6-6-2018 10:30 AM

The Rise of Decentralized Autonomous Organizations: Coordination and Growth within Cryptocurrencies

Ying-Ying Hsieh
The University of Western Ontario

Supervisor
Vergne, Jean-Philippe
The University of Western Ontario

Graduate Program in Business
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Recommended Citation

Hsieh, Ying-Ying, "The Rise of Decentralized Autonomous Organizations: Coordination and Growth within Cryptocurrencies" (2018). *Electronic Thesis and Dissertation Repository*. 5393.
https://ir.lib.uwo.ca/etd/5393

Abstract

The rise of cryptocurrencies such as Bitcoin is driving a paradigm shift in organization design. Their underlying blockchain technology enables a novel form of organizing, which I call the "decentralized autonomous organization" (DAO). This study explores how tasks are coordinated within DAOs that provide decentralized and open payment systems that do not rely on centralized intermediaries (e.g., banks).

Guided by a Bitcoin pilot case study followed by a three-stage research design that uses both qualitative and quantitative data, this inductive study examines twenty DAOs in the cryptocurrency industry to address the following question: How are DAOs coordinated to enable growth? Results from the pilot study suggest that task coordination within DAOs is enabled by distributed consensus mechanisms at various levels. Further, findings from interview data reveal that DAOs coordinate tasks through "machine consensus" and "social consensus" mechanisms that operate at varying degrees of decentralization. Subsequent fuzzy-set qualitative comparative analyses (fsQCA), explaining when DAOs grow or decline, show that social consensus mechanisms can partially substitute machine consensus mechanisms in less decentralized DAOs.

Taken together, the results unpack how DAO growth relies on the interplay between machine consensus, social consensus, and decentralization mechanisms. To conclude, I formulate three propositions to outline a theory of DAO coordination and discuss how this novel form of organizing calls for a revision of our conventional understanding of task coordination and organizational growth.

Keywords

Task Coordination, Organizational Growth, Decentralized Autonomous Organization, Blockchain, Cryptocurrency, fsQCA.

Acknowledgments

Participating in Ivey's PhD program has been an exciting and inspiring intellectual experience. I have been extremely fortunate to witness and work on the intriguing blockchain innovation at the forefront of the FinTech revolution. Writing a dissertation on Bitcoin and the cryptocurrency space was a bold decision to make with lots of experimentations, especially in the early days when the industry was mainly associated with shady images. The completion of this dissertation and of my PhD was an intellectual adventure that would not have been possible without the support of many important people.

I would like to thank my supervisor, Prof. Jean-Philippe Vergne, the perfect scholar to work with on this difficult phenomenon. He showed me how an academic can attend to both creativity and rigor. On the one hand, he is ambidextrous while navigating the research landscape; on the other hand, he stays laser-focused working on a specific problem. He encouraged me to think about transcending the boundaries of management theory by challenging the underlying assumptions. As a scholar, Dr. Vergne sets very high academic standards for his students. As a mentor, he is always there to provide clear guidance and timely feedback. He gives his students top priority and is always the first to celebrate their achievements and provide honest feedback when they need improvement.

I would also like to thank my thesis supervisory committee, comprised of Prof. Tima Bansal, Prof. Claus Rerup, and Prof. Michael King. They played an important role in shaping the early stages of my work by providing valuable and constructive feedback that helped me build my dissertation on a solid foundation. I will never forget Prof. Bansal's advice that a PhD dissertation should aspire to top-journal quality. She has always provided excellent advice on how to craft qualitative research in a way that is both insightful and sophisticated. I also learned a great deal from Prof. Rerup about how to formulate my research by asking the right questions and by sitting in the reader's chair. He is a serious scholar who thinks deeply about the nature of phenomena and attends to the rich details that shed new light on the research question. Finally, I benefited immensely from Prof. King's expertise in finance and FinTech. He has helped me connect my work with the real world and to make it relevant. I feel privileged to have had these leading scholars on my committee.

I also would like to thank the members of my examination committee who took the time to be part of the developmental process of my dissertation. I am fortunate to have Prof. Tima Bansal from the Ivey thesis supervisory committee, Prof. Diane-Laure Arjalies from Ivey, Prof. Aleksander Essex from the Computer Science Department of Western University, and Prof. Phanish Puranam from INSEAD as the external examiner on the committee. I benefited tremendously from their comments and insights which help me move forward not only this dissertation but my broader research ideas.

I would like to thank the Ivey PhD program for its financial and research support. The faculty and staff at the PhD program office have provided an enriching environment and have equipped me with the necessary skillsets for a future academic career. I am also indebted to the Scotiabank Digital Banking Lab at Ivey, which provided me with the opportunity to work as a research fellow conducting FinTech-related research. My participation in the First Annual Toronto FinTech Conference would not have been possible without the tremendous support of the Lab. Chairing the conference was an invaluable learning experience, which will inform my research and teaching as a junior faculty member in the years to come. I also owe a big thank you to all of the Ivey and non-Ivey friends I met over the course of the last five years. Your friendship has brightened up my doctoral studies, and your support has been a strong force driving me forward.

Finally, this journey could not have begun without the support of my family. My parents have always been my strongest supporters and biggest fans. I would like to thank them for looking after my children while I pursued my studies. Big thanks are due also to my husband, TC, who put his academic career as a tenure track faculty member in Taiwan on hold to support me in my dream. And most of all, I am grateful to my wonderful children, Lillian and Yong, who have been patient while I was busy, cheered me when I was down, and inspired me when we learnt together. You are my sources of power and motivation. You are the best gift I have from God.

Table of Contents

List of Tables

List of Figures

List of Appendices

Chapter 1 Introduction

1 Introduction

"Bitcoin is the first breed of a new type of organization that simply did not exist before . . ."

Daniel Diaz, Business Development Director, Dash

"It makes most sense to see Bitcoin . . . as a decentralized autonomous organization."

Vitalik Buterin, co-founder, Ethereum cryptocurrency

Bitcoin is the first and most famous "cryptocurrency," defined as a digital asset transacted securely, transparently, and peer-to-peer by means of cryptography. At a basic level, cryptocurrencies are powered by software that enables decentralized and disintermediated online transactions using distributed ledger (or "blockchain") technology (Nakamoto, 2008; Lee, 2015). Between 2009, when Bitcoin was first introduced, and December 2017, the market capitalization of the cryptocurrency industry increased from nothing to $800 billion (CoinMarketCap, 2018).

One industry expert contends that, "Bitcoin is the first breed of a new type of organization that simply did not exist before" (Daniel Diaz, interview #2, 2016). In fact, industry experts and legal scholars alike (Atzori, 2015; Wright & De Filippi, 2015) argue that cryptocurrency transactions all fundamentally take place within a new form of organizing (Puranam, Alexy & Reitzig, 2014) known as the "decentralized autonomous organization" (DAO) (Buterin, 2014). In this dissertation, I define DAOs *as non-hierarchical organizations that perform and record routine tasks on a distributed, cryptographically secured, public ledger; and that rely on the voluntary contributions of their internal stakeholders to operate, manage, and evolve the organization through a democratic consultation process* (see also Van Valkenburgh, Dietz, de Filippi, Shadab, Xethalis & Bollier, 2015; Dietz, Xethalis, de Filippi & Hazard, 2016).[1]

[1] While some industry experts prefer the term "distributed organization," I have opted for "DAO" to avoid confusion. The term "distributed organization" is already used in the management literature to describe work organized across geographically dispersed locations (e.g., Hinds and Kiesler, 2002; Lee and Cole, 2003; Orlikowski, 2002).

In contrast with traditional organizations, DAOs do not have a CEO or other top managers who “write the rulebook,” i.e., define and write governance rules into the software code (Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016: 173–175). A DAO does not have headquarters, subsidiaries, or employees. Instead, it has “network validators” who lend computing power to validate and record transactions on the public ledger in exchange for compensation in the form of digital tokens that represent ownership; for example, Bitcoin tokens represent ownership of Bitcoin currency. Rather than having shareholders, a DAO has early adopters who can buy in during “initial coin offerings.” A DAO makes decisions through community-based voting processes. While DAOs can perform tasks similar to those carried out by traditional organizations, the way in which tasks are coordinated is substantially different. In a nutshell, DAOs place “automation at the center [and] humans at the edges” (Buterin, 2014).

The past few decades have seen the emergence of new forms of organizing. In contrast with traditional organizations, in which tasks are determined centrally and channeled through hierarchies, organizations such as Wikipedia, Uber, and AirBnB offer novel solutions to such problems as division of labor and integration of effort (Puranam, Alexy & Reitzig, 2014). Post-bureaucratic and humanistic organizations, similarly, are self-managing organizations rooted in “radical decentralization,” in which the degree and scope of formal authority (e.g., reporting relationship) is hugely mitigated by organizational democracy (Lee & Edmondson, 2017).

Despite the growing interest in alternative forms of organizing, the examples cited above are largely owned and controlled by centralized corporations. DAOs differ from these in terms of both design and coordination. The blockchain, meanwhile, may be understood as a “new coordination technology,” representing not just a technological but organizational innovation (Davidson, De Filippe & Potts, 2016a; 2016b). DAOs enable new forms of governance and coordination by revolutionizing well-received management concepts such as trust (Seidel, 2017). Despite the growing economic importance of DAOs, scholars have paid insufficient attention to this intriguing phenomenon. While a few management scholars have recently highlighted the opportunity to study the organization design and task coordination in this new and fascinating context (Dodgson, Gann, Wladawsky-Berger, Sultan & George, 2015), I seek to address a more specific question, namely:

How are DAOs coordinated to enable growth?

Given the lack of prior studies in the management literature, I will take a mixed-methods and inductive theory-building approach to investigate how DAOs coordinate tasks (Young-Hyman, 2017) and how such novel approaches to organizational design affect growth. In order to answer the central research question posed above, I will rely on fuzzy-set Qualitative Comparative Analysis (fsQCA) as my main methodological tool, in combination with qualitative interviews and archival data.

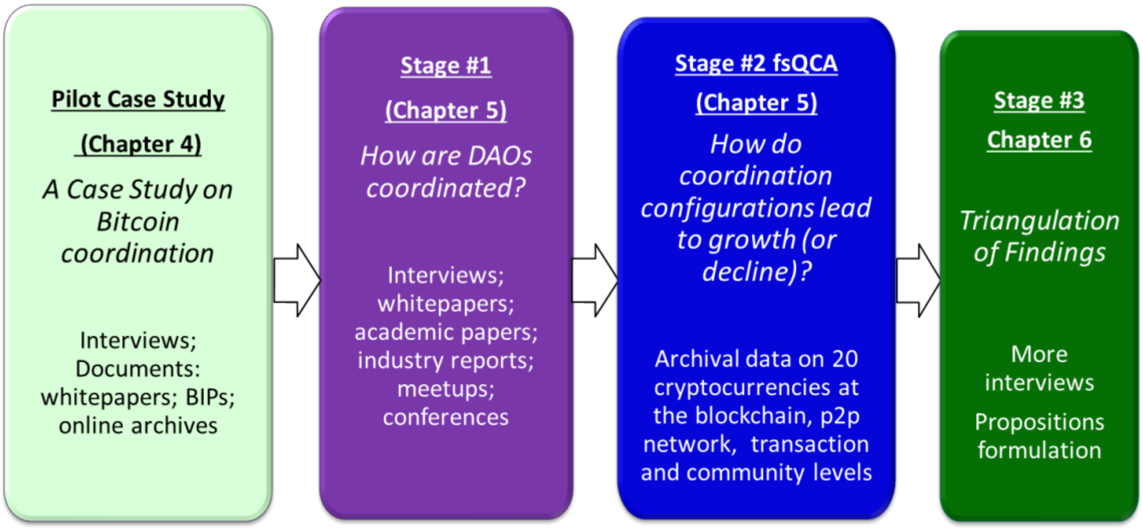
By theorizing about DAOs with empirical evidence, this research contributes to the management literature in the following ways. First, I identify, describe, and analyze the DAO as a novel form of organizing that cannot be fully explained by the extant literature. DAOs not only provide novel solutions to the universal problems of organizing, namely task division, task allocation, reward provision, and information flows (Puranam et al., 2014), but, by incorporating a new class of stakeholder that integrates tasks at the organizational level, DAOs enable an extreme form of decentralization (e.g., Baldwin & Clark, 2006; O'Mahony, 2007; West & O'Mahony, 2008; Von Hippel & von Krogh, 2003). Second, this research enhances our understanding of DAOs by unpacking the interplay between various coordination mechanisms and the implications of these for organizational growth. Growth is no longer driven by the need for external financial resources, managerial control, or power (Chandler, 1977; 1990; Perrow, 2002), but by the essential need to provide a secure, stable, and decentralized network (Narayanan et. al., 2016; Lee, 2015). Third, I distinguish task-level coordination from organizational-level coordination to explore how the roles of integrative conditions, such as accountability, predictability, and common understanding, have been shifted when applied to the study of DAOs (Okhuysen & Bechky, 2009). Finally, DAOs can be applied to industries beyond cryptocurrencies. This study theorizes about DAOs by proposing propositions that shape the foundations for future work to build on. For example: how can alternative currencies be organized in post-capitalist societies to balance the efficiency and stability of that society? (Cohen, 2016; Arjaliès, Hsieh & Vergne, 2017); and how does this new form of organizing and coordination help resolve the technical and social challenges associated with a cryptographically secured voting system (Essex & Hengartner, 2012)?

1.1 Dissertation Structure

The remainder of the dissertation is structured as follows:

Chapter 2 offers a detailed description of the cryptocurrency context, starting with Bitcoin. In this chapter I provide readers with background information on cryptocurrencies and explain what Bitcoin is, how Bitcoin works, and the unique features enabled by the blockchain technology underlying Bitcoin. My goal here is to set the stage for later conceptualization of DAOs. **Chapter 3** provides a review of the literature germane to my research question, including research on organization design, coordination, and growth. **Chapter 4** lays out an exploratory pilot study of Bitcoin, and describes the defining features of coordination mechanisms within DAOs. **Chapter 5** outlines the 3-stage research design, which extends the scope from Bitcoin to include multiple cases with variations in coordination mechanisms and growth patterns. In the first stage, I will inductively identify key dimensions for DAO coordination and growth from interviews and archival data. In the second stage, I will conduct fsQCA analysis to identify necessary and sufficient configurations for DAO growth (or decline). In the third stage, described in **Chapter 6**, I will triangulate my earlier findings and supplement these with interviews in order to propose a generalizable framework for DAO coordination and growth. I will also present the results of the empirical analyses and inductively develop theoretical propositions. In **Chapter 7**, I will discuss how my findings contribute to the extant literature and describe future directions for research. I will conclude this dissertation by summarizing the higher-level practical implications of my research. Figure 1 summarizes the study stages of this dissertation and the corresponding chapters.

Figure 1 Summary of Study Stages and Corresponding Chapters


Pilot Case Study
(Chapter 4)
A Case Study on Bitcoin coordination
Interviews; Documents: whitepapers; BIPs; online archives
Stage #1
(Chapter 5)
How are DAOs coordinated?
Interviews; whitepapers; academic papers; industry reports; meetups; conferences
Stage #2 fsQCA
(Chapter 5)
How do coordination configurations lead to growth (or decline)?
Archival data on 20 cryptocurrencies at the blockchain, p2p network, transaction and community levels
Stage #3
Chapter 6
Triangulation of Findings
More interviews
Propositions formulation

Chapter 2 The Context: It All Begins with Bitcoin

2 The Context: It All Begins with Bitcoin

In this chapter, I will provide descriptive background information on cryptocurrencies starting with Bitcoin. I will then link cryptocurrencies with DAOs as the theoretical representation.

2.1 What is Bitcoin?

Bitcoin, the first decentralized cryptocurrency ever created, is a peer-to-peer, decentralized payment system that does not rely on centralized authorities or trusted intermediaries such as banks (e.g., the Federal Reserve, Wells Fargo) or payment companies (e.g., Visa, PayPal). The Bitcoin white paper was first published in 2008. In the following year, the first "coin" (in the form of a computer file) was created and the first Bitcoin transaction took place. The true identity of Bitcoin's founder remains unknown; Satoshi Nakamoto, the reputed creator, is a pseudonym of the lead developer or development team.

A key motivation behind the creation of Bitcoin was the desire to eliminate the inefficiencies of the intermediated banking model that has prevailed in capitalist societies since the early 17th century[2]. Whereas Bitcoin was the first decentralized cryptocurrency, the elemental technologies underlying Bitcoin had been created way before its formation. Specifically, a large part of the development was driven by the cypherpunk movement, a social movement advocating for libertarianism with minimal governmental interference of the financial system in the 1980's and 1990's. The initial goal was to create money that could facilitate online exchanges with the anonymity (or fungibility) of cash at the same time. As a result, research projects based on strong online privacy and strong cryptography were proposed. For example, David Chaum proposed digital cash systems,

[2] This model is premised on the existence of national central banks whose role is to mediate the supply of money, both directly (e.g., through the issuance of coins and bills) and indirectly (e.g., through loan-issuing and regulated private banking). The first central bank, the Bank of Amsterdam, was founded in 1609 in the Dutch Republic.

DigiCash and eCash based on *public key cryptography* combined with centralized electronic currency (Chaum, 1983; 1985). The idea then evolved into Wei Dai's b-money rooted in the privacy model of public-private key cryptography, also known as *digital signatures* (Dai, 1998). Thus, ownership can be secured through the matching process between the public key for verification and the private key for signing and accepting funds without revealing the true identity. At around the same time, the core technology for securing the Bitcoin network—*proof-of-work cryptographic hashing*, was proposed by Adam Back's (1997; 2002) Hashcash and Hal Finney's (2004) creation of the first reusable proof of work (RPOW). The idea is to build in economic cost functions to "deter denial-of-service attacks" (Lee, 2015:10).

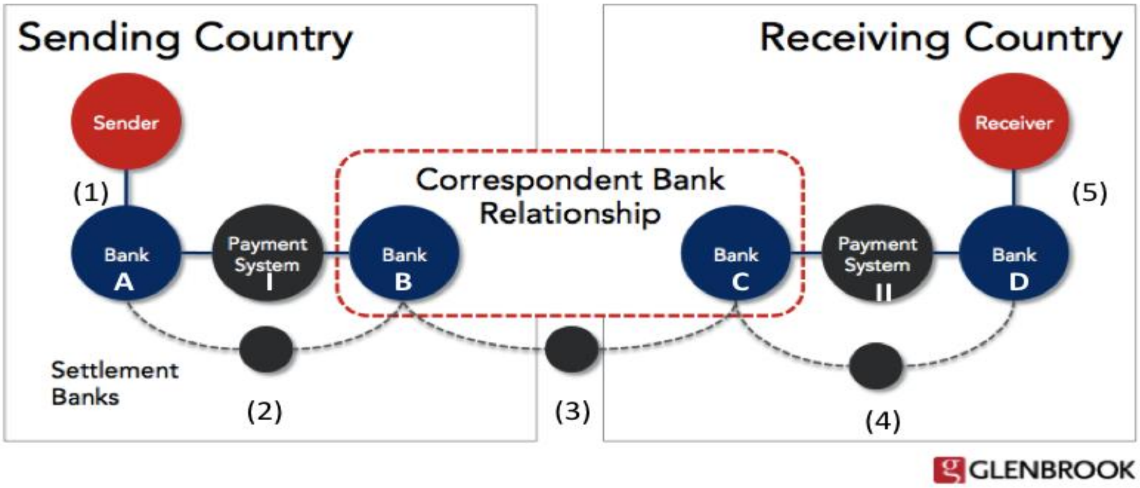
However, Bitcoin was the first to integrate the three technologies—public key cryptography, digital signatures, and proof of work—to achieve distributed consensus within a "blockchain" ledger. The resulting system is peer-to-peer and does not rely on trusted third parties; and ensures transactional privacy and security (Wood & Buchanan, 2015:392-393). This is where the true value of Bitcoin resides. More details will be provided in section 2.2.

As a result of the 2008 financial crisis, the public increasingly lost faith in financial institutions. For many, Bitcoin became the logical alternative to the out-dated banking system. Bitcoin enables a completely disintermediated, peer-to-peer system that significantly reduces the delays and transaction fees that accompany traditional payments, e.g., international wire transfers.

An international wire transfer between two countries typically involves four different banks (including two "correspondent" banks), two national payments systems, and an international settlement service (e.g., SWIFT). A standard international payment takes between three and 15 business days to complete, depending on the destination country. Expensive bank fees and punitive exchange rates add to the cost.

Figure 2 shows the steps involved in an international wire transfer. First, assuming a sender in New York, USA wishes to send $1,000 USD to a receiver in London, UK, the sender must visit a local branch or give instructions online to his bank A to transfer the specified amount to the receiver’s bank D in London. At this stage, Bank A charges a $25 transaction fee. Second, Bank A works with a domestic correspondent Bank B through payment system (I) to effect the international transfer. Bank B is normally a large international bank that has settlement agreements with banks in the receiving country. The $25 fee is split between A and B. Third, Bank B notifies Bank C about the payment, and transfers funds through their clearing and settlement agreements. Bank C charges a 2 per cent foreign exchange spread, which is around $20 in our case. Fourth, Bank C makes a payment to the receiver’s bank D through another payment system (II). Finally, Bank D transfers the $1,000 to the receiver but may charge an incoming wire fee of $15. The entire process involves 4 banks, two national payment systems, and an international agreement. Transaction fees and unfavorable exchange rates add up to $60 (sometimes more) costs to the process, making it cumbersome and costly. In addition, it is a slow process that takes up to 3 to 5 days for the transfer to complete given the number of intermediaries involved.

Figure 2 International Clearing and Settlement



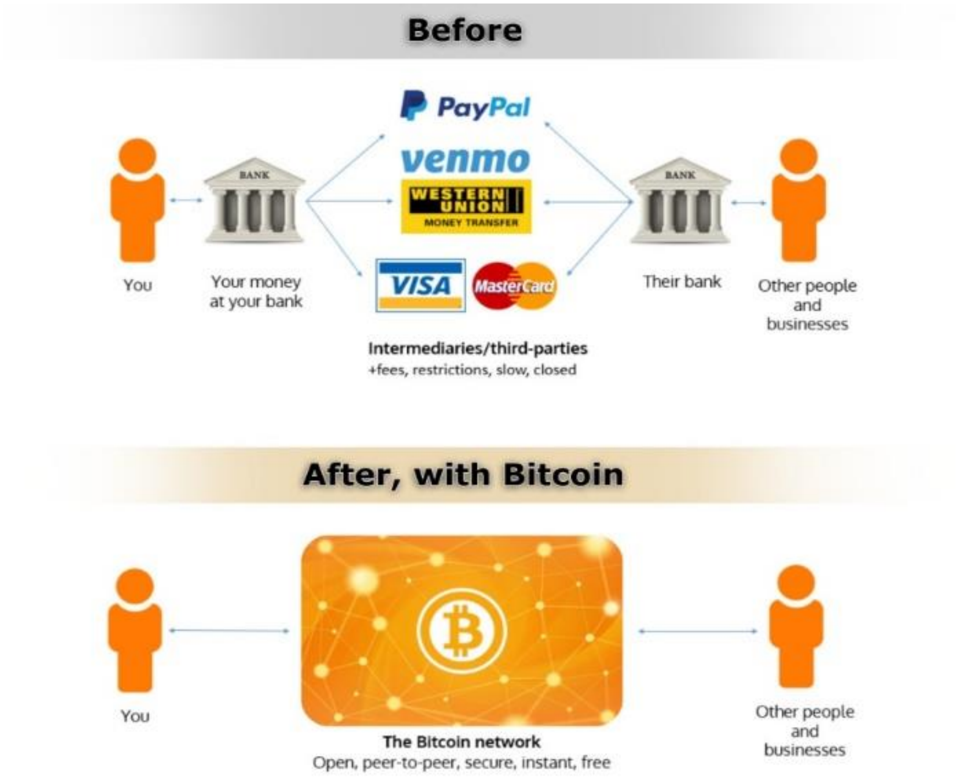
(Source: http://paymentsviews.com/2014/05/15/there-is-no-such-thing-as-an-international-wire/ (modified))

By contrast, Bitcoin payments are collected, validated, and updated every 10 minutes on average in so-called “blocks” by network validators called “miners” who “can leave and rejoin the network at will” (Nakamoto, 2008). Miners update and maintain a copy of the blockchain, a distributed public ledger shared on the Internet across thousands of network nodes. It is inherently borderless and protected by strong cryptography. This means that editing the blockchain without consensual approval by stakeholders is infeasible, and that it cannot be forged or destroyed, even by insiders. Transactions on the blockchain are publicly auditable (Nian & Lee, 2015: 15), which results in greater transparency. No intermediaries (e.g., banks, credit card companies, clearing houses) are required, which reduces transaction fees by one or two orders of magnitude relative to the traditional payments industry (i.e., users only need to pay a small fee to the miners who power and secure the network). Thus, an international transfer of $5,000 with Bitcoin would involve a fee[3] of perhaps $2 whereas a retail bank would typically charge in excess of $100 to complete the same transaction.

Figure 3 represents a simple comparison between traditional banking and Bitcoin transactions.

[3] Fees are given as tips, therefore they are voluntary and market based,

Figure 3 Bitcoin vs. Traditional Banking


Before
PayPal
venmo
WESTERN UNION MONEY TRANSFER
VISA
MasterCard
BANK
BANK
You
Your money at your bank
Their bank
Other people and businesses
Intermediaries/third-parties
+fees, restrictions, slow, closed
After, with Bitcoin
You
The Bitcoin network
Open, peer-to-peer, secure, instant, free
Other people and businesses

(Source: https://medium.com/@liamzebedee/3-essential-takeaways-from-the-mit-microsoft-bitcoin-talk-54a4cd71a702#.l7zeppbil)

2.2 How Does Bitcoin Work ?

A payment system powered by machine routines. As a software protocol, coordination of work is rooted in the idea that “code is law” (Lessig, 2006). In contrast to traditional organizations that use human managers to strategically design routines, Bitcoin follows machine routines written in the formal software protocol, which define organizational programs such as plans, rules, and incentives. Machine routines refer to formal agreements, such as responsibility for tasks (i.e., who does what), schedules (i.e., when things should happen), and rules (i.e., how things should be done) written in the self-executing protocol.

As a payment system, the Bitcoin protocol requires that all exchanges and contractual relationships be broadcasted, verified, and maintained by a distributed network and updated on a shared blockchain ledger that is append-only and tamper-proof. Bitcoin secures its network through a "competitive bookkeeping" process called "mining" (Yermack, 2017).

Mining is a process in which specific network nodes ("miners") compete to validate transactions, arrange new transactions into a sequence, and time-stamp them by solving a "hash algorithm." The process can be hastened by committing more computing power to the network. Thus, a miner's chance of being able to provide the "proof-of-work" (PoW) required to update the ledger is proportional to the computing power s/he controls. The computing power committed every 10 minutes to blocks of transactions recorded in the ledger accumulates and forms a barrier to hacking, making it practically impossible to edit past transaction records contained in the blockchain (i.e. the proof-of-work would have to be entirely redone for every block added after the edited one, which is too computationally intensive and too costly to achieve). Successful miners are rewarded in Bitcoin in accordance with protocol for their work, which involves costs in hardware and electricity, as per the Bitcoin protocol.

All miners perform the same task of collecting and verifying transactions, and compete to solve the hash algorithm using their own computing power. Only the first miner who solves the problem gets to record the collection of transactions on the public blockchain ledger; the thouands who have tried and failed get nothing. This process repeats itself every 10 minutes. As a result of mining, machine routines are able to prevent cyber-attacks and to continuously keep track of transactions (Antonopoulos, 2014).

The process is not dissimilar to gold mining, insofar as rewards are determined randomly. According to the Bitcoin white paper, "[t]he steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation" (Nakamoto, 2008). It would be inconceivable for a traditional business organization to ask all employees to perform the same routine task but to only reward one person with all other people's effort going wasted. A system that creates thousands of redundancies is highly inefficient if most of the resources used as input are purposefully wasted (Swanson, 2015)[4]. Yet, the counter-intuitive reward distribution process employed by Bitcoin allows it to provide both security and decentralization (Lopp, 2016). By reducing the likelihood of having a single point of failure, the reward distribution process makes the system highly reliable (Swanson, 2015). Given the size of the mining network, it would be impossible for a single miner to have enough computing power to control over 51 per cent of the representation for decision making (Nakamoto, 2008; Swanson, 2015).

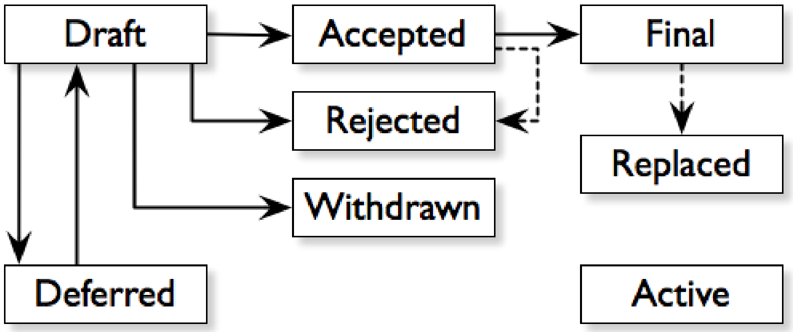
2.3 Protocol Update

What happens when decisions need to be made about the code? For issues such as bugs, code modifications, and community decisions, coordination needs to happen within and between stakeholder groups to ensure effective communication. Formal and informal channels exist to faciliate communication and decision making. Moreover, miners can cast votes on the blocks they upload to siginal support for a proposed protocol change.

Take, for example, the Bitcoin Improvement Proposal (BIP), “a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment” (GitHub BIPs, 2018). The BIP addresses issues, proposes features, or documents decisions with “concise technical specification of the feature and a rationale for the feature” (GitHub BIPs, 2018). As shown in Figure 4, The coordination process involves developers making a proposal, e.g., asking miners to vote on a code implementation. A majority vote for yes would move the implementation forward. This BIP is open and can be extended to all interested parties.

[4] It is important to distinguish mining from the “winner-take-all” logic of innovation (Katz & Shapiro, 1994), in which the dominant design claims all the network effects. While slack resources are necessary for exploratory activities involving risk-taking, experimentation, and creativity resulting in highly uncertain outcomes that are difficult to value (March, 1991), mining is concerned with well defined, highly formalized routine tasks with specific goals.

Figure 4 Bitcoin Improvement Proposals (BIPs) Voting Process



(source: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki)

2.4 Bitcoin as the First Decentralized Autonomous Organization

Bitcoin effectively "runs a payment system" and "employs subcontractors who are miners" and who are paid "with newly issued bitcoin shares" (Latimer, as quoted by Vigna and Casey, 2015: 229). Unlike traditional corporations, Bitcoin is a non-hierarchical organization that does not have shareholders, managers, or employees. Tasks related to currency issuance, payment processing, and maintenance of the shared public ledger are performed through machine routines written as open-source software, by volunteers who contribute programming skills and computing power to the network. The Bitcoin system thus shares the four core features common to all conceptualizations of the "organization": it is a "multi-agent system […] with identifiable boundaries and [a] purpose […] towards which the constituent agents' efforts make a contribution" (Puranam, 2017: 6). Thus, Bitcoin is not only a technological breakthrough that establishes the possibility of consensual agreement on the state of a distributed database without having to rely on a trusted authority[5], but also an organizational design innovation.

[5] This represents an innovative solution to an old network engineering problem known as the "Byzantine Generals' Problem" (Lamport, Shostak & Pease, 1982; Fisher, Lynch, and Paterson, 1985). Please see Appendix A for detailed explanation.

Bitcoin differs from “distributed organizations” such as Wikipedia (Lee & Cole, 2003; Shah, 2006) by grounding its design and task coordination in a cryptographically secured blockchain that cannot be edited without consensus among network participants. Unlike an online encyclopedia, a payments network must be highly predictable; it cannot tolerate the temporary editing of database entries until further verification has occurred. Otherwise, a user who holds $1 million worth of Bitcoin could see her account balance reduced to zero for some period of time, which would destroy her trust in the system. To prevent this, Bitcoin puts machine routines at the center of the system, and self-interested humans at the edges. Reliability is rooted in the code, in cryptography, and in the distributed network rather than in intermediaries (Nian & Lee, 2015: 14-21; Antonopoulos, 2014: 15). In other words, Bitcoin is simultaneously autonomous and decentralized—that is, it is a “decentralized autonomous organization” (DAO). These considerations lead us to the following question: how can tasks be adequately coordinated to enable organizational growth without placing human decision makers at the centre?

2.5 Cryptocurrencies beyond Bitcoin

Two years after the formation of Bitcoin, a number of other DAOs were created to compete against it in the cryptocurrency industry. For example, Peercoin introduced a new class of machine routines that relied on “proof-of-stake” (PoS) algorithms. With PoS, the chance that a “network validator” will be selected to add a new block of transactions to the chain depends on her “stake” in the ecosystem, i.e., how much cryptocurrency she owns, whereas, with PoW, her chance of being selected depends solely on the amount of computing power she is able to commit to the network (Narayanan et al., 2016: 40–45; 206–211). Network validators are voluntary contributors who invest their own resources (e.g., computing power or capital in the form of digital tokens) to maintain and secure the network in exchange for cryptocurrency rewards. In PoW systems, network validators are known as “miners.” Hybrid implementations, with mixed PoW and PoS mechanisms, meanwhile, provide a rich setting in which to study a broad range of coordination mechanisms.

At the time of writing, there were more than 1,500 cryptocurrency DAOs on the market. 40 cryptocurrencies have a market capitalization of $100 million or more, including 7 “unicorns” worth at least $1 billion (Coinmarketcap.com, July 13, 2017). Each cryptocurrency offers its own design features and coordinates organizational tasks in different ways in order to provide a variety of services to users looking for decentralized and disintermediated alternatives to traditional competitors (e.g., Visa, Western Union, Wells Fargo). It should be noted that, while our study of DAOs takes place within the cryptocurrency industry, DAOs are also used to manage transactions of non-currency assets such as diamonds, artwork, and shipping containers. My decision to focus on cryptocurrencies was motivated by the fact that this industry represents the largest and most mature sector in which the DAO form has been implemented.

2.6 Other Unique Features of Cryptocurrencies

There are a number of features that are unique to cryptocurrencies, which cannot be found in other open source software projects. These features are mostly enabled or enhanced by economic agents, i.e., miners or network validators, through the competitive bookkeeping (mining) process.

Digital scarcity. Mining based on PoW is energy intensive (Swanson, 2015). Yet, it is this very characteristic that artificially creates an “unforgeable scarcity” (Tschorsch & Scheuermann, 2015), endowing Bitcoin with gold-like properties. It is important to note that, while artificial scarcity can be achieved through control of the coin supply, it takes mining to make this scarcity unforgeable and decentralized. I will elaborate on these characteristics in following sections. At present, I will focus on the issue of scarcity per se.

As noted above, the distribution of Bitcoin does not rely on centralized issuers, but PoW mining. The seignorage, i.e., the difference between the cost of minting a coin and the value of the coin, is distributed as a reward to miners as new Bitcoin issued to the market (Swanson, 2014). “This scarcity creates a value, which is backed up by the real-world (computational) resources required to mint it” (Tschorsch & Scheuermann, 2016). In other words, the task of coin issuance is coordinated through artificial scarcity backed by intensive energy consumption. The speed of coin issuance is regulated by “mining difficulty," and the hash algorithm is adjusted every 14 days. For Bitcoin, scarcity is purposeful.

Given the value generated by new coin issuance, however, the required energy consumption seems disproportionate. It is estimated that, by 2020, Bitcoin could consume as much electricity as Denmark (Deetman, 2016).

Immutability and Security. Recall that scarcity produced by PoW is "unforgeable" (Tschorsch & Scheuermann, 2015). Recall as well the centrality of the concept of immutability to Bitcoin. Immutability is reflected by the fact that once transaction records are updated on the blockchain ledger they cannot be reversed (Lopp, 2016; Narayanan et al., 2016).

Traditional banking is plagued by both data security and agency problems. Bank managers and employees are under tremendous pressure to bring in new customers to meet sales targets. Both the incentivization of opportunistic practices and misconduct are common characteristics of the financial industry—the Wells Fargo scandal, involving 2 million fake accounts created by 5,300 employees, exemplifies the potential scale of agent misconduct in this sector (Egan, 2016).

Bitcoin also offers a solution to the biggest security threat to any decentralized digital payment system, namely, double spending. Double spending occurs when digital money (e.g., digital tokens) is sent (and spent) more than once (Nian & Lee, 2015: 15). Immutability permits high security in the Bitcoin system, thus minimizing the threat of double spending (Swanson, 2015).

PoW consensus requires that the correct chain used for payment validation is always the "longest chain." The amount of work required to reverse the transaction history increases exponentially relative to the length of the transaction history (i.e., the "block height") and the size of the network (Leonardos, Kiayias & Garay, 2014). The security and reliability of Bitcoin also increase is relation to the length of the blockchain and the size of the mining network. Any attempt to tamper with the blockchain does not make economic sense, because an attacker needs to control over 51 per cent of the computing power of the entire network to assume control and dominate decision making. This is simply too expensive (Nakamoto, 2008; Swanson, 2015). Energy consumption and the capital costs of the mining hardware thus serve as a barrier to attempts to tamper with the blockchain or to double spend (Torpey, 2015). As a result, the distributed network is both “resistant to and…resilient against attack” (Killeen, 2015).

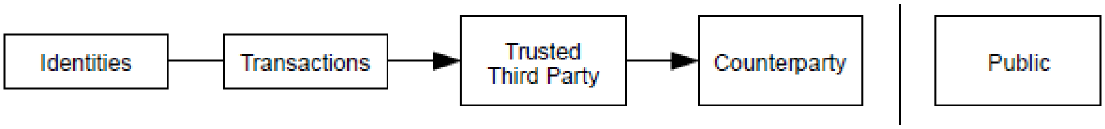
2.7 Other Features (not directly enabled through mining)

Transparency. Transparency is another unique feature of Bitcoin. Not only is the Bitcoin code open source for testing and development, but transactions on the blockchain are also publicly auditable (Nian and Lee, 2015: 15). Information transparency significantly reduces the interdependency caused by information asymmetry.

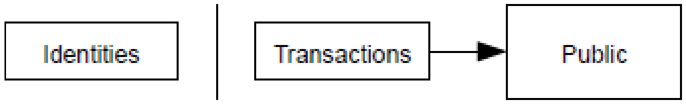
Pseudonymity. Bitcoin transactions do not require exchange parties to reveal their real-world identity. One cannot open a traditional bank account without official identification; in the developing world, this often prevents access to banking. By contrast, anyone can become a Bitcoin user and freely obtain a pseudonymous Bitcoin address. In essence, a Bitcoin address is a public key cryptographically linked to a private key acting as a password to spend funds. The key pair is for digital signatures—whereas the public key is used to verify incoming funds, the private key is used to sign and spend funds. This enables a new privacy model that separates transactions from identity (Nakamoto, 2008). Figure 5 compares the Bitcoin privacy model with the traditional banking model. The vertical bar in the New Privacy Model indicates where Bitcoin interrupts the flow of information.

Figure 5 Traditional Privacy Model vs. the Bitcoin Privacy Model

<u>Traditional Privacy Model</u> (adopted from Nakamoto, 2008)



<u>New Privacy Model</u>



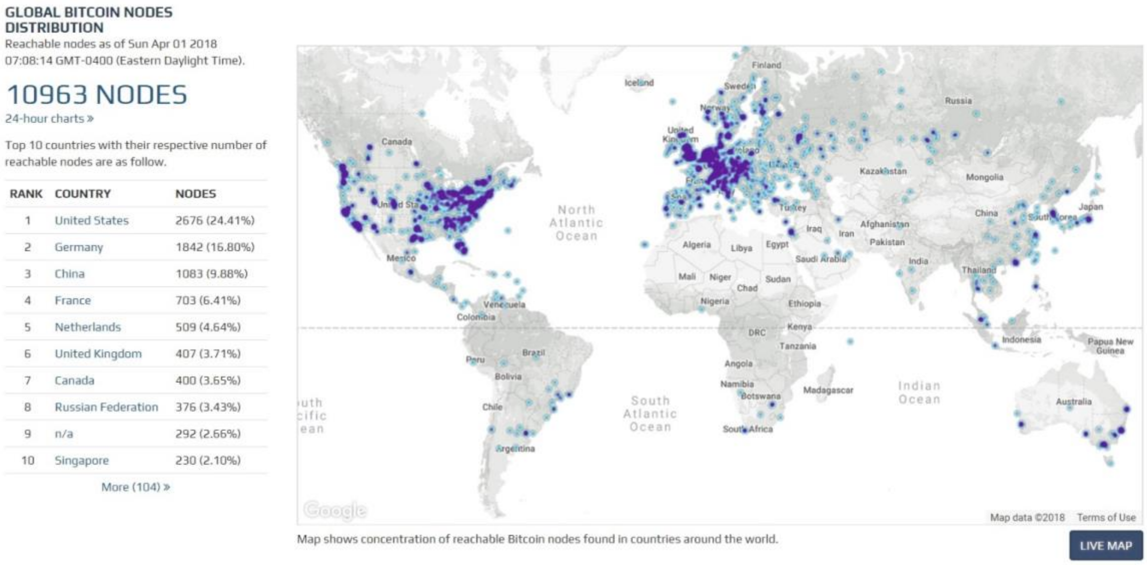
Insofar as public keys are recorded and are trackable, Bitcoin is pseudonymous rather than anonymous. Nevertheless, pseudonymity adds another layer of protection and security to Bitcoin. This property endows cryptocurrencies with the cash-like characteristics, e.g., fungibility, with interchangeable units whose value is not attached to any user identities.

2.8 The Growth of Cryptocurrency DAOs

In the 9 years since its formation, Bitcoin's market capitalization has increased from $0 to $300 billion (at its height). Over 450 developers regularly contribute to the code (with many more contributing on an ad hoc basis); 200,000 transactions (worth, on average, $3,500) are processed every day; more than 11 million user accounts, known as "Bitcoin wallets," currently exist (GitHub.com, 2017; Blockchain.info, 2017). To put things into perspective, the computing (or "hashing") power that fuels the Bitcoin DAO is 100 times greater than that of Google.

Figure 6 indicates the geographic distribution of the Bitcoin network. Currently, there are more than 10,000 nodes worldwide.

Figure 6 Bitcoin Global Network



GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Sun Apr 01 2018 07:08:14 GMT-0400 (Eastern Daylight Time).

10963 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2676 (24.41%)
2	Germany	1842 (16.80%)
3	China	1083 (9.88%)
4	France	703 (6.41%)
5	Netherlands	509 (4.64%)
6	United Kingdom	407 (3.71%)
7	Canada	400 (3.65%)
8	Russian Federation	376 (3.43%)
9	n/a	292 (2.66%)
10	Singapore	230 (2.10%)

More (104) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

(Source: https://bitnodes.21.co/, Accessed March 2018.)

How can a DAO without centralized authority achieve market capitalization comparable to that of such major banks as JP Morgan ($376 billion) or Bank of America ($300 billion)? How can a 9 year-old DAO perform tasks more effectively than banks that have been around for more than a century? How can a DAO without professional managers and employees provide faster, cheaper, and arguably more secure services than traditional financial institutions? These questions matter to practitioners and to management scholars alike. According to experts, the true innovation that makes this growth possible is the way in which various stakeholders within the DAO are coordinated and agree on the evolution of the organization (Ryan Zurrer, keynote speaker at the First Annual Toronto FinTech Conference, 2017; Narayanan et al., 2016; Buterin, 2017a). To understand coordination and growth within DAOs in the cryptocurrency industry requires that we review our current thinking about organizational growth, coordination, and consensus.

Chapter 3 Literature Review

3 Literature Review

In the following chapter I will review three related concepts: organizational growth, coordination, and consensus. Using an organization design perspective, I will unpack the novelty of DAOs and identify opportunities for theory building.

3.1 Theoretical Motivation: Why the Organization Design Lens?

Organization design focuses on the problem of how to optimally align the internal structure of the organization with the tasks it performs and the technological environment in which it operates (Thompson, 1967; Tushman & Nadler, 1978; Galbreith, 1974). Therefore, an important objective of organization design is to devise strategic solutions to such universal problems as task division, task allocation, reward provision, and information flows (Puranam et al., 2014). As a result, new organizational forms emerge as strategies that may be used to enable different forms of coordination, thus highlighting the need for organizational flexibility, learning, and change (Daft & Lewin, 1993).

3.1.1 The Divide: Organizational Innovation vs. Technological Innovation

Organization design is currently undergoing an exciting phase of expansion and transformation. Powered by technological innovations, new forms of communication and collaboration have emerged. Faced with technological shifts, organizations often need to adopt new forms to respond to the changing landscape. Organizations experiencing technological change may adopt modular forms (Schilling & Steensma, 2001; Puranam & Jacobides, 2006), boundary structures (O’Mahony & Bechky, 2008), or autonomous units (Birkinshaw, Nobel & Ridderstråle, 2002) in order to deal with inter- or intra-organizational learning, integration, and innovation. It is believed that technologies spawn new possibilities for organizational designs, which, in turn, bring about novel forms (Daft & Lewin, 1993; Kapoor & Lee, 2013; Puranam, Singh & Zollo, 2006; Vaast & Levina, 2006).

In the past two decades, the scope of organization design has also been broadened from “intentionally designed” organizations to include “emergent” organizations (Puranam et al., 2014). Many Open Source Software Development (OSSD) projects, for example, are managed in community forms to facilitate knowledge sharing and participation. They follow an emergent architecture, which relies on voluntary workers to develop the codebase (O’Mahony, 2007; O’Mahony & Ferraro, 2007; von Hippel & von Krogh, 2003; Zammuto, Griffith, Majchrzak, Dougherty & Faraj, 2007; von Krogh & von Hippel, 2006).

Common to these organizational design themes is that they have relied on two implicit assumptions to make sense of technologies. The first assumption is that technology may be conceptualized as tools and artifacts that are mindfully adopted to enable certain organizational features (e.g., virtual teams) and to influence organizational performance (Huber, 1990; Faraj, Jarvenpaa & Majchrzak, 2011; Garud, Kumaraswamy & Sambamurthy, 2006). In other cases, technology may be conceptualized as a product category (as in the case of OSSD), or a context (Barley, 1986), in which organizational forms are treated as separate entities designed to facilitate the exploitation or the development of the technology. The second implicit assumption is that human agents are at the centre of decision making for the four organizing problems: task division, task allocation, reward provision, and information provision (Puranam et al., 2014).

The emergence of DAOs and blockchain technology casts doubt on these assumptions. For DAOs, the relationship between technology and organization appears to be reversed; alternatively, the two may be understood to have converged. In contrast to the traditional belief that organizational innovation is enabled by technology, I will argue that blockchain technology cannot be implementable unless organizational participants are organized in a decentralized and autonomous manner. Yes, one can argue that the blockchain program was made possible by the 30,000 lines of code written by Nakamoto (2008), and that the blockchain program is indispensable to the blockchain technology underlying DAOs. The protocol is enabled by computer science technologies, such as cryptography, and is not so very different from other computer-aided organizational forms. However, at least one miner and a few users need to act as “seed nodes”

(Antonopoulos, 2014: 145), and form a “seed DAO” ex ante to kick off the bootstrapping[6] process (Narayanan et. al., 2016). For blockchain technology to enable faster, cheaper, and secure peer-to-peer transfer of value without relying on third party intermediaries, it is necessary to have mining that coordinates and integrates the tasks performed by various stakeholders across different levels. This also means that coordination, technology, and, consequently, organizational growth become intertwined.

A number of scholars have theorized about this convergence. For instance, Garud and colleagues (2006) maintain that technology is part of organization design and plays an important role in the evolution of the organization. Baldwin and Clark (2006) examine the ways in which the architecture of the OSSD codebase interacts with the architecture of the organization through code modularity and option values. These two properties are thought to mitigate free riding, thus allowing developers’ personal interests to better align with organizational goals (Baldwin & Clark, 2006). Neverthleless, we need to think more about these technologies. As an organization design innovation, DAOs take our conceptualization about technology to another level by decentralizing authority, trust, and governance. DAOs play a central role in blockchain-based technological innovation, and require us to think about organizational growth, coordination, and consensus at a different level of abstraction. We need to theorize more deeply about DAOs, and the means by which they have used codebase architecture to serve as both organizational architecture and organizing principle.

While scholars have long acknowledged that the emergence of new forms of organization outpaces academic research, this gap has widened as the boundaries of organization design and technological innovation increasingly blur (Daft & Lewin, 1993; Miller, Greenwood & Prakash, 2009). My research responds to this call by identifying DAO organization design as the bedrock of the blockchain innovation.

[6] Bootstrapping refers to the process by which the three preconditions for a cryptocurrency DAO, namely, “the security of the blockchain, the health of the mining ecosystem, and the value of the cryptocurrency” begin to interact with one another and reinforce one another to kickstart growth (Narayanan et al., 2016).

3.2 Organizations as Coordination Systems

Coordination is the main focus of organizational design and redesign (Galbraith, 1973; 1974; Lawrence & Lorsch, 1967; March & Simon, 1958; Thompson, 1967; Tushman & Nadler, 1978). An organization may be understood as a coordination system "that integrates a collective set of interdependent tasks" (Okhuysen & Bechky, 2009). Therefore, task coordination patterns should be adjusted to the type of interdependence in question.

Although early conceptualization treated coordination mechanisms as inherently strategic (Daft & Lewin, 1993), scholars have recently argued that the human agents who design and adjust the coordination mechanisms need not be managers (Srikanth & Puranam, 2014; Okhuysen & Bechky, 2009). Coordination research also incorporates emergent practices and bottom-up approaches to management, and adopts a dynamic perspective to study coordination of organizational routines, learning, and the emergence of organizational structure (Brown & Duguid, 2001; D'Adderio, 2014; Malnight, 2001; Parmigiani & Howard-Grenville, 2011; Young-Hyman, 2017). In this line of research, coordination mechanisms are conceived of as dynamic processes through which organizations iterate and modify routine activities to achieve stable outcomes (Jarzabkowski, Le & Feldman, 2012). As such, distributed coordination is made possible through communities of practice in which collective competence, knowledge, and capabilities are enacted rather than treated as given (Brown & Duguid, 1991; 2001; Orlikowski, 2002).

While these recent studies have shifted the focus of organizational coordination from top managers at the corporate level to frontline employees at the team level, they still regard coordination as a function embedded in a hierarchy, though, this time, from the bottom up.

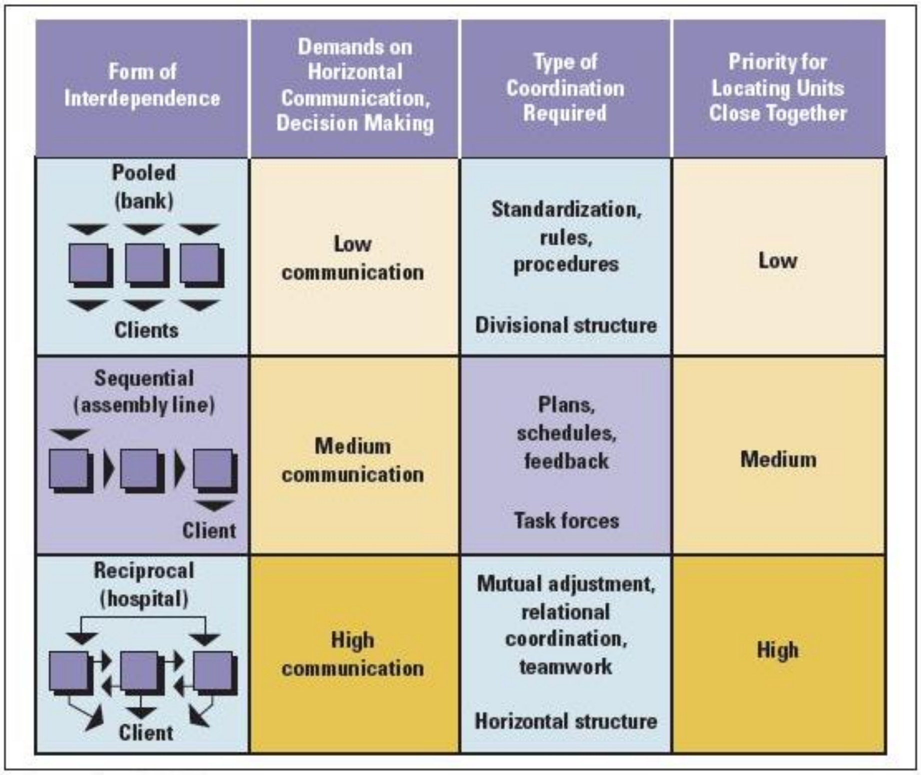
3.3 What is Being Coordinated? The Nature of Task Interdependence

Since coordination concerns the integration of interdependent tasks, the type of coordination required corresponds closely to the nature of task interdependence

(Thompson, 1967; Daft & Armstrong, 2012). Interdependence is defined as “the extent to which departments depend on each other for resources or materials to accomplish their tasks” (Daft & Armstrong, 2012). Consequently, the value generated by performing interdependent tasks together will differ from the value generated by performing individual tasks separately (Puranam, Raveendran & Knudsen, 2012).

Table 1 lists the classic categories of interdependence, namely, pooled (e.g., banks), sequential (e.g., assembly line), and reciprocal (e.g., hospital) (Thompson, 1967; Daft & Armstrong, 2012).

Table 1 Thompson’s Classification of Interdependence and Management Implications



Form of Interdependence	Demands on Horizontal Communication, Decision Making	Type of Coordination Required	Priority for Locating Units Close Together
Pooled (bank) Clients	Low communication	Standardization, rules, procedures Divisional structure	Low
Sequential (assembly line) Client	Medium communication	Plans, schedules, feedback Task forces	Medium
Reciprocal (hospital) Client	High communication	Mutual adjustment, relational coordination, teamwork Horizontal structure	High

© Cengage Learning 2013

(Source: Daft, 2013)

Pooled interdependence, for instance, involves tasks performed independently and then pooled back to the overall organizational level (e.g., banks divide transactions into independent subtasks that can be dealt with independently by various divisions and their multiple branches). Typically, pooled tasks can be coordinated through standardized rules and procedures due to low interdependence (Thompson, 1967; Daft & Armstrong, 2012; Okhuysen & Bechky, 2009).

When the input of one task is dependent on the output of another, sequential or reciprocal interdependence will be present. These two forms entail greater interdependence than the pooled form, and thus require different types of coordination, such as feedback, schedules, or lateral communication and mutual adjustment (Thompson, 1967; Daft & Armstrong, 2012; Okhuysen & Bechky, 2009). The next section explains coordination mechanisms in greater detail.

3.4 Coordination Mechanisms

Although the literature on coordination discusses both inter- and intra-organizational levels, my research focuses on the latter. Traditionally, coordination mechanisms entail the use of: (1) programing, i.e., coordination by programs, plans, rules, routines, targets, and goals; (2) feedback, including mutual adjustment and communication; and (3) hierarchy, i.e., supervision required for issues beyond programming and feedback (Galbraith, 1973; 1974; Tushman & Nadler, 1978; Okhuysen & Bechky, 2009; Puranam et al., 2012). The greater the uncertainty caused by task interdependence, the greater the need for coordination.

For tasks with low interdependence, work can be coordinated through standardized procedures, such as rules or programs, which define responsibilities and resource allocation. Formal components, such as schedules, routines, and meetings, can be used to implement formal coordination mechanisms (Thompson, 1967; Okhuysen & Bechky, 2009). In addition, tools and information technologies can assist teams to align their work. For example, boundary objects allow groups to better communicate progress (Bechky, 2003; Carlie, 2002).

As we shift from a manufacturing-centered to knowledge-based economy characterized by greater complexity, coordination also shifts from being standardized and formal to being characterized by knowledge sharing (Carlile, 2002; Deken, Carlile, Berends & Lauches, 2016), communication (Dahlander & O’Mahony, 2011), and flexibility (Bechky, 2006). Work is aligned through the creation of mutual understanding. In response, scholars have adopted a more dynamic view, treating coordination as an emergent process that changes with the design (which unfolds as things happen) (Weick, 1995; Garud et al., 2006). Finally, for uncertainties and interdependence originating from the need for supervision, formal hierarchies enable actors to use their roles to obtain consistent understanding of project status and coordination (Bechky, 2006; Okhuysen & Bechky, 2009; Tushman & Nadler, 1978).

3.5 Coordination without Hierarchy: The Case of OSSD

While hierarchies based on centralized authority have traditionally served as the backbone of organizational coordination, decentralized organizations found in the OSSD sector have recently emerged as non-hierarchical alternatives to this model (O’Mahony, 2007). Indeed, studies on OSSD examine the possibility of decentralizing organizational coordination in projects that govern software development through online communities, non-profit foundations, or corporate consortia (O’Mahony & Ferraro, 2007; Dahlander & O’Mahony, 2011; O’Mahony & Ferraro, 2007; O’Mahony, 2007; O’Mahony & Bechky, 2008; Shah, 2006). In OSSD contexts, community governance is a common feature (O’Mahony, 2007; Shah, 2006), and projects are characterized by non-hierarchical, self-organized decision making by voluntary contributors who are motivated by practical needs or intrinsic fulfilment (O’Mahony, 2007; Shah, 2006).

Typically, this type of coordination is based on technical contribution and open communication. Despite being non-hierarchical, OSSD communities evolve in such a way that certain forms of formal authority and career progression to the center are sought after (O’Mahony & Ferraro, 2007; Dahlander & O’Mahony, 2011). For example, contributors who do good work that gets noticed by the community gain legitimacy and reputation over time (Dahlander & O’Mahony, 2011), and the very best (non-anonymous) contributors can acquire an informal “advisor” status, which positions them at the center of the project’s network of stakeholders. This means that, despite a lack of formal hierarchy, a certain degree of centralization can emerge over time in OSSD projects, and thus it is best to conceive of (de)centralization as a continuum, rather than as a binary feature of organizational life.

As Mintzberg (1979) proposes, “the fundamental ways in which organizations coordinate their work . . . should be considered the most basic elements of structure, the glue that holds organizations together.” Given that organizations can accomplish complex tasks with or without a formal hierarchical structure, we would argue that, although it may be true that an organization can function without hierarchy, it certainly cannot function without coordination.

3.6 Integrating Conditions for Coordination: Accountability, Predictability, and Common Understanding

A universal working assumption in early coordination research (Taylor, 1911; Fayol, 1949) is that we need human decision makers—typically, managers—to design and adjust the “three integrative conditions for coordinated activity: accountability, predictability, and common understanding” (Okhuysen & Bechky, 2009: 463). The three integrating conditions provide the means for “people [to] collectively accomplish their interdependent tasks in the workplace” (Okhuysen & Bechky, 2009). Accountability pertains to the definition of responsibilities channeled through formal and informal structures. Scholars have also long argued that hierarchy is a typical and effective coordination mechanism for achieving accountability (Lawrence & Lorsch, 1967). Predictability refers to the understanding of how subsequent tasks are related to each other and what to anticipate (Okhuysen & Bechky, 2009). Expectations can also be aligned among interdependent parties about their work with “predictive knowledge” about other parties’ behavior (Puranam et al., 2012; Okhuysen, 2005). Lastly, common understanding entails “a shared perspective on the whole task and how individuals’ work fits within the whole” (Okhuysen & Bechky, 2009). Common understanding coordinates work by establishing shared knowledge about specific tasks (Hoegl, Weinkauf & Gemuenden, 2004; O’Mahony, 2003).

Organizations can achieve these integrative conditions through various configurations of coordination mechanisms. For instance, accountability can be enhanced by using roles in the hierarchy and through monitoring, feedback, and communication to establish trust (Bechky, 2003; Mark, 2002; Jarzabkowski, Le & Feldman, 2012; Okhuysen & Bechky, 2009). “Common understanding can be developed when plans are created by senior managers and handed down a hierarchy to be implemented by those lower in the organization” (Okhuysen & Bechky, 2009: 488). Similarly, mechanisms for allocating resources, defining roles and responsibilities, sharing information, monitoring performance, or creating proximity all enhance coordination by contributing to organizational accountability, predictability, or common understanding.

3.7 Coordination and Consensus

Consensus is an important enabler for coordination in that it reflects the level of agreement necessary for common understanding (Okhuysen & Bechky, 2009; Kellermanns, Walter, Lechner & Floyd, 2005; St. John & Rue, 1991). According to the definition of Kellermanns and colleagues (2005), strategic consensus is defined as “the shared understanding of strategic priorities among managers at the top, middle, and/or operating levels of the organization” (Kellermanns, Walter, Lechner & Floyd, 2005). Despite being ubiquitous in organization studies, the nature of consensus has mostly been discussed as a state in which top management teams, groups, or organizational control systems are employed for effective coordination (Mintzberg, 1979: 142; Barker, 1993; Amason, 1996; St. John & Rue, 1991). For example, Barker (1993) delineates how value consensus among self-managed team members enables “concertive control” (based on normative rules) through manifests, resulting in a flatter organization. At the organizational level, the viability of consensus is contingent upon various internal and external resource constraints (Dess, 1987; Dess & Origer, 1987; Homburg et al., 1999). At the field level, institutional theorists have studied how consensus forms and falls apart in the formative stage of a field, during which conflict can be resolved through communication, managerial authority, formal or informal rhetoric, and action (Grodal & O’Mahony, 2015). Overall, consensus is considered a desired state or “common end” for both centralized and emergent strategic decision making as it facilitates coordination (Grodal & O'Mahony, 2015; St. John & Rue, 1991).

In addition to a "common end" state, consensus is also treated as a by-product of the group approach toward strategic decision making (Schweiger, Sandburg & Ragan, 1986; Amson, 1996; Eisenhardt & Zbaracki, 1992). "Human systems ought to have a clear, consensus-based goal to guide behavior" (Bourgeois, 1980). The assumption is that consensus facilitates decision-making quality and performance outcomes (Amason, 1996). While studies on consensus focus primarily on strategic decision making among top managers in the strategy formulation stage (e.g., Bourgeois, 1980; Dess, 1987; Dess & Origer, 1987; Eisenhardt & Zbaracki, 1992; Homburg, Krohmer & Workman Jr., 1999; Priem, 1990), consensus in the strategy implementation stage receives relatively little attention.

This is because the scope of consensus research mainly focuses on the role of top managers. The conjecture is that once the top management team agrees on the goals and actions of a policy, organizational members (i.e., employees) follow the mandates that have been agreed upon. There is a clear group of "strategic decision makers," devising goals and policy alternatives either following a rational-comprehensive logic or a political-incremental rationale in the strategy formulation stage (Bourgeois, 1980; Dess & Origer, 1987; Wooldridge & Floyd, 1989; Kellermanns, Walter, Lechner & Floyd, 2005).

In recent years, consensus at much lower levels of the organization has begun to receive attention from scholars studying less-hierarchical self-managing organizations (Lee & Edmondson, 2017). For example, organizations such as Zappos or Ternary adopt an organizational system called Holacracy, in which individuals are directed by role-based definition rather than managers (Bernstein, Bunch, Canner & Lee, 2016). Full autonomy is granted to organizational members who follow formal role definitions but, at the same time, have the flexibility to discuss rule changes in "governance meetings." Members propose, discuss, and consent to proposals in governance meetings to activate change. Similarly, in participatory decision making, consensual agreement serves as the means of organizational governance (Black & Gregersen, 1997). Overall, for organization designs in which authority is distributed, consensus about the normative features of the organization—how different roles should be defined or how work should be designed□is bottom-up and formed among the participants (Lee & Edmondson, 2017). With an emphasis on the task level, the literature on self-managing organizations extends the scope of consensus from the management level to the operating level and from top-down to bottom-up.

Arguably, blockchain-based consensus is of a different nature. Instead of agreeing on the normative features, organizational participants agree on the basic facts in a deterministic way. The DAO network must, for instance, agree on which transactions have taken place, when they happened, and who relayed which block of transactions (e.g., as in blockchain explorers such as https://btc.com/). In section 3.9 and in Chapter 4, I will elaborate on how the idea of consensus has shifted in blockchain-based organizations.

3.8 Coordination and Growth

With or without a hierarchy, a properly coordinated organization should be able to scale its operations. Specifically, coordination affects organizational growth by enhancing—and sometimes balancing—efficiency (Nickerson & Silverman, 2003) and effectiveness (Doty, Glick & Huber, 1993; Lewin & Minton, 1986).

3.8.1 Growth based on Efficiency

From the standpoint of efficiency, organizations are more successful than markets in coordinating activities with high transaction costs; this is a key determinant for the expansion of organizational boundaries (Williamson, 1975). On the other hand, knowledge-based conceptualizations suggest that organizations are more efficient at coordinating knowledge assimilation, transfer, and integration (Cohen & Levinthal, 1990; Kogut & Zander, 1992; 1993; 1996; Garicano & Wu, 2012; Whetten, 1987). Managers typically assume a strategic role in designing the organizational structure by which tasks are allocated and integrated for enhanced efficiency, i.e., by way of optimal resource deployment (Faraj and Xiao, 2006).

Through social relationships, top managers are able to make decisions on resource allocation and capability building, leading to more effective exploratory and exploitative innovation and growth (Lavie, Stettner & Tushman, 2010; March, 1991). Similarly, in the case of new ventures or community-based non-profits, organizational growth relies on coordination based on social resources and social capital (Khaire, 2010; Galaskiewicz, Bielefwld & Dowell, 2006), founding team human capital (Tzabbar & Margolis, 2017; Baum & Bird, 2010), and development of managerial strategies to foster external partnership with high-status firms (Khaire, 2010). Coordinating through social relationships provides a basis for reputation and trust building within the organization, which brings down communication costs and enhances efficiency.

In non-hierarchical OSSDs, communities can evolve in such a way that certain forms of leadership emerge through the identification of informal advisors recognized as authoritative by community members (O'Mahony & Ferraro, 2007; Dahlander & O'Mahony, 2011). However, meeting efficiency requirements can be trickier in community-based organizations in which decision-making power is diffused and in which organizational members can come and go at will (O'Mahony & Ferraro, 2007; Okhuysen & Bechky, 2009).

3.8.2 Growth based on Effectiveness

From an effectiveness perspective, coordination also helps organizations achieve their goals by increasing the fit between the internal and external environment (Argote, 1982; Crowston, 1997; Galbraith, 1973, 1974; Lawrence & Lorsch, 1967; Srikanth & Puranam, 2014; Thompson, 1967; Tushman & Nadler, 1978). For example, coordination mechanisms such as planning, sharing updates, or trust building can help to mobilize organizational members around goals and objectives that are aligned with customer needs.

Overall, organizations are able to capitalize on efficiency and effectiveness and to achieve growth by mechanisms such as communication, routine, and learning (Starbuck, 1965; Whetten, 1987; Salomon & Martin, 2008). Note that the relationship between coordination and growth is particularly important for organizations that rely on network effects to scale. In fact, much of the OSSD literature attends to how community governance is linked to growth-enhancing network externalities (O’Mahony & Lakhani, 2011; West & O’Mahony, 2008; Dahlander & O’Mahony, 2011).

3.9 Opening the Black Box of Coordination within DAOs

How, in the absence of top management and a centralized decision-making process that ensures optimal efficiency and effectiveness, do DAOs coordinate tasks and achieve growth?

DAOs represent a case in which exchanges of value take place in non-hierarchical organizations governed by peer-to-peer, open networks. In many ways, DAOs epitomize an extreme form of decentralized organization. However, DAOs’ defining features go beyond decentralization and represent an under-socialized organizational terrain yet to be explored. According to the original Bitcoin white paper, which encapsulates key elements of Bitcoin’s coordination mechanisms, “nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone” (Nakamoto, 2008).

While it may be true that DAOs in the cryptocurrency industry require “little coordination” compared to traditional payment corporations, what is more striking is the fact that some of the coordination mechanisms on which DAOs rely are completely new. Scholars have always seen human agents (from managers to frontline staff) as the main source of task coordination. But DAOs, by placing “automation at the center [and] humans at the edges” (Buterin, 2014) of the organization, coordinate tasks using open-source software and a distributed ledger. Moreover, while DAOs rely on a community-based form of governance, they differ fundamentally from OSSD projects in terms of organization design and task coordination mechanisms. In fact, DAOs achieve accountability, predictability, and common understanding—the three integrative conditions for coordination (Okhuysen and Bechky, 2009)—in ways previously unseen.

Specifically, for DAOs to secure the network without a third-party intermediary vouching for every single exchange, agreement needs to be reached among the network validators.

> We need a way for the payee to know that the previous owners did not sign any earlier transactions […] The only way to confirm the absence of a transaction is to be aware of all transactions […] To accomplish this without a trusted party, transactions must be publicly announced[7], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.
>
> [The Bitcoin white paper, Nakamoto, 2008]

To provide security, consensus based on unanimity rule appears to be deterministic and central in DAOs insofar as every node runs the same protocol and agrees on one and only one true state of the blockchain ledger. However, unanimity rule in organization research is little studied. Romme (2004) argues that unanimity rule at a critical threshold enhances the organization's performance and the quality of its decision making. Unsurprisingly, Romme found that large groups are less responsive to unanimity rule than small units in a hierarchical structure. Unanimity rule is uncommon in traditional organizations, hence the lack of visibility in the literature. For traditional banks, the ledger is a database that stores transaction information and is separate from the evolution of the organization itself. This is not the case for DAOs, for whom consensus on the true state of the ledger is a prerequisite and a centripetal force which holds the organization together.

To conclude, in contrast to the extant literature that treats consensus as a state, common end, or by-product, for DAOs consensus is a precondition for task coordination. A lack of consensus implies a rejection of the organizing principle, which can bring progression to a halt or result in organizational division. How we think about consensus within such a sizable network requires that we take the consensus concept to a different level of abstraction and place it in the forefront of DAO coordination. I will discuss the notion of

[7] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998. Original citation in Nakamoto, 2008.

consensus and the lack thereof in Chapter 4, which details a pilot case study of the black box of coordination within DAOs using Bitcoin as the primary example.

Chapter 4 Distributed Consensus: The Case of Bitcoin

4 Distributed Consensus: The Case of Bitcoin*

** This chapter draws heavily from my paper "Bitcoin and the rise of decentralized autonomous organizations" co-authored with Dr. Jean-Philippe Vergne, forthcoming in the Organization Zoo Series of Journal of Organization Design.*

This chapter outlines a pilot case study and is intended to be descriptive and explanatory. My goal here is to identify the defining features of task coordination mechanisms within DAOs and to answer the following question:

How are decentralized autonomous organizations coordinated?

As the first and most established DAO, Bitcoin serves as a prototype, and allows for a deep understanding of DAO coordination. Launched in 2009, Bitcoin, with its underlying blockchain technology, has been characterized as a game changer by the mainstream media (e.g., the Economist, 2015a, 2015b; Wadhwa, 2015). As noted in Chapter 2, Bitcoin's market capitalization was $300 billon at its peak in in December 2017, equivalent to that of Bank of America — only that Bitcoin was created out of a piece of software code! Given its significance as a DAO and its real-world economic impact, Bitcoin provides valuable data and a rich setting for my research.

For the sake of clarity, throughout this chapter "Bitcoin" (upper case) will be used to refer to the DAO, while "bitcoin" (lower case) will be used to refer to the cryptocurrency tokens.

4.1 Research Design: A Pilot Case Study

Case studies serve as an appropriate method to build theories (e.g., Gersick, 1988; Gilbert, 2005) and as a source from which theoretical insights may be derived from rich data. For novel phenomena that are little understood and cannot be fully explained by extant theories, a case study may be used to inductively investigate emerging patterns and their underlying logic (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Siggelkow, 2007).

In the course of my research, I collected data on Bitcoin from its formation in 2009 through 2017. Between July 2016 and March 2018, I conducted twelve 60- to 90-minute semi-structured interviews with 13 industry experts who have direct experience or relevant knowledge of Bitcoin. Interviewees included Bitcoin developers, Bitcoin Improvement Proposal (BIP) authors, cryptocurrency miners, and experts on cryptocurrency start-ups. Questions revolved around two categoriess, namely: (1) what is the defining feature of coordination within Bitcoin which distinguishes it from OSSD; and (2) how do stakeholders[8] coordinate tasks at various organizational levels? With these primary questions in mind, I also inquired into the communication and decision-making processes characteristic of a DAO like Bitcoin. The interview guide is included in Appendix B.

In addition to conducting interviews, I studied documents such as white papers, BIPs, technical and non-technical archives, academic papers, and industry reports. Finally, I accessed important online data at the blockchain level (e.g., blockchain.info), protocol level (e.g., GitHub Bitcoin repositories at https://github.com/bitcoin/bitcoin), peer-to-peer network level (e.g., bitinfocharts.com), organizational level (e.g., coinmarketcap.com), and community level (e.g., the Bitcoin sub-reddit at https://www.reddit.com/r/Bitcoin/). Using multiple data sources enhanced the robustness of my findings (Eisenhard, 1989).

I went back and forth between the extant literature and the data I obtained to support subsequent theory building. Follow-up data collection was required to ensure internal validity. The goal was to arrive at a convergent theoretical framework that was tightly linked with empirical evidence (Eisenhardt, 1989).

[8] Throughout this dissertation, I define organizational boundaries to include those network actors who directly maintain or provide services for the decentralized autonomous organization. In the case of Bitcoin, internal stakeholders of interest include network validators (i.e., miners) and developers.

4.2 Findings

4.2.1 Two Major Types of Task at Various Levels

To understand how DAOs coordinate tasks to solve the universal problems of organizing, I will first identify the tasks performed by Bitcoin.

4.2.1.1 Task #1: Network Validation at the Blockchain and Protocol Levels

Bitcoin represents a partial substitute for banks, albeit with notable differences. First, at an aggregate level, traditional banks store transaction histories in a centralized fashion. Users only get to view their personal bank statements and must trust that their information is protected from both cyber attacks and employee misconduct. Traditionally, banks employ clerks to process payments. Human agents are prone to agency problems which can lead to misconduct, such as theft. Human agents are also expensive. With Bitcoin, all transactions are recorded publicly and electronically onto the immutable blockchain and stored in a distributed fashion across thousands of network nodes. As a result, records are easier to maintain, and cyber attacks are less likely to succeed (transaction information is not held in one central location). The blockchain technology provides the multi-site copies of "ledgers," which are essentially aggregations of past transactions (like a bank account statement). The technology also provides encryption to validate transactions. This is similar to the personal security devices used in online banking, which generate a unique transaction-specific signature based on a personal key.

Second, whereas banks prevent double-spending by checking for funds sufficiency in a centralized server, in a peer-to-peer system like Bitcoin, payees cannot verify whether payers still have the funds they claim to have due to unpredictable network delays (e.g. an email sent now can reach its recipient before another email sent a minute earlier). To resolve this issue, the Bitcoin network relies on cryptographic routines to verify, timestamp, and order transactions in a non-reversible way, thereby avoiding the need for human reconciliation. The key idea is that somebody in the network will legitimately time stamp a block of transactions, but we cannot predict who that will be (e.g. replacing a bank clerk, who can be corrupted to fake time stamps, with a system that cannot be corrupted). Table 2 illustrates the difference in coordination between Bitcoin and traditional banks and payment organizations.

Table 2 Forms of Organizing: Banks and Payment Organizations vs. Bitcoin

(Adopted from Hsieh & Vergne, 2017)

Goal	Provision of a Payment System	
	Banks and Payment Organizations	**Bitcoin**
Main Task	Payment processing: verification, validation, recording, settlement, clearing, reconciliation	Network validation: broadcasting, verification, validation and recording.
Mechanism	Centralized hierarchies	Mining: competitive bookkeeping
Task Division	Centralized task division by job descriptions/ definitions, divided by formal organizational structure	Task division is based on the criterion of computing power dedicated to mining and is *automated* by the blockchain software in a decentralized fashion.
Task Allocation	Assigned by formal hierarchies	Miners self-select in the network. However, competitive bookkeeping only allocates payment validation tasks to the winning miner (essentially chosen at random, though the probability of winning is proportional to the computing power committed).
Reward Distribution	Defined by formal compensation/ incentive programs. In general, reward schemes are not publicly available.	Automated, randomized, transparent. Linked with task allocation through competitive bookkeeping.
Information Flows	Centrally controlled by organizational rules. Inconsistencies can persist across teams, divisions, or subsidiaries.	Transaction history is recorded in the blockchain, which is publicly auditable and immutable. Information is distributed among network nodes and all nodes have to run the same software protocol and keep the same transaction record on the blockchain public ledger.

For network validation tasks, coordination is achieved through a process whereby the blockchain produces agreement (aided by miners' efforts) on the ordering of transactions through the timestamping created by miners' success at guessing random numbers generated by the protocol (Hsieh & Vergne, 2017).

4.2.1.2 Task #2: Protocol Update at the Peer-to-Peer Network Level

Underlying the Bitcoin payment system is the blockchain software supported by ongoing protocol updates (Wang & Vergne, 2017). In terms of governance, miners voting on protocol update proposals resemble the community-based management OSSD observed in projects such as Linux. This aligns stakeholder expectations (Lopp, 2016), and facilitates knowledge sharing, problem solving, and the realization of collective outcomes (O'Mahony & Lakhani, 2011). Like OSSD, Bitcoin software development is also open source, decentralized, and community based. Bitcoin communities of volunteer software developers collaborate in a non-hierarchical network and self-select into tasks and roles based on expertise and preference. Over time, a team of core Bitcoin developers has formed and become increasingly influential in the community, even though their work is not funded by a centralized organization, but by a sponsorship program that relies on donations.

The key organizational novelty of Bitcoin is that, in addition to developers, miners play an equally important role in protocol modification. Specifically, Bitcoin software is updated through BIPs, which are design documents proposing new features, changes, or processes for the protocol. BIPs allow developers to make proposals on software updates that miners must vote on. Proposals are first reviewed by BIP editors, and miners then indicate a "yes" or "no" vote in a block during the polling period (e.g., 100 blocks totalling 1,000 minutes). Voting power is proportional to the computing power a miner contributes to the network. A code change will only be implemented when 55 per cent of voters approve a given proposal (Franco, 2014: 90). Table 3 compares OSSD with Bitcoin software development in light of the four core dimensions of organizing: task division, task allocation, reward distribution, and information flows (Puranam, Alexy & Reitzig, 2014).

Table 3 Updating Software Protocol: Open-Source Software Development vs. Bitcoin

(Adopted from Hsieh & Vergne, 2017)

Goal	Protocol Update	
	OSSD	**Bitcoin**
Main Task	Software development	Standard development
Mechanism	Community governance	Voting: Bitcoin improvement proposals (BIPs)
Task Division	Some centralization based on the structure provided by the founder; evolvable with community.	Founder is unknown; BIPs proposed by developers and voted on by miners coordinate code modification. Centralization is undesirable.
Task Allocation	Open participation through self-selection into the community	Developers contribute to code upgrades through open participation and self-selection. Miners vote on the protocol change based on computing power.
Reward Distribution	Intrinsic motivation, professionalism, visibility,	Developers volunteer and are motivated by intrinsic motivation. Miners are paid in Bitcoin and are driven by mining profitability.
Information Flows	Information is processed through "virtual support infrastructure and tools" (Puranam et al., 2014)	Information is shared and communicated through BIP communication on the code repository (i.e., GitHub) and reflected in miners' voting outcomes on the blockchain.

We can compare tasks performed by Bitcoin and OSSD in terms of their goals, their coordination, and the subsequent security requirements.

> So development for the individual clients is very much like Linux and Python and so on … it's an open source project that welcomes contributions from anyone …

> But the goal … isn't quite the same because you're not developing a, a piece of software, you're developing a standard, or a set of rules. That means that … it doesn't quite work the same way because you can't just commit a change in the code … It relies on human validation and so forth . . . It's not software development, it's standard development. [Nick Johnson, interview #26]

Since protocol update in Bitcoin means setting up standards for the entire network to follow, this necessarily affects consensus layer.

> It's very similar. The only difference is probably the consensus layer, which is not so highly fragile in Linux or other open sources . . . when you look at Linux, there is not much in [terms of] consensus—maybe some drivers need to follow a standard and it doesn't hurt too much if you don't. While in Bitcoin if the consensus changes then you at the end have two chains like we have now with Bitcash and Bitcoin. And this is like an additional element, you not only split the [software] distribution like Linux, Ubuntu, as Debian, but you kind of split the financial system. [Jonas Schnelli, interview # 21]

This leads to some fundamental differences between cryptocurrencies and other security-critical projects.

> Bitcoin and Namecoin and Monero are security critical projects. And so, if you compare any security critical project . . . to a typical open source project that's not security critical, there will definitely be a much a higher standard involved for [the] security critical project, just because the stakes are higher if something goes wrong . . . so that's one aspect. The other aspect is that cryptocurrencies are decentralized consensus protocols . . . which interact [with economic agents] in weird ways . . . which historically have never all interacted at once before cryptocurrencies existed . . . There tend[s] to be a much higher standard for those systems compared even to other security critical projects. [Jeremy Rand, interview #31]

According to Nick Johnson, a major difference between developing a standard and developing a piece of code is that “a lot of the best practices in software development can’t be applied” (interview #26). The distinction between “software development” and “standard development” points to a fundamental difference between Linux and Python, on the one hand, and cryptocurrencies like Bitcoin, on the other. This creates an intriguing scenario whereby a straightforward software update in OSSD could have complex interactions with a decentralized consensus system. A security update that would normally be deployed as quickly and as broadly as possible in OSSD, could be deemed to pose a security threat to Bitcoin.

> [N]ormally in a security critical project, if some other project that's a codependency of yours releases a security update, normally you would want to merge that as fast as possible and deploy to everyone as fast as possible . . . because how could a security update be a security issue in itself? Right? But in the context of things like Bitcoin, Namecoin and Monero, [if] I'm merging a security update for dependency without being very careful about how you test its interaction with the existing system, that can actually introduce security issues of its own. [Jeremy Rand, interview #31]

Thus, these two categories of task, network validation and protocol update, lead to important insights into the nature of “distributed consensus.”

4.2.2 Distributed Consensus Mechanisms: The Defining Feature of Task Coordination in Bitcoin

> “Any needed rules and incentives can be enforced with this consensus mechanism.” (Nakamoto, 2008)

As the Bitcoin white paper rightly concludes, it is an almost insurmountable task to study coordination within Bitcoin without touching on the concept of consensus. Jeremy Rand elaborated:

> Bitcoin is basically the first ever implementation of what's called a decentralized consensus protocol, which basically means I'm having a large number of users[9] on the Internet, who by some mechanism all end up coming to an exact agreement on an order to [the] series of events . . . this was the problem that was previously believed to be impossible to solve. There was actually a mathematical impossibility . . . and [B]itcoin ends up taking advantage of a really interesting loophole in the important proof and basically solves it by relying on both cryptography and economic incentives rather than just cryptography. [Jeremy Rand, interview #31]

The "mathematical impossibility" mentioned by Rand refers to the Fischer-Lynch-Paterson theorem, which demonstrates the impossibility of reaching consensus about the true state of the network in a distributed network with dishonest actors (Fischer, Lynch & Paterson, 1985). Distributed consensus (or in computer science terms, decentralized consensus) is at the heart of Bitcoin's coordination mechanism for network validation tasks.

By design, network validators (e.g., Bitcoin miners) only belong to a DAO if the protocol is unanimously adopted. "You only use the system that has the rules that you agree with" (Nick Johnson, interview #26). Consensus is no longer a state, but a set of rules that must be met for the organization to function and which serves as a prerequisite for organization members adopting the same protocol to stay in the same network. Think about how miners must agree on the true state of the ledger; consider how the network agrees on which protocol to follow (e.g., Bitcoin vs. Bitcoin Cash[10]), and how miners cast votes to signal support for important updates proposed by developers through BIPs or other

[9] According to the interviewee, "users" refers to all "miners (or network validators)" and "full nodes" who run the same Bitcoin protocol and keep the entire history of Bitcoin blockchain on their computer.

[10] Bitcoin Cash is a hard fork of Bitcoin that features a larger block size to enable faster transaction processing.

platforms—these are characteristics specific to cryptocurrencies such as Bitcoin but not to OSSD. Specifically, consensus rules for network validation are deterministic.

> [E]very single user on the Bitcoin peer-to-peer network, they need to come to [a] deterministic conclusion about what the state of the blockchain is. And even a trivially insignificant change in how they ended up computing . . . even if it's just one very obscure signature in one transaction and the entire blockchain isn't valid anymore. If there's even one tiny deviation, then they will fail to come to a deterministic agreement on what the state of the blockchain is. And as a result of that, that means suddenly now there's a disagreement on who has how much money . . . And the only way that Bitcoin can work is if everyone is in 100 percent deterministic agreements on that state. [Jeremy Rand, interview #31]

Thus, blockchain-based consensus is distinctive in that it requires all participants to agree on basic organizational facts and states instead of outlining a common strategic goal for members to follow. In other words, blockchain-based consensus no longer attends to the ends of coordination (i.e., the desired outcome), but the mechanisms of coordination. Blockchain-based consensus is guided primarily by formal rules and supported by informal communication among stakeholders. Traditionally, coordination mechanisms such as plans, rules, and routines were intended to foster agreement among organizational members and contribute to a common understanding (Okhuysen & Bechky, 2009). In the case of Bitcoin, by contrast, consensus is a default, i.e., a pre-condition for coordination at the blockchain and protocol levels.

Before getting into a finer-grained view of "how" consensus mechanisms work, we first need to understand "who" the internal stakeholders with direct decision-making power actually are.

4.2.3 Defining Organizational Boundaries: Internal Stakeholders of DAOs

Although in practice, there are various types of nodes in the extended Bitcoin network connected by various protocols (see Figure 14-15 in Appendix C), in this study, I will adopt the generally accepted definition of a cryptocurrency network as a collection of nodes running a cryptocurrency protocol. Organizational boundaries are drawn to include only those nodes running the Bitcoin protocol, i.e., those connected by the orange ties in Figure 16 in Appendix C.

Specifically, I focus on two classes of stakeholder groups: *miners* and *developers*. The choice is based on their level of direct decision-making power and involvement in task coordination.

Who has agency? Every human participant in the Bitcoin network has agency. As the Bitcoin white paper states, "nodes can leave and rejoin the network at will" (Nakamoto, 2008). Members make voluntary decisions to join the network and self-select into roles. Joint decisions are made through democratic community voting.

Who has power? According to Narayanan and colleagues (2016:173-175), there are a few internal stakeholder groups that have power, including: developers, who write the code as a rulebook that everyone uses; and miners, who compete to write the history and validate transactions. Externally, investors can influence the value of DAOs by holding Bitcoin and users can utilize cryptocurrency to transfer value. Other external stakeholders include: regulators, merchants, and customers, who generate basic demands for cryptocurrency; and payment services, exchanges, and wallet providers who handle transactions. In general, external stakeholders build their products and services upon the Bitcoin blockchain and protocol. This classification is in line with how industry experts think about the difference between internal and external stakeholders in terms of governance: "we have kind of two cohorts or two classes of network participants, you know, what I call the retail layer or the end users and then what I call the utility or the keepers in general with respect to governance" (Ryan Zurrer, Principal and Venture Partner at Polychain Capital, interview # 30).

The "keepers" referred to by Zurrer correspond to internal stakeholders, whereas the "retail layer" or "end users" correspond to external stakeholders. In this dissertation, I will focus on those internal stakeholders—developers and miners—who have a direct influence on operations, decision-making, and the value of the cryptocurrency. External stakeholders are beyond the scope of this study.

Who are the "shareholders"? Anyone who owns bitcoin has "shares". Investors and users hold and transact with bitcoin, the value of which is demonstrated by market capitalization and the total number of transactions (Narayanan et al., 2016: 47, 173).

The following section examines the consensus mechanisms corresponding to tasks at the blockchain and protocol levels.

4.2.4 Consensus Mechanism at the Blockchain and Protocol level: Coordinating Network Validation

At both the blockchain and protocol levels, mining based on consensus provides the utility layer necessary for DAOs such as Bitcoin. Ryan Zurrer called this class of network participant the "keeper."

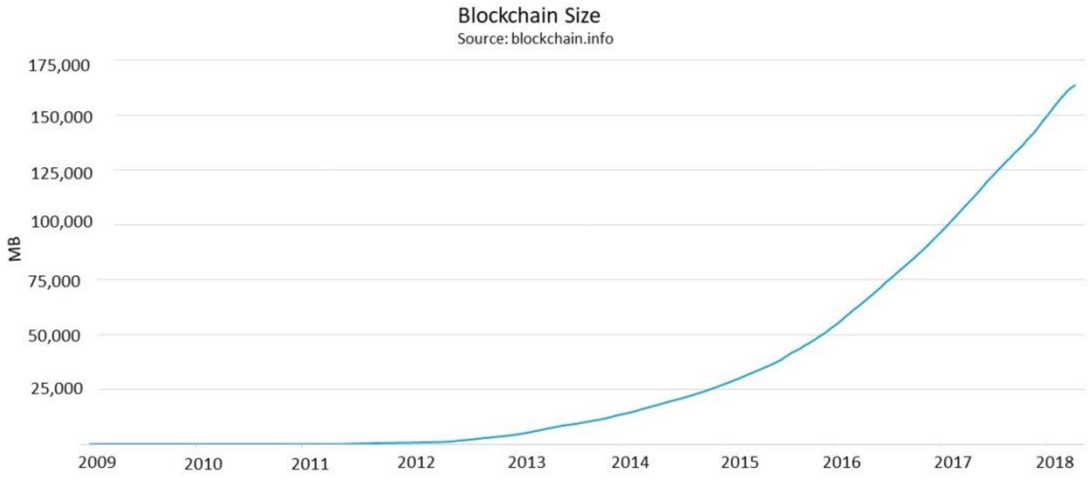
> [T]hat utility layer, that'd be called keeper, [which] provides a specific resource or . . . a function to the network. So either it provides storage and computation or maybe it does validation or something like that . . . these sort[s] of permissionless actors can come and go and, and in providing the specific resource to the network for the retail layer, for the end users, end users get to use of that network basically nearly for free. [Ryan Zurrer, Principal and Venture Partner at Polychain Capital, interview #30]

In the case of Bitcoin, miners are the main providers of value in the network. In accordance with the coordination of machine routines in the Bitcoin protocol, Bitcoin keeps its maximum block size at 1MB. Bitcoin is also able to maintain a stable block generation speed averaging 10 minutes per block; this ensures that the Bitcoin blockchain size (i.e., the total number of blocks in the blockchain) grows at a constant speed (see Figure 7). To make sure this happens, the consensus mechanism needs to take into account the expansion of network computing power, which directly influences miners' probability of solving hashes. Figure 8 shows the growth trajectory of the Bitcoin hash rate, which is the number of calculations the mining network performs each second. Every 14 days the machine routine adjusts the difficulty of the mathematical puzzles generated by the mining algorithm so that the average block time remains stable (see Figure 9). Over the course of the last three years (2015-2018), the slope of the Bitcoin blockchain size growth curve (see Figure 7) remained constant while the slope of difficulty (see Figure 9) increased exponentially in response to the soaring growth in network computing power indicated in Figure 8.

Miners are profit driven. The Bitcoin machine routine thus coordinates the reward distribution schedule to miners with new bitcoin injected into the economy in a deflationary fashion. At its launch in 2009, the initial reward started off at 50 BTC[11]. It is programed to halve approximately every 4 years until 2140, when the maximum supply of 21 million BTC is expected to run out (https://en.bitcoin.it/wiki/Controlled_supply).

Figure 7 Bitcoin Blockchain Size (MB)

(Defined as "the total size of all block headers and transactions. Not including database indexes.)"

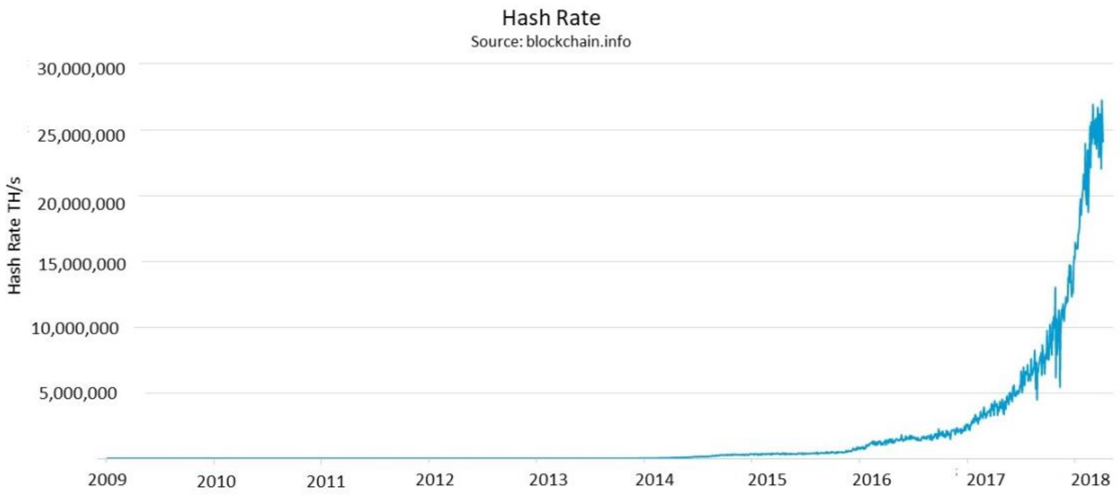


(Source: blockchain.info)

[11] BTC is the unit of one bitcoin. Additionally, while the upper case "Bitcoin" refers to the name of the cryptocurrency and decentralized autonomous organization, the lower case "bitcoin" stands for the currency itself.

Figure 8 Bitcoin Hash Rate (TH/s)

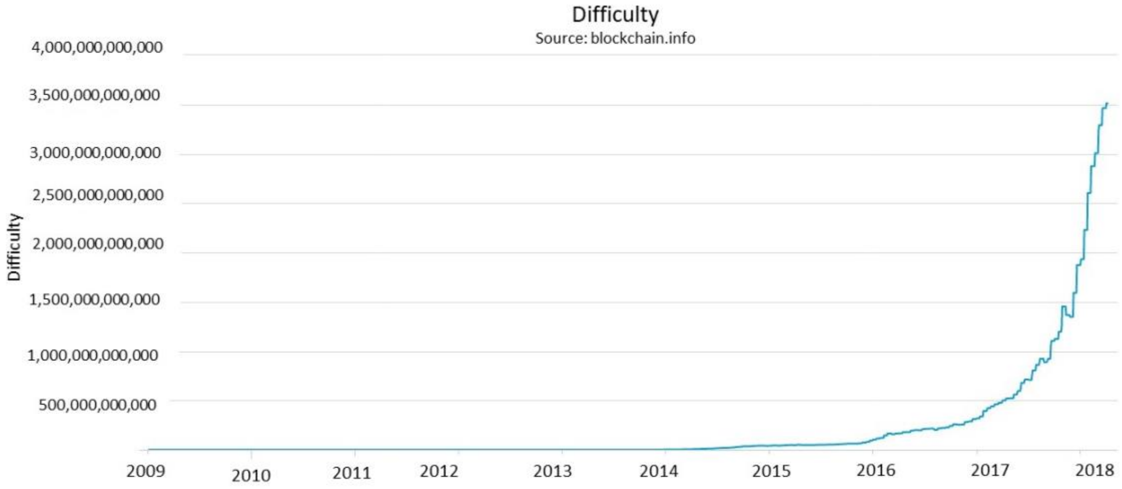
(Defined as “the estimated number of terahashes per second (trillions of hashes per second) the Bitcoin network is performing.”)



(Source: blockchain.info)

Figure 9 Bitcoin Difficulty

(Defined as “a relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.”)



(Source: blockchain.info)

For Bitcoin and other DAOs, the consensus mechanism that coordinates network validation tasks at the blockchain protocol level requires that every node in the network run the Bitcoin protocol and that everyone keeps the same copy of the blockchain ledger. According to Hudson Jameson, “You show that you agree to the consensus by running the software. And if you chose to run the software or a different software or a modified version of the software, that's you disagreeing” (interview #32).

The amount of “work” committed to PoW mining serves as a cost to validate the network. This “ante” cost makes Bitcoin highly resistant to cyber attacks. According to Adam Reeds, Vice President, Energy and Infrastructure at Dream, and an expert in mining, “if you think about a game of poker, if you're betting on the result of it, it's like you're ante” (interview #29). Reeds’ business partner, Mauricio Di Bartolomeo, elaborated: “[B]itcoin is the honeypot. Everybody's trying to get a piece of it and nobody has been able to. That’s why it is where it is” (interview #29).

It follows that Bitcoin’s true organizational novelty lies in those unique solutions consensus-based mining provides to organizing. Coordination is characterized by: (1) pre-determined task division written into the protocol; (2) randomized task allocation that is proportional to computing power; (3) randomized reward distribution subject to task assignment; and (4) peer-to-peer information flow among network nodes in the blockchain. It is important to note that the Bitcoin code does not assume away the problem of agency costs. Rather, Bitcoin explicitly deals with these long-standing problems by incorporating counterbalancing incentives in the code, making the payment system incorruptible.

4.2.5 Consensus Mechanism at the Peer-to-Peer Network Level: Coordinating Protocol Update

An important channel for code update is the BIP, a formal document used to propose protocol changes. There are three kinds of BIP: a standard-track BIP that describes a universal change to the protocol; an informational BIP that address a Bitcoin design issue; and, a process BIP, which pertains to changes to procedures and decision-making processes (Github BIPs, 2018). Appendix D lists all BIPs (including authors and status); Appendix E shows a sample BIP (BIP #151), with its key components. The BIP structure and process is not unlike the academic journal review process. New ideas and proposals are discussed in the community or in focus groups in order to get feedback. Proposals are then submitted to BIP editors, who can either reject or approve them. Approved proposals are then moved to a repository and their status changed to “draft,” as indicated in Figure 1. The draft will not be finalized until the reference implementation is completed (e.g., in the form of code). Each BIP follows a well-defined format and is reviewed in a standardized process. However, the decision to adopt any proposed change is made by the user at the client end.

While miners consent to playing by the rulebook, they can vote to change it using the influence derived from their computing power. When it comes to solving related issues, making changes to the code, or deciding which protocol to adopt with clients, decision making is coordinated through consensus within and between stakeholder groups, as in

OSSD. “Most of these processes actually happen a bit more fluid[ly] and more casual[ly],” said Fabian Vogelsteller, EIP[12] developer (interview #27).

However, an important distinction between DAOs and OSSD projects is the use of cryptocurrency tokens as an economic incentive. In contrast to OSSD contexts, Bitcoin relies on a mixed community of volunteer developers and paid miners who jointly revise the organizational design through BIPs. Put simply, Bitcoin offers a novel solution to “the universal problems of organizing” (Puranam et al., 2014), by involving a new class of stakeholders, incentivized by both machine routines and community discussions, and through the design of an organization whose parameters cannot be changed unilaterally by any stakeholder group and whose routine operations cannot be derailed by insiders’ covert misconduct.

As shown in Figure 4 in Chapter 2, a BIP draft can progress to various stages of approval, e.g., deferred, proposed, rejected, withdrawn. What determines the acceptance of a proposal? Andy Chase, a Bitcoin developer and BIP author explained:

> Whether [a BIP] goes to final/active . . . depends on the BIP. Some BIPs are just . . . standard, like the UI schemes so you can just switch it to final when you're done making it. For active, it's just whether you were able to submit a change and the vast majority of users are using the change. So if it's a fork . . . [with] a feature change, then at least a certain number of users have to be using it. And then you get to that point where it gets more complicated because if it's in Bitcoin Core[13] then . . . you have to figure out, in order for enough users to use it, you either have to go through the Bitcoin Core process, which is like writ[ing] the code, get[ting]

[12] EIP stands for Ethereum Improvement Proposal. It is a concept based on Bitcoin’s BIPs repository. Similar to BIPs, EIP developers share protocol updates, discuss ideas and issues, and make a pull request as an EIP document. Once the pull request is merged, one could say that it has been officially accepted by the community. (Vogelsteller, interview # 27).

[13] Bitcoin Core refers to the Bitcoin software protocol with all four functions: wallet, mining, blockchain, and network routing. See also Figure 14 and Figure 15 in Appendix C.

> PR[14] requests, which just like submitting code for review, getting it approved and then waiting for the next version or . . . a convincing people to use your own software (interview #28).

In general, acceptance depends on the nature of the protocol update, i.e., whether it is contentious (e.g., changing blockchain consensus rules) or uncontentious (e.g., changing software behavior decisions unrelated to blockchain consensus rules).

> Generally, we don't end up adopting a proposal unless it has pretty much near unanimous agreement whether it's a good idea. Now, this can vary somewhat in the sense that ... if it's a blockchain consensus rule that would require a hard fork[15] then, obviously it must be pretty much unanimous agreement that it's a good idea because contentious hard forks tend to cause disasters as [the] kind of thing over in Bitcoin. If it's something like either a soft fork to the consensus rules or something that's not consensus critical . . . like a software behavior decision that isn't specific blockchain consensus rules . . . we won't require quite as much consensus. Generally, we try to avoid doing things that are particularly contentious. [Jeremy Rand, Lead developer of Namecoin, interview #31]

While BIPs are intended to provide a formal structure to the proposal assessment process, less formal means of communication are also used to help developers reach consensus. Intriguingly, the threshold is usually so high that almost unanimous consensus is expected.

[14] PR stands for “pull requests”, which are a feature of code repositories such as GitHub, which allows developers to push code changes, discuss, and review the proposed modifications and add follow-up commits before the changes are merged into the repository (source: https://help.github.com/articles/about-pull-requests/).

[15] A hard fork refers to a protocol change in which the new version of the software is not backward compatible. For blockchain DAOs, this creates a new blockchain that requires the entire network to update their protocol to the new version in order to stay in the same DAO. Otherwise, a new blockchain will be created as a result. For this reason, changes to consensus rules can only be achieved through hard forks.

> Part of the reason for this is that we generally recognize that we all kind of have varying areas of specialty and as a result, we tend to have somewhat . . . varying perspectives on how to solve the same problem. In our experience, it tends to be more effective to actually discuss a problem . . . until we reach a near unanimous consensus rather than to just do something like . . . a majority vote. Majority votes simply don't work very well in a project like this, especially security critical projects. Generally speaking, if there's a significant portion of the developer community who are strongly against a particular change, then usually that's a sign that there really is a problem with it and then it needs to be addressed in some way.   [Jeremy Rand, interview #31]

For miners to signal support for a particular proposal, a threshold (e.g., 95 per cent of network computing power) may be identified. According to Jonas Schnelli, developer and BIP author, “In the past [the] threshold was [up] to 95 per cent of miners . . . signaling readiness. And if the 95 per cent has been reached, the BIP or the change was locked in[16], so [it was] universally activated” (interview #21).

For the case of individual BIPs, Tanaka Khan, Bitcoin developer and BIP author explained:

> Usually, this means miners will code the blocks they find with a signal (version bits) indicating their support. Basically, miners vote for particular changes to the code by indicating their willingness to run that code. If the miner voting yields above that threshold, then the code activates, and everyone must run it or be forked off the main network (interview #25).

Following the example of BIPs, code development proposals for other DAOs have been created. For example, Bitcoin Unlimited has its own version called “Bitcoin Unlimited

[16] A BIP proposal being “locked in” refers to the status of a BIP being scheduled to activate at a certain block height.

Improvement Proposals" (BUIPs), Ethereum uses "Ethereum Improvement Proposals" (EIPs), and Bitcoin has another proposal called "Bitcoin Enhancement Proposals" (BEPs).

"Most minor code changes don't require a BIP, and instead are merged into the main code branch with pull requests on GitHub", explained Khan (interview #25). Alternatively, developers may use less formal online forums to communicate ideas to different communities, e.g., "Bitcointalk" and "Bitcoin subreddit." These are less technical and oriented toward the broader community.

4.2.6 What happens when Consensus cannot be reached?

Consensus is vital for DAOs as it constitutes the core of decision making and change. Consensus on the true state of the blockchain public ledger MUST be achieved—any disagreement will result in the splitting of the network through hard forks.

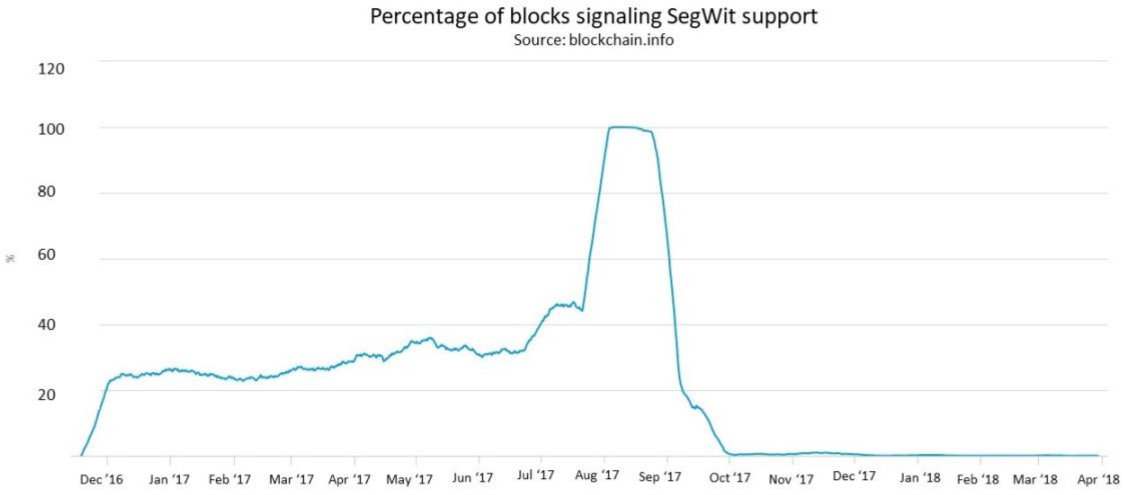
> [H]ard fork works like this: if you have . . . a network of 10 nodes and one node updates and say from block 2,000 on, I will change the consensus rules. Then from this block on, he will have a different hash in this block, so therefore his blocks will look different than the rest of the network. He will split off even alone . . . so if you have two of these 10 people, then these two split off, and 8 stay . . . so there's no majority vote necessarily. [Fabian Volgelsteller, interview #27]

To give an example, Bitcoin Cash split from Bitcoin on August 1, 2017, over a disagreement concerning the means required to improve Bitcoin's transaction processing speed. This is known as the scalability issue. Proposed solutions included implementing SegWit 2X[17] (BIP #91) and increasing the Bitcoin block size limit to include more transactions per block. While the first proposal received nearly 100 per cent support from

[17] Segregated Witness (SegWit) is a solution to the scalability problem proposed in BIP#91 and, subsequently, by BIP #141 via BIP #9 activation. SegWit proposes that Bitcoin transaction data be segmented in two. By restructuring the data removing the unlocking signature ("witness" data) from the original transaction data and appending it as a separate layer, a Bitcoin block will be able to almost double its capacity. [https://en.wikipedia.org/wiki/SegWit, accessed April 2018]

Bitcoin miners (see Figure 10) and was scheduled for activation, those in favor of the second proposal followed a hard fork (i.e., a new software version) and became Bitcoin Cash, a separate DAO. Bitcoin Gold, meanwhile, was created as a result of another hard fork on October 24, 2017, which involved an attempt to restore GPU mining[18], which had been replaced by the expensive specialist mining hardware, ASIC[19]. By changing the algorithm, a new DAO was created. As explained in the Bitcoin Gold (2017) white paper, "[a] blockchain hard fork occurs when a block is mined that does not comply with the network consensus rules" (Btcgpu.org).

Figure 10 Percentage of Blocks Signaling SegWit Support from Miners



To conclude, while disagreements in traditional organizations tend to be resolved through social and political means, for DAOs like Bitcoin, dissension means "the split of the

[18] GPU (or graphics processing unit) mining is a much more efficient way of mining Bitcoin using graphic cards.

[19] ASIC (application-specific integrated circuit) is mining hardware specifically designed for Bitcoin mining. It is a circuit and not typically capable of general computing in the sense of a "computer". ASIC is computing-power intensive and a cause of concern for mining centralization.

universe," according to Nick Johnson, Ethereum Core Developer and EIP author. "Basically, the hard fork is the upgrade process and, in many ways, similar to a regular software upgrade process. But the difference [is] that everyone has to upgrade and anyone who doesn't team up ends up with the version of the chain without the upgrade. (interview # 26)

The split of universe resulting from disagreements can also mean *organizational innovation and change* for DAOs.

> I think one of the strength[s] [of] blockchains is the ability to split . . . [It] is a sign as the health of the community is how well it's able to come to consensus . . . When people really do have fundamental disagreements, they can resolve them by going off on their own and starting their own system or continuing the old system as the case may be . . . A sign of the health of the community is how well it's able to come to consensus. So sometimes [there] will be irreconcilable differences, but in a healthy community that happens as little as possible. [Nick Johnson, Ethereum Core Developer and EIP author, interview #26]

Johnson added, "*hard forks are pretty much the only way we can institute change*, then we can add new features and that we can change the system . . . soft forks are proven to be effectively impossible and it also much more restrictive in terms of what they can achieve" (interview #26).

In fact, some even consider *forking as the only way a DAO like Bitcoin can innovate*: "We can replace the words 'hard fork' and 'soft fork' with 'software upgrade.' They're the only ways to innovate inside Bitcoin (or any other mined cryptocurrency), and they're necessary when making changes that either aren't backwards compatible (hard fork) or are (soft fork). [Tenaka Khan, Bitcoin developer and BIP author, interview #25]

4.2.7 Integrating Consensus at Varying Levels: the Organizational Level

While task integration in traditional settings focuses on rules and processes designed, in large part, by managers (Okhuysen & Bechky, 2009; Rivkin & Siggelkow, 2003; Stan &

Puranam, 2016), Bitcoin network validation and protocol update tasks are integrated by miners, a brand new class of paid stakeholders incentivized by cryptocurrency tokens.

An important defining feature of cryptocurrency is the economic value of the tokens used to exchange value (Ryan Zurrer, Polychain Capital, interview #30). Given that cryptocurrency tokens are also offered as an incentive to network validators, high security requirements are fundamental. This can be achieved through the implementation of the consensus protocol—the cryptocurrency network will have to be in complete agreement to reach distributed consensus (Jeremy Rand, Namecoin Core Developer, 2018 Interview #31) The fact that token holders overlap with network validators and users provides a mechanism by which distributed consensus may be integrated at varying levels.

4.2.8 Decentralization is a Continuum

It is important to note that the decentralization of decision making at the organizational level is relative. Recently, a decision was made by a small group of members to suspend the scheduled implementation of SegWit 2X[20].

> Prior to [SegWit2X] cancelation, it had enough miner support to be activated. Support obviously fell dramatically after the release was cancelled. ‘Lack of consensus’ in this case basically means a perceived lack of consensus, without any hard numbers to back it up ... There wasn’t much discussion on it and no decisions were made through its BIP [#144]. [Tenaka Khan, Bitcoin developer and BIP author, interview # 25]

[20] The suspension was announced on November 8, 2017, in an email written by Mike Belshe, one of the leaders of the SegWit2X project. He wrote: "Unfortunately, it is clear that we have not built sufficient consensus for a clean block size upgrade at this time. Continuing on the current path could divide the community and be a setback to Bitcoin’s growth. This was never the goal of SegWit2X…Until then, we are suspending our plans for the upcoming 2MB upgrade." (https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html, accessed December 2017)

Although SegWit2X was supported by 95 per cent of the miners, it was canceled due to a lack of consensus among the sponsors[21] and developers of the project. A concern about the possibility of the highly contentious hard fork dividing the Bitcoin community and fear of subsequent market destabilization were the main reasons behind the suspension. Thus, miners, developers, and the rest of the network may not always arrive at the same decision. The presence of centralized sponsors or foundations associated with a cryptocurrency can mitigate the magnitude of decentralized decision making.

Decisions on code modification by developers and miners can diverge in similar ways:

> [Y]ou could have all the miners wanting to double the mining reward and the . . . software implementers (developers) would go, no, that’s a bad idea for the network. We’d refuse. As long as you have a limited number of clients and a limited number of people working on those, then there's going to be some degree of centralization . . . On the other hand, if . . . you preach you really wanted [it] and it was not a terrible idea they knew could drive it forward even if you are . . . a complete outsider. So you propose an idea and if it seems like a good one and it will get implemented. If it's like, well this is good, but low priority you could put your own effort into implementing it yourself. And if you do the work you'll get the feature pretty much because even though it seems like [a] good idea and you've done for us. So great ([Nick Johnson, interview #26]

In the next chapter, I will examine more closely determinants of the degree of decentralized decision making.

4.3 Conclusions from the Pilot Case Study

As a pilot study, this chapter drew on the example of Bitcoin in order to lay out a foundational understanding of DAO coordination. My findings reveal the following observations. First, separate *levels* define the two types of tasks performed by DAOs like

[21] The SegWit2X project is sponsored by various industry start-ups, such as the enterprise blockchain technology company Bloq, wallet providers Blockchain and BitGo, and mining hardware provider Bitmain.

Bitcoin, namely, *network validation* and *protocol update*. Second, the two types of tasks are coordinated by *distributed consensus mechanisms* and integrated through mining. Third, consensus mechanisms need to be studied at the corresponding levels at which tasks are performed—the *blockchain and protocol levels* versus the *peer-to-peer network level*. Fourth, complex *interactions* exist between these levels and influence organizational decision making. Finally, *decentralization of strategic decision making* at the organizational level needs to be studied as a continuum. I will delve into these concepts and examine their implications for growth in the following chapter.

Chapter 5 Research Design

5 Research Design*

** This chapter draws heavily from the front end of my paper, "The Rise of Decentralized Autonomous Organizations: New Forms of Task Coordination and the Growth of Cryptocurrencies," co-authored with Dr. Jean-Philippe Vergne. The paper is currently in the first round of revision-and-resubmission (R&R) with Administrative Science Quarterly (ASQ).*

Building on the Bitcoin pilot study discussed in Chapter 4, I will now examine a range of blockchain-based cryptocurrency DAOs and perform a comparative study across multiple cases. The goal of this chapter is to provide a fine-grained picture and generalizable framework of how various coordination mechanisms work within DAOs, in order to answer the central research question identified, namely:

How are DAOs coordinated to enable growth?

To answer this question, I conducted fsQCA following a three-stage design. The first stage of the study extended the preliminary findings from the pilot study and identified important features of task coordination within DAOs through 16 semi-structured interviews with DAO founders and core developers, as well as through specialized archival sources such as industry reports, expert blogs, and white papers. I also attended 11 industry conferences[22] to conduct field observations and informally engage with insiders. I thickly described and elaborated upon concepts of consensus mechanisms at the blockchain and protocol versus peer-to-peer network levels by reconnecting them to recent theory that argues that coordination is about achieving accountability, predictability, and common understanding (Okhuysen & Bechky, 2009).

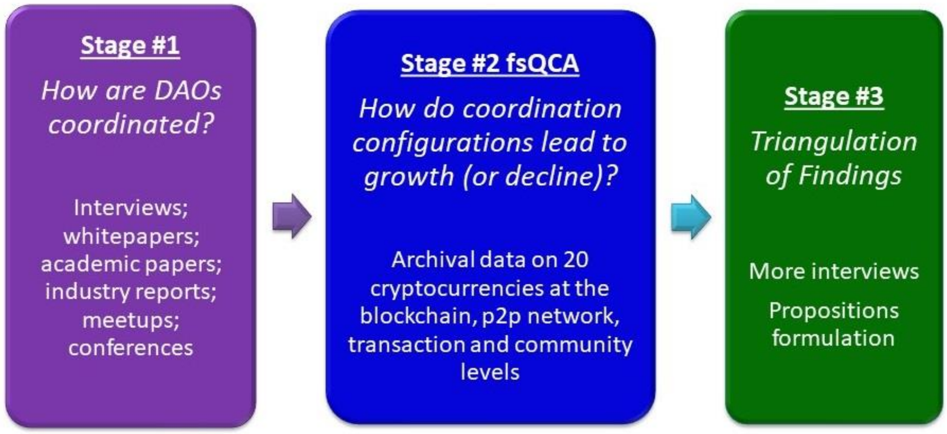
In the second stage, based on these findings, I sampled 20 DAOs in the cryptocurrency industry that differ in terms of how they coordinate such tasks as transaction verification, maintenance of the public ledger, and the rewarding of internal stakeholders along the

[22] My co-researcher attended some of these conferences to conduct separate observations.

previously identified dimensions of consensus mechanisms at various levels and decentralization of strategy making. I then conducted fsQCA using archival data to understand which configurations of task coordination features foster DAO growth (or decline).

Finally, in a third stage, I triangulated the fsQCA results and fleshed these out in light of a second wave of interview data (n=10). Based on this inductive study, three propositions were formulated to outline a theory of DAO coordination. Figure 11 outlines the three-stage design.

Figure 11 The Three-Stage Research Design


Stage #1
How are DAOs coordinated?
Interviews; whitepapers; academic papers; industry reports; meetups; conferences
Stage #2 fsQCA
How do coordination configurations lead to growth (or decline)?
Archival data on 20 cryptocurrencies at the blockchain, p2p network, transaction and community levels
Stage #3
Triangulation of Findings
More interviews
Propositions formulation

5.1 Study Stage #1: How Are DAOs Coordinated?

5.1.1 Method

Building on the findings of the pilot study in Chapter 4, Stage #1 allowed me to inductively obtain a deep understanding of how DAOs are coordinated by consensus mechanisms. From multiple data sources, I identified key characteristics and distinguishing features of DAO coordination. To begin, I reviewed: 15 cryptocurrency white papers; over 150 industry reports, articles, and academic papers; and 10 books authored by experts on Bitcoin, blockchain technology, and cryptocurrency. I also reviewed the primary websites of 20 cryptocurrencies to delve into the technology, use cases, and special features of each cryptocurrency. These technical, industry, and research documents laid the foundation for my understanding of how cryptocurrencies work in general, and how they vary in terms of design and task coordination.

I then conducted 16 semi-structured interviews to delve further into DAO design and task coordination. The interviewees included cryptocurrency founders who are also lead developers, directors of cryptocurrency foundations, network validators, and blockchain start-up founders in the FinTech industry. These are industry experts who have direct experience in creating, developing, or managing DAOs in the cryptocurrency industry. Each interview lasted 60 to 90 minutes. The questions asked focused on coordination and decision making, as well as on the design philosophy and evaluation of cryptocurrencies. In particular, I asked questions related to the origins, processes, and consequences of different types of coordination among stakeholders (e.g., how algorithms affect the DAO's accountability vis-à-vis stakeholders; how developers and miners coordinate on code modifications; how stakeholders make decisions and come to agreements; and, how decentralization can be implemented).

Finally, my co-researcher and I participated in 11 cryptocurrency conferences and workshops, during which I extensively observed and engaged with industry insiders in a more informal manner. I tap into these data to provide a thick description of how DAOs are coordinated.

5.1.2 Findings

5.1.2.1 Machine Consensus Based on Machine Routines at the Blockchain and Protocol Levels

As noted in Chapter 4, at their core, DAOs rely on machine routines (as opposed to human routines) (Antonopoulos, 2014) that are written in the blockchain, protocol, and scripting code to coordinate network validation tasks. For instance, Bitcoin's blockchain software entails a set of routines governing the "competitive bookkeeping" process, known as "mining" (Yermack, 2017: 13). In this process, voluntary network validators ("miners") try to guess a very long random number to provide a PoW to the system and obtain the chance to earn a reward in the form of Bitcoin currency (Nian & Lee, 2015: 8). Proof-of-work mining is not dissimilar to gold mining, in that it resembles the process of “gold miners expending resources to add gold to circulation”—except that for mining bitcoins, they expend computing power to validate user transactions and record them in the ledger (Nakamoto, 2008: 4). Machine routines also require that, at any point in time, the true ledger must be the one containing the largest amount of “proven work” (in the form of previously expended computing power).

As a result, the Bitcoin DAO makes it much more expensive for potentially malicious users to tamper with the blockchain history (e.g., by adding 1,000 units of Bitcoin currency to their account) than to play by the rules. A past block cannot be edited without redoing all of the PoW leading up to the current one—a process that would not go unnoticed and that would be prohibitively expensive in terms of hardware and electricity. Thus, when it comes to processing, validating, and recording user transactions in a secure way, “any needed rules and incentives can be enforced with this consensus mechanism” that tells network validators what the true state of the ledger is (Nakamoto, 2008: 8). Following industry experts, I call this set of automated coordination mechanisms based on machine routines *machine consensus mechanisms*, defined as *self-executing formal software protocols that define and implement rules, routines, and incentives for organizational participants to follow* (Lopp, 2016; BlockchainHub.net, 2017). Machine consensus, for instance, makes it unnecessary to coordinate teams of employees whose primary task is the manual reconciliation of transaction balances that do not match across ledgers maintained by different financial institutions.

I will now discuss two core dimensions of machine consensus along which DAOs in the cryptocurrency industry can differ substantially. Based on interview data and documents, I identified *security* and *stability* mechanisms as the foundational elements that support the exchange of value in a peer-to-peer, open network that does not rely on trusted intermediaries or personal identity. Subsequent investigation of these dimensions allowed me to capture variation in machine consensus across the DAOs in our fsQCA analysis.

Machine Consensus #1: Providing security. A common feature across DAOs in the cryptocurrency industry is the provision of a peer-to-peer, decentralized, open payment system powered by cryptocurrency tokens which reward miners for their work. Since financial transactions are involved, to operate effectively DAOs must ensure that cybersecurity is maximal and that record immutability is guaranteed—otherwise users will simply look for alternatives. Two broad categories of machine consensus mechanisms are implemented to coordinate security provision. As Jackson Palmer, co-founder and lead developer of Dogecoin (interview #9), explains,

> The number one thing you want to look at with any DAO is how it secures the network. The network ultimately has to be secured through proof of something. Earlier coins had [PoW] via mining, which [relies on] intense computing. Some coins moved to [PoS] … Obviously the people that carry the greatest consensus in the network are those who own the highest stake.

In contrast to PoW, PoS consumes little external energy, and correlates the probability of a network validator's being chosen to validate the next block with the amount (and sometimes age) of the cryptocurrency that the validator holds (Narayanan et al., 2016: 40-45; 206-211). As Douglas Pike, core developer and co-founder of Vericoin puts it,

> A lot of [PoS network security] depends on the value of the coin. If the coin has a very high value. [. . .] it is much more secure because it's more costly to gain majority control of the network [. . .] In both cases, the consensus is protected by cost, and it greatly depends on the value of the coin in [PoS], and greatly depends on the difficulty level in [PoW] mining (interview # 12).

Although industry insiders hold different views on the effectiveness of PoW as opposed to PoS, the general belief is that expending external resources (electricity or capital) is necessary to coordinate security provision because it anchors the network to exogenous factors that insiders cannot control.

Machine consensus #2: Ensuring stability. Since DAOs in the cryptocurrency industry are open organizations that anybody can join and leave at will (network validators included), characteristics such as network size or transaction validation speed change constantly, thereby affecting how quickly transactions are processed. Indeed, "decentralized things are hard to stabilize, just by the fact that they're decentralized"

(Patrick Noskar, founder of Vericoin, interview #6, 2016). Thus, to remain stable, DAOs must have the capacity to adjust autonomously to a changing landscape.

Bitcoin does this by automatically adjusting mining difficulty (i.e., the difficulty of guessing the random numbers) every 14 days to reset the target of an average transaction-processing time of ten minutes. As the mining difficulty increases, "the coin distribution . . . mimics the distribution pattern of a precious metal . . . As you dig up more and more, it becomes more scarce," according to Palmer (interview #9). The machine routines in charge of adjusting mining difficulty also stabilize the speed of new coin issuance (i.e., inflation) by taking into account factors such as the overall network's computing power, the size of miners' rewards, and transaction-processing times.

These dynamic adjustments, governed by publicly auditable algorithms, determine the stability of rewards earned by network validators. While more frequent adjustments can jeopardize validators' ability to earn cryptocurrency rewards, they also make DAOs more responsive to shocks in their environment. Thus, they play an important role in balancing efficiency (resource allocation) and effectiveness (maintaining fit between the internal and external environments to achieve the DAO's high-level goals).

5.1.2.2 Social Consensus Mechanisms based on Multi-Stakeholder Consultations at the Peer-to-Peer Network Level

As noted in Chapter 4, another key layer of task coordination pertains to protocol update at the peer-to-peer network level. Lopp (2016) points out that "humans must first decide what protocol to run before the machines can enforce it." In line with industry experts, I define *social consensus mechanisms* as *the means by which DAO stakeholders reach an agreement about the higher-level DAO protocol (which acts as a strategic plan for the organization)* (Buterin, 2014; Lopp, 2016). DAO software is open source and thus fully disclosed for auditing, testing, and improvement purposes; as a consequence, the multi-stakeholder consultation around DAOs is coordinated in ways comparable to those which characterize OSSD projects (O'Mahony & Lakhani, 2011).

In order to fix bugs, to implement new code, or to release a new version of the software (a "fork"), DAOs rely on formal and informal community voting processes. For example, Bitcoin uses BIPs to discuss and align developers' and miners' expectations. A BIP serves as a formalized technical design document that proposes new features or documents decisions (GitHub BIPs, 2018). As noted in Chapter 4, coordination around BIPs involves developers proposing code modifications that miners vote on by adding a record of their decision into the blockchain. While the BIP author defines the threshold, the rule of thumb suggests that a majority vote in favor of the proposal, representing at least 55 per cent of the DAO's computing power, leads to the adoption of the proposal. When network validators, representing 95 per cent of the DAO's computing power, have implemented the software update, the proposal is considered "activated." Any developer can propose a new BIP, and anyone can become a Bitcoin developer. Note, however, that not all DAOs in the cryptocurrency industry have formal voting mechanisms such as BIPs. In some cases, developers rely on informal communication channels such as forums to discuss protocol changes with the community. Unless a majority of network validators is willing to implement the change by updating their software, however, proposals for protocol change are bound to remain at the draft stage.

I will now discuss two core dimensions of social consensus over which DAOs in the cryptocurrency industry tend to differ substantially. An examination of these dimensions subsequently allowed us to capture variations in social consensus mechanisms across DAOs in the fsQCA analyses.

Stakeholder discussions. The role of social consensus mechanisms is to facilitate agreement within and between developers and miners, and amongst the broader community (e.g., users and merchants who accept the cryptocurrency as payments). Developers play a key role in the community and are trusted by its members in terms of their capabilities to drive and implement code modifications (Narayanan et al., 2016). Without substantial and frequent developer contributions, DAO development may, according to James Lovejoy, core developer of Verticoin, become "hemorrhaged" (interview #5). Looking back at the challenges he faced as a developer, Lovejoy remarked: "If you want the coin to grow and expand . . . active development is probably one of the more important things . . . There are a number of ideas of things people wanted to develop. It really required a lot more time and thought than people had available or were willing to give" (interview #5).

While it is important that numerous developers contribute to stakeholder discussions so that a DAO can gain exposure to a variety of new and innovative ideas, it is even more crucial for the community to be mature enough to converge on a subset of these ideas and to move on to implement them. An important indicator of the community's ability and willingness to do so is reflected in their code development activities on the repository. According to David Cohen, executive and business development director at the Blackcoin Foundation, "people will go to look at the GitHub and see how frequently commits are being made to the code, so you see that there's . . . active development and meaningful . . . ongoing work being done. That creates trust" (David Cohen, interview #7).

Validators' commitment. Network validators signal their commitment to a DAO by devoting computing power to its blockchain. Without their continued support, a DAO cannot evolve and is bound to fail due to questionable security (e.g., bugs are not fixed) or competition (e.g., competitors improve their operations at a faster pace to leverage network effects). As Cassini (pseudonym of a miner, interview #16) explains, "usually, it's the developers who make proposals or decisions. But in the end, it boils down to the miners. If they don't follow the ideas of the developers, then they turn to other ventures." In other words, validators' commitment to the project is essential if social consensus at the organizational level is to be reached; this represents a major difference between DAOs and OSSD projects (which do not rely on network validators). Jeremy Rand, the core developer of Namecoin (interview #15), recalled how Namecoin developers tried to obtain validators' consent to activate a software upgrade proposed in BIP#66 to solve a vulnerability issue. [23]

[23] Namecoin closely follows Bitcoin's development proposal, since Namecoin is built on the Bitcoin source code and can be mined using the same hardware (i.e., "merge mined" alongside Bitcoin).

> We haven’t yet activated BIP66 [. . .], so we’re vulnerable. And so we immediately contacted all of the mining pools and said, hey, you need to upgrade to the latest version ASAP. And most of the mining pools were fairly quick to respond. But we were not able to quickly contact sufficient hash power to reach the 95 per cent threshold that’s needed to activate a soft fork, so we were hovering around 92 per cent [. . .] After about a week or so, we were still having no luck reaching the last seven or eight percent of hash power, and finally [. . .] F2Pool contacted us [. . .] [with] enough hash power [. . .] We can activate that soft fork right now without waiting for the other miners to do their thing.

It follows that machine consensus and social consensus occur at different but overlapping timescales. On the one hand, each entry on the blockchain ledger is an instantiation of machine consensus and only protocol updates (e.g., changes proposed through BIPs) require social consensus; on the other hand, validators’ commitment (as one dimension of social consensus) is required for both payment validation and protocol update, thus plays a dual role concurrently in integrating the two tasks. It should also be noted that network validators form a new class of stakeholders that has never existed before, either in traditional corporations or in distributed organizations such as OSSD projects.

5.1.2.3 Decentralization of Strategy Making

The origins of DAOs may be traced to the desire to remove the need for central authority. At the organizational level, both machine consensus and social consensus mechanisms operate in a decentralized fashion. However, certain organizational design elements create variation in the extent to which strategy making is decentralized. Thus, while traditional corporations typically rely on hierarchy to coordinate high-level activities, DAOs rely on decentralized strategy making. However, as noted in Chapter 4, decentralization is best seen as a continuum insofar as a DAOs’ coordination structure revolves around an “uneasy but inevitable and necessary alliance of decentralization with centralization” (Cohen, interview #7). Cohen uses Ethereum as an example:

> On the one hand, [Ethereum] to a great extent has been incredibly successful at offering a very decentralized approach. But there is the Ethereum Foundation,

> there are known personalities, Vitalik Buterin and Vlad Zamfir and so forth, who are out there and . . .the respect that they've garnered, you know, for their judgement and intelligence carries a lot of weight and is very helpful in reassuring mainstream institutional players that this is not just a bunch of crazy geeks operating in some haphazard way . . . So in that sense you have centralization within decentralization.

Specific coordination mechanisms within particular DAOs can mitigate the extent to which they are decentralized in the following ways. First, some DAOs have active foundations—typically, not-for-profit organizations composed of developers, managers, and community members serving on a voluntary basis. The goals of DAO foundations include user education, adoption by merchants, business development, expansion of the user base, branding, and strategic actions such as political lobbying (Andrew Vegetabile, director of the Litecoin Association, interview #4, 2016). Additionally, an important role of the foundation is to establish trust with the community:

> [The foundation] was an attempt to bring legitimacy and human faces . . . How can you trust a coin where you don't know who any of these people are, like, who could disappear or do anything at any time, and that's not a very friendly and transparent impression it makes on the public. [David Cohen, executive and business development director at the Blackcoin Foundation, interview #7]

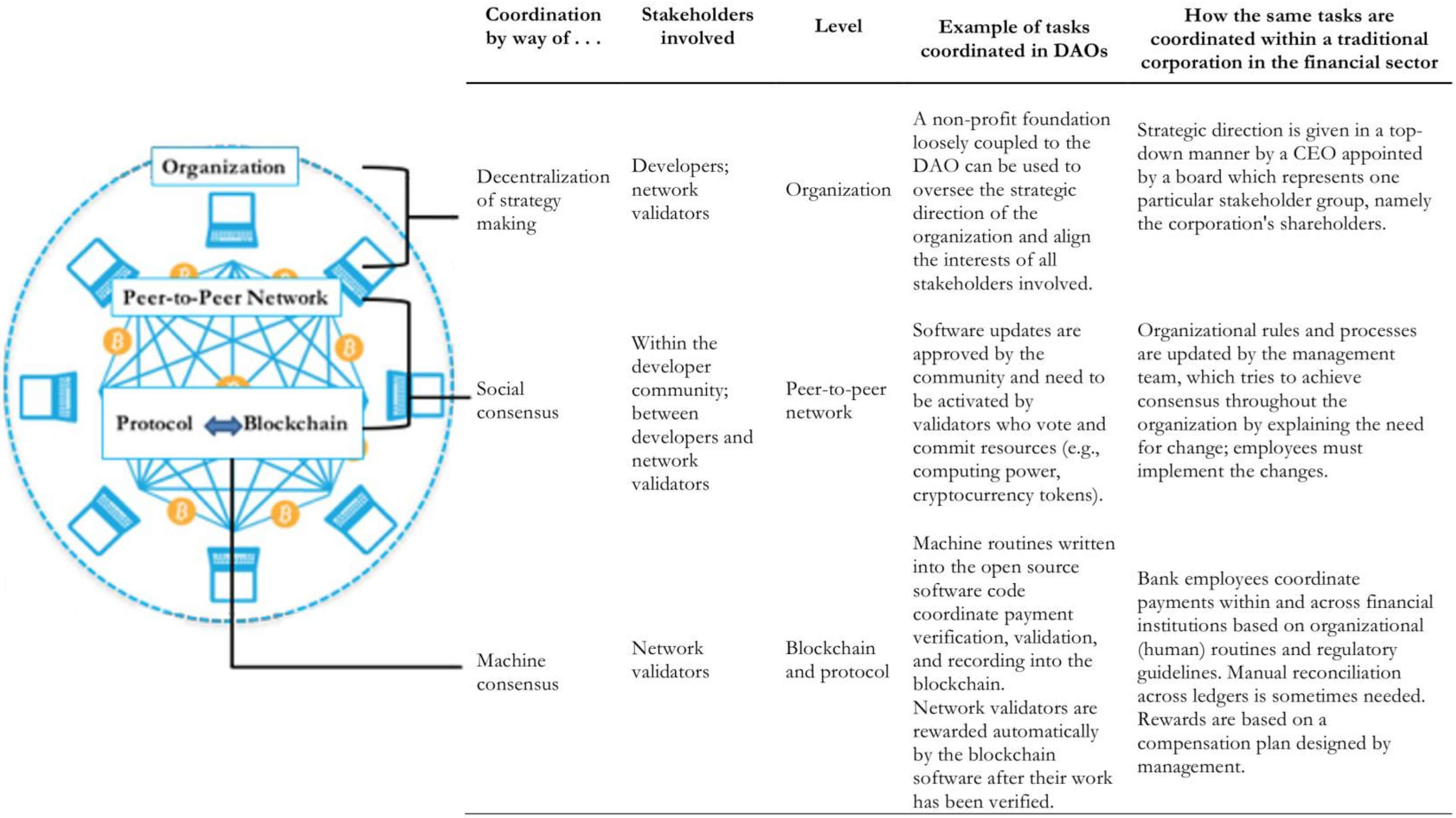
While foundations remain independent of cryptocurrency founders and core developers to avoid conflicts of interest, there is a constant dialogue between the two sides. This serves to to align interests, limiting the extent to which a DAO is decentralized when it comes to strategic decision making (interview #7, 2016).

Second, for some DAOs (e.g., Bitcoin and Peercoin), the real-world identity of the co-founder(s) is unknown, which removes any association between the DAO and a leadership figure that can be consulted for strategic direction. Thus, DAOs with anonymous or pseudonymous co-founders (e.g., Bitcoin) tend to be more decentralized and autonomous.

Third, DAOs can have various design philosophies, ranging from the promotion of distributed social innovation (e.g., Namecoin, Dogecoin, Peercoin) to business development (e.g., Dash, Ethereum). A business-oriented development philosophy, for instance, entails the creation of specific positions and roles aimed at growing the user network to secure a competitive advantage in the cryptocurrency industry. By contrast, DAOs with an innovation-oriented philosophy leverage decentralization for the greater good, with minimal centralized control (Patrick Noskar, founder of Vericoin, interview #6, 2016; Sunny King, co-founder of Peercoin, interview #3, 2016). For example, while expressing his lack of interest in adopting a "mainstream business model" by providing Namecoin domain names through a central server, Daniel Kraft, lead developer of Namecoin (interview #8, 2016), stated: "We don't want to endorse such a system, even if it could simplify and bring users [together] ... I think that the philosophy of not just me but also other main contributors in the community is that we don't want that. We want to really be decentralized."

As a result, while decentralization represents the formative logic of DAOs in the cryptocurrency industry, the degree of decentralization at the organizational level tends to vary. Figure 5.2 summarizes our discussion thus far and provides an example of how task coordination differs between DAOs and traditional corporations.

Figure 12 Task coordination within Decentralized Autonomous Organizations (DAOs)



Coordination by way of . . .	Stakeholders involved	Level	Example of tasks coordinated in DAOs	How the same tasks are coordinated within a traditional corporation in the financial sector
Decentralization of strategy making	Developers; network validators	Organization	A non-profit foundation loosely coupled to the DAO can be used to oversee the strategic direction of the organization and align the interests of all stakeholders involved.	Strategic direction is given in a top-down manner by a CEO appointed by a board which represents one particular stakeholder group, namely the corporation's shareholders.
Social consensus	Within the developer community; between developers and network validators	Peer-to-peer network	Software updates are approved by the community and need to be activated by validators who vote and commit resources (e.g., computing power, cryptocurrency tokens).	Organizational rules and processes are updated by the management team, which tries to achieve consensus throughout the organization by explaining the need for change; employees must implement the changes.
Machine consensus	Network validators	Blockchain and protocol	Machine routines written into the open source software code coordinate payment verification, validation, and recording into the blockchain. Network validators are rewarded automatically by the blockchain software after their work has been verified.	Bank employees coordinate payments within and across financial institutions based on organizational (human) routines and regulatory guidelines. Manual reconciliation across ledgers is sometimes needed. Rewards are based on a compensation plan designed by management.

5.2 Study Stage #2: The Growth Implications of Task Coordination Patterns

5.2.1 Method: Fuzzy-set qualitative comparative analysis (fsQCA)

Building on my findings from Stage #1, Stage #2 examines the interplay between various forms of consensus mechanisms managed under different degrees of decentralization of strategy making and explores how they jointly explain DAO growth (or decline). For emerging complex social phenomena, relationships between constructs are often "better understood in terms of set-theoretic relations rather than correlations" (Fiss, 2011: 395; Ragin, 2008: 2; Schneider & Wagemann, 2012: 1–3). A set-theoretic approach is both a methodological and an analytical tool that identifies which configurations of conditions are necessary or sufficient to obtain an outcome (Ragin & Fiss, 2008: 190). A necessary condition is one that must be present for the outcome to take place. In other words, without the necessary condition, it is impossible to obtain the outcome. A sufficient condition is a one that produces the outcome. FsQCA has the ability to disentangle the complexity underpinning poorly theorized social phenomena, especially when they involve "equifinality, conjunctural causation, and causal asymmetry" (Ragin, 2008; Fiss, 2011; Schneider & Wagemann, 2012)[24]. This methodology has been increasingly used in recent management research to explain outcomes of strategic importance, e.g., firm adaptation (Vergne & Depeyre, 2016), organizational typologies (Fiss, 2011), and decoupling (Crilly, Zollo & Hansen, 2012). In the context of this study, fsQCA helps to connect the various configurations of coordination mechanisms observed at various levels and decentralization with the growth (or decline) of DAOs in the cryptocurrency industry.

[24] Equifinality arises in situations in which the same outcome can be produced by different configurations of conditions, a situation commonly observed in organizational design research (Gresov & Drazin, 1997; Puranam et al., 2014). Conjunctural causation refers to the idea that outcomes are rarely the product of single conditions taken independently, but, rather, are produced by configurations involving multiple conditions. Causal asymmetry is the idea that the conditions leading to the presence of an outcome differ from those leading to the absence of the outcome (Fiss, 2011; Schneider & Wagemann, 2012: 78,198), i.e., DAO growth and decline may be underpinned by different factors.

5.2.1.1 Organizational Configurations

Methodologically, configurations have been identified as a useful approach to study organizational designs as clusters of attributes (such as ideal types and typologies) (Miles & Snow, 1978; Mintzberg, 1979; Puranam et al., 2014; Doty, et al., 1993; Fiss, 2007; Meyer, Tsui & Hinings, 1993). A configurational approach is appropriate to the study of within-form variations, because it unpacks how organizations of the same form can be configured differently to achieve growth (Puranam et al., 2014). Different structural configurations can be equally effective, thus leading to the aforementioned idea of equifinality (Gresov & Drazin, 1997; Puranam et al., 2014). Okhuysen & Bechky (2009) note that those integrating conditions for coordination—accountability, predictability, and common understanding□are "necessary but not always sufficient" for coordination. In addition, the relationships between the three conditions are highly context specific. They can coexist, work as complements, or work as substitutes together (Okhuysen & Bechky, 2009). A hypothesis-testing approach will not be appropriate for capturing this complexity. These limitations further reinforce the validity of using fsQCA to study coordination mechanisms as configurations.

5.2.1.2 Sampling Strategy

I selected 20 cryptocurrencies founded between 2009, when Bitcoin was first introduced, and early 2015, when we started to collect data. The sampling is stratified by period. My dataset includes: one cryptocurrency founded before 2010 (Bitcoin); three founded between 2011 and 2013, when the industry was still in its infancy and had not achieved mainstream public visibility; seven founded in 2013, when the industry underwent a period of steep growth; eight founded in 2014; and one founded in early 2015. For each period, I randomly selected a number of cryptocurrencies in proportion to the prevailing founding rate in the industry in order to obtain a balanced and representative sample. I selected cryptocurrencies within the top 200 in terms of market capitalization, which together account for over 99 per cent of the industry’s total value. [25]

The sampled cryptocurrencies vary in terms of their coordination mechanisms. For example, 13 use PoW as their primary consensus algorithm, five use PoS, and two are hybrids (i.e., they use both PoW and PoS). The 20 cryptocurrencies also vary in terms of their degree of decentralization. As of May 2017, the 20 cryptocurrencies sampled accounted for about 70 per cent of the industry’s total market capitalization.

5.2.1.3 Overview of the Data and Conditions Included in the fsQCA Analyses

I chose to study growth in the first two quarters that followed each cryptocurrency’s founding. This choice was motivated by two reasons. First, most failed cryptocurrencies disappear within six months, so this time frame appears to be a critical threshold□a fact confirmed by. In fact, industry insiders confirmed that the first two quarters were crucial. One interviewee, Douglas Pike, stated, “I would say if you’re not meeting your goals within three to six months, you’re not going to get them.” (interview #12) Second, while comparing DAOs founded at different times allowed me to examine a representative sample of the cryptocurrency industry’s early years, it also came a drawback, given that I was not studying a cohort. This meant that, at any given point in time, the sampled cryptocurrencies were in different stages of their idiosyncratic trajectories (i.e., they were not the same “age”). Thus, II remedied this potential issue by examining them all during the first six months of their existence, thereby making them comparable.

I collected longitudinal archival data on market transactions, network validation, and developer activity from leading specialist websites, code repositories, and executive

[25] The sample includes cryptocurrencies that are currently active (e.g., Bitcoin, Litecoin, Dogecoin), ones that are declining (e.g., Zetacoin, Megacoin), and those that became inactive over time (e.g., Paycoin, XCurrency). During the observation period, three cryptocurrencies fell outside of the top 200, so our sample contains a balanced set of cases with substantial variance in terms of growth. Following prior research (Wang & Vergne, 2017, Ong, Lee, Li, & Lee, 2015: 85), I excluded cryptocurrencies that were obvious scams from the sampling pool.

interviews.[26] I also obtained blockchain-level data from technical documents such as cryptocurrency white papers. I coded variations of each sampled DAO's design based on our qualitative interviews with co-founders and lead developers.

Building on the results of the first stage of the study, I developed and calibrated an indicator for DAO growth and indicators for each of the three sets of coordination mechanisms identified. In line with my findings, I captured machine consensus mechanisms using two indicators: security provision and stability provision. I captured social consensus mechanisms using two indicators of the depth and breadth of stakeholder discussions, and one indicator of validators' commitment. Finally, I created a tridimensional indicator of the decentralization of strategy making, which takes into account such factors as: the design philosophy of the DAO; whether its co-founders are known; and, whether it works with a foundation.

5.2.1.4 Outcome Calibration: DAO Growth (and Decline)

For DAOs, attracting new users rapidly is vital for generating positive network effects to kick-start organizational growth (e.g., the more users a DAO has, the more secure its network becomes, and the more attractive it becomes to new users) (Gandal & Halaburda, 2016). Users drive up demand for a cryptocurrency by conducting transactions (Narayanan et al., 2016: 171–173; Ong et al., 2015: 82–90). As Pike explained,

> The goal is at some point you break into an actual currency closed loop where [. . .] people get their currency, and then they buy something with it, and then that merchant [. . .] buys something with it, and then [. . .] you've created a new currency in a full loop. [. . .] It's very hard to get to that point, but that's the end goal. [. . .] Once the coin is released, most of the development and feature releases also occur and those typically happen within, you know, six months. There is this

[26] Web data sources include: https://bitinfocharts.com; https://coingecko.com/; www.coinwarz.com/cryptocurrency; coinmarketcap.com; and, https://github.com. Various academic papers and book chapters have used CoinGecko's data to compare cryptocurrencies (e.g., Ong et al., 2015).

> new shiny object dynamic [. . .] [serving as] an opportunity [for cryptocurrencies] to gain value, gain users, to reach more people when you're new and you're shiny. And then once that wears off it's much more difficult to meet your goals (interview #12).

I calculated DAO growth based on the number of user transactions that took place during the first two quarters after the founding of the DAO. I measured DAO growth by looking at transaction growth between the first and second quarters (Q1 and Q2 respectively) of the cryptocurrency's existence:

$$DAO\ growth\ (or\ decline) = \frac{\text{Average number of unique transactions per day in Q2} - \text{Average number of unique transactions per day in Q1}}{\text{Average number of unique transactions per day in Q1}}$$

A positive sign indicates growth. A negative sign indicates decline. In terms of the fsQCA calibration, the crossover point for growth and decline is clear cut: I set the calibrated condition to 0.5 for growth rates equal to 0. A twofold increase in transactions can be considered fast growth that outperforms that of most newly created cryptocurrencies, so to growth rates greater than 100 per cent, I allocated a score of 1. I allocated a score of 0 when the rate of decrease was 100 per cent.

5.2.1.5 Explanatory Conditions

I calibrated all explanatory conditions using Q1 data to explain growth outcomes from Q1 to Q2 in order to account for the lagged effect of coordination on growth and to enhance explanatory power. The paragraphs that follow outline my calibration strategy for each explanatory condition; related technical details about measurement can be found in Appendix F.

Machine consensus mechanisms

Security provision. Within DAOs, cryptographic proof is supposed to rely mostly on external resources to provide security. Proof-of-work mining's external resource requirements in the form of electricity help DAOs achieve higher security and reliability by increasing the cost of attacking the network or of tampering with the records stored in the ledger. The more secure the DAO's network, the more predictable organizational task coordination will be. On the other hand, because PoS algorithms rely primarily on capital internalized within the DAO (i.e., existing cryptocurrency holdings), they offer an alternative that is more energy efficient but potentially less secure (i.e., insiders might be able to influence cryptocurrency prices but not electricity prices). To capture the difference, I coded the extent to which a DAO uses PoW. A cryptocurrency relying more on PoW was assigned a score above 0.5: a cryptocurrency relying more on PoS was assigned a score below 0.5.

Stability provision. As noted earlier, machine consensus algorithms adjust themselves regularly to adapt to changing conditions in the environment (e.g., variations in transaction-processing speed). The key variable here is the extent to which the difficulty level set for network validators (e.g., miners) fluctuates. More fluctuation makes a DAO more responsive to shocks in its environment (thereby enhancing stability and effectiveness), but it can jeopardize network validators' ability to earn cryptocurrency rewards (thereby potentially creating inefficiencies in resource allocation). Using data from Coinwarz.com on difficulty fluctuation over 14-day periods, I calibrated the 0.5 anchor based on the median variance of normalized bi-weekly difficulty values in Q1. Scores greater (lower) than 0.5 indicate higher (lower) levels of stability provision.

Social consensus mechanisms

The OSSD literature examines developers' engagement and efforts in relation to subprojects to capture coordination at the individual level (Dahlander & O'Mahony, 2011). Building on this insight, and in line with our earlier findings, to capture social consensus in a DAO context, I aggregated developers' and network validators' activities to capture the breadth and depth of stakeholder discussions as well as network validators' commitment to the organization.

Breadth of stakeholder discussions. I measured the breadth of stakeholder discussions by calculating the average number of unique contributors to the code based on each cryptocurrency's open-source code repository on GitHub.com—the largest and most commonly used platform for cryptocurrency software-development projects. Contributors can “commit” (i.e., make changes) or propose additions and deletions to the code. The median number of contributors—20—was used to set the 0.5 anchor. Scores above 0.5 indicate a broader involvement of contributors in stakeholder discussions.

Depth of stakeholder discussions. I measured the depth of stakeholder discussions by calculating the average number of additions and deletions to the cryptocurrency source code on GitHub. Each of these contributions is typically discussed informally by the broader community in online forums such as Reddit. I used GitHub records to proxy their depth, because such records represent an objective and exhaustive list of discussion topics (i.e., each code modification is time stamped and clearly associated with one specific DAO). I set the 0.5 anchor at the median—30,000. Scores above 0.5 indicate a deeper involvement of contributors in stakeholder discussions.

Validator’s commitment. As previously noted, network validators signal their commitment to a DAO by devoting computing power to its blockchain. This commitment is essential to coordinate a variety of tasks, e.g., voting on proposed changes or activating a new software update after reaching a wide consensus. An indicator known as the “network hash rate” is readily available on bitinfocharts.com to measure the computing power committed by each DAO’s network validators. It refers to the total number of calculations per second made by network validators. A higher hash rate implies greater commitment by network validators, who, it should be recalled, can choose to opt out anytime and instead commit their computing power to a competing DAO. I set the 0.5 anchor at the median value of the network hash rate—10^9 hashes per second. Scores above 0.5 indicate a stronger commitment of network validators to a given DAO.

Decentralization of strategy making

As our findings from this study’s first stage indicate, DAOs that are overseen by foundations, that have publicly known (co-)founders, or that have a business-oriented design philosophy tend to be less decentralized. I collected data from interviews, cryptocurrency websites, and online forums on these three dimensions separately and then combined them (Crilly et al., 2012) to calibrate our indicator of centralization of strategy making. The least decentralized DAOs are coded as 1 (and possess all three features), while the most decentralized DAOs are coded as 0.

5.2.2 FsQCA findings: Necessary and Sufficient Conditions for Growth and Decline

Out of 20 cryptocurrencies, seven experienced growth and 13 decline in the first six months of their respective existences. The fully calibrated dataset is shown in Table 4 below to enable reproducibility of the findings (Bergh, Sharp, Aguinis & Li, 2017). I ran all analyses with the freeware fsQCA 2.5 software package (Ragin & Davey, 2014).

Table 4 Fs-QCA Calibration Table

DAO	Security provision	Stability provision	Breadth of stakeholder discussions	Depth of stakeholder discussions	Validators' commitment	Decentralization	Transaction growth (or decline)
Bitcoin	1	0	0.2	0.6	0	0.66	0.4
Ethereum	0.8	0.33	0.6	1	0.4	0.33	0.8
Litecoin	0.8	0.66	0.6	0.6	0.2	0.33	0.2
Paycoin	0	0	0.4	0.2	1	0.66	0.4
Dogecoin	0.8	0.66	1	1	0.8	0.33	0.2
Peercoin	0.4	1	0.2	0	0.8	1	0.4
Namecoin	1	0.66	1	0.6	0.8	0.66	0.4
Blackcoin	0.2	0	0.4	1	0.4	0.33	0.6
Novacoin	0.4	0.66	0.2	0.6	0.4	0.49	0.4
Vericoin	0.2	0	0	0	0.4	0.33	0.4
Vertcoin	0.8	0.66	1	0.4	0.6	0.49	0.4
Reddcoin	0.2	0.33	1	1	0.6	0.66	0.4
Zetacoin	1	0.33	0.8	0.4	1	0.66	0.49
Dashcoin	0.8	0.33	1	0.8	0.6	0	0.6
Worldcoin	0.8	0.33	0.6	0.2	0.4	0.33	0.49
Feathercoin	0.8	0.66	0.8	0.6	0.6	0.49	0.4
Quarkcoin	0.8	0.66	0.2	0.2	0.4	1	1
Megacoin	0.8	0.66	0	0	0.4	0.66	0.8
Auroracoin	0.8	0.33	0.2	0.8	0.6	0	0.2
XCurrency	0.2	0	0	0	0.6	0.33	0.4

I ran four rounds of fsQCA analyses to identify necessary and sufficient conditions for both DAO growth and DAO decline. Each round of analysis yielded consistency and coverage scores that indicate the reliability of the results. More specifically, "consistency indicates the extent to which [DAOs] with high membership in a given solution set exhibit similar properties (i.e., consistency can be seen as a measure of a solution's internal validity)"; "coverage indicates the proportion of . . . outcomes explained by a given solution set (e.g., a coverage score of 1 would mean the solution explains all the cases" (Vergne & Depeyre, 2016: 11). In line with best practices, I used high thresholds for both reliability and proportional reduction in inconsistency (PRI) scores when searching for necessary and sufficient conditions (Ragin, 2008). Specifically, I used a 0.90 cutoff in consistency for all conditions, and PRI thresholds of 0.74 and 0.64 for sufficient conditions leading to growth and decline, respectively. No truth table row contains true logical contradictions, and I did not make any directional assumptions in the logical-minimization procedure, in line with the fact that there was no prior theory on DAOs available to guide our analyses.

I will discuss the configurations identified at this stage in Chapter 6.

5.3 Study Stage #3: Triangulation and Proposition Formation

Given the novelty of the DAO phenomenon and the fact that the present study is the first one to investigate coordination in this context, I felt that it was important to go back into the field and conduct a second wave of 10 interviews to triangulate and flesh out some of the findings from studies #1 and #2. For this reason, four of the interviews conducted during this second wave are follow-ups with respondents previously interviewed during study stage #1. These interviews shed additional light on the interpretation of the fsQCA results.

I will discuss the three propositions formulated at this stage in Chapter 6.

Chapter 6 Results

6 Results*

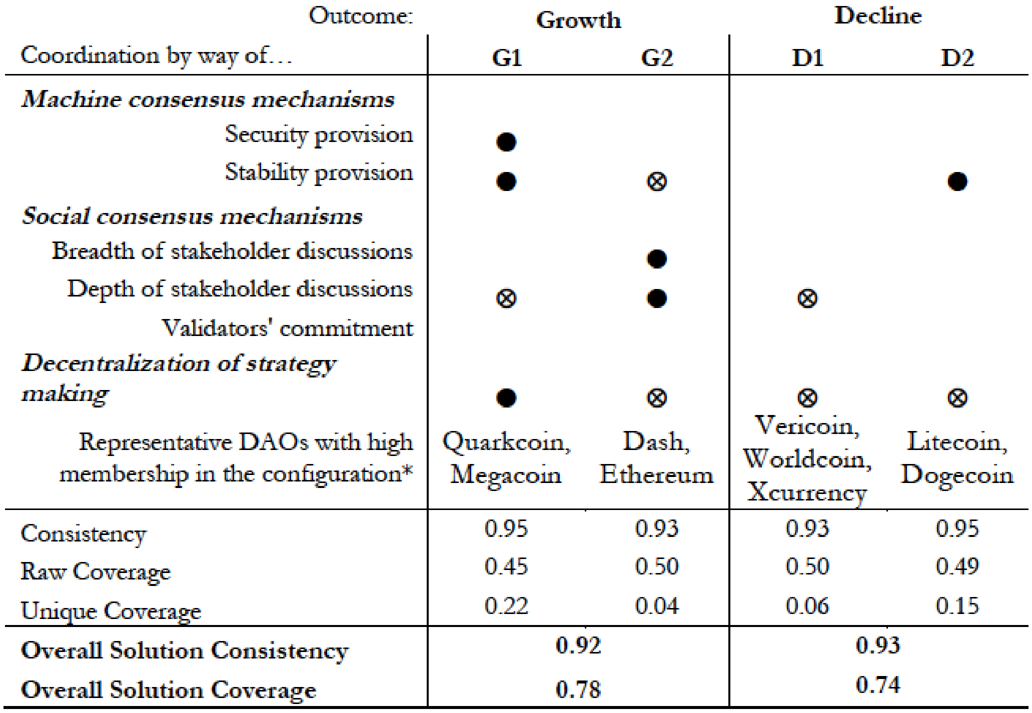
** This chapter draws heavily from the results section of my paper, "The Rise of Decentralized Autonomous Organizations: New Forms of Task Coordination and the Growth of Cryptocurrencies," co-authored with Dr. Jean-Philippe Vergne. The paper is currently in the first round of revision-and-resubmission (R&R) with Administrative Science Quarterly (ASQ).*

In this chapter, I discuss the results of the fsQCA analyses detailed in Chapter 5. As is often the case, I did not find any necessary conditions with an acceptable consistency score—the solutions yielded scores between 0.53 and 0.83, all falling short of the 0.90 threshold. This simply means that there is no single "recipe" that must be followed every time to produce growth (or decline). I did, however, identify sufficient configurations of coordination mechanisms leading to DAO growth and decline. Sufficient conditions represent alternative paths that produce the same outcome.

For the sake of conciseness, and in keeping with the exploratory character of the present study, Table 5 below depicts configurations with high explanatory power and in which I have high confidence. I thus report the so-called "parsimonious solution," which "contains only core conditions that have the strongest evidence linking them to the outcomes" (Crilly et al., 2012: 1439; Fiss, 2011) and is independent of the researcher's assumptions about the phenomenon. [27]

[27] For similar reasons, the table does not report two configurations with low explanatory power (e.g., low unique coverage); the configuration "contains" only one cryptocurrency, thereby raising doubts about its generalizability. Blackcoin (growth) and Auroracoin (decline), two small DAOs in the industry, are thus not mentioned in the table, but the full results can be reproduced from Table 4 or provided by the authors upon request. To obtain growth configurations, I selected the minimum number of "prime implicants" required by the software (2) to proceed with the logical minimization—specifically, I chose *~stability breadth depth ~decentralization* and *security stability ~depth decentralization* since they represent theoretically relevant cases observed frequently in our data.

Table 5 Configurations for Early Transaction Growth and Decline



Outcome:	Growth		Decline	
Coordination by way of…	**G1**	**G2**	**D1**	**D2**
Machine consensus mechanisms				
Security provision	●			
Stability provision	●	⊗		●
Social consensus mechanisms				
Breadth of stakeholder discussions		●		
Depth of stakeholder discussions	⊗	●	⊗	
Validators' commitment				
Decentralization of strategy making	●	⊗	⊗	⊗
Representative DAOs with high membership in the configuration*	Quarkcoin, Megacoin	Dash, Ethereum	Vericoin, Worldcoin, Xcurrency	Litecoin, Dogecoin
Consistency	0.95	0.93	0.93	0.95
Raw Coverage	0.45	0.50	0.50	0.49
Unique Coverage	0.22	0.04	0.06	0.15
Overall Solution Consistency	**0.92**		**0.93**	
Overall Solution Coverage	**0.78**		**0.74**	

●: Condition is present; ⊗: Condition is absent; *: non-exhaustive list

6.1 Configurations of Coordination Mechanisms Sufficient for DAO Growth (G1 and G2)

Overall, either a strong use of machine consensus mechanisms combined with decentralization of strategy making (G1) or a strong use of social consensus mechanisms (G2) needs to be present for DAO growth in the cryptocurrency industry. Quarkcoin and Megacoin, which can both be found in G1, kicked off growth by relying on strong machine consensus. Founded around the same time in 2013, the two cryptocurrencies have a good deal in common. Both are strongly committed to the value of decentralization, and in line with this claim, both have pseudonymous co-founders and are not overseen by foundations. In addition, both DAOs refused to "pre-mine" cryptocurrency, that is, to distribute tokens to core developers and co-founders before the official launch date. As Sunny King (pseudonym of Peercoin's co-founder) explains: "It was generally regarded as shady if you 'pre-mined' a bunch of coins" (interview #3) because it gave some insiders an unfair advantage over other users. Pre-mining, though, can be used successfully to lubricate social relationships by creating a common pool of resources shared by a small circle of innovators who know each other and guide organizational development.

This is precisely what happened with Ethereum (G2), one of the most successful DAOs to date. Pre-mining can incentivize developers to drive the success of software development by providing them with a (future and uncertain) source of income. A community member stated that, “it is similar to start-up founders, where the founding team has a certain amount of equity, and investors come in only to take a part of it. It is not in the interests of investors to leave the founders with nothing” (Ethereum Community Forum, 2014). More generally, G2 describes a path to growth that relies on strong social consensus. This is not to say that coordination around machine consensus is ignored, or that decentralization is inexistent, but simply that the emphasis, relative to competitors, is placed on social consensus mechanisms, especially the fostering of broad and deep discussions with stakeholders.

Specifically, the DAOs that took this path (G2) relied on a large community of developers, which they nurtured using a less decentralized approach than their G1 counterparts. For instance, they are concerned with project development and provide developer support—much as Google did in the early days of the Android operating system designed for smartphones. Launched in 2015, Ethereum managed to build considerable awareness among users and developers in relation to its core innovation, namely the ability to implement self-executing “smart contracts” within the blockchain. As a result of strategic decision making and with the goal of mainstream adoption, Ethereum has integrated a “Coinbase[28] Buy” widget into their Mist Beta 0.8.2. In the case of Dash, the DAO pioneered the development of the X11 hashing algorithm to make “mining” faster, more secure, and more energy efficient. The organization sees itself as

[28] Coinbase is a major player in the cryptocurrency exchange sector.

composed of "investor volunteers"—"people [who] come together to invest in a network, and also work on developing the network" (Daniel Diaz, interview #2, 2016).

6.2 Configurations of Coordination Mechanisms Sufficient for DAO Decline (D1 and D2)

All configurations leading to decline are low in decentralization. More specifically, deviating from the industry's original vision about the need to remove central authorities from organizational systems appears to be detrimental to early DAO growth, unless there is a strong reliance on social consensus mechanisms, as is the case with G2. In D1, for example, the DAOs that declined (e.g., Vericoin, Worldcoin, XCurrency) started off with low reliance on the social consensus mechanism related to the depth of stakeholder discussions. Without deep involvement from the developer community, DAOs based on weaker decentralization schemes seem to suffer in the early stages of their development.

Compared to G2, D2 does not feature a strong reliance on social consensus mechanisms. Instead, it relies on the use of machine routines to provide organizational stability (e.g., adjusting network validators' rewards frequently to reduce their risk level and provide them with a stable flow of income). It appears that blockchain system stability is better coordinated by relying on a decentralized community than a centralized one (see, for instance, Andreas Antonopoulos's speech at the MIT Bitcoin Expo; Antonopoulos, 2016).

With regard to decentralized DAOs, some believe that "more usage will drive development rather than [that] more development will drive the usage" (Pétur Árnason, 2017 interview #11, core developer of Auroracoin). But our results point to the primacy of the breadth and depth of stakeholder discussions (G2) required to kick-start growth. These discussions, in turn, lead to software updates that represent increases in the innovation potential of the DAO, as recent research has demonstrated (Wang & Vergne, 2017). As Cassini explains, "It's not the cryptography or the proof [. . .] that has an influence on the profitability, but it's more what community is behind that coin" (emphasis added, interview #16). So, our results suggest that development drives usage, at least among DAOs that are less reliant on decentralization to coordinate their activities.

6.3 Propositions

Following the fsQCA results, I put forward three propositions.

6.3.1 Machine Consensus and Decentralization of Strategy Making as Complements

Effective coordination, resting on accountability, predictability, and common understanding (Okhuysen & Bechky, 2009), is a precondition for organizational growth (Mintzberg, 1979). Based on my study of Bitcoin, I conjectured that machine consensus mechanisms helped achieve common understanding in novel ways, to the extent that they relied on machine routines that are open source, publicly auditable, and built by the community. Generally speaking, common understanding is difficult to achieve in decentralized organizations precisely because there is no centralized authority conveying a clear sense of what the organization's vision, strategy, and goals are.

Looking at the fsQCA findings from study #2, I found that organizational growth results from a combination of strong reliance on both machine consensus and decentralization (G1). I also found that centralization without strong social consensus always leads to decline (D1 and D2).[29] Taken together, these findings clearly point to the complementary roles played by machine consensus and decentralization. Indeed, machine consensus mechanisms are powerful drivers of common understanding—the one pillar of effective coordination that is hard to achieve in decentralized settings.

In general, it is when strong machine consensus mechanisms are in place that decentralization produces its most positive effects (e.g., high predictability, since no insider has the discretionary power to affect operations) because its downsides are then mitigated by a countervailing force (i.e., common understanding provided by machine routines). An interview with Worldcoin's core developer, Berzek (pseudonym, interview #10), provides a concrete example of how machine consensus mechanisms (here, related

[29] The decline configuration associated with Auroracoin, not reported in Table 2, also features decentralization and the absence of strong machine consensus.

to stability provision) can provide the kind of predictability that is often missing from decentralized organizations, thereby affecting their ability to coordinate effectively for growth:

> The problem with pure [PoW] coins (like us) is that many miners dump the coins immediately for a profit so there is a constant downward pressure on the price [. . .] This pressure is alleviated in a defined period of time—four years for Bitcoin, [and] one per cent weekly in our case [. . .] So our curve does not have discrete jumps [. . .] It is very smooth, therefore more predictable, and causes no anxiety for investors or supporters.

Similarly, study stages #1 and #2 combined suggest that machine consensus fosters accountability at the organizational but not at the task level, where random assignment of tasks prevails. On the other hand, decentralized strategy making does the exact opposite by giving autonomy and proper incentives to DAO members at the task level—even if that implies less accountability at the organizational level, e.g., if a DAO causes harm, who can be held responsible? From a coordination perspective, it thus makes sense for machine consensus and decentralization mechanisms to complement each other effectively, and our study demonstrates that this is indeed the case in the cryptocurrency industry. I thus propose:

> **Proposition 1:** Within DAOs, coordination based on machine consensus mechanisms enhances common understanding at both the organizational and task levels, but it enhances accountability and predictability only at the organizational level. By contrast, coordination based on decentralized strategy making does not enhance common understanding, but it does enhance accountability and predictability at the task level. Therefore, coordination mechanisms based on machine consensus and decentralized strategy making are complementary, at both the organization and task levels. These complementarities make coordination particularly effective and lead to DAO growth.

6.3.2 Social Consensus as a Substitute for the Machine Consensus-Decentralization Pair

Looking at G2, I find that social consensus mechanisms foster the growth of DAOs that do not heavily rely on machine consensus or decentralized strategy making. This hints at the existence of a substitution effect between social consensus, on the one hand, and machine consensus and decentralization, on the other. The importance of social consensus mechanisms is highlighted by Riccardo Spagni, the lead developer of the Monero DAO (interview #18, 2017): “Focusing on things like getting investors is pointless because all you’re doing is creating something that looks like a scam. Really all you can do is just focus on building up the community so that you have contributors to the project and you have people that are interested in testing the project and everything else sort of comes from that.”

On a related note, Cohen emphasizes the crucial role played by stakeholder discussions in the developer community:

> Honestly, I think [. . .] the developer, main developer, and the circle of contributing developers is particularly strong, [so] Blackcoin has retained, even now, two years later, a degree of respect and you know, it is sort of the brand—I mean of course this is a totally different consideration from the purely technical ones, but brand recognition and stable user base and sense of trust that, you know, this blockchain will not be dead tomorrow, those are very important in terms of adoption. (interview #7)

So, even though DAOs tend to place “automation at the center” (Buterin, 2014), machine consensus mechanisms need not be too heavily relied upon to generate growth (as shown in G2), nor be too much in the background to produce decline (as shown in D2). Arthur Breitman, core developer of the Tezos DAO, stated in an online interview, “to be sure, there is some math that does give you strong guarantees . . . and these are very, very strong guarantees. And then you have the [social] consensus itself, which . . . is going to be an economic and social problem, and not a mathematical one” (Breitman, 2016).

To further unpack the substitution effect between social consensus and the machine consensus-decentralization pairing, we need to look at how social consensus mechanisms provide the kind of common understanding, accountability, and predictability needed for effective DAO coordination. Social consensus mechanisms bring together communities of developers, users, and network validators in both formal (e.g., BIPs) and informal (e.g., online forum discussions) ways. The breadth and depth of these discussions, alongside network validators' commitment to the DAO, create a sense of common understanding at both the task and organizational levels, much like machine consensus mechanisms. Social consensus mechanisms also enhance accountability and predictability at the task level by connecting proposals for organizational change to real-world identities—something that machine consensus mechanisms are, by design, unable to achieve (even though they enhance accountability and predictability at the organizational level). However, without a heavy reliance on machine routines, social consensus mechanisms may lead to inertia, since stakeholder involvement is at risk of getting stuck at the discussion stage, without its being translated into action due to lower automation levels. This is where a degree of centralized strategy making can come into play to aggregate stakeholder contributions and define a course of action going forward. Therefore, I postulate:

> **Proposition 2:** Within DAOs, coordination based on social consensus mechanisms enhances common understanding at both the organizational and task levels (in a similar manner to machine consensus), but it enhances accountability only at the task level (unlike machine consensus). By contrast, coordination based on some degree of centralized strategy making enhances accountability at the organizational level. Therefore, coordination based on social consensus mechanisms acts as a substitute for coordination based on a combination of machine consensus and decentralized strategy making. DAOs that are not too decentralized but rely heavily on social consensus are able to grow, even in the absence of strong machine consensus.

6.3.3 Balancing Efficiency and Effectiveness—but Privileging Effectiveness

A strong reliance on machine consensus mechanisms often leads to inefficiencies because it entails duplication of effort (i.e., every miner must work on solving the next block) and wasting resources (e.g., electricity and hardware). Nonetheless, consistent with the G1 configuration in Table 2, I found that DAOs that generate such inefficiencies can coordinate effectively in order to grow. So it appears that seeking efficiencies is not a precondition for success for DAOs. As Spagni explains, “It’s the same inefficiencies that exist in blockchain technology. It’s a good sort of inefficiency. It’s the inefficiency you want. You want some of these things to be difficult to do because it means that it’s also difficult to shut down.” (interview #18)

A DAO that cannot be shut down becomes more predictable for its stakeholders, and in turn this predictability enhances the DAO’s effectiveness (e.g., a system that holds billions of dollars’ worth of cryptocurrency in user deposits cannot effectively process payments when it risks being shut down, even if only temporarily). Besides, inefficiencies at the level of machine consensus have an interesting implication in that they enable the DAO to function with very little coordination at the task level. Indeed, when each task is assigned by default to every organizational member in a way that demands efforts that will ultimately be wasted, there is no need to coordinate either task assignment or the corresponding allocation of resources (e.g., every network validator must commit costly resources and try to solve the next block, even though only one network validator will ultimately be rewarded). Instead, resources are allocated using market mechanisms. As Evan Duffield, founder and lead developer of Dash explains, the work of network validators within a DAO represents “a market within itself” (interview #2, 2016):

> We have a free-floating masternode network [i.e., paid nodes that have decision-making power based on voting rights], and so if there’s too many masternodes, they’ll start making too little, a couple will drop off. And if there’s too few masternodes, they’ll start making too much, and then that’ll increase incentives, and some people will buy it. And so this is a stabilizing factor.

In a similar fashion, reliance on extremely decentralized coordination structures—as I argued before, these are a useful complement to machine routines—can lead to inefficiencies because it inevitably brings about redundancies and slower decision making. In line with our findings, Pike states, “The conundrum is you don’t really want [a centralized organization or a foundation] if you believe in decentralization, but without it, you’re not as efficient as you would otherwise be. So it’s kind of a more organic process that is really undefined. I would say at this stage, everyone’s just trying to figure out how to make decisions.” (interview #12)

Regarding the same trade-off, Spagni states, “[Decentralized self-organizing] is not as efficient, but [. . .] from the perspective of a cryptocurrency, it creates an environment that is impossible to shut down.” (interview #18)

I thus propose:

> **Proposition 3:** DAOs balance efficiency with effectiveness. The more a DAO relies on decentralization and machine consensus, the more likely it is to be inefficient in terms of resource usage, but the more effective it becomes at coordinating in order to grow.[30]

In what follows, I will discuss these findings in terms of theoretical implications, future directions, followed by conclusions.

[30] The optimal balance between efficiency and effectiveness depends on factors that are beyond the scope of this study, such as the cost of external resources (electricity), the price of the cryptocurrency (a higher price provides stronger incentives for network validators), the strength of the network effects, and the extent to which the effectiveness of the DAO depends on the reliability of its blockchain infrastructure. In the cryptocurrency/payments industry, the level of reliability expected from users is extremely high, but this may not be the case in other industries in which DAOs compete.

Chapter 7 Discussion and Conclusions

7 Discussion and Conclusions

DAOs are a new form of organizing that provide novel solutions to the four universal problems—task division, task allocation, reward distribution, and information flows (Puranam, Alexy & Reitzig, 2014). Motivated by establishing a deeper understanding of the coordination mechanisms of DAOs, this research offers a theoretical framework based on distributed consensus mechanisms.

Throughout this study, I have asked the following question: how can tasks be adequately coordinated to enable organizational growth without placing human decision makers at the center of an organization? Guided by findings from the Bitcoin pilot study, the three-stage inductive research design provides tentative answers to this question, which I have summarized in the three propositions developed above. In essence, this study identified a new set of coordination mechanisms based on machine routines, which interact with coordination mechanisms around social consensus and decentralized strategy making to produce growth (or decline) under certain conditions that are detailed in the fsQCA analyses. Effective coordination occurs through reliance on a previously unseen class of stakeholders called "network validators" and, due to the random assignment of ultimately redundant tasks to network validators, DAO growth sometimes occurs at the expense of efficient resource usage.

In this concluding section I will highlight the high-level contributions of this study to the literature on organizational task coordination, and I will outline some of the broader implications of the rise of DAOs for organizational and management scholarship, against the backdrop of a decreasing presence of the public corporation in contemporary business life.

7.1 DAOs as a Novel Form of Organizing

DAOs are characterized by several unique organization design features that were previously unseen in traditional organizations.

DAOs enable extreme forms of decentralization. This research takes a first stab at investigating blockchain-based implementations as a new form of organization design. It contributes to the organization design literature by developing a theoretical framework to make sense of DAOs. Specifically, it shows that machine consensus mechanisms, powered by incentivized voluntary contributors who validate and record stakeholder transactions, make DAOs uniquely positioned to offer new solutions to "the universal problems of organizing" faced by "distributed organizations" (e.g., Wikipedia) that do not rely on machine consensus (Puranam, Alexy & Reitzig, 2014: 166–169). Machine consensus may bear resemblance with other technology-enabled coordination systems such as version control, Uber, and Wikipedia, in the way task division and task allocation is based on self-selection and is embedded in the algorithm. However, fundamentally, version control is a technology system (instead of an organization), and unlike DAOs, Uber and Wikipedia are centrally owned and managed by corporations or foundations, which coordinate a large part of their tasks through centralized authorities.

It is important to distinguish DAOs from open source projects like Wikipedia in that, while DAOs distribute ownership, governance, and control to various stakeholder groups, platforms such as Wikipedia are centrally owned and managed by a centralized organization, e.g., the Wikipedia Foundation Inc. The content on Wikipedia is also centrally controlled and censored. The recent formation of Everipedia, a blockchain-based open source encyclopedia, serves as an application of DAO to provide an uncensorable, decentralized encyclopedia that incentivizes voluntary contributors with a token called "IQ." Everipedia stands as a perfect example how DAOs compare and contrast with distributed organizations, and how DAOs can be applied to make such projects truly decentralized. Admittedly, DAOs enable an extreme form of decentralization powered by consensus mechanisms.

Similarly, in contrast to community-governed organizational forms (e.g., OSSD projects), DAOs have a distinctive goal that guides the "standard development" of the organizing principle rather than "software development" for the product (interview #26). The DAO organizing principle, rooted in decentralization and automation, transforms the dynamics of community-based organizing to focus extensively on consensus-based decentralization of decision making and coordination. As a result, while formal authority tends to develop in OSSD communities over time (O’Mahony & Ferraro, 2007), DAOs aim to mitigate and distribute authority by integrating machine consensus with social consensus mechanisms.

Organizational innovation vs. technological innovation: Two significant innovations underpin Bitcoin: a technological one, namely the public and distributed ledger technology called blockchain, which securely maintains an immutable record of all user transactions; and an organizational innovation, namely, the existence of an open network of users with special roles and rights called miners, who lend computing power to secure the network in exchange for newly minted bitcoins and voting rights with respect to future protocol revisions (Davidson, De Filippi & Potts, 2016a; 2016b).

As an industry expert puts it, a blockchain will not work without Bitcoin or the consensus algorithm (e.g., PoW) behind it (Antonopoulos, 2016 speech[31]). And the reason is simple—a blockchain can only ensure the core of its true innovation, namely an open, borderless and censorship-resistant system, through the organization design that performs tasks and provides rewards in novel and unique ways. The DAO’s innovation drives the blockchain technology, and this logic is fundamentally different from what we have seen in OSSDs and other self-organized organizations (Lee & Edmondson, 2017).

7.2 Distributed Consensus Mechanisms

Coordination by consensus mechanisms. Results from the pilot study suggest that distributed consensus is what makes the DAO organizational innovation possible. Subsequently, findings from the first stage reveal three key features of task coordination within DAOs. First, ***machine consensus mechanisms***, driven by sets of machine routines, are meant to deliver provable security for user transactions and to ensure organizational stability in a context in which stakeholders can come and go at will.

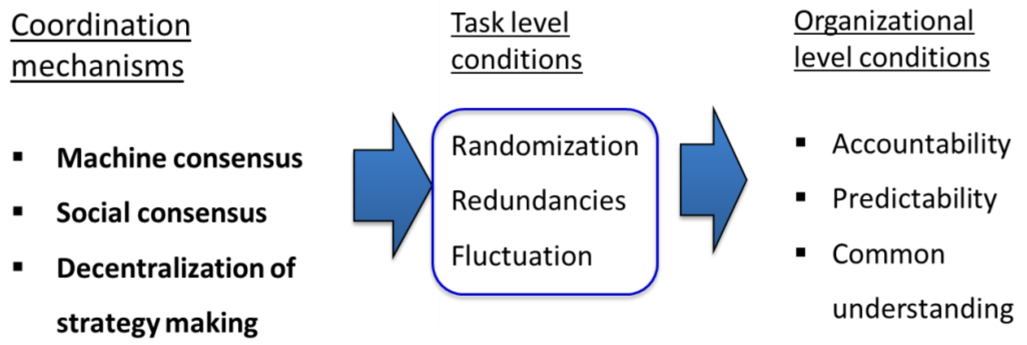
[31] Sources: https://www.newsbtc.com/2016/06/01/andreas-antonopoulos-explains-blockchain-nothing-without-bitcoin/; https://youtu.be/mRQs9Y6CUSU.

Machine consensus, both at the level of the tasks that it governs (e.g., record keeping) and at the broader organizational level, contributes rather straightforwardly to common understanding (i.e., all the machine routines are open source and publicly auditable). But its contribution to the other two integrative conditions for coordination, namely predictability and accountability, deserves a more nuanced explanation.

Since every transaction remains traceable indefinitely based on its immutable blockchain record—this characteristic ties transactions to a specific network validator, a sender, and a recipient—accountability seems ensured at the organizational level. However, network validators are not assigned ex ante to specific transactions, since DAOs do not rely on hierarchy to assign tasks. In fact, network validators are randomly assigned to their tasks (e.g., with Bitcoin, the first miner who is lucky enough to guess a long random number will add the next block to the ledger and receive the coin rewards). This feature is meant to prevent malicious users from attacking particularly valuable nodes in the network; it is not unlike a situation in which a bank robber knows that, out of the 5,000 vaults out there, only one contains the gold reserves, but cannot know which one it is because that vault is chosen randomly by a computer program (and the gold is randomly moved to a new vault every ten minutes).

Consequently, DAOs achieve disintermediation through randomization of work and costs of validation. In particular, routine work is performed in a purposefully redundant and wasteful way to coordinate the main tasks; effectiveness, in the form of security provision and stability provision, can trump efficiency to serve as the primary organizational goal. By randomization, difficulty fluctuation, and inefficiency at the task level, DAOs ensure organizational level accountability and predictability. A conceptual framework is shown in Figure 13.

Figure 13 Conceptual Framework of Consensus Mechanisms and Conditions at the Task vs. Organizational Levels



So, even though, at the task level (e.g., transaction verification, generation of coin rewards), accountability cannot be assigned ex ante, this very feature contributes to accountability at the organizational level (i.e., it is a way to prevent cyber attacks and thus ensure data integrity for the ledger). Similarly, this random assignment of tasks is clearly at odds with enhancing predictability, but only at the task level. At the broader organizational level, randomization actually contributes to the DAO's predictability by ensuring that transactions will be processed as per the code, without outside interference. Interestingly, these coordination mechanisms do entail duplication of effort and redundancies. Instead of using one vault and protecting it very well, Bitcoin uses thousands of identical vaults and makes it too costly for thieves to guess which one contains the money. Put differently, in order to achieve their goals (e.g., building a peer-to-peer value-transaction network), DAOs deliberately waste resources (e.g., thousands of miners consume hardware resources and electricity simultaneously when only one miner would be enough to verify transactions). In short, DAOs work with coordination mechanisms that clearly emphasize effectiveness at the cost of efficiency.

As non-hierarchical organizations, DAOs face the same high-level predictability challenges as OSSD communities due to a lack of formalization in terms of role definition for strategy making (Okhuysen & Bechky, 2009). However, unlike OSSD communities, DAOs are able to overcome some of these predictability challenges by relying on machine consensus and by integrating it with ***social consensus*** through a new class of paid stakeholders, namely, network validators. In DAOs, social consensus is meant to produce agreement across stakeholder groups about organizational strategy by facilitating stakeholder discussions and network validators' commitment. Offline and online discussions, as well as votes recorded in the public ledger, readily contribute to enhancing accountability and common understanding and to providing stakeholders with updates regarding how predictable future organizational changes will be.

Machine consensus and social consensus are eventually integrated and aligned through reliance on network validators who make decisions in more or less decentralized ways. The third important feature of task coordination within DAOs is thus ***decentralization***, conceived of here as a continuum that underpins decision making at every stage. With Bitcoin, for instance, new ideas are generated in a decentralized way by developers across the world. These ideas are subsequently pooled together in discrete blocks called BIPs and then discussed informally in online discussion forums. Finally, they are voted upon formally by decentralized miners who ultimately update the software, which is released in a more centralized fashion by the DAO's core developers and is based on the accepted BIPs. Although decentralization makes DAOs' ability to adapt less predictable at the organizational level (e.g., the strategic direction may be unclear, resulting in inertia), it also makes them more predictable at the task level (e.g., no organizational insider has the power to defraud a user). On the other hand, decentralization removes some of the unpredictability that comes from the existence of high-level managers with a lot of discretionary power (e.g., there is no CEO with the power to decide on a merger), but which can at times decrease accountability (e.g., if something goes wrong, who can be held responsible?).

Interestingly, then, coordination mechanisms around machine consensus, social consensus, and decentralization of strategy making contribute to accountability, predictability, and common understanding in different ways and at different levels of the organization (task level vs. organizational level).

7.3 A New Form of Coordination: Coordination with Machine Consensus and Network Validators

DAOs offer an alternative to human-centered organizational design by introducing new coordination mechanisms based on machine consensus, which automates many of the routine tasks performed by the organization through the use of an immutable database shared across all stakeholder groups (the blockchain). It would be inconceivable for a traditional business organization to require all employees to perform the same routine task but then only reward one single employee drawn at random while discarding everyone else's work. Yet this counter-intuitive way of coordinating tasks is necessary for a DAO to achieve predictability, accountability, and common understanding, and for it to be able to reliably disintermediate transactions (Lopp, 2016). Besides, even though DAOs coordinate tasks rather formally, organizational members cannot feel coerced by management (since there is none) and can choose to leave and join another DAO at will—so DAOs offer an alternative to the usual trade-off between formal coordination and organizational member autonomy (Adler & Borys, 1996).

Beyond the mere identification of a new set of coordination mechanisms (machine routines), this study contributes to a finer understanding of task coordination within organizations. Specifically, while our research confirms the crucial role played by predictability, accountability, and common understanding in coordination (Okhuysen and Bechky, 2009), it also demonstrates the practical value of distinguishing between the task and organizational levels when examining these three pillars (Young-Hyman, 2017). Indeed, certain coordination mechanisms (e.g., decentralized strategy making) enhance predictability at the task level but not at the organizational level, while others (e.g., machine consensus) do the inverse. Thus, it becomes crucial for organizations to have integrating mechanisms in place to compensate for these discrepancies.

The mining process, which is based on competitive bookkeeping by network validators, plays such an integrating role. In the coordination literature, integrators are defined as "formally mandated managerial roles meant to promote coordination across specialized but interdependent organizational subunits, yet they do so without relying on formal authority" (Stan & Puranam, 2016). Integrators such as project managers (Wheelwright

& Clark, 1992) or account managers (Iansiti & Clark, 1994) play an essential role in the organizational structure by facilitating a “steady state of coordination” between stakeholder groups within and around organizations (Stan & Puranam, 2016; Mohrman, 1993). However, in DAOs, network validators are able to act as “integrators” without holding a “formally mandated managerial role,” thanks to the machine consensus mechanisms that provide incentives to stabilize the organization in the long run. Network validators integrate functions across levels—payment processing at the blockchain level, security provision at the network level, and voting at the protocol level—but their work goes beyond traditional role-based coordination (Bechky, 2006), as they can join or leave the organization at will and do not depend on managerial oversight (Stan & Puranam, 2016).

In this sense, there is no pooled task interdependence in DAOs, but instead a randomized assignment of tasks spawned by a new form of automated coordination (Thompson, 1967; Daft & Armstrong, 2012; Okhuysen & Bechky, 2009). This is precisely why coordination within DAOs differs from the forms of coordination observed in OSSD projects. As Okhuysen & Bechky (2009) rightly point out, “Post-industrial work requires assembling specialized knowledge in ways that we have not done before while facing new task environments.” In both DAOs and OSSD projects, communities of volunteers manage and maintain code on open-source software platforms, making it transparent and easy to share (O’Mahony, 2003; O’Mahony, 2007; O’Mahony, Puranam et al., 2014; West & O’Mahony, 2008). Yet while OSSD projects may face predictability problems due to the lack of clear governance structures (Okhuysen & Bechky, 2009; O’Mahony & Bechky, 2008), DAOs rely on machine consensus mechanisms to compensate for this while maintaining a high level of decentralization. And this is how DAOs provide novel solutions to the old problems of organizing.

7.4 Growth Implications: Organizational Growth: DAOs vs. Traditional

Organizational growth is historically conceived of as driven by the need to acquire external resources, such as financial capital, especially for new ventures. Centralization of production serves as the main enabler behind modern corporate growth as it is conceived of as having the ability to enhance coordination efficiency, corporate wealth or managerial strategic decision power (Chandler, 1977; 1990; Perrow, 2002). For industrial corporations that seek either scale or scope, financial indicators such as sales and financial returns are used to capture growth in the literature (e.g., Eisenhardt & Schoonhven, 1990; Larson, 1992; Weinzimmer, Nystrom & Freeman, 1998).

What does growth mean in the context of non-centralized, non-hierarchical DAOs, and how does it challenge the idea of growth as conventionally defined? On the one hand, if we focus on DAOs' ability to support a two-sided platform for value exchanges (e.g., as payment systems), mainstream adoption of a DAO will rely on the growth of users who use the DAO for transactions to generate the network effects. On the other hand, in theory, DAOs can survive as long as there is one validator and some users on the network, although the security of the network and the health of the blockchain may be compromised. Fundamentally, as my interviews revealed, mainstream adoption stands as an important goal for cryptocurrency DAOs to make mining efficient (because the same level of security generated by miners can now be used by a large user base), to ensure the health of the network, and to retain the value of the cryptocurrency token.

Specifically, early growth is an important indication of the success or failure of a crucial process called "bootstrapping" that is required to get a cryptocurrency DAO off the ground:

> There is a tricky interplay between three different ideas in Bitcoin: the security of the blockchain, the health of the mining ecosystem, and the value of the currency. We obviously want the blockchain to be secure for Bitcoin to be a viable currency. For the blockchain to be secure, an adversary must not be able to overwhelm the consensus process. This in turn means that an adversary cannot create a lot of mining nodes and take over 50 per cent or more of the new block creation . . . When Bitcoin was first created, none of these three existed. There were no miners other than Nakamoto himself running the mining software. Bitcoin didn't have a lot of value as a currency. And the blockchain was, in fact,

> insecure because there was not a lot of mining going on and anybody could have easily overwhelmed this process. (Narayanan et al., 2016: 70-71)

Thus, it is reasonable to say that growth in the user base measured by transactions captures the growth of the consensus base formed by key stakeholders—validators, users, and developers. Consequently, this consensus base determines the health and the value of the DAO. Early growth in the use of the cryptocurrency DAO captured by growth in the number of transactions instead of financial indicators also helps rule out speculations reflected in price or market capitalization. This consensus-based notion of growth challenges the traditional growth motivated by efficiency, scale and scope economies, and centralized power and control.

7.5 Limitations and Future Directions

7.5.1 Limitations

The limitations of this research come from several assumptions that shape the boundary conditions for the generalization of findings.

First, I focus on the internal stakeholders who have direct decision-making power over the blockchain and protocol. The reason for this decision is to focus on those organizational actors whose tasks are directly being coordinated by machine versus social consensus. Specifically, my decision to focus on network validators and developers is based on my interviews and readings. While fully acknowledging the role of other types of nodes in maintaining the network (e.g., full nodes without mining functions and lightweight nodes which do not have to store the full blockchain ledger), a simplified model better serves the purpose of this study as an early attempt to understand DAOs from a management and organizational perspective. Similarly, external stakeholders, such as merchants, regulators, and third-party services, who do not directly interact with the operations of DAOs are precluded from my current scope of organization design. Moving forward, they represent important research opportunities to study governance and inter-organizational coordination (e.g., Hsieh, Vergne & Wang, 2017).

Second, this study assumes stable external environments. This assumption simplifies the complexity a DAO faces. For example, even though the Bitcoin blockchain is extremely secure, when an external Bitcoin exchange is hacked (for example, in the most recent case, a Bitcoin exchange, NiceHash, was hacked with $64 million worth of bitcoin stolen), Bitcoin's transaction volume and value will certainly be affected. Network activities, such as mining, may also be affected by the drop of token value depending on the health of the mining ecosystem.

Finally, I assume a homogenously distributed network without concentration. For example, I do not distinguish the incentive structure between mining pools (i.e., miners pooling computing power together to have a better chance of winning) and solo miners. This is intended to simplify and focus the argument on general coordination problems of a distributed organization.

In terms of data analysis, as I pointed out in Chapter 5, there is a trade-off between sampling a range of cryptocurrency DAOs with variations in their design and focusing on cases founded at around the same time in order to control for cohort effects. I made a choice to focus on the former but sampled a number of cryptocurrency DAOs from different industry stages proportional to the founding rate to make my sample representative. Additionally, since fsQCA is not a variance-based method that requires control variables as in regression models, the absence of the explanatory condition "industry stage" will not take away the influence of other conditions as part of a necessary or sufficient configuration.

7.5.2 Future Directions

Inter-organizational coordination and governance between DAOs. DAOs have opened up ample opportunities for future organization research. For example, distributed trust has transformed traditional coordination relationships that defined organizational boundaries (Seidel, 2018). Specifically, to extend the research theme of this study, inter-organizational coordination relationships are of particular interest. For example, how does the utility layer of a DAO (e.g., Ethereum) coordinate with a second layer ICO token (e.g., VeChain or EOS) that builds its products and services on the utility platform?

How would the shift of trust relations change inter-organizational dynamics that were originally based on social relations or transaction costs (Seidel, 2017)? How do these external stakeholders exert influence on the decision-making process of DAOs? And how does the new form of coordination change how we think about internal and external governance?

Longitudinal studies on DAO growth. As the industry grows and matures, it is necessary to study the DAO growth trajectory over time and compare it with public corporations and identify whether and how fundamental differences exist in their growth patterns. In addition, performing cohort studies will be feasible and useful for longitudinal studies to control for industry effects and perhaps to compare patterns across various industry stages. Finally, alternative growth measures may shed light on the multiplicity of DAO objectives. For instance, while users contribute to generating network effects, investors drive up the value of DAOs, and regulators stand as the institutional gatekeepers that determine the growth or decline of the industry. By considering a broader range of stakeholders, it would be possible to capture what Buterin (2017) called "multifactorial consensus," where "different coordination flags[32] and different mechanisms and groups are polled, and the ultimate decision depends on the collective results of all of these mechanisms together."

In sum, the rich context, with abundant data sources, provides ample opportunity for future research on the evolution and sustained growth of DAOs, as well as contingencies under which DAOs are viable and can be implemented in varied applications (such as smart contracts, and signature services), in hybrid forms (e.g., centralized financial institutions integrating a distributed organizational form as a solution to enhance efficiency).

[32] Coordination flags refer to votes signaling preferences, for example, whether or not a hard fork is happening (Buterin, 2017b).

7.6 Managerial Implications

Insights from this study are directly relevant to the FinTech revolution in action right now. Traditional financial institutions are increasingly interested in blockchain technology and have been extensively experimenting with the possibility of blockchain integration. It is foreseeable that hybrid forms of traditional and DAO can emerge, similar to what has taken place between OSSD and private sponsors, such as private corporations (O'Mahony, 2007).

For large international banks to adopt the blockchain technology, permissioned[33] blockchains are often necessary for enterprise solutions to protect proprietary assets. While managers are contemplating the future of enterprise blockchains, this research provides a new way of thinking about adopting blockchains not in terms of technology adoption but in terms of the integration of new forms of governance and coordination. That is, if machine consensus and decentralization are complements, as suggested by the findings, large banks may choose to adopt the machine consensus (i.e., the blockchain and protocol) without adjusting the coordination structure toward the decentralization end of the continuum. The extent to which a highly centralized organization can capitalize on the unique features of blockchain technology is still a puzzle.

> Banking is, ultimately, a centralized system . . . It's great if you want to have a decentralized currency that isn't controlled by any one person, but if you have a bank or a central government providing it then it stops being decentralised and the whole blockchain technology aspect becomes, sort of, redundant . . . As soon as you centralize it and there's one controller it's unnecessary to use anything other than a database . . . The advantage of a block chain comes when you're farming out the data to anyone and you don't know who the actors are. But if it's a private chain and you know who the actors are and you can trust them then it's not worth it anymore. [James Lovejoy, Core developer at Vertcoin, interview #5]

[33] Permissioned or private blockchains refer to DAOs that only allow trusted nodes in the network to work as validators. The validation may or may not involve costs such as proof-of-work requires.

Therefore, for managers to think about blockchain adoption, the complementarity between machine consensus and decentralization cannot be overlooked. On the other hand, from the standpoint of social consensus, a private blockchain means the development team will be paid employees either of the financial institution or of the FinTech start-up that provides the service (e.g., Ripple and Stellar). How is this setting different from traditional firms and how will adopting firms capitalize on the advantages offered by early adoption?

The financial industry is only the first one to be impacted by distributed organization—any industry relying heavily on intermediaries (e.g., brokers) can be deeply affected by this form of organizing.

7.7 Organizations of the Future: An Under-Socialized Worldview?

In the last section of the dissertation, I conclude my research with a few extended higher-level thoughts.

1. Code is Law?

The emergence of DAOs, to an extent, reinforces the under-socialized post-capitalist worldview characterized by digitalization, decentralization, and disintermediation and by the idea that "code is law" (Lessig, 2006), that Bitcoin is the "trust machine" (Economist, 2015a) wherein human trust is no longer necessary, and that DAOs require "little coordination" (Nakamoto, 2008). Intriguingly, Vitalik Buterin, co-founder of Ethereum, who first proposed the idea of DAOs characterized by "automation at the center, humans at the edges," shared his concerns about DAO on-chain governance[34] that relies on token-holder voting rules built in machine routines in a recent post:

[34] On-chain governance refers to the practice of embedding DAO governance rules in the protocol. On-chain governance is intended to create a self-amending system that "seamlessly amends the rules governing its protocol and rewards protocol development" (https://www.tezos.com/governance). It is said to have the benefit of avoiding decentralized informal human-decision making systems and can evolve rapidly to incorporate any necessary technological advancement. Proponents of on-chain governance generally believe that it avoids the downsides of informal governance, including being unstable and prone to chain

> People who think that the purpose of blockchains is to completely expunge soft mushy human intuitions and feelings in favor of completely algorithmic governance (emphasis on completely) are absolutely crazy[.]…[L]oosely coupled voting as done by Carbonvotes[35] and similar systems [are] underrated. (Buterin, 2017b)

In contrast, Buterin thinks that informal governance mechanisms such as Carbonvotes, that are not based on token ownership, serve as an important social means for distributed consensus mechanisms to work. According to Buterin (2017a; 2017b; 2018), the under-socialized, on-chain voting that heavily relies on machine routines risks overlooking other representative stakeholders' roles in coordination by focusing solely on token holders. Instead, he argues that a balance needs to be struck among stakeholder groups for a collective consensus based on formal and informal votes from the core development teams, coin holders, in line with established norms and a roadmap. This view reinforces what we learned from this research, namely, that the growth of a DAO depends on balancing the three elements—machine consensus, social consensus, and decentralization of decision making. Code is not law, and social consensus still matters.

2. When is DAO a Viable Form?

Research indicates that the technological innovation potential behind cryptocurrencies stands as the key driver of their market value (Wang & Vergne, 2017). But, as the Economist (2015b) rightly points out, blockchain technology has far-reaching applications beyond cryptocurrency and payments. In fact, blockchain-based organizing and the resulting DAOs have the ability to replace centralized intermediaries in other applications requiring complex coordination such as asset ownership tracking, trade financing, digital identity provision, supply chain traceability, and more. Besides, in the

splits, and having the tendency to become centralized (Buterin, 2017b). On-chain governance is conceived of as "tightly coupled voting" across Buterin's articles on blockchain governance (e.g., Buterin, 2017b: 2018).

[35] CarbonVote is an informal voting platform for the Ethereum community (see: http://carbonvote.com/).

last three years, more than fifty new ventures received seed funding using blockchain-powered “initial coin offerings,” thereby bypassing, at least partly, the use of venture capitalist intermediaries to obtain funding faster and at more favorable valuations (e.g., in 2014, Ethereum raised $18.4 million in a few days and is now valued at $34 billion).

Therefore, DAOs are able to serve as intermediary organizations, in which a high level of security and immutability is a desired feature enabled by the consensus mechanism and distributed trust it produces.

3. Market? Hierarchy? Network? Broader Implications for Organizational and Management Scholarship

DAOs are coordinated by consensus mechanisms. Thus, DAOs are different from markets coordinated by price mechanism, hierarchies coordinated by fiat, or networks coordinated by social relations (Powell, 1991). How should one make sense of DAOs?

DAOs are not governed by principal-agent relationships, since they do not have shareholders or managers (Jensen & Meckling, 1976). Because they do not rely on fiat or hierarchies and operate transparently using public blockchains and open-source software, they are, to some extent, immune to the issues of opportunism and information asymmetry (Williamson, 1975). And because they operate with little human coordination and do not incur costs for monitoring employees, they may behave in ways that traditional perspectives in organizational economics are ill-equipped to capture. In particular, the growth of DAOs is likely not bound by increases in the marginal cost of organizing (because DAOs are not hierarchies) (Coase, 1937), and the cost of conducting additional transactions within DAOs can theoretically decrease with size owing to positive network externalities. Thus, at this stage, the scholarly community may lack the theoretical tools needed to understand either the growth of DAOs or, more generally speaking, what determines the boundaries of such organizations. The present study only begins to tackle this problem. Future scholarship is needed to propose revised theoretical frameworks to further our understanding of the DAO phenomenon.

4. Decentralized Autonomous Organizations: An Alternative to the Public Corporation?

In a thought-provoking essay, entitled “After the Corporation,” Gerald Davis remarks that:

> [T]here are fewer than half as many public corporations today as there were fifteen years ago . . . The public corporation in the US is now unnecessary for production [and] unsuited for stable employment . . . Although formal organizations have long been the go-to format for nearly every organized activity in the industrialized West . . . they are no longer the obvious default option . . . And while Linux and Wikipedia are cliché examples, they nonetheless serve as proof of concept: it is possible for voluntary, dispersed, collaborative, relatively non-hierarchical forms of organizing not just to work well, but to far surpass their privately-produced alternatives. (Davis, 2013: 284; 290; 299; 301)

Meanwhile, over the last few months, over 150 DAOs have gone public through initial coin offerings, a public sale through which the general public can acquire, early on, cryptocurrency tokens to support the development of the organization (ICOtracker, 2017). While the number of public corporations is dwindling—there are 37 per cent fewer today than there were in 1997 (VanderMey, 2017)—DAOs are on the rise.

Outside the payments sector, DAOs are providing new solutions for supply-chain management in the luxury goods industry, record keeping in trade finance, trusted-identity provision in online environments, and patient-history management in the healthcare sector. What these industries have in common is that their business activities are prone to moral hazard and behavioral uncertainty. As a result, expensive intermediaries are heavily relied upon to provide trust to the interacting parties (Zucker, 1986). Going forward, DAOs may be able to provide competitive alternatives for organizing in those sectors.

More than 30 years ago, Rothschild and Whitt (1986: 114) identified factors that should lead to the development of “collective organizations.” These included the demystification of knowledge, defined as the process whereby “formerly exclusive, obscure, or esoteric bodies of knowledge are simplified, explicated, and made available to the membership at large” (cited in Davis, 2013: 301). By publishing all software related to the blockchain, protocol, and peer-to-network in an open-source format, DAOs are well on track to achieve this demystification. In fact, the Economist (2015b) argues that, building on the vision of Ethereum co-founder Vitalik Buterin, the ultimate goal of DAOs is to serve as “virtual companies that are basically just sets of [open-source] rules running on . . . blockchain[s].”

At a theoretical level, the shift from the public corporation to the DAO may be a radical one, and this research represents a first attempt at exploring its implications from the viewpoint of organizational scholarship. I hope that organizational and management scholars will pay attention to these developments that are currently changing the face of the heavily intermediated form of capitalism that has prevailed in our economies since the seventeenth century.

References

Adler, P. S., Borys, B. 1996. Two types of bureaucracy: Enabling and coercive." ***Administrative Science Quarterly***, 41(1): 61-89.

Arjaliès, D. L., Hsieh, Y., & Vergne, J.-P. 2017. A reply to Cohen's "The Rise of Alternative Cryptocurrencies in Post-Capitalism." http://www.socadms.org.uk/rise-alternative-currencies/. Online commentary, ***Journal of Management Studies***, January 17, 2017.

Antonopoulos A. M. 2014. ***Mastering Bitcoin: Unlocking Digital Cryptocurrencies.*** Sebastopol, CA: O'Reilly Media, Inc.

Agarwal, R., Anand, J., Bercovitz, J., & Croson, R. 2012. Spillovers across organizational architectures: The role of prior resource allocation and communication in post-acquisition coordination outcomes**.** ***Strategic Management Journal***, 33(6): 710-733.

Amason, A. C. 1996, Distinguishing the effects of functional and dysfunctional conflict on strategic decision making: Resolving a paradox for top management teams. ***Academy of Management Journal***, 30(1): 123-148.

Argote, L. 1982. Input uncertainty and organizational coordination in hospital emergency units***. Administrative Science Quarterly***, 27: 420–434.

Atzori, M. 2015. Blockchain technology and decentralized governance: Is the state still necessary? https://ssrn.com/abstract=2709713. [Accessed September 2017]

Back, A., 1997. A partial hash collision based postage scheme. http://www.hashcash.org/papers/announce.txt. [Accessed June 12, 2018).

Back, A., 2002. Hashcash-a denial of service counter-measure. http://www. hashcash.org/ papers/ hashcash.pdf. [Accessed June 12, 2018].

Baldwin, C. Y. & Clark, K. B. 2006. The architecture of participation: Does code architecture mitigatee free riding in the open source development model? ***Management Science***. 52(7): 1116-1127.

Barker, J. R. 1993. Tightening the iron cage: Concertive control in self-managing teams. ***Administrative Science Quarterly***, 38(3): 408-437.

Baum, J. R. & Bird, B. J. 2010, The success intelligence of high-growth entrepreneurs: Links to new venture growth. ***Organization Science***, 21(2): 397-412.

Bechky, B. A. 2003. Sharing meaning across occupational communities: The transformation of understanding on a production floor. ***Organization Science***, 14: 312–330.

Bechky, B. A. 2006. Gaffers, gofers, and grips: Role-based coordination in temporary organizations. ***Organization Science***, 17(1): 3-21.

Bernstein, E., Bunch, J., Canner, N. & Lee, M. 2016. Beyond the holacracy hype. ***Harvard Business Review***, 94(7-8): 38-49.

Bergh, D. D., Sharp, B. M., Aguinis, H. & Li, M. 2017. Is there a credibility crisis in strategic management research? Evidence on the reproducibility of study findings.” ***Strategic Organization***, 15: 423–436.

Birkinshaw, J., Nobel, R. & Ridderstråle, J. 2002. Knowledge as a contingency variable: do the characteristics of knowledge predict organization structure?. ***Organization Science***, 13(3): 274-289.

Bitcoin Gold (BTG). 2017. https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf. [Accessed January 2018].

Bitcointalk.org. 2013. Topic: What exactly are hashes and how are they created. https://bitcointalk.org/index.php?topic=214442.5. [Accessed August 2017].

Blockchain.info. 2017“Bitcoin Block Explorer.” https://blockchain.info/. [Accessed August 2017]

BlockchainHub.net. 2017. What is blockchain? https://blockchainhub.net/blockchain-intro/. [Accessed July 2017].

Breitman, A. 2016. Tezos—A self-amending crypto-ledger. https://www.youtube.com/watch?v=3mgaDpuMSc0&t=92s. [Accessed January 2017].

Black, J. & Gregersen, H. 1997. Participative decision-making: An integration of multiple dimensions. Human Relations, 50(7): 859-878.

Bourgeois, L. 1980. Performance anc consensus. Strategic Management Journal, 1(3):227-248.

Brown, J. S, and Duguid, P. 1991. Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. Organization Science, 2: 40-57.

Brown, J. S, and Duguid, P. 2001. Knowledge and organization: A social-practice perspective. ***Organization Science***, 12: 198-213.

Btcgpu.org. 2017. BitcoinGold main page. [Accessed September 2017]

Buterin, V. 2014. DAOs, DACs, DAs and more: An incomplete terminology guide.” Ethereum Blog. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide. [Accessed February 21, 2017]

Buterin, V. 2017a. Engineering security through coordination problems. https://vitalik.ca/general/2017/05/08/coordination_problems.html. Vitalik Buterin’s Website. [Accessed December 2017]

Buterin, V. 2017b. Notes on blockchain governance. Vitalik Buterin’s Website. https://vitalik.ca/general/2017/12/17/voting.html. [Accessed April 2018]

Buterin, V. 2018. Governance, Part 2: Plutocracy is still bad. https://vitalik.ca/general/2018/03/28/plutocracy.html. Vitalik Buterin’s Website. [Accessed April 2018]

Carlile, P. R. 2002. A pragmatic view of knowledge and boundaries: Boundary objects in new product development. ***Organization Science***, 13(4), 442-455.

Chandler, A. D. 1977. The Visible Hand. Cambridge. MA: Harvard Univer.

Chandler, A. D. 1990. ***Scale and scope: The dynamics of industrial competition***. Cambridge, MA, Harvard Business School.

Chaum, D., 1983. Blind signatures for untraceable payments. In ***Advances in Cryptology***. p. 199-203. Springer, Boston, MA.

Chaum, D. 1985. Security without identification: Transaction systems to make big brother obsolete. ***Communications of the ACM***, 1985.

Cohen, B., 2016. The Rise of Alternative currencies in post-capitalism. ***Journal of Management Studies***. DOI: 10.1111/joms.12245.

Cohen, W. M., & Levinthal, D. A. 1990. Absorptive capacity- A new perspective on learning and innovation. Administrative Science Quarterly, 35(1).

CoinMarketCap. http://coinmarketcap.com. [Accessed March 2018]

Coinwarz.com. 2017. Cryptocurrency mining vs. Bitcoin mining profitability. http://www.coinwarz.com/cryptocurrency. [Accessed September 2017]

Crilly, D., Zollo, M., & Hansen, M. T. 2012. Faking it or muddling through? Understanding decoupling in response to stakeholder pressures. ***Academy of Management Journal***, 55(6): 1429-1448.

Crowston, K. 1997. A coordination theory approach to organizational process design. ***Organization Science***, 8(2): 157-175.

Daft, R. L. 2013. ***Organization Theory and Design***. Mason, OH: South-Western College Pub

Daft, R. L. & Armstrong, A. 2012. ***Organization Theory and Design***. Toronto: Nelson Education.

Daft, R. L., & Lengel, R. H. 1986. Organizational information requirements, media richness and structural design. ***Management Science***, 32(5): 554-571.

Daft, R. L., and A. Y. Lewin. 1993. Where are the theories for the ‘new’ organizational forms? An editorial essay. ***Organization Science***, 4: i–vi.

Dahlander, L., & O'Mahony, S. 2011. Progressing to the Center: Coordinating Project Work. ***Organization Science***, 22(4): 961-979.

Dai, W. B. 1998. B-Money. http://www.weidai.com/ bmoney.txt.

Davidson, S., De Filippi, P. & Potts, J. 2016a. Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. SSRN: http://ssrn.com/abstract=2811995

Davidson, S., De Filippi, P. & Potts, J. 2016b. Economics of Blockchain. SSRN: http://ssrn.com/abstract=2744751 or http://dx.doi.org/10.2139/ssrn.2744751

Davis, G. 2013. After the corporation. ***Politics & Society***, 41: 283-308.

Deetman, S. 2016. http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. Motherboard March 29. [Accessed Novemeber 28, 2016]

Deken, F., Carlile, P. R., Berends, H., & Lauche, K. 2016. Generating novelty through interdependent routines: A process model of routine work. ***Organization Science***, 27(3): 659-677.

Dess, G. G. 1987. Consensus on strategy formulation and organizational performance: Competitors in fragmented industry. ***Strategic Management Journal***, 8(3): 259-277.

Dess, G. G. & & Origer, N. K. 1987. Environment, structure, and consensus in strategy formulation : A conceptual integration. ***Academy of Management Review***, 12(2): 313-330.

Dietz, J., Xethalis, G., De Filippi, P. & Hazard, J. Model Distributed Collaborative Organizations. Stanford Working Group. [Accessed 2016].

Dodgson, M., Gann, D., Wladawsky-Berger, I., Sultan, N., & George, G. 2015. Managing digital money. ***Academy of Management Journal***, 58(2): 325-333.

Doty, D. H., Glick, W. H., & Huber, G. P. 1993. Fit, equifinality, and organizational effectiveness: Atest of two configurational theories. ***Academy of Management Journal***, 36: 1196–1250.

Economist. 2015a. "The trust machine: The promise of the blockchain". http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine [28 Aug 2016]

Economist. 2015. The great chain of being sure about things. http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. [Accessed April 2017].

Egan, M. 2016. http://money.cnn.com/2016/09/08/investing/wells-fargo-created-phony-accounts-bank-fees/. [Accessed September 11, 2016].

Eisenhardt, K. M., 1989. Building theories from case study research. ***Academy of Management review***, 14(4): 532-550.

Eisenhardt, K. M., & Graebner, M. E. 2007. Theory building from cases: Opportunities and challenges. ***Academy of Management Journal***, 50(1): 25-32.

Eisenhardt, K. M. & Schoonhoven, C. B. 1990. Organizational growth: Linking founding team, strategy, environment, and growth. ***Administrative Science Quarterly***, 35(3):504-529.

Eisenhardt, K. M. & Zbaracki, M. J. 1992. Strategic decision making. ***Strategic Management Journal***, 13(S2): 17-37.

Essex, A. & Hengartner, U., 2012. Hover: Trustworthy elections with hash-only verification. ***IEEE Security & Privacy***, 10(5):18-24.

Ethereum Community Forum. 2014. Founders and Issuance. https://forum.ethereum.org/discussion/11/founders-and-issuance

Faraj, S. and Xiao, Y. 2006. Coordination in fast-response organizations. ***Management Science***, 52(8): 1155-1169.

Faraj, S., Jarvenpaa, S. L. & Majchrzak, A. 2011. Knowledge collaboration in online communities, ***Organization Science***, 22(5): 1224-1239.

Fayol, H. 1949. ***General and Industrial Management***. London: Pitman Publishing Company.

Finney, H., 2004. RPOW-Reusable proofs of work. https://nakamotoinstitute.org/finney/rpow/index.html. [accessed June 13, 2018].

Fischer, M. J., Lynch, N. A. & Paterson, M. S. 1985. Impossibility of distributed consensus with one faulty process. ***Journal of the Association for Computing*** Machinery, 32(2): 374-382.

Fiss, P. 2007. A set-theoretic approach to organizational configurations. ***Academy of Management Review***, 32(4):1180-1296.

Fiss, P. C. 2011. Building better causal theories: a fusszy set approach to typologies in organization research. Academy of Management Journal, 54(2): 393-420.

Franco, P. 2014. ***Understanding Bitcoin: Cryptography, Engineering and Economics***. West Sussex, UK: Wiley/The Wiley Finance Series (Book 1).

Galaskiewicz, J., Bielefeld, W. & Dowell, M. 2006. Networks and organizational growth: A study of community based nonprofits. ***Administrative Science Quarterly***, 51:337-380.

Galbraith, J. R. 1973. ***Designing Complex Organizations***. Reading, Mass.: Addison-Wesley Pub. Co.

Galbraith, J. R. 1974. Organization design: An information processing view**. *Interfaces*** 4(3): 28-36.

Gandal, N. & Halaburda, H. 2016. Can we predict the winner in a market with network effects? Competition in cryptocurrency market. ***Games***. 7(16): 1-21.

Garicano, L. & Wu, Y. 2012. Knowledge, communication and organizational capabilities. ***Organization Science***, 23(5): 1382-1397.

Garud, R., Kumaraswamy, A. and Sambamurthy, V., 2006. Emergent by design: Performance and transformation at Infosys Technologies. ***Organization Science***, 17(2): 277-286.

Gersick, C. J., 1988. Time and transition in work teams: Toward a new model of group development. ***Academy of Management journal***, 31(1): 9-41.

Gilbert, C. G., 2005. Unbundling the structure of inertia: Resource versus routine rigidity. Academy of Management Journal, 48(5): 741-763.

GitHub.com. 2017. Bitcoin—Bitcoin core integration/staging tree. https://github.com/bitcoin/bitcoin. [Accessed August 2017.]

GitHub BIPs. https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki. [Accessed April 1, 2018]

Gresov, C. & R. Drazin. 1997. Equifinality: Functional equivalence in organization design. ***Academy of Management Review***, 22: 403–428.

Hinds, P. J.& Kiesler, S. 2002. ***Distributed Work***. Cambridge, MA: MIT Press.

Hoegl, M., Weinkauf, K., & Gemuenden, H. G. 2004. Interteam coordination, project commitment, and teamwork in multiteam R&D projects: A longitudinal study. ***Organization Science***, 15(1): 38-55.

Homburg, C., Krohmer, H. & Workman Jr, J. P. 1999. Strategic consensus and performance: The role of strategy type and market-related dynamism. ***Strategic Management Journal***, 20(4): 339-357.

Hsieh, Y.-Y. & Vergne, J.-P. 2017. Bitcoin and the rise of decentralized autonomous organizations. ***Journal of Organization Design***, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3082911.

Hsieh, Y.-Y., Vergne, J.-P., & Wang, S. 2017. The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In Campbell-Verduyn, M. (ed.), ***Bitcoin and Beyond: Blockchains and Global Governance.*** RIPE/Routledge Series in Global Political Economy. 48-68.

Huber, G.P. 1990. A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making. ***Academy of Management Review***, 15(1): 47- 71.

ICOtracker. 2017. Actual Crowdsales—ICO Tracker. https://icotracker.net/past. [Accessed August 2017].

Jarzabkowski, P. A., Le, J. K., & Feldman, M. S. 2012. Toward a Theory of Coordinating: Creating Coordinating Mechanisms in Practice. ***Organization Science***, 23(4): 907-927.

Jensen, M. C. & Meckling, W. H. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure**. *Journal of Financial Economics***, 3: 305–360.

Kapoor, R., and Lee, J. M. 2013. Coordinating and competing in ecosystems: How organizational forms shape new technology investments. ***Strategic Management Journal***, 34(3): 274-296.

Kellermanns, F. W., Walter, J., Lechner, C. & Floyd, S. 2005. The lack of consensus about strategic consensus Advancing theory and research. ***Journal of Management***, 31(5): 719-737.

Killeen, A. 2015. The confluence of Bitcoin and the global sharing economy. In D. K. C. Lee (Ed.). 2015. ***Handbook of Digital Currency***. Amsterdam: Elsevier. 485-503.

King, S. & Nadal, S. 2012. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf. Peercoin white paper.

Kogut, B., & Zender, U. 1992. Knowledge of the firm, combinative capabilities, and the replication of technology. ***Organization Science***: 3(3), 383-397.

Kogut, B., & Zander, U. 1993. Knowledge of the firm and the evolutionary theory of the multinational corporation. ***Journal of International Business Studies***, 24(4).

Kogut, B., & Zander, U. 1996. What firms do? Coordination, identity, and learning. ***Organization Science***, 7(5): 502-518.

Lamport, L., Shostak, R. & Pease, M. 1982. The Byzantine generals problem. ***ACM Transactions on Programming Languages and Systems***. 4 (3): 382–401.

Larson, A. 1992. Network dyads in entrepreneurial settings: A study of the governance of exchange relationships. ***Administrative Science Quarterly***, 37(1): 76-104.

Lavie, D., Stettner, U., & Tushman, M. L. 2010. Exploration and Exploitation Within and Across Organizations. ***Academy of Management Annals***, 4.

Larimer, D. 2013. Overpaying for security: The hidden costs of Bitcoin. https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security#.UjtiUt9xy0w. [Accessed April 2017].

Lawrence, P. R., & Lorsch, J. W. 1967. Differentiation and integration in complex organizations. ***Administrative Science Quarterly***, 12(1): 1-47.

Lee, D. K. C. 2015. ***Handbook of Digital Currency***. Amsterdam: Elsevier.

Lee, G. K. & Cole, R. E. 2003. From a firm-based to a community-based model of knowledge creation: The case of the Linux kernel development. ***Organization Science***, 14: 633–649.

Lee, M. Y. & Edmondson, A. C. 2017. Self-managing organizations: Exploring the limits of less-hierarchical organizing. ***Research in Organizational Behavior***, 37: 35-58.

Lessig, L. 2006. ***Code: Version 2.0***. New York: Basic Books.

Leonardos, N., Kiayias, A. and Garay, J. A. 2014. The Bitcoin Backbone Protocol: Analysis and Applications.

Lewin, A. Y., & Minton, J. W. 1986. Determining organizational effectiveness- Another look, and an agenda for research. ***Management Science***, 32(5): 514-538.

Lopp, J. 2016. Bitcoin: The trust anchor in a sea of blockchains. http://www.coindesk.com/bitcoin-the-trust-anchor-in-a-sea-of-blockchains/ [25 July 2016]

Malnight, T. W. 2001. Emerging structural patterns within multinational corporations: Toward process-based structures. ***Academy of Management Journal***, 44(6): 1187-1210.

March, J. G. & Simon, H. A. 1958. ***Organizations***. New York: Wiley.

March, J. G. 1991. Exploration and exploitation in organizational learning. ***Organization Science***, 2(1).

Mark, G. 2002. Extreme collaboration. ***Communications of the ACM***, 45: 89–93.

Meyer, A. D., Tsui, A. S., & Hinings, C. R. 1993. Configurational approaches to organizational analysis. ***Academy of Management Journal***, 36: 1175–1195.

Miles, R. E. & Snow, C. C. 1978. ***Organizational Strategy, Structure, and Process***. New York: McGraw-Hill.

Miller, D., Greenwood, R. and Prakash, R. 2009. What happened to organization theory?. ***Journal of Management Inquiry,*** 18(4): 273-279.

Mintzberg, H. 1979. ***The Structuring of Organizations: A Synthesis of the Research***. Englewood Cliffs, NJ: Prentice Hall.

Mohrman, S. A. 1993. Integrating roles and structure in the lateral organization. In ***Organizing for the Future: The New Logic for Managing Complex Organizations***, 109-141. San Francisco: Jossey-Bass.

Nakamoto S. 2008. Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. 2016. ***Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.*** New Jersey, USA: Princeton University Press.

Nian, L. P. & Lee, D. K. C. 2015. Introduction to Bitcoin. In Lee, D.K.C. (Ed.), 2015. ***Handbook of Digital Currency***. Amsterdam: Elsevier. 6-29.

Okhuysen, G. A. 2005. Understanding group behavior: How a police SWAT team creates, changes, and manages group routines. In Elsbach, K. D. (Ed.), ***Qualitative Organizational Research***. Charlotte, NC: Information Agency Publishing. 139-168.

Okhuysen, G. A., & Bechky, B. A. 2009. Coordination in Organizations: An Integrative Perspective. ***Academy of Management Annals***, 3: 463-502.

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

O'Mahony, S., & Bechky, B. A. 2008. Boundary Organizations: Enabling Collaboration among Unexpected Allies. Administrative Science Quarterly, 53(3): 422-459.

O'Mahony, S., & Ferraro, F. 2007. The emergence of governance in an open source community. ***Academy of Management Journal***, 50(5): 1079-1106.

O'Mahony & Lakhani, 2011. Organizations in the shadow of communities. In ***Communities and Organizations***, pp.3-36. Emerald Group Publishing Limited.

O'Mahony, S. 2003. Guarding the commons: How community managed software projects protect their work. ***Research Policy***, 32(7): 1179-1198.

Ong, B., Lee, T. M., Li, G. & Lee, D. K. C. 2015. Evaluating the potential of alternative cryptocurrencies. In Lee, D. K. C. (Ed.), 2015. ***Handbook of Digital Currency***, Elsevier, Amsterdam.

Orlikowski, W. J. 2002. Knowing in practice: Enacting a collective capability in distributed organizing. ***Organization Science***, 13: 249–273.

Parmigiani, A., & Howard-Grenville, J. 2011. Routines revisited: exploring the capabilities and practice perspectives. ***Academy of Management Annals***, 5(1): 413-453.

Perrow, C. 2002. ***Organizing America***. Princeton: Princeton University Press.

Priem, R. L. 1990. Top management team group factors, consensus, and firm performance***. Strategic Management Journal***, 11(6): 469-478.

Puranam, P. 2017. An introduction to the micro-structural approach to organization design. Chapter 1 In Puranam, P. 2018 (Forthcoming). ***The Microstructure of Organizations***, Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2495909.

Puranam, P., Alexy, O., & Reitzig, M. 2014. What's new about new forms of organizing? ***Academy of Management Review***, 39(2): 162-180.

Puranam, P., & Jacobides, M. G. 2006. The dynamics of coordination regimes: Implications for organizational design. London Business School discussion paper (April).

Puranam, P. & Raveendran, M., 2012. Interdependence and organization design. ***Handbook of Economic Organization***, A. Grandori, ed., Edward Elgar, 2012

Puranam, P., Raveendran, M., & Knudsen, T. 2012. Organization design: The epistemic interdependence perspective. ***Academy of Management Review***, 37(3): 419-440.

Puranam, P., Singh, H. and Zollo, M. 2006. Organizing for innovation: Managing the coordination-autonomy dilemma in technology acquisitions. ***Academy of Management Journal***. 49(2): 263-280.

Ragin C. C. & Fiss, P. 2008. Net effects versus configurations: An empirical denmonstration. In CC. Ragin (Ed.), 2008 ***Redesigning Social Inquiry: Fuzzy Sets and Beyond***. University of Chicago Press: Chicago.

Ragin C. C. 2008. ***Redesigning Social Inquiry : Fuzzy Sets and Beyond***. University of Chicago Press: Chicago.

Ragin, C. & Davey. S. 2014. fs/QCA [Computer Programme], Version [2.5/3.0]. Irvine, CA: University of California.

Rindova, V. P., & Kotha, S. 2001. Continuous “morphing”: Competing through dynamic capabilities, form, and function. ***Academy of Management Journal***, 44(6): 1263-1280.

Rivkin, J. W., & Siggelkow, N. 2003. Balancing search and stability: Interdependencies among elements of organizational design. ***Management Science***, 49(3): 290-311.

Rothschild, J. & Whitt, J. A. 1968. ***The Cooperative Workplace: Potentials and Dilemmas of Organizational Democracy and Participation***. New York: Cambridge University Press.

Salomon, R. & Martin, X. 2008, Learning, knowledge transfer, and technology implementation performance: A study of time-to-build in the global semiconductor industry. ***Management Science***, 54(7): 1266-1280.

Schilling, M. A., & Steensma, H. K. 2001. The use of modular organizational forms: An industry-level analysis. ***Academy of Management Journal***, 44(6): 1149-1168.

Schneider C. Q., Wagemann C. 2012. ***Set-Theoretic methods for the social sciences: A guide to qualitative comparative analysis***. Cambridge University Press: New York.

Shah, S. 2006. Motivation, governance, and the viablity of hybrid forms in open source software development. ***Management Science***. 52(7):1000-1014.

Siggelkow, N. 2007. Persuasion with case studies. ***Academy of Management Journal***, 50(1): 20-24.

Srikanth, K., & Puranam, P. 2014. The Firm as a Coordination System: Evidence from Software Services Offshoring. ***Organization Science***, 25(4): 1253-1271.

Stan, M., & Puranam, P. 2016. Organizational adaptation to interdependence shifts: The role of integrator structures. ***Strategic Management Journal***. 38: 1041–1061.

St. John, C. H. & Rue, L. W. Coordinating mechanisms, consensus between marketing and manufacturing groups, and marketplace performance. ***Strategic Management Journal***, 12(7): 549-555.

Swanson, T. 2014. The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin. Creative Commons.

Swanson, T. 2015. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. R3.

Schweiger, D. M., Sandberg, W. R. & Ragan, J. W. 1986. Group approaches for improving strategic decision making: A comparative analysis of dialectical inquiry, devil's advocacy, and consensus. ***Academy of Management Journal***, 29(1): 51-71.

Taylor, F. W. 1911. ***The Principles of Scientific Management***. New York, London: Harper & Brothers.

Thompson, J. D. 1967. ***Organizations In Action: Social Science Bases of Administrative Theory***. New York: McGraw-Hill.

Tushman, M. L., & Nadler, D. A. 1978. Information processing as an integrating concept in organizational design. ***Academy of Management Review***, 3(3): 613-624.

Tschorsch, F. & Scheuermann, B. 2016. Bitcoin and beyond: A technical survey on decentralized digital currencies. ***IEEE Communications Surveys & Tutorials***, 18(3): 2084-2123.

Torpey, K. 2015. https://bitcoinmagazine.com/articles/bitcoin-doesn-t-waste-electricity-it-s-used-for-security-1446482572. [Accessed November 28, 2016]

Vaast, E., and Levina, N. 2006. Multiple faces of codification: Organizational redesign in an IT organization. ***Organization Science***. 17(2): 190-201.

VanderMey, A. 2017. IPOs Are Dwindling, So Is the Number of Public Companies. fortune.com. http://fortune.com/2017/01/20/public-companies-ipo-financial-markets

Van Valkenburgh, P., Dietz, J., de Filippi, P., Shadab, H., Xethalis, G. & Bollier, D. 2015. Distributed collaborative organisations: Distributed networks and regulatory frameworks. Harvard Working Paper.

Vergne, J. P. & Depeyre, C. 2016. How do firms adapt? A fuzzy-set analysis of the role of cognition and capabilities in U.S. defense firms' responses to 9/11. ***Academy of Management Journal***, 59(5): 1653-1680.

Vigna, P. & Casey, M. J. 2015. ***The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order***. St. Martin's Press.

Von Hippel, E., & von Krogh, G. 2003. Open source software and the "private-collective" innovation model: Issues for organization science. ***Organization Science***, 14(2): 209-223.

Von Krogh, G. & Von Hippel, E. 2006. The promise of research on open source software. ***Management Science***, 52(7): 975-983.

Wadhwa V. 2015. 2015 was a tipping point for six technologies that will change the world. https://www.washingtonpost.com/news/innovations/wp/2015/12/28/2015-was-a-tipping-point-for-six-technologies-which-will-change-the-world/. The Washington Post.

Wang, S. & Vergne, J.-P. 2017. Buzz factor or innovation potential: What explains cryptocurrencies' returns? PLoS One, 12. http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0169556

Weick, K. E. 1995. ***Sensemaking In Organizations***. Thousand Oaks, London: Sage Publications.

Weinzimmer, L. G., Nystrom, P. C. & Freeman, S. J. 1998. Measuring organizational growth: Issues, consequences and guidelines. ***Journal of Management***, 24(2): 235-262.

West, J. & O'Mahony, S. 2008. The role of participation architecture in growing sponsored open source communities. ***Industry And Innovation***, 15(2): 145-168.

Wheelwright, S. C. & Clark, K. B. 1992. Organizing and leading 'heavyweight' development teams. ***California Management Review***, 34: 9–28.

Whetten, D. A. 1987. Organizational growth and decline processes. ***Annual Review of Sociology***, 13(1): 335-358.

Williamson, O. E. 1975. ***Markets and Hierarchies, Analysis and Antitrust Implications : A Study in the Economics of Internal Organization***. New York: Free Press.

Wood, G. & Buchanan, A. 2015. Advancing egalitarianism. In Lee, D. K. C. (ed.), ***Handbook of Digital Currency***. San Diego, CA: Academic Press. 385-402.

Wooldridge, B. & Floyd, S. W. 1989. Strategic process effects on consensus. ***Strategic Management Journal***, 10(3): 295:302.

Wright, A. and De Filippi, P. 2015. Decentralized blockchain technology and the rise of Lex Cryptographia. SSRN: http://ssrn.com/abstract=2580664

Yermack, D. 2017. Corporate governance and blockchains. ***Review of Finance***, 21: 7-31.

Young-Hyman, T. 2017. Cooperating without Co-laboring: How Formal Organizational Power Moderates Cross-functional Interaction in Project Teams. ***Administrative Science Quarterly***, 62: 179-214.

Zammuto, R. F., Griffith, T. L., Majchrzak, A., Dougherty, D. J. & Faraj, S. 2007. Information technology and the changing fabric of organization. ***Organization Science***, 18(5): 749-762.

Zucker, L. G. 1986. Production of trust: Institutional sources of economic structure, 1840–1920.” In B. M. Staw and L. L. Cummings (eds.), ***Research in Organizational Behavior***.

Zurrer, R. 2017. Keeper: Workers that maintain blockchain networks. Keynote speech at the First Annual Toronto FinTech Conference, Scotiabank Digital Banking Lat at Ivey Business School.

Appendices

Appendix A The Byzantine Generals Problem

The Byzantine Generals Problem refers to the problem of reaching synchronous consensus in a distributed network with the presence of dishonest actors. The name originates from the hypothetical situation under which a group of generals in the Byzantine army surround an enemy city. The Byzantine generals first need to agree on a common battle plan of action, for instance, whether to attack or to retreat—at the same time (Lamport et al., 1982). A half-hearted attack leads to coordination failure, which results in a defeat. Second, the generals can only communicate via messengers, and third, one or more of the generals may be traitors and may mislead others.

As traitors may decide to go against the group decision or deliver misinformation such that loyal generals cannot arrive at a unified plan, the goal of the Byzantine Generals Problem is to find a solution for all the loyal generals to arrive at a plan while neutralizing the possibility of the traitorous generals causing coordination failures (i.e., the adoption a bad plan) (Narayanan et al., 2015). It has been proved that this goal is impossible to achieve if over one-third of the generals are traitors (Lamport et al., 1982; Narayanan et al., 2015).

Fischer and colleagues (1985) further extend the analysis to asynchronous systems in which nodes behave deterministically. They show that consensus is impossible with even only a single faulty process. “The problem is for all the data manager processes that have participated in the processing of a particular transaction to agree on whether to install the transaction’s results in the database or to discard them” (Fischer, Lynch & Paterson, 1985), hence the presence of the “transaction commit problem”. In this commit problem, “all data managers must make the same decision in order to preserve the consistency of the database” in a distributed system where data is being exchanged and processed. The solution is only possible if and only if *all* network actors are completely honest and reliable, which is impossible to achieve.

Bitcoin combines public key cryptography, digital signatures, and proof of work and, for the first time and solved the impossibility theorem proposed by Fischer and colleague. Bitcoin solves the Byzantine Generals Problem by providing the “generals” (i.e., network validators) with economic incentives through block reward. It also imposes costs as disincentives for being dishonest through proof of work and by compromising on consensus timing (i.e., the 10-minute block time on average). This explains why Bitcoin and the underlying blockchain technology represent such a significant technological break-through.

Appendix B: Semi-Structured Interview Guide

** Each interview begins with a brief introduction of myself, the research project, and the objective of the interview. The open-ended structure permits conversations to develop and allows me to follow up on ideas the participants wish to elaborate on.

1. Please describe your background and how you got into Bitcoin.

2. Please describe your role, your involvement and experience working on Bitcoin.

3. How are BIPs (or similar proposals) different from (or similar to) existing open-source software development projects in terms of their code modification processes?

4. What determines the success/failure of a BIP?

5. Who determines how much consensus is enough consensus?

6. What does “lack of consensus” mean in the cryptocurrency context?

7. What are miners’ role in activating BIPs?

8. How does coordination between developers and miners happen?

9. What are the biggest challenges for BIPs (or similar proposals) moving forward?

Appendix C Types and Roles of Nodes

As shown in Figure 14, a Bitcoin node is a combination of four functions: wallet services (W), mining (M), full blockchain database (B), and network routing (N) (Antonopoulos, 2014: 140). Where this research focuses on mining (M), wallet services (W) refer to the software that keeps users' Bitcoin addresses and private keys. Wallet services allow users to send, receive, and store bitcoins (Antonopoulos, 2014). The blockchain database (B) function refers to the maintenance of a full copy of the entire Bitcoin transaction history on the blockchain public ledger. The network routing (N) function is required for all nodes to communicate with one another and to participate in the network. All nodes have this routing function (Antonopoulos, 2014).

Figure 14 The four functions of a Bitcoin network node: Wallet, Miner, full blockchain database, and network routing

(Adopted from Figure 6-1, Antonopoulos, 2014: 140)

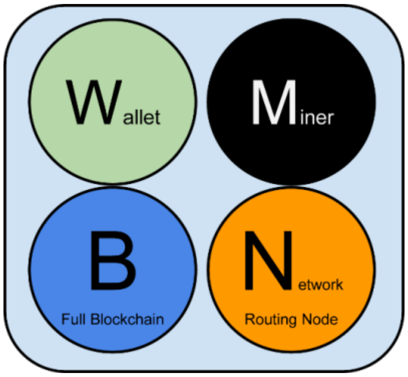


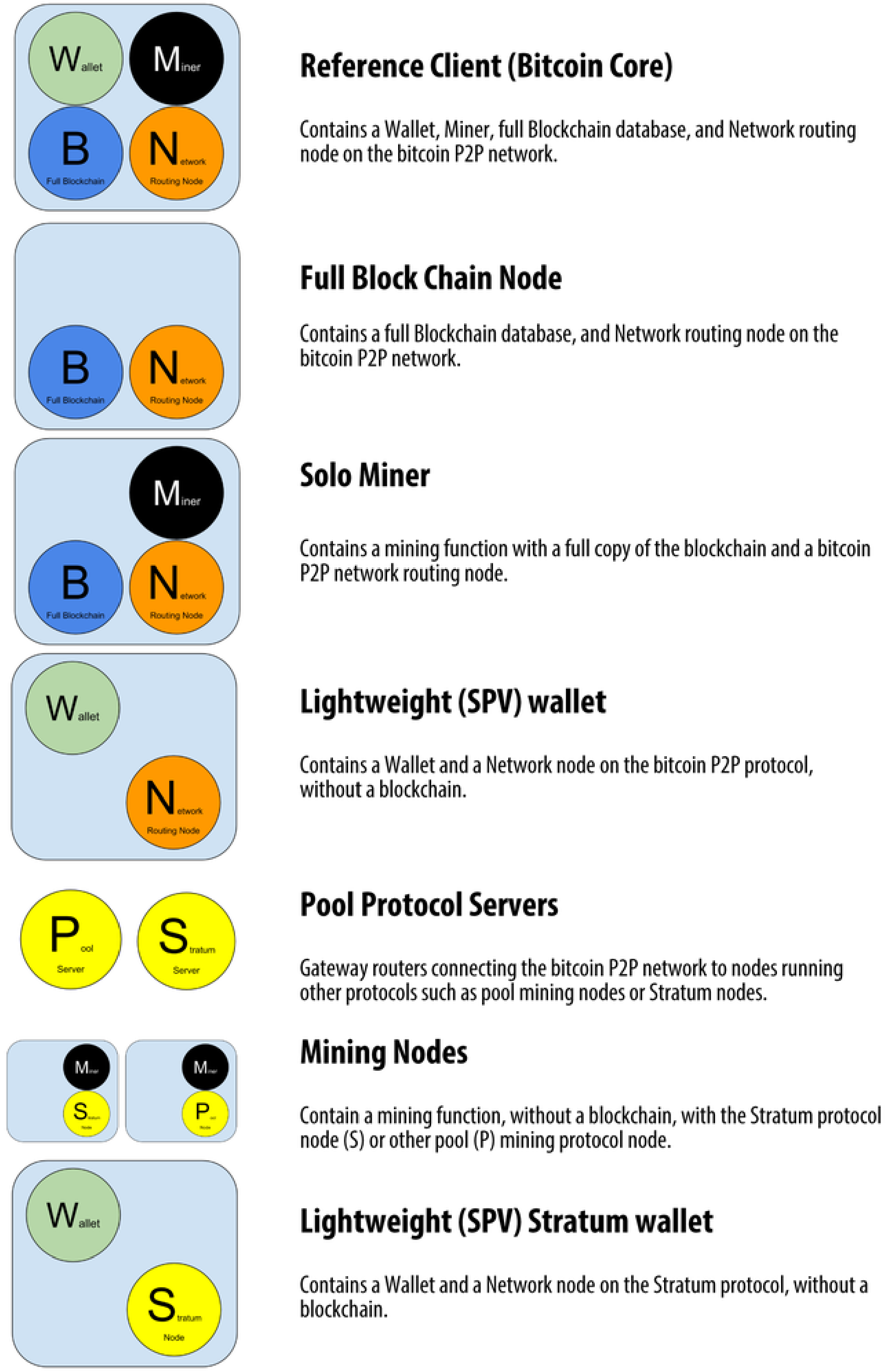
Figure 15 lists various types of nodes with different combinations of these functions. Please note that pool protocol servers such as "Stratum" (S) or "Pool" (P) are additional routing services that connect lightweight mining pools to the main Bitcoin peer-to-peer network. They do not belong to the immediate Bitcoin peer-to-peer network, but to the extended network, which is not considered internal to the organization. A lightweight client (or simplified payment verification (SPV) client) does not have to store a copy of the full blockchain history. Instead, it tracks only the user's wallet, and is not responsible for transaction validation. It relies on a third party (e.g., Stratum) or peers to obtain partial information of the blockchain and interact with the Bitcoin network (Antonopoulos, 2014).

Individual miners can join mining pools to pool their hash power and increase their chance of winning. Miners participating in such pools may get a share of the reward. Mining pool participants interact indirectly with the Bitcoin network through a third party via the mining protocol (Antonopoulos, 2014).

Figure 16 illustrates the Bitcoin network. For the purposes of this study, organizational boundaries are defined to include only those nodes connected by the Bitcoin protocol (orange ties).

Figure 15 Types of Nodes on the extended Bitcoin Network

(Adopted from Figure 6-2, Antonopoulos, 2014: 142)



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

Mining Nodes

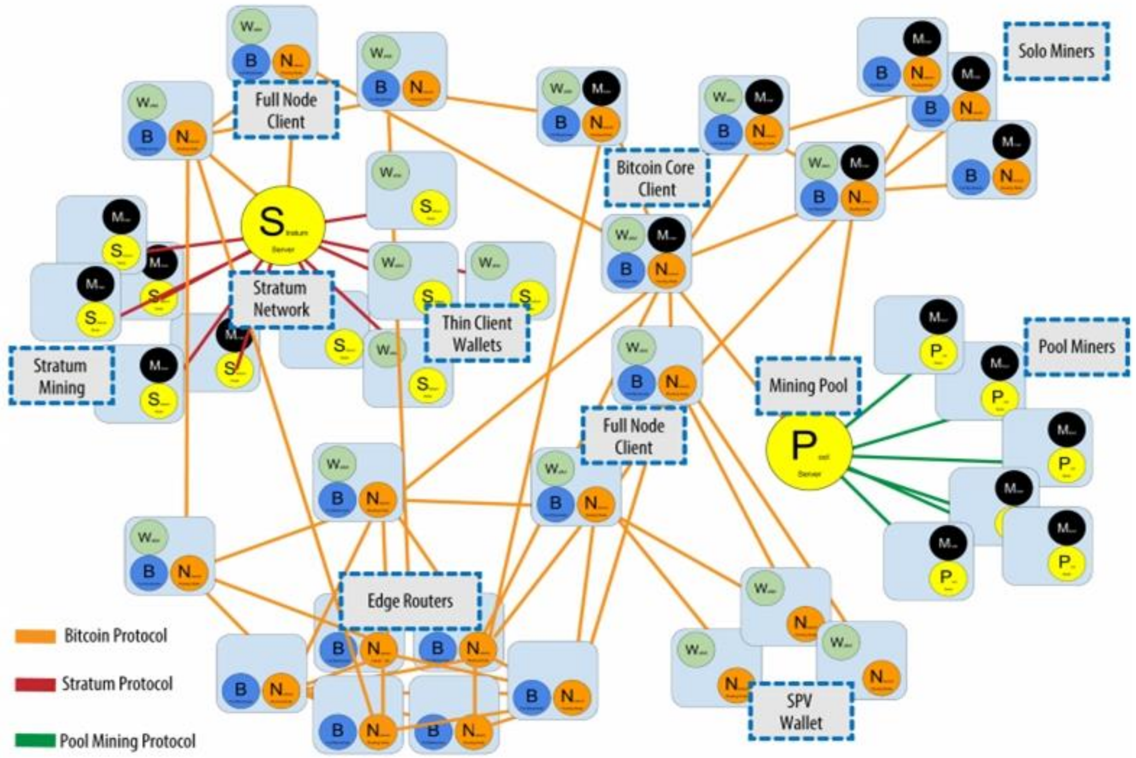
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.

Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

Figure 16 The extended Bitcoin Network

(Adopted from Figure 6-3, Antonopoulos, 2014: 143)



Appendix D List of All BIPs

#	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Replaced
2		BIP process, revised	Luke Dashjr	Process	Active
8		Version bits with lock-in by height	Shaolin Fry	Informational	Draft
9		Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Final
10	Applications	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	Applications	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	Consensus (soft fork)	OP_EVAL	Gavin Andresen	Standard	Withdrawn
13	Applications	Address Format for pay-to-script-hash	Gavin Andresen	Standard	Final
14	Peer Services	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Standard	Final
15	Applications	Aliases	Amir Taaki	Standard	Deferred
16	Consensus (soft fork)	Pay to Script Hash	Gavin Andresen	Standard	Final
17	Consensus (soft fork)	OP_CHECKHASHVERIFY (CHV)	Luke Dashjr	Standard	Withdrawn
18	Consensus (soft fork)	hashScriptCheck	Luke Dashjr	Standard	Proposed

19	Applications	M-of-N Standard Transactions (Low SigOp)	Luke Dashjr	Standard	Draft
20	Applications	URI Scheme	Luke Dashjr	Standard	Replaced
21	Applications	URI Scheme	Nils Schneider, Matt Corallo	Standard	Final
22	API/RPC	getblocktemplate - Fundamentals	Luke Dashjr	Standard	Final
23	API/RPC	getblocktemplate - Pooled Mining	Luke Dashjr	Standard	Final
30	Consensus (soft fork)	Duplicate transactions	Pieter Wuille	Standard	Final
31	Peer Services	Pong message	Mike Hearn	Standard	Final
32	Applications	Hierarchical Deterministic Wallets	Pieter Wuille	Informational	Final
33	Peer Services	Stratized Nodes	Amir Taaki	Standard	Draft
34	Consensus (soft fork)	Block v2, Height in Coinbase	Gavin Andresen	Standard	Final
35	Peer Services	mempool message	Jeff Garzik	Standard	Final
36	Peer Services	Custom Services	Stefan Thomas	Standard	Draft
37	Peer Services	Connection Bloom filtering	Mike Hearn, Matt Corallo	Standard	Final
38	Applications	Passphrase-protected private key	Mike Caldwell, Aaron Voisine	Standard	Draft
39	Applications	Mnemonic code for generating deterministic keys	Marek Palatinus, Pavol Rusnak,	Standard	Proposed

			Aaron Voisine, Sean Bowe		
40	API/RPC	Stratum wire protocol	Marek Palatinus	Standard	BIP number allocated
41	API/RPC	Stratum mining protocol	Marek Palatinus	Standard	BIP number allocated
42	Consensus (soft fork)	A finite monetary supply for Bitcoin	Pieter Wuille	Standard	Draft
43	Applications	Purpose Field for Deterministic Wallets	Marek Palatinus, Pavol Rusnak	Informational	Draft
44	Applications	Multi-Account Hierarchy for Deterministic Wallets	Marek Palatinus, Pavol Rusnak	Standard	Proposed
45	Applications	Structure for Deterministic P2SH Multisignature Wallets	Manuel Araoz, Ryan X. Charles, Matias Alejo Garcia	Standard	Proposed
47	Applications	Reusable Payment Codes for Hierarchical Deterministic Wallets	Justus Ranvier	Informational	Draft
49	Applications	Derivation scheme for P2WPKH-nested-in-P2SH based accounts	Daniel Weigl	Informational	Draft
50		March 2013 Chain Fork Post-Mortem	Gavin Andresen	Informational	Final
60	Peer Services	Fixed Length "version" Message (Relay-Transactions Field)	Amir Taaki	Standard	Draft

61	Peer Services	Reject P2P message	Gavin Andresen	Standard	Final
62	Consensus (soft fork)	Dealing with malleability	Pieter Wuille	Standard	Withdrawn
63	Applications	Stealth Addresses	Peter Todd	Standard	BIP number allocated
64	Peer Services	getutxo message	Mike Hearn	Standard	Draft
65	Consensus (soft fork)	OP_CHECKLOCKTIME VERIFY	Peter Todd	Standard	Final
66	Consensus (soft fork)	Strict DER signatures	Pieter Wuille	Standard	Final
67	Applications	Deterministic Pay-to-script-hash multi-signature addresses through public key sorting	Thomas Kerin, Jean-Pierre Rupp, Ruben de Vries	Standard	Proposed
68	Consensus (soft fork)	Relative lock-time using consensus-enforced sequence numbers	Mark Friedenbach, BtcDrak, Nicolas Dorier, kinoshitajona	Standard	Final
69	Applications	Lexicographical Indexing of Transaction Inputs and Outputs	Kristov Atlas	Informational	Proposed
70	Applications	Payment Protocol	Gavin Andresen, Mike Hearn	Standard	Final
71	Applications	Payment Protocol MIME types	Gavin Andresen	Standard	Final

72	Applications	bitcoin: uri extensions for Payment Protocol	Gavin Andresen	Standard	Final
73	Applications	Use "Accept" header for response type negotiation with Payment Request URLs	Stephen Pair	Standard	Final
74	Applications	Allow zero value OP_RETURN in Payment Protocol	Toby Padilla	Standard	Draft
75	Applications	Out of Band Address Exchange using Payment Protocol Encryption	Justin Newton, Matt David, Aaron Voisine, James MacWhyte	Standard	Draft
80		Hierarchy for Non-Colored Voting Pool Deterministic Multisig Wallets	Justus Ranvier, Jimmy Song	Informational	Deferred
81		Hierarchy for Colored Voting Pool Deterministic Multisig Wallets	Justus Ranvier, Jimmy Song	Informational	Deferred
83	Applications	Dynamic Hierarchical Deterministic Key Trees	Eric Lombrozo	Standard	Draft
84	Applications	Derivation scheme for P2WPKH based accounts	Pavol Rusnak	Informational	Draft
90	Consensus (hard fork)	Buried Deployments	Suhas Daftuar	Informational	Draft
91	Consensus (soft fork)	Reduced threshold Segwit MASF	James Hilliard	Standard	Final

98	Consensus (soft fork)	Fast Merkle Trees	Mark Friedenbach, Kalle Alm, BtcDrak	Standard	Draft
99		Motivation and deployment of consensus rule changes ([soft/hard]forks)	Jorge Timón	Informational	Draft
101	Consensus (hard fork)	Increase maximum block size	Gavin Andresen	Standard	Withdrawn
102	Consensus (hard fork)	Block size increase to 2MB	Jeff Garzik	Standard	Draft
103	Consensus (hard fork)	Block size following technological growth	Pieter Wuille	Standard	Draft
104	Consensus (hard fork)	'Block75' - Max block size like difficulty	t.khan	Standard	Draft
105	Consensus (hard fork)	Consensus based block size retargeting algorithm	BtcDrak	Standard	Draft
106	Consensus (hard fork)	Dynamically Controlled Bitcoin Block Size Max Cap	Upal Chakraborty	Standard	Draft
107	Consensus (hard fork)	Dynamic limit on the block size	Washington Y. Sanchez	Standard	Draft
109	Consensus (hard fork)	Two million byte size limit with sigop and sighash limits	Gavin Andresen	Standard	Rejected
111	Peer Services	NODE_BLOOM service bit	Matt Corallo, Peter Todd	Standard	Proposed

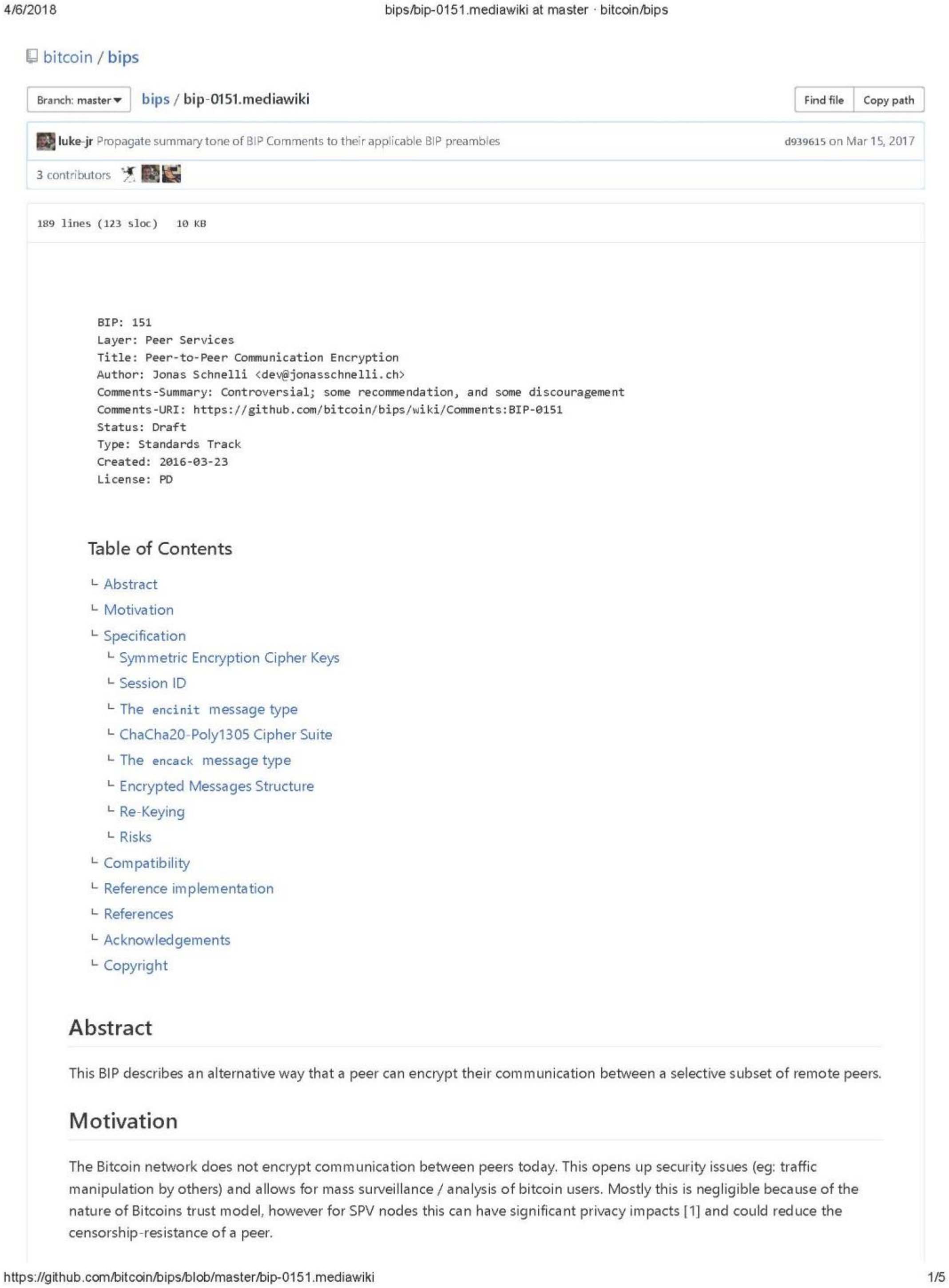
112	Consensus (soft fork)	CHECKSEQUENCEVERIFY	BtcDrak, Mark Friedenbach, Eric Lombrozo	Standard	Final
113	Consensus (soft fork)	Median time-past as endpoint for lock-time calculations	Thomas Kerin, Mark Friedenbach	Standard	Final
114	Consensus (soft fork)	Merkelized Abstract Syntax Tree	Johnson Lau	Standard	Draft
115	Consensus (soft fork)	Generic anti-replay protection using Script	Luke Dashjr	Standard	Draft
116	Consensus (soft fork)	MERKLEBRANCHVERIFY	Mark Friedenbach, Kalle Alm, BtcDrak	Standard	Draft
117	Consensus (soft fork)	Tail Call Execution Semantics	Mark Friedenbach, Kalle Alm, BtcDrak	Standard	Draft
120	Applications	Proof of Payment	Kalle Rosenbaum	Standard	Withdrawn
121	Applications	Proof of Payment URI scheme	Kalle Rosenbaum	Standard	Withdrawn
122	Applications	URI scheme for Blockchain references / exploration	Marco Pontello	Standard	Draft
123		BIP Classification	Eric Lombrozo	Process	Active
124	Applications	Hierarchical Deterministic Script Templates	Eric Lombrozo, William Swanson	Informational	Draft

125	Applications	Opt-in Full Replace-by-Fee Signaling	David A. Harding, Peter Todd	Standard	Proposed
126		Best Practices for Heterogeneous Input Script Transactions	Kristov Atlas	Informational	Draft
130	Peer Services	sendheaders message	Suhas Daftuar	Standard	Proposed
131	Consensus (hard fork)	"Coalescing Transaction" Specification (wildcard inputs)	Chris Priest	Standard	Draft
132		Committee-based BIP Acceptance Process	Andy Chase	Process	Withdrawn
133	Peer Services	feefilter message	Alex Morcos	Standard	Draft
134	Consensus (hard fork)	Flexible Transactions	Tom Zander	Standard	Draft
135		Generalized version bits voting	Sancho Panza	Informational	Draft
140	Consensus (soft fork)	Normalized TXID	Christian Decker	Standard	Draft
141	Consensus (soft fork)	Segregated Witness (Consensus layer)	Eric Lombrozo, Johnson Lau, Pieter Wuille	Standard	Final
142	Applications	Address Format for Segregated Witness	Johnson Lau	Standard	Withdrawn
143	Consensus (soft fork)	Transaction Signature Verification for Version 0 Witness Program	Johnson Lau, Pieter Wuille	Standard	Final
144	Peer Services	Segregated Witness (Peer Services)	Eric Lombrozo, Pieter Wuille	Standard	Final

145	API/RPC	getblocktemplate Updates for Segregated Witness	Luke Dashjr	Standard	Final
146	Consensus (soft fork)	Dealing with signature encoding malleability	Johnson Lau, Pieter Wuille	Standard	Draft
147	Consensus (soft fork)	Dealing with dummy stack element malleability	Johnson Lau	Standard	Final
148	Consensus (soft fork)	Mandatory activation of segwit deployment	Shaolin Fry	Standard	Final
149	Consensus (soft fork)	Segregated Witness (second deployment)	Shaolin Fry	Standard	Withdrawn
150	Peer Services	Peer Authentication	Jonas Schnelli	Standard	Draft
151	Peer Services	Peer-to-Peer Communication Encryption	Jonas Schnelli	Standard	Draft
152	Peer Services	Compact Block Relay	Matt Corallo	Standard	Draft
154	Peer Services	Rate Limiting via peer specified challenges	Karl-Johan Alm	Standard	Draft
157	Peer Services	Client Side Block Filtering	Olaoluwa Osuntokun, Alex Akselrod, Jim Posen	Standard	Draft
158	Peer Services	Compact Block Filters for Light Clients	Olaoluwa Osuntokun, Alex Akselrod	Standard	Draft
159	Peer Services	NODE_NETWORK_LIMITED service bit	Jonas Schnelli	Standard	Draft
171	Applications	Currency/exchange rate information API	Luke Dashjr	Standard	Draft

173	Applications	Base32 address format for native v0-16 witness outputs	Pieter Wuille, Greg Maxwell	Informational	Proposed
174	Applications	Partially Signed Bitcoin Transaction Format	Andrew Chow	Standard	Draft
175	Applications	Pay to Contract Protocol	Omar Shibli, Nicholas Gregory	Informational	Draft
176		Bits Denomination	Jimmy Song	Informational	Draft
180	Peer Services	Block size/weight fraud proof	Luke Dashjr	Standard	Draft
199	Applications	Hashed Time-Locked Contract transactions	Sean Bowe, Daira Hopwood	Standard	Draft

Appendix E A Sample BIP (BIP #151)



4/6/2018 bips/bip-0151.mediawiki at master · bitcoin/bips

luke-jr Propagate summary tone of BIP Comments to their applicable BIP preambles d939615 on Mar 15, 2017

3 contributors

189 lines (123 sloc) 10 KB

```
BIP: 151
Layer: Peer Services
Title: Peer-to-Peer Communication Encryption
Author: Jonas Schnelli <dev@jonasschnelli.ch>
Comments-Summary: Controversial; some recommendation, and some discouragement
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0151
Status: Draft
Type: Standards Track
Created: 2016-03-23
License: PD
```

Table of Contents

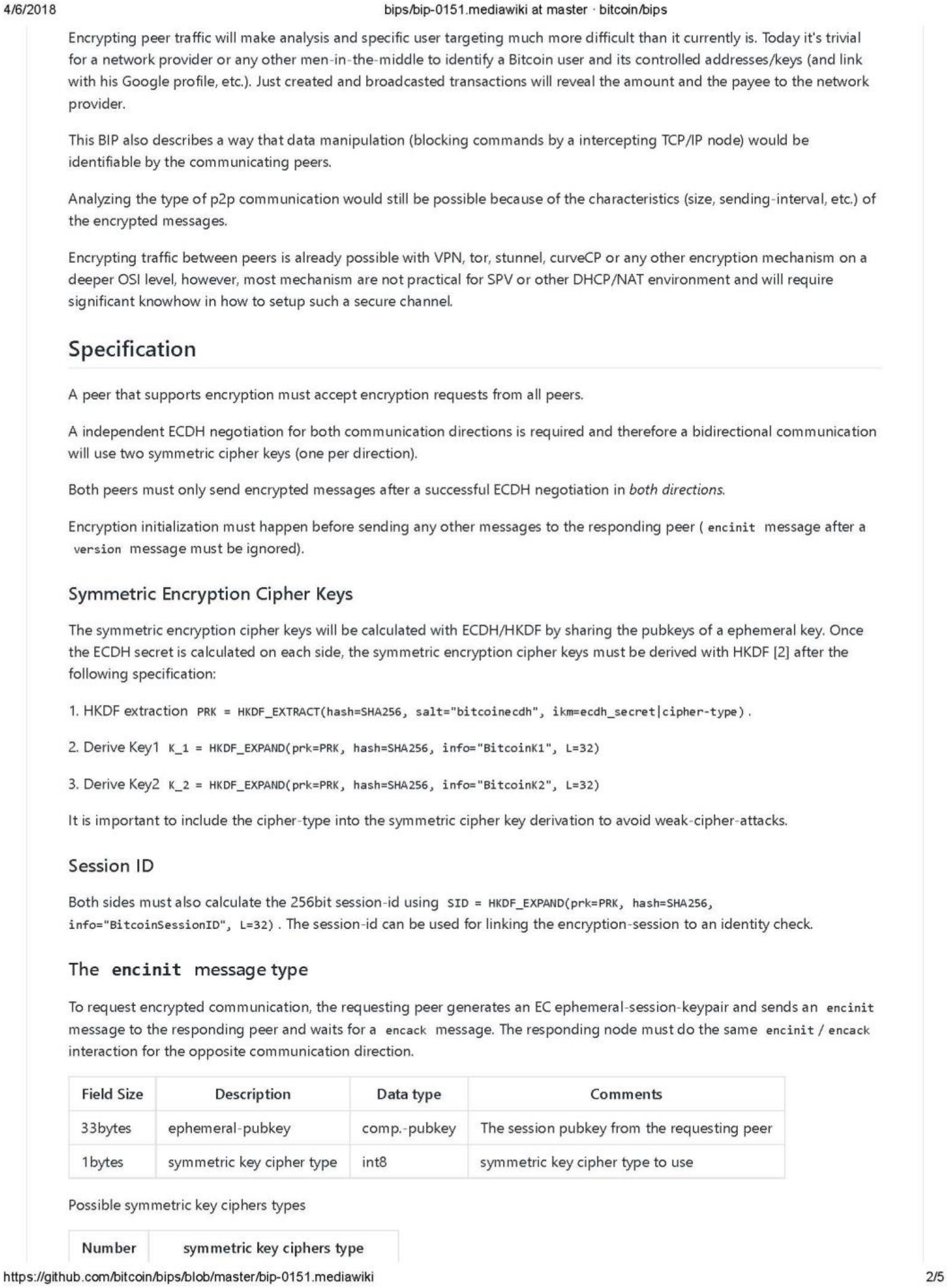
Abstract

This BIP describes an alternative way that a peer can encrypt their communication between a selective subset of remote peers.

Motivation

The Bitcoin network does not encrypt communication between peers today. This opens up security issues (eg: traffic manipulation by others) and allows for mass surveillance / analysis of bitcoin users. Mostly this is negligible because of the nature of Bitcoins trust model, however for SPV nodes this can have significant privacy impacts [1] and could reduce the censorship-resistance of a peer.

https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki 1/5



Encrypting peer traffic will make analysis and specific user targeting much more difficult than it currently is. Today it's trivial for a network provider or any other men-in-the-middle to identify a Bitcoin user and its controlled addresses/keys (and link with his Google profile, etc.). Just created and broadcasted transactions will reveal the amount and the payee to the network provider.

This BIP also describes a way that data manipulation (blocking commands by a intercepting TCP/IP node) would be identifiable by the communicating peers.

Analyzing the type of p2p communication would still be possible because of the characteristics (size, sending-interval, etc.) of the encrypted messages.

Encrypting traffic between peers is already possible with VPN, tor, stunnel, curveCP or any other encryption mechanism on a deeper OSI level, however, most mechanism are not practical for SPV or other DHCP/NAT environment and will require significant knowhow in how to setup such a secure channel.

Specification

A peer that supports encryption must accept encryption requests from all peers.

A independent ECDH negotiation for both communication directions is required and therefore a bidirectional communication will use two symmetric cipher keys (one per direction).

Both peers must only send encrypted messages after a successful ECDH negotiation in *both directions*.

Encryption initialization must happen before sending any other messages to the responding peer (`encinit` message after a `version` message must be ignored).

Symmetric Encryption Cipher Keys

The symmetric encryption cipher keys will be calculated with ECDH/HKDF by sharing the pubkeys of a ephemeral key. Once the ECDH secret is calculated on each side, the symmetric encryption cipher keys must be derived with HKDF [2] after the following specification:

1. HKDF extraction `PRK = HKDF_EXTRACT(hash=SHA256, salt="bitcoinecdh", ikm=ecdh_secret|cipher-type)` .

2. Derive Key1 `K_1 = HKDF_EXPAND(prk=PRK, hash=SHA256, info="BitcoinK1", L=32)`

3. Derive Key2 `K_2 = HKDF_EXPAND(prk=PRK, hash=SHA256, info="BitcoinK2", L=32)`

It is important to include the cipher-type into the symmetric cipher key derivation to avoid weak-cipher-attacks.

Session ID

Both sides must also calculate the 256bit session-id using `SID = HKDF_EXPAND(prk=PRK, hash=SHA256, info="BitcoinSessionID", L=32)` . The session-id can be used for linking the encryption-session to an identity check.

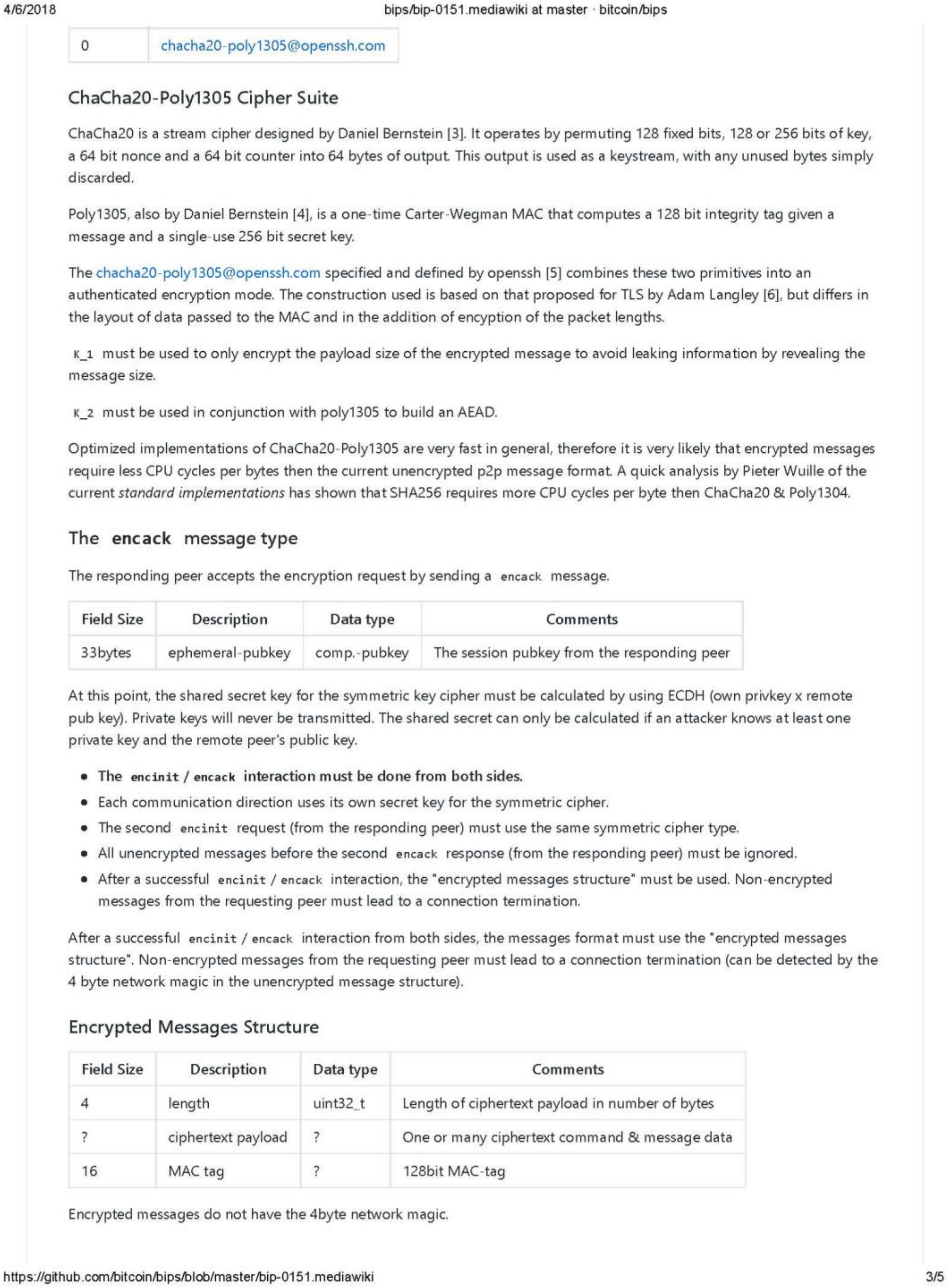
The `encinit` message type

To request encrypted communication, the requesting peer generates an EC ephemeral-session-keypair and sends an `encinit` message to the responding peer and waits for a `encack` message. The responding node must do the same `encinit` / `encack` interaction for the opposite communication direction.

Field Size	Description	Data type	Comments
33bytes	ephemeral-pubkey	comp.-pubkey	The session pubkey from the requesting peer
1bytes	symmetric key cipher type	int8	symmetric key cipher type to use

Possible symmetric key ciphers types

Number	symmetric key ciphers type



0	chacha20-poly1305@openssh.com

ChaCha20-Poly1305 Cipher Suite

ChaCha20 is a stream cipher designed by Daniel Bernstein [3]. It operates by permuting 128 fixed bits, 128 or 256 bits of key, a 64 bit nonce and a 64 bit counter into 64 bytes of output. This output is used as a keystream, with any unused bytes simply discarded.

Poly1305, also by Daniel Bernstein [4], is a one-time Carter-Wegman MAC that computes a 128 bit integrity tag given a message and a single-use 256 bit secret key.

The chacha20-poly1305@openssh.com specified and defined by openssh [5] combines these two primitives into an authenticated encryption mode. The construction used is based on that proposed for TLS by Adam Langley [6], but differs in the layout of data passed to the MAC and in the addition of encyption of the packet lengths.

`K_1` must be used to only encrypt the payload size of the encrypted message to avoid leaking information by revealing the message size.

`K_2` must be used in conjunction with poly1305 to build an AEAD.

Optimized implementations of ChaCha20-Poly1305 are very fast in general, therefore it is very likely that encrypted messages require less CPU cycles per bytes then the current unencrypted p2p message format. A quick analysis by Pieter Wuille of the current *standard implementations* has shown that SHA256 requires more CPU cycles per byte then ChaCha20 & Poly1304.

The `encack` message type

The responding peer accepts the encryption request by sending a `encack` message.

Field Size	Description	Data type	Comments
33bytes	ephemeral-pubkey	comp.-pubkey	The session pubkey from the responding peer

At this point, the shared secret key for the symmetric key cipher must be calculated by using ECDH (own privkey x remote pub key). Private keys will never be transmitted. The shared secret can only be calculated if an attacker knows at least one private key and the remote peer's public key.

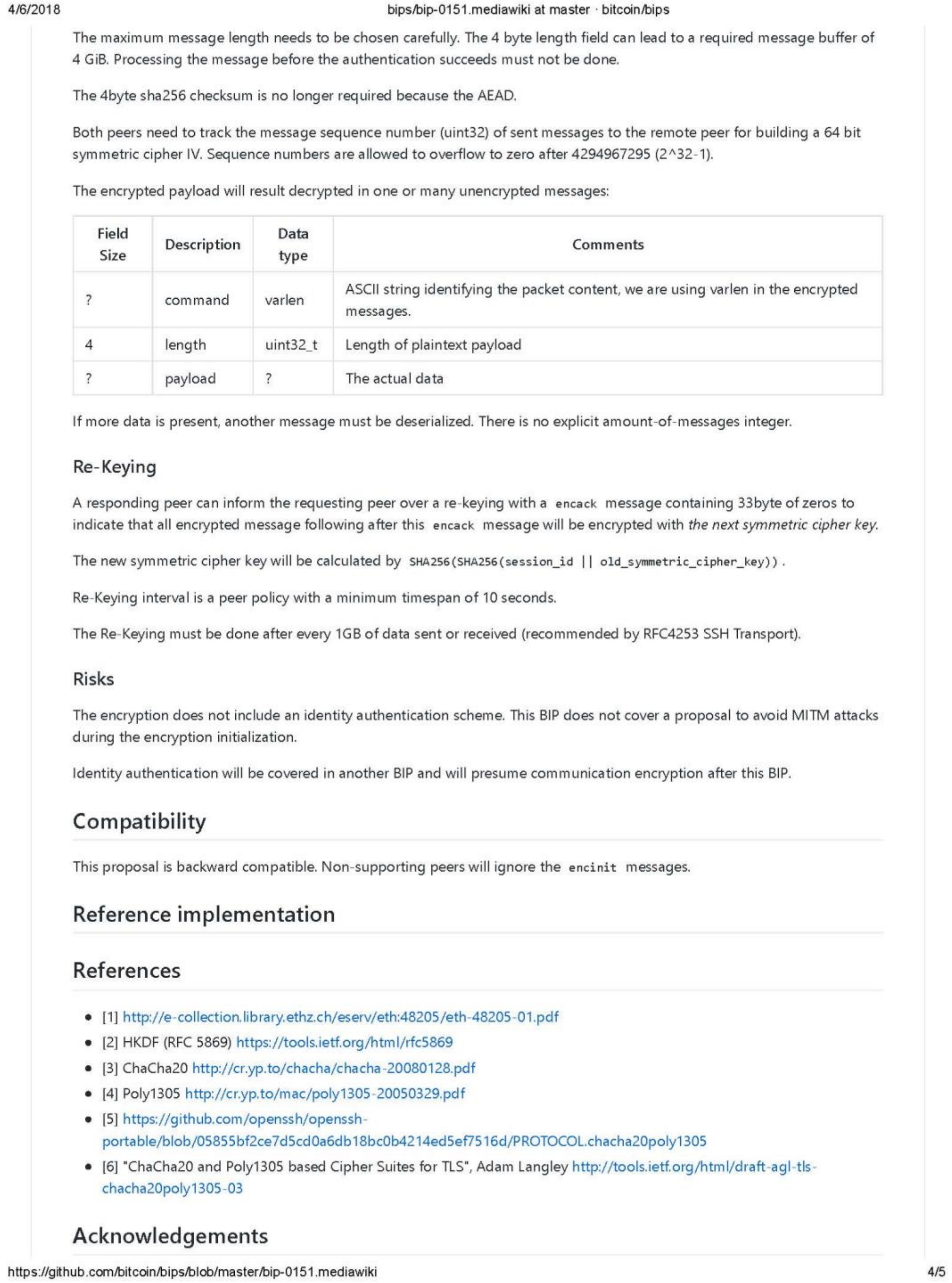
- **The `encinit` / `encack` interaction must be done from both sides.**
- Each communication direction uses its own secret key for the symmetric cipher.
- The second `encinit` request (from the responding peer) must use the same symmetric cipher type.
- All unencrypted messages before the second `encack` response (from the responding peer) must be ignored.
- After a successful `encinit` / `encack` interaction, the "encrypted messages structure" must be used. Non-encrypted messages from the requesting peer must lead to a connection termination.

After a successful `encinit` / `encack` interaction from both sides, the messages format must use the "encrypted messages structure". Non-encrypted messages from the requesting peer must lead to a connection termination (can be detected by the 4 byte network magic in the unencrypted message structure).

Encrypted Messages Structure

Field Size	Description	Data type	Comments
4	length	uint32_t	Length of ciphertext payload in number of bytes
?	ciphertext payload	?	One or many ciphertext command & message data
16	MAC tag	?	128bit MAC-tag

Encrypted messages do not have the 4byte network magic.



The maximum message length needs to be chosen carefully. The 4 byte length field can lead to a required message buffer of 4 GiB. Processing the message before the authentication succeeds must not be done.

The 4byte sha256 checksum is no longer required because the AEAD.

Both peers need to track the message sequence number (uint32) of sent messages to the remote peer for building a 64 bit symmetric cipher IV. Sequence numbers are allowed to overflow to zero after 4294967295 (2^32-1).

The encrypted payload will result decrypted in one or many unencrypted messages:

Field Size	Description	Data type	Comments
?	command	varlen	ASCII string identifying the packet content, we are using varlen in the encrypted messages.
4	length	uint32_t	Length of plaintext payload
?	payload	?	The actual data

If more data is present, another message must be deserialized. There is no explicit amount-of-messages integer.

Re-Keying

A responding peer can inform the requesting peer over a re-keying with a `encack` message containing 33byte of zeros to indicate that all encrypted message following after this `encack` message will be encrypted with *the next symmetric cipher key*.

The new symmetric cipher key will be calculated by `SHA256(SHA256(session_id || old_symmetric_cipher_key))`.

Re-Keying interval is a peer policy with a minimum timespan of 10 seconds.

The Re-Keying must be done after every 1GB of data sent or received (recommended by RFC4253 SSH Transport).

Risks

The encryption does not include an identity authentication scheme. This BIP does not cover a proposal to avoid MITM attacks during the encryption initialization.

Identity authentication will be covered in another BIP and will presume communication encryption after this BIP.

Compatibility

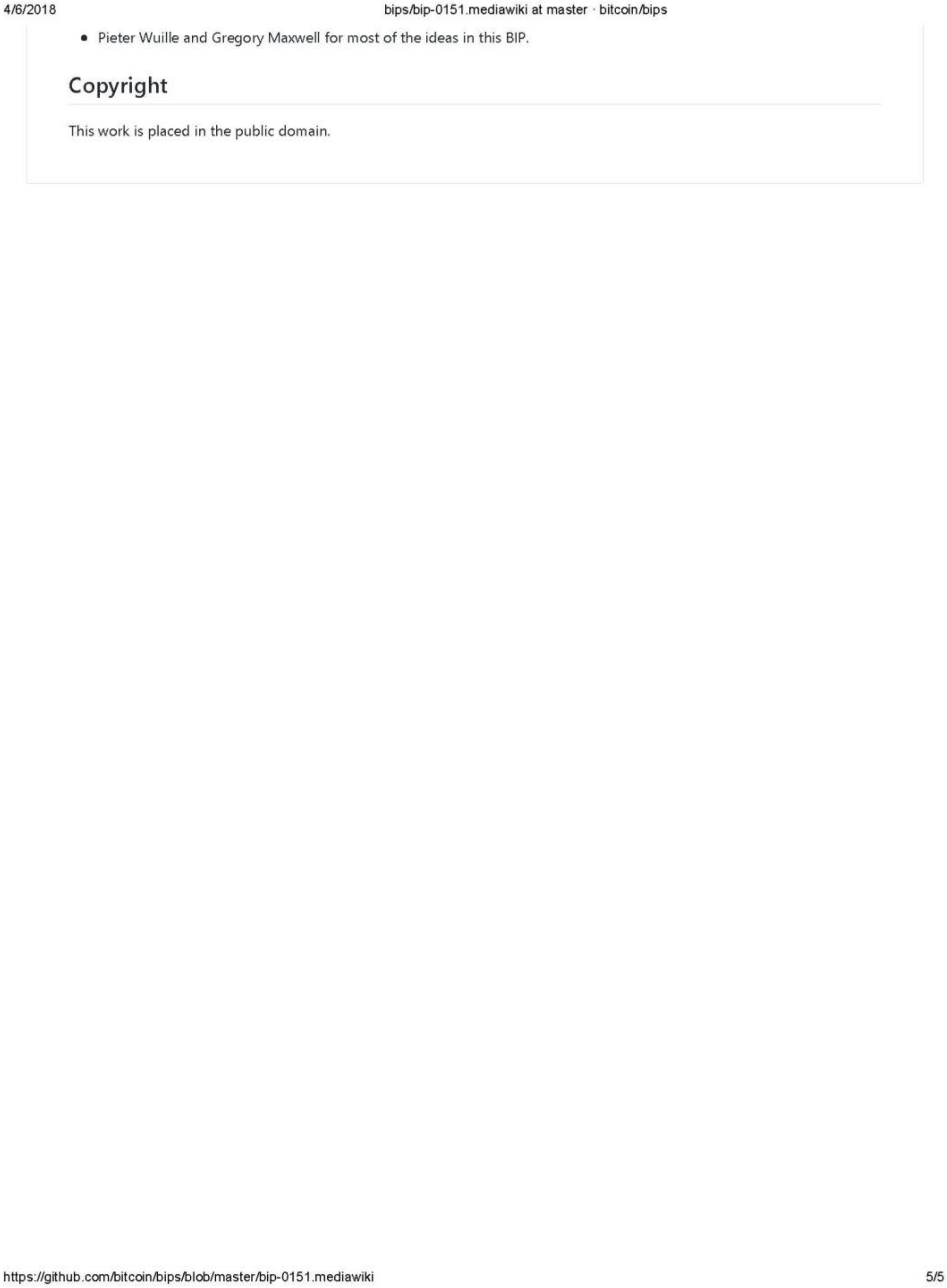
This proposal is backward compatible. Non-supporting peers will ignore the `encinit` messages.

Reference implementation

References

- [1] http://e-collection.library.ethz.ch/eserv/eth:48205/eth-48205-01.pdf
- [2] HKDF (RFC 5869) https://tools.ietf.org/html/rfc5869
- [3] ChaCha20 http://cr.yp.to/chacha/chacha-20080128.pdf
- [4] Poly1305 http://cr.yp.to/mac/poly1305-20050329.pdf
- [5] https://github.com/openssh/openssh-portable/blob/05855bf2ce7d5cd0a6db18bc0b4214ed5ef7516d/PROTOCOL.chacha20poly1305
- [6] "ChaCha20 and Poly1305 based Cipher Suites for TLS", Adam Langley http://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-03

Acknowledgements



4/6/2018 bips/bip-0151.mediawiki at master · bitcoin/bips

- Pieter Wuille and Gregory Maxwell for most of the ideas in this BIP.

Copyright

https://github.com/bitcoin/bips/blob/master/bip-0151.mediawiki 5/5

Appendix F Fs-QCA Calibration

1. Calibration of Machine Consensus Mechanisms

I used explanatory conditions' Q1 values to explain growth (or decline) from Q1 to Q2.

Security Provision: I calibrated security provision based on the extent to which proof-of-work (PoW) mining was used in Q1. PoW cryptocurrencies received scores greater than 0.5, while Proof-of-Stake (PoS) cryptocurrencies received scores below 0.5. A full membership (1) in security provision was assigned when the cryptocurrency was based solely on SHA-256 proof-of-work, the algorithm used by Bitcoin. SHA-256 is the most intensive algorithm in terms of computing power, and it requires specialized hardware designed to carry out heavy-duty computing tasks. In addition to SHA-256, other proof-of-work cryptocurrencies have used algorithms such as Scrypt (e.g., Litecoin) and X11 (e.g., Dash) that require less computing power. These were coded as less than 1.

DAOs with a hybrid design (e.g., Peercoin and Novacoin), which run PoS and PoW simultaneously, were calibrated between 0 and 0.5, depending on the degree to which they incorporate PoW. These DAOs use only PoW for the initial issuance and distribution of the cryptocurrency, and PoW is therefore non-essential in the long run (King & Nadal, 2012; King, interview #3). Some PoSe designs use PoW in the first two to three weeks for coin distribution and then become purely PoS (i.e., PoW discontinues) after the initial period. A PoS design that has never incorporated PoW was considered as pure PoS and coded as 0 (e.g., Paycoin).

In sum, beyond the 0.5 anchor, PoW dominates the payment validation process.

Stability provision: I calibrated stability provision by calculating the variance of network validation difficulty. I first normalized the raw difficulty data to make it comparable across cryptocurrencies. I then calculated a moving 14-day variance, and computed the quarterly average for Q1. The 0.5 anchor was set at the median score in our sample (0.8). A full membership (1) was assigned to variances over 1.0, indicating very high difficulty fluctuation. Conversely, a non-membership (0) was assigned to variances below 0.3, indicating very low difficulty fluctuation.

2. Calibration of Social Consensus Mechanisms

Breadth of stakeholder discussions: I capture it by calculating the monthly number of unique contributors working on the code repository of the cryptocurrency. I chose the median—20, to be the 0.5 qualitative anchor. I assigned a full membership (1) to cases with over 40 unique contributors and a non-membership (0) to cases with fewer than one contributor.

Depth of stakeholder discussions: To capture the depth of stakeholder discussion, I calculated monthly code frequency changes, i.e., the average number of additions and deletions to the cryptocurrency source code on GitHub for Q1. I calibrated the 0.5 qualitative anchor at 30,000, the median observed in our sample. I assigned a full membership of 1 to a code frequency over 60,000, indicating a high depth of stakeholder discussions. And we assigned a non-membership (0) for a code frequency below 1,000, indicating a low depth of stakeholder discussions.

Validators' commitment: The network hash rate measures the aggregate computing power of the cryptocurrency network. I set the 0.5 anchor at the sample median hash rate of 1 Ghash/sec. A large mining network typically contains substantial computing power with a hash rate over 100 Ghash/sec, to which I allocated a full membership. Conversely, a network with a hash rate below 0.01 Ghash/sec was allocated a non-membership (0).

3. Calibration of Decentralization of Strategy Making

I calibrated it by jointly considering three dimensions: the *design philosophy*, the presence of an *active foundation*, and whether the *founder's identity* was known. I first evaluated each dimension individually and determined its degree of decentralization; I then combined the three dimensions to generate the final calibration for decentralization. Our logic closely follows Crilly et al. (2012: 1435, Table 2), in which evaluations of high, medium, and low memberships are given to each category of CSR-related criteria, before they are pooled together for calibration.

Active foundations: As I have noted, the presence of an active foundation signals more centralized control of a cryptocurrency. I considered cryptocurrencies that have active foundations to be low in decentralization, and cryptocurrencies without active foundations to be high in decentralization.

Founders' identity: I considered those cryptocurrency DAOs with known founders to be low in decentralization. DAOs with pseudonymous and unknown founders were considered to have a mid-range or high level of decentralization, respectively.

Design philosophy: At one end of the spectrum, some cryptocurrencies have a more centralized design philosophy. For example, some business-oriented cryptocurrencies resemble business entities in that they have a clear strategic orientation. These cryptocurrencies are concerned with growing the network with incentive systems, business development plans, and interorganizational alliance strategies (e.g., Litecoin, Dash, and Worldcoin). Some consider themselves as DAOs governed by the network of "investor volunteers" or "master nodes" with decision and voting rights (Daniel Diaz, 2016, interview #2). DAOs in this category were considered low in decentralization.

At the other end of the decentralization spectrum, I find more decentralized DAOs focused on the social dimension. Such DAOs are established with formative ideologies and value propositions built into their design. For example, Dogecoin appealed to the community by promoting awareness of cryptocurrencies and backing charitable causes (e.g. the NASCAR Sprint Cup Series rally). DAOs in this category are considered to have a mid-range level of decentralization.

Finally, innovation-oriented DAOs that focus on decentralization received a higher score. In contrast to cryptocurrencies with a business-oriented model, these DAOs see themselves as technology leaders governed by meritocracy. For example, Namecoin aims to protect free speech and prevent Internet censorship by assigning domain names that cannot easily be tracked by centralized organizations or governmental agencies. In addition, Bitcoin and Peercoin promote disintermediation and mining efficiency based on technological innovations.

I combined the three dimensions for each case. I allocated a full membership (1) to DAOs that were highly decentralized in all three dimensions and non-membership (0) to those that were low in all three dimensions. The 0.5 anchor indicates DAOs with mid-range scores and inconsistent decentralization profiles, in line with the calibration strategy proposed by Crilly et al. (2012).

Curriculum Vitae

Name:	Ying-Ying Hsieh
Post-secondary Education and Degrees:	National Tsing-Hua University Hsinchu, Taiwan 1992-1996 B.Sc.
	National Tsing-Hua University Hsinchu, Taiwan 1996-1998 M.Sc.
	The University of Western Ontario London, Ontario, Canada 2013-2018 Ph.D.
Honours and Awards:	The George E Connell Graduate Scholarship 2017-2018
	The Plan for Excellence Award Doctoral scholarship 2013-2017
Related Work Experience	Teaching Assistant The University of Western Ontario 2016-2017
	Research Fellow Scotiabank Digital Banking Lab at Ivey Business School 2016-2018

Publications:

Hsieh, Y.-Y., Vergne, J.-P., & Wang, S. (2017). Forthcoming. The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In Campbell-Verduyn, M. (ed.), *Bitcoin and Beyond: Blockchains and Global Governance. RIPE/Routledge Series in Global Political Economy*. 48-68.

Hsieh, Y.-Y. & Vergne, J.-P. (2017). Bitcoin and the rise of decentralized autonomous organizations*. Journal of Organization Design*, Forthcoming.

Chakravarty, D., Hsieh, Y., Schotter, A. P., & Beamish, P. W. (2017). Multinational Enterprise Regional Management Centres: Characteristics and Performance. *Journal of World Business*, 52(2), 296–311.