traditional markets is that the compliance obligations that are associated with running a traditional financial market are quite high. The bar is set quite high. I think it is likely that if you were simply to apply the existing framework to platforms that sell digital currency, most would find it uneconomic to sustain in Australia. And because the market for these bitcoins is global, a lot of that activity would move offshore and Australian consumers would probably still end up being able to speculate with digital currency by buying and selling on foreign trading platforms.[70]

There is a lot of uncertainty surrounding digital currency and blockchain as "we are dealing with a very disruptive and fast-moving technology that has only recently emerged into the limelight"[71] According to Antonopoulos: "We do not really know where Bitcoin will be in a couple of years … There are many unanswered questions at the moment." If global experts have yet to fully appreciate the nuances of the technology (not to mention entrepreneurs that possess intimate and tacit knowledge of it) how can regulators presume to know the most appropriate regulatory framework? Put simply, regulators suffer from a knowledge problem, and the knowledge deficit is compounded by the general-purpose nature of blockchain technology. The Australian Payments Clearing Association believes there to be a "striking" lack

[67] PayPal, *Submission 45*, p. 9.

[68] Adam Thierer. Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom. Mercatus Centre, George Mason University: 2014.

[69] Australian Securities and Investments Commission, *Submission 44*, p. 23.

[70] Mr Michael Saadat, Australian Securities and Investments Commission, *Committee Hansard*, 7 April 2015, p. 38.

[71] Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, p. 6.

of information about the levels of activity in digital currencies and suggests that additional research in this area is required.[72] Ripple Labs is of the same view, arguing that the actual risks and opportunities presented by different digital currency businesses should be clarified before regulation proceeds.[73]

Current regulatory conversation in Australia

The three sources of difficulty for regulators—decentralisation, globalisation, and uncertainty—are evident in the current conversation between regulators and innovators in Australia. Two government inquiries in recent times have been the forum for such conversations: the Treasury Financial System Inquiry (FSI) in 2014[74] and the Senate Digital Currency Inquiry (DCI) in 2015-16.[75] While only tangentially related to digital currency, the FSI found that:

> Digital currencies are not currently widely used as a unit of account in Australia and as such may not be regarded as 'money'. However, their use in payment systems could expand in the future. It will be important that payments system regulation is able to accommodate them, as well as other potential payment instruments that are not yet conceived. Current legislation should be reviewed to ensure payment services using alternative mediums of exchange can be regulated—from consumer, stability, competition, efficiency and [anti-money laundering] perspectives—if a public interest case arises.[76]

The Financial System Inquiry supported broadening regulation to include digital currency, but also recommended graduated regulation in order to "enable market entry and ensure regulation is targeted to where it is most needed." The FSI concluded that while graduated regulation "may increase risks for some consumers, it is expected to improve consumer outcomes overall."[77]

In October 2014, the Senate referred the matter of digital currency to the Economics References Committee for inquiry. This was a much more comprehensive investigation, seeking to examine:

> (a) how to develop an effective regulatory system for digital currency that:
>
> (i) ascertains the most appropriate definition of digital currencies under Australian tax law,
>
> (ii) promotes competition and growth of the digital currency industry,
>
> (iii) ensures ongoing stability in the financial services industry,
>
> (iv) secures protection of consumers and businesses against illegal activity,

[72] Mr Christopher Hamilton, Australian Payments Clearing House, Committee Hansard, 7 April 2015, p. 2.

[73] Ripple Labs, *Submission 21*, p. 13.

[74] The Treasury, 'Financial System Inquiry Final Report', 7 December 2014, http://treasury.gov.au/ConsultationsandReviews/Consultations/2014/FSI-Final-Report (accessed 30 October 2015).

[75] Citation for the Senate Inquiry into Digital Currency.

[76] The Australian Government the Treasury, *Financial System Inquiry: Final report*, November 2014, p. 166.

[77] The Australian Government the Treasury, *Financial System Inquiry: Final report*, November 2014, p. 146.

(v) incorporates digital currencies into Australia's national security framework, and

(vi) ensures the financial stability of the industry;

(b) the potential impact of digital currency technology on the Australian economy, including the:

(i) payments sector,

(ii) retail sector, and

(iii) banking sector;

(c) how Australia can take advantage of digital currency technology to establish itself as a market leader in this field; and

(d) any other related matters.[78]

Lack of regulatory clarity

The Digital Currency Inquiry came at a crucial point in the emergence of blockchain technology, giving experts, entrepreneurs, and regulators the opportunity to share views on how best to support innovation and address the needs of the nascent Australian digital currency industry. There is a view that whether the technology succeeds no longer depends on technical or economic viability (which by now has already proven to be sustainable) but rather will depend on the ability of the industry to operate in a more regulated framework. Which is to say "a well designed and proportionate legal and regulatory regime will support user confidence in, and therefore growth of, innovative payment systems such as virtual currencies."[79]

For the entrepreneurs, the primary concern was a perceived lack of regulatory clarity. PayPal, an online payments service, explained that this factored into its decision not to add Bitcoin as an additional type of currency in the PayPal wallet.[80] According to Australian company CoinJar "much of the uncertainty faced by digital currency companies is not the absence of a rulebook, but rather an abundance of possible existing rulebooks and no clarity on which one will ultimately apply."[81] Another submission (name withheld) explained that Australian banks had "uniformly turned down any involvement with our company, citing the regulatory restraints imposed by the Australian government."[82] Indeed, access to banking services, and other associated business partners, was a common concern among entrepreneurs. The Bitcoin Foundation and Bitcoin Association of Australia[83] and The Melbourne Bitcoin Technology Center[84] both noted that their

[78] *Journals of the Senate*, No. 59, 2 October 2014, pp. 1583–1584.

[79] Dr Rhys Bollen, *Submission 46*, p. 37.

[80] PayPal, *Submission 45*, p. 7.

[81] CoinJar, *Submission 12*, p. 5.

[82] Name withheld, *Submission 2*, p. [1].

[83] Bitcoin Foundation and Bitcoin Association of Australia, *Submission 13*, p. 20.

[84] Melbourne Bitcoin Technology Center, Submission 36, p. [2].

members had experienced discrimination and refusal of service due to a "Blanket classification of all bitcoin businesses and users as 'high risk' customers."

The Australian Securities and Investment Commission (ASIC) noted that it was "aware of a number of banks taking steps to cease dealing with Bitcoin related businesses due to concerns that digital currency providers pose an unacceptable level of risk to the banks' business and reputation." The main reason for this appears to be uncertainty surrounding the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act, as Westpac explained:

> From the point of view of a bank that is providing banking services, if we cannot satisfy ourselves that we can do all the things that we have to do under the legislation to understand the nature of the transactions and what is going on there, it puts us in a very difficult position to be able to provide those banking services. The issues are particularly intense when it comes to moving payments internationally, because obviously we have counterpart banks to deal with globally and they have got their own anti-money laundering, counter-terrorism-finance obligations, and they will expect us to understand the nature of the payments as well.[85]

Essentially, banks find themselves in a vulnerable position when offering designated services to digital currency businesses. Clarifying the regulatory framework that blockchain businesses operate within, particularly with regards to anti-money laundering and 'know your customer' requirements, will help bridge this impasse.

Reserve Bank of Australia (RBA)

Since 1959 the Reserve Bank of Australia has occupied dual statutory functions in: (1) the central bank role of the setting and conduct of monetary policy, including ancillary roles of banknote provision and banking services to the Federal government; and (2) the regulation of the payments system. The RBA's general regulatory approach under the *Payment Systems (Regulation) Act 1998* (PSRA) relies principally on "industry- or market-driven solutions", intervening only when necessary on the grounds of its "responsibility for efficiency and competition in the payments system and controlling systemic risk." It would then seem reasonable that the RBA should regulate Bitcoin and other digital currencies in its second role overseeing the payments system. Indeed, the Governor of the RBA, Glenn Stevens, recently reported "the Board and Bank staff also pay close attention to new technologies, including distributed ledger technologies and other forms of 'fintech', which have the potential to significantly change the payments landscape."[86]

The RBA recognises that the emergence of digital currencies and blockchain technology represents a "fundamental change" to payments and notes that the "use of these systems in Australia has been

[85] Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, p. 22.

[86] RBA Payment Systems Board Annual Review 2016: http://www.rba.gov.au/publications/annual-reports/psb/2016/pdf/2016-psb-annual-report.pdf. Governor's Foreword (p. 3).

extremely limited, but the underlying techniques may find greater use in the years to come."[87] The RBA considers that at this point in time digital currencies do not yet raise any significant concerns with respect to competition, efficiency or risk to the financial system; and are not currently regulated by the RBA or subject to regulatory oversight.[88] If and when the RBA does, however, decide that digital currency and blockchain applications represent a stability issue, it will certainty have authority to designate and regulate over them.[89]

Australian Securities and Investments Commission (ASIC)

The Australian Securities and Investment Commission (ASIC) enforces company and financial services laws to protect consumers, investors and creditors. As such, ASIC might also have remit to regulate digital currencies and blockchain innovations if they can be defined as 'financial products.' Under the current *Corporations Act*, a financial product is a facility through which a consumer "(a) makes a financial investment (b) manages financial risk; or (c) makes non-cash payments."[90] During the 2014 Parliamentary Joint Committee on Corporations and Financial Services, ASIC announced its approach to digital currency:

> ASIC monitors new developments in the marketplace and, accordingly, ASIC is considering whether and how the legislation it administers, such as the Corporations Act, applies to virtual currencies.
>
> ASIC's view is that Bitcoins themselves (and other virtual currencies) are not financial products and are not regulated under the legislation we administer.[91]

This means that "a person is not providing financial services when they operate a digital currency trading platform, provide advice on digital currencies or arrange for others to buy and sell digital currencies."[92] As such they do not require:

(a) an Australian market licence to operate a digital currency trading platform; and

(b) an Australian financial services (AFS) licence in order to:

(i) trade in digital currency;

(ii) hold a digital currency on behalf of another person;

(iii) provide advice in relation to digital currency; and

[87] Review of Card Payments Regulation – Issues Paper. Available online: http://www.rba.gov.au/payments-and-infrastructure/review-of-card-payments-regulation/review-of-card-payments-regulation-issues-paper.html.

[88] Reserve Bank of Australia, Submission 19, p. 9; Dr Anthony Richards, Reserve Bank of Australia, *Committee Hansard*, 7 April 2015, p. 45.

[89] Mr Christopher Hamilton, Australian Payments Clearing House, *Committee Hansard*, 7 April 2015, p. 7.

[90] Australian Securities and Investments Commission, *Submission 44*, p. 8.

[91] Parliamentary Joint Committee on Corporations and Financial Services, *Statutory Oversight of the Australian Securities and Investment Commission, the Takeovers Panel and the Corporate Legislation Report No. 1 of the 44th Parliament*, November 2014, p.25.

[92] Australian Securities and Investments Commission, *Submission 44*, p. 11.

(iv) arrange for others to buy and sell digital currency.[93]

However, this is not the end of the story. Even though digital currency does not fit within the definition of a financial product, if a currently regulated financial services provider was to expand its product offerings into digital currencies, these products *would* be considered financial products. The same would be true conversely if a digital currency business was also providing a facility that qualified as a financial product.

> A digital currency, in and of itself, is not a financial product. Providing advice about a digital currency is not financial product advice, buying and selling digital currency means you are not making a market in a financial product. But some ancillary services you might provide that are associated with digital currencies could be regulated by ASIC.[94]

For example, when PayPal entered into an agreement with Bitcoin payments processors Bitpay, Coinbase and GoCoin (to enable its merchants to accept Bitcoin) it had to comply with the usual financial services licensing, conduct, and disclosure obligations for financial products in the Corporations Act.[95]

Recall also that digital currency is but one application of blockchain technology, and some other blockchain applications—as well as other facilitates associated with digital currencies—might fall within the definition as financial products.[96] The upshot is that because entrepreneurs do not yet know all the applications of the technology, ASIC does not know, and cannot say, whether future innovations will qualify as financial products and be subject to their regulatory requirements. It does seem likely, however, that some classes of blockchain innovations will meet this condition and therefore that ASIC will have some regulatory role. But because neither ASIC nor the public yet have this knowledge, we are left at another impasse of entrepreneurial and regulatory uncertainty.

Australian Competition and Consumer Commission (ACCC)

The Australian Competition and Consumer Commission (ACCC) has the responsible of ensuring that individuals and businesses comply with Australian competition, fair trading, and consumer protection laws—in particular the *Competition and Consumer Act*. These general consumer protection provisions state that businesses must not make false or misleading representations or engage in unconscionable conduct.[97]

While ASIC does not consider digital currencies to be a financial product for the purposes of the Corporations Act or the ASIC Act, the consumer protection obligations of the *Competition and Consumer Act* do apply to digital currencies. They would also likely apply to all manner of new product and service innovations that are derived from blockchain technology.

[93] Australian Securities and Investments Commission, *Submission* 44, p. 3.

[94] Mr Michael Saadat, Australian Securities and Investments Commission, *Committee Hansard*, 7 April 2015, p. 43.

[95] Australian Securities and Investments Commission, *Submission* 44, p. 15.

[96] Australian Securities and Investments Commission, *Submission* 44, p. 11.

[97] Australian Securities and Investments Commission, *Submission* 44, p. 8.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Australian Transaction Reports and Analysis Centre (AUSTRAC) is an Australian government financial intelligence agency set up to combat money laundering, organised crime, tax evasion, welfare fraud and terrorism. It does this under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

In late 2015, during the Parliamentary Joint Committee on Law Enforcement inquiry into financial related crime[98], the Australian Crime Commission (ACC) said in relation to Bitcoin and financial crime:[99]

> The anonymity that this process affords, and the ease with which virtual currencies can be exchanged within and across borders, make them attractive to serious and organised crime. Virtual currencies are also attractive to individuals seeking to engage in criminal activities and the 'darknet', such as the former Silk Road, which relied solely on Bitcoin for the trade in illicit goods, including illicit drugs.[100]
>
> Although virtual currencies such as Bitcoin are seen as vulnerable for exploitation by organised crime seeking to facilitate money laundering activities, evidence that this is occurring on a large scale is yet to be identified.[101]

The AML/CTF Act defines e-currency as "an internet-based, electronic means of exchange that is… backed either directly or indirectly by precious metal or bullion or a thing of a kind prescribed by the AML/CTF Rules." This means the majority of digital currencies—including Bitcoin—are not currently covered under the Act because most are not backed by precious metal or bullion. This exception also extends to most other non-currency applications of blockchain technology as well. AUSTRAC could however exercise authority over digital currency and blockchain applications using the 'thing of a kind prescribed by the AML/CTF Rules' clause, but no such rules have been issued to date. This does not mean, however, that AUSTRAC has absolutely no regulatory oversight, because whenever digital currencies are exchanged for fiat currencies the transactions will generally intersect with banking or remittance services which are regulated under the AML/CTF regime.[102] AUSTRAC current position is that while digital currency may pose a greater risk in the future, "right now we are not seeing that there is the sort of risk that has us saying to government, "It is imperative that you give us greater sight over this''".[103]

[98] Parliamentary Joint Committee on Law Enforcement, Inquiry into financial related crime. Available online: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Report.

[99] Parliamentary Joint Committee on Law Enforcement, 'Inquiry into Financial Crime', http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime; see for example AUSTRAC, *Submission 10*, pp. 20–21.

[100] ACC, Submission 5, Attachment 1, p. 17.

[101] ACC, Submission 5, Attachment 1, p. 18.

[102] Attorney-General's Department, *Submission 42*, p. 11.

[103] Ms Jane Atkins, Australian Transaction Reports and Analysis Centre, *Committee Hansard*, 7 April 2015, p. 52.

Self-regulation: Australian Digital Currency Commerce Association (ADCCA)

The digital currency industry is not objecting to regulation. In fact, as the Treasury notes "the industry, domestically, is trying to do self-regulation that in some respects mirrors some of the actual legal requirements, because they see that there is benefit in having a self-regulatory model."[104] In order to help manage relationships with banking services and be prepared for future regulation, some digital currency businesses have tried to mirror the obligations that are required by designated services under the AML/CTF regime, such as implementing know your customer programs.

The Australian Digital Currency Commerce Association (ADCCA) is the country's leading council and representation of and for digital currency businesses:

> The organisation's founding mandate is intended to act as the essential connection between merchants, industry, governments, regulators, financial institutions and influential policy forums which give direction to this emerging industry at home and abroad.

ADCCA recommended a self-regulatory model for the digital currency businesses:

> ADCCA believes a self-regulatory model enforced through its industry Code of Conduct, to which ADCCA members must adhere, is the ideal regulatory environment to support the Digital Currency industry. This framework will enable customers to have greater confidence in the entities providing Digital Currency FinTech services. The Code of Conduct comprises several best practice requirements benchmarked against requirements for Australian financial services institutions.[105]

According to ADCCA:

> In Australia the vast majority of Digital Currency businesses and users are law-abiding and desire the enhanced legitimacy of appropriate legal oversight and recognition. Incorporating Digital Currency into law enforcement legislation, particularly through the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, is a necessary step toward guaranteeing the security and legitimacy of Digital Currencies in Australia.[106]

Efforts at self-regulation are hampered by the fact that the AML/CTF Act currently does not fully cover digital currencies. As a consequence of this, digital currency businesses are not able to access the Document Verification Service, which would better facilitate identity checking to meet AML/CTF requirements. It would seem reasonable to applying AML/CTF regulations to digital currency exchanges. In the very least this would assist bodies like ADCCA in their self-regulatory efforts.

[104] Mr McAuliffe, Treasury, *Committee Hansard*, 4 March 2015, p. 23.
[105] Australian Digital Currency Commerce Association, *Submission 15*, p. 3.
[106] Australian Digital Currency Commerce Association, *Submission 15*, p. 14.

3. Recommendations

Bitcoin, a cryptocurrency, and the underlying technology upon which it is based—blockchain, or distributed ledger technology—is a new general purpose technology, and like other GPTs (such as lasers or personal computers) will have substantial and deep impact over many industries and over many years and decades to come. Its application to digital money and internet-based payments is just one of what is likely to be hundreds of domains of subsequent application. The fundamental risk that regulators face at this early juncture is that in the effort to control the technology *as it exists now*, they inadvertently lock-in or bias particular use-cases or product categories and foreclose future development and opportunities. The costs of early regulation accrue to stifled and truncated future technological development and the lost productivity gains that might bring. This suggests that the value of a wait-and-see attitude focused around regulatory learning will likely maximize the societal and economic gains through rapid exploration, experimentation and adoption of the new technology.

We recommend the following:

1. Regulate products and services as they develop, not the technology. That is, regulate particular applications and services based on cryptocurrencies, not cryptocurrencies themselves.

    - Wait for products to emerge then regulate case-by-case or 'business as usual'. This should be done through specialist extant regulators in these product categories (e.g. ASIC).
    - Adopt a 'permissionless innovation' approach (Thierer 2014), otherwise known in Australia as 'wait and see' regulation. As indicated in section 3 above, the Productivity Commission and ASIC have already signalled they intend to take this path.
    - Engage in regulatory learning through local experimentation, such as the use of a regulatory sandbox approach.

2. Allow self-regulation (e.g. through the Australian Digital Currency Commerce Association, ADCCA) and graduated regulation to develop

    - This allows local knowledge and experience to accumulate, indicating where regulatory agencies do and do not need to act.

3. Adopt a functional regulatory approach

    - Distributed ledger technology and cryptocurrencies are a general purpose technology and have multiple uses besides payments, many of which are still undiscovered. Specialist regulators should focus only on the products and services as they emerge and can be identified into functional product categories.

4. Conclusion

A particular conclusion we draw from this report is that the Reserve Bank of Australia should not be involved in regulation of cryptocurrencies in Australia.

In a previous ATA/IAEP report 'Who Should Regulate the Bank Interchange Fee?' it was argued that the RBA should not regulate the bank interchange fee, but that it should be done by a specialist regulator, such as the ACCC, on grounds of transparency and specialist competence. A similar argument applies here. Cryptocurrencies and distributed ledger technologies are a general purpose technology and should only be regulated at the point of particular applications and uses, which then falls to specialist regulatory domains.

Payments is a fast moving technological space, and the burgeoning development of cryptocurrencies, such as bitcoin, does much more than just introduce electronic money into an existing payments system. Because blockchain platforms such as Ethereum can be used to embed smart contracts (among other features, such as multisig transactions and decentralised autonomous organisations) into the payments ecosystem, the governance and regulation of payments platforms becomes inseparable from the underlying code or technology. Code is law, as Laurence Lessig put it. The regulatory role cannot stand outside the design and implementation of the technology, thus requiring specialised competence. As a specialist in monetary policy, the RBA does not have, nor should it have, these technical capabilities in code development or platform design. The Payments System Board was never well-placed within the Reserve Bank of Australia because of the very different specialisations.

These exciting developments in cryptocurrency as a new technology for payments furnish yet another reason why the *Payment Systems (Regulation) Act 1998* should be repealed, and Payment Systems regulation moved to a specialist regulator.