Economics of Blockchain

Sinclair Davidson, Primavera de Filippi, Jason Potts

Economics of Blockchain

Sinclair Davidson[*], **Primavera De Filippi**[†], **Jason Potts**[‡]

Abstract. Claims blockchain is more than just ICT innovation, but facilitates new types of economic organization and governance. Suggests two approaches to economics of blockchain: innovation-centred and governance-centred. Argues that the governance approach—based in new institutional economics and public choice economics—is most promising, because it models blockchain as a new technology for creating spontaneous organizations, i.e. new types of economies. Illustrates this with a case study of the Ethereum-based infrastructure protocol and platform Backfeed.

Keywords: blockchain, cryptoeconomics, catallaxy, public choice institutional eocnomics

1 Introduction – a most curious technology

A *blockchain* is a way of creating a robust, secure, transparent distributed *ledger*.[1] This revolutionary new technology is also an unusual technology in that while manifestly an information and computation technology (an ICT)—as a software protocol based on cryptography, a blockchain is a new technology for public databases (of digital information)—it is actually better understood as an institutional or social technology for coordinating people.

The purpose of this paper is to elaborate the economics of blockchain, and specifically the implication that what at first appears to be part of the ICT revolution is actually better understood as a revolution (or evolution) in institutions, organization and governance. Which is to say that this is a job for new institutional economics and public choice economics, rather than what would *prima facie* seem the more obvious approach as an economics of money (because blockchain underpins Bitcoin, a cryptocurrency, Böhme *et al* 2015, Hendrickson *et al* 2015, White 2015), or an

[*] School of Economics, Finance & Marketing, RMIT University, Melbourne, Australia
[†] Berkman Centre, Harvard University, Cambridge, USA, & CNRS, Paris, France
[‡] School of Economics, Finance & Marketing, RMIT University, Melbourne, Australia, jason.potts@rmit.edu.au (contact & presenting author)

economics of information, innovation and technological change (because blockchain is a disruptive new technology, Swan 2015, Wiles 2015, Pilkington 2016).

A public choice/new institutional approach to the economics of blockchains can help illuminate how this new technology is likely to affect the economy. We use a case study of an *Ethereum*-based platform (*Ethereum* is a decentralized generalized blockchain, a foundation protocol for a cryptographically secure transaction-based state machine) called *Backfeed* that is a generic token-based reputational-scoring consensus-discovering engine for evaluating contributions to projects on a network (e.g. a knowledge or innovation commons). This *blockchain-Ethereum-Backfeed* complex is, we suggest, best analyzed not as a new technology in an economy of markets and organizations, but, more interestingly, as *a new type of economy*: a 'spontaneous organization', which is a self-governing organization with the coordination properties of a market (Hayek 1945, 1978), the governance properties of a commons (Ostrom 1990), and the constitutional properties of a nation state (Brennan and Buchanan 1985).

Section 2 examines blockchain as a new technology. 2.1 reviews the economics of blockchain as an innovation. 2.2 explains why this is really a technology of decentralization, and 2.3 explores blockchain as cryptoeconomics. Section 3 argues that blockchain is better understood as a governance technology, and therefore new institutional (i.e. transaction cost) economics and public choice economics are appropriate analytic frameworks. Using these, a case study of Backfeed is presented in section 4. Section 5 concludes.

2 Technological approaches to the economics of blockchain

2.1 Economics of innovation: A public decentralized ledger

We can start at the beginning, which incredibly was only eight years ago (Nakamoto 2008). Blockchain is perhaps best known as the technology underpinning Bitcoin (Swan 2015). A blockchain is a public decentralized ledger platform (Evans 2014). As a specific technology for digital currencies, the blockchain is a technical solution to the double-spending problem (what in computer science is called the 'Byzantine General's problem') that hither-to had defeated all endeavors to create a non-centralized peer-to-peer electronic cash system. In Nakamoto's[2] solution, the blockchain solves this problem using a decentralized database (or ledger) with network-enforced processes that are based on a proof-of-work consensus mechanism for updating the database.

However, the worth and significance of blockchain does not depend upon the value and prospect of Bitcoin (Buterin 2015). Bitcoin is an application of blockchain technology in which the ledger entries are bitcoins generated by the Bitcoin protocol. Rather, blockchain is better understood as a new 'general purpose technology' (Bresnahan and Trajtenberg 1995, Lipsey et al 2005) in the form of a highly

transparent, resilient and efficient distributed public ledger (i.e. decentralized database). Such a distributed ledger can be applied to disrupt *any* centralized system that coordinates valuable information (Wright and De Filippi 2015). (Government money is one example of a centralized ledger; government property titling or identity registration is another.) The blockchain technology is *trustless*, meaning that it does not require third party verification (i.e. trust), but instead uses a powerful consensus mechanism with cryptoeconomic incentives to verify authenticity of a transaction in the database, which also makes it safe, even in the presence of powerful or hostile third parties trying to prevent users from participating.

Ledgers are a very old technology, not greatly changed since double entry bookkeeping was developed in the Venetian Republic in the 15th century. By the late 20th century they have been digitized, but until the blockchain, invented in 2008, they always remained centralized. The ledger is a technology of accounting, of keeping track of who owns what, and is instrumental to modern capitalism (Nussbaum 1933, Yamey 1949, Allen 2011). But so too is trust in the ledger, which is most effective when it is centralized and strong, and so centralized ledgers for property titling, contracts, money, etc, are also critical in connecting government to modern capitalism.

Centralized solutions are expensive in the same way that governments are expensive, and have many problems, particularly in relation to problems of trust and its abuse. Yet until very recently no effective decentralized solution has existed. In a recent lead article on blockchain—which they dubbed 'The trust machine'—*The Economist* (2015) explained that:

> "Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them."

The basic economics of blockchain can be thought of the case for why decentralized solutions to ledgers, now technically possible, are likely to become increasingly cost effective compared to centralized solutions as they run down three exponential cost curves: (1) *Moore's law* (cost of processing digital information, i.e. speed, halves every 18 months); (2) *Kryder's Law* (cost of storing digital information, i.e. memory, halves every 12 months); and (3) *Nielsen's Law* (cost of shipping digital information, i.e. bandwidth, halves every 24 months) (Wiles 2015).

One way to model the economics of blockchain, then, is as a new technology (a decentralized ledger) rapidly running down a learning curve (Arrow 1962), or equivalently as a technology cost curve rapidly falling, such that it becomes increasingly competitive against the mature technology of a centralized ledger, driving technological substitution. Because of network effects and switching costs, we would expect the substitution pathway to exhibit non-linearities. The innovation-adoption approach, for instance, underpins the study of cryptocurrencies from the perspective of modern monetary theory that recognizes the competitive efficiencies of

private currencies (Hayek 1978, White 2015). The central question here is whether there exist 'tipping points' to mass adoption.

Entrepreneur-driven technological competition is often met with political response (Stigler 1971, Olson 1982). So we should expect that while centralized ledgers may not always be able to compete on cost, they can still compete through co-option of force, through enacting legislation or regulation to artificially drive up the cost of decentralized technologies—including by rendering them illegal (Hendrickson et al 2015, Lessig 2015). This suggests Chicago-style political economy approach based on technological competition in the context of regulatory responses (Thierer 2014).

Analysis of the shifting relative production costs of competing technology substitutes (centralized versus decentralized ledgers) suggests analysis of a technology adoption process. From this perspective, the blockchain is in the early disruptive phase of a Schumpeterian process of 'creative destruction' that will likely unfold along a logistic adoption-diffusion trajectory (Rogers 1996). This is a model of an evolutionary process of market and industrial dynamics (Dopfer and Potts 2008)—in which blockchains are a new species in the 'technium' (Arthur 2009)—eventually forming a new techno-economic paradigm (Perez 2009). Buterlin (2015) argues that there is no 'killer app' for blockchain, just as there was not for 'open source', but rather a very long tail of marginal use cases among particular groups, all of which adds up to a lot. This diffusion trajectory of the blockchain technology will unfold as sequential applications are discovered and adopted. A Schumpeterian or evolutionary economics of blockchain would seek to study this entrepreneur-led market process of industrial dynamics in the adoption and diffusion of this new technology.

Applications of microeconomic theory to blockchain are still nascent (Pilkington 2015). Zamfir (2015) proposes a new discipline he calls *Cryptoeconomics*, as a view of economics for cryptography, rather than cryptography for economics. He defines cryptoeconomics as:

> "A formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols."

This would place cryptoeconomics as a branch of mechanism design, which is a branch of microeconomics. Buterlin (2015) uses the word 'cryptoeconomic' to refer to any decentralized cryptographic protocol "that uses economic incentives to ensure that it keeps going and doesn't go back in time or incur any other glitch." The proof-of-work bitcoin mining protocols are cryptoeconomic in this sense. At the other extreme, Babbitt and Dietz (2015) propose a definition of a *cryptoeconomy* as an economy unconstrained by geography and political and legal institutions in which blockchains rather than trusted third parties constrain behavior all transactions recorded on a decentralized public ledger.[3] MacDonald (2015b) explains how this may lead to a political-economy rupture called cryptosecession. Similar domain

claims can be made about cryptofinance (Harvey 2015) and cryptolaw (Wright and De Filippi 2015).

2.2 A technology of decentralization, like a market

Blockchains are a technology of decentralization and are an open platform in the same way the internet is an open platform (Benkler 2006). So, another approach to the economics of blockchain is to focus on the economics of decentralized systems and to represent blockchains as a technology for decentralization.

The basic argument for the qualities of open decentralized systems is an old one, going back to Adam Smith and the Scottish Enlightenment, that in essence is an evolutionary argument about *dynamic efficiency*. Hayek elaborated this in his claims about the informational and communication efficiency of the price system (Hayek 1945) and the institutions of a market order (Hayek 1973). The same type of argument—evolution toward complexity (Kauffman 1993, Potts 2000)—appears in *computation* (open architectures, open source and P2P networks are decentralized systems), *political governance* (democracy is a decentralized system, cf. autocracies), *law* (common law systems are decentralized, cf. statute law systems), and *communication* (social media is a decentralized system).

The basic developmental pattern in evolving complex systems is from centralization to decentralization. Systems begin with centralization because this is the most efficient structure to create, establish and enforce rules, i.e. to create knowledge structures. This minimizes duplication and establishes clear hierarchy, and can adjudicate disputes. But those very features mean that centralization has costs that begin to accumulate as these powers become vulnerable to exploitation. In economic systems, this manifests as inflation, corruption, and rent-seeking. Eventually, adaptation and differential selection drives such systems toward decentralization as the costs of centralization rise along the path of exploitation while at the same time the costs of decentralization fall, often due to technological progress (e.g. cryptography and computers, in the case of blockchain). Centralization brings order, but this order can be brittle, and adaptation toward decentralization begins to make the system more robust, flexible, secure and efficient.

As a technology, blockchains have been described in various ways to emphasize different points of functionality. As a consensus mechanism (based on proof-of-work/stake) blockchains are a truth-discovery or verification engine. This makes them valuable as a ledger (database) to securely record value transfer. They commoditize trust through public protocols. But the most general service blockchains perform is that they decentralize. We argue that the economics of blockchains is best approached from this perspective, because it lines them up in context of organizations and markets. Organizations are centralized; markets are decentralized. Markets of course are the other open platform technology that performs this general service of decentralization. Markets are also rule systems (Gode and Sunder 1997, Mirowski

2001, Mirowski and Somefun 1998) that are both designed systems (e.g. auctions) and evolved spontaneous orders (Potts 2001).

A blockchain is a new technology, a product of cryptography, invented as a solution to a problem in the design of digital money. This would seem to place it well within the ambit of the economics of information and new technology, or the economics of money. But it has quickly escaped that box, now appearing as something far more general, namely a technology for decentralization. This renders it a new competitor to the central objects that economics studies, namely organizations and markets. When coupled with token systems, blockchains seem to describe institutional orders that we might reasonably call an economy, or following Hayek (1960) a catallaxy.

2.3 A magic computer for the world

As a specific technology, blockchains solve the double-spending problem in digital money. As a general technology, blockchains facilitate decentralization. A more concrete interpretation, furnished by Vitalik Buterin and Gavin Wood from *Ethereum*, is that blockchains are converging on being a 'world computer', as a global singleton (Wood 2015). Without reference to any mention of ledgers, cryptocurrency, hash rates or transactions, Buterlin (2015) offers a startling definition of blockchains:

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

If you want to know what a 'magic computer' is, then the internet is also a magic computer. The notion of a 'world computer' speaks to the idea that any application that runs on such a platform will be global in reach (without national or geopolitical boundaries) and extend without bound into the future.

This definition lays bare the notion that blockchains are a technology for 'building economic and social institutions'. They are a technology for creating and executing the types of rule-systems (i.e. smart contracts, DAOs) that enable bespoke socio-economic coordination. Economists normally think of economic coordination as resulting from a combination of organizations and institutions: e.g. the organization of the firm, the organization of a club (Buchanan 1965), the institutions of a commons (Ostrom 1990), the institutions of the market, the institutions of law, the institutions of money, the institutions of government. All of these organizations and institutions are at base rule-systems (North 1990; Hodgson 2006, 2015; Dopfer and Potts 2008).

A blockchain is in this sense a new species of rule-system for economic coordination: so, alongside firms, markets, clubs, commons, and governments we now also have blockchains.

A leading example of this endeavor to turn blockchains into magic world computers is *Ethereum* (Buterin 2013).[4] If you think of Bitcoin as a specialized technology, a cryptographically secure transaction-based state machine, then you can think of Ethereum as a project that attempts to build the *generalized technology* (a virtual machine) on which all transaction-based state machine concepts may be built. It is a platform for zero-trust computing. Wood (2014b) explains that

> "Ethereum aims to be a superior foundational protocol, and allow other decentralized applications to build on top of it instead of Bitcoin, giving them more tools to work with and allowing them to gain the full benefits of Ethereum's scalability and efficiency. … [It aims to] provide a system such that users can be guaranteed that no matter with which other individuals, systems or organizations they interact, they can do so with absolute confidence in possible outcomes and in how those outcomes might come about."

The generalized technology is the Turing-complete scripting language and protocols for building decentralized applications, which runs on the Ethereum blockchain (which contains a cryptocurrency called *ether*). In Ethereum agents can write and execute *smart contracts* (a self-executing digital contract), from which can be created decentralized applications including *Distributed Autonomous Organizations* (DAOs). Smart contracts and DAOs enable the internet of things (IoT), which ultimately must require a decentralized register because its scale will vastly exceed any possible centralized ledger. In section 4 below, we will meet *Backfeed*, an Ethereum-based protocol for large-scale decentralized collaboration, including *Distributed Collaborative Organizations* (DCOs).

What the 'magic world computer' perspective and Ethereum make clear is that the nature of blockchain technology is different to the standard way that economists model new technologies, namely as a shift in the aggregate production function, that translates into multifactor productivity growth. Blockchains may well have this effect, and can be studied with neoclassical and evolutionary economics. But the far more transformational aspect of this technology is that they give rise to new organizational and institutional forms of economic governance. And this requires a different analytic approach that draws upon wholly distinct domains of economic theory – namely new institutional and public choice economics.

3 Governance approaches to the economics of blockchain

3.1 The transactions cost approach to blockchain

Blockchain is a new institutional technology that makes possible new types of contracts and organizations. Appropriately enough, this suggests that the correct analytic framework is the new institutional economics (NIE), also known as Transaction Cost Economics (TCE). NIE originates in the work of Coase (1937, 1960), who explained why firms exist by positing the idea of *transactions costs* of using the market. The basic unit of analysis in TCE is the transaction (in neoclassical economics, the basic unit of analysis is the choice over scarce resources). Organizations and markets are thus alternative economic institutions for economic coordination—i.e. for organizing transactions—and therefore the efficient mix of institutions in an economy will be shaped by agents seeking to economize on transactions costs. Economizing on production costs leads to an efficient allocation of resources and economizing on transactions costs leads to an efficient institutional structure of economic organization and governance. These insights also established the modern approach to law and economics (examining the economic efficiency of law), and the theory of the organization (a firm is a nexus of contracts).

Williamson (1975, 1985) operationalized Coase's work by formulating the economics of organization through the lens of contract rather than choice. In Williamson (1973, 1975, 1985) the governance problem begins with *uncertainty*, as bounded rationality, giving rise to contractual incompleteness. And because of *asset specificity* (any investment where your payoff depends on the investment of others) there is scope for *opportunism* (i.e. reneging on a contract, modeled in game-theoretic terms). The value of individual investments—the quasi-rents—depends upon the continuity of the group relationship: these are transaction specific investments (Williamson 1979). This creates *ex post* hazards of opportunism that can be met with efficient governance structures.[5] Markets are often efficient governance institutions for spot contracts (a pure exchange economy), but where economic activity requires coordinated investment through time (asset specificity), or an ongoing relation between parties (frequency), or involves uncontractable dealings (uncertainty), alternative governance institutions, including hierarchies and relational contracting, can be efficient ways to deal with the hazards of opportunism.

The basic insight TCE brought was to ask why do some transactions occur in firms (hierarchies) rather than in markets? The answer was that because of transactions costs in dealing with uncertainty, asset specificity (and associated opportunism) and frequency of dealings, some transactions are more efficiently conducted in hierarchies rather than markets. Transactions costs thus determine the efficiency of different governance institutions. The basic insight that TCE can bring to blockchain is to ask the same, but now extended, question: why do (might) some transactions occur in blockchains, rather than in firms or markets?

The first thing we note is that in the Williamson (1985) scheme the problem of *efficient governance* arises when we combine bounded rationality with asset specificity and opportunism. A hierarchical organization is a method for controlling opportunism. It is protection against opportunism that gives rise to the transaction cost

efficiency of hierarchies and relational contracting over markets. But the valuable prospect of blockchain (as smart contracts and DAOs) is precisely to eliminate opportunism by cryptoeconomic mechanisms by enabling a spot market exchange to carry forward indefinitely a pure promise.

Now on the face of it, this is a revolutionary implication because it undermines the strong case for the economic efficiency of hierarchies (which exploits incomplete contracts) and relational contracting (which requires trust between parties) over markets. If blockchains can eliminate opportunism, then they will outcompete traditional organizational hierarchies and relational contracts. (How do blockchains eliminate opportunism? In essence, by radical public transparency coupled with crypto-consensus mechanisms, executed automatically with smart contracts.) But the obvious problem is that blockchains only work on *complete contracts*, whereas most in-the-world firms (*cf*. DAOs) are largely (entirely?) made of *incomplete contracts* (Hart 1989).

Blockchains refer to a particular class of economic system that Coase (1939) taught us to see through the lens of contracts: namely a blockchain is an economic world of *complete contracts*. This then enables us to understand the relation between blockchains, firms and markets, because in the nexus of contracts view firms exist as a nexus of contracts, but specifically as a nexus of *incomplete contracts* (Jensen and Meckling 1976, Williamson 1985, Hart and Moore 1990).

Contractual incompleteness is the origin of the study of economic organization and governance because in a world with zero transactions costs, all contracts would be complete and all economic transactions would be market transactions. Incomplete contracting models (Tirole 1999) usually invoke transactions costs arising from: (1) uncertainty, or unforeseen contingencies; (2) costs of writing contracts; (3) costs of enforcing contracts. Uncertainty refers to information problems. Blockchain enabled smart contract facilitated transactions should experience less of the efficiency problems of information asymmetries – adverse selection (*ex ante* to a transaction) and moral hazard (*ex post* to a transaction). We would therefore not expect to observe the various efficiency mechanisms designed to overcome these problems such as *costly signaling* (Spence 1973), or *screening* (Akerlof 1970). But smart contracts could be effective ways to load significant numbers of low probability state-contingencies into contracts. To the extent that these could function like open source libraries that could be inserted into machine-readable contracts, the complexity cost of writing contracts could scale linearly, and so the blockchain would lower transaction costs. However, at the same time, bargaining and haggling costs, both *ex ante* discovery and *ex post* renegotiation are likely to be unaffected by a shift to blockchain. Costs of enforcing contracts will depend upon the extent to which human discretion remains part of at least one side of the transaction.

Williamson (1985: 64-7) argues that organizational form is largely shaped by the need to control *opportunism*. Opportunism has a proximate and an ultimate cause. The proximate cause is because of the conjoint pay-offs to idiosyncratic investment

(asset specificity), a normal part of all economic production that requires coordination of joint inputs. But the ultimate cause of opportunism arises because of 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, then all agents can engage in comprehensive contracting and so there is no need for trust. But if information is imperfect, if transactions are not costless (i.e. conditions of bounded rationality) then trust operates at the economic margin of contracting.

In this view, blockchains are a mechanism to control opportunism by eliminating the need for trust by using crypto-enforced execution of agreed contracts through consensus and transparency. Which is to say that there can be no opportunism with distributed autonomous organizations. This extends the domain of the market and shrinks the domain of organizations. So, if the Williamson model of firms and markets is correct, and effective teamwork and cooperative activity and investment is indeed stymied by both threats and engagement of opportunism, the blockchain will indeed be a major revolution. If governance exists for reasons other than opportunism, however, then blockchain is less significant at the firm-market margin.

Another hypothesis about the economic efficiency of organizations versus markets is due to Alchian and Demsetz (1972) who emphasize the role of 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 characterize firms as the team use of inputs plus the centralized position of some party in the contractual arrangements of all other inputs, than to govern these transactions using markets. While not essentially spelled out, the Alchian and Demsetz model can be characterized as the argument for the efficiency of centralized monitoring. However, what blockchains introduce is a new prospect of distributed or *decentralized monitoring*. (To the extent that this monitoring is not tacit.) In this instance, blockchains undermine the main argument for the comparative efficiency of the firm (in the context of the generalized efficiency of production with shared inputs). As such, if either the Williamson model (opportunism) or the Alchian and Demsetz models (monitoring) of the firm are correct, we can expect that blockchains will erode at the margin of the comparative efficiency of firms.

As a new technology, there is a great deal of interest in the way in which existing firms and industries will adopt and use blockchains (including consortium and private blockchains, where restricted access protocols are used instead of trustless cryptoeconomic incentives, i.e. proof of work, proof of stake). But the question we have sought to focus on here, through the lens of transactions cost economics, is not how firms and markets will adopt and use blockchains, but rather how blockchains will compete with firms and markets. In other words, we have systematically adopted the Coase/Williamson perspective in which firms, markets, relational contracts and now also blockchains are alternative governance institutions whose relative efficiency is determined by micro-institutional transaction cost considerations. Which is also to

say that the basic analytic unit of blockchain economics is the transaction (i.e. the executable contract). This is the fullest expression of blockchains not as a new informational and communications technology, but as a new institutional technology.

3.2 Public choice economics of blockchain

A blockchain is a catallaxy

This transaction cost/new institutional economics perspective on blockchain in terms of efficient governance was a necessary step toward a coherent economics of blockchains, which can be seen through the lens of public choice economics. To get to public choice economics of blockchains we have to go through the NIE of blockchains.

It might at first seem strange to nominate public choice economics—nominally the economics of politics, government and collective action—as the natural foundation for the economics of blockchain (rather than say innovation economics, or economics of information or money). But once we see blockchains as alternative governance institutions, alongside firms, markets and relational contracting (in the Williamson schema), it is a short step from there to see that by adding a few more operational features: namely constitutions (Hayek 1960, Buchanan 1990), collective decision making rules and procedures (Buchanan and Tullock 1962, Olson 1965, Ostrom 1990, Ostrom *et al* 1992), and private money (Hayek (1978), then we can perceive blockchains as a technology for making economies.

Blockchains in this sense compete with organizations, but they are not organizations. Rather, they are a type of 'spontaneous organization'. Blockchains have market-like properties, but they are not markets—they facilitate transactions, not (just) exchange. They coordinate a distributed group of people, making them actually closer to being an economy. Hayek, following Ludwig Mises, was a pioneer of the study of decentralized economies and distributed information processing (Hayek 1945). Hayek (1968/2002: 14) defined an *economy*[6] as 'an organization or an arrangement in which someone conspicuously uses means in the service of a uniform hierarchy of ends.' Hayek's point was to distinguish the concept of an economy from the spontaneous order brought by the market—for which he preferred the term *catallaxy*. For Hayek (1982: 109) "a catallaxy is a special kind of spontaneous order produced by the market by people acting within the rules of the law of property, tort and contract." All members of an economy must serve the uniform hierarchy of objectives in all their actions, which he contrasted this with

> "the two advantages of a spontaneous order or catallaxy: it can use the knowledge of all participants, and the objectives it serves are the particular objectives of all its participants in all their diversity and polarity."

From the Hayekian perspective then, blockchains are actually catallaxies, not economies, for they serve not one particular end, "but contribute to the realization of a

number of individual objectives which no one knows in their totality" (Hayek 2002). The order of a catallaxy is one in which

> "the expectations of particular transactions with other persons, upon which the plans of all the economy's participants are based, are to a considerable extent realized. The mutual adjustment of individual plans is brought about by a process of negative feedback."

A catallaxy is characterized by a multitude of agents living within an 'extended order' (Hayek 1988). Agents are (1) social, and governed by social rules, (2) they have specialised/distributed knowledge, (3) they form their own plans, and (4) these are mutually coordinated through the market/price system. Now when Hayek wrote those words, and particularly in reference to point (4), blockchains did not exist. But it can readily be seen that blockchains are 'orders of economies' in the same way a market order is a catallaxy of mutually adjusting individual plans (economies). The price system in Hayek's conception operates at the macro level (i.e. a nation), but a further surprising property of blockchains is that they provide a mechanism to radically reduce the size and scale of effective catallaxies (or, perhaps equivalently, to significantly increase the viable scale of 'spontaneous organizations'). Wealth is a consequence of the increasing flow of knowledge, and coordination of knowledge, that a catallaxy enables, so any new technology that expands the effectiveness of catallaxies is a wealth or value creating mechanism. (We will see this perspective clearly expressed in the application protocol *Backfeed* in the next section.)

This economy/catallaxy perspective finally enables a foundation for the public choice economics of blockchains.

Constitutional choice – from catallaxy to constellaxy

Buchanan (1990: 4) defines Constitutional economics as the study of choice among constraints (*cf*. choice over scarcity) in which cooperative economic agents seek to 'live by the rules that they can also choose'. Agents make these choices

> "as part of an exchange in which the restrictions on their own actions are sacrificed in return for the benefits that are anticipated from the reciprocally extended restrictions on the acts of others whom they interact along the boundaries of private spaces and within the confines of acknowledged public spaces."

In this sense, agents make constitutional choice exchange when they mutually agree to conduct transactions on a blockchain—i.e. to choose a reciprocally binding constraint—that implies mutually accepting the contractual execution protocols. This is mutual choice of a legal jurisdiction (MacDonald 2015a).

A blockchain embodies constitutional choice by the presumption of *unanimity* in adopting or using one (more so that implied consent upon citizenship). A blockchain is thus a constitutional community. A further aspect of this is the process

of discovery of effective constitutional constraints. We would expect this to play out as an entrepreneurial discovery process (Hayek 1968/2002) of blockchain conjectures subject to the market test of subsequent adoption (Allen and MacDonald 2016).

Blockchain as Commons 3.0

Lin and Vincent Ostrom explored the domain of polycentric governance (Ostrom, Tiebout and Warren 1961, Ostrom and Ostrom 1977) and the governance of common pool resources (Ostrom 1990) to explain phenomena that do not fit into the dichotomous world of 'the market' and 'the state' (Ostrom 1986). A key finding from this 'Commons 1.0' work was the existence of effective real-world institutional solutions to social dilemmas (Ostrom 2010), something previously thought impossible (Hardin 1968). Ostrom's work showed that under certain conditions—approximated by small, trustful, communicative groups engaged in repeated interactions—commons were efficient institutional solutions, often superior to market or government institutions. Using both meta-analysis of case studies and laboratory experiments, Ostrom identified the particular 'design rules' of that characterised successful commons governance (Wilson, Ostrom and Cox 2013).

Commons 1.0 covered the economic universe of natural resource commons, e.g. forests, fisheries and irrigation systems (Ostrom 1990). Commons 2.0 has developed over the past two decades by extending analysis to information and knowledge commons, particularly digital commons, e.g. open source software, peer production, open science, open innovation (Benkler 2006, Ostrom and Hess 2007, Madison et al 2010, Frishmann et al 2014, Allen and Potts 2015). Commons 1.0 showed how effective institutions of private governance could create *small-scale* cooperation with cheap talk and monitoring. Commons 2.0 showed how publically observable reputational mechanisms could also overcome the free-rider problem (the social dilemma) at larger scale to generate cooperation in the production and maintenance of quasi-public goods.

Blockchain is Commons 3.0 in that it provides a technical solution (cyrptographic consensus) to the problem of cooperation in joint or group production at scale while still maintaining the benefits of commons-type (i.e. polycentric) institutional governance. A blockchain is a *trustless commons* in which effective rules are embedded in constitutional smart contracts that are cryptographically secure and crypto-economically implemented. The working hypothesis is that the structure of these rules is likely to be similar to the eight 'design rules' identified by Ostrom (1990) (Cox et al 2010).

Rent-seeking and competitive federalism

Centralization requires trust, which can be exploited to create rents when this trust is manufactured politically. This leads to rent-seeking (Tullock 1967), which we can diagnose as an endemic dysfunction of centralised systems arising from the

dissipation of resources in pursuit of these rents. Decentralization is therefore a cure when this trust can be manufactured cryptographically rather than politically.

The political economy of blockchain is thus a kind of private order competitive federalism (Tiebout 1956)—free entry to one or multiple blockchains is equivalent to 'voting with ones feet'—in which its efficiency advantage comes from the elimination of rent seeking, which itself derives from the elimination of a centralised monopoly control over the constitutional rules of the game. MacDonald (2015b) calls this cryptosecession. However, governments, i.e. politicians and bureaucrats, themselves have rents to protect in the continuity of a monopoly over governance, and thus competitive threats from crypto-governance can be expected to be resisted in proportion to the rents at risk (Lessig 2015, Hendrickson et al 2015).

Private governance & anarchy on the blockchain

A blockchain-based economic order can fully automate and execute smart contracts through DAOs, but the problem of contractual enforcement remains, particularly when these voluntary contracts may not be sanctioned by centralised government, and so are not necessarily even conducted in the shadow of the law. (Note that this quality of not being observable by government may be the source of the efficiency gain, where the private agents are seeking to avoid government predation in relation to taxes, regulations or other constraints.) This is analogous to situations of spontaneous private ordering rules emerging under conditions of anarchy or an underground economy (Leeson 2007, 2008, 2014; Skarbek 2011; Stringham 2015).

Yet public choice analysis has furnished is ample reason (both theoretical and empirical) for optimism about the viability of such privately governed contracts from the likely spontaneous emergence of conflict minimizing or regulating rules for ordering disputes (Benson 1989, Mildenberger 2015). While agents may be in conflict within a contract, they still have a common interest in preserving the blockchain system, or their reputations within it, because of the value of future action. Screening or costly signalling mechanisms can also be expected to evolve to deal with information asymmetries about contractual intentions.

The induced competition ushered in by a blockchain governance revolution may well have the same 'structural cleansing effect' on a nation state that periodic collapse of the state does in washing away accumulated regulatory restrictions and burdens (Olson 1982).

Collective choice: Voting on the blockchain

A blockchain is a cryptographic consensus mechanism. Beyond applications to finance, law, and economics, a further application of the blockchain technology is politics, i.e. crypto-democracy, by facilitating secure low-cost tamper-proof 1P-1V voting. By lowering the cost and raising the perceived trust in voting institutions and

outcomes, crypto-democracy can shift the margins on the efficient use of democracy (e.g. toward more frequent referenda, or tournament-style voting), and efficient scale (e.g. toward global). A new research program follows from running through the suite of public choice results and models modified for a world of crypto-democracy. For example, Condorcet cycles on voting and Arrow's "impossibility theorem" still hold unchanged, but claims to the strategic significance of agenda setting may need to be weakened, and Down's (1957) logic about the irrationality of voting, Brennan and Lomasky's (1993) claims about expressive voting, and Caplan's (2007) claims about voter ignorance may require modification. This follows from a key finding of public choice economics, namely that the problems with democracy cannot be fixed with better quality people (i.e. more noble politicians, better informed voters), but only with better institutions. Constitutional constraints are one pathway (Buchanan and Wagner 1977), but another is polycentric governance by which the domain of democracy is matched to the most efficient information and incentive context. Blockchain-based governance is highly scalable, and can therefore potentially enable collective choices at the lowest feasible level of political authority. The tyranny of the majority (Buchanan and Tullock 1962), exploitation by organized minorities (Olson 1965) and rational voter ignorance are all significantly mitigated when self-organizing communities can adapt to optimal size based on governance not resource conditions.

4 Case study: Backfeed

A decentralized infrastructure is a necessary but as such insufficient condition for the emergence of decentralized organizations. If the blockchain is to be used to coordinate individuals beyond a basic set of algorithmically-verifiable actions (such as proof-of-work in Bitcoin), it needs to come along with an additional governance layer that is capable of regulating the interactions between people in a decentralized manner.

We examine here an innovative governance model designed to support the emergence of new institutional forms to be deployed on the blockchain. This specific governance structure goes under the name of Backfeed. Backfeed introduces a social protocol on top of blockchain-based infrastructures to coordinate individuals through the creation and distribution of economic tokens and reputation scores so as to eventually allow for the emergence of meritocratic systems and emergent alternative economies.

What is Backfeed?

At its core, Backfeed is an engine for decentralized cooperation. It implements a *Social Operating System* for decentralized organizations, enabling massive open-source collaboration without any form of centralized coordination.

Backfeed builds upon the power of open-source collaboration and enhances it with a distributed governance system for decentralized value production and distribution. The system is inspired from the model of *stigmergic* coordination found in nature, whereby certain species of animals—such ants, termites, birds, etc.—create complex social structures that do not rely on any hierarchical structure, but rather require individual agents to coordinate themselves indirectly by embedding traces into their own environment so that others can subsequently act upon it. The goal with Backfeed is to elaborate a system that can replicate the same model, but transpose it in the context of much more complex and sophisticated human organizations. This is where the blockchain comes in.

When combined together with the underlying blockchain infrastructure and smart-contract platform provided by Ethereum, Backfeed can be used to implement a generic decentralized governance structure for blockchain-based applications. Indeed, the Backfeed protocol allows for the collaborative creation and distribution of value in spontaneously emerging networks of peers. The system relies on a specific protocol that enables these distributed networks of peers to contribute freely and spontaneously to an organization, and to coordinate themselves indirectly in order to achieve the full potential of collective intelligence. A peer-to-peer evaluation system is used to determine the perceived value of each contribution in a decentralized fashion, in order to allocate influence and rewards accordingly.

In contrast to Bitcoin's Proof-of-Work consensus algorithm, which ultimately rely on algorithmically quantifiable and verifiable actions (i.e. how much computational resources have been donated to the network), Backfeed implements an alternative and more generic consensus algorithm called Proof-of-Value, which rely on human evaluations in order to discover the value of every contribution—as perceived according to the distinctive value system of each individual network (Hayek 1966).

Individual members of a community or organization evaluate the contributions 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 organization. The reputation score 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, that is in line with the community's value system (Earl and Potts 2004). Hence, individuals are judged not only by their actions (or contributions), but also by their judgment (or evaluations) of the actions of others (Foss and Klein 2012).

The result is a decentralized reputation system that dynamically distributes authority amongst community members, with a view to organically organize individuals into a meritocracy with a decentralized topology. The values of every individual that partake in the organization, weighted according to the influence that they each hold within that organization, will constitute—as an aggregate—the overall value system of the organization. As the dynamics of the organization evolve, with

new contributors coming and old contributors leaving, the influence of every individual will change, and so will ultimately the value system of that organization.

All these components combined provide the basic building blocks for the deployment of so-called Decentralized Collaborative Organizations (DCO), organizations that are not controlled by any given entity, but rather consist of a large number of individuals contributing out of their own free will to a common (collaborative) project. One might argue that this kind of spontaneous and distributed collaboration already exists in the realm of open source software, where many developers collaborate towards the achievement of a common goal in a coordinated but decentralized manner. Perhaps, but open source software represents only a small part of modern society. A proper model for DCOs should enable decentralized large-scale and systematic collaboration in potentially every sector of activity: from content creation to online gaming and networked communications, from fundraising to financial transactions, from corporate management to organizational matters, etc. Besides, without a proper incentive structure, Github did not manage to bring the model of decentralized collaboration into the mainstream, and has left the open-source movement as a niche even within the software development community.

As opposed to the traditional open source model, where people contribute for mere ideological reasons or for the purpose of increasing their social capital, in the case of any Backfeed-enabled DCO, decentralized cooperation can be achieved in a way that is both effective and sustainable over time. Contributions in a DCO are motivated by a specific system of economic and reputational incentives, and the resulting value produced by every contribution is shared among all collaborators through a specific evaluation protocol which lies at the core of the Backfeed protocol.

Imagine, for instance, thousands of people writing books and publishing them on their own, without any publisher or middleman; millions of people insuring each other, without the need to rely on centralized insurance companies; thousands of freelancers gathering together into a decentralized crowd-based journalism organization, thousands of citizens coming together to form a decentralized real-time ride-sharing or park-sharing network; and millions of internet users contributing to a decentralized social search-engine. By combining blockchain infrastructure with Backfeed's distributed governance model, this vision is now beginning to unfold—eventually leading to a revolution in the way people work and organize themselves today. In this sense, Backfeed can be seen as a tool capable of changing the nature of the blockchain from that of a *catallaxy* (i.e. a spontaneous organization driven solely and exclusively by market dynamics) into that of an *economy* (i.e. an open but more circumscribed organization driven by a uniform hierarchy of ends, and which incorporate its own economic or monetary system).

The same protocol also incorporates some of the characteristics of traditional organisation, in that it require constant monitoring of everyone's actions, in order to constantly update the reallocation of tokens and reputation according to the perceived value of contributions and evaluations that everyone brings to the network. Yet, as

opposed to the traditional model of governance based on *centralized monitoring*, where one central authority is in charge of monitoring and assessing the value of everyone else's action, in the case of Backfeed, monitoring is achieve in a distributed manner, through collective action and peer-to-peer evaluation, thus incarnating the concept of *distributed monitoring* at the governance layer, and in addition to the distributed consensus algorithm that is found at the blockchain infrastructure layer.

5 Conclusion

Blockchains are a new but potentially revolutionary technology as a cryptographically secure decentralized ledger upon which can be placed any information requiring public validation (e.g. money, contracts, property titles, identity, etc.). One way to look at the economics of blockchain is as a new general-purpose technological innovation that is undergoing the Schumpeterian phases of adoption and diffusion through the economy, as a kind of internet 2.0. Yet this nascent characterisation of the blockchain (including bitcoin) as an epochal new ICT, thus emphasising disruptive new markets and industries, while not wrong, is nevertheless misleading. For blockchain is also an 'institutional technology', a governance technology for making catallaxies, or rule-governed economic orders. Blockchains thus compete with firms, markets and economies, as institutional alternatives for coordinating the economic actions of groups of people, and may be more or less efficient depending upon a range of conditions (behavioural, cultural, technological, environmental, etc). This is what makes blockchains interesting from an institutional and public choice perspective.

This suggests a new research program on the economics of blockchains that builds around the work of, at minimum: Ronald Coase (on efficient institutions); FA Hayek (on distributed knowledge and private constitutional ordering, including money); Elinor Ostrom (on commons governance); Oliver Williamson (on incomplete contracts); and James Buchanan (on constitutions and collective action). What pulls these literatures together is a view of blockchains not as a new technology, but as a new type of economy. The Ethereum enabled platform Backfeed furnishes a paradigmatic case of how blockchains can construct new types of economies built on cryptoeconomic institutions.

References

Alchian, A,. Demsetz, H. (1972) 'Production, Information Costs, and Economic Organization' *American Economic Review*,

Allen, D. (2011) *The Institutional Revolution: measurement and the economic emergence of the modern world*. University of Chicago Press.

Allen, D., MacDonald, T. (2016) 'The entrepreneurial problem of the blockchain' Working paper, RMIT.

Arthur, W.B. (2009) *The Nature of Technology*. The Free Press: New York.

Babbitt, D., Dietz, J. (2015) 'Cryptoeconomic design: A proposed agent-based modeling effort' Swarmfest 2014. http://www3.nd.edu/~swarm06/SwarmFest2014/Babbitt.pdf

Benkler, Y. (2006) *The Wealth of Networks*.

Benson, B. (1989) 'The Spontaneous Evolution of Commercial Law.' *Southern Economic Journal*, 55,

Boettke, Peter J. (2005) Anarchism as a progressive research programme in political economy. In: E. Stringham (ed) *Anarchy, State and Public Choice*. Cheltenham, UK: Edward Elgar.

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

Brennan, G., Buchanan, J. (1985) *The Reason of Rules: Constitutional Political Economy*. Cambridge, UK: Cambridge University Press.

Brennan, G., Lomasky, L. (1993) *Democracy and decision: The pure theory of electoral preference*. Cambridge: Cambridge University Press.

Bresnahan T, Trajtenberg M (1995) 'General Purpose Technologies "Engines of Growth?' Journal of Econometrics, vol. 65, no. 1, pp. 83-108.

Buchanan, J., Wagner, R. (1977) *Democracy in Deficit*.

Buchanan, J. (1990) 'The Domain of Constitutional Economics' *Constitutional Political Economy*, 1(1):

Buchanan, J. Tullock, G. (1962) *The Calculus of Consent*.

Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. http://ethereum.org/ethereum.html

Buterin, V. (2014a) 'DAOs, DACs, DAS and more: An incomplete terminology guide' 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 & Decentralized Application Platform' https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf.

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

Coase, R. (1937) 'The Nature of the Firm' *Economica*, 4(16): 386–405.

Coase, R. (1960) 'The problem of social cost'

Cox, M., G. Arnold, Villamayor-Tomás, S. (2010) A review of design principles for community-based natural resource management. *Ecology and Society* **15**(4): 38.

De Filippi, P (2014) Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review*, 3. Online at: http://policyreview.info/articles/analysis/bitcoinregulatorynightmarelibertarian-dream.

Downs A (1957) *An Economic theory of Democracy*. Harper & Row. New York.

Evans D (2014) 'Economic aspects of Bitcoin and other decentralised public-ledger currency platforms' Coase-Sandor Institute for Law and Economics working paper #685.

Earl, P. Potts, J. (2004) 'The market for preferences' *Cambridge Journal of Economics*,

Fleetwood, S. (1995) *Hayek's Political Economy*. London: Routledge.

Frishmann, B. Madison, M., Strandburg, K. (2014) Governing Knowledge commons. Oxford University Press: Oxford.

Gode D, Sunder S (1997) 'What makes markets allocatively efficient?' *Quarterly Journal of Economics* 105: 603-30.

Hart, O. (1989) 'An economists perspective on the theory of the firm' Columbia Law Review, 89: 1757-74.

Hart, O., Moore, J. (1990). "Property Rights and the Nature of the Firm". *Journal of Political Economy* 98: 1119–58.

Harvey, C. (2015) 'Cryptofinance' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438299

Hayek, F.A. (1945) 'The Use of Knowledge in Society' *American Economic Review*, 35(4): 519-30.

Hayek, F.A. (1948) *Individualism and Economic Order*. Chicago: University of Chicago Press.

Hayek, F.A. (1960) *The Constitution of Liberty*, Chicago: The University of Chicago Press.

Hayek, F.A. (1966) 'Competition as a discovery procedure'

Hayek, F.A. (1973) *Law, Legislation and Liberty. Volume 1: Rules and Order*. Chicago: University of Chicago Press.

Hayek, F.A. (1974) 'The Pretence of Knowledge' *American Economic Review*, 79,

Hayek, F.A. (1978) *The Denationalisation of Money The Argument Refined*. London: Institute for Economic Affairs.

Hayek, F.A. (1988) *The Fatal Conceit. The Errors of Socialism*. London: Routledge

Hendrickson, J., Hogan, T., Luther, W. (2015) 'The political economy of bitcoin' SSRN

Hodgson, G. (2006) 'What are institutions?' *Journal of Economic Issues*, 40(1): 1-25.

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

Kauffman, S. (1993) *The Origins of Order*.

Leeson, P. (2007) 'An-arrgh-chy: the law and economics of pirate organization' Journal of Political Economy, 115(6): 1049-94.

Leeson, P. (2008) 'Coordination without command: Stretching the scope of spontaneous order.' *Public Choice*, 135, 67-78.

Leeson, P. (2014) *Anarchy Unbound. Why Self Governance Works Better Than You Think*. Cambridge Studies in Economics, Choice and Society. Cambridge: University Press.

Lessig L (2015) 'De ja vu all over again' Talk given at Sydney Blockchain workshop.

Lipsey, R., Carlaw, K., Bekhar C. (2005). *Economic Transformations: General Purpose Technologies and Long Term Economic Growth*. Oxford University Press.

MacDonald, T. (2015a) 'Spontaneous Order in the Formation of Non-Territorial Political Jurisdictions'. http://ssrn.com/abstract=2661250

MacDonald, T. (2015b) 'Theory of non-territorial internal exit' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2661226

MacDonald, T. (2015c) 'The social media spontaneous order is a constellaxy' Journal of Brief Ideas, http://beta.briefideas.org/ideas/2e9e15b6adb3e76e44f4cf2a9f8f9a01

Madison, M., Frishmann, B., Strandburg. (2010) 'Constructing commons in a cultural environment' Cornell Law Review, 95:

Mildenberger C.D. (2015) 'Virtual world order: the economics and organizations of virtual pirates' *Public Choice*, 164: 401-21.

Mirowski P. (2001) *Machine Dreams: How Economics Became a Cyborg Science*. Cambridge University Press; Cambridge.

Mirowski, P., Somefun, K. (1998) 'Markets as evolving computational entities' *Journal of Evolutionary Economics*, 8(4): 329-56.

Nakamoto S (2008) 'Bitcoin: A peer-to-peer electronic cash system' https://bitcoin.org/bitcoin.pdf

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

Nussbaum, F. (1933): *A History of the Economic Institutions of Modern Europe: An Introduction of 'Der Moderne Kapitalismus' of Werner Sombart.* New York: Crofts.

Olson, M (1965) *The Logic of Collective Action*. Harvard University Press: Cambridge, MA.

Olson, M. (1982) *The Rise and Decline of Nations*. Yale University Press: New Haven.

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

Ostrom, E. (2010) 'Beyond markets and states: polycentric governance of complex economic systems.' *The American Economic Review:* 641–672.

Ostrom, E. and C. Hess. (2006). A Framework for Analyzing the Knowledge Commons. In *Understanding Knowledge as a Commons: from Theory to Practice*. eds. Hess, C. and E. Ostrom, 41–82. Cheltenham: Edward Elgar.

Ostrom, E., Walker, J., Gardner, R. (1992) 'Covenants with and without a sword: Self-Governance is possible' *American Political Science Review*, 86(2), 40417.

Ostrom, Elinor, 1990: Governing the Commons. The Evolution of Institutions for Collective Action. New York: Cambridge University Press.

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.X. Olleros and M. Zhegu. (eds) *Research Handbook on Digital Transformations*, Edward Elgar. Available at SSRN: http://ssrn.com/abstract=2662660

Potts J (2001) 'Knowledge and markets'

Potts, J. (2000) *The New Evolutionary Microeconomics*. Edward Elgar.

Skarbek, D. (2011) 'Governance an dprison gangs' American Political Science review, 105(4): 702-16.

Stigler, G., (1971) 'The theory of economic regulation.' *Bell Journal of Economics and Management Science* 2: 3-21.

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

Swan, M. (2015) *Blockchain: Blueprint for a New Economy*. O'Reilly Media: Sebastopol.

Thierer, A. (2014) *Permissionless Innovation*. Mercatus Centre. http://mercatus.org/permissionless/permissionlessinnovation.html

Tiebout, C. (1956) A pure theory of local expenditures. *Journal of Political Economy* 64: 416-424.

Tirole, J. (1999) 'Incomplete contracts: where do we stand?' *Econometrica*, 67(4): 741-81.

Tullock, G. (1967) "The Welfare Costs of Tariffs, Monopolies and Theft." *Western Economic Journal* 5: 224–232.

White L (2015) 'The market for cryptocurrencies' Cato Journal, 35(2): 383-402.

Wiles N (2015) 'The radical potential of blockchain technology' https://www.youtube.com/watch?v=JMT0xwmFKIY

Williamson, O. E. (1973) 'Markets and hierarchies: some elementary considerations' *American Economic Review 63*(2): 316-25.

Williamson, O. E. (1975) *Markets and Hierarchies: Analysis and Antitrust Implications*, New York: Free Press.

Williamson, O. E. (1979) 'Transaction cost economics: the governance of contractual relations' *Journal of Law and Economics 22*(2): 233–61.

Williamson, O. E. (1983) 'Credible Commitments: Using Hostages to Support Exchange' *American Economic Review 73*(4): 519–38

Williamson, O. E. (1985) *The Economic Institutions of Capitalism*, New York: Free Press.

Williamson, O. E. (1991) 'Comparative Economic Organization: The Analysis of Discrete Structural Alternatives' *Administrative Science Quarterly 36*: 269–296.

Williamson, O. E. (1996) *The Mechanisms of Governance.* New York, NY: Oxford University Press.

Williamson, O. E. (2002) 'The lens of contract: private ordering' *American Economic Review: P&P, 92*(2): 438–43.

Williamson, O. E. (2005) 'The economics of governance' *American Economic Review 95*(2): 1–18.

Wilson, D. S., Ostrom, E., Cox, M. (2013) 'Generalizing the core design principles for the efficacy of groups' *Journal of Economic Behavior and Organization*.

Wood, G. (2014a) 'DApps: What Web 3.0 looks like' & 'What is Web 3.0' http://gavwood.com/dappsweb3.html, and http://gavwood.com/web3lt.html,

Wood, G. (2014b) "Ethereum: a secure decentralized generalized transaction ledger' http://gavwood.com/Paper.pdf

Wood, G. (2015) 'Ethereum for dummies' https://www.youtube.com/watch?v=U_LK0t_qaPo

Wright, A., De Filippi, P. (2015) 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' SSRN: http://ssrn.com/abstract=2580664

Yamey B (1949) 'Scientific bookkeeping and the rise of capitalism' Economic History Review 1(2&3): 99-

ENDNOTES

[1] A ledger is a value recording and transfer system.
[2] Satoshi Nakamoto is a pseudonym.
[3] Economic agents in such a world include *decentralized autonomous organizations* (Buterin 2014a).
[4] Another is *Counterparty*, which runs on the bitcoin blockchain.
[5] This same idea can be framed using another of Williamson's (1979, 1985) terminological and conceptual innovations: the *fundamental transformation*. This refers to the effect of specificity (idiosyncratic investment) that arises from joint production has on the structure of competition. *Ex ante* competitive contracting is transformed by asset specific investment into *ex post* bilateral monopoly, giving rise to the hazard of opportunism (Klein, Crawford and Alchian 1978, Alchian and Woodward 1988). The value of an investment is thus contingent on the continuity of the contracts supporting it.

[6] For Hayek an economy refers to a created institution, a household or firm where a given set of means are allocated according to a consciously designed plan where an optimal outcome can be described. A catallaxy invokes no such notion of a consciously designed or optimal end state, but is a spontaneous emergent order. It describes an "order brought about by the mutual adjustment of many individual economies in the market." (Hayek 1976, 108-9).