Markets for rules: the promise and peril of blockchain distributed governance

Nick Cowen, School of Social and Political Sciences, University of Lincoln

Forthcoming in the ***Journal of Entrepreneurship and Public Policy***

Abstract

Purpose: Explore the possible contributions of blockchain technology to creating new governance structures that facilitate social cooperation.

Methodology: Conceptual analysis with key ideas in new institutional economics and political theory.

Findings: Blockchain technology provides a new tool through which political entrepreneurs can credibly alienate some of their power within a system of rules that they have established.

Originality: Links discussion of blockchain entrepreneurship in commercial markets to research into private governance and political thought.

Keywords

Blockchain, cryptocurrency, private governance, new institutional economics, political entrepreneurship, liberalism, limited government

1. Introduction

Classical liberals seek the paradoxical: government powerful enough to protect individuals from preying off each other, but limited enough to prevent it becoming a fierce predator itself (Buchanan, 2000). Theory and history show us two promising related solutions. The first is constitutional government establishing legal protections for persons and their property along with procedural constraints to prevent officials from abusing their positions (Buchanan and Congleton, 2003; Hayek, 2011). The second is competitive jurisdictions that allow individuals to select their rulers, thus disciplining governments that fail in their legitimate role (Buchanan, 2001; Hirschman, 2004; Weingast, 1995). At the radical limits of these approaches, the classical

liberal project blends with the anarchist and libertarian projects of having government exclusively by consent and contract (D'Amico, 2012; Leeson, 2014; Meadowcroft, 2014; Nozick, 2013). Where successfully adopted, even in piecemeal and uneven fashion, these solutions have been responsible for the remarkable peace and prosperity witnessed in what is commonly called the developed world (McCloskey, 2007; Shleifer, 2009). But they have still failed in their endeavor to prevent government, local, national and international, from being the single biggest threat to individual liberty and prosperity.

Against this backdrop, blockchain could turn out to be what Davidson *et al.* (2018, p. 640) and Berg *et al.* (2018, p. 386) describe as a new 'institutional technology' that supplements existing forms of market governance and may eventually offer political actors a more effective way to limit government. Blockchains offer a more secure and transparent way of implementing rules while permitting individual choice between rulesets that can co-exist at the same time and place. What this could ultimately mean is that a great deal of what has traditionally been conceived as governance might be disintermediated from the territorially defined monopolistic coercive authorities that classically define states. James Buchanan (2000, chap. 8) imagines an ideal constitutional government to be a programmable agent that once established mechanically enforces the rules of the social game. What blockchains can do is bring that thought experiment a little closer to reality. With lower barriers to producing and choosing self-enforcing rulesets, the project of seeking better governance can come closer to the competitive discovery procedure that, as Hayek (1976, 2014) identifies, consistently produces enormous social gains in the provision of other goods and services.

How can government be reasonably conceived as an enterprise potentially subject to competition? In making this a point of departure, this paper draws on private governance, a buoyant sub-field of New Institutional Economics (NIE). Central to NIE is the study of transaction costs (Coase, 1937; Williamson, 1985). The basic premise is that people possess enormous potential to cooperate in productive ways, but in the absence of systems of co-ordination, lack the necessary knowledge and mutual trust to succeed. In other words, there are prohibitive transaction costs to successful cooperation that institutions (that is durable norms and laws) can reduce, mediated by other factors such as culture, available resources and technology.

NIE's focus on transaction costs permits a more refined understanding of the paradox facing classical liberalism. The key challenge of liberal political economy is designing protective and productive institutions (those that lower transaction costs for ordinary people) in such a way that political elites are incentivized to supply those institutions, and not simply exploit their privileged position to extract rents from the population (Acemoglu, 2003). From this realistic standpoint, it is not enough simply to know what rules would work best between equals. The presently powerful must be persuaded that it is in their interests to abide by rules they set for others, as well as assure ordinary people that the powerful will hold up their side of the bargain.

Through this lens, scholars have conceptualized the challenges that political actors face as paralleling the kind that private actors must solve when attempting to cooperate. The private governance research program proposes that establishing and enforcing governing rules is a kind of enterprise undertaken by people who see opportunities for profit from supplying order to a community, and thus end up solving widespread challenges to cooperation (Leeson and Boettke, 2009). There is an anti-establishment anarchic bent to this literature insofar as it conceives even modern states not as intrinsically noble enterprises aimed at achieving the public good but more as the unintended beneficial result of the successful organized violence of the past whose resulting political settlements have been refined so as to spread the gains of social order to a wider population (North et al., 2009; Skarbek, 2014). From this perspective, whether a governing institution is formally considered a state or part of the state, as opposed to a private organization, does not establish a particularly important distinction since state legitimacy is often founded on agreements between self-interested, powerful private actors (Salter, 2015a, 2015b) while private association often end up producing widespread social good more normally associated with public activity (Stringham, 2015). Despite this profound skepticism of the inherent legitimacy of political authority and individuals who seek political power, underlying this research agenda is a fundamental recognition of the value of fixed rules, especially those that provide for the ownership and exchange of property, and enforceable contracts for goods and services. So there is recognition of the positive contribution that relatively well-ordered states have made to human welfare.

In addition to these concepts from private governance, this paper uses an older idea from political thought: the lawgiver,[1] someone who establishes a fundamental new governance regime. This role bares a close resemblance to the role of the political entrepreneur in the private governance literature. On my account, what blockchains offer is a new mechanism by which a lawgiver can selectively alienate themselves from some of their power and thus commit not to predate off their subordinates in the future. In the ideal, they could alienate their elite status altogether and become subject to the exact set of institutions that are enforced equally on all members of a community. But leaving utopian ideas aside, as it stands, changing governing rules either implies violent revolution or costly contestation within a democratic process. Neither approaches look anything like a competitive market and offer little guarantee of improvement over a *status quo*. In essence, blockchains are a technology for lowering at least some of the formidable transaction costs associated with moving from one set of rules to another. My account has parallels with Catalini and Gans' (2018) account of blockchain as a technology that lowers costs associated with verification and networking in commercial setting. I extend this idea to include costs associated with establishing credibility and assurance between rulers and ruled.

This explanation for the role of blockchains for the liberal enterprise proceeds as follows. The paper continues with a description of the characteristics of blockchain technology, including what has made it suitable for developing cryptocurrencies, autonomous systems of monetary exchange that are supposed to replace state-backed currencies. Then it discusses how this technology can facilitate other ways of reducing transaction costs over physical distance and in absence of personal trust, especially establishing contracts and record-keeping. It illustrates the particular power of blockchains' decentralized process to challenge bad policy with an example of it filling gaps in regulation left by the refusal of governments to supply legal protection and security to sex workers. Then it discusses how this experience can be applied to the wicked problem of contracting between political elites and subjects when it comes to establishing government itself. It ends with a discussion of some vulnerabilities facing political reformers

[1] The term lawgiver is used here as it is sufficiently general as to include political actors operating as part of state government as we presently understand it, while leaving open the possibility of rule-making actors operating outside of state authority. It also refers to the classical concept of the lawgiver as constitutional founder found in Aristotle (1981) and Rousseau (1923). The potential institutional ramifications of blockchain technology are sufficiently revolutionary that their explanation is best understood with reference to fundamental problems and models in political thought. Section 4 has more detailed explanation of the role of the lawgiver in this explanation for the contribution of blockchain technology to governance.

who wish to use blockchain governance in a democratic direction, and some ways that contemporary policymakers can use blockchain technology to improve the quality of governance.

2. What is a blockchain?

The precise definition of a blockchain is contested, as is often the case for innovations that are partly conceptual. However, they are essentially the combination of two technologies that are already widely used. The first is distributed ledgers, publicly shared databases of transactions that are replicated and shared across networks. The second is asymmetrical cryptography (the use of paired public and private keys) which allows for the secure transmission of transactions across a public network that are only accessible to a recipient holding the correct private key.

These transactions are secured through participating nodes on the network algorithmically generating hashes that are periodically added as a new block. A hash is a string of data of consistent (relatively short) length that acts as a unique identifier that can validate the transactions that were recorded in making it. This result is that, unlike other shared ledgers, transactions recorded on a blockchain cannot be singled-out, manipulated or reversed by any authority once added (Böhme et al., 2015).

In this early and evolving sector, classifying different kinds of blockchains is a significant challenge. Davidson *et al.* (2018, pp. 642–646) have made a valuable contribution to this task by distinguishing the core discovery. The original blockchain, Bitcoin, and several others are essentially a *public ledger* where copies of the underlying history of transactions are disseminated throughout a network rather than being possessed by a trusted state or corporation. The cryptographic rules generate a *consensus engine* which ensures all the network nodes agree on what transactions took place as they are added to the growing record. With the addition of a programmable scripting language, a *public ledger* can be turned into *a smart ledger*, of which Ethereum is currently the most prominent example. This is a publicly accessible chain that stores not only data, but executable programs and applications that are publicly readable and secured in such a way that users can be confident they will execute predictably given the correct inputs. This is the basis for smart contracts, essentially exchanges of value or control rights that are agreed and complete automatically when one party delivers a particular input.

What makes blockchains interesting from the perspective of private governance is that they can function like constitutional rules, dispersing rights and powers to configure elements of a shared environment, and introducing constraints on each actor's behavior (Rajagopalan, 2018). However, traditional constitutions require a human administration that is committed to enforcing the rules in particular cases to work (paradigmatically a state administration in large communities). It is easy for such an administration to end up enforcing rules and rights selectively. By contrast, due to the crypto-embedded nature of individual events on the blockchain, the discretion that individuals have to selectively enforce (or reverse) such events or decision is substantially reduced. Participants can ignore the results of interactions within a blockchain altogether (and cease supporting it), or they can accept them more or less as a whole. This broadens the scope for maintaining procedural integrity and general enforcement without relying on particular individual officers to do the enforcing in an impartial way.

2.1 Use as currency

To better explain this use of blockchain technology, it is perhaps best to compare it to cash. This is apt because the initial aim of blockchain development has been as cryptocurrency, monetary systems resistant to manipulation and surveillance, especially by governments. Cash notes are easily transferable artefacts denoting value. Notes are almost perfectly interchangeable with each other so it is impossible to decode or unravel the series of transactions that have led to you having that note in your hand. They are self-certifying. Having cash in your hand is sufficient to establish that you possess its value. There is no need for anyone to check your personal ownership of the note against a central authority such as a bank, as is the case for credit and money transfers. Indeed, it is for these reasons that governments and policymakers have increasingly come to treat cash with such suspicion despite it being such a useful ally of state capacity in the past. Police in many jurisdictions are now authorized and encouraged to arbitrarily seize suspiciously large cash holdings. Government policies increasingly encourage people to use transfers and savings mechanisms whose legitimacy are ultimately determined by some reachable authority.

So how does cryptocurrency differ from cash? Cash is difficult to forge but far from impossible. This necessitates criminal prohibition and expensive schemes of enforcement to secure its value. Although lightweight and convenient, cash is still physical with inevitable additional costs to

transfer (especially over large distances). By contrast, cryptocurrency can be transferred instantaneously across the Internet and stored discreetly on portable digital media. Unlike electronic money orders, personal access to a cryptographic artefact (through a private key) is what determines ownership. There is no other agent that has to recognize its authenticity for it be valid. These artefacts are also essentially impossible to forge as they are validated against a constantly updated public record.

Critically, no central agency is capable of unilaterally creating and spending new currency. The blockchain records transactions through nodes processing new blocks as part of a network. Blockchain schemes permit 'mining' which produces new artefacts through a computationally intensive hashing algorithm but this activity is accessible to anyone participating in the network. New blocks are created according to pre-established rules that the blockchain designers themselves cannot unilaterally manipulate once it is part of a larger network. Unlike state-backed fiat currencies, or bank credit systems, no agent stands behind the process to offer some final backing. Instead, it is the collective production and consensus formation of the network based on fixed rules that determines holdings. It is ultimately the participants in the network that constitute the system and its value. Currency issuance, previously the preserve of powerful elites, could instead be subject to significant competition and public participation.

2.2 Use for purchases and contracting

As described above, blockchains do not only provide exchangeable artefacts that are highly resistant to forgery. They also create a permanent, growing record of all transactions. So thinking back to the cash comparison, imagine that when you are handed a cash note, not only is it a self-certifying artefact of value, but that on inspection you can quickly see the transaction history of the note from when it was printed to the point you received it (cf. Kocherlakota, 1998). This has the disadvantage of reducing the anonymity of the exchange as the transaction history of each artefact, and each entry on the public ledger, is unique (Biryukov et al., 2014). But it also opens up a lot more potential uses for these blockchain artefacts than currency alone.

Software designers and entrepreneurs are starting to exploit this feature. In principle, it is possible to validate any information against a blockchain. This can include identity documents, digital signatures, as well as media files. So association with a block can be used to validate the time and place of production as well as establish title over digital information. It is also possible

to set up conditional transactions. For example, an artist could setup a scheme to release a piece of media automatically on receipt of a certain monetary value. The release could be limited to specific recipients or made free to the public once a certain value is pledged by purchasers acting independently. Indeed, the majority of transactions on the Ethereum blockchain now take the form of smart contracts such as these.

Entrepreneurs are also beginning to work out how to integrate such systems into the provision of 'real-world' goods and services (Zhao et al., 2016). For example, a decentralized replacement to Uber or Lyft could automatically construct a smart contract that pays a driver on condition that a passenger (with a blockchain integrated app on their smartphone) is delivered to their destination. This is without the need for a company middleman. One currently active decentralized enterprise allows air travelers to insure against flight delays by paying into a decentralized insurance pool.[2] The insurance policies pay out automatically according to public online flight data. The upshot of these experiments could be the replacing of many traditional firms, with human owners and managers, with decentralized autonomous organizations (DAOs): mutual participatory schemes that establish individual roles, duties and payoffs through transparent self-executing rules built into computer code rather than hierarchies.

3. Decentralization to avoid prohibition

DAOs might be able to replace the human management layer of some firms. But what are the implications of DAOs for the provision of governance in particular? Technology firms already provide a great deal of governance services. But these firms up until now have relied critically on a centralization of administration to establish an organized network that lowers transaction costs. This creates both an opportunity for monopoly profits from whoever has built the network. As Catalani and Gans (2018) have argued, this presents a problem in itself as, absent effective competition, it permits private platform-owning incumbents to censor and degrade services. Moreover, it also presents an obvious target for authorities that wish to exert control over the system. As a result these systems of governance inevitably become entangled with state authorities (Allen et al., 2018; Wagner, 2016). For example, mass surveillance of a weakly connected population relying on lots of small and informal schemes to communicate is a very

[2] https://etherisc.com/

costly affair. But it is quite different once a population is carrying smart devices built by a handful of firms, served by a few telecommunications companies and a dozen major content providers. Then it is relatively easy for state actors to identify a number of strategic choke points that allow them access to vast amounts of information about people's public and private lives. These points in the system are controlled by firms that can be easily coopted to achieve political ends or threatened should they refuse to cooperate.

The vulnerability of technology-aided private enterprise to unilateral state regulation is illustrated by the recent prohibition of advertising for sex work following the passing of the FOSTA-SESTA acts by the United States government and the resulting seizure of *Backpage*, a website and platform that helped sex workers to meet and vet their clients (Q, 2018). Suppressing sex work can be costly and unpopular. It involves sending police to harass an economically marginalized group (usually female sex workers) as well as prosecuting members of the public who are willing to pay for sex. It is, however, much easier to prohibit platforms that facilitate sex work: to ban the advertising and remote coordination of sex work services. This can be expected to have a substantial negative impact on the sector as sex workers have become increasingly reliant on technology to secure their safety when meeting clients (Sanders et al., 2018). In this case, the state not only refuses to facilitate transactions between consenting adults on spurious moral grounds but, in addition, can prevent anyone else from creating a private governing framework that allows such transactions to take place with relative safety.

Critical to this strategy of prohibition working is the reliance of individual market participants (sex workers and clients) on platforms. Up until now, these platforms had a personal or commercial owner that can usually be identified and punished by state officials. By contrast, DAOs, once released, have no owner and persist through the decision of individuals to participate in them. If these individual participants are able to coordinate enough to get this practice initially off the ground, then the state has to go back to the costly practice of identifying individual users to punish rather than a central owner who can be publicly identified and punished as a 'criminal exploiter' in their role as middleman. This system would not be able to be shut off at a single point. A blockchain start-up, Spankchain[3] is entering this sector and may

[3] https://spankchain.com/

eventually provide a critical replacement for sex workers seeking a safe and secure framework for marketing their services out of reach of state regulation.

4. Prospects for political entrepreneurship

The potential to replace some traditional firms with DAOs is enough on its own to indicate the disruptive potential of blockchains, precisely because DAOs can better resist regulation from state authorities. Indeed, blockchain organizations are already being used to ameliorate the worst cases of government failure, for example in the case of currency collapse in Venezuela (England and Fratrik, 2018). This is without any pretense of taking over traditional state functions under ordinary circumstances. But technology that disrupts the formation of firms in such a fundamental way as blockchains might be able to similarly challenge states before too long.

The 'business' of government is supplying the peace, law and order necessary for ordinary people to engage in mutual cooperation. This is traditionally achieved through establishing a territorial monopoly on the use of violence. The challenge that a sovereign government faces is eliciting economic production from the land and people under her control. Paradoxically, this is no easy feat for an absolute sovereign facing little internal or external competition. Even if she wants to encourage productive activity, she has little means to credibly show she will not expropriate the fruits of her people's labor (Ma and Rubin, 2019). That is, unless she is willing to alienate at least some of her power which could also undermine the security of her position as sovereign, a dangerous proposition when the control over legitimate violence is at stake (Bueno de Mesquita et al., 2005). Even if the possibilities of productive exchange between ruler and ruled is widely acknowledged, the institutions that benefit both sovereign and the people can be hard to reach through a series of decisions that make rational sense at each stage to both parties.

In a well-functioning market economy, credibility amongst private actors can be assured through the state protecting people's property and enforcing voluntary contracts. But no such mechanisms are available to facilitate exchanges of rights and duties between the sovereign herself and her subjects. The historical record suggests that credibility can be established either when subjects have independent capacity to exit unfair arrangements or when external threats (such as the existence of enemy states that threaten subject and sovereign alike) happen to bring their interests together (Salter, 2015b). This is why the history of liberal political economy is one

of elites and citizens grappling and fumbling towards mutually beneficial arrangements that very occasionally, and mostly by good fortune, turn out to be stable.

The same challenge of reaching a fair and successful political settlement between an elite and the people crops up under slightly different descriptions throughout the history of political thought when examining the founding of new regimes. This was a challenge for Rousseau in particular who in *The Social Contract* envisaged an ideal society based on democratic equality where each citizens follows the general will: the common and true interests of an entire body of people (Rousseau, 1923, bk. 1 Ch 6). Although certainly not a classical liberal project aiming at limited government, Rousseau's polity faces the same vexing issue of transition: how to reform the laws of a corrupt regime when the laws themselves habituate citizens to shirking their duties, leaving them unable and unfit to rule themselves effectively (Rousseau, 1923, bk. 2 Ch 6). Rousseau's answer, a *deus ex machina* figure, is that a successful regime-change or democratic reform requires a special individual: a lawgiver[4] who establishes new laws that drives out corruption and allows the people to transition to true self-government (Rousseau, 1923, bk. 2 Ch 7).

The key challenge is getting a lawgiver with the power to defeat corruption within the people while driving out external threats; the knowledge to enact with care the laws best suited to the new polity; yet at the same the strength of moral commitment not to exploit her privileged position; and willingness to step down at the right moment. The responsibility and skill required of the lawgiver as Rousseau outlines seem to require virtually divine qualities.[5] The problem for any lawgiver is that the ability to change the law or control its execution after establishing a new constitution involves an overwhelming temptation to corruption, to end up favoring oneself and one' associates. Any new regime, where credible norms of public spiritedness and general legal constraints have yet to be established, is particularly vulnerable to fall back into opportunistic predation within the political sphere. Rousseau drew from the quasi-mythological figures of ancient Greek founders, as well as several Italian city states, to propose that the closest you can get to a non-divine lawgiver is often a foreign founder (Rousseau, 1923, bk. 2 Chapter 7). The advantage of a foreign lawgiver is that she has fewer personal interests in the area where the

[4] This is sometimes translated as 'legislator'. 'Lawgiver' helps to distinguish the constitutional founder from legislators in representative governments that Rousseau did not consider to be the same role.
[5] Unsurprisingly, this legendary persona that represents the true interests of a presently corrupted people has also been deployed to support some of the most authoritarian political movements in modern history.

regime is established and can credibly assure the people that she will depart when the time is right. She can act more effectively as a more neutral arbiter between factions and interests, and then execute judgement from a position of independent. Honig (2001) shows that the 'foreigner as founder' myth crops up repeatedly from ancient to contemporary fiction, including in such diverse places as the Western movie *Shane* and the *Wizard of Oz*, and that establishing several successful modern constitutional regimes has often involved having foreigners in positions of power. All this reminds us how important and special the lawgiver is for developing well-performing institutions. Yet it also shows how her effectiveness relies not just on her intrinsic qualities but the circumstances in which she finds herself and her particular background. We are reminded that the process of political reform relies on accidents and fortunes of history.

How can blockchains help with overcoming these challenges to establishing the circumstances in which a lawgiver can demonstrate some of these rare qualities? In essence, blockchain institutions means that the circumstances in which a lawgiver could act to introduce impartial rules is wider than has traditionally been possible. First, they offer a new way of tackling the assurance problem between the governor and the governed. Traditional laws have to be enforced continuously by inevitably partial and fallible human agents. Worse, those in power can ultimately renege on their commitments to abide by them. By contrast, a lawgiver acting as an entrepreneur with blockchain programming knowledge can develop a ruleset, release it, and then stand down from their privileged institutional position. If the ruleset is advantageous to social cooperation, then people will start participating in the scheme and its use will spread.

A traditional political entrepreneur (very often a conqueror) profits from their enterprise by establishing the authority to tax others. By contrast, a law-giving entrepreneur with a blockchain constitution can set aside some assets or tokens associated with their governance structure for themselves. If their structure is successful, then those assets will become valuable and exchangeable for ordinary goods and services. Just as a private entrepreneur can look forward to reaping a profit by selling off an asset they have developed, this offers a way for a governance provider to 'cash' out their investment in rulemaking.

Second, decentralized systems can be designed to be somewhat resistant to entanglement with existing political authorities. Once a designer releases a blockchain to the public, it is no longer under their control. Hence there is no individual to co-opt, threaten or manipulate. The successful

lawgiver does not need to stand apart from the regime so as not to be corrupted but, without any additional power over others, blends back into the society as an ordinary citizen. This means that any lawgiver, and not just a foreigner who finds themselves in the circumstances of being able to enact reform, can credibly commit to leave their position. Moreover, anyone with knowledge of blockchain programing can design and reform governance systems. It will be impossible to suppress a successful ruleset as it can be easily reproduced. So changing the rules to reflect narrow interests after the fact will be much harder.

Finally, because of their nature as digital media, blockchains can facilitate rapid competition between rulesets. They rely very little on physical infrastructure or human administrators for efficacy as states traditionally do. As a result, there is little physical limit to how many of these schemes can be in operation simultaneously. They can be made interoperable: blockchains can be established so that they can read data off each other. Blockchains can also be cloned privately and edited before being re-released. They do not have to be built each time from scratch. So when one particular system fails or requires upgrading, people can switch to a new one with different rules but with the same private keys accessing the same parts of the new public ledger based on the previous iteration. This means that the rules of the game going forward can be changed by the mutual consent of participants moving to a new blockchain (Markey-Towler, 2018). This can happen without displacing the particular positions and entitlements of the existing participants.

These three contributions from blockchain technology can bring us closer to an ideal of private governance. Government itself can start to become subject to the relatively rational and benign principles of commerce rather than the coercive processes of politics.

5. Vulnerabilities of blockchain governance

This paper has painted quite a rosy future for blockchain based governance so far. But blockchain users face distinct vulnerabilities as well, and these will probably bite the more apparent the revolutionary potential of this technology becomes. An obvious issue is physical theft of private keys, as well as hacking computer systems in order to steal private key information. Hacking has proved to be a particular problem because of the unanticipated emergence and popularity of blockchain exchanges that hold digital assets on behalf of users. These exchanges function rather like banks for traditional currencies with all the usual security

concerns but operate across national boundaries and without specific legal protections. One exchange, Coinbase has attempted to ameliorate this vulnerable position by keeping 99 per cent of its assets inaccessible to the Internet, with the remaining 'live' one per cent insured by Lloyd's of London (Fung, 2018).

Another problem is that ownership within blockchains are currently extremely lumpy with a handful of 'whales' heavily invested in both assets and the specialized hardware for mining new blocks. This problem is compounded by the high-energy requirements for economically productive mining. At a certain scale, these market actors can distort the participatory hashing process by refusing to validate some transactions. As a result, a critical challenge for designers is working out network rules that minimize the use of energy resources and punish badly behaved network nodes by withholding mining fees from actors that deviate from generating blockchain consensus.

5.1 Democratic conceits

Besides external hacking from outside a ruleset, a key challenge is developing code that cannot be manipulated within the rules of the game itself. The most prominent failure so far was the first DAO whose code was exploited to transfer assets to a single account and then exchanged out of the system (Dhillon et al., 2017). The flaw in the code was the result of attempts to integrate participatory voting into the decision process along with constraints to prevent the majority from exploiting the minority. Catastrophic failures such as these are forcing blockchain designers a to discover fundamental insights already well-known in social choice theory that show that no open-ended decision procedure outside of dictatorship is immune to manipulation or chaotic outcomes (Arrow, 1950; Boettke and Leeson, 2002). This does not imply that introducing democratic processes into a blockchain governance mechanism is impossible or unwise, only that designers must be particularly alert to the problem of outcome-manipulation within democratic rules in the absence of trust. This is a particular challenge in anonymous governance schemes because there are few constraints on self-dealing (people can make use of multiple private identities which is harder in physical interactions). An important step in making blockchain democratic processes resistant to manipulation will likely include the promulgation of a credible self-sovereign identity scheme (Der et al., 2017).

In the meantime, attempts to integrate classic democratic mechanisms like majority voting into blockchain governance could show premature ambition. Blockchain governance solutions do not lack for democratic credentials even without formal voting mechanisms or systems of representation. Blockchains allow a wider range of people not only to propose new governing rules, but also to implement and test them. Meanwhile, it allows people to select the rules governing their interactions much more easily. In this sense, a blockchain ecosystem helps to tackle the perennial problem of agenda-setting and manipulation of more traditional democratic processes. In this context, the process of writing and implementing particular rulesets does not need to be conducted by vote or committee for the process to be democratic in this broad sense of reflecting and responding to the interests of participants in the governing scheme.

Classical liberals emphasize the power of exit from political arrangements as a necessary part of political accountability (Pennington, 2010). Blockchain schemes allow people to exit without needing to use their actual feet as often. In comparison, voting, especially at large scale, can often be an ineffectual way of providing feedback to a system or holding rulers to account. To be successful, blockchain governance entrepreneurs should approach democratic mechanisms with great care while recognizing that processes of competition can play a substantial role in holding the relatively powerful to account.

6. Policy implications

What should the response of state regulators and other more traditional political actors be to the emergence of blockchains as a new institutional technology? A significant portion of early participants in blockchain saw the movement as a direct challenge to state government and an anarchist strain is still prominent in contemporary innovators in the field. Satoshi Nakamoto (2008) launched bitcoin out of dissatisfaction with the way that state-backed central bankers manage fiat currency with the intent of providing a means of exiting existing monetary regimes in favor of an entirely new currency system. This paper too places some emphasis on the way that blockchain technology allows for extra-legal governance that challenges existing policy priorities, especially in the way that a decentralized governance regime can protect transactions (such as those involving consensual sex work) that state authorities do not wish to facilitate or actively wish to discourage. So it might appear that the interests of existing political authorities

are necessarily at odds with any new governing mechanism that blockchain technology causes to emerge (cf. Berg, Markey-Towler, et al., 2018).

That interpretation of this account would be an over-simplification. From the perspective of private governance, there is little difference in kind between public officials and governance provided through private means and civil society. The ability to choose to place credible constraints on one's conduct dramatically expands the scale and scope of cooperation regardless of one's formal institutional position. This is precisely what makes the protection of property and the ability to enforce contracts valuable for a community. This basic insight applies to traditional political actors as much as private citizens or radical reformers. This is also reflected in historical analysis of political development that suggests that both the scope and complexity of market exchange has grown in parallel to state capacity and that the two are often mutually supporting (Johnson and Koyama, 2017). It plausible for an institutional technology like blockchain to simultaneously facilitate the growth of market exchange while also helping to expand the protective and productive capacities of the state.

So there is not necessarily much to fear and instead quite a lot of new opportunities for policymakers to use blockchains to supply public services more effectively. For the time-being, during this initial period of experimentation and innovation, prudent policymakers should allow the new sector to develop and refrain from introducing prohibitive regulation, especially those that attempt to slot blockchain artefacts into inappropriate regulatory architecture. Formal legal recognition (rather than direct regulation) of prevailing blockchain entities and practices might be useful for signaling that the sector has a role in the legitimate economy and encouraging mainstream commercial entrepreneurs to enter the sector. An example of this approach is found in Wyoming where the state legislature that has attempted to pre-empt federal regulatory interest in defining blockchain assets as securities (which would place significant limits on who is permitted to hold them), by defining digital assets as real property and money (Bain, 2018). Similarly, Ohio has announced that it welcomes tax payments in Bitcoin and this is likely to help facilitate the growth and legitimacy of blockchain ventures (Vigna, 2018).

Even at this relatively early stage, there are some more direct ways in which blockchain technology might be used to facilitate better public governance. A promising use-case is enhancing the way that private data can be shared securely and voluntarily with government

agencies (Allen et al., 2018). Both public services and private companies alike make systematic use of sensitive private data, and both frequently lose or corrupt data in ways that can end up harming individuals. Information about citizens is useful (occasionally critical) for making service provision more effective. In the public sector, things like the sharing of patient medical data across a health system and to allied social and welfare services can save and improve lives. At the same time, the widespread dissemination of personal information about health, wellbeing and lifestyle can violate dignity and make people vulnerable to fraud and exploitation.

The way that official databases are organized typically renders vast amounts of data accessible in general to an unnecessarily large number of individuals. As a result, it is quite easy for data to be lost, stolen, sold to third parties, changed in error or in unauthorized ways. The way that the data is collected and stored in what can amount to a common pool means that it is amenable to function creep. For example, health-service data can be deployed to aid immigration enforcement or policing. The fact that this can happen means that some citizens reasonably fear sharing data with any government agency. This makes some citizens fearful of giving data even for legitimate public uses. We can conceive this current situation as an example of the assurance problem outlined in the previous section. It is in the interests of both citizens and government to share data. But government agencies lack the credibility that the data will only be used to protect citizens and produce public goods. The data can also be used in exploitative or predatory ways.

Blockchain technology can provide more opportunities for citizens to hold authorities accountable for failures to uphold data security (Muzammal et al., 2019). The blockchain can allow database information to be distributed in a secure format across the Internet so there is less reliance on a single organization to keeping it accessible and ensuring it is free of errors. Storing it cryptographically can render it impossible to decrypt the whole database and steal data *en masse*. Access rules can be refined and customized so that data records are only accessible with permission from the user or authorized controller. In addition, by offering access to a permanent, growing history, it can be possible to track exactly when and where a data record has been accessed, and how and when it has been amended. Hence, blockchains can contribute to assuring data protection *by design* rather than by policy or administrative procedure. It reduces the amount of trust in other institutions required to keep data secure (Davidson et al., 2018, p. 644). It is thus a promising development that the State of Colorado recently passed legislation

encouraging their local government agencies to consider using encryption and blockchain for public recordkeeping (Huillet, 2018).

7. Conclusion

Unlike many other social processes, governments have yet to be subject to an effective competitive discovery procedure. This is because of the huge transaction costs associated with transitions from one set of rules to another, especially the challenge of establishing credible commitments with actors whose power is based on existing rulesets. Blockchains offer a path to competitive governance because they allow people to create and participate in self-enforcing rulesets. They can be copied and reformed quickly and can co-exist much more easily than traditional governance structures.

Blockchains have already produced promising applications for navigating around government regulation that fails to serve the interests of market participants. Imaginative policymakers and reformers are starting to explore ways of using blockchains to contribute to public service provision by helping to generate credible commitments about the way personal data will be used by authorities. Before too long, blockchains might begin to subject core aspects of government itself to competition.

References

Acemoglu, D. (2003), "Why Not a Political Coase Theorem? Social Conflict, Commitment and Politics", *Journal of Comparative Economics*, Vol. 31 No. 4, pp. 620–652.

Allen, D.W.E., Berg, C. and Novak, M. (2018), "Blockchain: an entangled political economy approach", *Journal of Public Finance and Public Choice*, Vol. 33 No. 2, pp. 105–125.

Aristotle. (1981), *The Politics*, Rev. ed., Penguin Books, Harmondsworth, England New York, N.Y.

Arrow, K.J. (1950), "A Difficulty in the Concept of Social Welfare", *Journal of Political Economy*, Vol. 58 No. 4, pp. 328–346.

Bain, B. (2018), "Wyoming Aims to Be America's Cryptocurrency Capital", *Bloomberg Businessweek*, 15 May, available at: https://www.bloomberg.com/news/articles/2018-05-15/wyoming-aims-to-be-america-s-cryptocurrency-capital.

Berg, A., Markey-Towler, B. and Novak, M. (2018), “Blockchains = Less Government, More Market”, *SSRN Electronic Journal*, available at:https://doi.org/10.2139/ssrn.3301714.

Berg, C., Davidson, S. and Potts, J. (2018), “Blockchains as Constitutional Orders”, in Wagner, R.E. (Ed.), *James M. Buchanan*, Springer International Publishing, Cham, pp. 383–397.

Biryukov, A., Khovratovich, D. and Pustogarov, I. (2014), “Deanonymisation of Clients in Bitcoin P2P Network”, presented at the ACM Conference on Computer and Communications Security, ACM Press, pp. 15–29.

Boettke, P.J. and Leeson, P.T. (2002), “Hayek, Arrow, and the Problems of Democratic Decision-Making”, *Journal of Public Finance and Public Choice*, Vol. 20.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), “Bitcoin: Economics, Technology, and Governance”, *Journal of Economic Perspectives*, Vol. 29 No. 2, pp. 213–238.

Buchanan, J.M. (2000), *The Limits of Liberty: Between Anarchy and Leviathan*, Liberty Fund, Indianapolis.

Buchanan, J.M. (2001), “Criteria for a free society”, *Federalism, Liberty, and the Law*, Liberty Fund, Indianapolis, Ind, pp. 173–184.

Buchanan, J.M. and Congleton, R.D. (2003), *Politics by Principle, Not Interest: Toward Nondiscriminatory Democracy*, Liberty Fund, Indianapolis.

Bueno de Mesquita, B., Smith, A., Siverson, R.M. and Morrow, J.D. (2005), *The Logic of Political Survival*, 1. paperback ed., MIT Press, Cambridge, Mass.

Catalini, C. and Gans, J.S. (2018), *Some Simple Economics of the Blockchain*, Working Paper No. 22952, National Bureau of Economic Research, Cambridge Massachusetts.

Coase, R.H. (1937), “The Nature of the Firm”, *Economica*, Vol. 4 No. 16, p. 386.

D’Amico, D.J. (2012), “Comparative political economy when anarchism is on the table”, *The Review of Austrian Economics*, Vol. 25 No. 1, pp. 63–75.

Davidson, S., De Filippi, P. and Potts, J. (2018), "Blockchains and the economic institutions of capitalism", *Journal of Institutional Economics*, Vol. 14 No. 4, pp. 639–658.

Der, U., Jähnichen, S. and Sürmeli, J. (2017), "Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution", *Arxiv.Org Pre-Print*, p. 6.

Dhillon, V., Metcalf, D. and Hooper, M. (2017), "The DAO Hacked", in Dhillon, V., Metcalf, D. and Hooper, M. (Eds.), *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You*, Apress, Berkeley, CA, pp. 67–78.

England, C. and Fratrik, C. (2018), "Where to bitcoin?", *The Journal of Private Enterprise*, Vol. 33 No. 1, pp. 9–30.

Fung, B. (2018), "Firm tries to take cryptocurrency mainstream", *Washington Post*, 20 May.

Hayek, F.A. von. (1976), *Law, Legislation and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy. 2, the Mirage of Social Justice*, University of Chicago Press, Chicago.

Hayek, F.A. von. (2011), *The Constitution of Liberty: The Definitive Edition*, edited by Hamowy, R., University of Chicago Press, Chicago.

Hayek, F.A. von. (2014), "Competition as a discovery procedure", in Caldwell, B. (Ed.), *The Market and Other Orders*, University of Chicago Press, pp. 304–313.

Hirschman, A.O. (2004), *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*, Harvard University Press, Cambridge, Mass.

Honig, B. (2001), "The Foreigner as Founder", *Democracy and the Foreigner*, Princeton University Press, Princeton, N.J, pp. 15–40.

Huillet, M. (2018), "Colorado Passes Bill Advocating Blockchain For Gov't Data Protection And Cyber Security", *Cointelegraph*, 8 May, available at: https://cointelegraph.com/news/colorado-passes-bill-advocating-blockchain-for-govt-data-protection-and-cyber-security.

Johnson, N.D. and Koyama, M. (2017), "States and economic growth: Capacity and constraints", *Explorations in Economic History*, Vol. 64, pp. 1–20.

Kocherlakota, N.R. (1998), "Money Is Memory", *Journal of Economic Theory*, Vol. 81 No. 2, pp. 232–251.

Leeson, P.T. (2014), *Anarchy Unbound: Why Self-Governance Works Better than You Think*, Cambridge University Press, Cambridge.

Leeson, P.T. and Boettke, P.J. (2009), "Two-tiered entrepreneurship and economic development", *International Review of Law and Economics*, Vol. 29 No. 3, pp. 252–259.

Ma, D. and Rubin, J. (2019), "The Paradox of Power: Principal-agent problems and administrative capacity in Imperial China (and other absolutist regimes)", *Journal of Comparative Economics*, Vol. 47 No. 2, pp. 277–294.

Markey-Towler, B. (2018), "Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain", *The Journal of the British Blockchain Association*, Vol. 1 No. 1, pp. 1–14.

McCloskey, D.N. (2007), *The Bourgeois Virtues: Ethics for an Age of Commerce*, University of Chicago Press ;, Chicago.

Meadowcroft, J. (2014), "Exchange, unanimity and consent: a defence of the public choice account of power", *Public Choice*, Vol. 158 No. 1–2, pp. 85–100.

Muzammal, M., Qu, Q. and Nasrulin, B. (2019), "Renovating blockchain with distributed databases: An open source system", *Future Generation Computer Systems*, Vol. 90, pp. 105–117.

Nakamoto, S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", p. 9.

North, D.C., Wallis, J.J. and Weingast, B.R. (2009), *Violence and Social Orders: A Conceptual Framework for Interpreting Recorded Human History*, Cambridge University Press, Cambridge; New York.

Nozick, R. (2013), *Anarchy, State, and Utopia*, Basic Books, a member of the Perseus Books Group, New York.

Pennington, M. (2010), “Democracy and the deliberative conceit”, *Critical Review*, Vol. 22 No. 2–3, pp. 159–184.

Q, S. (2018), “New Law Forces Sex-Trafficking Victims to Streets, Dark Web”, *Rolling Stone*, 25 May, available at: https://www.rollingstone.com/culture/features/sesta-fosta-forces-sex-trafficking-victims-streets-dark-web-w520720 (accessed 31 May 2018).

Rajagopalan, S. (2018), “Blockchain and Buchanan: Code as Constitution”, in Wagner, R.E. (Ed.), *James M. Buchanan*, Springer International Publishing, Cham, pp. 359–381.

Rousseau, J.-J. (1923), *The Social Contract and Discourses*, J.M. Dent and Sons, London and Toronto, available at: http://oll.libertyfund.org/titles/638#Rousseau_0132_375 (accessed 28 January 2015).

Salter, A.W. (2015a), “Sovereignty as exchange of political property rights”, *Public Choice*, Vol. 165 No. 1–2, pp. 79–96.

Salter, A.W. (2015b), “Rights to the Realm: Reconsidering Western Political Development”, *American Political Science Review*, Vol. 109 No. 04, pp. 725–734.

Sanders, T., Scoular, J., Campbell, R., Pitcher, J. and Cunningham, S. (2018), *Internet Sex Work: Beyond the Gaze*.

Shleifer, A. (2009), “The Age of Milton Friedman”, *Journal of Economic Literature*, Vol. 47 No. 1, pp. 123–135.

Skarbek, D. (2014), *The Social Order of the Underworld: How Prison Gangs Govern the American Penal System*, Oxford University Press, Oxford.

Stringham, E. (2015), *Private Governance: Creating Order in Economic and Social Life*, Oxford University Press, Oxford ; New York.

Vigna, P. (2018), “Pay Taxes With Bitcoin? Ohio Says Sure”, *The Wall Street Journal*, 26 November.

Wagner, R.E. (2016), *Politics as a Peculiar Business: Insights from a Theory of Entangled Political Economy*, Edward Elgar Publishing, Cheltenham.

Weingast, B.R. (1995), "The economic role of political institutions: Market-preserving federalism and economic development", *Journal of Law, Economics, & Organization*, pp. 1–31.

Williamson, O.E. (1985), "Reflections on the new institutional economics", *Zeitschrift Für Die Gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics*, No. H. 1, pp. 187–195.

Zhao, J.L., Fan, S. and Yan, J. (2016), "Overview of business innovations and research opportunities in blockchain and introduction to the special issue", *Financial Innovation*, Vol. 2 No. 1, p. 28.