17

Blockchain and Buchanan: Code as Constitution

Shruti Rajagopalan

Introduction

This chapter discusses Blockchain, a technology that was invented and publicly released in 2008 under the pseudonym Satoshi Nakamoto as the platform underpinning *bitcoin*, a cryptocurrency. Bitcoin is a decentralized, stable, and transparent time-stamped public ledger resolving the double-spending problem[1] by using blockchain technology combined with the benefits of cryptography with a peer-to-peer network using the internet, to create a tamper-proof record of transactions (Nakamoto 2008).

Blockchain is referred to as a distributed ledger technology or a trustless consensus engine (Swanston 2014). The technological novelty of a blockchain is that it can create consensus about the true state of a

[1]Double-spending is the act of using the same digital currency for more than one transaction.

S. Rajagopalan (✉)
State University of New York, Purchase College, Purchase, NY, USA

R. E. Wagner (ed.), *James M. Buchanan*, Remaking Economics: Eminent Post-War Economists, https://doi.org/10.1007/978-3-030-03080-3_17

ledger (that might record, for instance, exchanges, contracts, ownership, identity, data) without participants required to trust any centralized authority, or an intermediary (like an auditor, government, or an exchange). Consequently, there is much to evaluate and learn from the institutional structure that the technology and its various applications provide, especially within the constitutional political economy and public choice literature, wrestling with designing collective action rules that are robust to capture by interest groups.

Blockchain has been described as a as disruptive force that can disrupt *any* centralized system, that coordinates valuable information (Wright and De Filippi 2015), reduce the size of government by increasing cooperative efficacy (Nair and Sutter 2018), and as a system of institutional evolution that leads to many kinds of entrepreneurial actions (Davidson et al. 2018).

As an extension of this literature on blockchain as a new institutional and governance platform, this article argues that one can conceptualize computer code as constitutional rules and constraints in blockchain technology and governance. The Bitcoin protocol is essentially a set of rules written in computer code, governing what is, and what is not, allowed by the participants in the Bitcoin network. No single participant can change the rules, and even when new rules (in the form of upgrades to the open source software) are advanced by different participants, the key to understanding Bitcoin is through understanding consensus. In this context, Buchanan's scholarship is relevant to this new technology.

There are two aspects of Buchanan's scholarship that can be extended by studying blockchain; in particular, cryptocurrencies like Bitcoin. First, as a currency, Bitcoin fits Buchanan's vision of an automatic and not a managed monetary system (Buchanan 1962). Second, if the Bitcoin currency is an automatic system, operating without any centralized direction, it is useful to understand the rules governing the decentralized network, that actually make it a predictable monetary system, as desired by Buchanan. In particular, Buchanan's scholarship on consent and unanimity is quite illustrative (Buchanan and Tullock 1962). For this analysis, I argue that it is useful to think of computer

code as rules, and as constitutional rules, or the rules for rule-making (Buchanan 1990).

One mark of long lasting scholarship is when its fundamental insights can explain the world decades later, even when the world looks unrecognizable through technological transformation. James Buchanan's scholarship can be used to both understand and analyze Blockchain technology as a governance platform. Though Bitcoin is a harbinger of the future of technology and governance, the building blocks of the classic literature in constitutional political economy have much to contribute.

This chapter is organized as follows. Section "Bitcoin" describes the basic functioning of the Bitcoin system. In section "Code as Constitutional Constraints", I introduce the idea of conceptualizing computer code as constitutional rules. Section "Mining Bitcoin: Consensus and Verification" discussing the process of mining Bitcoin—or to find an analogous idea in Buchanan's terms—the level of choice and actions within rules. Section "Forking: The Calculus of Crypto Consent" discusses the process of Forking, or in Buchanan's terms—the choice of rules. Section "Conclusion" concludes.

Bitcoin

Blockchain technology was first used in the development of the digital cryptocurrency, Bitcoin (Nakamoto 2008). Though the Blockchain structure extends past the application of Bitcoin to other kinds of cryptocurrencies and kinds of ledgers, it is useful to understand its origins through Bitcoin.

Bitcoin is a completely decentralized cryptocurrency, that is not issued, controlled, or distributed by any centralized authority. As a decentralized currency, Bitcoin started as a publicly available ledger of all trades or transfers of Bitcoin among its users anywhere in the world. The ledger file is not stored any central institution. It is distributed across the world via a network of private computers that are both storing data and executing computations. Each of these computers represents a "node" of the blockchain network and has a copy of

the ledger file. The interesting thing about Bitcoin as a currency, and blockchain as a technology for keeping ledgers, is that the idea of not centralizing power to prevent capture, is inherent in its core design, and therefore it is constitutionally more robust to capture by special interests or coordinated attacks by small and powerful groups.

Bitcoin is an excellent illustration of Buchanan's idea of a monetary constitution where Buchanan argued that the appropriate standard is monetary predictability (instead of monetary stability). Buchanan distinguishes a managed monetary system—"that embodies the instrumental use of price-level predictability as a norm of policy, either loosely by discretionary authorities possessing wide latitude for independent decision-making powers, or closely in the form of specific rules constraining discretionary authorities within narrow limits" from an automatic monetary system "which does not, at any stage, involve the absolute price level, the price index, or any other macroeconomic variable, in guiding monetary policy" (Buchanan 1962, pp. 164–165).

Leaning towards the latter, Buchanan argues that automatic systems are characterized by an organization "of the institutions of private decision-making in such a way that the desired monetary predictability will emerge spontaneously from the ordinary operations of the system" (Ibid., p. 164, footnote omitted).

In reality, Bitcoin does not fit the commodity standard as described by Buchanan's illustration of an automatic system consisting "solely of the designation of a single commodity or service as the basis for the monetary unit, as the standard, and the firm fixing of the future course of the price, in monetary units, of this commodity" (Ibid.). The automatic nature of a non-commodity-based currency implies that a group requires no monetary authority to either manage the monetary base or monetary rule using discretion.

Although Buchanan perceived money with some features of a public good, requiring strictly controlled government provision, Bitcoin, a completely decentralized cryptocurrency, is an excellent illustration of such an automatic system that will result in monetary predictability.

The total supply of Bitcoin is capped by its code at 21 million. This essentially ensures scarcity with an absolute limit on the supply of this currency. In 2018, about 17 million Bitcoin have been mined and are

in circulation.[2] Developers expect another three million Bitcoin to be mined over the next 5–10 years. And, it is expected to take close to a century (at current computing speeds and capacity) to mine the last one million of Bitcoin. The Bitcoin code issues new currency to miners for verifying transactions. This is done at a controlled pace, and the verification process also becomes more complex as more Bitcoin are generated and traded (Antonopoulos 2014). So, the process of getting new Bitcoin through verification increases at a decreasing rate. In this aspect, the process of increasing Bitcoin supply mimics the increase in the supply of gold, it increases only at a decreasing rate (Nair and Sutter 2018).

The foundation of Bitcoin is cryptography. Its protocol uses a public-private key to store and spend money and allow cryptographic validation of transactions. Standard cryptography allows any individual to create a public key (designed to be shared widely) and an associated private key.[3]

Encrypted messages with a public key can only be unscrambled by the holder of the associated private key. This allows individuals in a large network to encrypt messages that only the specified recipient can access and read. Messages encrypted with the private key can only be unscrambled with the associated public key, allowing messages to be confirmed as authentic from a given sender.

For instance, Sender 'A' publishes a message in the Bitcoin network announcing her plan to transfer 10 of her bitcoins to receiver 'B'. This announcement includes a reference to the transaction on

[2]See https://www.blockchain.com/charts/total-bitcoins.

[3]Every public key is 256 bits long and the resulting hash from the public key is 160 bits long. The public key is used to indicate the ownership of an address to receive funds. *A private key* is a randomly generated string (numbers and letters), allowing bitcoins to be spent. A *private* key is always mathematically related to public key or the wallet address, but only known to the owner and not required to be shared for transactions. The public key is mathematically derived from the corresponding private key, but the beauty and benefit of cryptography is that it would be nearly impossible to use the public key to derive the private key, requiring about a trillion years for a supercomputer to crack the reverse mathematics solution.

how she acquired or received those Bitcoin. Part of this message is encrypted by sender A's private key to demonstrate that this message was sent by Sender A. Once receiver B has the Bitcoin and wishes to engage in a new transaction, he becomes the Sender. Now Sender B, in order to conduct a transaction with receiver 'C' announces his intention encrypted with the private key, and also with a reference to the transaction with A, from whom he received these Bitcoin. A, B, and C are all identified on the network through their public keys for these transactions.

The network does not need to know the private key. All that the network requires is to know if the private key corresponds to the public key, and then the transaction is validated. And since the public key is known, the network can check if the Bitcoin was spent previously, since all the previous transactions are on a public ledger.

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 length that acts as a unique identifier that can validate the transactions that were recorded in making it. For instance, the following string of data generate the following SHA256 hashes.

String	Hash
James Buchanan	e806362b5be794dbb9c81162c4a8dcf-3864c81082004ee536f98a8fd8326de50
James M Buchanan	0a1489e8f1a881ccec84ee7ba3fab435c59a2b-e184b121b90289b0adf8319016
James McGill Buchanan	8a2612d6e8b70697fefa83cfa5749d1076be-0911b0e42e4403f788469aa19110

Hash functions are deterministic, i.e. a particular input through a hash function will always lead to the same result. Further, even a small change in the input, there is a big difference in the hash. Each of these hashes is then added to a block. And the block of transactions is linked to previous blocks or chain of transactions, hence blockchain. The result is that, unlike other shared ledgers, transactions recorded on a blockchain are extremely difficult to manipulate or reverse by any authority.

Code as Constitutional Constraints

My main argument is that for governing the decentralized network of nodes, the code of the Bitcoin protocol can act as both rules and as constitutional rules.[4] By 'constitution' I mean 'rules for rule-making' as defined by Buchanan. While the code has a technical aspect, much of it is intended to constrain what individual nodes can and cannot do. And in this sense, it is a rulebook for computing, but the nodes or computers act out the intentions of individuals who participate in the Bitcoin network, and therefore the code, in essence, constraints the individual participants. The constitutional rules governing the interactions in the Bitcoin network are through the computer code in the Bitcoin Core software and its upgrades. The code determines how the different nodes or computers within the network interact with one another.

One of Buchanan's most important contributions is to distinguish between two levels of choice—the choice of rules, and the choice within rules (Buchanan 1990). This way, constitutional politics places boundaries over the realm of ordinary politics. One can think about the Bitcoin code as a constitution and the Bitcoin network engaging in both the choice of rules and choice within rules.

The original Bitcoin constitution was coded or written by Satoshi Nakamoto and was not a set of rules and protocols that was collectively decided by the participants in the Bitcoin network. But Nakamoto adopted an open source system and the source code was publically available. In addition, coders and developers could write changes to the code or upgrades to the Bitcoin Core software. However, all the software upgrades and changes to protocol need to be accepted by the group, and are adopted only if the participants can agree on the rule/code change. The choice of rules since the creation of Bitcoin, is really an emergent

[4]A similar argument has been made for cyberspace and other technologies by Lessig (1999). Lawrence Lessig famously described the code that regulates cyberspace as law, in that this code, or architecture, sets the terms on which life in cyberspace is experienced. If code is the law that regulates behavior or the individual participants, then the changes in code also lead to changes in the behavior of the participants.

process within an open source network. Various proposals for a new set of rules, or changes to the existing set of Bitcoin Core rules, need to be accepted by the nodes within the network.

These rule changes are governed by consensus requirements to create and change the code that governs Bitcoin, i.e. at the constitutional level. This is described in detail in section "Forking: The Calculus of Crypto Consent" while discussing forks in the Bitcoin network. An example of choosing the rules of the game is increasing the size of the block of transactions. Since Satoshi Nakamoto capped the block size at 1 MB, the network requires a change to the existing code (akin to amending the constitution) to increase block size. An increase in the block size will affect the choice within rules, i.e. the process of verifying transactions and adding them to the public distributed ledger.

At the level of choice within rules or constraints, is the everyday business of Bitcoin participants interacting with one another within the network, mainly to verify transactions (which is the process to mine or issue new Bitcoin). For instance, mining new Bitcoin will take on different forms depending on what is the allowed block size. At a block size of 1 MB, most computers can effectively participate and use their computing power to produce proof-of-work or the verification for transactions that mines new Bitcoin. An increase in the block size to 4 MB, automatically favors larger processing power, which means that the verification system will have fewer and more powerful participants—those with access to higher processing power. This has significant consequences, for the nature of the network, the concentration of hashing power, and therefore making the public ledger more vulnerable to attack or capture.

The 'original constitution' by Satoshi Nakamoto (2008) created a set of rules governing the network, the most important of which was the supply of the currency. Unlike most fiat currencies, Bitcoin is constitutionally capped. i.e. the total supply of Bitcoin is capped at by its code at 21 million. Bitcoin can be bought, sold, and spent in fractions, with the smallest fraction called Satoshi (1 Satoshi = 0.00000001 Bitcoin). So even with the absolute limit on Bitcoin, and its increasing value, it is easy to use as a medium. Therefore, even if the network gets close to mining almost all the Bitcoin, there is no incentive for current Bitcoin

holders to change the code and increase the total cap from 21 million to a larger number, because doing so will reduce the value of their holdings.

Bitcoin, as a version of the Buchanan's automatic system, is far less vulnerable to manipulation or political capture than the typical forms of ordinary automatic system backed by physical commodities. Given that the process of verifying transactions is an increasingly complex mathematics puzzle, the process of getting new Bitcoin increases at a decreasing rate. Both these aspects, the limited supply, and the slow increase in the new supply, are constitutionally enforced, and cannot be changed, and are the main reasons for the value of Bitcoin as a cryptocurrency.

Given that the network is completely decentralized and relies on consensus for collective action, there is the question of who is allowed to participate and to vote in the Bitcoin governance system. There are two types of participants in the Bitcoin network. The first group is the miners, who actually verify transactions on the blockchain and the second is every participant on the network—Bitcoin owners, exchanges, nodes maintaining the public ledger etc. When it comes to having a "vote" or a say in either verifying transactions or changing the protocol, only miners have a vote. However, there are no barriers to entry and anyone can become a Bitcoin miner. The software is open source, and anyone can download Bitcoin Core, and download and maintain the complete blockchain on their computer and participate in verifying transactions in exchange for new Bitcoin. In 2018, the number of computers storing the Bitcoin ledger is estimated at close to 10,000.[5] And each of these nodes has low barriers to entry, as well as the ability to exit the system, and the voice to accept or reject any rule changes.[6] If the default rule in

[5]This is only an estimate. No one knows how many nodes there in the Bitcoin network since all are not reachable. Some website like https://bitnodes.earn.com update the number of reachable nodes frequently.

[6]At this point it is important to understand the difference between nodes and miners. Full nodes are the computers have a complete record of the blockchain and verify all the transactions in the system and enforce consensus rules using Bitcoin Core. There are also nodes that are not full nodes, which only have a small portion of the blockchain and are mainly used to transact and can be used to connect with full nodes for transactions. Miners are full nodes, but in addition to maintaining the complete blockchain, they also perform proof-of-work to mine new Bitcoin.

democracy is 'one individual one vote' one can say that in Bitcoin, it is "one processor one vote." And because the decision-making or voting is done through nodes participating in the Bitcoin network, there must be rules governing this kind of democratic decision-making.

There are two levels of choices—the choice that takes place within those rules in order to mine, verify, and exchange Bitcoin, and the choice of rules or software upgrades that change the Bitcoin protocol. Therefore, there are two types of consensus required for Bitcoin.

The first is the consensus over any transaction—falling within the category of choice within rules. This consensus, as discussed above, is based on the proof-of-work by miners, and once such consensus is achieved, then the transactions cannot be changed later. In the cases where there is a failure to achieve consensus, there is a split in the blockchain. This means that temporarily, there is more than one blockchain in the network. But the chain that is the first to find or connect to the next block of transactions becomes the longest chain, and therefore other chains that form temporarily are abandoned. While there is no specific voting or majority rule, at the core of the decentralized decision-making is the idea of consensus. The greater the consensus around a given chain, that chain will be adopted by the network as "the" chain. Part of this is informed or governed by some informal norms emerging from the network. Currently, transactions are considered final, if they are six blocks deep in the blockchain, because given current hash power and its concentration, it would be almost impossible to manipulate change the ledger once it is six blocks deep. If the hashing power concentrations increase, the norm may also increase from six blocks to a higher number of blocks before a transaction is accepted as final in the network.

A second type of consensus is required at the level of the code or protocol—or the choice of rules. As the technology is used over time, many of the developers and coders find bugs or wish to eliminate certain problems and propose changes to the code. However, for changes to be adopted there is consensus required within the network.

Like any constitutional framework, it is impossible to expect that the original set of rules adopted will always be relevant. Rules change and

evolve over time, either by changing the text of the rule, or its interpretation/meaning. So, an important question arises when we compare code as constitutional rules. How does any change in the code or protocol compare to constitutional rules? And in a decentralized network, who decides how to change the rules? The simple answer is that no single individual decides these rules changes, and even when a single individual writes the updated set of rules, a very large majority must agree. This emergent aspect of Bitcoin and block chain technology has made it an extremely fertile experimental space for different rules and systems.

Vitalik Buterin has described the immense flexibility to change the rules within blockchain. "Blockchains are not about bringing to the world any one particular ruleset, they're about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They're Lego Mindstorms for building economic and social institutions" Buterin (2015).

Furthermore, the code that runs the Bitcoin network is a hard constraint and cannot be overcome by manipulation or interpretation. The only way of getting around a given set of rules or constraints is to upgrade the software which requires the consent of the nodes present in the network. In this sense, unlike the modern-day constitutions, whose custodians are elected representatives and unelected judges, and changes can be made and implemented without the explicit consent of citizens or voters; Bitcoin requires consent of the individual nodes, since these nodes have to upgrade to the new set of rules before the computer can perform the requisite function.

Second, unlike modern constitutions, often executed by bureaucrats and interpreted by judges, there is no room for interpretation of the Bitcoin code. Any action is either permitted or not permitted by the code governing that particular protocol. And if there is more than one set of rules in operation (as may be the case since it is an open source system), then the Bitcoin protocol will either allow both sets of rules to exist simultaneously or invalidate transactions of one of the sets of rules.

Mining Bitcoin: Consensus and Verification

The process of issuing new Bitcoin is completely decentralized. New Bitcoin are generated as a reward for mining—a process that verifies the transactions within the decentralized peer system. The process of mining is essentially solving a very difficult mathematic puzzle using computing power. Finding the solution requires trying all possible combinations and the speed of success is determined by the availability of computing power. The one with the access to the most computing power will most likely solve the problem first.

Since Bitcoin lacks a central auditor, every transaction must be verified and agreed upon by the decentralized network. There are many ways to achieve this like majority voting on transactions, having randomly selected parties within the network verify transactions, etc. Bitcoin however, uses a costly and robust system called the proof-of work.

The core idea of Bitcoin is that for voting on any transaction, the miners must solve a problem, or a mathematical puzzle, that is difficult to solve, but easy to verify by the nodes once solved. Each and every node adds to the layer of security or protection from capture by storing the ledger in this decentralized way. Miners take on the costs of supplying this service of adding security to the decentralized ledger. For supplying this costly and valuable service, miners are rewarded with newly created Bitcoin.

Given the absence of a trusted centralized authority, the value of Bitcoin emerges from the system of a public decentralized transparent ledger. However, it takes time to verify each transaction because each transaction must be verified by multiple nodes.

As mentioned before, solving the puzzle, or proof-of-work, makes Bitcoin a highly democratic system where each computation cycle equals one vote. If the network simply required some kind of consensus on the correct or authentic record of transactions, then such a system could be rigged by creating multiple identities and therefore voting many times and capturing the system. However, requiring proof-of-work, is a very costly method of participating or voting (for which miners are rewarded with Bitcoin). Therefore, it fosters authenticity,

discourages fake identities and provides the right incentives to the participants within the network to verify transactions (Bohme et al. 2015).

Once this mathematical puzzle is solved, proving proof of the authenticity of the transaction, the miner will publish the proof-of-work in a block. This proof-of-work shows the solution and then other miners and nodes can verify the solution. Nodes can add a block only if the block follows all the rules in the consensus mechanism. Therefore, the software running on each node checks the validity of a block and will reject any block with an invalid transaction. One example of an invalid transaction, and therefore an invalid block, is someone sending Bitcoins that they have not received from someone else in a transaction, or not received from mining a block. After the solution is verified, the miners start working on the new block of pending transactions (Ibid.).

The process comprises mining and verifying the blocks, and comparing the block to the most recent blocks, such that the entire network agrees on the historical ordering or chain. No transaction will clear or become final, until it has been added to the consensus blockchain i.e. there is consensus among the nodes over a transaction. And consensus means that most of the nodes in the Bitcoin network have the same block in their locally validated best blockchain. It takes time because it takes time to provide proof-of-work and then verify the solution using consensus rules of the network (Ibid.).

The system is coded such that blocks are added approximately every 10 minutes, though there have been times when the congestion in the Bitcoin network takes hours for transactions to clear. Because of this time lag—there are times when a transaction batch may be added to a blockchain, but it is changed because the miners reached a different consensus on the solution. To ensure that there is no problem of double-spending, the informal consensus in the network is to wait for a transaction to be 6 blocks deep before the transaction is confirmed. While this provides greater validity and assurance for the transaction, it also increases the time taken to confirm a transaction. The more transactions in the network, the greater the delay. Transactions are processed in the order in which they are received by the network, though there are mechanisms to move up in the line by paying fees.

Like in any system requiring consensus, Bitcoin transactions are costly, and take time to verify. Sometimes it may take up to an hour to verify a transaction as final. Compared to other systems like credit card networks that take mere seconds to verify and vet a transaction, Bitcoin has high decision-making costs. However, it is precisely this high degree of consensus for verification of transactions that fosters trust within the network and provides robustness to Bitcoin, and therefore provides value as a currency.

The Calculus of Consent (Buchanan and Tullock 1962) highlights the tradeoff between external costs and decision costs arising from any given voting rule within a group. This is also true for the consensus rules governing Bitcoin. The lower the consensus requirement, the higher the chance of an attack compromising the blockchain. And the higher the consensus requirement, the greater the time taken to verify transactions. Given this tradeoff, it is quite obvious that as the network evolves, a different rule will minimize total costs of arriving at consensus over a transaction. However, this changing these rules also requires a high level of consensus, as discussed in the following section.

Forking: The Calculus of Crypto Consent

In the Bitcoin network, consensus means that most of the nodes in the Bitcoin network have the same block in their locally validated best blockchain. However, to maintain consensus, it is important that all the nodes in the network follow the same consensus rules, or the same block validation rules. Since Bitcoin software is open source, developers and participants in the network often propose new rules and features that they believe will improve Bitcoin.

Within the blockchain technology, any time there is a change in the code, there is the potential for a fork. Because the technology is open source, every single Bitcoin node must be compatible with the rest of the network. Any node that is not compatible with the version of the software that all the other participants in the network are using, could face two possibilities. First, even though there are differences in the versions being used, these different versions are compatible, and lead

to mining the same blockchain (because consensus is required at that level). A second possibility is that the two different versions are incompatible, and this leads to the nodes mining different blockchains.

When new rules are introduced and implemented, there is the question before all the nodes on whether they choose to upgrade to the new set of rules or follow the old set of rules. And this choice is similar to a constitutional choice, or in modern terms voting on a constitutional amendment. Except, in the Bitcoin network these changes require a high degree of consensus that is near unanimity. The argument in *The Calculus of Consent*, is that behind the veil of uncertainty, in the absence of decision-making costs, the unanimity rule will be chosen, because when the costs of decision-making are absent the external costs are minimized only at the point of unanimity. The rule of unanimity makes every single acceptance of rule change a voluntary one. All exchanges will be efficient, as every single member in the network consents (Buchanan and Tullock 1962).

The Bitcoin network however has learnt first-hand, the difficulty with the unanimity requirement. In practice, rules have evolved which are similar to super majority rules, and not unanimity rules. Unanimity is achieved eventually, once the high threshold is reached, because the remaining nodes upgrade to the new set of rules.

When new rules are introduced, some nodes upgrade to follow the new set of rules while other nodes continue to follow the old set of rules. This creates a situation where the consensus over the blockchain can split. If a block of transactions is mined and accepted by the upgraded nodes but is rejected by the non-upgraded nodes, i.e. the old version of the rules and the new version of the rules are incompatible, this leads permanently divergent blockchains, one for the non-upgraded nodes following the old rules and the second for the upgraded nodes following the new rules. This is known as a hard fork. In theory, the only way to prevent a hard fork is if every single node upgrades to the new set of rules or every single node rejects the new set of rules i.e. unanimity. In practice, if a sufficiently large number of nodes upgrade to the new set of rules and that becomes the longest blockchain, then there is a greater incentive for the rest of the nodes to upgrade, since their fork will be the less valuable fork. Conversely, if too few nodes upgrade

to the new set of rules, the new fork or upgrade will be abandoned since there are insufficient users/miners.

A second scenario is when a new set of rules is introduced, and the newly upgraded nodes reject a block violating the new rules (following the old rules), but the block is accepted by the non-upgraded nodes still using the old rules. In this case the new set of rules are backwards compatible, i.e. the non-upgraded nodes will accept all the blocks mined by the upgraded and the non-upgraded nodes as valid. But upgraded nodes will not accept transactions under the old set of rules. This is called a soft fork. In case of soft forks, it is possible to prevent a split if the upgraded nodes control more than 50% of the hash rate. Since the non-upgraded nodes accept all the blocks (by upgraded and non-upgraded nodes) as valid, if the upgraded nodes get the majority of the hash power, they can build the chain that non-upgraded nodes accept as the best blockchain.

The interesting thing about Bitcoin rule changes, especially hard forks, is that no one can impose a new set of rules on any node in the network without consent. If a sufficiently large number of nodes change or upgrade to the new set of rules, then that blockchain becomes more valuable, and there is a benefit in upgrading to the new set of rules. In both hard forks and soft forks, it is impossible for a minority to impose a new set of rules on the majority. At best, the minority can carve out a new set of rules for itself. This abstract splitting of hard forks and soft forks becomes clearer with actual examples from the recent history of the Bitcoin network.

On the issue of congestion of transactions in the Bitcoin network, there was a major disagreement within the Bitcoin community. The problem within the Bitcoin protocol was that it would get slower and more congested as it grew more popular. The original Bitcoin code by Satoshi Nakamoto placed a limit on the number of transactions that could be processed within the network every 10 minutes. The reason for the cap was to make sure that the individual computers processing the transactions within the network, could handle the cumulative global load of transactions. However, as the number of transactions in the overall network increase, this limit on the number of transactions created congestion and delays.

One solution suggested by Mike Hearn, one of the coders in the core group, was to upgrade the code for processing transactions. Hearn argued that the "Bitcoin Core has no code in it to handle a permanent and growing transaction backlog. Transactions just queue up in memory until the node runs out" (Hearn 2015). Consequently, each node might become very slow, or crash. Hearn's main argument was that these consequences would eventually harm users, and Bitcoin's reputation, leading to a loss in Bitcoin value. And the only way to preserve value was to raise the limit on the number of transactions processed in each block.

Hearn's main opposition for increasing the block size, Gregory Maxwell, talked about the various tradeoffs. One important consequence, he pointed out, was that larger blocks of transaction might overwhelm the small or ordinary individual computers. The result would be that only large companies, or miners within the network would process the claims (Popper 2016). The original point of creating the decentralized network was that both the transactions and the ledgers would be stored across a larger number of computers, and anyone could join the network and become a miner or node. This would change the barriers to entry to become a node within the network, with fears of capture by larger firms.

This point was more than just technology, but about a system that would fundamentally change the democratic nature of the Bitcoin network. If only very large processing capacity could solve the transactions, because of the increase in block size, then even with the one vote rule, only the elite and larger miners with extensive computing power get a vote in the system.

Within the Bitcoin community, there was the struggle between the classic external costs and decision-making costs on the question of who processes or "votes" on a transaction. The original code took on high decision-making costs, limited the size of the block, and allowed anyone to be a miner with the proof-of-work qualifying as a vote on a legitimate transaction. The new faction led by Hearn preferred lower decision-making costs in the same tradeoff. Because it was a question about changing the code of the Bitcoin protocol, it is similar to a constitutional question. There are two fundamental constitutional questions

raised in this kind of issue—first, who should be allowed to vote within a system. And second, what should be the voting rule once the network agrees upon the participants.

In national boundaries, this question manifests itself as the decision over the voting rule—first past the post, primary system, etc. Or the distribution of authority between the legislature and executive decision-making.

The factions were not just about code, but more fundamental, about how the participants viewed Bitcoin. Some viewed Bitcoin as a currency primarily like gold, with a store value, that was preserved due to the decentralized nature of the network and the anonymity provided by the protocol. Others viewed Bitcoin as a medium of exchange, where the value would come from ability to support a large number of transactions very quickly, like MasterCard or Square. This division within the Bitcoin network also posed more basic questions, as there are often at the time of constitutional framing.

The issue of congestion of transactions in the Bitcoin network caused a lot of internal debate and turbulence within the Bitcoin network. One of the first few suggestions was to increase the block size (forwarded by Mike Hearn and Gavin Andersen, a lead maintainer of the bitcoin project) by introducing a software upgrade leading to a fork known as Bitcoin XT.

The main issue was increasing the block size would cause a change of rules that was not backwards compatible. If the block size limit were to be increased from 1 MB to say 4 MB, a 3 MB block would be accepted by nodes running the new version but rejected by nodes running the older version. Therefore, unless all the miners upgrade to the new protocol, there would be a split in the community, or a hard fork. Bitcoin XT was a split off the original Bitcoin Core.

To avoid a hard fork and still have the XT protocol to replace the Bitcoin Core protocol requires unanimity. i.e. in theory all nodes must accept the new protocol or exit the system. In practice, however, sufficiently high number of nodes should upgrade to the new XT protocol, to make the XT blockchain the longest and dominant blockchain after the hard fork. To this end, if a sufficient number of all the bitcoin node owners had chosen to adopt XT—75% to be precise—Bitcoin

Improvement Protocol 101 (BIP101) would have become active and the block size for those running that software would increase from 1 MB to a maximum of 8 MB, with a provision to double every two years. However, the Bitcoin XT protocol was never adopted by 75% of the nodes and at its maximum it had about 10% acceptance, which has since fallen. Bitcoin XT is considered a hard fork in the Bitcoin protocol that failed (Palmer 2016).

After the failure of Bitcoin XT, the same idea to increase the block size, but in a less drastic way from 1 to 2 MB was introduced with Bitcoin Classic. Unlike XT which was a result of a sharp divide within the community, Bitcoin Classic initially showed signs of reaching some consensus within the community, but like XT, this hard fork also failed.

An example of a successful hard fork is Bitcoin Cash, which was not an attempt to build close to unanimous consensus the traditional way. In August 2017, the blockchain forked at block 478558. This was done as a surprise announcement by a small group of miners, who instead of waiting for consensus within the Bitcoin community, simply performed a hard fork and used their hash power to trade the new cryptocurrency, Bitcoin Cash. Trading started after an hour of announcement, taking the Bitcoin community (which was debating a different user activated soft fork called Segwit) by surprise. While starting with only a few hundred nodes, at present Bitcoin Cash has over 2000 nodes processing transactions, and a block size limit of 32 MB.

Thus, multiple attempts to improve the original Bitcoin Core protocol and move to a faster network benefitting all the participants have consistently failed. One reason is the requirement for the very high level of consensus required to make these changes, and the consequent tendency to stick to the status quo. Hard forks impose a high bar. To prevent a split in the blockchain, all nodes must upgrade to the new rule and accept the new rule unanimously and almost in unison. This high bar makes hard forks or splits in the blockchain more likely. And splits in the blockchain can reduce the value of Bitcoin, which imposes a cost on all the participants in the network. So even when participants reject a new set of rules, the value of the Bitcoin Core may reduce depending on the kind of split within the network. Too many hard forks do not bode well for the network as a whole or the individual Bitcoin holder.

And therefore, there has to be a mechanism to bring about agreement upon the new set of rules.

Aside from the issue of decision-making costs, which can make unanimous decisions inefficient, Buchanan also accepts other limits of using the unanimity rule. "In effect, a unanimity rule allows the status quo values of all existing entitlements to be preserved against any unpredictable possible intrusions from the special effects of new and untried ventures, with distinction between physical (technological) and financial (pecuniary) effects" (Buchanan and Faith 1981, p. 108).

In this sense, there is a lot of turmoil within decentralized communities, choosing and voting on rules. In particular, there is a strong tendency to maintain the status quo rules. However, unlike closed communities, the Bitcoin network has a high level of entry and exit of miners, coders, and developers. This churn of individuals and ideas is the source of new and better rules. And usually rules improving the system are adopted by the network or will split off into a new blockchain creating value with a new variant of the currency.

To prevent splits and to ensure that the Bitcoin Core currency does not lose its value because of frequent changes, many of the upgrades are announced in advance with a flag day. If sufficient number of users or nodes have upgraded on the flag day, then they enforce the new rules after flag day. This is known as User Activated Soft Forks. Another innovation in this area is to rely on the acceptance miners with hash power to activate a new set of rules. This is known as Miner Activated Soft Forks where soft forks wait for the signal or acceptance of a super majority of miners (usually 75 or 95%) for the new set of rules. Once this super majority accepts the new rules, all the nodes operate under the new set of rules.

After the failure of Bitcoin XT and Bitcoin Classic, but before the introduction of Bitcoin Cash, there was an attempt to increase the block size, without splitting the community. This proposal, called Segwit (or segregated witness) was introduced into make a marginal improvement in technology and maintain consensus within the network. And the upgrade allowed all transactions mined under the new set of rules to be backwards compatible, i.e. compatible with the Bitcoin Core software.

It replaced the Bitcoin block size by a block weight limit, which would allow for blocks up to 4 MB in size, existing simultaneously with 1 MB blocks.

This would be accomplished through a soft fork, to avoid forcing everyone running Bitcoin Core to upgrade to the new software. Another interesting feature of the Segwit upgrade was that it was intended through a User Activated Soft Fork, which required 95% of the miners to upgrade in order to activate Segwit.

The intention was that after the activation of Segwit through a soft fork in August 2017, they would adopt an upgrade to increase the block size to 2 MB through a hard fork on November 16, 2017. The proposal for the hard fork split in the blockchain as abandoned in November 2017 due to lack of consensus. The introduction of the Segwit upgrade was not a success because of the high threshold for activation (95%) (Rizzo 2015).

Though these examples of the hard and soft forks, and the difficulty in achieving consensus in the Bitcoin network make it seem volatile and problematic, in fact this is the kind of emergent process that adds to the long-term robustness of Bitcoin. The Bitcoin network seems extremely robust, in this aspect, to any capture by minority or even the standard majority interests and requires a very high level of agreement. It simultaneously, due to its open source software system, experiences a lot of challenges to status quo and introduction and experimentation with new rules.

Conclusion

Bitcoin, as a cryptocurrency, may seem like the new frontier of technology and governance. However, studying the rule changes and debates within the Bitcoin community only shows that the debates and problems are age old problems of consensus.

Conceptualizing computer code as constitutional rules can be quite illuminating to create a framework to understand the issues affecting Bitcoin, other cryptocurrency, and blockchain as a technological platform. Any network, without a central auditor, relying on decentralized

nodes and participants to create and maintain a valid ledger through consensus rules, is effectively grappling with the same problems as age old constitutional framing and constitutional maintenance debates. One commonality is to govern the actions of individuals within the network and prevent or mitigate opportunistic behavior. A second, is to navigate a fast-changing world, that requires the evolution of rules and constraints.

Buchanan's framework is particularly useful to understand the consensus problems of Bitcoin and other blockchain technology. Given that decentralized ledgers are worried about losing value due to capture and attack by minority and majority factions; the rules to achieve consensus are often geared to prevent such attacks. They face the classic tradeoff between external and decision costs and find voting or consensus rules that minimize the costs of collective action and maximize the value of the cryptocurrency.

References

Antonopoulos, A. M. (2014). *Mastering Bitcoin*. Sebastopol, CA: O'Reilly Media.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives, 29*(2), 213–238.

Buchanan, J. M. (1962). Predictability: The Criterion of Monetary Constitutions. In L. Yeager (Ed.), *In Search of a Monetary Constitution* (pp. 155–183). Cambridge: Harvard University Press.

Buchanan, J. M. (1990). The Domain of Constitutional Economics. *Constitutional Political Economy, 1*(1), 1–18.

Buchanan, J. M., & Faith, R. L. (1981). Entrepreneurship and the Internalization of Externalities. *The Journal of Law and Economics, 24*(1), 95–111.

Buchanan, J. M., & Tullock, G. (1962). *The Calculus of Consent*. Ann Arbor: University of Michigan Press.

Buterin, V. (2015, April 12). Visions Part 1: The Value of Blockchain Technology. *Ethereum Blog*. Available at https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/.

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics, 14*(4), 639–658.

Hearn, M. (2015, May 7). Crash Landing. *Medium*. Available at https://medium.com/@octskyward/crash-landing-f5cc19908e32.

Lessig, L. (1999). *Code: and Other Laws of Cyberspace*. New York: Basic Books.

Nair, M., & Sutter, D. (2018). The Blockchain and Increasing Cooperative Efficacy. *Independent Review, 22*(4), 529–550.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf.

Palmer, D. (2016, January 11). Scalability Debate Continues as Bitcoin XT Proposal Stalls. *Coindesk*. Available at https://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls/.

Popper, N. (2016, January 14). A Bitcoin Believer's Crisis of Faith. *The New York Times*.

Rizzo, P. (2015, December 8). Is Segregated Witness the Answer to Bitcoin's Block Size Debate? *Coindesk*. Available at https://www.coindesk.com/segregated-witness-bitcoin-block-size-debate/.

Swanson, T. (2014). Great Chain of Numbers. *A Guide to Smart Contracts, Smart Property, and Trustless Asset Management*. Mountain View, CA: Creative Commons.

Wright, A., & De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Available at http://dx.doi.org/10.2139/ssrn.2580664.