WHAT DOES THE BLOCKCHAIN MEAN FOR GOVERNMENT?

- CRYPTOCURRENCIES IN THE AUSTRALIAN PAYMENTS SYSTEM -

WHAT DOES THE BLOCKCHAIN MEAN FOR GOVERNMENT? CRYPTOCURRENCIES IN THE AUSTRALIAN PAYMENTS SYSTEM

Chris Berg, Sinclair Davidson and Jason Potts

EXECUTIVE SUMMARY

- This paper introduces the radical opportunities that the invention of distributed ledger technologies offer for government, using the Australian payments system as a case study.
- Blockchains were invented as the underlying technology behind the Bitcoin cryptocurrency in 2009.
- With the blockchain the pseudonymous inventor 'Satoshi Nakamoto' solved the 'double spending' problem endemic to digital currencies and created a fully distributed ledger.
- The paper presents a guide to some of the major cryptocurrencies released since 2009.
- However, blockchains have more uses than just as cryptocurrencies. Blockchains are an 'institutional technology' which allow for the creation of new methods of exchange.
- The paper presents a model for the reform of government in light of the blockchain based on the new comparative institutional economics literature.
- In response to invention of the blockchain, governments should:
  - Allow firms to experiment and introduce blockchain enabled services – that is, take "permissionless innovation" approach.
  - Adapt regulatory environments to accommodate the use of blockchain applications where those applications cross over existing regulatory requirements – for example, in the space of taxation, and financial and prudential reporting.
  - Directly adopt blockchain technologies for delivering government services and to enhance (or replace) existing government processes.
- The paper presents as a case study the use of blockchain for the Australian payments system
- It provides a brief history of the development of the payments system since the colonial period
- Blockchains bring the payments system closer to the monetary system envisaged by Friedrich Hayek, where money and payments systems were structured by the market, rather than political demands
- The paper explores the implications of payments systems as two-sided market.
- Interchange fees exists to rebalance financial relationships within a two-sided market
- The paper explores how blockchains could be used more deeply in the financial system, suggesting the possibility of a 'cryptobank'
- The nature of blockchain technologies means that their adoption presents significant governance challenges for the Australian government
- The paper recommends that the Australian government adopt the organisational approach of the United Kingdom, which has a payments system regulator institutional separate from the central bank.
- Realising the huge opportunity of the blockchain will require forward-thinking and often dramatic reform.

1. INTRODUCTION

Blockchains and the cryptocurrencies they support offer potentially revolutionary opportunities for the Australian economy. In coming years, it is likely that we will see blockchain and distributed ledger technologies introduced into some of our most important economic and legal institutions, from the financial system, to identity management, to the organisation of private property rights.

The benefits from these blockchain applications could be immense. Blockchains can reduce and even eliminate some of the most fundamental barriers to efficient markets. They can drive deeper and more liquid markets, reduce the costs of finding and building economic relationships, and can return economic control to individuals away from hierarchical firms and states.

For policymakers, blockchains present a particular form of the 'innovation problem'. Most innovation policy questions focus on where the ideas for new innovations come from, how that development can be funded, and how innovations can be commercialized. There is a large amount of work globally on blockchain applications, and no obvious need for government intervention in their development. Australia is already participating in that work and has a number of promising blockchain firms.

However, the most potentially revolutionary and beneficial blockchain applications cross over, and often contradict, much of the existing regulatory and economic system. The significance of this is that the countries which best take advantage of blockchain opportunities will not necessarily be the ones that develop the technologies themselves. Rather, the countries which are able to adapt and reform their institutional frameworks will be best placed to take advantage of the blockchain revolution.

Taking advantage of the blockchain revolution means having regulatory environments that are able to accommodate blockchain applications. It means being willing to experiment with and adopt blockchains for the delivery of public services. It means having a taxation system that is adapted to the needs of blockchain-enabled firms and smart contracting arrangements.[1] In summary, to take exploit this opportunity, governments need to:

- Allow firms to experiment and introduce blockchain enabled services – that is, take "permissionless innovation" approach.[2]
- Adapt regulatory environments to accommodate the use of blockchain applications where those applications cross over existing regulatory requirements – for example, in the space of taxation, and financial and prudential reporting.
- Directly adopt blockchain technologies for delivering government services and to enhance (or replace) existing government processes.

[1] We raise some issues in this area here http://chrisberg.org/2017/10/opening-statement-to-house-standing-committee-on-tax-and-revenue-inquiry-into-taxpayer-engagement-with-the-taxation-system/

[2] A.D. Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Mercatus Center, George Mason University, 2014).

This paper addresses the latter two points, by looking at one relatively simple blockchain use-case: the introduction of cryptocurrencies into the Australian payments system. Cryptocurrencies were the first application developed on the blockchain and are currently in the most advanced state of development. Introducing cryptocurrencies into the payment system offers a wide array of potential benefits, including faster and more reliable transaction processing, automatic auditing (that is, verifiability), and transaction permanence. However, integrating cryptocurrencies into the regulatory framework that governs payments is a non-trivial problem. The existing institutions have been developed and structured around specific technologies that have distinct economic properties and limitations. Blockchains materially change the economics of payments systems, and, if Australia is to realize the benefits of cryptocurrencies, will require significant regulatory reform.

This paper proceeds as follows. In Part 2 we provide a brief introduction to blockchain technologies. In Part 3 we explore the blockchain as an institutional technology and introduce the field of 'institutional cryptoeconomics'. In Part 4 we outline some economic principles that will underpin the introduction of the blockchain into political, legal and regulatory systems. In Part 5 we look at how blockchains can be used in the Australian payment system, beginning with a history of the payments system, and how the introduction of cryptocurrencies will have broad consequences for regulation and the monetary system. In Part 6 we offer a speculative proposal for a 'cryptobank' that follows from the prior analysis. Part 7 discusses the institutional framework that should govern these changes. Part 8 concludes.

2. A BRIEF INTRODUCTION TO THE BLOCKCHAIN

The blockchain is the underlying technology that powers the cryptocurrency Bitcoin and other cryptocurrencies. It was first outlined in 2008 by the pseudonymous 'Satoshi Nakamoto' in his white paper "Bitcoin: A Peer-to-Peer Electronic Cash system".[3] The blockchain is a decentralised, distributed ledger that records transactions without the need for a trusted third party or intermediary. Nakamoto's purpose was to develop a native digital currency that was not vulnerable to centralised authorities. In this sense he was contributing to a project that was already two decades old, and had been contributed to by DigiCash (founded in 1990), E-Gold (founded in 1996), and PayPal (founded in 1998).

Digital currencies are vulnerable to the 'double spending' problem. This problem derives from the fact that it is trivially easy to copy a digital item. Opportunistic users might try to buy two goods with one unit of currency. The double spending problem is similar to the counterfeiting problem with fiat currency. Typically this problem has been solved with a trusted intermediary that validates transactions to ensure they are not double spent. Bitcoin decentralised that validation, creating an open network governed by a protocol in which 'miners' compete to solve a difficult puzzle to validate the most recent transactions on the network.

The technologies which make up the blockchain were not especially new when they were brought together by Nakamoto. The blockchain uses **asymmetric cryptography**. Where symmetric cryptography uses the same key to both encrypt information and decrypt it, asymmetric cryptography has separate keys for encryption (a public key) and decryption (a

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (www.bitcoin.org2008).

private key). This system of cryptography allows strangers to deposit information with a user but prevents strangers from withdrawing that information. Blockchains are distributed **peer-to-peer networks**. Networks can be either client-server or distributed. Client-server networks are easy to administer, secure and police but rely on a trusted client to update the network, and consequently present a single point of vulnerability. By contrast, peer-to-peer networks are decentralized, robust, hard to police and censor, but also hard to administer and ensure consistency (consensus) about the state of the network. Blockchains also utilize an **append-only database**, where information is immutable, and transactions are recorded as additional data rather than overwriting existing data (as, for instance, a simple Excel spreadsheet does). Each block in the blockchain includes a 'hash' (a secure cryptographic summary) of the previous block in a chain all the way back to the genesis block mined by Nakamoto himself.

Finally, the blockchain uses **game theory** in order to distribute consensus about the state of the network. In the Bitcoin blockchain, miners solve a difficult cryptographic puzzle for the right to update create a new block on the chain containing recent transactions. Successful miners are awarded with an amount of Bitcoin (currently 12.5 Bitcoin) for each correctly solved block. The difficulty of the puzzle updates periodically and the reward decreases periodically in order to maintain a steady rate of inflation. Mining is a costly signal that seeks to make the blockchain incentive compatible; that is, align users incentives to maintain and protect valid data and reject invalid data (such as double spending). The resulting network bakes economic incentives into the structure of the network itself, distributing economic value to those who maintain it.

Bitcoin was the first implementation of the blockchain but blockchains have been used for a wider range of applications. Bitcoin provides a public ledger which raises privacy issues, leading to the development of privacy-focused cryptocurrencies like ZCash and Monero. Developers quickly realized that other information – that is, records of ownership other than 'money' – could be carried on the blockchain. In 2011 Namecoin was established: a cryptocurrency that resolves domain names. Bitcoin includes a scripting language allowing users to develop contingent contracts – such as escrow services and multisignature transactions – into the network itself.

Blockchain technologies are in a rapid state of development. For example, Bitcoin (in its current form) does not scale well, transactions can be slow to reconcile, its verification algorithm is vulnerable to centralization, is extremely energy intensive, its scripting language is limited, and has governance problems surrounding technical updates. Each of these problems are being tackled by developers and entrepreneurs. Ethereum, launched in 2015, is a blockchain implementation that offers a more complex ('turing complete') scripting language, and is developing a 'proof of stake' consensus mechanism that seeks to resolve the high cost and potential centralization of Bitcoin mining. Other blockchains and adaptations of the original Bitcoin protocol provide solutions to these problems.

In 2017, the range of blockchain use cases has blossomed. Utilizing the enhanced scripting of Ethereum, more complex 'smart contracts' ensure that financial and other transactions are completed exactly as they have been written, without the need for human intervention or the possibility of censorship. A 'decentralised autonomous organisation' could utilize smart

contracts and pays in cryptocurrency in order to solve economic problems, such as managing a fleet of self-driving cars or an insurance network. Private and permissioned blockchains enable organisations to implement their own blockchains in a trusted or semi-trusted environment. In the next section we describe some of the main cryptocurrencies as a guide to the blockchain ecosystem.

A guide to significant cryptocurrencies

Bitcoin

Bitcoin is the original cryptocurrency. Invented by the pseudonymous Satoshi Nakamoto, Bitcoin was released as open-source software in 2009. Bitcoin is limited to 21 million bitcoins, a limit which is expected to be reached around 2140. Nakamoto stepped back from development in 2010. The software which manages the Bitcoin network is managed by a team of volunteer developers. The miners, who validate transactions in return for the right to forge new Bitcoins, also exercise influence over changes to the network.

Namecoin

Namecoin was the first 'fork' of the Bitcoin network, which occurred in 2011. Namecoin's key usecase is as a censorship proof domain system. In the current internet, domain registration and resolution is provided by the Internet Corporation for Assigned Names and Numbers (ICANN), a centralised non-profit multistakeholder authority. Namecoin runs .bit, a distributed rather than centralised top level domain. Namecoin has broader uses for identity management.

Litecoin

Litecoin was established in 2011 as a fork of Bitcoin designed to resolve some of the technical issues in Bitcoin. Litecoin speeds up the creation of new blocks, aiming at a target of a new block every 2.5 minutes rather than every 10 minutes. Litecoin also has a different hashing algorithm and a larger limit on total coins (84 million).

Ripple

Ripple is a real-time currency exchange settlement initialed released in 2012. Ripple does not use a public blockchain. Rather, it is secured by a private blockchain connected a set of verified nodes (such as participating financial institutions). Ripple's coins, XRP, are not mined but are issued. Ripple is being experimented with and used by a large number of major financial institutions to speed up interbank payments.

Dash

Dash was originally released as XCoin in 2014. Dash is a fork of Litecoin, which divides its governance and verification into two tiers. Blocks are created by miners. Governance functions are provided by masternodes, that operate Dash as a decentralised autonomous organisation. Dash also has privacy features utilizing a coin-mixing tool (PrivateSend) and features near instant transactions (InstantSend).

Ethereum

Ethereum was developed by Vitalik Buterin and went live in July 2015. Ethereum is a cryptocurrency with a large number of distinct features from Bitcoin. Its primary feature is that it offers a 'turing complete' scripting engine which allows for complex computation. Ethereum acts as a universal global computer. Ethereum's currency is called Ether and computations on the network require 'gas' to pay for and ration scarce computational resources.

Monero

Monero was released in 2014 as a privacy focused cryptocurrency. Monero hides the sender, recipient and volume of a transaction by mixing addresses for recipients,, generating 'stealth' addresses for senders, and hiding transaction volumes.

Zcash

Zcash was released in 2016 as a privacy focused cryptocurrency that both utilizes a public blockchain and allows users to conduct private transactions that conceal the sender, recipient, and volume of a transaction. Zcash utilizes zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), a type of cryptography that allows provers to demonstrate to verifiers that a statement is true without providing any information beyond the verification.

Augur

Augur is a decentralised prediction market built on top of the Ethereum network. Released in 2016, Augur has its own native cryptocurrency (reputation or REP). REP is used to resolve predictions and successful predications are paid out in Bitcoin or Ethereum.

3. THE BLOCKCHAIN AS AN INSTITUTIONAL TECHNOLOGY

Beyond the internet payments envisioned by Nakamoto and early digital currency proponents, some early and obvious financial use cases of blockchains include trade finance, the facilitation of international payments, banking and financial settlement, the creation and maintenance of new financial instruments. Other uses include permanently recording property ownership on the blockchain, such as property titles, caveats, and encumbrances, and for supply chain management, such as offering a permanent and indelible record of provenance. Further down the track but potentially revolutionary is digital identity management on the blockchain which, when combined with privacy enhancing features, could significantly change the relationship between the government and citizen data.[4]

Institutional cryptoeconomics is an economic approach to understand the economic consequences of the adoption of blockchain technologies for governments, firms and society

[4] See Chris Berg, "Medicare Details Available on Dark Web Is Just Tip of Data Breach Iceberg," *Canberra Times*, 17 July 2017.

more generally. Institutional cryptoeconomics provides a framework to identify potential uses of blockchains and how the institutions of society might shift and adapt in response.

The study of blockchain technologies is in a very early stage but we can distinguish two schools of thought. The first conceptualises blockchain as a new *general purpose technology*.[5] General purpose technologies are innovations which are characterised by their broad potential use-cases ('pervasiveness'), their capacity for technological improvement and their complementarity with other technologies. In this, blockchain joins the ranks of steam power, electricity, and the semi-conductor. Blockchains reduce the costs of verifying identifies and networking without intermediaries, opening up the possibility of new markets and to significantly reduce transaction costs in existing markets.[6]

By contrast, institutional cryptoeconomics sees blockchain as an *institutional technology*. Rather than enhancing existing economic institutions, blockchains opens up new opportunities for exchange – that is, to create new *economies*.[7] Blockchain is a distributed computation technology for coordinating activity in a distributed economy. Institutional cryptoeconomics is in the transaction school tradition of Nobel laureates Ronald Coase and Oliver Williamson and sees the blockchain as a new type of economic institution that enhances (and competes with) the existing economic institutions of capitalism: firms, markets, commons, relational contracting, and governments.

A decentralised distributed ledger is significant because ledgers have a previously unheralded critical role in economic organisation. Ledgers consist of data structured by rules. A ledger records (that is, maintains consensus about) ownership and provides a mechanism to verify that ownership. As Davidson, Potts and De Fillipi write,

> A ledger is an ancient accounting technology to record (i.e. maintain consensus about) whom (or what) owns what, of who (or what) has agreed to what, of what counts as a what, and to record when anything of value is transacted. As the fundamental instruments of transactional legitimation, ledgers are an elemental technology of modern market capitalism and statecraft (Nussbaum 1933, Yamey 1949, Allen 2011). So a significant shift in ledger technology—from a centralised method of producing consensus in the ledger (using trust) to a distributed approach to consensus (using the blockchain)—could transform the transactional mechanics of a modern economy.[8]

This approach places ledgers at the center of any structure of property ownership. Any system of property rights needs a ledger to record ownership and for owners and others to consult.

---

[5] Timothy F Bresnahan and Manuel Trajtenberg, "General Purpose Technologies: 'Engines of Growth'?," *Journal of econometrics* 65, no. 1 (1995); Trent J MacDonald, Darcy WE Allen, and Jason Potts, "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking," in *Banking Beyond Banks and Money* (Springer, 2016).

[6] Christian Catalini and Joshua S Gans, "Some Simple Economics of the Blockchain," (National Bureau of Economic Research, 2016); Marc Pilkington, "Blockchain Technology: Principles and Applications," in *Research Handbook on Digital Transformations*, ed. F Olleros and M Zhegu (Cheltenham: Edward Elgar, 2015); David Yermack, "Corporate Governance and Blockchains," *Review of Finance* 21, no. 1 (2017).

[7] Sinclair Davidson, Primavera de Filippi, and Jason Potts, "Blockchains and the Economic Institutions of Capitalism," *Journal of Institutional Economics* (forthcoming); Chris Berg, "What Diplomacy in the Ancient near East Can Tell Us About the Blockchain," *SSRN* (2017).

[8] Davidson, Filippi, and Potts.

Institutional cryptoeconomics says it is not enough to assert the existence of a property rights regime. Property rights require institutional technologies (firms, markets, governments, etc.) to maintain ledgers of ownership. Owners need their ownership to be recorded on the ledger to draw on the rights associated with that property. Buyers need to know what they are buying can be legitimately sold.[9]

As this suggests, the most basic property right is a property and land title register. But much of what government does is maintain ledgers of property rights. The register of Births, Deaths and Marriages records the existence of individuals at key moments in their life. Business registers record information about taxable corporate forms. Citizenship is a ledger, recording who enjoys the privileges and responsibilities of citizenship – voting, taxation, and jury duty - and who (through their absence on the ledger) is excluded from their privileges and responsibilities. Ledgers record who can sit in parliament, who can work with children, who has security clearance. Social security rights are a ledger, recording who (and under what circumstances) has a right to an entitlement – subsidized health care, subsidized education, disability and old-age pension support.

Much regulation and regulatory technology is structured around ledgers. Ledgers structure tax obligations. Ledgers record who can practice medicine, who can serve liquor, and which firms can mine and where. Ledgers record who can offer banking services (authorized deposit institutions) and which firms (and accounts) have their deposits protected by law. Governments audit firms (or license private auditors) to ensure they are solvent. The monetary system is a ledger. Since the end of the free banking system in Australia, the government has assumed the role of the maintenance and validation of the ledger of money ownership. While the ownership of physical currency is indicated by its possession, the existence of a note is recorded, released, authorised and validated by the Reserve Bank of Australia.

The ideal ledger has ten properties: completeness (all relevant economic elements of the real world are mapped on the ledger), correspondence (its data corresponds to the real world), compactness (it is a minimum efficient representation of the real world), predictability (it changes only when the real world changes), robustness (it is resistant to changes that are not reflected in the real world), integrity (the ledger only contains 'good' information), legibility (the ledger needs to be readable), accessibility (the ledger can be accessed a low cost), and updatability (the ledger is immutable – it cannot be rewritten, only added to). Finally, and most fundamentally the ideal ledger represents a social consensus about the state of the world.

Each of these ledgers described above operated (or supervised) by the hierarchical institution of the state. Government variously plays the role of trusted authority with the responsibility of maintaining the ledger, authorizing transactions on (that is, changes to) the ledger, and verifying ledger entries. Government plays these roles because it was both practically and technically necessary for it to do so. The government, with a monopoly of the use of force and funded by compulsory taxation, is in the best position to manage ledgers that approximate the attributes of an ideal ledger.

[9] Chris Berg, Sinclair Davidson, and Jason Potts, "The Blockchain Economy: A Beginner's Guide to Institutional Cryptoeconomics," *Medium* 2017.

The invention of the blockchain significantly changes this technical and economic calculus. On a number of characteristics blockchains can more closely approximate the ideal ledger than government run ledgers. The censorship-resistance of the blockchain makes has superior robustness and integrity properties. The distributed nature of the blockchain is more accessible than government ledgers: the blockchain is 'always-on' (by comparison with a government ledger which can often only be accessed during, for instance, business hours) and accessible to users who simply have internet access. The blockchain is immutable – and verifiably so – unlike many government databases. For the purposes of both verification and updating the blockchain is decentralised and (for public blockchains at least) accessible to all.

At the first approximation this means that many ledgers maintained and operated by the government can now be more effectively and efficiently operated by the blockchain in a decentralised fashion. In the next section we outline some principles to understand how introducing the blockchain to government policy and process represents a fundamental institutional change.

4. REFORM OF GOVERNMENT AND THE STATE IN LIGHT OF THE BLOCKCHAIN

The blockchain is just as likely to disrupt government as it will disrupt industry and the private sector. Government, however, is a very loose term that describes the public, and usually not-for-profit, sector of the economy. There is much more to government than the traditionally understood executive, legislature, and judiciary. At this very high level of abstraction the blockchain is likely to disrupt a lot of the activities currently perform by the judiciary. In order to gain a better understanding of disruption it is worthwhile examining some of the functions of the state (rather than a narrow examination of government).

Adam Smith prescribes three governmental functions: national defence, the administration of justice, and public works "which though they may be in the highest degree advantageous to a great society, [they] are, however, of such a nature, that the profit could never repay the expense to any individual or small number of individuals".[10] Smith, however, provides a strong caveat to his public goods argument; these public works exist chiefly to "facilitate the commerce of society" and "instruction of the people". Herbert Spencer had a more limited role for government; "to defend the natural rights of man – to protect person and property – to prevent the aggressions of the powerful upon the weak – in a word, to administer justice".[11] Ludwig von Mises provides a similar perspective.[12]

> As the liberal sees it, the task of the state consists solely and exclusively in guaranteeing the protection of life, health, liberty, and private property against violent attacks. Everything that goes beyond this is an evil. A government that, instead of fulfilling its task, sought to

[10] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (Chicago: University of Chicago Press, 1976), vol 2, p. 244.
[11] Herbert Spencer, "The Proper Sphere of Government," in *The Man Versus the State: With Six Essays on Government, Society, and Freedom* (Indianapolis: Liberty Fund, 1982), 187.
[12] Ludwig von Mises, *Liberalism: The Classical Tradition* (Indianapolis: Liberty Fund, 2005), 30.

> go so far as actually to infringe on personal security of life and health, freedom, and property would, of course, be altogether bad.

A minimal state that exists simply to deter violence and administer justice will not suffer too much disruption – apart from fewer contractual dispute entering the courts. The modern state, however, does much more than simply deter violence. According to Friedrich Hayek, there are at least (additional) four areas when government action occurs.[13]

- First, where the market would not provide any service, for example, "a reliable and efficient monetary system", "setting of standards of weights and measures", "land registration, statistics, etc". Hayek includes here "the support, if not also the organization, of some kind of education".
- Second, those services that are clearly desirable, including "most sanitary and health services, often the construction and maintenance of roads, and many of the amenities provided by municipalities".
- Third, other activities such as to "encourage the advancement of knowledge".
- Fourth general regulation is a legitimate function of government.

Tellingly Hayek describes the first of these four activities as facilitating "the acquisition of reliable knowledge about facts of general significance". In other words being either an information broker or a trusted third party. It is here that the activities of the government and state will be directly disrupted. Any organisation be it public or private that simply acts as an information broker or trusted third party is very likely going to be disrupted by the blockchain. Importantly to the extent that the government earns revenue from those roles that revenue is also likely to be disrupted. Hayek's idea that the private sector cannot or will not provide a reliable and efficient monetary system is discussed below. It is also very likely that many – but not all – of the regulatory functions of the state will be disrupted.

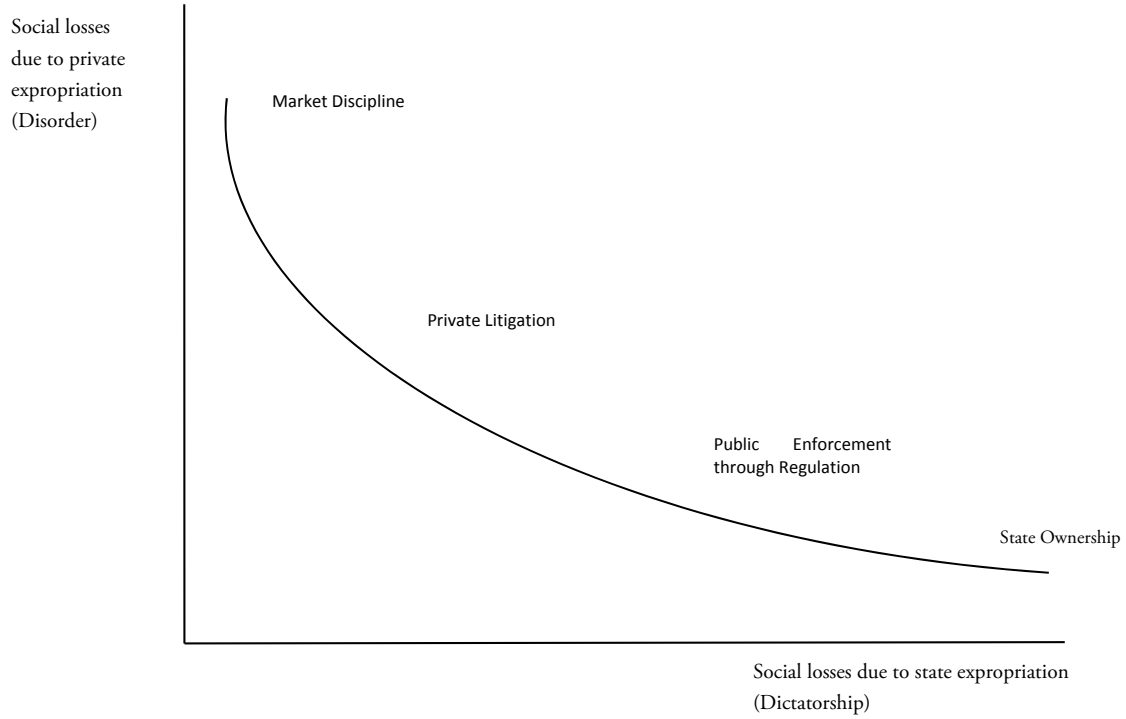
When it comes to government intervention and regulation James Buchanan has argued that society stands between anarchy and leviathan.[14] A regulatory model that incorporates this insight has been proposed by Andrei Shleifer (and co-authors) who developed an institutional regulatory theory that posits regulation as emerging from societal trade-offs between the *costs of private disorder* (anarchy) and the *costs of government dictatorship* (leviathan).[15] Disorder relates to the ability of private individuals to inflict harm on others, while dictatorship relates to the ability of government and its bureaucrats to inflict harm on citizens.

Shleifer then investigates examines four broad governance strategies that 'society' can pursue in order to achieve some objective relative to the trade-offs associated with those strategies. These strategies are; 'market discipline', 'private litigation', 'public enforcement through regulation', and 'state ownership'. The relationship between the trade-off between disorder

[13] Friedrich Hayek, *The Constitution of Liberty: The Definitive Edition* (Taylor & Francis, 2013), 332-34.
[14] James Buchanan, *The Limits of Liberty: Between Anarchy and Leviathan* (Indianapolis: Liberty Fund, 2000).
[15] Andrei Shleifer, *The Failure of Judges and the Rise of Regulators*, Walras-Pareto Lectures (Cambridge, Mass.: MIT Press, 2012)..

costs and dictatorship costs and these four strategies is traced out in figure showing the so-called institutional possibilities frontier.

Figure 1. Institutional Possibilities Frontier



In this framework, market discipline should be considered as the regulatory default. Of course, that is not always possible and at this point the control strategy becomes private litigation. The state begins to play a role as the rules of contract and tort law are administered by courts of law staffed by bureaucrats and judges. Courts of law exist, at this level, to enforce private agreements and to adjudicate disputes between private parties.

Chicago school economists have argued that the combination of market discipline and courts of law should suffice for any regulatory framework. Shleifer, however, has argued that courts cannot always resolve disputes cheaply, predictably, or impartially. This is especially the case when the parties to the dispute have vastly different resources that they can deploy to a legal dispute.

Regulation occurs when the state not only provides a dispute resolution mechanism but also writes the rules that govern economic behaviour and transactions. There is substantial variation in how government can enforce its regulations. It can, for example, allow bureaucrats to engage in a regime of inspection and verification with fines being issued for non-compliance. Alternatively, the state can provide a set of rules that are privately litigated, or publicly litigated. Public litigation can consist of either civil or criminal charges. Similarly the regulatory agency can initiate litigation itself for breeches of the regulations, or act once a complaint has been received. This notion has been extensively debated in the context of financial regulation.

La Porta, Lopez-de-Silanes, and Shleifer investigate the impact of security laws on financial markets across 49 economies including Australia.[16] In particular they investigate how security laws operate to protect investors and whether regulators with public enforcement or rules with private enforcement lead to better outcomes. After exhaustive empirical analysis, they find that legal rules matter, but that regulators do not always matter. So long as rules can be enforced in courts investors do not need to be protected by regulators. Barth, Caprio and Levine (2006) find an analogous result in their investigation of bank regulation and supervision across 107 countries including Australia.[17] They summarise their results as raising a cautionary flag against regulatory practices that involve direct oversight and restrictions on banks. Barth et al. (2006) conclusions are remarkably similar to the La Porta et al. results. Regulations involving prescriptive behaviour and powerful regulators using public enforcement mechanisms are not the better techniques to employ for the purpose of social control.

The important point being that even before the advent of the blockchain that the role of regulators (as opposed to regulation) was being questioned.

Finally, state ownership appears to be an efficient response to those situations where the disorder costs are likely to be very high. Shleifer gives the examples of prisons, police force, and military where this is likely to be the case. The costs of disorder resulting from private ownership here are potentially so large that government needs to maintain control over these institutions. A group of scholars at RMIT University have applied this general model to several very specific instances, including the scope for regulatory reform leading to productivity improvements, environmental protection laws, the regulation of free speech, the institutions of innovation policy and entrepreneurship, prudential bank regulation, tobacco control, and education.[18] Berg and Allen extend the institutional possibility frontier to incorporate subjective perceptions of dictatorship and disorder costs.[19]

---

[16] Rafael La Porta, Florencio Lopez-de-Silane, and Andrei Shleifer, "What Works in Security Laws?," *The Journal of Finance* 61 (2006).

[17] James R. Barth, Gerard Caprio, and Ross Levine, *Rethinking Bank Regulation : Till Angels Govern* (Cambridge England ; New York: Cambridge University Press, 2006).

[18] Sinclair Davidson, "Productivity Enhancing Regulatory Reform," in *Australia Adjusting: Optimising national prosperity* (2013). "Environmental Protest: An Economics of Regulation Approach," *Australian Environment Review* 29, no. 10 (2014). Chris Berg and Sinclair Davidson, "Section 18c, Human Rights, and Media Reform: An Institutional Analysis of the 2011-13 Australian Free Speech Debate," *Agenda: a Journal of Policy Analysis and Reform* 23, no. 1 (2016). Sinclair Davidson and Jason Potts, "Social Costs and the Institutions of Innovation Policy," (2015); "A New Institutional Approach to Innovation Policy," *Australian Economic Review* 49, no. 2 (2016); Chris Berg, "Safety and Soundness: An Economic History of Prudential Bank Regulation in Australia, 1893-2008" (RMIT University, 2016); Sinclair Davidson, "Some (Micro)Economics of Red Tape and Regulation," in *Australia's Red Tape Crisis*, ed. Darcy Allen and Chris Berg (Connor Court Publishing, forthcoming); Darcy WE Allen, "The Subjective Political Economy of Innovation Policy," (2016); Aaron Lane, "Institutions of Public Education," (SSRN2017).

[19] Darcy WE Allen and Chris Berg, "Subjective Political Economy," *New Perspectives on Political Economy* (Forthcoming).

Introducing the impact of blockchain into this regulatory framework requires an analysis of the source of disorder costs. The full definition of disorder is as follows:[20]

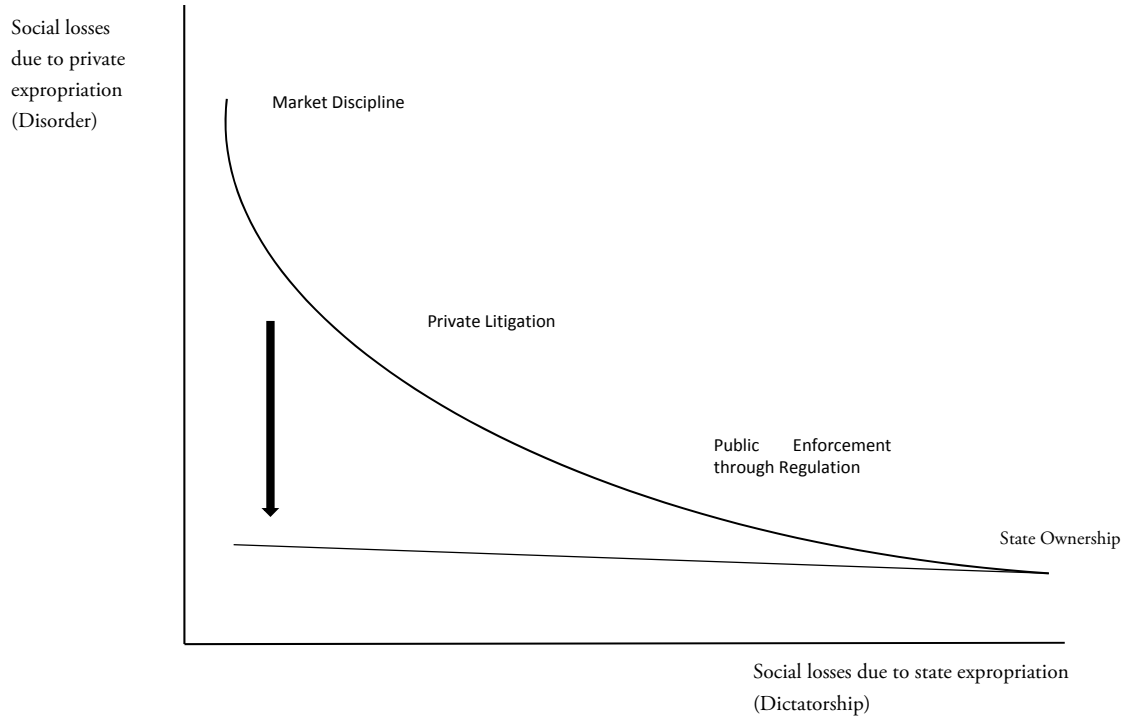
> Disorder refers to the risk to individuals and their property of private expropriation in such forms as banditry, murder, theft, violation of agreements, torts, or monopoly pricing. Disorder is also reflected in the private subversion of public institutions, such as courts, through bribes and threats, which allows private violators to escape penalties.

From that definition there are two sources of disorder: violence and opportunism. Violence is easy to understand and quite legitimately the state works to suppress violence. Opportunism requires some more explanation. Economists generally assume that individuals are self-interested. This seems to be an uncontroversial assumption – but in standard economic theory there are strict limits to self-interest. In standard theory individuals do not cheat, do not lie, and do not steal. It is well-known, however, even by economists that individuals do engage in dishonest practices, and these practices are usually discussed under the headings of adverse selection and moral hazard. Oliver Williamson, the 2009 economics laureate, has suggested the term opportunism to describe a strong-form of self-interest.[21] He argues that individuals engage in "self-interest seeking with guile", specifically "calculated efforts to mislead, distort, disguise, obfuscate, or otherwise confuse". In Williamson's scheme adverse selection and moral hazard are special cases of opportunism. In the presence of opportunism disorder costs are likely to be high as individuals cannot trust their trading partners. Consequently some transactions never occur or do occur at price discounts (the market for lemons) or resources need to be expended to either engage in monitoring or bonding. In such an environment auditing and surveillance by both private actors and the government (via regulatory agencies) becomes efficient. Efficient – but at great cost to society as resources are diverted from otherwise productive use to these activities.

The blockchain is often (incorrectly) described as being a "trustless" technology. Rather than being a trustless technology, the blockchain has design principles that incentivize good behaviour on the part of market participants and ensure that transactions are self-verifying. In other words, opportunism is severely constrained – if not actually eliminated from transactions. To the extent that opportunism is constrained, the disorder costs associated with transacting on the blockchain are much lower than otherwise. This in turn has a profound impact on the shape of the institutional possibilities frontier.

[20] Simeon Djankov et al., "The New Comparative Economics," *Journal of comparative economics* 31, no. 4 (2003).
[21] O.E. Williamson, *The Economic Institutions of Capitalism* (Free Press, 1985).

Figure 2: Institutional Possibilities Frontier with Constrained Opportunism



Social control to ensure good private behaviour is largely unnecessary. The design of the blockchain ensures cooperative behaviour amongst market participants and the scope for private litigation declines. So too the role of regulators is diminished. As those industries whose business models are based on information brokerage and the creation of trust are disrupted, so the regulators of industries will be disrupted too. This argument, however, does not mean that policing activities will necessarily be disrupted – to the extent that the blockchain is deployed for purposes that are illegal the need for criminal enforcement remains unchanged.

5. A CASE STUDY: REFORMING THE AUSTRALIAN PAYMENTS SYSTEM

The Australian financial system developed in the wake of the Victorian gold rush. Payments were made in private bank notes, coins, and by cheque. Even in the earliest periods of the Australian financial system currency and coins were only a small portion of the payments system – most payments were made by cheque. Prior to the establishment of a clearing house in Melbourne in 1867, cheques were settled manually, with bank clerks carting gold around the city between banks.[22] One of the minor consequences of the banking crisis of 1893 was the establishment of more formal cheque clearing houses the year later.

The framework of the Australian payments system was established as part of the takeover of Commonwealth control of the financial sector. Until 1911 the Australian financial system was a free banking system. Banks and bank-like firms were (relatively) unregulated, and Australia had no central bank with regulatory or monetary policy function. In the wake of the 1893 crisis

[22] C. B. Schedvin, *In Reserve : Central Banking in Australia, 1945-75* (St Leonards, NSW: Allen & Unwin, 1992).

there was a concerted political push for a central bank. The government took over note issue in 1910 (imposing a prohibitive tax on private notes). The Commonwealth Bank was established in 1911 as a competitor to the private banks. The Commonwealth Bank Act 1924 handed control of the note issue to the central bank, and simultaneously sought to nationalize exchange settlement by requiring banks to keep an exchange account for interbank settlement at the central bank. The Commonwealth Bank's status as a fully-fledged central bank (both with monetary and prudential regulatory purposes) was established after the 1936 Royal Commission into Money and Banking and the Banking Act 1945 which implemented the Royal Commission's recommendations.[23] In 1959 the Commonwealth Bank was divided between its commercial arm and its central banking functions, now called the Reserve Bank of Australia (RBA).

Banking deregulation and the introduction of foreign banks put significant pressure on the structures of the payments system. Non-bank financial institutions (NBFIs) chafed against the privileges held by banks in the financial sector. In 1993 the establishment of the Australian Payments Clearing Association gave foreign banks and NBFIs direct access to the payments system. Previous to this, the non-banks and foreign banks would need to have their cheques settled by the domestic major banks. Amendments to the *Reserve Bank Act* in 1998 in the wake of the Wallis inquiry gave the RBA a specific mandate for control and regulation of the payments system.

Today, the RBA both directly provides payments system services and regulates private sector payments services.[24] The RBA designates which payments systems are subject to regulation, determines the rules for access to those systems (including controlling which financial institutions and users can access those systems), sets technical and regulatory standards for the systems, and arbitrates disputes. The RBA oversees and sets standards for licensed clearing and settlement facilities. The continued responsibility for the note issue is one of the key direct services provided by the RBA. But RBA also hosts settlement exchange accounts for the final settlement of payments between banks, credit unions and building societies, and operates the Reserve Bank Information and Transfer System (RITS), a real time gross settlement service for high value settlements. The RITS was established in 1998 to reduce settlement risk between Australian banks.

The RBA's longstanding role in the payments system has a number of unappreciated downstream consequences. Historically, the prudential control of banking was justified (albeit not entirely) on the specific importance of the payments system and the reduction of settlement risk between financial institutions.

Banks have long been accorded special privileges within the Australian financial system. Section 51 (xiii) gave the Commonwealth responsibility for the banks (and state banking that extends beyond the limits of the state) and the 1909 *Huddart Parker* decision gave

[23] A history of prudential bank regulation in Australia is provided in Berg, "Safety and Soundness: An Economic History of Prudential Bank Regulation in Australia, 1893-2008."
[24] A useful overview of the Australian payment system and the RBA's role within it is Committee on Payments and Market Infrastructures, "Payment, Clearing and Settlement Systems in Australia," (Bank for International Settlements, 2011).

responsibility for NBFIs such as building societies to the states. This divided regulatory control between the Commonwealth-regulated banks and state-regulated NBFIs that gave each a distinct regulatory character. Entry to the banking sector was strictly controlled, and requests by foreign banks to enter the market knocked back, reducing competitive pressure in the sector. The *quid pro quo* provided was that banking products – particularly interest rates - were strictly regulated.

The landmark 1981 Committee of Inquiry into the Australian Financial System which set the stage for the subsequent reform of the financial system (known colloquially as the 'Campbell committee') identified competitive neutrality was one of the desirable attributes of an efficient financial system. Nevertheless, it maintained that banks had a 'special' place in the financial system, demanding higher levels of prudential regulation than NBFIs. It based this argument on three reasons: small depositors needed a safety haven for their funds, a banking collapse could have systemic consequences, and "Trust is a pre-condition for an efficient payments system: cheque-clearing institutions must be able to deal confidently with one another".[25]

The 1996 Wallis inquiry sought to make the financial system more competitively neutral in part by eliminating the distinctions between financial institutions. Banks, building societies and other NBFIs were compressed into a category 'authorised deposit institution' (ADI) which was categorized by providing deposit services that had a high 'intensity' of promise. A major goal of the Wallis inquiry was to try to remove implication that the government would support depositors in the wake of a banking failure.[26] One of the strategies by which it sought to achieve that was by removing any suggestion that banks were 'special' in a public policy sense. Yet this was only partial. Rules surrounding access to the payments system was still under Wallis pegged to the higher prudential standards that applied to banks. As Rayna Brown and Kevin Davis wrote, much competitive advantage conferred on banks would be lost under the ADI distinction but the perseverance of banks' unique regulatory position in the payments system would "do little to dispel the notion that banks are special".[27]

As this suggests, government regulatory control over the payments system is one of the key factors behind the continued 'specialness' of banks. Why does it matter if banks are special? As one of us has argued, the implied and explicit guarantee of Australian bank deposits is a reflection of the stubborn policy belief that banks are unique institutions in the financial system that require unique policy settings.[28] The development of the explicit deposit guarantee between 2001 and 2008 in Australia was facilitated by this continued belief; a belief that was justified in part because of the role banks had in the payments system.

The consequences of that relationship are significant. Deposit guarantees represent a transfer of wealth from taxpayers to depositors of failed banks. Guarantees reduce the effectiveness of market discipline on banks, distort incentives for bank management and can

[25] Committee of Inquiry into the Australian Financial System, *Final Report* (Canberra: A.G.P.S, 1981), 296.
[26] For a prehistory of the deposit guarantee in Australia, see Chris Berg, "The Curtin-Chifley Origins of the Australian Bank Deposit Guarantee," *Agenda: A Journal of Policy Analysis and Reform* 22, no. 1 (2015).
[27] Rayna Brown and Kevin Davis, "The Wallis Report: Functionality and the Nature of Banking," *Australian Economic Review* 30, no. 3 (1997).
[28] Berg, "Safety and Soundness: An Economic History of Prudential Bank Regulation in Australia, 1893-2008."

make a financial system less stable. Charles W. Calomiris and Stephen H. Haber have documented how political alliances between populist politicians and depositors can make a financial system significantly less stable.[29] As we have shown here, government regulation and control over the payments system is one (mostly unrecognized) mechanism by which that political relationship can manifest itself.

The Payments System Board determines the RBA's payment system policy. The Board is intended to be separate from the RBA's monetary policy approach by its existence as a board distinct from the Reserve Bank Board. However the RBA Governor sits on the top of each board with a mandate resolve inconsistencies. To the extent that decisions about payments system may contradict the RBA's monetary stance – as it is quite possible crypto currency decisions may do – the payments system is subordinate to monetary policy.

Bringing blockchain into the payments system

The monetary system very heavily relies on trust. Money is a social institution of trust that overcomes the double coincidence of wants that makes barter so inefficient. An instrument that can be traded for any other good or service and that has wide social acceptance as such increases the scope for mutually beneficial trade and enriches society. What is important to understanding money is the understanding of the role of trust. The individuals who receives money, however, defined must be confident that they can and will be able to exchange that money for goods and services of equal value to what they have just sold.

Money is very often defined in terms of its functions:

- Medium of exchange – money breaks the double coincidence of wants.
- Unit of account – money can be used to express prices.
- Store of value – money can be stored for future usage.

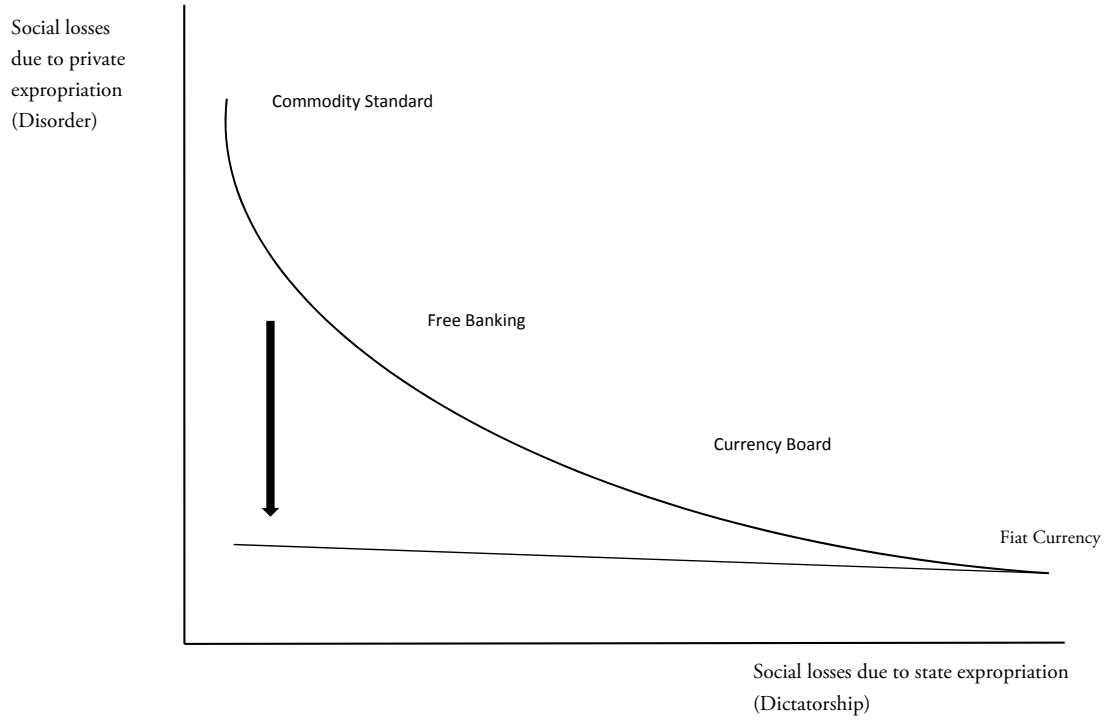
These functions, however, provide little guidance as what it is that can be used as money. Money can be plotted along an institutional possibilities frontier showing the relative disorder and dictatorship costs of the various instruments used as money (see figure 3). Disorder costs in this sense can be summarised as counterfeiting while dictatorship costs can be summarised as inflation. An obvious commodity standard would be the gold standard. In such a monetary system gold is used as money but is subject to large value fluctuations as gold supplies become relatively scare (i.e. no new sources of gold are discovered) or inflations (as new supplies of gold become available due to gold rushes or colonial acquisition). The social cost of using gold is that both individuals and governments have an incentive to debase the gold. In this instance individuals have to trust the circulating medium itself. The government has very little control over money itself.

In a free banking environment each bank is able to issue its own bank notes and individuals have to trust the institution issuing the notes to not inflate the currency. In this environment counterfeiting is the biggest problem facing the monetary system. A currency board exists where government set a fixed exchange rate between the domestic currency and a foreign

[29] Charles W. Calomiris and Stephen H. Haber, *Fragile by Design the Political Origins of Banking Crises and Scarce Credit*, The Princeton Economic History of the Western World (Princeton: Princeton University Press, 2014).

currency and simply exchange currency at that rate. Finally a fiat currency system exists where government declares money to be valuable *and* individuals accept that declaration. The biggest social costs associated with fiat currency is inflation.

Figure 3: The Monetary System on an Institutional Possibilities Frontier



Before we explain how the blockchain and cryptocurrencies can modify the institutional possibilities frontier we first discuss the dictatorship costs associated with the monetary and payments system.

It is important to clearly define what inflation is, and the assign blame for inflation. Hayek defines inflation as 'an excessive increase in the quantity of money which will normally lead to an increase in prices'.[30] Modern readers may have difficulty with this definition; inflation is now taken to mean a general and sustained increase in the level of prices. Prices increases, however, are a symptom of inflation as Milton Friedman makes clear, 'more rapid increase in the quantity of money than in the quantity of goods and services available for purchase will produce inflation, raising prices in terms of that money'.[31]

Hayek did propose, that for practical purposes, the monetary authority could aim to stabilise 'some comprehensive price level'.[32] That does appear to be the standard anti-inflation technique. Hayek, however, indicated that the index should not only contain consumer prices and that the index should be based on international prices and not just local consumer prices. Hayek was emphatic that there can be no such thing as 'cost-push' inflation. Inflation is a

[30] Friedrich Hayek, "Further Considerations on the Same Topic," in *New Studies in Philosophy, Politics, Economics and the History of Ideas* (London: Routledge, 1975), 217.
[31] Milton Friedman and Rose D. Friedman, *Free to Choose: A Personal Statement* (Pelican, 1980), 297.
[32] Hayek, *The Constitution of Liberty: The Definitive Edition*, 464.

monetary phenomenon; 'neither higher wages nor higher prices of oil, or perhaps of imports generally, can drive up the aggregate price of all goods *unless the purchasers are given more money to buy them*' (emphasis original).[33]

Hayek did believe that government was responsible for inflation and that it had become easy to inflate after the 'destruction of the gold standard'. He sympathised with people who regarded a return to that system as being the 'real solution' to inflation. He went as far as to say, 'I still believe that, *so long as the management of money is in the hands of government*, the gold standard with all its imperfections is the only tolerable safe system' (emphasis original).[34] He did not think, however, that a return to the gold standard was a practical proposition. He gave two reasons for this; first the gold standard was an international standard and international coordination would be required to reintroduce it and second, the gold standard relied on the 'mystique of gold' and 'the general belief that to be driven off the gold standard was a major calamity and a national disgrace'.[35] This attitude and belief had ceased to exist.

By the 1970s Hayek had come to support the denationalisation of money – choice in currency. Choice in currency is the idea that individuals should be able to transact in any currency or commodity that they choose.[36]

> There could be no more effective check against the abuse of money by the government than if people were free to refuse any money they distrusted and to prefer money in which they had confidence.

By exposing national currency to competition governments' would have to behave responsibly and maintain the value of their currency. Under such an arrangement, 'those countries trusted to pursue a responsible monetary policy would tend to displace gradually those of a less reliable character'.[37] Hayek did propose that various banks or other institutions issue their own currencies and that these currencies be allowed to trade alongside all other currencies. He also suggested that the notion of legal tender be abandoned, except that if the government were to issue its own currency that it should specify what currency be accepted for tax purposes, the settlement of debt, and the payment of torts. With some minor exceptions financial institutions do not issue their own currencies and the notion of 'legal tender' is still with us.

One critic of Hayek's proposal Douglas Jay wrote:[38]

> But in thinking you can take control of the currency out of the hands of modern elected governments, and put it in the hands of some mysterious wise men meditating in some ivory tower, Professor Hayek is flying in the face of reality. The public simply will not allow

---

[33] *Denationalisation of Money: The Argument Refined*, Hobart Special Papers (London: Institute of Economic Affairs, 1978), 91.
[34] Ibid., 126.
[35] *The Constitution of Liberty: The Definitive Edition*, 462.
[36] "Choice in Currency: A Way to Stop Inflation," in *New Studies in Philosophy, Politics, Economics and the History of Ideas,* (London: Routledge, 1976), 225.
[37] Ibid., 227.
[38] Douglas Jay, "Commentary," in *Choice in Currency: A Way to Stop Inflation* (London: Institute of Economic Affairs, 1976).

> control of money to be put beyond their control any more than control of laws or taxes. The only hope, even if a frail one, is to educate governments to act sensibly.

Jay's critique is quite prescient – it is not clear why trust should be placed in 'in the hands of some mysterious wise men'. On the other hand, that appears to be his only criticism of Hayek's proposal.

The current domestic and international financial monetary system does not immediately resemble what Hayek called for in his proposal – yet the monetary system does have remarkable similarities to Hayek's proposals. Governments' continue to issue their own currency, but most financial institutions issue their own credit cards. Individuals can, in many economies, hold a credit card from any bank in the world. Individuals can own bank accounts anywhere in the world – often denominated in (almost) any currency. Currencies do compete against each other in international markets and in many economies the US dollar has displaced the local currency as the currency of choice. Exchange controls have been lifted in many parts of the world, and the control of money is largely beyond public control. Individuals can chose to contract in any currency, yet in most advanced economies are happy to use the local currency. As Hayek indicated, 'unless the national government all too badly mismanaged the currency it issued, it would probably continue to be used in everyday retail transactions'.

At face value then it appears that bank issued credit cards can approximate Hayek's denationalized money proposal. There are, however, two vulnerabilities to this notion. First credit cards are subject to government regulation and censorship, and second credit cards require banks to resolve asymmetric information problems and as such involve trust within the banking system.

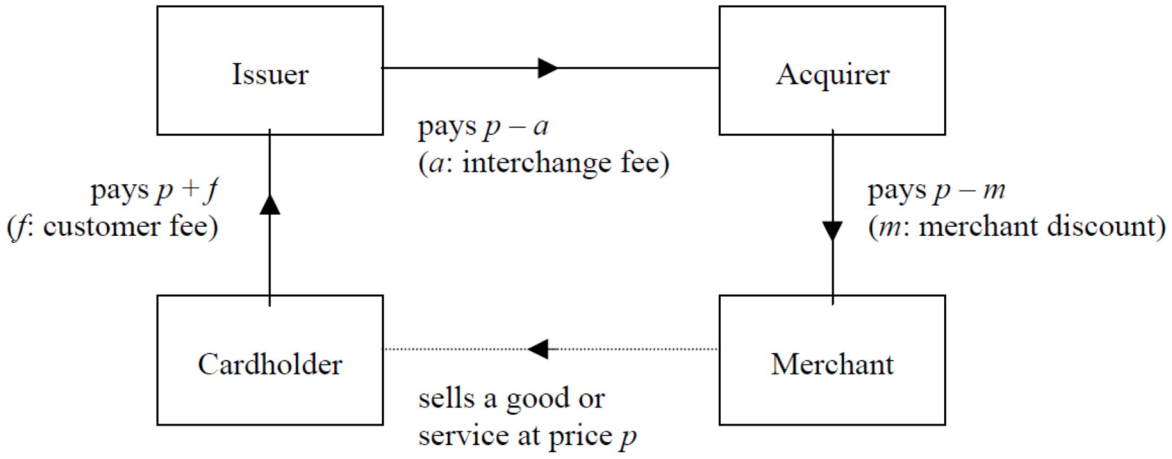
Governments around the world have used their regulatory powers to undermine the use of credit cards by alleging that so-called interchange fees are excessive or anti-competitive. Ronald Coase famously argued that "if an economist finds something – a business practice of one sort or other – that he does not understand, he looks for a monopoly explanation".[39]

Interchange fees and two-sided markets

Interchange fees are fees that banks charge each other as a result of their respective clients entering into a credit card transaction. The regulatory 'concerns' relate to excessive pricing, price fixing, abuse of market power, the creation of barriers to entry, increased consumers prices generally, and excessive use of credit cards relative to alternate payment methods.

[39] Ronald H Coase, "Industrial Organization: A Proposal for Research," in *The Firm, the Market, and the Law* (University of Chicago Press, 2012), 67.

Figure 4: The operation of an interchange fee



Source: Rochet and Tirole[40]

This depiction shows the net cash flows in the various relationships. The consumer (cardholder) buys goods and services from the merchant. The consumer then pays the price (p) and a net fee to his financial institution. The consumer's financial institution then pays the price (p) less the interchange fee (a) to the merchant's financial institution who then pays the merchant the price (p) less their own net fee. This depiction of the issue makes very plain that if both financial institutions are to remain profitable that m > a. The merchant pays the interchange fee. Of course, this is not surprising. The interchange fee exists to rebalance financial relationships within a market arrangement often described as being a two-sided market – sometimes also referred to as a platform economy.

Two-sided markets exist when two distinct groups of economic agents must be simultaneously satisfied to facilitate trade. The traditional media model is a typical and easily understood example. A platform (e.g. a newspaper) must simultaneously meet the needs of both advertisers and subscribers in order to be profitable. In the traditional media business model advertisers pay for the news, not subscribers. In the equivalent credit card model, merchants more often than not pay for the use of credit cards, not credit card users. This is due to consumers requiring more of an inducement to hold and use credit cards than merchants need to accept those cards. To argue that this relationship is somehow inefficient is to argue that consumers have monopoly power over merchants.[41]

In a competitive market for financial services, the interchange fee would be used to reduce the net consumer fee for credit cards.[42] The basic issue, then, is not one of monopoly exploitation, but rather is one of efficient contracting in the shadow of what 2009 economics

[40] Jean-Charles Rochet and Jean Tirole, "An Economic Analysis of the Determination of Interchange Fees in Payment Card Systems," *Review of Network Economics* 2, no. 2 (2003).
[41] For more discussion on this point see Sinclair Davidson and Jason Potts, "Australian Interchange Fee Regulation: A Regulation in Search of Market Failure," (International Alliance for Electronic Payments, 2015).
[42] See the corresponding case of debit cards see Mark Manuszak and Krzysztof Wozniak, "The Impact of Price Controls in Two Sided Markets: Evidence from Us Debit Card Interchange Fee Regulation," in *Working Paper* (Federal Reserve System, 2017).

laureate Oliver Williamson called the Fundamental Transformation that occurs in consequence of transactions that require both parties to make idiosyncratic investments – transforming ex ante competition into an ex post bilateral monopoly – that can subsequently give rise to opportunism.[43]

The credit payments system is not and cannot ever be an interlinked series of anonymous spot markets exchanging financial commodities because the information asymmetries and moral hazards inherent in these exchanges require the parties to the transactions to make idiosyncratic investments (also known as asset specificity) that bind them into a bilateral monopoly – i.e. the fundamental transformation – in which quasi-rents are only secured through mechanisms to inhibit opportunism by aligning incentives to long term relational contracting.

The interchange fee, we argue, has evolved as an efficient governance mechanism to achieve this outcome without requiring horizontal integration – i.e. collapsing the four party payments system into a three-party payments system, and the associated losses of technical and information efficiency and competition that would imply. Banks need to make transaction specific investments in acquiring information about the properties of customers and merchants, the value of which – the quasi-rent – is realised through a long term relationship.

Cryptocurrencies, like Bitcoin for example, are an even closer approximation to Hayek's notion of private money than are credit cards issued by private banks. In the very first instance cryptocurrency is less likely to be subject to government regulation and censorship than are credit cards. Furthermore cryptocurrencies – Bitcoin in particular – were developed for the very purpose of making them non-counterfeit (i.e. Bitcoin cannot be double-spent) and trustless. Depending upon the design of the cryptocurrency they may also be inflation-proof. This is especially the case if we accept the Hayekian argument that inflation is driven by government. Our argument is that cryptocurrency substantially reduces disorder costs within the monetary system; indeed it could also reduce dictatorship costs. Furthermore the blockchain while recording and facilitating transactions acts as an automatic clearing system, with clearance occurring on average every ten minutes, it becomes difficult to imagine what role, if any, the government or any of its agencies would play in the payments system if payments occur on the blockchain.

The important question is whether cryptocurrency can operate as money. In terms of the functions it can perform all three and does. The government has previously expressed some concerns around the use of Bitcoin:[44]

> The Australian Crime Commission's acting chief executive, Paul Jevtovic, says the virtual currency's anonymity makes it highly attractive to criminals and money launderers, though little is yet known about how widespread it is in illicit markets. Bitcoin has become of growing concern to the agency. "The ACC is currently working with partners to explore the

[43] Williamson.

[44] Ilya Gridneff, "More Than Play Money: A Virtual Currency Loved by Geeks Is Fast Becoming the Currency for Crooks," *Sydney Morning Herald*, 1 June 2013.

> Bitcoin market and other digital currencies, to better understand its size and criminal threat," he said.
>
> Meanwhile, Bitcoin is being used legitimately in Australia for everything from buying meat via online butcher Honestbeef to electronics at Gadget Direct, clothes from Patcht or books from Favoryta.

The problem being that those “concerns” are just as true for the use of cash.

> The Australian Crime Commission's acting chief executive, Paul Jevtovic, says [cash’s] anonymity makes it highly attractive to criminals and money launderers, though little is yet known about how widespread it is in illicit markets. [Cash] has become of growing concern to the agency. "The ACC is currently working with partners to explore the [cash] market and other […] currencies, to better understand its size and criminal threat," he said.
>
> Meanwhile, [cash] is being used legitimately in Australia for everything from buying meat via online butcher Honestbeef to electronics at Gadget Direct, clothes from Patcht or books from Favoryta.

An argument can be mounted that Bitcoin is too volatile to serve as a store of value or as a unit of account. Yet most government backed currencies are also somewhat volatile in value on the foreign exchange markets and all suffer from persistent inflation. By contrast, we believe that Bitcoin in particular is too valuable to use for day-to-day transactional purposes. That, however, does not preclude some or other cryptocurrencies being developed for day-to-day usage.

6. FROM PAYMENTS SYSTEMS TO CRYPTOBANKING

The introduction of cryptocurrencies into the payments systems is likely just the beginning of the more widespread adoption of blockchain for economic activity throughout the economy. Smart contracts provide an opportunity for financial institutions to be built directly on blockchain, as a ‘layer’ above the cryptocurrency. Such applications would take advantage of the immutability and cryptographic verifiability of the blockchain to algorithmically manage financial transactions and contracts.

To understand the possibilities blockchain offers the monetary and financial system, we should first consider how blockchains are likely to affect the accounting profession. As a Deloitte report published in 2016 outlined,

> Blockchain technology may represent the next step for accounting: Instead of keeping separate records based on transaction receipts, companies can write their transactions directly into a joint register, creating an interlocking system of enduring accounting records. Since all entries are distributed and cryptographically sealed, falsifying or destroying them to conceal activity is practically impossible. It is similar to the transaction being verified by a notary – only in an electronic way.
>
> The companies would benefit in many ways: Standardisation would allow auditors to verify a large portion of the most important data behind the financial statements automatically. The cost and time necessary to conduct an audit would decline considerably. Auditors

> could spend freed up time on areas they can add more value, e.g. on very complex transactions or on internal control mechanisms.[45]

This automated verification process would have significant consequences for regulatory and legal systems that currently rely on direct or third-party auditing. For example, governments impose prudential controls on banks in order to ensure that they have adequate liquidity and capital buffers in the case of an economic crisis. At the first instance, publicly verifiable and secure blockchains could lower the cost observing banks to ensure they are compliant with prudential requirements.

However, these blockchains also change the regulatory dynamics in more fundamental ways. One of the primary justifications for prudential regulation in banking is that shareholders and depositors lack the information to observe the financial practices and stability of their bank. Shareholders and depositors are therefore unable to impose market discipline on banking practices, freeing management to act recklessly with their funds, and consequently creating a need for external government regulation. As Barth, Caprio and Levine describe the perverse dynamic of a lack of information in banking,

> If depositors and other creditors cannot readily verify the condition of banks, the once some begin withdrawing funds, others, not knowing the condition of the bank, may also withdraw their funds, thereby setting in motion a bank run. And if a run is going on at one bank, unless there is an explanation that is specific to that institution, it can spill over to neighbouring banks.[46]

Barth, Caprio and Levine contrast this with a situation where there is "literally perfect information (all eventualities in the world known with certainty)" where runs would not occur. Banks tend to be less transparent than other firms as their assets are both non-physical and consist of long term liabilities. However, publicly verifiable blockchains go some way to reversing this. Algorithmically audited records of liabilities on a publicly verifiable blockchain has the potential to make financial firms significantly *more* transparent than firms which have their assets tied up in physical capital and real property. This application reduces information asymmetries between depositors and shareholders on the one side and bank management on the other, providing the former with the information necessary to impose market discipline.

An extension of this idea is what we call a cryptobank. As we have written, a cryptobank is

> an autonomous blockchain application that borrows short and lends long, perhaps matching borrowers with lenders directly. A cryptobank structured algorithmically by smart contracts would have the same transparency properties as the bank with a public blockchain ledger but with other features that might completely neglect the need for regulators. For example, a cryptobank could be self-liquidating. At the moment the cryptobank began trading while insolvent, the underlying assets would be automatically disbursed to shareholders and depositors.[47]

[45] Deloitte, "Blockchain Technology: A Game-Changer in Accounting?," (2016).
[46] Barth, Caprio, and Levine.
[47] Berg, Davidson, and Potts.

This is necessarily speculative. But it demonstrates the far reaching consequences of blockchain for the regulatory structures that have governed Australia's financial and monetary system for a century.

7. INDEPENDENT PAYMENTS REGULATION: THE UK MODEL

Australia has an opportunity to be a world leader in the adoption of blockchain technology. Australia's regulatory system is robust and (compared to many other developed countries) relatively adaptable. A number of Australian authorities are already investigating blockchain applications. In this paper we have discussed challenges and opportunities for integrating blockchains into the Australian payment system. Blockchains are in a state of rapid development. The question is what governance arrangement is best placed to oversee the introduction of cryptocurrencies and to bring about the necessary reform.

The RBA itself is an independent statutory authority, meaning that it is formally separated from the lines of delegation and accountability in a Westminster democracy.[48] This structure has a number of benefits and weaknesses. Central banks were the first independent regulators, instituted in this way under the belief that political incentives might harm the neutral application monetary policy.[49]

At the international level, the institutional framework for the implementation of payments system regulation varies considerably. Here we recommend the Australian government consider the institutional example of the United Kingdom, which has a structurally separate payments regulator.

The UK's *Financial Services (Banking Reform) Act 2013* created a new independent regulator for payments, Payment System Regulator (PSR). Until the 2013 legislation, payments regulation was governed largely by the Bank of England and the Financial Services Authority. The UK Treasury was empowered to designate a system as a regulated ('recognised') payment system. In addition the Payments Council existed as a self-regulatory body for firms involved in the payments system. In 2009 the Payments Council announced that cheques were to be phased out in a decade. Controversy surrounding this decision (which was reversed) led to a series of reviews that culminated in the 2013 reforms.

The 2013 reforms established the PSR as an independent body subsidiary to the Financial Conduct Authority. The PSR has its own statutory objectives and PSR board. The chair of the board is also the chair of the Financial Conduct Authority. The PSR is funded by a levy on the regulated payments firms. The industrial representation embodied by the former Payments

[48] For discussions on independent regulatory authorities, see Chris Berg, *Liberty, Equality & Democracy* (Ballarat, Victoria: Connor Court Publishing, 2015); *The Growth of Australia's Regulatory State: Ideology, Accountability and the Mega-Regulators* (Melbourne: Institute of Public Affairs, 2008).

[49] On the other side, independent regulators suffer a democratic legitimacy problem, as their powers derive from a democratic mandate but are not controlled democratically. Rather than relitigating that debate here, in this paper we assume the bipartisan agreement that monetary and payments system regulation ought to be independent is maintained.

Council is included in the Payment Systems Regulator Panel. This body is established by statute as an advisory panel, and takes positions that are independent of the PSR.

The United Kingdom provides a model for payments system regulation in Australia. It provides more legitimacy than the current arrangement: interchange fee regulation in particularly is a form of regulatory taxation, and ought not to be the province of the central bank. Vesting payments regulation in a dedicated regulatory authority would encourage greater regulatory expertise. The creation of the Australian Prudential Regulatory Authority in 1998 was driven by the recognition that the task of central banking and the task of financial regulation are distinct and can create conflicts of interest as single authorities try to balance the needs of one of its mandates against the other.

Finally, and more crucially for the blockchain economy, an independent payments system regulatory brings greater adaptability than the current system. As Potts and MacDonald have argued:

> 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.[50]

The analysis in this paper supports those recommendations. The United Kingdom's system of a dedicated payments regulator – potentially subsidiary to the Australian prudential regulator, APRA – provides a model for the Australian government to manage the introduction of blockchain financial services and cryptocurrencies into the Australian payments system.

8. CONCLUSION

The analysis in this paper suggests that the optimal regulatory control over cryptocurrencies in the payment system – indeed in the financial system in general – is likely to look significantly different than that which prevails in a pre-blockchain world. As we have argued, cryptocurrencies look a lot more like Friedrich Hayek's private banking and private money than the state fiat currency which has dominated the twentieth century financial system. Blockchain powered smart contracts will also reshape the structure of financial institutions. Blockchains are a potentially revolutionary technology that could shape almost every part of the political and economic system. The questions that policymakers will have to face as blockchain applications become more widespread are not just *how* government regulates, but *why* it regulates.

[50] Jason Potts and Trent MacDonald, "Who Should Regulate Bitcoin? Challenges and Opportunities for Blockchain Technology in Australia," (2016).

9. ABOUT THE AUTHORS

Chris Berg is a Postdoctoral Fellow at RMIT University, a Fellow with the RMIT Blockchain Innovation Hub, a Senior Fellow with the Institute of Public Affairs, and an Academic Fellow with the Australian Taxpayers' Alliance. He is the author of five books including *The Libertarian Alternative*. He has been a regular columnist with the *Sunday Age* and ABC's *The Drum*. In addition, his articles have appeared in the *Wall Street Journal, The Australian*, the *Australian Financial Review*, and the *Sydney Morning Herald*, as well as magazines such as *Quadrant, Spectator Australia* and *Overland*. He is a frequent media commentator on television and radio and appears regularly throughout the electronic press. His scholarly contributions have appeared in the *Australian Journal of Political Science*, *Econ Journal Watch, Agenda,* and *Trends in Anaesthesia and Critical Care*. His website is chrisberg.org and his twitter is @chrisberg

Sinclair Davidson is Professor of Institutional Economics in the School of Economics, Finance and Marketing at RMIT University, a Fellow with the RMIT Blockchain Innovation Hub, a Senior Research Fellow at the Institute of Public Affairs, and an Academic Fellow at the Australian Taxpayers' Alliance. He is a member of the Centre for Independent Studies Council of Academic Advisers. Sinclair has published in academic journals such as the *European Journal of Political Economy*, *Journal of Economic Behavior and Organization*, *Economic Affairs*, and *The Cato Journal*. He is a regular contributor to public debate. His opinion pieces have been published in The Age, The Australian, Australian Financial Review, The Conversation, Daily Telegraph, Sydney Morning Herald, and Wall Street Journal Asia. He blogs at Catallaxy Files and Tweets @SincDavidson.

Jason Potts is Professor of Economics at RMIT University, Director of the Blockchain Innovation Hub at RMIT, and Adjunct Fellow at the Institute of Public Affairs in Melbourne. His research work focuses on the economics of innovation and new technologies, economic evolution, institutional economics, and complexity economics. He has written 5 books and published over 80 articles on topics including growth theory, creative industries, economics of cities, innovation commons, and recently on crypto-economics and blockchain. He is editor of the *Journal of Institutional Economics,* Vice President of the International Joseph A Schumpeter Society, and a Board Member of Australian Digital Commerce Association.

10. BIBLIOGRAPHY

Allen, Darcy WE. "The Subjective Political Economy of Innovation Policy." (2016).

Allen, Darcy WE, and Chris Berg. "Subjective Political Economy." *New Perspectives on Political Economy* (Forthcoming).

Barth, James R., Gerard Caprio, and Ross Levine. *Rethinking Bank Regulation : Till Angels Govern*. Cambridge England ; New York: Cambridge University Press, 2006.

Berg, Chris. "The Curtin-Chifley Origins of the Australian Bank Deposit Guarantee." *Agenda: A Journal of Policy Analysis and Reform* 22, no. 1 (2015): 21.

———. *The Growth of Australia's Regulatory State: Ideology, Accountability and the Mega-Regulators*. Melbourne: Institute of Public Affairs, 2008.

———. *Liberty, Equality & Democracy*. Ballarat, Victoria: Connor Court Publishing, 2015.

———. "Medicare Details Available on Dark Web Is Just Tip of Data Breach Iceberg." *Canberra Times*, 17 July 2017.

———. "Safety and Soundness: An Economic History of Prudential Bank Regulation in Australia, 1893-2008." RMIT University, 2016.
———. "What Diplomacy in the Ancient near East Can Tell Us About the Blockchain." *SSRN* (12 August 2017).
Berg, Chris, and Sinclair Davidson. "Section 18c, Human Rights, and Media Reform: An Institutional Analysis of the 2011-13 Australian Free Speech Debate." *Agenda: a Journal of Policy Analysis and Reform* 23, no. 1 (2016): 5.
Berg, Chris, Sinclair Davidson, and Jason Potts. "The Blockchain Economy: A Beginner's Guide to Institutional Cryptoeconomics." *Medium*, 2017.
Bresnahan, Timothy F, and Manuel Trajtenberg. "General Purpose Technologies: 'Engines of Growth'?". *Journal of econometrics* 65, no. 1 (1995): 83-108.
Brown, Rayna, and Kevin Davis. "The Wallis Report: Functionality and the Nature of Banking." *Australian Economic Review* 30, no. 3 (1997): 310-15.
Buchanan, James. *The Limits of Liberty: Between Anarchy and Leviathan*. Indianapolis: Liberty Fund, 2000. 1975.
Calomiris, Charles W., and Stephen H. Haber. *Fragile by Design the Political Origins of Banking Crises and Scarce Credit*. The Princeton Economic History of the Western World. Princeton: Princeton University Press, 2014.
Catalini, Christian, and Joshua S Gans. "Some Simple Economics of the Blockchain." National Bureau of Economic Research, 2016.
Coase, Ronald H. "Industrial Organization: A Proposal for Research." In *The Firm, the Market, and the Law*, 57-74: University of Chicago Press, 2012.
Committee of Inquiry into the Australian Financial System. *Final Report*. Canberra: A.G.P.S, 1981.
Committee on Payments and Market Infrastructures. "Payment, Clearing and Settlement Systems in Australia." Bank for International Settlements, 2011.
Davidson, Sinclair. "Environmental Protest: An Economics of Regulation Approach." *Australian Environment Review* 29, no. 10 (2014): 283-86.
———. "Productivity Enhancing Regulatory Reform." In *Australia Adjusting: Optimising national prosperity*, 2013.
———. "Some (Micro)Economics of Red Tape and Regulation." In *Australia's Red Tape Crisis*, edited by Darcy Allen and Chris Berg: Connor Court Publishing, forthcoming.
Davidson, Sinclair, Primavera de Filippi, and Jason Potts. "Blockchains and the Economic Institutions of Capitalism." *Journal of Institutional Economics* (forthcoming).
Davidson, Sinclair, and Jason Potts. "Australian Interchange Fee Regulation: A Regulation in Search of Market Failure." International Alliance for Electronic Payments, 2015.
———. "A New Institutional Approach to Innovation Policy." *Australian Economic Review* 49, no. 2 (2016): 200-07.
———. "Social Costs and the Institutions of Innovation Policy." (2015).
Deloitte. "Blockchain Technology: A Game-Changer in Accounting?", 2016.
Djankov, Simeon, Edward Glaeser, Rafael La Porta, Florencio Lopez-de-Silanes, and Andrei Shleifer. "The New Comparative Economics." *Journal of comparative economics* 31, no. 4 (2003): 595-619.
Friedman, Milton, and Rose D. Friedman. *Free to Choose: A Personal Statement*. Pelican, 1980.
Gridneff, Ilya. "More Than Play Money: A Virtual Currency Loved by Geeks Is Fast Becoming the Currency for Crooks." *Sydney Morning Herald*, 1 June 2013.
Hayek, Friedrich. "Choice in Currency: A Way to Stop Inflation." In *New Studies in Philosophy, Politics, Economics and the History of Ideas,*. London: Routledge, 1976.
———. *The Constitution of Liberty: The Definitive Edition*. Taylor & Francis, 2013.
———. *Denationalisation of Money: The Argument Refined*. Hobart Special Papers. London: Institute of Economic Affairs, 1978.

———. "Further Considerations on the Same Topic." In *New Studies in Philosophy, Politics, Economics and the History of Ideas*. London: Routledge, 1975.
Jay, Douglas. "Commentary." In *Choice in Currency: A Way to Stop Inflation*, 27-28. London: Institute of Economic Affairs, 1976.
La Porta, Rafael, Florencio Lopez-de-Silane, and Andrei Shleifer. "What Works in Security Laws?". *The Journal of Finance* 61 (2006): 1-32.
Lane, Aaron. "Institutions of Public Education." SSRN, 2017.
MacDonald, Trent J, Darcy WE Allen, and Jason Potts. "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking." In *Banking Beyond Banks and Money*, 279-96: Springer, 2016.
Manuszak, Mark, and Krzysztof Wozniak. "The Impact of Price Controls in Two Sided Markets: Evidence from Us Debit Card Interchange Fee Regulation." In *Working Paper*: Federal Reserve System, 2017.
Mises, Ludwig von. *Liberalism: The Classical Tradition*. Indianapolis: Liberty Fund, 2005. 1927.
Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." www.bitcoin.org, 2008.
Pilkington, Marc. "Blockchain Technology: Principles and Applications." In *Research Handbook on Digital Transformations*, edited by F Olleros and M Zhegu. Cheltenham: Edward Elgar, 2015.
Potts, Jason, and Trent MacDonald. "Who Should Regulate Bitcoin? Challenges and Opportunities for Blockchain Technology in Australia." 2016.
Rochet, Jean-Charles, and Jean Tirole. "An Economic Analysis of the Determination of Interchange Fees in Payment Card Systems." *Review of Network Economics* 2, no. 2 (2003).
Schedvin, C. B. *In Reserve : Central Banking in Australia, 1945-75*. St Leonards, NSW: Allen & Unwin, 1992.
Shleifer, Andrei. *The Failure of Judges and the Rise of Regulators*. Walras-Pareto Lectures. Cambridge, Mass.: MIT Press, 2012.
Smith, Adam. *An Inquiry into the Nature and Causes of the Wealth of Nations*. Chicago: University of Chicago Press, 1976. 1776.
Spencer, Herbert. "The Proper Sphere of Government." In *The Man Versus the State: With Six Essays on Government, Society, and Freedom*. Indianapolis: Liberty Fund, 1982.
Thierer, A.D. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Mercatus Center, George Mason University, 2014.
Williamson, O.E. *The Economic Institutions of Capitalism*. Free Press, 1985.
Yermack, David. "Corporate Governance and Blockchains." *Review of Finance* 21, no. 1 (2017): 7-31.