2018

An Analysis of Cryptocurrency Governance

Mira Nagarajan
University of Pennsylvania, mira.nagarajan@gmail.com

An Analysis of Cryptocurrency Governance

Abstract

Cryptocurrency, or digital currency that utilizes blockchain technology and cryptography to encode transactions, has excited many with the promise of minimizing governance. Although the structure of cryptocurrency is inherently decentralized, cryptocurrency relies upon complex relationships between different actors with various functions and roles.. The execution of cryptocurrency thus depends on the mutually satisfying interactions of these actors, who form the basis for non-technical governance structures.

This paper investigates the extent to which technical governance mitigates traditional governance problems by examining the governance structures of two cryptocurrencies. It first gives background into the origin and technical value proposition of cryptocurrency, as well as governance theory, before analyzing Bitcoin and Ethereum to understand whEther technology mitigates actors' motivations. This paper finds that despite cryptocurrency's promise of minimizing governance, both Bitcoin and Ethereum rely heavily on trust networks, indicating that elements of non-technical governance are, in fact, crucial to their effectiveness.

Keywords

cryptocurrency, bitcoin, governance theory

Disciplines

Business

AN ANALYSIS OF CRYPTOCURRENCY GOVERNANCE

By

Mira Nagarajan

An Undergraduate Thesis submitted in partial fulfillment of the requirements for the

JOSEPH WHARTON SCHOLARS

Faculty Advisor:

Vincent Buccola

Associate Professor of Legal Studies & Business Ethics

THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA

MAY 2018

Table of Contents

Abstract

Cryptocurrency, or digital currency that utilizes blockchain technology and cryptography to encode transactions, has excited many with the promise of minimizing governance. Although the structure of cryptocurrency is inherently decentralized, cryptocurrency relies upon complex relationships between different actors with various functions and roles.. The execution of cryptocurrency thus depends on the mutually satisfying interactions of these actors, who form the basis for non-technical governance structures.

This paper investigates the extent to which technical governance mitigates traditional governance problems by examining the governance structures of two cryptocurrencies. It first gives background into the origin and technical value proposition of cryptocurrency, as well as governance theory, before analyzing Bitcoin and Ethereum to understand whEther technology mitigates actors' motivations. This paper finds that despite cryptocurrency's promise of minimizing governance, both Bitcoin and Ethereum rely heavily on trust networks, indicating that elements of non-technical governance are, in fact, crucial to their effectiveness.

Keywords: cryptocurrency, governance theory, blockchain

Research discipline: Business

INTRODUCTION

Origins of Cryptocurrency

Although many consider cryptocurrency to be a recent phenomenon, the idea of applying cryptographic elements to digital currency was in fact first pioneered in 1982. Dr. David Chaum, a researcher in the field of cryptography and mathematics, put forth the idea as the first solution to high governance costs in monetary contractions. Chaum was primarily concerned with finding a e-money solution that was both anonymous and free from double spending, a common issue in digital payments where a unit of money can be spent on multiple transactions simultaneously (Chaum 1983, 200). At the time, there were two major hurdles in the creation and adoption of digital currency: the first was the ability of digital signatures to be easily copied and reproduced, endangering users' personal information and bank account data; the second was people's concern with the level of automation inherent in digital systems (Lee ed. 2016, 1015). Chaum's solution to these problems incorporated a trusted third party (TTP), usually a bank, to approve the use of e-money through a cryptographic digital signature. The signature was designed to be randomized such that banks could not track the payment or amount back to the spender, ensuring anonymity (Lee ed. 1016). Chaum's exploratory digital currency, DigiCash, and other similar digital currencies appeared in the 1980s and 1990s but were commercially unsuccessful, largely due to a declining user base (Higgins 2014). Furthermore, the inclusion of TTPs did not provide a valid enough incentive to use an online system at a time when technology had not reached widespread adoption, and DigiCash incurred high costs to integrate e-commerce practices with established banks (Higgins). However, this period saw the rise of digital payment verification systems and online cards, such as PayPal, which increased awareness for the application of technology to personal banking (Higgins). Despite its failure, DigiCash dictated future research into digital

currencies that completely eliminated the need for institutional structures and TTPs to generate user buy-in, which set the stage for the creation of the modern cryptocurrency.

Emergence of Bitcoin:

It is impossible to discuss the emergence of cryptocurrency without first characterizing blockchain, its underlying technical infrastructure. Blockchain refers to the system of independently verified and cryptographically linked blocks that comprise a single immutable ledger. On a blockchain, transactions are stored using Merkle Tree, a structure that stores a hierarchy of hashes of data, to record all previous blocks on the system (Conti et. al. 4). The system thus preserves a history of all activity that exists electronically across multiple participants and cannot be modified by any single user. The idea of blockchain was first conceptualized by Satoshi Nakamoto (pseudonym) in 2008 in his landmark paper "Bitcoin: A Peer-to-Peer Electronic Cash System" as the infrastructure to support his digital currency, Bitcoin. Its creation was aimed to stem the growing transaction costs and security concerns that consumers faced in the financial markets by building upon Chaum's initial ideas, and improving the technology behind digital currency. Thus, cryptocurrency was essentially founded on the basis of reducing costs associated with governance that had largely been handled by TTPs.

The technical infrastructure of Bitcoin has two major developments from previous digital currencies. As the first successful decentralized "cryptocurrency", Bitcoin applied the use of cryptography, or the practice of securing data using algorithms and protocols, to protect information that existed on the currency's network (Dent 2006, 3215). Specifically, Bitcoin employed hash functions, or functions that mapped inputs to outputs, in order to identify payments (Lee ed. 1017). Furthermore, Bitcoin used digital signatures as binding approvals to

legitimate the transfer of money (Lee ed. 1017). The creation of both hash functions and digital signatures preempted Bitcoin's success relative to its predecessors, ensuring security on the system.

Bitcoin primarily mitigated the need for TTPs by employing a distributed ledger, effectively replacing trust with cryptographic proofs (Nakamoto 2008, 1). Nakamoto defined a Bitcoin as a "chain of digital signatures" that effectively linked a hash of previous payments to the account of the future coin owner (2). For transactions to occur between participants in the system, this required they be publicly announced, and developed a central immutable history of when payments were received. As such, the system proposed the use of a timestamp server, which published the hash of a block of transactions onto the chain while simultaneously reinforcing the timestamps before it. In place of a single TTP, Nakamoto proposed to employ a system of widely distributed intermediaries, termed "miners" because their activities correlated with the creation of new coins, in order to approve transactions. Bitcoin also used an asymmetric cryptosystem, which utilized both a public key, an identifier that could be used to send and receive payments on the network, and a private key, known only to the user to protect personal information (Dent 3217). Theoretically, this would allow users to interact with the blockchain network without using any unique identifiers, preserving anonymity, instead of conferring sensitive information in TTPs to process payments.

An end-to-end overview of a common Bitcoin transaction according to Nakamoto would occur as follows. A user might generate a transaction to another user by using the payee's public key. This transaction would contain several key components: the version of Bitcoin; the hash or ID of the transaction; and several inputs, including a reference to the previous transaction that coin was involved in (transferring it from an output to an input), an index of previous unspent

output, and unlocking script conditions that ensure that the unspent previous transaction output (UTXO) is sufficient to cover the subsequent transaction. Because the new input would be generated entirely from the previous transaction, the entire value of the previous transaction would also be featured in the output. If the value of the amount to be transferred were to be less than the UTXO, the sender would provide the public key of an additional wallet (usually one of their own) to receive the difference. This would give every coin, spent or unspent, a historical ledger account. The transaction is then added to a block, which refers to the series of successive transactions that are grouped togEther in the ledger (Nakamoto 3-4).

In order to prevent double spending, Bitcoin utilizes a distributed consensus and proof-of-work mechanism. Distributed consensus refers to the majority of miners that validate a transaction before it is added to the blockchain (Lee ed. 1099). The proof-of-work (PoW) mechanism is a cryptographic puzzle that requires miners to find a value, termed a nonce, that when hashed, produces a number with a certain number of zeroes that precedes it (Nakamoto 3). The puzzle increases in difficulty every two weeks in order that the system stays competitive; this, in turn, ensures that the money supply grows at a fixed rate in its pursuit of the Bitcoin fixed supply (3). PoW has a consensus algorithm that imposes five primary rules: input/output values must be rational; transactions can only spend unspent outputs; all inputs have to contain valid digital signatures (e.g. valid historical transactions); transactions must be spent within a certain number of blocks of their creation; and no transactions can spend inputs before the stated locktime (Nakamoto 7). Miners collect transactions in blocks by calculating the hash of that block in addition to the nonces of the individual transactions (3). Most cryptocurrencies employ a unique hash function that corresponds to the target hash value (Bitcoin's hash function is termed SHA-256 for the 256 bit number that is produced) (Lee ed. 1016). The difficulty of the

puzzle is correlated directly to the target value ascribed, as lower target values correspond to fewer solutions. When a miner calculates the correct hash value for a block, it immediately broadcasts the block in the network, after which all other nodes will independently verify the value by comparing it to the target value, and add it to their local blockchains (Nakamoto 4). The Bitcoin infrastructure targets an average mining time of 10 minutes per block (Bitcoin Wiki "Block"). Miners are compensated with a fixed fee of newly mined coins, as well as a transaction fee (decided at the discretion of the user who initiates the transaction). (Nakamoto 3-4)

In sum, Bitcoin's value proposition primarily promises a governance system that is based on blockchain. It grants a number of benefits: anonymity to users and miners through its asymmetric cryptosystem; cheaper transactions due to the elimination of TTPs; incentive structures for miners built into its technical infrastructure; stable currency value; inclusive financial access; and finally, public documentation of all transactions that can be viewed by any and all parties (The Bitcoin Foundation "The Bitcoin Foundation Manifesto" 2). The technical system proposed by Nakamoto distributes power across a larger network that eliminates the need for traditional governance systems, as the infrastructure purports to replace systems of trust and relationships with anonymity and distributed power in an open source network. Enabling anonymity in the infrastructure through distributed governance was considered a crucial benefit derived from blockchain, as Nakamoto theorized that the lack of anonymity would create low barriers to entry, higher buy-in from stakeholders, and more efficient payment processing speeds (2).

Bitcoin has since spawned new types of cryptocurrencies based on the blockchain, leading to a robust and competitive market. As of 2018, there are over one thousand cryptocurrencies in existence; Bitcoin remains the largest by market capitalization, peaking at a

value of nearly $20,000 per coin in late 2017, and has since fallen to around $9,000 in 2018 (Kharpal "Cryptocurrencies are heading for a 90 percent correction in 'mass market wipe out,' investment bank warns"). The most viable competitor that has emerged to Bitcoin is Ethereum, a cryptocurrency that is executed under a system of smart contracts (discussed in further detail in this paper's analysis), an infrastructure that represents a stark divergence from the original Bitcoin framework. The novel value proposition of cryptocurrency has also generated a significant amount of investor interest in the growth of the industry. Meanwhile, the blockchain infrastructure itself has been widely applied to a number of industries, including financial services, healthcare, and entertainment (Olleros and Zhegu ed. 243).

Issues of Governance in Cryptocurrency

The technical infrastructure Nakamoto outlined for Bitcoin implies a non-technical governance structure with different actors. The nature of the system itself distributes technical power, forming the basis for decentralized governance. The cryptocurrency system is defined by several key stakeholders that each carry a crucial function: users, who choose to send and receive payments on the blockchain network; miners, who both verify transactions and mine new coins at a preordained rate set by the system to keep the money supply consistent; developers, who create and update the system; and finally, external stakeholders, such as nonprofit foundations, wallets, and currency exchanges, that affect the funding and development of cryptocurrency. The promise of cryptocurrency thus fundamentally does not entirely eliminate governance, but redefines it from traditional employer/employee or contractual relationships toward trustless, virtual interactions that attempt to reduce the existence of formal governance structures.

One explicit way that non-technical governance is addressed and alluded to in the Bitcoin White Paper is through Nakamoto's discussion on miner attacks. As a whole, he considers the system tamper proof because each block of transactions contains a hash of the previous block; attempting to change, for example, the unique hash or timestamp server of a transaction would be caught almost immediately by other miner nodes. However, he identifies instances in which miners may not behave as expected by the system in order to gain advance rights to mining. Another potential issue he identifies is unintential forking, or the creation of multiple transaction recording blockchains, usually caused by delayed signaling due to network latency and traffic. Nakamoto contends that although multiple blockchains will temporarily be created, miners will be incentivized to add only to the longest chain. Nakamoto also addresses types of miner attacks that could occur, but emphasizes that when the majority of miners are "honest", or mine according to protocol, the entire system runs smoothly. These attacks, along with the rise of different mining groups, will be discussed in subsequent Bitcoin specific analysis, but their inclusion in the White Paper itself implies that Nakamoto was considering aspects of governance in the creation of Bitcoin (6).

Furthermore, despite the novelty of cryptocurrency's technical infrastructure, recent developments indicate that governance may play a larger role than anticipated by cryptocurrency creators. Four primary areas, examined in further detail in the ensuing paragraphs, are particularly salient: the multitude of currency forks; emerging private cryptocurrencies reevaluating the very value proposition of Bitcoin and imposing centralized governance systems; the involvement of the SEC in regulating cryptocurrency; and finally, investor interest and financing mechanisms surrounding cryptocurrency introducing the notion of external influence on governance systems.

Currency forks occur when there is a fundamental disagreement about a technical characteristic in a cryptocurrency, leading to the creation of a new digital infrastructure (Gervais, Karame, Capkun and Capkun 4-5). There are two primary classifications of currency forks. Soft forks can be made to a software upgrade that cause a temporary split in the blockchain; these changes are usually non-controversial and implemented by majority, and transition quickly as nodes, who vote to improve the system, simply upgrade to the new system and mine on the new chain instead. Soft forks have the advantage of being able to apply to previous transactions seamlessly, making them reverse compatible (Liew and Hewlett 2017, 5). In contrast, hard forks represent a permanent split from the original blockchain that occurs when there are conflicts about fundamental issues in the underlying system (Liew and Hewlett 5). Hard forks require all nodes to upgrade: thus, if a majority of nodes do not choose to adopt the new system, and two independent cryptocurrencies begin to operate on separate system. Meanwhile, users and miners can only operate on one since they are incompatible (Liew and Hewlett 5). The rise in the number of currency forks in recent years brings into question the stability of cryptocurrency and has drawn attention to governance, especially decision rights; who has the right to initiate or approve forks and to what extent forks are beneficial for the users of cryptocurrency.

One of the key value propositions from Nakamoto's original paper was the anonymity associated with cryptocurrency, and its open source infrastructure to encourage widespread adoption as a mode of payment. However, many investors have recently begun to call this anonymity into question. While each user employs a private key to encode his or her transactions, the public availability of all transactions on a ledger theoretically could allow for someone to trace multiple transactions back to the same individual (Tennant 2017, 1). One solution that has been developed to this issue is "mixing", a process by which users form

collectives to mix up the coins they transact with in order to prevent any transactions to be traced back to a single individual (Tennant 1). Leading cryptocurrencies have also been adopting private networks to further combat the issue of security (Olleros and Zhegu 2016, 231). These networks differ fundamentally both amongst cryptocurrencies and from the original infrastructure proposed by Nakamoto. The emergence of these structures brings about questions referring to the changing value proposition of cryptocurrencies and the governance systems that are now being employed to support them.

The questions surrounding the legal viability of cryptocurrency have been promulgated around the world in the last several years. Recently, the SEC has moved to define cryptocurrency as a security, and imposed regulations on cryptocurrency exchange (Michaels 2018). This brings into question the potential of the SEC to classify cryptocurrency as a security, which in turn would lead to the potential for capital gains tax. External questions about the viability of cryptocurrency are closely tied to the internal regulation of the systems; who is in charge, how can security breaches be compensated, and how are shareholders protected. The next several years will see heightened attention drawn to the internal governance of cryptocurrency, and will force these systems themselves to rethink how they approach internal governance.

Most visibly, cryptocurrency has gained widespread public notoriety and attention in the investor market. Heightened awareness of cryptocurrency has resulted in extreme price volatility. The price of Bitcoin, for example, peaked at nearly $20,000 in late 2017, and has declined over 50% in 2018 (Adkisson 2018). Ethereum has also appreciated 5000% in value since the beginning of the year (*Coinbase* 2018). While some industry experts speculate that the rapid price increase in cryptocurrency represents a temporary bubble, other investors are clamoring for the novel technology and in the power of consensus for the wide use of cryptocurrency. This

interest has also led to the integration of cryptocurrency with financial markets, introducing cryptocurrency to a whole host of investors and contingent factors. Bitcoin Futures have recently debuted to high prices, allowing investors to speculate on the price of coins without owning the currency (Reuters 2017). Given that the internal governance of cryptocurrency is highly geared toward aligning stakeholder interest through ownership of the currency, this new development poses new risks for the correlation between speculation and actual cryptocurrency value due to potential external influence (Pauw 2017). Finally, the increase in visibility of cryptocurrency has called into question how investors should evaluate the different types of cryptocurrency available in the market and how governance structure will play into long-term success.

The technical premise of cryptocurrency, along with these four recent trends, seem to indicate that the non-technical attributes of cryptocurrency warrant further analysis. This idea seems to be promulgated among the cryptocurrencies as well. Specifically, the interplay between the non-technical interactions of economic actors within the cryptocurrency governance system and the technical system itself creates a space for further analysis.

RESEARCH QUESTION:

Nakamoto's thesis for cryptocurrency outlines a technical structure that is built on the notion of decentralization. However, he simultaneously sets the stage for a rich non-technical ecosystem that exists to support the technical infrastructure. Given the unique nature of cryptocurrency and how relatively little attention has been paid to its non-technical attributes, this paper will examine to what extent the promise of technology mitigates governance by analyzing what strategies of governance Bitcoin and Ethereum have put in place. Specifically, this paper aims to relate the technical value proposition of each currency to understand whEther

aspects of traditional governance are successfully circumnavigated or replicated. In effect, the research question this paper aims to answer is: *what strategies of governance are in place for cryptocurrencies?* It hypothesizes that cryptocurrency's technical infrastructure does not effectively lessen the need for formal governance; the development of non-technical governance structures are inevitable in cryptocurrency. Furthermore, this paper finds that non-technical attributes of governance, specifically trust and intrinsic motivation, are, in fact, crucial to the successful utilization of cryptocurrency and that further attention should be paid to how these structures are put in place.

In defining the scope of the research question, this paper will focus on the two largest cryptocurrencies, Bitcoin and Ethereum; this choice was consciously made to ensure that there would be sufficient information and development of governance structures for analysis across two different technical structures. While there are a number of governance issues that have surrounded cryptocurrencies from outside legal entities, including their status and allowance by the SEC, and the dubious legality of initial coin offerings (ICOs) as funding mechanisms, this paper focuses exclusively on the impact of governance structures internal to each cryptocurrency. One of the reasons for this is the international nature of cryptocurrency itself has resulted in inconsistent external policy that has not yet provided a space for meaningful analysis.

OVERVIEW OF GOVERNANCE THEORY:

At a basic level, governance refers to the rules that manage the actions of any type of entity (Rezaee 2009, 17). The goal of governance is to create a system of checks and balances to enhance overall shareholder value while simultaneously protecting the interests of all stakeholders (30). Governance thus functions to curb the potential powers of different groups of

actors who have stake in the firm. The theoretical foundation of governance depicts the types of outcomes that are predicted by the analysis of the behavior of actors within a firm, and how types of transactions define firm and governance structures. In addition to providing a short overview of classical governance theory, and its shift toward behavioral explanations, this section explores the emergence of open source software programs and the governance structures they have implemented to better understand what aspects of traditional governance technology has begun to minimize

Governance theory emerged to explain and provide alternative structures to contracting, which exists as the most common and salient alternative to enforce rules. A contract is legally enforceable agreement between two or more parties (Werbach 2015, 315). Generally, according to Grossman and Hart (1986) governance is considered more advantageous than contracting when the roles of stakeholders are clearly defined and there are multiple contributors or joint ownership of a resource, leading to less predictable ex post outcomes that can be accurately contracted at efficient costs ex ante (718). Contracts thus create a tradeoff by imposing specific monetary consequences to curb malicious action, but also require costs of enforcement. The definition of "contracting" has also come to include "implicit" contracts in addition to traditionally observed explicit formal contracts. Klein et al. (1978) define implicit contracts as a "guarantee enforced by the market mechanism of withdrawing future business if opportunistic behavior occurs" (303). Implicit contracts occur when the advantage of joint ownership is decreased relative to economizing on contracting costs necessary to insure non-opportunistic behavior (299). In effect, governance and implicit contracts rely on the complex and often interrelated behaviors of multiple individuals, given that contracting is a viable option. A central theme in governance is simultaneously offering incentives for good behavior (e.g. behavior that

works toward the overall goal) while placing restriction on negative behavior to ensure task completion at ultimate efficiency. Governance is also only considered useful as long as it is effective relative to alternative incentive structures.

Early governance theory serves to demonstrate that systems of governance or contracting emerge to enforce relationships associated with economic activity, and are viewed as necessary only for particular transactions. Central to corporate governance theory is the characterization of the firm: how and why it comes into being, what properties it naturally contains, and why it represents an efficient structure of governance. The first work to delineate the characteristics that define different types of firm governance was Ronald Coase's "The Nature of the Firm" in 1937. Coase (1937) posited that firms were centralizing authorities that existed to economize the cost of coordinating economic activity, as dependent on both the costs of organizing and the efficiency of the coordination (390). Coase also characterized the idea of "agency" costs, or finding a transaction type and incentive structure that could minimize the negative actions of a manager, or residual claimant to firm value (395). Coase defined the costs of transacting across a number of dimensions, including search costs, bargaining costs, and enforcement costs that could be used to assess alternative actions of stakeholders in cryptocurrency (396-7). To Coase, centralization naturally implied stricter and more costly types of governance that were only relevant for certain types of market transactions (394). In essence, not every type of transaction required a firm, and therefore governance.

Oliver Williamson built upon Coase's landmark findings in his theory of transaction cost economics. Specifically, Williamson (1979) argued that certain dimensions of a transaction dictate the structure of governance that should surround it (244). He determined that transaction costs are naturally higher in contexts with high uncertainty, low frequency, and high asset

specificity; in effect, costs are defined on dimensions of whether transactions are predictable and skill specific to both the firm and its economic actors (239). Williamson also theorized that the time horizon of a transacting relationship also had important implications for governance, as it increased potential transaction costs and required greater stakeholder incentive in the system (251). This language will be used to describe the tradeoffs made by stakeholders in cryptocurrency in subsequent analysis. Together, Coase and Williamson created a basis for governance theory that serves as a way to control and motivate individuals acting toward a common goal. Understanding the types of transactions and the roles or functions required to achieve the end goals are crucial in shaping a governance structure that allows for specific characteristics of the exchange, including its asset specificity and time horizon. Additionally, actors are motivated to work within a governance system, as opposed to a contractual obligation for which there are legal ramifications if not followed, given their own limitations, namely opportunism and bounded rationality, as well as the costs they incur of completing the transaction relative to other actions. Thus ultimately governance theory is built around human behavior, leading to subsequent analysis from Williamson and James March on the varying composition of the firm in relation to actor incentives.

The link between transaction costs and incentive structures to Williamson (1979) was determined by two key constraints on economic actors: opportunism, self interest with guile, and bounded rationality, inherent information asymmetries in the knowledge of economic actors. Williamson then argued that the unintentional effects of bounded rationality led individuals to behave opportunistically to the detriment of the firm (241). Thus, Williamson argued that organizations should economize on bounded rationality while limiting stakeholder opportunism to create the most potential value (245-6). This idea was also reflected in Alchian and Demsetz'

(1972) analysis of employee incentives. The authors' main finding was that when individual output was difficult to directly observe and benefits were collectively born, but costs were born individually, individual contracting was costly and ineffective (777)**.** Two distinct problems, those surrounding metering and shirking incentives amongst workers in a group, characterized whether hierarchy, and thus a firm structure, arose. Alchian and Demsetz also characterized a "residual claimant" who is incentivized by ownership to contribute and accurate monitor production (783). Williamson ultimately theorized that actors within a firm are constrained by their bounded rationality and self-interest through opportunism, indicating that the formal structure of governance should reflect behavioral elements of actors rather than the distinctive nature of the transaction.

In his seminal essay "The Business Firm as a Political Coalition", James March (1962) moved beyond describing the behavioral motivations of individual action from Williamson to impute game theory models of conflict resolution onto firm decision-making. He began by noting that traditional models of firm theory that treat individuals within a firm as units with discrete interests that come together to maximize their joint preference have nearly always been disproved (669). He then argued that the imputation of a superordinate goal (most commonly profit maximization) as the driving force for firm activities was a facetious lens into firm decision making (670). Instead, he applied political theory frameworks that viewed actors within a firm as different interest groups that make various demands on the system (671). In March's model. each coalition has potential control over the system, mirroring the natural divergence of interests among actors in the firm. He ultimately argued that these conflict systems required a centralized "politician" to both mediate conflict by ordering the coalitions by viability and importance (e.g. maximize resource use within the firm) (672). He wrote that the goals and

composition of a firm are negotiated and bargained in the pursuit of hierarchically organizing these interests (672). In determining that superordinate goals did not in fact exist, March argued that governance by centralization was a natural tendency of the firm, a fact that had been ignored in viewing the firm as a fixed construct. This occurred naturally as actor interests shifted overtime and therefore shifted firm goals to align with them.

Building on his theory of transaction cost economics, Williamson (1993) determined that exogenous factors in the firm that arise as a result of relationships can have profound impact on the effectiveness of the structure. He asserted that trust based systems exist differently in the presence of contractual safeguards, placing heightened importance on the systems in which contracts are embedded within (476). He defined trust as "the risk one takes depend[ing] on the performance of another actor" which was undertaken "when the expected gain from placing oneself at risk to another is positive, but not otherwise" (463). Trustworthiness implies cooperation with potential, net-neutral penalty rather than a fixed financial reward guiding one's actions. The conditions for trust according to Williamson (stemming from Dasgupta) were as follows: individuals must have repeated encounters and memory of previous experiences; there must be a cost to honest behavior; and finally, reputation must have stake within the system, (466). Trust thus required relationships between actors to form in order to exist. Williamson built on his writing on the contextual factors of transaction types to include the concept of institutional environments, calling for further specification in the types of governance systems employed. In effect, he theorized that institutional environments provided safeguards against undesirable behavior to varying degrees that characterized further the types of transactions being conducted (476). Additionally, culture plays a large role in defining institutional environments, and serves as a check on opportunism by imposing social conditioning on the acts of members of a

particular institutional environment. Strong cultures increase the potency of social sanctions and remorse on the part of an individual with malicious intentions, which makes organizations more effective (476). Institutional environments are often maintained by the upkeep of social accounts that become ineffective when turned into financial or legal obligations; as such, Williamson wrote that "there are some transactions for which the optimal level of *conscious* metering is zero" (481). He defined personal trust by the absence of monitoring, favorable preferences, and discreteness amongst individuals; in effect personal trust fosters greater alignment between individuals and organizations (483-4). Through these arguments, Williamson demonstrated that contracting is impaired when institutional factors already incentivize certain types of behavior, further indicating that trust and other non-institutionalized factors actually play a huge role in the overall effectiveness of a governance structure. In effect he theorized that trust is an inevitable source of governance enhancement.

Together, the arguments of Williamson and March introduce a new concept of governance that is based around its actors alone: that people are influenced by one another and their social structures, and as this happens, their interests relative to one another change, forcing the governance structures themselves to change. The implications that the firm derives its activity based on actors' interests inherently means that its composition, and therefore governance structure, will always inevitably change. The superordinate goal is in fact to adapt to the incentives and behaviors of the actors within the system, because, as both March and Williamson assert, actors in the system will always advance their own agenda without regard for firm processes.

March's characterization also brought to light the key role of decision rights within the firm. Decision rights refer to the systems, constraints, and roles that firms use in decision making

(Athey and Roberts 2001, 200). March compared the decision rights structure of the firm to the influence of interest groups on political coalitions, with competing resource and interest offerings defining their abilities to perform tasks effectively and defines governance as a series of conflict resolution techniques (671). He noted that the demands actors make in a political system shift in response to experience within the system, and the perception of problems they might face (673). Goals and decisions in the firm thus appeared to be paired but decentralized. Athey and Roberts have added to this analysis by characterizing decision rights in the non-classical firm. The design of incentive schemes and decision rights structures are inevitably interlinked, as the means of affected a specific behavior usually result in offering incentives for alternative behaviors; the incentives for effort and for decisions are inextricably tied together (200). In effect, decision rights constitutes yet another behavior that motivates governance structure by reflecting constituent interest. The collective bargaining that occurs in the very creation of the firm also occurs at the level of decision rights, when future outcomes are measured by the utility of each individual actor.

Given cryptocurrency's reliance on blockchain as a technical interface to act as governance, this paper would be remiss if it did not explore new types of governance structures that have emerged to reflect the ability of technology to facilitate decentralized communication. Crucial to the analysis of cryptocurrency is the rise of community-based governance, a system that has emerged in the context of open source software (OSS), development communities with decentralized contribution schemes. The typical stakeholder structure of open source projects is analogous to many cryptocurrencies, and can help parse which contributors should and can have the rights to the decision rights structure. As Siobhan O'Mahony (2007) notes, although the term open source software (OSS) seems to implicate free access for contributors, most successful OSS

projects have structured governance systems, including formal leadership roles, representative decision making, and funding from nonprofit foundations (140). This governance structure mirrors closely the relationship between developers, users, and miners in the cryptocurrency stakeholder infrastructure. At a high level, the intricacy of governance in OSS implies a similar structure could be required for cryptocurrency given the task of balancing multiple contributors, and indicates that the behavioral components of governance.

As governance theory predicts, the structures of governance in OSS stem directly from contributor incentives. For example, most OSS encourages development from multiple sources but restricts access to the code base, usually to only founding members or "executives"; structuring levels of restricted membership around joint production serves to limit a singular actor's interest in the scope of the larger community (147). Decision-making authority in community governance is thus sometimes constructed in a hierarchy from community-approved improvements to complex code level decisions (147). Sonali K. Shah's (2006) research on hybrid OSS development similarly finds that the governance structure of a system affects participation (1000). In addition to decision rights, Shah also found that property rights and ownership of information remained crucial to initiating buy in, noting "the creation of a neutral and accessible commons is crucial for fostering community-based innovation" in the absence of face to face relationships (1011). The neutrality of the commons is constructed by the governance system and its managers in order to curb opportunism. Yochai Benkler (2003), a renowned scholar in the field of internet governance, notes that social systems "tremendous investment, acculturation, and maintenance" (110). He described that "social transactional frameworks are likely to be substantially less expensive than market transactions for pooling large number of discrete, small increments of the excess capacity from the perspective of the

contributors" (116). He also characterized two key components of peer sharing models: modularity, the property of a project that describes the extent to which it can be broken down into smaller components that can be independently produced before assembled; and granularity, the size modules in terms of the time and effort that an individual must invest in producing them (110). This mirrors the way that individuals approach work in the firm, by the size and effort required to earn incentive. Community based governance in OSS has no clear superordinate goal unless imposed by its participants, and thus requires intrinsic motivation for participation, rather than financial incentive. Rather than removing the need for trust, this in fact increases the strength of relationships among people on the network whose shared interest is entirely voluntary.

Thus, OSS exemplifies the impact of technology on traditional theories of governance. It decreases communication and search costs among actors and facilitates decentralized joint production for outputs that are separable. Communities that are able to forge trust-based relationships through repeated interaction and reputation thrive despite lacking typical transacting relationships. Decision rights in the absence of physical community takes on a new level of heightened awareness for relationship-building. The implication for open source software is despite the ability to work in a decentralized manner, governance structures are still richly visible to underlie the technical infrastructure. In the end, it appears that technology does not eliminate the need for governance as long as joint contributions are the key outcome. Since actors are always innovating to increase their position relative to a firm, the behavioral basis for their actions surrounding joint production seem to necessitate some form of governance, an idea that will be explored further in the analysis of cryptocurrency.

ANALYSIS

Bitcoin

As the first cryptocurrency, Bitcoin introduced the typical system of technical governance described in the introduction. This section will examine the non-technical attributes of the current governance structure of Bitcoin, through the lens of incentive structures and decision rights of the major participants. In order to analyze the incentive structures within governance of Bitcoin, this paper will primarily look at the two stakeholder groups with the largest amounts of power, developers and miners, while also giving a brief overview of the influence potential of external groups and users.

Developers hold a range of incentives for participating in the Bitcoin network: some developers view their contributions to Bitcoin as volunteer work, while others are sponsored by private businesses to take part (Wirdum 2016). This follows Benkler's analysis that because opt in for open source projects is entirely voluntary, the choice to contribute is colored by intangible gains from a social transaction, such as social standing and recognition (96). Bitcoin does not establish a strict hierarchy of contributing developers, which seems to be common practice in OSS, but the system does differentiate between the incentive structures for ordinary contributors and core developers. Core developers have the distinction of holding the Bitcoin source code, and are seen as both the de facto internal and external leaders of the organization (BitcoinCore 2018, "Team"). Core developers on the Bitcoin system are tasked with improving its software. As stated on the official Bitcoin Foundation website developers "can't force a change in protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users" (Bitcoin.org 2018,

"FAQ"). Thus, core developers hold "commit access" to merge new software proposals that invoke community agreement with the system. They are compensated through the Bitcoin Foundation, a nonprofit entity that "coordinates the efforts of the members of the Bitcoin community, helping to create awareness of the benefits of Bitcoin, how to use it and its related technology requirements, for technologists, regulators, the media and everyone else globally" (The Bitcoin Foundation 2018, "About"). Modeled off of the Linux Foundation, a nonprofit corporation that supports the development of many open source projects, the Bitcoin Foundation engages in activities such as organizing conferences, funding protocol development, political lobbying, and administering research grants (The Bitcoin Foundation 2018, "About"). It chiefly deals with developers, and follows Nakamoto's original goals closely in order to promote creative development to further the currency. Contributing developers are often well known in OSS, and are not explicitly contracted anywhere on the platform; as mentioned above, most are externally compensated, if at all.

The governance structure within the Bitcoin Foundation has also undergone tumultuous change, with many directors quitting and the Foundation declaring bankruptcy on multiple occasions since its inception in 2009. As a result, Bitcoin Foundation has since sought more consistent funding from a few primary sources, among them the MIT Digital Currency Initiative, an interdisciplinary research laboratory that intends to provide a neutral academic working environment for developers, to fund their salaries. The organization employs core developers to further research into blockchain and applications to financial inclusions, and other technology companies that have a stake in the improvement of blockchain (Wirdum). For example, Blockstream, a for-profit technology company, employs developers in Bitcoin. To align their incentives, Blockstream developers have time-locked Bitcoins to ensure they are incentivized to

work toward Bitcoin's success. Their contracts also include "morality clauses": if Blockstream asks any of them to work against what they consider to be in Bitcoin's best interest, they can refuse to do so while still guaranteed a salary (Wirdum) Rather than putting up a significant amount of money to fund development, the Initiative relies on compiling unrestricted gifts from sponsors, such as mining experts and high net worth individuals, who may in turn be funded by venture capitalists and other larger institutional investors (Wirdum). In order to combat the perceived conflict of interest, the developers are said to have complete freedom over their work, including retaining the ability to research alternative currency implementations (e.g. a core developer named Gavin Andresen's work and proposal for a hard fork of Bitcoin came out of his efforts in paid research at the Initiative) (Wirdum). These systems seem to curb systematic opportunism among developers, although the implications of doing "research" on blockchain does not necessarily always align with the time sensitive code decisions core developers are often tasked to make. Thus the Bitcoin Foundation appears to be accepting of any type of development in the area of Bitcoin improvement, regardless of whEther developers are working toward their own motivations or toward the betterment of the specific system.

Unlike the majority of the Bitcoin network that remains decentralized (both spatially and computationally), the core developers of Bitcoin seem to retain close knit ties. The few who have the privilege of holding commit access do seem to have rampant opportunities to act in their own self interest; however, the balance of core developers on the system ensures that malicious action taken by any single developer would immediate result in his or her expulsion and a revocation of their commit access (Lombrozo 2017) For example, Gavin Andresen's continued attempts to initiate forks led the core development team to remove his access rights because they believed he was not acting to the benefit of the Bitcoin community.

The use of the Bitcoin Foundation to coordinate the funding for Bitcoin also calls into question the purpose and the typical governance structures of nonprofit foundations. In effect, nonprofits' purposes are inherently non-monetary; as a result, trust, intrinsic motivation, and strong networks are the biggest drivers of nonprofit actions. Centered around mission and ideology, nonprofits do not typically rely on stakeholder incentives. This insinuates that a potential power overreach by, for example, members of the board of the Bitcoin Foundation might have disruptive consequences in that the system itself is built on trust while the surrounding technology deliberately avoid these networks.

Much like contributing developers, the users of Bitcoin encompass a wide variety of individuals who buy into the currency with different purposes. Investors in Bitcoin are often individuals, rather than institutions, and have shown to be predominantly male (Leinz 2018). Crucially, a strong investing pool in Bitcoin occurs from non-technology oriented, libertarian groups that believe in the power of Bitcoin as an alternative to traditional government issued currency (Leinz). It can be inferred that users also buy into Bitcoin in order to profit off of the growth of the technology. Recent developments have also allowed the trade of Bitcoin financial instruments on the market, leading a wider variety of people to become exposed to the volatility of the currency. The composition of ownership in Bitcoin varies, but it is well known that several individuals hold a significant proportion of the currency (e.g. the Winklevoss twins and Nakamoto) (Pollack 2017). Users contribute to the governance of Bitcoin primarily through online message boards, where many users have developed significant discourse surrounding important issues related to Bitcoin, including the fork (Bitcoin.org, "Community").

In contrast to the visibility of many developers in Bitcoin, miners' identities are necessarily shrouded in secrecy; they comprise diverse communities of programmers across the

world (Bitcoin Magazine, “What is Bitcoin Mining?”) . As stated previously, miners have two primary functions within the Bitcoin ecosystem: to approve transactions and to mine new coins. Miners are incentivized by compensation from each of those two activities: receiving transaction fees from transactors and by holding coins as a store of value. Most Bitcoin miners view it as a full time job, and owing to systematic differences between types of cryptocurrency, they typically only mine Bitcoin, or Bitcoin offshoots called altcoins (Bitcoin Magazine, “What is An Altcoin?”) In examining whEther miner incentives are aligned with that of Bitcoin as a whole, most attention will be directed to these two forms of compensation, and whEther they are mutually satisfying for miner goals.

The rise of mining pools, or coordinated groups of miners that split the benefits of mining equally among themselves, poses several problems for the technical integrity of the system (Eyal and Sirer 2013, 437). Mining pools have arisen in order to combine hashrate power amongst groups of individuals to be able to receive the highest transaction fees and mine the greatest number of blocks (437). There are several distinct advantages to mining in pools: it results in guaranteed payments; it results in a greater concentration of payments, because the combined hashrate speed ensures that the pool will mine more coins; finally, miners in third party pools do not need to be connected to the entire Bitcoin blockchain, a factor that tends to make their processing feeds much more quick (StackExchange 2014, “How do mining pools work?”). . The third party miners are connected to the Bitcoin network through the administrator of the pool, who functions as a full Bitcoin node (StackExchange 2014, “How do mining pools work?”). . Administrators solve metering and shirking potential amongst members within the mining pool by having them solve a hash that is not nearly as difficult as it would be on the network. This

ensures that miners will work to mine new blocks in third party entities (StackExchange 2014, "How do mining pools work?").

The rapid concentration of power in Bitcoin puts the network at risk for intentioned miner attacks due to the attractiveness of opting into pools. Mining pools have also effectively made it impossible to mine as an individual; as pools become the predominant source of mining, power concentrates in the hands of few organizations that could undermine the system due to competing interests. Mining pools are responsible for mining and synthesizing new blocks of transactions; thus, their acceptance of rules is essential in order that the new types of blocks and transactions can actually be added to the blockchain. As Benkler notes, "The number of people who can, in principle participate in a project is therefore inversely related to the size of the smallest-scale contribution necessary to produce a usable module", indicating that as the crucial function of mining becomes more important and require a larger investment of time, the universe of potential miners decreases, leading to increased accumulation of power in mining pools (101). In addition to aggregating computing power, miners can also cause adverse effects on the system itself through pools. Conti, Lal, and Ruj (2017) identify eight different types of major attacks on the PoW based consensus protocol in Bitcoin that are amplified by mining pools. These include: double spending, or spending the same bitcoins on multiple transactions; privately mining on blockchain fork; and block withholding attacks. Many of the types of attacks are facilitated by mining pools in order to drive individual minors and to weaken the consensus protocol of PoW (Eyal and Sirer 438). The types of attacks that mining pools can conduct are more lethal if they accumulate a majority of the hashrate on the network, which would contradict Nakamoto's vision that miner attacks would be safeguarded through distributed governance. Recent data indicates that 65% of the hashrate of the Bitcoin network is contained by five dominant mining

cartels, increasing the chance of malicious activity (Rosic 2018). The question then becomes: why haven't these pools launched a coordinated attack? While there have not been any definitive answers for why that is the case, one widely speculated explanation is that attacks would provide power only in a limited time frame. The long term implications of a 51% attack might include being shunned from the system by other members and tanking the price of the cryptocurrency, which could have adverse effect on the selfish miners. (Eyal and Sirer 452) In a sense this poses a transaction cost for malicious mining. To prevent these types of attacks, core developers of Bitcoin have been relatively successful in the guidance they provide through the Bitcoin Foundations to users through the community; Gavin Andresen has written to urge miners to transfer to smaller, decentralized mining pools, which might in fact result in higher PoW costs for miners (Cawrey 2014). In articles and commentary surrounding Bitcoin, many appeal to "Bitcoin purists" who should act for the integrity of the network, regardless of the cost structures in place (Bitcoin.org, "Community"). Thus, it seems that the ideology of Bitcoin has been successful in preventing power overreach.

Mining pools seem to arise because of the combined hashrate power they provide in block creation (Eyal and Sirer 437). Meanwhile, these pools demonstrate a more formalized governance system. The structure of mining pools itself implies a single residual claimant who distributes coins to participants according to the work they contribute. The behavior of this single person is unregulated, except through implicit contracting within the pool, and yet this individual holds a significant amount of power in the way that money is produced in the system, which underlies almost all actions that can be taken on it and any transactions that can be conducted. In effect, miners have established a centralized system, having internally determined that the cost of metering is far less than the aggregate power acquired from having a monitor.

Miners' second mode of compensation is through transaction fees that are added on top of any coin transaction between two users at the discretion of the initiating party. The fees are not standardized and comprise a wide range that correlates to the value of the transaction to the transacting party. This poses a significant problem for the future of the Bitcoin ecosystem for two primary reasons: first, that it gives miners inordinate control over the system, and second, because it subverts Nakamoto's intentions for Bitcoin. If miners are compensated for the tasks that underlie the system, they can effectively choose which transactions to complete based on the fee attached, resulting in increasingly high transaction fees in order to use the system. There is evidence that this is already happening; transaction with low fees are known to suffer from starvation, when miners deny the transaction service because the opportunity cost of other transactions is too high (Conti et. al. 4). Given that Nakamoto advocated for Bitcoin to solve the issue of paying third party processors for transactions, it seems antithetical to the system itself that transaction fees will be a valid mode of compensation for miners moving forward. Furthermore, because the block size is fixed, transactions will naturally become expensive, and limit user profitability in the types of payments a few types of transactions such as settlement transactions between financial intermediaries, while transactions representing everyday purchases will get pushed off the main network into "side chains" or off-chain payment channels, and ultimately become more obscure (Conti et al. 32).

Miners' incentives to create new coins when the overall money supply has a finite capacity presents another conundrum. Specifically the present and future interests of miners differ significantly. Present miners are focused on creating coins as quickly as possible in order reap maximal financial benefits. This is the dominant and necessary strategy because there is limited upside potential for miners due to the PoW mechanism becoming more and more

difficult every 2 weeks. Furthermore, the number of newly mined coins that are rewarded halves every 210,000 blocks (bitcoinwiki 2017, “Protocol rules”). However, future miners, as the supply of money nears its cap, will be more focused on transaction fees and will have little incentive to take on mining as a full time activity. The lower incentives could result in lower difficulty than what the public desires from a security perspective, and might compromise the integrity of the system. This problem, defined by the economic conundrum “Tragedy of the Commons”, is an example of how bounded rationality manifests in Bitcoin, and has been widely regarded as a major threat facing the community (bitcoinwiki 2015, “Tragedy of the Commons”).

The second key area of analysis within governance of cryptocurrency is the structure of decision making. Decision rights in the Bitcoin framework take on two primary functions: code changes and code forks. Code change approval requires developers to have control over a source code repository, and is enacted by core developers. This mechanism was controlled by Nakamoto, and subsequently by Gavin Andresen (after Nakamoto stepped down in 2011) (Simonite 2014). These privileges now lie in the hands of Bitcoin’s four major developers, who are entrusted with major administrative rights (De Filippi and Loveluck 6). Code change occurs at the discretion of these individuals; however, any Bitcoin or external stakeholder can submit a Bitcoin Improvement Proposal (BIP), a design document for introducing features or information to Bitcoin that provides technical specifications of the feature and rationale for its implementation (bitcoinwiki, “Bitcoin Improvement Proposals”). There are three primary types of BIPs: standards track BIPs, informational BIPs, and process BIPs. Standards track BIPs are generally the most impactful in the changes proposed and require community consensus. After core developers approve and consolidate the BIPs, they will put the proposal out to the

community; all members of the community (users, contributing developers, miners) have the opportunitiy to comment on it. The final vote is made primarily by miners who operate full functioning nodes by including a small piece of "voting code" in the blocks that they mine through PoW. The results are then broadcasted and then accepted or rejected. Generally, BIPs will achieve community approval before reaching the level of critical decision-making, which is examined in further detail in a later discussion on forks. The BIP process requires that all source code and documentation be released and made available to anyone, so that the entire community of individuals can discuss and improve them with subsequent proposals (De Filippi and Loveluck 2016, 13). The BIP process exemplifies the use of technology to minimize governance, although the ultimate enactment of the code change is put in the hands of core developers.

Bitcoin has experienced several forks that draw attention to the unique consensus formation it employs. Specifically, although the fork itself is created by software and ideological divergences among developers, miners ultimately choose what system to work on, analogous to "veto power" in shareholder votes. As explained by De Filippi and Loveluck, Bitcoin's first fork, Bitcoin XT, occurred because of ideological differences on optimal block size: the limited block size of 1 MB allowed for the system to be stable and secure, but limited the number of transactions that could be processed at any given time (11). In addition to slowing transaction speeds for users, the block size also limited the upside potential of mining rewards, which, according to fork proponents, prevented the currency as a whole from scaling effectively (11). Those against block size increase cited the inclusivity and decentralization of the original proposed system as threatened because of the greater computing power needed to produce on larger blocks. According to some cryptographers, the increase in block size would also compromise the security of the network and delays in confirmation times (11). In August 2015,

two core developers of Bitcoin, Mike Hearn and Gavin Andresen, released Bitcoin XT, a variation of the Bitcoin software that increased the block size to 8 MB (roughly 24 transactions per second), with the cap on block size expected to double every two years (11). The system would require that 75% of 1,000 of the most recently mined blocks to be attributed to a system with the new block size (11). The new types of signature on Bitcoin XT would constitute a system that was then incompatible with the original Bitcoin. Bitcoin XT was well received upon its launch, and was run by 1,000 nodes. The controversy surrounding the launch of Bitcoin XT, including online attacks and censorship of Bitcoin XT supporters within the Bitcoin community, ultimately led to low adoption rates among users and miners, and forced Hearn to resign in the wake of its failure. Andresen withdrew the XT BIP when it became clear that the currency was not going to gain acceptance over the original Bitcoin protocol, now termed Bitcoin Core, and its functionality was near dead by early 2016. This began a series of forks, including Bitcoin Classic in February 2016, which increased the block size to 2 MB to aim for a more market driven approach , and Bitcoin Unlimited (12).

As discussions about how and if Bitcoin should scale came to a head in late 2015, a second proposal, termed Segregated Witness (SegWit), was made by several core developers as a compromise to the increase in block size. SegWit would increase the effective block size by reducing the size of each individual transaction, a soft fork in Bitcoin Core rather than a hard fork (Torpey 2017). The decrease in transaction size would come from the removal of digital signatures that comprised over 60% of the entire Bitcoin blockchain. The first Segwit soft fork was approved almost universally by 95% of miners and activated in August 2017 (Torpey). However subsequent SegWit2x hard forks faced low approval from miners who faced very high opportunity costs from switching to the system (roughly the difference between mining fewer but

higher value blocks vs. more, lower value blocks) (Torpey). This was also because SegWit2x was capped at a 2GB blocksize (a seemingly arbitrary number), and due to difficulties in signaling actually indicating miner votes (Torpey).

Miner incentives within the decision to fork perhaps hold the greatest capacity to diverge from the overall good of the currency. For one, under Williamson's theory, multiple Bitcoin forks lower switching and search costs for miners to seek rewards. This upside is also realized almost exclusively by mining pools: because the underlying hash algorithm for most Bitcoin altcoins is the same in all proposed forks, mining pools experience low switching costs, and will mine whichever currency is offering the highest potential reward at a given time. These profit switching mining pools both capture a significant amount of value across all currencies and also further push individual miners out of the system. Thus, mining pools have incentive to distort signaling effects, and keep as many coins in the market as possible. The precedent introduced by the first Bitcoin fork in 2015 has led to greater instability within the currency to find the optimal software, which also continually places miners in advantageous bargaining positions. The tradeoff between security and block size also strongly favors mining pools and makes the entire system more subject to selfish miner attacks and further manipulation.

The interplay between users and miners forms another basis for decision rights. In effect, miners' consideration to signal for a fork is a function of the added complexity of the fork and user support. User support is largely determined by strong trust networks within the Bitcoin community. It is no accident that forks have been initiated by core developers, whose visibility and reputation enable trust more easily than external actors. Users are in turn influenced by external stakeholders, such as crypto focused funds and financial instruments that speculate about the currency. Meanwhile, because users often have less stake and knowledge of the

system, they tend to be risk averse against token volatility. Ultimately, if miners signal for a change on the system, greater community acceptance in using Bitcoin on the new system determine its "success".

The conditions for trust according to Williamson/Dasgupta were as follows: individuals must have repeated encounters and memory of previous experiences; there must be a cost to honest behavior; and finally, reputation must have stake within the system, (466).

In sum, Bitcoin's technical infrastructure aims to eliminate third parties and complex transaction costs that are associated with bureaucratic elements of payment processing. Among the potential powers of the actors in the system, miners and developers hold the greatest capacity for opportunism, with miners forming powerful coalitions to dominate the computing power of the network and developers, especially those in the core and sponsored by the Bitcoin Foundation, gaining the ability to push their own personal vision of Bitcoin due to their high profile. Within decision rights, this may manifest in miners signaling votes for software changes that may not benefit the overall system. However, exempting the Bitcoin hard fork, the non-technical governance of the system has been relatively stable. Relationships between individuals, especially among core developers and with the user and mining communities virtually, seem to form the basis of decision making in the absence of formal governance.

Ethereum

The largest successor cryptocurrency that has emerged to Bitcoin is Ethereum, an open-source public software platform that utilizes blockchain technology, and an independent cryptotoken, Ether. Ethereum's own governance structure can be analyzed through examining its history as a direct descendant of Bitcoin, the incentives and decision rights systems it employs,

and two important historical events on the network: the movement to Proof of Stake (PoS) mining and the highly publicized hacking of "the DAO".

Ethereum was first conceptualized in 2013 by Vitalik Buterin, an active developer in the Bitcoin community, who strove to apply blockchain technology to the creation of decentralized applications (Hertig). Its mission and goals are markedly different from that of Bitcoin. The creation of Ethereum reflected Buterin's belief that Bitcoin's technical infrastructure was underutilized. Specifically, in his landmark 2013 White Paper, Buterin proposed Ethereum as "the ultimate abstract foundational layer" that would allow users greater functionality in creating autonomous organizations, applications, and automatically executable contracts (Ethereum White Paper). The promise of Ethereum is thus centered around its functionality as a platform, rather than as a currency system.

Ethereum employs a system of "smart contracts", or digital assets that are controlled by a single piece of code when certain conditions (e.g. contractual obligations) are met (Ethereum White Paper). Buterin envisioned smart contracts as "autonomous agents" that lived within the Ethereum execution environment (Ethereum White Paper). The notion of smart contracts was first described by Nick Szabo in the late 1990s as a "proactively enforced form", much like a vending machine that delivers an easily defined product for a specific amount of cash (Szabo 1997, 1). In short, smart contracts would ensure that all parties would not be able to change the terms of the contract once executed. The development of Ethereum accelerated after the foundation of smart contracts. In 2014, Gavin Wood, a computer science PhD who had researched blockchain, published the Ethereum Yellow Paper to further hone the technical specifications of the project. Wood introduced yet another dimension, termed Ethereum Virtual Machine (EVM), the runtime environment for Ether, and translated the first functional

implementation into seven programming languages (Wood 2015, 11). In structuring Ethereum as such, Wood and Buterin aimed to create a widely accessible platform for developers, which they hoped would cultivate a large community of like-minded followers.

As described in the Ethereum White Paper from 2015, which was initially authored by Buterin and has since been continuously updated and modified, Ethereum employs a technical system that resembles Bitcoin's blockchain, but with several significant differences. Ethereum itself is made up of units, termed "accounts", that can engage in "state transitions", or transfers of value and information. This differs from Bitcoin, which utilizes unspent transaction outputs (UTXO) to conduct payments. The cryptotoken and source of value within Ethereum is termed "Ether"; Buterin envisioned Ether as a "fuel" for the system that powered internal transactions, rather than a distinct currency. He proposed two general types of accounts: externally owned accounts, which could execute only transactions; and contract accounts, which could be encoded to send transactions or create contracts. In addition to the sending and receiving address, each Ethereum transaction would contain specifications regarding the amount of Ether "gas" required to execute the transaction, as well as the fee to miners associated with the transaction. Unlike Bitcoin, where transaction fees are attached voluntarily to transactions to be processed, Ethereum would require fees to compensate miners for each execution on the network. The amount of gas associated with a transaction from an externally owned account (a non contractual account) would be directly correlated to the number of computational steps required for miners and users to complete the transaction, usually through the size of the transaction in bytes; this represents another departure from Bitcoin, where transaction fees are not required. Similarly, messages that originate from contract accounts could "call" another contract account, allowing different contracts to activate one another depending on the type of transaction desired. The amount of gas

specified for messages between contract accounts would extend over all desired actions begun on the chain. The contract's code could either be run to completion or until the execution ran out of gas. From start to finish, a transaction would be first verified to make sure it had all necessary components, before a miner could transfer the transaction value from the sender's account to the receiver's while taking a transaction fee. All remaining fees in excess of the amount necessary to execute the transaction would refunded to the seller. At every step of the process, the amount of gas from the sender would be required to be equal to or greater than the amount needed to generate the transaction, or the system will throw an error. This also ensures safety from double spending, and ensures every action is paid for before it is conducted.

The EVM also allows developers to execute at the code level. All Ethereum contracts are written in low-level stack-based bytecode language that can access account information on the Ethereum network. As such, Ethereum is classified as Turing Complete, which ensures that any type of code can be executed on the blockchain. At its inception, Buterin envisioned Ethereum mining as PoW much like Bitcoin, but the system has since transitioned to proof-of-stake (PoS), which is described in further detail below. Regardless, the blockchain in Ethereum is similar to that of Bitcoin: each block is checked by miners to ensure that the timestamp precedes the new transaction and that the PoW/PoS is valid. However, Ethereum stores all state information within a block, removing the need for the blockchain to store all history of the chain, saving both data and space. Transactions and contracts are both executed in blocks (Ethereum White Paper). Thus, Buterin conceptualized Ethereum as an improvement to Bitcoin that utilized different types of opportunities on blockchain's technical interface. Buterin's ideas have since been hailed as successes: currently, Ethereum is trading at over $600, and has the second largest market share of all cryptocurrencies after Bitcoin (Ethereumprice.org)

In light of corporate governance theory surrounding the optimal use of contracting, it is interesting to consider the ways in which smart contracts successfully subvert the main barriers commonly held to contracting. Almost paradoxically, the system of smart contracts expects immutable transactions to be executed by those without clearly defined roles. Contracting, according to corporate governance theory, is most useful when specifying specific transactions only because the cost of contracting is so high. Smart contracts eliminate most of the costs involved with enforcing contracts by having those costs programmed into the contract's existence. This form of technical governance eliminates costs associated with decision rights, as it quickly compiles data from multiple users and takes actions on the network without any need for outside influence.

Ethereum has many potential applications that arise from the functionality of smart contracts, including tokens, financial derivatives, and decentralized autonomous organizations (DAOs). The latter is perhaps one of the most novel uses of blockchain. The Ethereum White Paper defines DAOs as virtual entities that have a shareholder base, and can facilitate votes among this base to change its code. A simple version of a DAO might include code that alters itself if a certain percentage of shareholders (e.g. 51% or 67%) vote for the alteration. For example, Bitcoin is considered a fully functional DAO because it has a preprogrammed set of rules and functions autonomously through a distributed consensus protocol (CoinTelegraph, "What is DAO"). The code might include different levels of transactions that assign certain votes to shareholders, register votes in favor, and to finalize proposals once the vote count hits the desired total. Each of these actions would be represented as a clause in the contract, with each clause storing a history of changes. Additional features of DAOs could allow shareholders to add and remove members or buy and sell shares.

DAOs are funded through open investment; the rationale for investing in a DAO varies, but often investors interested in the premise of a DAO buy in to acquire voting rights and to influence operations (CoinTelegraph). Once deployed, a DAO is autonomous from its founders and any people; it operates on a microscale like a cryptocurrency that makes decisions only based on consensus and a rigid proposal process. It is worth noting that DAOs themselves cannot create products and do require system upkeep, usually through a "contractor" (often a founder), and immediately voted upon by investors. Creators of DAOs experience similar incentives to buy into technology that they aligns with their own ideology. An analysis of "The DAO", a DAO that received widespread public attention due to issues of governance and hacking is presented below in further discussions on decision rights. In sum, DAOs represent a technical governance system built on smart contracts that operate independently from human control.

The governance of Ethereum mirrors the general structure of Bitcoin with a nonprofit foundation, developers, miners, and users. However there are distinctive differences in the composition of Ethereum within these structures. For one, the Ethereum Foundation seems to hold significant power over the direction of the currency due to its creation preceding the existence of Ethereum itself. According to its official historical documentation, Ethereum was released in a coordinated presale in order to both fund ongoing development and establish a network of developers, miners, investors (Ethereum Homestead 2016, "History of Ethereum"). The legal complexities of the presale led to the creation of the Ethereum Foundation, a nonprofit headquartered in Switzerland that facilitated the sale; the profits of the sale went toward the legal fees associated with creating the Ethereum Foundation as well as prior uncompensated developer fees. The sale was based in Bitcoin, and netted over 50 million Ether, which was about $18 million at the time (Ethereum Homestead). The involvement of the Ethereum Foundation in the

creation of Ethereum as an individual entity implies that the Foundation's agenda, which is shaped primarily by core developers, holds precedence over the development of the system. This seems to indicate that entities that formed Ethereum are staked because they have a specific vision for its future. The Ethereum Foundation thus constitutes a more typical firm shareholding model, with the holders of Ether actively buying into the system and distributed ownership across a range of individuals and institutions, rather than coordinated through a singular third party. This represents a departure from the Bitcoin Foundation, which is independently funded. The Foundation also issues grants to developers in order to incentivize them utilize the system, indicating that the developers that use the system may be less intrinsically motivated toward a common goal. It is worth noting that there are some external funding sources that buy Ether to invest in the novel technical premise. Recently, the Ethereum Foundation has fielded donations from dubious sources including a Russian state bank (O'Leary 2017, 'Misunderstanding': Vitalik Buterin to Create New Entity for Russian Bank Deal.). The use of these sources indicate that it might be possible for actors external to Ethereum to influence the ideological direction that the Foundation chooses to implement through its developer grants.

Due to its developer friendly,open-run environment, Ethereum has attracted a wide array of developers with different motivations that hope to utilize and build upon Ethereum's many potential applications. The barriers to entry to create an application on Ethereum's network are quite low, which incentivizes a greater range of potential participant developers to use the system (Github.com/go-Ethereum 2017, "Developer's Guide"). As a result, more developers use Ethereum than any other cryptocurrency (Keys 2018). Furthermore, the broad, exploration oriented mission of Ethereum ensures that the developers who join the system retain nearly autonomous creative control. While this has spawned a diverse set of applications, it also

indicates that developers are not necessarily united toward a common purpose; for example, widely varied implementations have sometimes been criticized by experienced developers as marketed deliberately to uneducated developers and have led to many unfinished projects (Breen 2018). Many prominent academic computer scientists have come out against the logic that is required on the Ethereum system that makes it vulnerable to security threats, precisely because it attempts to allow for multiple implementations of applications (Russell 2017). Most recently, a temporary bug in the Ethereum system trapped hundreds of millions of dollars in the system, to users' detriment (Russell). There seems to be a tradeoff between overall system effectiveness, and the ability to distribute technical and creative control across multiple individuals, leading to security concerns. The lack of governance toward developers in Ethereum may thus have unintentional negative consequences for the technical wellbeing of the currency.

Just as developer interest in Ethereum is wide ranging, user incentives to participate in Ethereum are also more varied. Users on the Ethereum system hold Ether tokens, vote on DAO proposals in the network, and utilize smart contracts for immutability in payments. They tend to be more technology oriented than the average Bitcoin user because the decentralized applications they opt into on the Ethereum system are worth Ether investment primarily for voting rights: knowledge of what technical changes to make and to operate in a DAO, for example, would lead to better and more rational decision making than an uninformed person (Olpinski 2016). Users of Ethereum also tend not to own other types of cryptocurrency, especially Bitcoin; their support is usually ideological and unilateral. There are no Ethereum instruments currently trading in the financial markets, but they will presumably come into being given the SEC's approval, giving Ethereum further exposure to external actors.

Miner incentives in Ethereum have shifted since the inception of the currency. They originally faced a similar circumstance to Bitcoin while utilizing PoW; however, the shift toward a PoS system from PoW has fundamentally changed the role of mining. According to the Ethereum website, PoS is a consensus algorithm that depends on the actor's economic stake in the network[1]. While PoW uses the speed at which miners can solve cryptographic puzzles as a method to designate which miner is compensated for the transaction and to create new coins, PoS uses a more complex system of voting amongst miners that depends on the size of their Ether stake. PoS was proposed in order to combat the inherent problems with PoW that Bitcoin had come to exemplify: the rise of mining pools predisposed the network to a 51% attack, the energy consumption required to mine prohibited individuals from entering the system to prevent further mining pools. While Ethereum had originally used a PoW system, Buterin had always expressed desire to transition to PoS; the Ethereum community was largely supportive of the shift, as many problems, especially coordinated miner attacks, had come to light surrounding PoW (Github.com/go-Ethereum, "Proof-Of-Stake_FAQs"). Currently, Ethereum employs a variant of the Byzantine fault tolerant (BFT) type of PoS that was released as "The Casper Protocol" in October 2017 (Buterin and Griffith 2017). Ethereum as a whole is thus more conscious of the potential for miners to accumulate power, and strives to minimize it.

Casper was envisioned as a security-deposit based consensus protocol that required miners to buy into Ether in order to paricipate. Buterin and Griffith proposed that Casper would help mitigate some of the main problems with the existing iteration of PoS, specifically the "Nothing at Stake" problem, and "long range attacks". The Nothing at Stake problem resulted from properties of the PoS algorithm that specified both the stake and random frequency of success; in effect it incentivized miners to mine on every possible chain, and with enough of a

majority, could have led to miners coordinating forks in order to send and receive coins themselves. Long-range attacks occured when miners attempted to start a fork that was very far back on the chain, in order to replicate the entire blockchain; this confused participants because it led them to question which chain was technically "valid" (Li 2017). In essence, PoS required a trusted source for the initial blockchain data to avoid replication. Casper eliminated both of these key issues through mechanisms that forced miners to form consensus blockchains, translating to miner activity becoming further restricted and removing much of the potential for miner power overreach.

The role of miners was impacted by the shift to PoS because of the need for miners a superior stake, rather than superior computing power, to retain a competitive advantage. PoS constructs a system where miners bet their security deposits on a blockchain based on how they expect everyone else to bet their deposits; the consensus derived from this bet creates the "objective" blockchain, and ensures that there will be a single chain that miners use. Miners first mine to discover blocks, and then attempt to validate the block by placing a bet on it; if and when the block gets appended, then miners receive a reward proportionate to their bets (A. Kiayias et al. 258). If they bet correctly, they earn their deposit back through fixed transaction fees and token issuance (A. Kiayias et al. 2017, 258). Miners are thus incentivized to bet correctly because they would otherwise lose their deposit, lessening the stake and their potential to mine in the future(A. Kiayias et al. 258) . This game theory approach ensures that through multiple rounds of betting, miner bets eventually converge to the "true" chain. Coordinated hard forks by a collusion of miners could be reversed by the remainder of the community moving to the "true" chain; furthermore, the extensive supply of Ether necessary to fund an attack would inevitably

cause the currency value to increase. Thus, the primary role of miners in Ethereum is to approve the execution of the transaction, rather than its contents.

The transition to PoS has many important implications for miners. Because success is tied to the amount of Ether miners have, the alignment between the overall goals of Ethereum and successful validation is more salient, as it would seem counterproductive for a miner to sabotage a system in which their stake was reliant on the value of that system. This seems to reflect O'Mahony's argument that the presence of property rights increases the buy in of economic actors in OSS. However, while the system is designed to curtail the rise of mining pools, it increases the wealth of individual miners by ensuring that the richest ones will continue to receive the benefits of validation. This would, over time, decrease the speed of block validation, even as the number of transactions per second on the Ethereum network increases exponentially. Because individual miners hold a great deal of power on the system, and because power is correlated to stake size, there is very little incentive for new miners to enter. Thus while PoS ensures that the system overall will be manipulated less easily by coalitions of miners, it makes individual miners more powerful instead. Over time, this could cause problems for Ethereum, as fewer miners will be incentivized the join the system and slow transaction speed and use. Meanwhile, the presence of fixed transaction fees that are proportional to the size and complexity of the transaction could eventually lead to transaction starvation for smaller payments, as has occurred in Bitcoin.

Because of the inherent structure of DAOs, decision rights in Ethereum are inextricably bound to the incentives for various actors, as the greatest influence an actor can wield is through voting power. Code changes and forks also comprise the majority of decision thus far for Ethereum. Much like in Bitcoin, code changes in Ethereum occur through formal Ethereum

improvement proposals (EIPs) that require community consensus. Because of the multifaceted nature of the Ethereum system, there are many more types of proposals, including those that are application specific and "Meta" EIPs that formalize the processes themselves (Ethereum.org, "Ethereum Improvement Proposals"). This in itself indicates a meta heightened awareness of how rules of governance should be structured in Ethereum by its users. Included in the EIP process is a "Deferred" status that anticipates potential adoption of a recommendation in the event of a future hard fork. This is emblematic of the overall EIP process attempting to normalize change on the system, even proposing software forks as an alternative to bureaucracy to get wider user buy in. In effect, Ethereum strives to allow users and developers to operate as self contained actors, rather than improving processes to achieve consensus around all issues. Core developers' openness to flexibility has also caused them to embrace hard forks in order to promote continuous change in the system (Demeester 2016). The core development team of Ethereum, consisting of Buterin and six other developers hold commit access to EIPs, and also sit on the Ethereum Foundation Council. Many of Ethereum's developers also worked on Bitcoin and thus also have pre-existing relationships with one another. In the interest of transparency, the notes to all the core development agenda meetings can be found online and users routinely comment with ideas, reactions, and feedback ('Ethereum', Github.com)

Perhaps the most salient example of the power developers exert in decision rights occurred in the prominent hacking of the infamous "DAO" in 2015. In understanding the significance of the event, it is first important to understand the purpose of DAOs from a governance perspective. Much like Williamson theorized, DAOs seek to mitigate transaction costs, specifically agency costs in which residual claimants hold important power hierarchies, information flow, and financial resources over shareholders. DAOs intend to eliminate agency

costs by putting power in the hands of shareholders; in the case of Ethereum, this means allowing people to vote on basic governance decisions with their Ether stake. For example, DAOs can allow for votes that determine when and if to hire an employee, and also can pay that person if the vote passes (Mehar 2017, 7). As Mehar notes, DAOS substitute "voluntary compliance to a corporation's charter with actual compliance with a pre-agreed computer code" (7). One of the major advantages of the voluntary and distributed governance structure in DAOs is its ability to empower minority owners in decision making (in contrast to shareholder governance groups like ISS/Glass Lewis that represent shareholder views to companies).

The infamous DAO was created by Christoph and Simon Jentzsch, who envisioned a company called Slock.it that was the foundation of a decentralized sharing economy (Mehar 8). The basic structure of the DAO implied token holders that could release funds following successful votes on detailed proposals on various types of investments (8). The DAO gained considerable interest from investors around the world, with investments totaling $150 million**.** In June 2016, a developer on the web based software development platform Github revelaed a flaw in the DAO's smart contract that allowed users to empty user balances over time without the balance change being recorded. Despite protestations by Ethereum founders and Slock.it founders, the DAO continued operations until it was hacked, five days later. The method of attack was exactly as had been foreshadowed: the so-called "hacker" used the code flow to repeatedly split the DAO's balance into valid accounts in a duplicate DAO that could not be accessed until one month after the request (Mehar 10). Counterattack measures were taken to prevent the hacker from continuing the withdrawal, but he or she ultimately walked away with $50 million, constituting nearly 15% of the worldwide supply of Ether.

There were three courses of action proposed in reaction to the DAO "hack". The first was to protect the integrity of the code and do nothing; the rationale for this argument was that the attacker had technically not committed a crime or injustice against the system in his or her actions. The ability to slowly siphon money constituted a loophole in the smart contract. The second alternative was to soft fork in order ban use of the duplicate DAO that contained the "stolen funds". The major ramification of this course of action was the loss of all investors' Ether. Finally, the third choice was to get nearly universal consensus from all miners in order to return stolen Ether to the original DAO. Surprisingly, the third solution was strongly advocated for by the founders and core development of Ethereum, despite the fact that it violated the core principle of immutability on the network. After a vote, the majority of miners chose to hard fork and create a new chain where the blocks could not be tampered with. This spawned a forked altcoin, Ethereum Classic, whose miners operated on the original network, having chosen not to accede to the vote. The vote itself was controversial in that it prioritized voting power by users' stake rather than "one user one vote" (12). As a result, users saw their Ether amounts double as they now existed simultaneously on two different chains.

This event demonstrated some of the flaws in the decentralized governance system proposed by DAOs. Developers' decision to hard fork and thus deny the malicious attacker his earned reward demonstrated that core developers in Ethereum view their role as managing the technical system, and therefore superior to it. As Dupont (2017) notes, the algorithmic governance\, governance of a system by code and code alone, promised by DAOs was never in reality technology alone, involving the complex interplay of developers, miners, token holders, and even the Ethereum Foundation, much like the basis for this analysis of the macro-level cryptocurrency (12). In effect, Dupont notes "The DAO relied on a model of human behavior

and social constitution notionally based on liberal ideologies, where humans act as rational, self-interested, and untrusting agents" (13). The way that the funds were taken represents a deviation from the expected result of the algorithmic structure, causes actors to fall back on social ties and community orientation. For example, the Ethereum Foundation's support of the hard fork left many users themselves questioning the promise of decentralized governance when central authorities clearly had the capacity to dramatically influence outcomes to protect their reputations. In this particular situation, the return of the funds was only secondary to the wellbeing of the system to external shareholders: to ensure safe and continued use, developers ultimately had to make drastic code changes to protect their own vested interests. The developers' themselves probably constituted a large degree of the favorable vote. The method of voting during the DAO crisis also demonstrates some of the limitations in distributed governance with respect to decision rights. Most crucially, decentralized voting procedures that require a large percentage of stakeholder buy in to achieve consensus often must evolve over a long period of time in order to achieve a result. The Ethereum community quite literally observed the hacker stealing funds from the DAO without the ability to take action. Thus, the smart contract system of aggregating votes was sufficient but not optimal for the particular situation given the time horizon they were working on.

The issues faced during the DAO hack have been replicated in recent events, including multiple hacks of the Parity startup system that have led to public calls for a more standardized fund recovery system (O'Leary 2018, "Ethereum Users Are Losing Money and Developers Don't Quite Know What to Do") A recent article by CoinDesk details this internal conflict. Led by developers from a startup, Tap Trust, internal conflict regarding the ability of users to be able to effect "state changes" in response to malicious activity has recently been present in the

network. The hack had resulted in four proposed code changes that according to core developers "conflicted with the ethos of Ethereum". In essence, if exceptions to code could exist on the network, the code itself would not immutable and its entire value proposition, its immutability and automatic execution, would be threatened. A second attempted fork, to core developers, would lead to more instability and set the precedent for continued regulation by developers of malicious activity. A distinct compromise has arisen between the speed of response and loyalty to code among users; many have voiced that Ethereum's ability to adapt and act in users' best interests at odds with the code is one of its greatest advantages. In a sense, community wide sentiment for code upgrades and changes should not be limited by the desires of core developers if there is a majority shareholding interest. Those in favor of greater restrictions point to the ability of core developers to heavily influence decisions as a negative aspect of the system (O'Leary). Youchi Hirai, a core developer on the network, wrote in a recent post: "I wouldn't move a finger for a recovery unless the amount is going to a few parties that can threaten the network (then I would prefer vaporizing away the amount rather than giving it back)". This brings into question whEther and when certain governance structures should be used, and who should be controlling their implementation (Hirai 2018).

Ethereum developers are now seeking to improve and expand governance infrastructure on top of the network. A follow up article by CoinDesk that covered the recent Ethereum conference in Paris draws light on the ways developers are now considering governance. One of the biggest issues with the most recent proposal was the lack of clarity/transparency with which it was communicated to users. Greg Colvin, a prominent developer on the Ethereum network, has recently formed a coalition to coordinate best practices for open-source development. Colvin recalled the DAO decision among others as reasons to strengthen policies surrounding

governance of the system in order to find better ways to achieve consensus. The Ethereum community has expressed desire for more input in decision-making, which brings into question what the role of core developers should be on the network. Colvin cited the close-knit relations of core developers in the early stages of Ethereum development as crucial to achieving consensus in top down decision-making, a factor that has since become more complex by the addition of more core developers around the world. Colvin thus noted "in person communication" as deeply important to the network's integrity.

Colvin's coalition aims to mitigate issues between the two major schools of thought within Ethereum: the notion that "code is king" and the desire from users to see greater transparency from the Ethereum Foundation regarding the direction and types of changes that it wishes to enact. Stemming from the DAO fork decision, developers ultimately have the power to propose action and thus control the two most important stages in the process: proposal and enaction. Furthermore, even though there is an approval process, the discourse surrounding whEther the change should be implemented is ultimately politicized. The purpose of the process is to both create productive debate among stakeholders and allow the market to decide which version of the software is more valuable externally. Ultimately, Colvin writes that he has found that "it's hard to arrive at a technical proficiency if there's a lack of clarity as to the direction of Ethereum". Thus, the non-technical and technical governance aspects of Ethereum are inextricably bound (O'Leary 2018, "Ethereum is Throwing Out the Crypto Governance Playbook").

In conclusion, Ethereum has attempted to build upon Bitcoin's success by creating a developing environment that is more open to change. The lack of governance surrounding developers, specifically the autonomous nature of developing in Ethereum and the involvement

of the core developers in the founding of Ethereum's primary funding structure, raises questions about the amount of power concentrated within the group. Ethereum seems to be primarily designed for developers, not non-technical users, thus making developers both the curators and customers of the system itself. The power of developers was demonstrated in the decision making process after the DAO hack, indicating the top-down and relationship driven processes that core developers envision for the network. Finally, the reactions of the Ethereum community from the DAO hack seem to demonstrate that increased attention will be paid to governance moving forward.

CONCLUSION

Analysis of both Bitcoin and Ethereum reveals that both cryptocurrencies have rich and developed non-technical governance structures that are crucial to their success. A descriptive overview of each cryptocurrency reveals that while each proposes a unique technical system to eliminate the need for TTPs, neither truly succeeds in eliminating the potential powers of stakeholders. In Bitcoin, the rise of mining pools and the ability of users to use external financial instruments to manipulate the price and profit gains create strong motivation to take over the system. In Ethereum, the precedent set by developers in rejecting the DAO and forcing a hard fork has created both the perception and potential for core developers to dictate the direction and composition of the system. In both cryptocurrencies, a lack of formalized structure in adapting to changes and accepting input from multiple stakeholders internal and external to the system has resulted in periods of instability.

Despite the potential for manipulations, both Bitcoin and Ethereum remain relatively popular. Their systems are utilized at a high rate across all stakeholder groups, and there remains

to be a tremendous amount of excitement around the long term and lasting consequences on the ways that transactions can be processed on each systems. Among cryptocurrencies, both Bitcoin and Ethereum have generated strong followings that indicate they have community support and potential to succeed. Furthermore, despite forking events and security concerns, the majority of potential power usurpations have not been undertaken on the network. For example, mining pools have existed and continued to grow without system-wide repercussions for Bitcoin, and DAOs continue to proliferate and seek funding in Ethereum. The relative success of these cryptocurrencies despite the demonstrated weaknesses in their technical interfact and governance structures beg the question: given that there have been a number of opportunities to take advantage of the system, why have there not been a proliferation of adverse events?

This paper hypothesizes that the answer lies in the very concept that Nakamoto believed Bitcoin could overcome: trust. Throughout research on the topic of cryptocurrencies, trust, especially among developers and by other stakeholders upon developers and miners to satisfy the needs of system, has been a key theme. For example, the emergence of new lead developers was based on their reputational value, rather than any technical interface. Much as Williamson and March hypothesized, trust served as a mitigating factor that underscored sometimes ill-defined governance based relationships within actors. Furthermore, trust could be a reason for their ineffectiveness: for example, the desire of Ethereum developers to return money in the DAO stems from the trust that they wanted to cultivate from users. This trust mitigates malicious behavior because of pre existing communities and because of the intrinsic desire that accompanies participation in the system. In effect, blockchain technology has in many ways strengthened the need for better understanding of trust networks among individuals in order to support the technological interface.

The ultimate conclusion of this analysis indicates that the governance of cryptocurrency reflects its theoretical promise: individuals' desire to innovate to increase their stake and power within any given system will always create the need for governance, regardless of the novelty of the technical interface that underlies it. The need for actors within cryptocurrency, especially miners and developer, to cooperate and collaborate across a joint resource in the long term necessitates non-technical governance to ensure this innovation does not occur. Far from achieving the utopian promise of technical governance, cryptocurrency has endured growing pains resulting from the absence of these very systems. The technology alone is and will not be enough to sustain the wellbeing of cryptocurrency in the long term. This is evidenced not just by the conclusions of this paper, but by the actors within these cryptocurrencies themselves: as previously mentioned, Bitcoin developers have begun to develop a richly nuanced decision rights system since its fork, and lead developer Colvin is actively leading discussions about strengthening the premise and rules within Ethereum governance. As March theorized, the structure of governance within cryptocurrency is being bargained for by multiple stakeholder groups (671). In effect, this paper highlights that stakeholders of Bitcoin, Ethereum, and other cryptocurrencies should actively be thinking about the design and structure of their governance systems instead of attempting to avoid it entirely.

REFERENCES:

'About.' The Bitcoin Foundation. Available at: http://bitcoinfoundation.org/about/. [Accessed 2 May 2018].

Adkisson, J. 2018. Why Bitcoin Is So Volatile. *Forbes* (February 9). Available at: https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/#4066906239fb

Alchian, A. A. and H. Demsetz. 1972. Production, Information Costs, and Economic Organization. *The American Economic Review* 62 (5): 777-795.

Athey, S. and J. Roberts. 2001. Organizational Design: Decision Rights and Incentive Contracts. *The American Economic Review* 91 (2): 200-205.

Bartling, B. E. Fehr, and H. Herz. 2014. The Intrinsic Value of Decision Rights. *Econometrica* 82 (6): 2005-2039.

Benkler, Y. 2006. *The Wealth of Networks*: *How Social Production Trnasforms Markets and Freedom*. New Haven and London: Yale University Press.

'Bitcoin.' StackExchange. Available at: https://bitcoin.stackexchange.com/questions/21769/how-do-mining-pools-work. [Accessed 2 May 2018].

Bitcoin Foundation, https://bitcoinfoundation.org/

'Bitcoin Improvement Proposals.' Bitcoinwiki. Available at: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals. [Accessed 2 May 2018].

'Block.' Bitcoinwiki. Available at: https://en.bitcoin.it/wiki/Block. [Accessed 2 May 2018].

Breen, A. 2018. How and Why Developing for Ethereum Sucks. [Blog]. *Medium*. Available at: https://medium.com/@aidobreen/how-and-why-developing-for-Ethereum-sucks-

1ff1a9873527. [Accessed 2 May 2018].

Buterin. V. 2016. A Proof of Stake Design Philosophy. [Blog]. *Medium.* Available at: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51. [Accessed 2 May 2018].

Buterin, V. and V. Griffith. 2017. Casper the Friendly Finality Gadget. Ethereum Foundation (Nov 5).

Cawrey, D. 2014. Are 51% Attacks a Real Threat to Bitcoin? *Coindesk* (June 20). Available at: https://www.coindesk.com/51-attacks-real-threat-bitcoin/.

Chaum D. 1983. Blind Signatures for Untraceable Payments. In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology. Boston, MA: Springer.

Coase, R. 1937. The Nature of the Firm. *Economica* 4, 386-405.

'Community.', Bitcoin.org. Available at: https://bitcoin.org/en/community [Accessed 2 May 2018].

Conti, M., C. Lal, and S. Ruj. 2017. A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*.

De Laat, P. B. 2007. Governance of open source software: state of the art. *Journal of Management Governance* 11, 165-177.

Dent, A. W. 2006. Fundamental problems in provable security. Philosophical Transactions of the Royal Society A 364: 3215-3230.

Demeester, T. 2016. Why I'm short Ethereum (and long Bitcoin). [Blog]. *Medium*. Available at: https://medium.com/@tuurdemeester/why-im-short-Ethereum-and-long-bitcoin-aee5b1c198fd. [Accessed 2 May 2018].

DeNardis, L. and M. Raymond. 2013. Thinking Clearly about Multistakeholder Internet Governance. *Paper Presented at Eighth Annual GigaNet Symposium*, Bali, Indonesia.

'Developer's Guide.' Github.com/Ethereum. Available at: https://github.com/Ethereum/go-Ethereum/wiki/Developers'-Guide. [Accessed 2 May 2018].

Dupont, Q. Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization. In: *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*, ed. Malcolm Campbell-Verduyn. Routledge,

'Ethereum Improvement Proposals.' Ethereum.org. Available at: http://eips.Ethereum.org/. [Accessed 2 May 2018].

'Ethereum price.' Ethereumprice.org. Available at: https://Ethereumprice.org/

Ethereum White Paper, 2013.

Eyal, I. and E. G. Sirer. 2014. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. International Conferene on Financial Cryptography and Data Security: 436-454.

Flood, J. and R. Lachlan. 2017. Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings. *Griffith University Law School Research Paper* : 17-23.

Gervais, A., Karame, G., Capkun, S. and Capkun, V., 2014. Is Bitcoin a decentralized currency?. *IEEE security & privacy*, *12*(3): 54-60.

'Frequently Asked Questions.' Bitcoin.org. Available at: https://bitcoin.org/en/faq#who-controls-the-bitcoin-network [Accessed 2 May 2018].

Grossman, S. J., and O. D. Hart. 1986. The costs and benefits of ownership: A theory of vertical and lateral integration. *Journal of Political Economy* 94 (4): 691-719.

Hertig, A. Who Created Ethereum?. Coindesk.com. Available at: https://www.coindesk.com/information/who-created-Ethereum/. [Accessed 2 May 2018].

Higgins, S. 2014. 3 Pre-Bitcoin Virtual Currencies That Bit the Dust. Coindesk. Available from: https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust/.

Hirai, Y. My attitude on protocol changes affecting particular Ethereum accounts. [Blog]. *Medium*. Available at: https://medium.com/@pirapira/my-attitude-on-protocol-changes-affecting-particular-Ethereum-accounts-13e26d1f37b4. [Accessed 2 May 2018].

'History of Ethereum.' Ethereum Homestead. Available at: https://Ethereum-homestead.readthedocs.io/en/latest/introduction/history-of-Ethereum.html. [Accessed 2 May 2018].

Keys, A. 2018. Ethereum Has 30 Times More DEvs than the Next Blockchain Community. [Blog]. *Consensys*. Available at: https://media.consensys.net/andrew-keys-Ethereum-has-30-times-more-devs-than-the-next-blockchain-community-27980a5ddc09. Accessed 2 May 2018].

Kharpal, A. 2018. Cryptocurrencies are heading for a 90 percent correction in 'mass market wipe out,' investment bank warns. CNBC. Available from: https://www.cnbc.com/2018/05/02/cryptocurrencies-heading-towards-90-percent-correction-investment-bank-warns.html.

Khidzev, A. 2016. Crypto-currency: Legal approaches to the concept formation. Russian Presidential Academy of National Economy and Public Administration.

Kiayias, A., Russel, A., David, B. and R. Oliynykov. 2017. Ourobors: A Provably Secure Proof-of-Stake Blockchain Protocol. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science 10401.

Klein, B., Crawford, R.G., and A. A. Alchian. 1978. Vertical Integration, Appropriable Rents, and the Competitive Contracting Process. *Journal of Law and Economics* 21 (2): 297-326.

Liew, J. K. and L. Hewlett. 2017. The Case for Bitcoin for Institutional Investors: Bubble Investing or Fundamentally Sound.

Lee, In. ed. 2016. *Encyclopedia of E-Commerce Development, Implmentation, and Management.* Hershey, PA: Business Science Reference.

Leinz, K. 2018. A Look at Who Owns Bitcoin (Young Men), and Why (Lack of Trust). *Bloomberg* (January 24). Available at: https://www.bloomberg.com/news/articles/2018-01-24/a-look-at-who-owns-bitcoin-young-men-and-why-lack-of-trust.

Li, M. YK. 2017. How Ethereum's Casper Protocol Will Address Problems With Proof of Stake. Seekingalpha. Available at: https://seekingalpha.com/article/4132934-Ethereums-casper-protocol-will-address-problems-proof-stake?page=5

Lombrozo, E. 2017. For the sake of accuracy, commit access is actually mostly a maintenance role… [Blog]. *Medium.* Available at: https://medium.com/@elombrozo/for-the-sake-of-accuracy-commit-access-is-actually-mostly-a-maintenance-role-making-sure-the-4251959756a3. [Accessed 2 May 2018]

March, J. G. 1962. The Business Firm as a Political Coalition.*The Journal of Politics* 24 (4): 662-678.

Mehar, M. et. al. 2017. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. (November 26. Available at: http://dx.doi.org/10.2139/ssrn.3014782

Nakamoto, S. 2008. Bitcoin: A Peer-To-Peer Electronic Cash System.

Olleros, F. X. and M. Zhegu. ed. 2016. *Research Handbook on Digital Transformations*. Northampton, MA: Elgar.

O'Leary, R. 2018. Ethereum Is Throwing Out the Cryptocurrency Governance Playbook. Coindesk.com. Available at: https://www.coindesk.com/Ethereum-throwing-crypto-governance-playbook/. [Accessed 2 May 2018].

O'Leary, R. 2018. Ethereum Users are Losing Money and Devs Don't Quite Know What To Do. Coindesk.com. Available at: https://www.coindesk.com/Ethereum-users-losing-money-devs-dont-quite-know/. [Accessed 2 May 2018].

O'Leary. R. R. 2017. 'Misunderstanding': Vitalik Buterin to Create New Entity for Russian Bank Deal. Coindesk.com. Available at: https://www.coindesk.com/misunderstanding-vitalik-buterin-create-new-entity-russian-bank-deal/), [Accessed 2 May 2018].

O'Mahony, S. 2007. The governance of open source initiatives: what does it mean to be community managed? *Journal of Management Governance* 11: pp. 139-150.

Olpinski. M. 2016. [Blog]. .*Medium*. Available at: https://medium.com/@maciejolpinski/on-risks-rewards-and-the-evolution-of-daos-c82db87a60a8. [Accessed 2 May 2018].

Pauw, Chrisjan. 2017. Bitcoin Futures, Explained. *Coin Telegraph* (December 17). Available at: https://cointelegraph.com/explained/bitcoin-futures-explained.

Pollock. D. 'Who Owns Bitcoin Universe: From Satoshi Nakamoto to Winklevoss Twins and More.' *Coin Telegraph*. Available at: https://cointelegraph.com/news/who-owns-bitcoin-universe-from-satoshi-nakamoto-to-winklevoss-twins-and-more [Accessed 2 May 2018].

'Price Charts: Ethereum 24H'. *Coinbase*. Available at: https://www.coinbase.com/charts?locale=en-US [Accessed 2 May 2018].

'Proof-of-Stake-FAQ.' 2018. Github.com/Ethereum. Available at:

https://github.com/Ethereum/wiki/wiki/Proof-of-Stake-FAQ

'Protocol rules.' Bitcoinwiki. Available at: https://en.bitcoin.it/wiki/Protocol_rules. [Accessed 2 May 2018].

Rapoza, K. 2017. What China Ban? Cryptocurrency Market Cap Rebounding. *Forbes*.

Reuters Staff. 2017. Bitcoin futures contracts at CME and Cboe. *Reuters* (December 15). Available at: https://www.reuters.com/article/uk-bitcoin-futures-contracts/bitcoin-futures-contracts-at-cme-and-cboe-idUSKBN1E92K9

Rezaee, Z. 2009. *Corporate Governance and Ethics*. John Wiley & Sons Inc.

Rice, D. T. 2013. The Past and Future of Bitcoins in Worldwide Commerce." *Business Law Today*

Rosic, A. 2018. What is Ethereum Casper Protocol? Crash Course. *Blockgeeks.com*. Available at: https://blockgeeks.com/guides/Ethereum-casper/. [Accessed 2 May 2018].

Russell, J. 2017. A major vulnerability has frozen hundreds of millions of dollars of Ethereum. *TechCrunch* (Nov 7). Available at: https://techcrunch.com/2017/11/07/a-major-vulnerability-has-frozen-hundreds-of-millions-of-dollars-of-Ethereum/.

Shah, S. K. 2006. Motivation, Governance, and the Viability of Hybrid Forms in Open Source Software Development. *Management Science* 52 (7): 1000-1014.

Simonite, T. 2014. The Man Who Really Built Bitcoin. *MIT Technology Review* (August 15). Available at: https://www.technologyreview.com/s/527051/the-man-who-really-built-bitcoin/.

'Team'. Bitcoincore.org. Available at: https://bitcoincore.org/en/team/ [Accessed 2 May 2018].

Tennant, L. 2017. Improving the Anonymity of the IOTA Cryptocurrency. 2017.

The Bitcoin Foundation. 2017. The Bitcoin Foundation Manifesto. Available from: https://bitcoinfoundation.org/wp-content/uploads/2017/03/Bitcoin_Foundation_Manifesto.pdf

Torpey, K. 2017. The Failure of SegWit2x Shows Bitcoin is Digital gold, Not Just a Better PayPal. *Forbes* (November 2017). Available at: https://www.forbes.com/sites/ktorpey/2017/11/09/failure-segwit2x-shows-bitcoin-digital-gold-not-paypal/#736ed3492233.

Tosh et al. 2017. Security Implications of Blockchain Cloud with Analysis of Block Witholding Attack. International Symposium on Cluster, Cloud, and Grid Computing.

'Tragedy of the Commons' Bitcoinwiki. Available at: https://en.bitcoin.it/wiki/Tragedy_of_the_Commons. [Accessed 2 May 2018].

Vogel, N. 2015. The Great Decentralization: How Web 3.0 Will Weaken Copyrights. *The John Marshall Journal of Intellectual Property Law*.

Werbach, K. D. and N. Cornell. 2017. Contracts Ex Machina. 67 Duke Law Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2936294

'What is DAO.' Coin Telegraph. Available at: https://cointelegraph.com/Ethereum-for-beginners/what-is-dao#how-daos-work. [Accessed 2 May 2018].

'What is an altcoin?' *Bitcoin Magazine*. Available at: https://bitcoinmagazine.com/guides/what-altcoin/. [Accessed 2 May 2018].

'What is Bitcoin Mining?' *Bitcoin Magazine*. Available at: https://bitcoinmagazine.com/guides/what-bitcoin-mining/. [Accessed 2 May 2018].

Williamson, O. E., 1979. Transaction-Cost Economics: The Governance of Contractual Relations. *The Journal of Law & Economics* 22 (2): 233-261.

Williamson, O. E., 1993. Calculativeness, Trust, and Economic Organization. *The Journal of Law & Economics* 36 (1): 453-486.

Wirdum, A. van. 2016. Who Funds Bitcoin Core Development? How the Industry supports Bitcoin's 'Reference Client'. *Bitcoin Magazine* (April 6). Available at: https://bitcoinmagazine.com/articles/who-funds-bitcoin-core-development-how-the-industry-supports-bitcoin-s-reference-client-1459967859/.

Wood, G. 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger EIP-150 Revision.