The Journal of Private Enterprise 35(2), 2020, 1–21

Blockchains: Less Government, More Market

Alastair Berg
Blockchain Innovation Hub, RMIT University

Brendan Markey-Towler
Blockchain Innovation Hub, RMIT University

Mikayla Novak
Blockchain Innovation Hub, RMIT University

Abstract
We provide a survey of blockchain's potential to propel private entrepreneurial discovery of institutions that challenge state hegemony. We introduce institutional cryptoeconomics, and then we describe blockchain as a technology that increases the opportunity set of entrepreneurial action. We then survey blockchain's potential to challenge state hegemony in five socioeconomic areas. We also discuss some implications of blockchain-based economic infrastructure for public policy and regulation. These contributions suggest an increasing scope for entrepreneurial action using blockchain to challenge state hegemony. They also suggest a necessary shift in the provision of public goods and government regulatory control.

JEL Codes: O33, O35, O39, P00, P40, P49
Keywords: blockchain, institutions, entrepreneurship, privatization, role of government

I. Introduction

Blockchain is an institutional technology that changes the scope of human interaction within and across the public and private spheres. While this technology was first used to transact value across the internet without any financial intermediary, it is now being used in private entrepreneurial discovery in several areas that have traditionally been the preserve of government. The central finding of the emerging field of institutional cryptoeconomics is that blockchain technology is not just a general-purpose technology, but rather an institutional technology of governance that competes with the other economic institutions of capitalism. Considered in such a manner, blockchains broaden the institutional suite of markets, hierarchies, and relational contracting through which economic exchange has

been hitherto facilitated (Davidson, De Filippi, and Potts 2018). Blockchains and the applications built upon them "industrialise trust" (Berg, Davidson, and Potts 2017) by mitigating opportunism (see Williamson 1985). These features enhance individuals' ability to engage in mutually beneficial and, crucially, voluntary exchanges that were difficult— until now.

Blockchain as an institutional technology can be understood by considering what it is and what it does. Blockchain in general is a type of distributed ledger technology that relies on peer-to-peer networking, asymmetric (public-key) cryptography, and economic incentives to generate agreement on a "true" public record of socioeconomic facts. This record is kept by each node in a network that supports the infrastructure (thus it is distributed), and each node must agree to the incorporation of a new "block" of records to be entered into the "chain" of such blocks. Thus, it creates protocols concerning what are valid interactions that may be verified as socioeconomic facts entered into a public record.

Any such algorithm necessarily creates institutions demarcating the scope of interactions that society deems valid (Ostrom 1990; Hodgson and Knudsen 2010; Lawson 2016), where institutions are considered as the mechanisms and protocols that constrain and shape human interactions (see North 1990). A multitude of algorithms has been proposed for how such blocks are to be compiled and added by the network to the chain constituting the public record of socioeconomic facts. These proposals' common objective is achieving decentralization of consensus (Ometoruwa 2018). Because individuals are free to interact within whatever blockchain-based platforms and associated institutional systems they see fit, and because entrepreneurs may develop new systems or "fork" existing ones as they see fit, the technology facilitates a process of institutional discovery (Berg and Berg 2017; Berg, Davidson, and Potts 2018a).

These platforms, and the institutional systems created by the protocols embedded in their infrastructure, are novel because they are an intermediate form between those we have previously observed. Specifically, they share characteristics of the institutional systems underlying both firms and markets as studied by Oliver Williamson (1975, 1985), and yet are not definitively of either kind. They are systems in which voluntary interactions are coordinated within an institutional framework to which individuals (in principle) voluntarily agree, and so they share the characteristics of the decentralized,

voluntary institutional system that underlies coordination in markets as studied by Friedrich Hayek (1945, 1988).

However, the platforms within which those interactions occur, and the institutions embedded within the protocols of their infrastructure, are also designed in the manner of a business firm's command-and-control hierarchy as identified by Coase (1937). The platforms and institutional systems that emerge from a blockchain-based infrastructure are thus of an intermediate form that we have not encountered before to any great extent.

In this paper, we draw on the field of institutional cryptoeconomic research to show how, as an institutional technology, blockchain is radically expanding the scope for private enterprise, even to areas traditionally under the hegemony of centralized governmental action. Blockchain is driving a process of institutional entrepreneurial discovery whereby entrepreneurial action is developing market-based solutions to "problems" traditionally handled by government. Blockchain protocols that provide for the immutable and transparent recording of socioeconomic facts, and whose rule sets can only be changed by noncoercive consensus, radically lower the costs of voluntary organization at the expense of public governance structures.

The premise of this paper is simple: to briefly survey areas of socioeconomic interaction that are now more open to market forces and dynamics due to the development of blockchain technology. We examine five main case studies: new monetary institutions (e.g., cryptocurrencies), new forms of smart contracting and dispute resolution, platforms that bolster civil society institutions such as social welfare, new forms of collective choice infrastructure (i.e., cryptodemocracy), and the decentralized, self-sovereign verification of identity. We then comment on the implications of an expansion in private enterprise for how we conceive and formulate public policy.

II. Case Studies: Where Blockchain Is Expanding the Scope of Private Enterprise

Institutional cryptoeconomics (see the seminal paper by Davidson, De Filippi, and Potts 2018) shows that blockchain is an institutional technology that allows for the creation of platforms for private—and, crucially, voluntary—socioeconomic interaction in which institutions emerge from the protocols embedded in that infrastructure. This new form of technology, platform, and institutional system presents a fundamental challenge to government hegemony in socioeconomic

systems. It also expands the scope of private enterprise to the design and formulation of institutions and platforms for socioeconomic interaction. The subsequent five case studies show that by creating an environment in which consensus over some shared "truth" can be achieved without the coercive power of a central authority, blockchain substantially increases entrepreneurial opportunities. This section outlines how this challenge is being presently realized in a variety of contexts, including money, contracts, civil society, voting, and identity.

A. Monetary Institutions and Cryptocurrency

The first use of blockchain as an infrastructure for new platforms and institutional systems was in the form of cryptocurrency. This expansion of entrepreneurial action into the design and formulation of privatized monetary institutions was of course not unprecedented, but it was given a new vigor by the advent of blockchain consensus algorithms. These allow for decentralized consensus across a network that previously relied on centralized governmental authority. Indeed, while several nonfiat digital currencies preceded bitcoin, they were susceptible to government interference. They also relied on the continued existence of a private company to maintain user balances (see, for instance, Popper 2015). The invention of bitcoin and its underlying blockchain—incorporating technologies used by these now-defunct digital currencies (see Narayanan and Clark 2017)—creates an infrastructure for monetary institutions where the record of socioeconomic facts upon which a decentralized network achieves consensus is a record of transfers (thus holdings) of purchasing power. As Luther and Olson (2015) argue, it serves to establish "memory" in privatized monetary systems.

The first such infrastructure was the famous bitcoin protocol originally developed by the pseudonymous Satoshi Nakamoto (2008). Bitcoin provided a new, privatized platform for socioeconomic interaction in which payments may be made in the context of a privatized institutional system concerning the validity of payments. The institutional system created by bitcoin emerges from the protocols embedded in the blockchain infrastructure upon which it operates. For instance, any transfer of "coins" cannot exceed the total number held by the individual; the transaction must be "signed" by the transferring party; the transfer must be reported to the network at large; there is an option and increasing expectation to

"tip" the miners who compile the block of records and prove it is true by expending "work"; and so on.

Bitcoin was not new insofar as it was a system with privatized monetary institutions; the history of privatized monetary institutions is well documented (Selgin 1988; White 1999). What was new about bitcoin was how it could challenge government hegemony through the decentralization and scale offered by its underlying blockchain infrastructure. Where prior (digital) privatized monetary systems tended to rely on centralized consensus processes, blockchain offered the potential for a new monetary system whose institutions were subject to privatized design, but whose operation was distributed and largely automated. Luther (2019) provides a history of bitcoin, the steps early users took to coordinate its launch, and its widespread adoption (see also Luther 2018). The infrastructure's key innovation was to significantly decrease and distribute the costs of creating and operating such a system. Blockchain significantly expanded the scope for private enterprise in monetary institutions, challenging a fundamental hegemony of government action in socioeconomic systems on a scale hitherto difficult.

Needless to say, bitcoin's ability to challenge government hegemony in the issuance of currency has itself been challenged (Luther 2016) as governments seek to maintain their monopoly in this sphere through coercion. It has been suggested that a large enough government might be able to restrict bitcoin's use by private actors in certain circumstances (Hendrickson, Hogan, and Luther 2016; Hendrickson and Luther 2017).

The further effect of this expansion of the scope for private enterprise and entrepreneurial action has been that blockchain-based cryptocurrencies have provided fresh vigor for institutional discovery in monetary systems. Nakamoto's bitcoin protocol was followed by the release of a range of new protocols for cryptocurrency platforms with different iterations of the institutions emergent from those protocols. Later iterations of cryptocurrency modified bitcoin's original institutional infrastructure with a view to preserving privacy above all else. The relative ease by which individuals can release new blockchain-based cryptocurrencies has seen their numbers increase dramatically since 2011 (White 2015). The open-source nature of most cryptocurrency projects allows users to take existing software code and modify it in a process of institutional discovery (Berg, Davidson, and Potts 2018d). For instance, the monero cryptocurrency requires multiple digital "signatures" to be obtained

and put to a given "coin" to mask the true origin of payments (van Saberhagen 2013). Other iterations of cryptocurrency such as basis (Al-Naji, Chen, and Diao 2017) modified the institutional structure for the creation of new "coins" with a view to using algorithmic central banks to support price stability, giving rise to the "stablecoin" trend. The freedom within cryptocurrency platforms and markets to secede or fork from one such system and accede to another means that such entrepreneurial activity drives a process of institutional discovery (see Hayek 1976). In this way, blockchain has expanded the scope for entrepreneurial action in monetary institutions and driven a new process of institutional discovery that challenges core government hegemonies.

B. Contractual Institutions and the "Smart Ledger"

After using blockchain to implement cryptocurrency protocols, entrepreneurial action expanded to using blockchain as infrastructure for the design of privatized institutions concerning the striking, recording, and executing of contracts. People quickly realized that blockchain could be used to achieve decentralized consensus on a record of "smart contracts." The smart contract was a concept originally proposed by computer scientist and legal scholar Nick Szabo (1994) by which a contract would be written into the operations of an algorithm and automatically executed when certain events occurred. The blockchain would then become a "smart ledger" of contracts struck, recorded, and then executed automatically upon the realization of particular states of the world.

One of the first protocols to operationalize the smart contract was Ethereum, developed by programmers Vitalik Buterin (2013) and Gavin Wood (2014), among others. The blockchain within the Ethereum platform acts as an infrastructure for a system of interaction in which consensus on a "smart ledger" is achieved by a decentralized network. The institutions concerning what is a valid smart contract and what is not—and thus the conditions under which a contract may be struck, recorded, and executed—emerge from the protocols embedded within the Ethereum protocol. As individuals enter into smart contracts, they are recorded on the Ethereum blockchain, a smart ledger distributed across the Ethereum network, and executed automatically as certain events occur.

Private individuals and groups have been striking and keeping records of contracts from time immemorial, including within large-scale public platforms subject to privatized design (Stringham 2015).

Traditionally, and notwithstanding significant efforts in the design of such contracts to avoid it, the ultimate verification and enforcement of contracts has been under the hegemony of government action in the form of contract law (Commons 1924). This hegemony is particularly acute when disputes arise over the contents and applicability of contracts to various environments in which action must be taken.

What was new about the blockchain-based smart ledger, and particularly Ethereum, was a significant decrease in and distribution of the costs of maintaining a privatized system in which contracts may be verified and automatically executed, and in which disputes may be resolved. The blockchain-based smart ledger provides a platform where quite complex and more complete contracts can not only be written and automatically executed, but also verified as a matter of course by a decentralized network. These characteristics expedite verification processes in the pursuit of dispute resolution, as well as action the outcomes thereof. Blockchain therefore significantly expands the scope for private enterprise, particularly in the development of institutions that verify and execute contracts and resolve contract disputes. Blockchain challenges the ultimate hegemony of government coercion in this regard.

Ethereum was followed by other iterations of smart ledgers with variations on the protocols embedded in their blockchain infrastructure from which their institutions emerge. NEO seeks to integrate a range of different applications of blockchain technology and deliberately aims to provide a platform for an alternative socioeconomic system formed by smart contracts and the decentralized applications built on them. EOS seeks to improve on the institutions by which consensus is achieved on the smart ledger by moving from an energy-intensive "proof-of-work" algorithm to a "delegated proof of stake" algorithm. It also seeks to address governance issues more generally (Grigg 2017).

The characteristics of smart contracting have also proved useful for the creation of decentralized applications, including online marketplaces such as OpenBazaar (Gulker and Stringham 2018). Thus, by expanding the scope for private enterprise and by facilitating entrepreneurial action in the design and formulation of institutions around the striking, recording, and executing of contracts, blockchain drives a newly invigorated process of institutional discovery in the core institutions of socioeconomic interactions.

C. Social Welfare Systems and the Coordination of Compassion

As an infrastructure that allows for the recording, storing, and validating of data and information by a decentralized and distributed network, blockchain can challenge the hegemony of government action. It could be harnessed to design institutional systems that promote social ends, informed by whatever notion of welfare (for instance Boettke and Subrick 2003; Diener et al. 1999; Gropper, Lawson, and Thorne Jr. 2011; Sen 1999) the designer wishes to promote. This possibility is especially important at present, where public opinion surveys indicate declining trust in organizations (even nongovernment ones) that have traditionally had hegemony in promulgating social welfare in countries such as the United States, Germany, France, Italy, Canada, and Australia (Edelman 2018). With its combination of automated code, cryptographic security, and cryptoeconomic security, blockchain may be able to challenge this hegemony. It could be harnessed to promote social welfare through new platforms whose institutions address problems using privatized systems for promoting social welfare.

It appears that the decline in trust in charities, foundations, social enterprises, and other bodies within civil society may be derived from the potential for opportunism in the presence of asymmetric information between contributors to such projects, the intermediary operators, and the ultimate beneficiaries. Unless the institutions that govern such projects create sufficient accountability mechanisms and have transparency safeguards in place, it is difficult for the contributor to observe that their financial or in-kind support has flowed through to the beneficiary with minimal disturbance. As highly publicized financial management and other scandals in certain developed countries have illustrated (Archambeault, Webber, and Greenlee 2015; Fremont-Smith and Kosaras 2003), intermediary groups within the social welfare sector are susceptible to malign or erroneous practices believed to undermine the efficacy and efficiency of organizations and to compromise the fulfilment of their objectives.

Challenges to the hegemony of government action in social welfare systems by private entities have likely been restricted due to charity and foundation scandals. Even though few entities have been subject to such scandals, these scandals can have consequences for the entire sector, such as potential contributors withdrawing their support from private platforms that promote social welfare (Boris and Steuerle 2017; Rooney, Wang, and Ottoni-Wilhelm 2018; Novak

2018b). The reputational impact may have consequences for the capacity of charities and other highly organized providers within civil society to promote cooperative efficacy (Nair and Sutter 2018). It is here that privatized institutional design for platforms supporting socioeconomic interaction, enabled by blockchain, is likely to bring benefits by reducing possibilities for opportunism. Blockchain-enabled platforms are characterized by institutions that interrelatedly promote:

- Radical transparency: Blockchain allows contributors, beneficiaries, and other interested parties to track the verified flow of funds in real time and to use smart contract arrangements to disburse funds to providers on the condition that pre-agreed social impacts have been achieved. An example of the use of blockchain to promote transparency is Alice, a social impact network built on the Ethereum blockchain that encourages social organizations to operate and report on their projects transparently (Mazet and Wojciechowski 2017). The Alice platform applies a number of techniques to promote transparency by charitable interests. One of these is to pay project proponents to publish milestone reports in a timely manner, while another is to instigate smart contracts that withhold some donated funds from charities until social impacts are achieved and validated.
- Cost reduction: Blockchain technology could be used to bypass traditional intermediaries that impose considerable costs and prescriptive conditions on money transfers, both domestically and internationally. A British charity, Positive Women, conducted a trial to fund school education in Swaziland using the Disburse blockchain platform. The trial reportedly saved approximately 3 percent on money transfer fees compared against conventional banking. The savings covered the costs of a year of education for three additional students (Allen 2017). A recent study of the feasibility of conducing philanthropic projects through blockchain refers to transaction-fee savings when transferring donated funds using bitcoin (Jayasinghe et al. 2018).
- Reorganization of assistance models: Smart contracts and blockchain protocols can be combined to create "decentralized collaborative organizations" (DCOs) with social welfare objectives. These could provide competitive pressure for third-party intermediary programs to ensure desirable social outcomes and to enhance social learning about the effective uses of donor

finances and other resources. The potentially disruptive implications of charitable DCOs have meant that such organizational models have been slow to implement in practice, although the advent of social assistance initial coin offerings (ICOs) in recent years points to a nontrivial level of conduct for charitable and philanthropic activities primarily using blockchain.

In general, entrepreneurial action is now, with blockchain technology, better able to design institutions around the allocation of contributions to realizing social welfare objectives and better challenge what has traditionally been the hegemony of government action. Through the process of institutional discovery this enables, we are likely to be able to better solve the economic problem of designing institutions that allocate resources and distribute funds to vulnerable persons (Martin and Petersen 2018).

D. Voting and Social Choice

A central realization of the institutional cryptoeconomics literature is that blockchain is, by its nature, a technology for governance (Davidson, De Filippi, and Potts 2018). It provides an infrastructure for platforms in which institutions may be designed to govern behavior within that system. In particular, it provides an infrastructure whereby institutions might be designed to coordinate action among a group by aggregating perspectives within that group on how action ought to be coordinated. One of the central coordination problems that governance structures seek to solve is group decision making. Viewed as an economic problem, collective choice involves both forming and coordinating contextual, distributed, and evolving preferences (Hayek 1937, 1945). Institutions for guiding collective action need to be able to coordinate the provision of information that forms individual perspectives and coordinate those perspectives once they are formed.

The suite of democratic institutions available to us is constrained by the available technologies. As new technologies are invented—from the kleroterion in ancient Athens that facilitated sortition (Dow 1939) to the modern printing press that enabled ballot papers—new forms of collective choice infrastructure become available. Technologies help us to create institutions that economize on the costs of making collective choices, including developing new ways to coordinate information to form those preferences. Those costs include ones derived from making choices under uncertainty (i.e.,

decision costs) and the costs of delegating power to representatives (i.e., agency costs) (Allen, Berg, and Lane 2019).

Blockchain is a novel technology for democratic governance. It provides scope for private enterprise to design institutions for the formation and aggregation of perspectives on collective action in a manner where validation is obtained by a decentralized and distributed network. It provides a technology whereby votes may be distributed and aggregated on particular questions of collective action promulgated throughout the network according to institutions specific to a given blockchain. We can call the ordering of collective choice through blockchain a cryptodemocracy (see Allen et al. 2018; Allen, Berg, and Lane 2019).

A cryptodemocracy has polycentric characteristics. It is characterized by dispersed centers of decision making that emerge from the actions of voters and political entrepreneurs in response to any range of collective choice problems, from public elections to corporate and union governance. Such an arrangement suggests a more competitive and dynamic discovery process.

Changes in the nature of collective choice institutions are profound, as the institutions for forming and aggregating preferences have traditionally been the hegemony of centralized authorities that validate the public record of aggregated perspectives. The institutional possibilities for coordinating collective action have been restricted. For instance, even within the most advanced liberal democracies, the bundle of rights that citizens hold is highly constrained. Voters are often placed within defined electoral boundaries and vote only every set number of years. Votes generally cannot be bought or sold in a market due to the necessity of the secret ballot. Taking a property rights perspective of voting rights (i.e., Demsetz 1967), the bundle of rights that governments afford their citizens is a heavily restricted bundle because existing technologies struggle to economize the costs of allowing for an expanded set of rights.

Because voting rights can be maintained and exercised through a shared, decentralized ledger using blockchain, it is an infrastructure that allows for a more liquid and emergent coordination of voting rights, including the buying and selling of votes and the delegation and re-delegation of votes through a series of contracts (Allen et al. 2018; Berg 2017a, b). While contemporary, centralized, and government-dominated democracies routinely reduce the rights that voters can express—for example, through secret ballots preventing

voting markets (Brent 2006; Crook and Crook 2007; Heckelman 1995; Kam 2017)—blockchain holds promise to expand the bundle of voting rights that people hold. Blockchain opens up new institutional possibilities based on emergent spontaneous coordination, a polycentric grouping of decision-making power, and a more contractarian democratic order (Allen et al. 2018; Allen, Berg, and Lane 2019).

Examples of cryptodemocratic institutions began to emerge shortly after the release of the first smart contract protocol, Ethereum. One was the Decentralized Autonomous Organization, or "the DAO." Holders of DAO "tokens" had the right to vote on investment decisions and received a return based on the performance of those investments. This corporate form was designed to enable "democratic" collective decision making outside of the traditional, hierarchical corporate process (Rennie and Potts 2016).

Unfortunately, a malicious actor quickly exploited an error in the code governing the DAO's function, which led to the withdrawal of ether (the cryptocurrency associated with Ethereum) worth some $50 million (in 2016 dollars) (Popper 2016). To rectify the DAO's perceived failure, a vote was held to determine participants' willingness to forcibly return the stolen funds via a "hard fork" in the DAO's code.

Although there are valid concerns over the method by which the vote was held, the timeframe given for participation, and the role played by prominent members of the Ethereum community (see, in particular, Breitman 2017), "the DAO" episode has illustrated the potential for both the coordination of voluntary commercial activity and the manner in which private mechanisms might be brought to bear on corporate governance.

By providing scope for private enterprise even in the most foundational of society's institutions, blockchain allows for greater institutional discovery in the coordination of social choice and collective action. It facilitates the spontaneous voluntary adaptation of institutions for coordinating social choice to changing circumstances. It also challenges what has been hitherto the province of centralized and particularly government action. Cryptodemocracy could make private institutions around forming and aggregating perspectives on social choice more institutionally efficient than public institutions as private institutions come to solve collective action problems in more effective ways.

E. Establishment and Verification of Identity

Some level of assurance over the attributes of a counterparty to an exchange is necessary for all but the least sophisticated transactions (Berg et al. 2017, 2018). The economic and political interactions individuals enter into are (usually) contingent on the presentation of proof as to particular identity attributes. Traditionally, these attributes have been proven using government-issued identity documents; commercial exchange typically free-rides off government-issued identities (Berg et al. 2017).

Recently, we have also seen less official but nonetheless important online identities controlled by a small number of commercial entities (such as Google, Facebook, and Twitter) and used to monetize an individual's habits, tastes and preferences via online advertising (Der, Jähnichen, and Sürmeli 2017). These corporations have transformed themselves into quasi-political entities because they have near-complete authority over maintaining users' online identities.

Whether controlled by governments or by corporations, the institutions through which we establish and prove identity have traditionally used entries in a centralized ledger. Blockchain-based identity management systems, by contrast, are decentralized. This structure, combined with the private storage of digital identity attributes, has the potential to challenge and supplant government hegemony over the institutions by which public identity is established, accessed, and managed.

Blockchain protocols are currently being developed to allow for the privatized, decentralized and distributed administration and governance of institutions by which identity is established, validated, and proven. In general, blockchain-based identity infrastructure provides a means to give certainty that an individual owns some identity attribute, while simultaneously obfuscating previous activities of that individual, thereby giving strong privacy protections (Der, Jähnichen, and Sürmeli 2017). Crucially, these blockchain-based identity platforms allow individuals to prove who they are for the purposes of commercial exchange without entirely relying on the actions or cooperation of any centralized authority such as a government or commercial entity with a monopoly on the means of coercion.

Loffreto (2012), Searls (2012), and Allen (2016) are among those who have developed the concept of self-sovereign identity, which expands the opportunity set of entrepreneurial actions around the

institutions of identity and identity management. Self-sovereign identity places the management of identity attributes within the purview of the individual and, among other things, emphasizes characteristics of individual control, portability, consent, and disclosure minimization (see Allen 2016). In general, it gives individuals complete and persistent control over their identity attributes while maintaining the ability to disclose only those attributes they desire in order to participate in exchange.

This system stands in stark contrast to how government entities normally provide public identity institutions. Identity provision is normally one of administrative necessity (Searls 2012), whereby states seek maximum legibility (see Scott 1998) such that their populations can be embraced (see Torpey 2000) for the purposes of taxation, conscription, and welfare administration. With self-sovereign identity, the crucial characteristics of control and portability over one's personal identity information, enabled through decentralized blockchain platforms and complemented by allied technology such as zero-knowledge proofs, allow entrepreneurial action to create previously impossible institutions for establishing and verifying identity—institutions that are controlled by individuals.

For instance, self-sovereign identity platforms such as Sovrin (2018) and Meeco (2018) are currently being developed to allow individuals to share their identity attributes as part of exchange without relying on the continued cooperation of government or commercial entities, while also allowing individuals to reduce the amount of identity information they expose in the first place. In general, such identity platforms allow for the verification of certain identity attributes, age or income for instance, without revealing the exact nature of that claim, and without storing personally identifiable information on a blockchain itself. For example, an individual could prove they are over the legal drinking age and gain access to some licensed premises without revealing their age or any other superfluous information, such as their home address.

In addition, individuals could maintain separate and noncorrelatable relationships with commercial or even government service providers, providing for added privacy protection in the event one provider suffers a security breach. The exposure of (potentially sensitive) financial information after the data breach of an individual's banking provider would, in effect, be isolated from other important information related to that individual.

This shift presents new institutional opportunities for the governance of individual identity. Entrepreneurs can develop new applications that allow individuals to manage, and perhaps even monetize, their own identity data. Blockchains provide scope for private enterprise so that entrepreneurial action is possible in the design of institutions concerning such a fundamental aspect of life as establishing, verifying, and proving our identities. This challenges the hegemony of government action and provides greater scope for institutional discovery of more effective ways to manage and verify identity.

III. Public Policy Implications

The policy consequences of the institutional entrepreneurial dynamics we have outlined are potentially far reaching. In the first decade of blockchains' existence, the policy response has focused on integrating blockchain applications—cryptocurrencies and initial coin offerings—into taxation and securities law (see Novak 2018a; Novak and Pochesneva 2018). But new institutional forms enabled by blockchain technology will briefly present new challenges and opportunities for the implementation of public policy. The penultimate section of this paper briefly outlines two public policy areas that blockchain technology has relevance for and that represent opportunities for future research.

A. Regulatory Oversight of New Corporate Forms

One example of such challenges is the rise of the V-form organization, where the vertical integration of a supply chain is outsourced to a blockchain (Berg, Davidson, and Potts 2018b). To the extent that industry adopts V-form organizations, we may see smaller, disaggregated firms, networked together with large-scale protocols. Smaller firms will undercut the dynamic of labor relations in economies where collective bargaining between large businesses and large unions is prevalent. Such organizational change has further complex implications for global tax competition, competition policy, and pension funds and other sovereign wealth funds that are limited to investing in the large public companies that have dominated the twentieth and early twenty-first centuries.

Berg, Davidson, and Potts (2018c) find that this "dehierarchicalization"—the competitive replacement of hierarchical organizations with decentralized governance—also potentially disrupts a longstanding regulatory dynamic that, following Marx, has

sought to tame the consequences of the concentration of power in hierarchical firms. In this argument, the growth of the regulatory state (Glaeser and Shleifer 2003) has been a response not only to the costs of opportunism in a complex economy, but also to the reduction in innovation that regulation has caused. Dehierarchicalization undercuts this dynamic, allowing for complex economic activity to be governed without the cost of hierarchical organization. As a consequence, regulatory control that seeks to tame hierarchy is no longer necessary.

B. Opportunism and Contract Disputes

We might be tempted to argue, however, that government will always have a role in regulating socioeconomic interaction within particular institutional systems to prevent or arbitrate disputes, including those implemented on blockchain-based platforms. Much public policy and regulation is designed to mitigate the costs of opportunism—that is, boundaries of potential distrust between buyers and sellers, owners, and managers. Traditionally, governments have provided the infrastructure to both enforce contracts and adjudicate disputes arising from opportunistic behavior. We can see, however, that the development of new institutions using blockchains that can complement, or compete with, the existing suite of economic institutions for regulating opportunistic behavior even here changes the appropriate balance between regulatory control and market control (Berg, Davidson, and Potts 2019).

While a number of scholars argue that the existing legal frameworks will continue to provide arbitration in a blockchain context, new, algorithmic arbitration systems and distributed jurisdictions are being developed to provide a competing service (De Filippi and Wright 2018). Blockchain offers private enterprise a new mechanism to manage and regulate opportunistic behavior. For example, smart contracts are self-enforcing. In their pure form—that is, where all triggers and conditions of the contract are managed on-chain—they do not need any external authority to enforce or otherwise manage disputes.

Of course, this is only true on the margin. Smart contracts that interface with the real, nonblockchain world—that require external triggers or involve incomplete contracts—need dispute resolution (arbitration) mechanisms. Some of those arbitration mechanisms may be provided through decentralized blockchain-based infrastructure

acting as "oracles" that work with smart contracts (Allen, Lane, and Poblet 2018).

Further, Cowen and Tabarrok (2015) have argued that technologies that allow buyers to rate sellers (such as Uber and eBay) reduce the asymmetric information that creates the market for lemons (Akerlof 1970). The lemons problem is a problem of trust that occurs when buyers have less access to information about the goods for sale than the sellers do. Blockchains provide further protection against opportunism in this context by providing a secure and validated record of such ratings. For instance, distributed ledgers can reliably link to reviews from pseudonymous identities and prevent platforms from altering reviews after the fact. At the margin, this technology implies still less need for regulation and the use of the legal system to mitigate against opportunistic behavior in the market.

IV. Conclusion

Institutions improve when they are subject to discovery processes by a variety of actors. This paper has drawn on institutional cryptoeconomics to show how, as an institutional technology, blockchain is radically expanding the scope for private enterprise and driving a process of institutional discovery.

Insofar as blockchain is allowing for more experimentation with the design of institutions that have traditionally been the province of government action, it offers significant opportunities for the improvement of the institutions that organize our society and the interactions within it. These challenges are being posed to areas of socioeconomic action that have traditionally been core functions of government. Blockchain technology makes these challenges possible. It provides infrastructure for platforms within which designed institutions may be implemented. The protocols embedded within the platform govern what is and isn't a valid interaction to be entered into the public record.

References

Akerlof, George A. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics*, 84(3): 488–500.

Al-Naji, Nader, Josh Chen, and Lawrence Diao 2017. "Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank." *Basis.io*.

Allen, Christopher. 2016. "The Path to Self-Sovereign Identity." *LifewithAlacrity.com*, April 25.

Allen, Darcy W. E. 2017. "The Private Governance of Entrepreneurship: An Institutional Approach to Entrepreneurial Discovery." Doctoral thesis, RMIT School of Economics, Finance and Marketing, Melbourne, Australia.

Allen, Darcy W. E., Chris Berg, and Aaron M. Lane. 2019. *Cryptodemocracy*. Lanham, MD: Lexington Books.

Allen, Darcy W. E., Chris Berg, Aaron M. Lane, and Jason Potts. 2018. "Cryptodemocracy and Its Institutional Possibilities." *Review of Austrian Economics* online, June: 1–12.

Allen, Darcy W. E., Aaron M. Lane, and Marta Poblet. 2018. "The Governance of Blockchain Dispute Resolution." Conference paper presented to the Australasian Law and Economics Conference. Brisbane, Australia.

Allen, Tom. 2017. "Charities Use Blockchain for Cost Savings." *V3.co.uk*.

Archambeault, Deborah S., Sarah Webber, and Janet Greenlee. 2015. "Fraud and Corruption in US Nonprofit Entities: A Summary of Press Reports 2008–2011." *Nonprofit and Voluntary Sector Quarterly*, 44(6): 1194–1224.

Berg, Alastair, and Chris Berg. 2017. "Exit, Voice, and Forking." Social Science Research Network Working Paper 3081291.

Berg, Alastair, Chris Berg, Sinclair Davidson, and Jason Potts. 2017. "The Institutional Economics of Identity." Social Science Research Network Working Paper 3072823.

Berg, Alastair, Chris Berg, Sinclair Davidson, and Jason Potts. 2018. "Identity as Input to Exchange." Social Science Research Network Working Paper 3171960.

Berg, Chris. 2017a. "Delegation and Unbundling in a Crypto-Democracy." Social Science Research Network Working Paper 30011585.

Berg, Chris. 2017b. "Populism and Democracy: A Transaction Cost Diagnosis and a Cryptodemocracy Treatment." Social Science Research Network Working Paper 3071930.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2017. "Blockchains Industrialise Trust." Social Science Research Network Working Paper 3074070.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2018a. "Institutional Discovery and Competition in the Evolution of Blockchain Technology." Social Science Research Network Working Paper 3220072.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2018b. "Outsourcing Vertical Integration: Introducing the V-Form Network." *Medium.com*, March 27.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2018c. "Capitalism after Satoshi: Blockchains, Dehierarchicalisation, Innovation Policy and the Regulatory State." Social Science Research Network Working Paper 3299734.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2018d. "Institutional Discovery and Competition in the Evolution of Blockchain Technology." Social Science Research Network Working Paper 3220071.

Berg, Chris, Sinclair Davidson, and Jason Potts. 2019. *How to Understand the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Cheltenham, UK: Edward Elgar.

Boettke, Peter, and J. Robert Subrick. 2003. "Rule of Law, Development, and Human Capabilities." *Supreme Court Law Review*, 10: 109–26.

Boris, Elizabeth T., and C. Eugene Steuerle. 2017. *Nonprofits and Government: Collaboration and Conflict*. Third edition. London: Rowman and Littlefield.

Brent, Peter. 2006. "The Australian Ballot: Not the Secret Ballot." *Australian Journal of Political Science*, 41(1): 39-50.

Breitman, K. 2017. "Why Ethereum's Hard Fork Will Cause Problems in the Coming Year." *Bitcoin Magazine*, February 3.

Buterin, Vitalik. 2013. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." *Ethereum.org*.

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

Commons, John R. 1924. *Legal Foundations of Capitalism*. New York: Macmillan.

Cowen, Tyler, and Alex Tabarrok. 2015. "The End of Asymmetric Information." *Cato Unbound* (April).

Crook, Malcolm, and Tom Crook. 2007. "The Advent of the Secret Ballot in Britain and France, 1789–1914: From Public Assembly to Private Compartment." *History*, 92(308): 449–71.

Davidson, Sinclair, Primavera De Filippi, and Jason Potts. 2018. "Blockchains and the Economic Institutions of Capitalism." *Journal of Institutional Economics*, 14(4): 639–58.

De Filippi, Primavera, and Aaron Wright. 2018. *Blockchain and the Law*. Cambridge, MA: Harvard University Press.

Demsetz, Harold. 1967. "Toward a Theory of Property Rights." *American Economic Review*, 57(2): 347–59.

Der, Uwe, Stefan Jähnichen, and Jan Sürmeli. 2017. "Self-Sovereign Identity – Opportunities and Challenges for the Digital Revolution." arXiv preprint arXiv:1712.01767.

Diener, Ed, Eunhook Suh, Richard E. Lucas, and Heidi Smith. 1999. "Subjective Well-Being: Three Decades of Progress." *Psychological Bulletin*, 125(2): 276–302.

Dow, Sterling. 1939. "Aristotle, the Kleroteria, and the Courts." *Harvard Studies in Classical Philology*, 50: 1–34.

Edelman. 2018. "2018 Edelman Trust Barometer: Global Report." *Edelman.com*.

Fremont-Smith, Marion. R., and Andras Kosaras. 2003. "Wrongdoing by Officers and Directors of Charities: A Survey of Press Reports 1995–2002." *Exempt Organization Tax Review*, 42: 25–59.

Glaeser, Edward L., and Andrei Shleifer. 2003. "The Rise of the Regulatory State." *Journal of Economic Literature*, 41(2): 401–25.

Grigg, Ian. 2017. "EOS – An Introduction." *Eos.io*, July 5.

Gropper, Daniel M., Robert A. Lawson, and Jere T. Thorne Jr. 2011. "Economic Freedom and Happiness." *Cato Journal*, 31(2): 237–55.

Gulker, Max, and Edward Peter Stringham. 2018. "The Prospects of Decentralized and Free Marketplaces with Privately Enforced 'Smart Contracts'? A Case Study of OpenBazaar." Paper presented at the Association of Private Enterprise Education, Las Vegas, April 2, 2018.

Hayek, Friedrich. 1937. "Economics and Knowledge." *Economica*, 4(13): 33–54.

Hayek, Friedrich. 1945. "The Use of Knowledge in Society." *American Economic Review*, 25(4): 519–30.

Hayek Friedrich. 1976. *Denationalisation of Money: The Argument Refined*. Auburn, AL: Ludwig von Mises Institute.

Hayek, Friedrich. 1988. *The Fatal Conceit*. Chicago: University of Chicago Press.

Heckelman, Jac C. 1995. "The Effect of the Secret Ballot on Voter Turnout Rates." *Public Choice*, 82(1–2): 107–24.

Hendrickson, Joshua R., Thomas L. Hogan, and William J. Luther. 2016. "The Political Economy of Bitcoin." *Economic Inquiry*, 54(2): 925–39.

Hendrickson, Joshua R., and William J. Luther. 2017. "Banning Bitcoin." *Journal of Economic Behavior & Organization*, 141: 188–95.

Hodgson, Geoffrey, and Thorbjorn Knudsen. 2010. *Darwin's Conjecture*. Chicago: University of Chicago Press.

Jayasinghe, Danushka, Sheila Cobourne, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes. 2018. "Philanthropy on the Blockchain." In *The 11th WISTP International Conference on Information Security Theory and Practice*, ed. Gerhard Hancke and Ernesto Damiani, 25–38. New York: Springer.

Kam, Christopher. 2017. "The Secret Ballot and the Market for Votes at 19th-Century British Elections." *Comparative Political Studies*, 50(5): 594–635.

Lawson, Tony. 2016. "Comparing Conceptions of Social Ontology: Emergent Social Entities and/or Institutional Facts?" *Journal for the Theory of Social Behaviour*, 46(4): 359–99.

Loffreto, Devon. 2012. "What Is 'Sovereign Source Authority'?" *Moxytongue.com*, February 16.

Luther, William J. 2016. "Cryptocurrencies, Network Effects, and Switching Costs." *Contemporary Economic Policy*, 34(3): 553–71.

Luther, William J. 2018. "Is Bitcoin Intrinsically Worthless?" *Journal of Private Enterprise*, 33(1): 31–45.

Luther, William J. 2019. "Getting Off the Ground: The Case of Bitcoin." *Journal of Institutional Economics*, 15(2): 189–205.

Luther, William J., and Josiah Olson. 2015. "Bitcoin Is Memory." *Journal of Prices & Markets*, 3(3): 22–33.

Martin, Adam, and Matias Petersen. 2018. "Poverty Alleviation as an Economic Problem." *Cambridge Journal of Economics*, 43(1): 205–21.

Mazet, Raphaël, and Jakub Wojciechowski. 2017. "Alice White Paper v. 0.9." *GitHub.com*.

Meeco. 2018. "Zero Knowledge Proofs of the Modern Digital Life." *Meeco.me*.

Nair, Malavika, and Daniel Sutter. 2018. "The Blockchain and Increasing Cooperative Efficacy." *Independent Review*, 22(4): 529–50.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org.

Narayanan, Arvind, and Jeremy Clark. 2017. "Bitcoin's Academic Pedigree." *Communications of the ACM*, 60(12): 36–45.

Novak, Mikayla. 2018a. "Crypto-Friendliness: Understanding Blockchain Public Policy." Social Science Research Network Working Paper 3215629.

Novak, Mikayla. 2018b. "Crypto-Altruism: Some Institutional Economic Considerations." Social Science Research Network Working Paper 3230541.

Novak, Mikayla, and Anastasia Pochesneva. 2019. "Toward a Crypto-Friendly Index for the APEC Region." *Journal of the British Blockchain Association*, 2(1): 39–45.

North, Douglass. 1990. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.

Ometoruwa, Toju. 2018. "Solving the Blockchain Trilemma: Decentralization, Security & Scalability." *CoinBureau.com*, May 16.

Ostrom, Elinor. 1990. *Governing the Commons*. Cambridge: Cambridge University Press.

Popper, Nathaniel. 2015. *Digital Gold*. London: Penguin.

Popper, Nathaniel. 2016. "A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency." *NewYorkTimes.com,* June 18.

Rennie, Ellie, and Jason Potts. 2016. "The DAO: A Radical Experiment That Could Be the Future of Decentralised Governance." *TheConversation.com*, May 11.

Rooney, Patrick M., Xiaoyun Wang, and Mark Ottoni-Wilhelm. 2018. "Generational Succession in American Giving: Donors Down, Dollars per Donor Holding Steady but Signs That It Is Starting to Slip." *Nonprofit and Voluntary Sector Quarterly*, 47(5): 918–38.

Scott, James. 2008. *Seeing Like a State*. New Haven, CT: Yale University Press.

Searls, Doc. 2012. "Sovereign-Source vs. Administrative Identity." *Blogs.Harvard.edu*, March 25.

Selgin, George A. 1988. *Theory of Free Banking*. Lanham, MD: Rowman and Littlefield.

Sen, Amartya. 1999. *Development as Freedom*. New York: Knopf.

Sovrin. 2018. "Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust." *Sovrin.org*.

Stringham, Edward. 2015. *Private Governance*. Oxford, UK: Oxford University Press.

Szabo, Nick. 1994. "Smart Contracts." *fon.hum.uva.nl/rob*.

Torpey, John. 2000. *The Invention of the Passport*. Cambridge: Cambridge University Press.

van Saberhagen, Nicolas. 2013. "CryptoNote v 2.0." *Cryptonote.org*.

White, Lawrence. 1999. *The Theory of Monetary Institutions*. Hoboken, NJ: Wiley.

White, Lawrence. 2015. "The Market for Cryptocurrencies." *Cato Journal*, 35(2): 383–402.

Williamson, Oliver. 1975. *Markets and Hierarchies*. New York: Free Press.

Williamson, Oliver. 1985. *The Economic Institutions of Capitalism*. New York: Free Press.

Wood, Gavin. 2014. "Ethereum: A Secure Decentralised Generalised Transaction Ledger, EIP-150 Revision." *GavWood.com*.