Blockchains and the economic institutions of capitalism

Sinclair Davidson, Primavera de Filippi, Jason Potts

Journal of Institutional Economics (2017), 00: 0, 1–20
 doi:10.1017/S1744137417000200

Blockchains and the economic institutions of capitalism

Q1

SINCLAIR DAVIDSON
School of Economics, Finance and Marketing, RMIT University, Melbourne, Australia

PRIMAVERA DE FILIPPI
Berkman Klein Center for Internet & Society, Harvard University, Cambridge, MA, USA
National Center of Scientific Research (CNRS), Paris, France

JASON POTTS*
School of Economics, Finance and Marketing, RMIT University, Melbourne, Australia

Abstract. Blockchains are a new digital technology that combines peer-to-peer network computing and cryptography to create an immutable decentralised public ledger. Where the ledger records money, a blockchain is a cryptocurrency, such as Bitcoin; but ledger entries can record any data structure, including property titles, identity and certification, contracts, and so on. We argue that the economics of blockchains extend beyond analysis of a new general purpose technology and its disruptive Schumpeterian consequences to the broader idea that blockchains are an institutional technology. We consider several examples of blockchain-based economic coordination and governance. We claim that blockchains are an instance of institutional evolution.

1. Introduction

Blockchains were invented anonymously and released publicly (under the alias Satoshi Nakamoto: see Nakamoto 2008) as the technology underpinning Bitcoin, a cryptocurrency. Blockchain was the technology that enabled Bitcoin finally to resolve the double-spending problem that hitherto bedevilled all previous attempts to create a digital currency, and thus to emerge as the first native internet-based currency (Evans 2014; Narayan *et al.* 2016).[1] A blockchain is a Q2
way to combine peer-to-peer networks, such as the internet, with cryptography (public key messaging and hash functions) to create an immutable time-stamped public ledger (Swan 2015; Pilkington 2016). The technological novelty of a blockchain is that can create consensus about the true state of a ledger (which might, for instance, record exchanges, contracts, ownership, identity or data)

*Email: jason.potts@rmit.edu.au

1 As a specific technology for digital cryptocurrencies, a blockchain (e.g. the Bitcoin blockchain) is a technical solution to the double-spending problem (the ‘Byzantine General’s problem’) using a decentralised database with network-enforced processes based on a proof-of-work consensus mechanism for updating the database.

without needing to trust any centralised or intermediating party – such as an auditor, a corporation, a market exchange or a government – and is in this sense referred to as '*distributed* ledger technology' or a '*trustless* consensus engine' (Swanson 2014, original emphasis).

Cryptocurrencies have certainly attracted the attention of economists (Böhme *et al.* 2015), particularly those concerned with digital money payments platforms (Mills *et al.* 2016; White 2015). Cryptocurrencies and blockchains together, in the past several years, have notably entered the hype-cycle of media, business and government attention (Tapscott and Tapscott 2016; Walport 2016). We argue that *blockchains* are the true innovation here, and however valuable cryptocurrencies do (or do not) turn out to be, they are simply the first instantiation of the technology. An economic analysis of blockchains should therefore proceed in terms of not only money on the blockchain, but also of all other possible data structures that could be on the blockchain as well. The problem with an economic analysis of blockchains qua cryptocurrencies is that the underlying technology is entirely separate from money and payments, which were just the problem domain in which it first emerged. Blockchains are understood better from an economic perspective as a public database or *ledger technology*, and ledgers are significant because they are a foundational institutional technology of market capitalism. This paper proposes a new way of understanding the economic significance of blockchains from the perspective that they are a new institutional technology.

Analysing the economic effect of blockchains as a new technology focuses attention on the question: What type of technology is this? There have been two broad categories of answer. The first is that blockchain is a general purpose technology, meaning that it is expected to have broad transformative application across many sectors of the economy and contribute to multifactor productivity growth (Bresnahan and Trajtenberg 1995; Lipsey *et al.* 2005).[2] This perspective, whether stated implicitly or explicitly, underpins the case for hype surrounding the prospects of blockchain technology as an 'engine of growth'. A second perspective places a different emphasis on the way in which the arrival of blockchain technology might impact the economy by viewing it through a Coasian, rather than a Schumpeterian, lens. Along this line, Catalini and Gans (2016) portray the 'simple economics of blockchain' as the analysis of a new technology that lowers *transaction costs* through costless verification and without the need for costly intermediation, which they suggest will improve the efficiency and scope of markets, moving them closer to a direct peer-to-peer ideal. This distinction comes down to whether the blockchain is understood to contribute to *production technology* (the general purpose technology view) or to *exchange technology* (the market-enhancing view). Our argument is that the blockchain – or distributed

2 Other recent examples of GPTs are, for instance, 3D printing, smart robots and machine learning, artificial intelligence, virtual reality, nanomaterials and gene editing.

ledger technology – is neither a production nor an exchange technology per se, although this is largely how it has been portrayed, but is better understood from the economic perspective as an *institutional technology*.

Why does this distinction matter? Surely with the flood of start-up companies doing ‘*X*, but on the blockchain’, and as *X* ranges across an ever wider range of applications and sectors, a case can be made that blockchains are indeed a general purpose technology that will improve the productive efficiency of some economic operations. Furthermore, irrespective of the extent of hype (high), or levels of adoption (growing, but still very low), or the actual speed and cost of each transaction (for instance, with the current blocksize constraints and without the use of sidechains, Bitcoin is still orders of magnitude slower and more costly than global payment platforms such as Mastercard/Visa or Paypal), blockchain is plainly a technology that will lower the transaction costs of some exchanges. Those who take a long position on blockchain technology are in effect arguing that it will improve the efficiency of economic systems by disintermediating many current patterns of exchange and production, thus improving economic efficiency. They see this as disruptive, in the Schumpeterian sense, because it disturbs the existing economic rents that can be controlled and captured by large intermediaries providing centralised trust, whether corporate or government.

Our claim that the significance of blockchain as an institutional technology amounts to the idea that blockchain is actually a new way of coordinating economic activity. That is, this technology is actually a *new type of economic institution*. This is different from the production or exchange efficiency perspectives, which are in effect arguing that it offers margins of improvement to existing economic institutions by raising multifactor productivity or lowering transaction costs. Put bluntly, our argument is that until 2009, the economic institutions of capitalism consisted – in the conjoint schemas of Hayek, Williamson, Buchanan, North and Ostrom – of firms, markets, commons, clubs, relational contracts and governments, and that these institutions collectively furnished money, law, property rights, contracts and finance through organisations and networks of production and exchange (Hodgson 2015). But since 2009, there has been an additional mechanism for groups of people to coordinate their economic activity, i.e. through the institutional mechanism of a blockchain.

We do not claim to know whether the technological development and adoption of blockchains will increase market efficiency (cf. Catalini and Gans 2016) or improve productivity in firms and governments (cf. Böhme *et al.* 2015; Walport 2016). It is unclear at this early stage whether any of the current hype surrounding blockchain is justified. Rather, we argue that blockchain ought to be of special interest to institutional economists because it appears to offer a new way of coordinating economic activity owing to the underlying technology possessing many institutional aspects of market capitalism itself: viz. property rights (ledger entry and private keys), exchange mechanisms (public keys and peer-to-peer networks) (native money (crypto-tokens), law (code) and finance (initial coin offerings). The argument of this paper is that blockchains are actually an institutional technology, and should be analysed from this perspective.

Section 2 reviews blockchain technology and how it works. Section 3 distinguishes between technological and institutional innovations and argues that distributed ledger technology is best understood as an institutional innovation (i.e. a governance technology). Section 4 places our argument in the context of the evolving institutions of capitalism.

2. The institutional technology of ledgers and the crypto-technology of blockchains

Blockchain is the technology that underpins Bitcoin, the first successful cryptocurrency. The breakthrough was the creation of a distributed ledger, such that each node in the network has a copy of the ledger, and there is a mechanism – a cryptographically secure and crypto-economically incentivised mechanism – to ensure consensus about the true state of the ledger without the need to trust a centralised node or authority.

A ledger is an ancient accounting technology to record (i.e. maintain consensus about) who (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 (Allen 2011; Nussbaum 1933; Yamey 1949). 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.

The basic qualities a ledger possesses are clarity (i.e. legibility), consistency and consensus as a factual and agreed-upon recording of the basic datum of an economy: of identity, property, contract and value, and usually recording time and sometimes location. A ledger is basically a recording of the state of an economy, and changes in the ledger register changes in the economy in consequence of economic actions and transactions. But the other quality a ledger must possess is that it is trusted. A well-trusted ledger creates a low transaction cost economy, a precondition for economic efficiency and prosperity (Nooteboom 2002; North 1990). Trust is highest when the ledger is centralised and strong, and so ledgers for property titling, contracts, money and suchlike have long cemented government at the centre of modern capitalism. The need for high-quality trusted ledgers is, in this sense, the same expression of the need for high-quality central government institutions (non-corrupt, efficient) and large centralised aggregating organisations. But large central governments and large aggregator corporations come at a cost, both in overhead processes associated with statecraft (Scott 1998), and in distorted incentives (the subject of public choice economics). Manufacturing trust is necessary, but often expensive.

The technology of blockchain combines mathematical cryptography, open-source software, computer networks and incentive mechanisms. A blockchain is a cryptographically secured and crypto-economically incentivised class of distributed ledger – in plain language, a decentralised database. By having a public distributed ledger the blockchain substitutes public verification and consensus for auditing by a trusted third party. Many of the technical specifics need not concern us here, details of which can be found in Buterin (2014b), Nakamoto (2008), Pilkington (2016), Swan (2015), Swanson (2014) and Wood (2014c). But three aspects of how they work are instrumental to our perspective of blockchains as a new institutional technology: first, a blockchain is a database that produces trustless consensus; second, blockchains operate on the internet, and so the possibilities of economic coordination are limited by the extent of the blockchain; and third, blockchains are a database, and anything digital can exist on a blockchain.

Blockchains are consensus engines

A ledger is a way of producing consensus about the facts that are necessary for commerce to function. Moreover, the institutional and organisational outline of a modern economy is a consequence of those ledgers needing to be centralised (i.e. in government, in layers of bureaucracy, in large corporations). A blockchain is a new approach to building and using ledgers, i.e. to producing consensus. The new part is to have figured out a way to use distributed ledgers (as opposed to centralised ledgers) securely and effectively and thus to produce consensus without requiring centralised trust, overturning the old technology of ledgers that needed to be centralised in order to be trusted. A blockchain is a 'trustless' distributed ledger. Cryptographically secured blockchains are said to be 'trustless' because they do not require third-party verification (i.e. trust), but instead use high-powered crypto-economic[3] incentive protocols to verify the authenticity of a transaction in the database (i.e. to reach consensus). This is how blockchains can disintermediate a transaction (a *consequence* of which is lowered transaction costs), resulting in new forms of organisation and governance. Examples are the 'distributed autonomous organisations' (DAOs) and 'initial coin offerings' (ICOs) that disintermediate the allocation of venture capital;[4] 'Steem' disintermediating user-generated content production and rewards (Larimer *et al.* 2016); and 'Backfeed'[5] disintermediating open

3 'Crypto-economic' refers to any decentralised cryptographic protocol that 'uses economic incentives to ensure that it keeps going and doesn't go back in time or incur any other glitch' (Buterin 2015). The proof-of-work Bitcoin mining protocols are crypto-economic in this sense.

4 The DAO (http:/daohub.org/) is a crowd-sourced investment fund running on the Ethereum blockchain. It is an example of a DAO (Decentralised Autonomous Organisation). 'A DAO is effectively a community, with its resources organised according torules agreed in advance and set out in its code' (Allen and Overy 2016: 3).

5 'Backfeed' is a protocol for building decentralised organisations, or distributed governance systems, through a proof-of-value consensus mechanism. It runs on the Ethereum blockchain. See http://backfeed.cc/.

source collaboration. In each case, blockchain provides the 'technology stack' to coordinate the economic actions of an emergent community without the need for a trusted (third-party, centralised, intermediating) coordinator.

By contrast, centralised ledger technologies, as deployed by governments and large corporations, are trust-based technologies because their functioning is conditional upon trust in their legitimacy and accuracy. The problem is that trust, and the high-quality institutions required to support it, can be expensive to manufacture conventionally. Klein (1997) contains several case studies demonstrating how trust is necessary to facilitate trade – yet establishing that trust can be very expensive, often involving large, visible and irreversible investments (De Long 1991; Klein and Leffler 1981). In the case of third-party enforcement via the nation state, this requires a monopoly on coercive powers (Olson 1993), and an implicit promise (a social contract) not to abuse that power. In consequence, enormous rents are locked up behind these centralised monopolies of trust. Trustless technologies are thus an important step in unlocking and releasing that value and in overcoming the hazards involved in manufacturing trust. By removing the need for powerful central third-party validation, verification and enforcement mechanisms, cryptographically secured blockchain technologies are in principle safe transaction environments, even in the presence of powerful or hostile third parties trying to prevent users from participating, and they achieve this with high transparency as well as furnishing scope for exit, when irreconcilable disagreements arise, through a 'fork' in the code.[6]

Blockchains are limited by the extent of the internet

Blockchains are ledgers (or databases) and anything that can be coded into a ledger can be recorded on a blockchain. The most obvious data are numbers recording units of account. But strings of numbers can be used to represent identities, or programs, and in this way ledgers can become units of computation. Blockchain protocols are mechanisms to arrive at consensus about which numbers or programs are the true and agreed-upon ones, and once time-stamped these enter as a block into a continuous chain, linked to all previous blocks (hence block-chain) all the way back to the genesis transaction.

Blockchains are a technology that operates on the internet, i.e. on networks of computers. In the same way the internet was the next generation beyond (unlinked) computers, blockchains are claimed to be the next generation beyond the internet. What blockchains bring to the internet are *public ledger protocols*. What this does, in effect, is to turn the internet into a 'public computer', or a 'world computer' (Wood 2014c). This was not initially obvious in the seminal

6 'Forking' is a term of art in software engineering when a copy of the source code is made to start (i.e. fork) a new line of development. In open source software, forking does not require developer permission. See https://bitcoin.org/en/glossary/hard-fork (accessed 30 April 2017).

version of blockchain, built to solve a specific problem – but by adding a general scripting language with programmable functionality blockchains can become a platform for creating 'smart ledgers' (Swanson 2014).

An example of a smart ledger is *Ethereum* (Buterin 2014b, De Filippi and Mauro 2014). If Bitcoin can be described as a specialised technology, a cryptographically secure transaction-based state machine, then Ethereum attempts to build the generalised technology (a virtual machine) on which all transaction-based state machine concepts may be built. It is a platform for zero-trust computing (Wood 2014c). The generalised Ethereum blockchain technology is the Turing-complete scripting language and protocols for building decentralised applications that run on the Ethereum blockchain using its own native cryptocurrency (Ether). In Ethereum agents can write and execute *smart contracts* (a self-executing digital contract), from which can be created decentralised applications including Distributed Autonomous Organisations (DAOs).[7] Smart contracts and DAOs enable the internet of things (IoT), which must ultimately require a decentralised register because its scale will vastly exceed any possible centralised ledger.

Blockchains enable the basic technology of a public ledger to evolve into a public computer for economic coordination. Vitalik Buterin (2015), co-founder of Ethereum, provides this definition of blockchains:

> A blockchain can upload programs 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.

Blockchains are platforms for building bespoke economic coordination using distributed ledgers augmented with computationally embedded features such as programmable money (cryptocurrencies), programmable contracts (i.e. smart contracts) and organisations made of software (DAOs). These are building blocks of new forms of economic governance. This is the sense in which blockchains are an institutional technology.

Blockchains are digital databases

Third, blockchains are a generalised economic institution in the same way a market is. Just as we can identify a market mechanism without specifying what is actually exchanged in that market, this is also true of a blockchain. Anything configurable or able to be represented in a digital database can be

7 Buterin (2014a), Wood (2014a, 2014b).

on a blockchain. Blockchains are of course a very new technology – viz. the Bitcoin blockchain has been operating continuously since 2009 and the Ethereum blockchain only since 2015 – and so beyond the initial proof of concept by putting money on the blockchain (i.e. cryptocurrencies),[8] much entrepreneurial attention being paid to the technology is focused on testing experimentally what else can be put on the blockchain, and the associated costs and benefits of that action (Allen 2016; De Filippi 2015). The number of blockchain start-up companies and the amount of venture capital invested has grown rapidly recently,[9] ranging across a large domain of applications including: identity, property and asset titles, financial securities, intellectual property, insurance, IoT, certification, health records, smart contracts, prediction markets, gambling, notaries, logistics platforms, provenance, wallets, social networks, and media and open science, among others.

3. What sort of technology is blockchain?

It is said that blockchains are a new general purpose technology (Pilkington 2016), of the same class of technological trajectories as, for instance, electricity, transistors, computers, the internet, mobile phones and so on (Perez 2009). Popular articles on blockchains often represent the technology as the next generation of the internet, or as the 'internet of value' (e.g. Swan 2015; Tapscott and Tapscott 2016). Such tropes are intended to foreshadow blockchains as being similarly large, disruptive and widespread as comparable to computers or the internet. Yet an economic analysis of blockchain technology needs to consider carefully just what sort of technology it really is. If blockchains are a *general purpose technology*, then their significance is in being next in a line of transformative information technologies, each powering a productivity revolution: e.g. transistors, computers, the internet and now blockchains. If so, then what matters is the estimate of the productivity dividend they might bring (i.e. whether it is large or small and how it is distributed). But if blockchains are better understood as a new *institutional technology*, then what we have is the arrival of a new species of economic coordination – *à la* Williamson (1985) and North (1990) – firms, markets, relational contracting and now blockchains. If this is the case, then what matters is what economic activities will shift to this mode of coordination, which is to say that the interesting question is the reorganisation of the institutional boundaries of economic coordination.

We can thus examine the economics of blockchain technology through a Schumpeterian lens of the productivity consequences of adopting and diffusing

8 See https://coinmarketcap.com/ for a listing of prices and trade volumes. As of April 2017, the market cap of all cryptocurrencies was about $USD 23 billion.

9 AngelList (https://angel.co/blockchains) lists over 500 blockchain start-ups, with an average valuation at $USD 4 million, as at March 2017.

a new information and communications technology, or through an institutional lens of efficient governance. A general purpose technology (GPT)-focused analysis will emphasise the gains in total factor productivity (TFP) to existing economic operations, as well as its creative-destructive effect on firms, markets, industries and jobs. But an institutionally focused analysis of blockchains as a new coordination technology focuses on a different aspect, viz. how blockchains compete with firms, markets and economies as institutional alternatives for coordinating the economic actions of groups of people.

Two sorts of technology

Blockchain is a new technology, and the invention, adoption and use of this new technology can be examined using economic theory. But there are two distinct (yet commensurable) approaches to the meaning of technological change: the neoclassical approach, and the institutional or evolutionary approach. In the neoclassical production-function model, technological change is a change in factor productivity. In the institutional/evolutionary approach, technologies also include 'social technologies', or institutions and organisations, as rules for coordinating people, and so institutional change is also a type of technological change (Nelson and Sampat 2001). In the social technology approach, technological change is a change in institutional efficiency.

In the neoclassical model, blockchain technology is factor augmenting. Its adoption drives economic growth by improving efficiencies, or reducing inefficiencies, using a superior technology to achieve a particular task, e.g. as a payments system or asset transfer register (Catalini and Tucker 2016). People adopt the new technology because of these marginal productive efficiency gains. Technological change makes one or more input factors more productive (i.e. it is factor augmenting) and so the aggregate measure of technological change is TFP. TFP is equivalently a measure of economic growth and real income because the rewards of increased factor productivity accrue to the owners of those factors. Technological change in any general purpose technology (say electricity, computers or blockchains) is factor augmenting. The benefit of adopting electricity or computers does not accrue just to the owners of those technologies, but under competition accrues to *all factors* that use those technologies, because their marginal productivity (and therefore marginal revenue product) has been enhanced. Blockchain innovations increase TFP by reducing the production costs associated with any endeavour to produce a particular output. An example is private or permissioned blockchains that reduce the cost of doing a particular thing (such as reconciliation, or international money transfers). Here blockchain technology reduces a production cost by eliminating an intermediate cost or lowering the cost of a process, such as verification (Catalini and Gans 2016). We can model blockchain as a productivity-enhancing technological change by treating it as the latest in a long line of general-purpose technologies. And while the specifics of the size of the aggregate effect and the form of the distributional gains and losses are *ex ante* unknowable, as are the shape of the entrepreneurial opportunities and also forms of consumer surplus, what can be inferred is that the new technology will contribute to economic growth and prosperity because, by making existing factors more productive, it 'economises' on scarce resources.

But there is another way that economising can occur, which is by economising not on *production costs*, but on *transaction costs*. This idea was elucidated by Ronald Coase (1937, 1960) to explain the existence of the firm and the existence of the law. The basic insight of new institutional economics was asking why some transactions occur in firms (hierarchies) rather than in markets? The answer was that because of transaction costs in dealing with uncertainty, asset specificity, and frequency of dealings, some transactions are conducted more efficiently in hierarchies rather than in markets (Williamson 1979, 1985). Transaction costs thus determine the efficiency of different governance institutions. The basic insight that transaction cost economics can bring to the economics of blockchain is to ask the same, but now extended, question: why do (or might) some transactions occur in blockchains, rather than in firms or markets?

Transaction costs are the costs of coordinating economic activities, and reductions in transaction costs do impact TFP measures. The mechanism of their effect, however, is different. Effective institutional innovations reduce the transaction costs of coordinating economic activities. Improvements in institutional orders reduce transaction costs, and drive investment in those economic orders, which eventually manifest as increases in economic activity per input unit, and so as TFP growth. In the neoclassical approach, technological change lowers production costs. In the new institutional approach, technological change lowers transaction costs.

So the question is – which type of technological change is blockchain? Which type of costs – production costs or transaction costs – does it affect most significantly? Now, blockchain is manifestly an information technology – as a software protocol based on cryptography, a blockchain is a new technology for public databases of digital information – but blockchain is also manifestly a GPT. So at first sight it seems to be a productivity-enhancing technology that economises on production costs. Yet when we dig deeper into the nature of blockchain-based economising, it is often a consequence of transaction cost efficiencies.

Blockchains are a technology for economic coordination

With a productivity enhancing innovation, the new technology enables more to be done with less. The new technology should outcompete the old technology on some important margin. If, however, we focus on blockchains as a cryptocurrency and payments system, e.g. Bitcoin, on many margins it seems a vastly inferior technology. With the current state of the technology (with an average blocksize less than 1MB, and without sidechains) it is slower than credit card-based payments platforms such as Visa, and has a lower capacity channel. But new technologies are usually worse on some dimensions, and their value often accrues to properties that were poor or non-existent in the competing technology. With cryptocurrency payments the relevant feature is the deep architectural change in how payments work, now entirely peer-to-peer. This has costs, including transactions being irreversible (although for some that is a powerful benefit). But the benefits relate to what is no longer required, namely corporate or government permissioning, monitoring and regulation of private finance (replaced by a crypto-wallet that can pay anyone, anywhere, who also has such a wallet). As such, the productivity gains come from the organisational efficiency gains, from stripping out layers of activity no longer needed because trusted third parties are not required, or can be achieved more efficiently using native capabilities in the blockchain technology stack, such as multisig protocols.[10]

Distributed ledgers are a technology of decentralisation. Centralisation can be an efficient source of order and control at small scales, but complex self-organising systems tend toward decentralisation as they grow because the coordination costs eventually overwhelm any centralised node, causing fragility. Loss of centralised control is a cost, but the benefit is that decentralised systems are more robust. Distributed systems still require system-wide coordination, however; this is usually achieved through adaptation, for example through the price system in a market (Hayek 1945).[11] Blockchains create distributed systems by eliminating centralisation, which was needed previously for reconciliation or consensus on a ledger with an alternative technology for achieving consensus about economic data. The implication is that by providing an alternative organisational mechanism to reach agreement about economic facts, which are used in turn to coordinate economic activity, this technology offers an alternative way of coordinating economic activity. Distributed ledgers are a technology for economic coordination that is a potential substitute for the economic coordination provided by markets, hierarchies, relational contracting and governments. Blockchains are in this sense an institutional innovation. The relevant margin of economic analysis is therefore not with TFP and growth, but rather with substitute mechanisms of economic coordination and governance. To unpack the relevant margins of governance efficiency that blockchains have over firms, markets, networks, relational contracting and governments, consider the underlying problem of the economics of efficient governance.

A transactions cost explanation of the economic efficiency of blockchains

The comparative economic efficiency of blockchains can be understood as a simple extension of Williamson's (1985) operationalisation of Coase's transactions cost analysis with respect to the comparative efficiency of firms

10 An explanation of multisig protocols is available here: https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do (accessed 30 March 2017).

11 Tokens within the blockchain can be thought of as being an 'inbuilt' price mechanism.

versus markets. Williamson argued that a hierarchical organisation and relational contracting are ways to control *opportunism* in the presence of bounded rationality and asset specificity, by internalising the (transaction) costs of opportunism. Control of opportunism is not the only economic reason that firms exist (Hodgson 2004; Langlois 1995) but it is one force that allocates economic activity across comparative economic institutions. Blockchains can also control opportunism, but they do so by harnessing market mechanisms and internalising them within a closed and guaranteed payments system. Williamson (1979) argued that under common behavioural, technological and organisational conditions, firms minimise the transaction costs of controlling opportunism, and are thus efficient ways to organise economic activity. A similar claim is that blockchain platforms can minimise opportunism by a combination of radical public transparency coupled with cryptographic enforcement and execution through smart contracts and their agents (e.g. DAOs) (Swanson 2014).

To the extent that opportunistic behaviour becomes searchable public information (overcoming bounded rationality), the private costs of opportunism are now higher. And to the extent that detailed contracts can be written and executed indefinitely inthe future, the counter-party risks associated with investment in specialised assets are reduced. The implication is that blockchain-based platforms for coordinating economic activity may compete effectively with hierarchies (which exploit incomplete contracts to overcome opportunism) and relational contracting (which requires trust between parties, and exploits the expectation of repeated exchanges) on some important margins. Where blockchains can mitigate opportunism through crypto-economic incentives and mechanisms at a relatively low transaction cost they will be more efficient (i.e. transaction-cost minimising) institutions for coordinating economic activity compared to organisational hierarchies and relational contracts (which are in turn, *à la* Williamson, more efficient than markets).

A possible counterargument is that while firms are made of *incomplete contracts* (Hart 1989), blockchain-based smart contracts and DAOs are by construction a domain of *complete contracts* (Wright and De Filippi 2015).[12] This sharpens the distinction between blockchains, firms, relational contracts and markets. In the Coasian view, a firm is a 'nexus of contracts', but specifically a nexus of *incomplete contracts* (Hart and Moore 1990: Jensen and Meckling 1976; Williamson 1985). In a world with zero transaction costs, all contracts would be complete and all economic coordination would be through market transactions. Incomplete contracting models (Tirole 1999) usually invoke

12 Abramowicz (2016: 362) observes that 'cryptocurrencies cannot solve the problem of incomplete contracts, and as long as contracts are incomplete, humans will need to resolve ambiguities'. Yet building on Wright and De Filippi's (2015) approach to 'Lex Cryptographica', Abramowicz proposes a model of peer-to-peer law in which cryptocurrency protocols incentivise collective human judgment both to make law and to resolve disputes with incomplete contracts.

transaction costs arising from: (1) uncertainty, or unforeseen contingencies, as information problems; (2) the costs of writing contracts; (3) the costs of enforcing contracts. The implication is that blockchains may not compete head-to-head with firms, but rather may carve out those parts of firms that can be rendered as complete contracts where they lower transaction costs on any of these three margins. For instance, blockchain-enabled smart contract-facilitated transactions should in principle experience fewer efficiency problems due to information asymmetries – adverse selection (prior to a transaction) and moral hazard (following a transaction). Smart contracts could also be effective ways to load significant numbers of low-probability state contingencies into contracts. These could function like open-source libraries able to be inserted into machine-readable contracts, reducing the complexity cost of writing large state-contingent contracts, and so lowering transaction costs. Both *ex ante* contractual discovery and *ex post* contractual renegotiation costs (i.e. bargaining and haggling costs) are an expected consequence of incomplete contracts. Such contracts have dynamic benefits, enabling adaptation, but in the shadow of these expected but uncertain costs all parties will contract less than is optimal. Blockchains potentially enable the known parts of these relationships to be carved out efficiently from the unknown parts, and executed automatically based upon state conditionals, increasing the range to which economic coordination can extend into the future.

In new institutional economic analysis, organisational form is shaped by the need to control opportunism (Williamson 1985: 64–7). The proximate cause of opportunism is the conjoint pay-offs to idiosyncratic investment – i.e. asset specificity, a normal part of all economic production requiring the coordination of joint inputs. But the ultimate cause of opportunism is the intent and ability of agents to exploit trust. Williamson calls this 'self-interest seeking with guile', and emphasises the connection with bounded rationality. With full rationality, complete information and costless transactions, all agents can comprehensively contract with no need for trust. But with bounded rationality (i.e. imperfect information and costly transactions) the economic margin of contracting is trust – i.e. contract up to the point where the marginal cost of supplying trust (accumulating agent-specific experience, monitoring reputation) equals the marginal benefit of that trust (the surplus, compared to the next best institutional alternative). In this view, blockchains are an additional mechanism for controlling opportunism, eliminating the need for trust by using crypto-enforced execution of contracts through consensus and transparency. Opportunism is significantly reduced in DAOs compared to in-the-world Williamsonian firms. As Catalini and Gans (2016) emphasise in their claims that blockchain technology lowers verification costs, the lowered costs of opportunism also extend the domain of the market and shrink the domain of organisations. So, if the Williamson model of firms and markets is correct that economic activity and investment is stymied by threats and engagement of opportunism, blockchains are an institutional innovation. If governance exists for reasons other than opportunism, however, then distributed ledger technologies may well be a source of productivity growth, but not the institutional revolution argued here.

Alchian and Demsetz (1972) suggest another possible avenue whereby a blockchain governance revolution may unfold at the margin of the economic efficiency of organisations *versus* markets. They proposed an alternative transaction costs theory of the firm that emphasised monitoring costs in team production. When production is more efficient with shared inputs than non-shared ones, it may be more efficient to establish sets of agreements that characterise firms as the team use of inputs plus the centralised position of some party in the contractual arrangements of all other inputs, than to govern these transactions using markets. The Alchian and Demsetz model argues for the efficiency of centralised monitoring. What blockchains introduce, however, is a new prospect of *distributed monitoring*, undermining the main argument for the comparative efficiency of the firm in the context of the generalised efficiency of production with shared inputs. In essence the blockchain is not simply a trustless technology, it is a *self-monitoring technology* too. To illustrate this point consider Alchian's (1983) definition of a firm:[13]

> A firm is a (1) coalition of interspecific resources, some of which are owned in common (2), and some of which are compensated according to some criteria other than separably additive outputs and other than by directly measured marginal productivity (3) of saleable products.

For Alchian (1983) asset specificity and quasi-rents are the defining features of the firm. The firm has to own specific assets to prevent *ex post* opportunistic expropriation. This necessitates a non-market-related monitoring and reward system within the firm. The blockchain, however, has the potential to resolve, or at least largely ameliorate, those issues. For example, Bitcoin relies on a proof-of-work algorithm that is analogous to the Alchian and Demsetz (1972) monitoring problem: has task A been performed or not? While this is a valuable function, it is possible to extend the principle.

For example, *Backfeed*,[14] a social protocol that builds upon blockchain-based infrastructure and the smart-contract platform provided by Ethereum, implements an alternative and more generic consensus algorithm called proof-of-value that relies on human evaluation to discover the value of every contribution as perceived according to the distinctive value system of each individual network. *Steem*,[15] a blockchain-based social media organisation, performs a similar function though community-voting using its native cryptocurrency. Individual members of a community or organisation evaluate the contributions

13 This paper is an extension and partial correction to the earlier Alchian and Demsetz (1972) paper.

14 See http://backfeed.cc/

15 See https://steem.io/.

of others, who will be rewarded (according to the value they bring to the community) with economic tokens (transferable) and a reputation score (non-transferable) that indicates the influence they hold within the organisation.[16] The Backfeed protocol that substitutes for monitoring deploys a market-like mechanism (reputation and price) to allow for the collaborative creation and distribution of value in peer networks. The system relies on a specific protocol to enable distributed peer networks to contribute to an organisation. Through the blockchain-based Backfeed protocol they can coordinate themselves indirectly, mutually exploiting their specialised knowledge (*à la* Hayek 1945). A peer-to-peer evaluation system determines the perceived value of each contribution in a decentralised fashion in order to allocate influence and rewards accordingly.

Backfeed is an experimental protocol that is itself built on an experimental platform – Ethereum – and Steem is a proof-of-concept social media platform. They may or may not succeed. They are interesting, however, because they appear to be a new type of economic institution. These blockchain protocols enable a decentralised reputation system to distribute authority among community members dynamically in order to organise individuals organically into a meritocracy with a decentralised topology. The values of every individual that partake in the organisation, weighted according to the influence they each hold within that organisation, constitute – in aggregate – the overall value system of the organisation. As the dynamics of the organisation evolve, with new contributors coming and old contributors leaving, the influence of every individual will change, and so ultimately will the value system of that organisation. The blockchain-based Backfeed protocol has firm-like, market-like and government-like properties, yet is a distinct form of economic governance.

The Williamson model of the firm (opportunism) and the Alchian and Demsetz model of the firm (monitoring) both provide theoretical reasons to expect that blockchain technology may erode the margin of the comparative efficiency of firms. Catalini and Gans (2016) make a similar point, indicating that blockchain shifts the margin of institutional efficiency toward markets. The point we have made in this paper is that all of these theoretical arguments can be sound, but that the Williamson, Alchian and Demsetz, or the Gans and Catalini predictions about the shifted boundaries of firms and markets may not follow because they failed to consider a further option: namely that the dynamic at work is not a reallocation of economic activity across a given set of institutions – markets, hierarchies, relational contracting – but rather the mass adoption of this new technology may lead to an evolution of the economic institutions of capitalism itself.

16 The reputation score in the Backfeed protocol can increase in two ways: (1) by making a contribution that is perceived as valuable by the community; and (2) by making a useful evaluation of someone else's contribution. Hence, individuals are judged not only by their actions (or contributions), but also by their judgment (or evaluations) of the actions of others.

4. Blockchains and institutional economic evolution

Blockchain-based distributed ledger technology adds an additional category to the suite of Williamson's (1985) 'economic institutions of capitalism' – viz. markets, hierarchies and relational contracting – with a *new type of economic order*: a decentralised collaborative organisation (DCO).[17] A DCO is a self-governing organisation with the coordination properties of a market, the governance properties of a commons and the constitutional, legal and monetary properties of a nation state. It is an organisation, but it is not hierarchical. It has the coordination properties of a market through the token systems that coordinate distributed action, but it is not a market because the predominant activity is production, not exchange. And it has the unanimous constitutional properties of a rule-of-law governed nation state, by complicit agreement of all 'citizens' who opt in to such a decentralised collaborative organisation, and the automatic execution of the rules of that DCO through smart contract enforcement (Atzori 2015).[18]

The central argument of this paper has been that much of the extant hype around blockchain as a new digital technology that will drive productivity growth – just as previous generations of ICT have done – actually misrepresents its nature as a technology. We have argued that the interesting thing about blockchain is that it is an institutional innovation. From this perspective, its significance is as an evolutionary development in the institutions of market capitalism (Hodgson 2015). An economy with blockchain technology is institutionally more varied and complex than an economy without it. From an analytic perspective, the relevant question is the margin upon which blockchain institutions compete with alternative modes of economic coordination – markets, hierarchies and relational contracting (Williamson 1979, 1991), as well as clubs, commons and government (North 1990; Ostrom 1990, 2005). We have suggested that transaction costs provide a lens through which to understand the comparative institutional advantage of blockchains and the co-evolutionary dynamics with other institutions of market capitalism.

One path by which the institutions of market capitalism may adapt to blockchain technologies is through the substitution of economic governance from firms, markets, and relational contracts with blockchains. The same economic activity is institutionally reallocated. Currency transactions or settlement of financial trades move 'to the blockchain' for instance. But another path is that blockchains-based coordination may enable new types of economic activity that were previously not able to be governed by firms, markets or governments because the transaction costs were too high to justify the expected benefits.

17 See Ostrom (2005) and Stringham (2015) on the evolution of private or community-level rule-governed economic orders.

18 Reijers et al. (2016) argue that blockchain governance is a special type of social contract mechanism, and thereby suffers the same basic problems that are invariably resolved through political action.

In this case, a more institutionally varied economy (now containing blockchain coordination) can support new types of economic activity. In this instance the economy becomes more institutionally and economically complex. The Ethereum blockchain-based examples of Backfeed and Steem discussed above illustrate this, bringing economic coordination and governance institutions to spaces that currently are either served poorly or served not at all by extant coordination mechanisms of markets, hierarchies and governments. In other words, the impact of blockchain technology may be less to improve the efficiency of existing economic orders (for example dis-intermediating payments and finance) than to expand the scope and depth of economic governance through the evolution of new types of coordinating institutions that are native to blockchains.

The evolutionary character of modern institutional economic analysis is Veblenian and Darwinian (Hodgson 1998; Hodgson and Knudsen 2010) or game theoretic (Schotter 2008). What it is not, generally, is Schumpeterian, for the simple reason that institutions are understood as coordinating rules, rather than as disruptive new technologies. But what is interesting about blockchain technology is that the current mix of hype and scepticism about its status as a new information technology or general purpose technology (GPT) has largely overlooked a further possibility: viz. that it is an *institutional technology*. New technologies of governance are relatively rare but it is important to identify them because unlike most GPTs, where the main dynamic effect is diffuse productivity gains, an institutional technology introduces a new mode of economic coordination and governance. We have argued in this paper that blockchain technology, while just one of a many Schumpeterian technologies driving economic evolution, ought nevertheless to be of particular interest to institutional economists, whether from a transaction costs perspective in seeking to understand the boundaries of firms and markets, or from the perspective of the evolution of economic institutions.

References

Abramowicz, M. (2016) 'Cryptocurrency-based law', *Arizona Law Review*, **58**(2): 359–420.

Alchian, A. (1983) 'Reminiscences of errors', in D. Benjamin (ed.) *Collected Works of Armen A. Alchian, Vol. 2*. Liberty Fund, Indianapolis.

Alchian, A. and H. Demsetz (1972) 'Production, information costs, and economic organisation', *American Economic Review*, **62**(5): 777–95.

Allen, D. (2011) *The Institutional Revolution*. University of Chicago Press, Chicago, IL.

Allen, D. (2016) 'Discovering and developing the blockchain cryptoeconomy', available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2815255 (accessed 30 April 2017).

Allen and Overy (2016) 'Decentralized autonomous organizations', available at http://www.allenovery.com/publications/en-gb/Pages/Decentralized-Autonomous-Organizations.aspx (accessed 30 April 2017).

Atzori, M. (2015) ‘Blockchain technology and decentralized governance: is the state still necessary?’ Available at https://ssrn.com/abstract=2709713 (accessed 30 April 2017).

Böhme, R., N. Christin, B. Edelman and T. Moore (2015) ‘Bitcoin: economics, technology, governance’, *Journal of Economic Perspectives*, **29**(2): 213–38.

Bresnahan, T. and M. Trajtenberg (1995) ‘General purpose technologies: engines of growth?’ *Journal of Econometrics*, **65**(1): 83–108.

Buterin, V. (2014a) ‘DAOs, DACs, DAS and more: an incomplete terminology guide’, available at Ethereum blog, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Buterin, V. (2014b) ‘Ethereum Whitepaper: A next generation smart contract and decentralized application platform’, available at https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/? (accessed 30 April 2017).

Buterin, V. (2015) ‘Visions Part I: The value of blockchain technology’, available at https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/ (accessed 30 April 2017).

Catalini, C. and J. Gans (2016) ‘Some simple economics of the blockchain’, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598 (accessed 30 April 2017).

Catalini, C. and C. Tucker (2016) ‘Seeding the S-curve: The role of early adopters in diffusion’, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2835854 (accessed 30 April 2017).

Coase, R. (1937) ‘The nature of the firm’, *Economica*, **4**(16): 386–405.

Coase, R. (1960) ‘The problem of social cost’, *Journal of Law and Economics*, **3**: 1–44.

De Filippi, P. (2015) ‘Blockchain-based crowd-funding: what impact on artistic production and arts consumption?’ Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725373 (accessed 30 April 2017).

De Filippi, P. and R. Mauro (2014) ‘Ethereum: the decentralised platform that might disrupt today’s institutions’, *Internet Policy Review* **3**(2), available at http://policyreview.info/articles/news/ethereum-decentralised-platform-might-displace-todays-institutions/318 (accessed 30 April 2017).

De Long, J. (1991) ‘Did J. P. Morgan’s men add value? An economist’s perspective on financial capitalism’, in D. Klein (1997), *Reputation*. University of Michigan Press, Ann Arbor, MI.

Evans, D. (2014) ‘Economic aspects of Bitcoin and other decentralised public-ledger currency platforms’, working paper #68, Coase-Sandor Institute for Law and Economics, University of Chicago, IL.

Hart, O. (1989) ‘An economists perspective on the theory of the firm’, *Columbia Law Review*, **89**(7): 1757–74.

Hart, O. and J. Moore, (1990) ‘Property rights and the nature of the firm’, *Journal of Political Economy*, **98**(6): 1119–58.

Hayek, F. A. (1945) ‘The use of knowledge in society’, *American Economic Review*, **35**(4): 519–30.

Hodgson, G. (2004) ‘Opportunism is not the only reason why firms exist: why an explanatory emphasis on opportunism may mislead management strategy’, *Industrial and Corporate Change*, **13**(2): 401–18.

Hodgson, G. (1998) ‘The approach of institutional economics’, *Journal of Economic Literature*, **36**(1): 166–92.

Hodgson, G. (2015) *Conceptualizing Capitalism*. University of Chicago Press, Chicago, IL.

Hodgson, G. and T. Knudsen (2010) *Darwin's Conjecture*. University of Chicago Press, Chicago, IL.

Jensen, M. and W. Meckling (1976) 'Theory of the firm: managerial behavior, agency costs and ownership structure', *Journal of Financial Economics*, **3**(4): 305–60.

Klein, B. and K. Leffler (1981) 'The role of market forces in assuring contractual performance', in D. Klein (1997) *Reputation*. University of Michigan Press, Ann Arbor.

Klein, D. (ed) (1997) *Reputation*. University of Michigan Press, Ann Arbor.

Langlois, R. (1995) 'Capabilities and coherence in firms and markets', in C. Montgomery (ed.) *Resource-based and Evolutionary Theories of the Firm*. Kluwer, Boston, MA, pp. 71–100.

Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee and M. Vandeberg (2016) 'Steem: An incentivised blockchain-based social media platform', available at https://steem.io/SteemWhitePaper.pdf (accessed 30 April 2017).

Lipsey, R., K. Carlaw and C. Bekhar (2005) *Economic Transformations*. Oxford University Press, Oxford.

Mills, D., K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng and M. Baird (2016) 'Distributed ledger technology in payments, clearing, and settlement', Board of Governors of the Federal Reserve System, Washington, available at https://doi.org/10.17016/FEDS.2016.095 (accessed 30 April 2017).

Nakamoto, S. (2008) 'Bitcoin: A peer-to-peer electronic cash system', available at https://bitcoin.org/bitcoin.pdf (accessed 30 April 2017).

Narayanan, A., J. Bonneau, E. Felton, A. Miller and S. Goldfeder (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, Princeton, NJ.

Nelson, R. and B. Sampat (2001) 'Making sense of institutions as a factor shaping economic performance', *Journal of Economic Behavior and Organisation*, **44**(1): 31–54.

Nooteboom, B. (2002) *Trust*. Edward Elgar, Cheltenham.

North, D. (1990) *Institutions, Institutional Change, and Economic Performance*. Cambridge University Press, Cambridge, MA.

Nussbaum, F. (1933) *A History of the Economic Institutions of Modern Europe*. Crofts, New York.

Olson, M. (1993) 'Dictatorship, democracy and development', *American Political Science Review*, **87**(3): 567–76.

Ostrom, E. (1990) *Governing the Commons*. Cambridge University Press, New York.

Ostrom, E. (2005) *Understanding Institutional Diversity*. Princeton University Press, Princeton, NJ.

Perez, C. (2009) 'Technological revolutions and techno-economic paradigms', *Cambridge Journal of Economics*, **34**(1): 185–202.

Pilkington, M. (2016) 'Blockchain technology: Principles and applications', in F. Olleros and M. Zhegu (eds) *Research Handbook on Digital Transformations*. Edward Elgar, Cheltenham.

Reijers, W., F. O'Brolchain and P. Haynes (2016) 'Governance in blockchain technologies and social contract theories', *Ledger*, **1**(1): 134–51.

Schotter, A. (2008) *The Economic Theory of Social Institutions*. Cambridge University Press, Cambridge.

Scott, J. (1998) *Seeing Like a State*. Yale University Press, New Haven, CT.

Stringham, E. (2015) *Private Governance*. Oxford University Press, Oxford.

Swan, M. (2015) *Blockchain*. O'Reilly Media, Sebastopol, CA.
Swanson, T. (2014) *Great Chain of Numbers*. Creative Commons, available at www.ofnumbers.com/the-guide/ (accessed 30 April 2017).
Tapscott, D. and A. Tapscott (2016) *Blockchain Revolution*. Penguin, New York.
Tirole, J. (1999) 'Incomplete contracts: where do we stand?' *Econometrica*, **67**(4): 741–81.
Walport, M. [Chief Scientific Officer] (2016) 'Distributed ledger technology: beyond blockchain', Government Office for Science, London.
White, L. (2015) 'The market for cryptocurrencies', *Cato Journal*, **35**(2): 383–402.
Williamson, O. (1979) 'Transaction cost economics: the governance of contractual relations', *Journal of Law and Economics*, **22**(2): 233–61.
Williamson, O. (1985) *The Economic Institutions of Capitalism*. Free Press, New York.
Williamson, O. (1991) 'Comparative economic organisation: the analysis of discrete structural alternatives', *Administrative Science Quarterly*, **36**(2): 269–96.
Wood, G. (2014a) 'DApps: what Web 3.0 looks like', available at http://gavwood.com/dappsweb3.html, and (accessed 30 April 2017).
Wood, G. (2014b) 'What is Web 3.0?', available at http://gavwood.com/web3lt.html (accessed 30 April 2017).
Wood, G. (2014c) 'Ethereum: a secure decentralized generalized transaction ledger', available at http://gavwood.com/Paper.pdf (accessed 30 April 2017).
Wright, A. and P. de Filippi (2015) 'Decentralized blockchain technology and the rise of lex cryptographia', available at http://ssrn.com/abstract=2580664 (accessed 30 April 2017).
Yamey, B. (1949) 'Scientific bookkeeping and the rise of capitalism', *Economic History Review* **1**(2/3): 99–121.