Journal of Organization Design
a SpringerOpen Journal

ORGANIZATION ZOO Open Access

Bitcoin and the rise of decentralized autonomous organizations

Ying-Ying Hsieh[1*] and Jean-Philippe Vergne[2]

* Correspondence: y.hsieh@imperial.ac.uk
[1]Imperial College Business School, Imperial College London, South Kensington Campus, Exhibition Road, London SW7 2AZ, UK
Full list of author information is available at the end of the article

Abstract

Bitcoin represents the first real-world implementation of a "decentralized autonomous organization" (DAO) and offers a new paradigm for organization design. Imagine working for a global business organization whose routine tasks are powered by a software protocol instead of being governed by managers and employees. Task assignments and rewards are randomized by the algorithm. Information is not channeled through a hierarchy but recorded transparently and securely on an immutable public ledger called "blockchain." Further, the organization decides on design and strategy changes through a democratic voting process involving a previously unseen class of stakeholders called "miners." Agreements need to be reached at the organizational level for any proposed protocol changes to be approved and activated. How do DAOs solve the universal problem of organizing with such novel solutions? What are the implications? We use Bitcoin as an example to shed light on how a DAO works in the cryptocurrency industry, where it provides a peer-to-peer, decentralized, and disintermediated payment system that can compete against traditional financial institutions. We also invited commentaries from renowned organization scholars to share their views on this intriguing phenomenon.

Keywords: Decentralized autonomous organization, Blockchain, Consensus mechanisms, New forms of organizing, Organizational forms

"[I]t makes most sense to see Bitcoin [...] as a decentralized autonomous organization."

Vitalik Buterin (2014), Industry Expert, Co-founder of Ethereum and Co-founder of Bitcoin Magazine.

Introduction

What is bitcoin?

Bitcoin is an open source software code that implements a decentralized, peer-to-peer digital cash payment system that does not require any trusted intermediaries to operate (e.g., banks or payment companies). The Bitcoin Whitepaper was published in 2008 by a developer (or development team) under the pseudonym Satoshi Nakamoto, and was soon followed by the first ever "coin" created in the form of a digital record in 2009. At the time of writing (October 2017), Bitcoin hit another record high price of over $4400, forming an economy of $73 billion.

Initially, Bitcoin's design aimed to solve the inherent inefficiencies and agency problems arising from the intermediated and centralized banking model. Typically, to make an international wire transfer between, say, Canada and China, the money goes through 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 3 and 15 business days to complete, depending on the destination country, and involves multiple agents such as bank tellers, employees, and managers from the aforementioned financial institutions. Expensive bank fees and exchange rates apply.

By contrast, Bitcoin is distributed in cyberspace across thousands of network nodes, and is inherently borderless. Payments are validated and updated by the network every 10 min. Intermediaries are not required (e.g., no correspondent banks are required). There are no bank fees for transactions, but users typically pay a small fee to payment validators (known as "miners"—to be discussed further below). Whereas for an international transfer of $5000, a bank wiring would charge a fee of around $125, a fee of around $1 would be expected for a Bitcoin transfer. It is no wonder, that Bitcoin is seen as a potentially significant disruptor of the current financial system based on banking.[1]

Bitcoin as a decentralized autonomous organization

Bitcoin "runs a payment system…employs subcontractors who are miners… paid for with newly issued bitcoin shares in itself" (Vigna and Casey 2015, p. 229, quoting Larimer 2013).[2] The Bitcoin system thus shares the four core features common to all conceptualizations of "organizations": it is a "multi-agent system […] with identifiable boundaries and [a] purpose […] towards which the constituent agents' efforts make a contribution" (Puranam 2017, p. 6). But in contrast to traditional organizations, Bitcoin does not have a CEO or top management team but instead developers who "write the rulebook," i.e., define governance rules for the program (Narayanan et al. 2016, pp. 173–175). Bitcoin does not have headquarters, subsidiaries, or employees, but a distributed network of users and miners who collect, verify, and update transactions on a shared public ledger that is publicly auditable. Decisions on code modifications are made through community-based democratic voting processes, backed by miners' computing power for implementation (Narayanan et al. 2016, pp. 173–175).

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 et al. 2016a, 2016b).

These innovations have led some industry experts to conceive of the Bitcoin system as the first real-world implementation of a new type of organization called "decentralized autonomous organization" (hereafter, DAO). Following prior work, we define DAOs as *non-hierarchical organizations that perform and record routine tasks on a peer-to-peer, cryptographically secure, public network, and rely on the voluntary contributions of their internal stakeholders to operate, manage, and evolve the organization through a democratic consultation process* (Valkenburgh et al. 2015; Dietz et al. 2016).[3] DAOs coordinate routine tasks through cryptographic routines (as opposed to human routines). Open source code defines rules for miners to agree on a shared history of transactions recorded securely and redundantly across network nodes, in order to avoid having a single point of failure (Nakamoto 2008). While Bitcoin was the first instance to be identified as a DAO, a few hundred more have then been created since 2009 (e.g., Ethereum, Litecoin).

Bitcoin vs. banks

Bitcoin represents a partial substitute for banks, albeit with notable differences.

First, one cannot open a bank account without providing a number of official identification documents, which in the developing world often prevents access to banking. By contrast, anyone can become a Bitcoin user and freely obtain a pseudonymous Bitcoin address (i.e., analogous to a bank account) not tied ex ante to a real-world identity. In essence, a Bitcoin address is a public key cryptographically linked to a private key acting as a password to spend funds. This enables a new privacy model that separates identity from transactions (Nakamoto 2008). The vertical bar in Fig. 1 demonstrates where Bitcoin breaks the information flow as compared to banks.

Second, 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 cyberattacks and employee misconduct. Traditionally, banks employ bank clerks to process payments. Human agents are prone to agency problems which can lead to misconduct such as theft. The cost of paying the human agents is also not trivial. With Bitcoin, all transactions are recorded publicly and electronically onto the immutable "blockchain" stored in a distributed fashion across thousands of network nodes—thereby making records easier to maintain and cyberattacks unlikely to succeed (because the information on transactions in this case is not held in one central location). The blockchain technology provides the multi-site copies of "ledgers"—which are really aggregations of past transactions (e.g., like a bank account statement). It also provides encryption to validate transactions as valid or invalid (e.g., like personal security device we currently use for online banking, which generate a unique transaction specific signature based on a personal key).

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, Bitcoin relies on cryptographic routines to verify, timestamp, and order transactions in a non-reversible way, thereby avoiding the need for human reconciliation. This process is called "mining." The key idea is that somebody in the network will legitimately time stamp

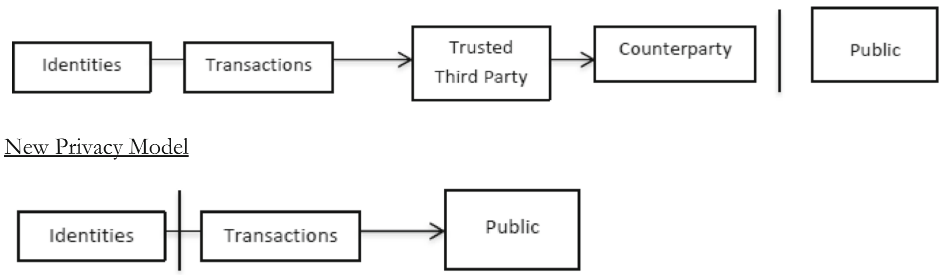

Fig. 1 Traditional privacy model vs. the Bitcoin privacy model (adopted from Nakamoto 2008)

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).

Bitcoin “hires” miners to process transactions in this way through a “competitive bookkeeping” process (Yermack 2017). Mining is a process whereby specific network nodes (“miners”) arrange new transactions into a sequence, and time-stamp them by solving a puzzle of sorts: by guessing an arbitrarily long number after making billions of random guesses. The guessing process can be made faster by committing more computing power to the network. Thus, a miner’s probability of being able to provide the “proof-of-work” required to update the ledger is proportional to the computing power s/he controls. The computing power committed every 10 min 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). Miners get rewarded in Bitcoin for their work, which involves costs in hardware and electricity, as per the Bitcoin protocol.

Consensus mechanisms: novel solutions to the universal problems of organizing

Whereas mining organizes Bitcoin payment processing, “humans must first decide what protocol to run before the machines can enforce it (Lopp 2016)”. To distinguish the logic of blockchain from its governance and re-design process, we define *machine consensus* as the process whereby blockchain produces agreement (aided by miners efforts) on the ordering of transactions through the time-stamping created by miners succeeding at guessing a random number; and *social consensus* as the process whereby miners vote on protocol update proposals introduced by volunteer developers. Machine consensus and social consensus fuel Bitcoin’s novel organizational model and become integrated through the unique mining process based on computing power provision.

Machine consensus: the bitcoin payment system

Proof-of-work mining is a computationally intensive and highly redundant process that generates inefficiencies in terms of energy consumption. But as a result, the blockchain record cannot be tampered with at a profit. With machine consensus, tasks are allocated based on commitments in computing power, and rewarded competitively based on the outcome of mining. All mining-related data are publicly auditable for the entire network. Table 1 shows how Bitcoin as a payment system organizes differently from banks and payment organizations.

Social consensus: protocol upgrades

Underlying the Bitcoin payment system is the blockchain software supported by ongoing protocol updates (Wang and Vergne 2017). In terms of governance, miners’ voting on protocol update proposals resembles the community-based management of open source software development (OSSD) observed for projects such as Linux. It aligns stakeholder expectations (Lopp 2016) and facilitates knowledge sharing, problem solving, and the realization of collective outcomes (O'Mahony and 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

Table 1 Banks and payment organizations vs. Bitcoin on their forms of organizing

Goal	Provision of a payment system	
	Banks and payment organizations	Bitcoin
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 for mining, and is *automated* by the blockchain software in a decentralized fashion.
Task allocation	Assigned by formal hierarchies	Miners self-select into the network. However, competitive bookkeeping only allocates ayment validation tasks to the winning miner (essentially chosen at random, though the probability of winning is proportional to 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 flow	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 machine consensus ensures all nodes have the same record.

and self-select into tasks and roles based on expertise and preferences. 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 as compared to OSSD is that in addition to developers, miners play an equally important role in protocol modifications. Specifically, the Bitcoin software is updated through Bitcoin improvement proposals (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 to trigger implementation. Proposals are first reviewed by BIP editors, and miners then include a "yes" or "no" vote in a block during the polling period (e.g., 100 blocks starting today, namely a 1000-min period). Voting power is proportional to the computing power a miner contributes to the network. A code change will only be implemented when a majority of 55% is obtained for a given proposal (Franco 2014, p. 90). Table 2 compares Bitcoin software development with OSSD along four core dimensions of organizing: task division, task allocation, reward distribution, and information flow (Puranam et al. 2014).

Bitcoin's true organizational novelty lies in how mining determines task division (based on computing power contribution), task allocation and reward distribution (through competitive bookkeeping), and information flows (on the blockchain and in the network). While task integration in traditional settings focuses on rules and processes designed in large part by managers (Okhuysen and Bechky 2009), with Bitcoin, machine consensus (e.g., competitive bookkeeping) and social consensus (e.g., voting) are coordinated through miners—a brand new class of stakeholders.

Miners consent to playing by the rulebook, but they can vote to change it using the influence derived from their computing power. However, it is important to note that the Bitcoin code does not assume away the problem of agency costs. Rather, Bitcoin

Table 2 Updating software protocol: open-source software development vs. Bitcoin

Goal	Protocol update	
	OSSD	Bitcoin (BIP)
Mechanism	Community governance	Voting: Bitcoin improvement proposal (BIPs) (social consensus)
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 to 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 flow	Information is processed through "virtual support infrastructure and tools" (Puranam et al. 2014)	Information is shared and communicated through BIPs communication on the code repository (i.e., GitHub) and reflected in miners' voting outcomes on the blockchain.

explicitly deals with these long-standing problems by incorporating counterbalancing incentives in the code, making the payment system incorruptible.

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 consensus algorithms and social consensus routines, with 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.

Similar blockchain implementations: cryptocurrencies

Bitcoin is the first and most established DAO implemented to date. Since Bitcoin, there have been over 800 other DAOs created based on similar designs, most of which are considered to be "cryptocurrencies" (i.e., like Bitcoin, they allow for value exchange). At the time of writing, cryptocurrencies form an economy of $110 billion and make a real impact on the world. Some cryptocurrencies are developed based on the Bitcoin source code (e.g., Litecoin, Namecoin, Dash), while others started from scratch with their own protocol (e.g., Monero, Ethereum). Variations have also emerged to embrace a wider range of applications other than just payments, such as decentralized domain registration (Namecoin), smart contracts (Ethereum), and privacy (Monero). Proof-of-work mining is not anymore the only way to achieve machine consensus, as alternative or complementary schemes such as proof-of-stake (whereby the security proof is based on the amount of cryptocurrencies payment validators hold) or proof-of-burn (whereby the network is secured by validators allocating coins to an unspendable address) have been developed and implemented in recent years. Preliminary research suggests that DAO performance varies with the extent of governance decentralization (Hsieh et al. 2018), so understanding how various forms of machine and social consensus contribute to the success and failure of DAOs represents an exciting avenue for future organizational research.

Companies of the future?

Research indicates that the technological innovation potential behind cryptocurrencies stands as the key driver of their market value (Wang and Vergne 2017). But, as the Economist (2015) rightly points out, blockchain technology has far-reaching applications beyond cryptocurrencies 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 last 3 years, more than 50 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). DAOs are on the rise, and it is an exciting time for management and organizational scholars to address this emerging phenomenon with new theory and solid empirical research.

Bitcoin: distributed ledger may be more important than distributed organization?

Philip Anderson

The authors’ article “Bitcoin and the Rise of Decentralized Autonomous Organizations” performs the welcome service of highlighting for organization theorists how so-called cryptocurrencies (more properly, tokens) are at root about organizing, not about money. We are living through an era of ferment in token technology. Bitcoin itself is unlikely to become the dominant design for tokens because its design limits the speed at which transactions can be confirmed and registered. (A typical credit card network can process about 1500 times as many transactions per second.) A superior alternative has already emerged that enables “smart contracts,” although its first-generation programming language will likely be superseded many times, just as COBOL gave way to more advanced tools for computing.

Even blockchain, the database architecture underpinning all tokens today will likely be supplanted by superior variants. As the authors note, the innovation of blockchain technology introduced some brilliant ideas for dealing with agency problems, incentivizing transparent, fraud-resistant bookkeeping that establishes publicly who owns and has a right to exchange tokens. Faster and more elegant designs may well replace blockchain, but the underlying idea it represents—a *distributed ledger*—will endure, transforming how people and things organize and transact with one another. By analogy, every element of today’s automotive technology is vastly superior to the 1901 Curved-Dash Oldsmobile, the first mass-produced car, but the idea it pioneered of an autonomous, engine-powered vehicle that travels across roads or open country transformed the world.

A distributed ledger is hosted and updated on a decentralized network of computers that nobody owns. As the authors note, the key innovation is a novel way to store and update a chain of information (e.g., a series of exchanges, or immutable copies of documents) that anyone can examine and verify without altering. Like cash, tokens in distributed ledgers are anonymous, although governments could easily compel taxpayers to reveal the addresses they own. Yet most cash exists today not as bills or coins but as computer data showing how much people have on deposit. These data are held in private, centralized ledgers controlled by institutions such as banks. Distributed ledgers are public and require no trusted intermediary to verify who has title to what.

Financial intermediaries enable strangers to transact because a state-backed trusted institution guaranteed transactions. Most money in global financial systems is actually credit extended by these institutions, not currency printed by governments. Periodic credit crises undermine confidence in these trusted institutions, as does the abuse of seignorage—the return to the issuer (e.g., a government) from the right to create money—typically by over-inflating a currency. A host of tokens using distributed ledgers are competing to institutionalize ways of creating trust among strangers that does not depend on trusted intermediaries.

For this reason, the impact of tokens on organizations is likely to be even greater than its impact on monetary economics. The authors note that the way in which miners are incentivized by seignorage[4] to perform distributed work facilitates decentralized task allocation, task division, reward distribution, and information flow. Blockchain technology and some clever mechanisms built into Bitcoin and its descendants create trust among self-interested actors at two levels. For token users, they minimize counterparty risk, assuring token buyers that the anonymous address at the other end of the transaction actually owns the token. They also transparently document and preserve each element of the blockchain in a way that is difficult to spoof or alter. For miners—parties who supply the computing power to run the system—they provide a means of compensation for providing infrastructure and running its software for the benefit of the users. The miners, not the users, have voting rights that allow them to decide when and how the software or its rules of use may be altered.

A decentralized autonomous organization (DAO) as described by the authors is an organization that uses software rules to execute organizational routines, plus votes from some class of members to alter and extend those routines. No direct management is required. In Bitcoin, the miners are the voters, but this is not strictly necessary.

For example, a group of neighbors could club together to buy a shared asset, such as a fleet of bicycles. Each member could receive tokens based on his or her investment, spending them when they use the asset. Spent tokens could be reissued according to rules, incentivizing people who perform useful services such as storing or repairing the asset. Token owners could vote on changes to rules or policies and make decisions such as when to buy new bicycles. The distinction between "owners," "contributors," and "users" is blurred because the same token acts as a voting right, a form of compensation, and a medium of exchange.

Organizations have long used what amount to private currencies to incentivize ownership, contribution, and usage. Shares of stock are frequently used to acquire companies or remunerate employees. Loyalty programs or privileged benefits are commonly used as a non-cash incentive for employees or customers. In a DAO, a token can represent ownership, compensation for contributions, and payment for usage all in one. Just as banks create money by extending credit, organizations can use tokens to create and sustain an internal economy whose currency can be converted into fiat money but does not depend on it.

In these early days of distributed ledgers and tokens secured by cryptographic methods, DAOs remain rare. Some organizers have raised money via initial coin offerings (ICOs), exchanging tokens for cash. These tokens secure voting and perhaps usage rights for projects that range from explicit to vague. For instance, an ICO can be pledged to the development of a software program. Token buyers may be compensated by low-cost or privileged access to the program as users. They may also have rights to participate revenues earned by the program, and they may be compensated for contributions to the software. Token holders may or may not have voting rights that govern how the software is developed. A central, hierarchical organization could also make those decisions, with the token's value depending on the quality of those choices and how well they are executed.

Distributed ledgers enable DAOs but will also find many applications inside more traditional organizations, as a transparent means of decentralized task allocation, task division, reward distribution, and information flow. For example, firms may develop internal reputation mechanisms enabled through the exchange of tokens, recorded in a distributed ledger free for all to inspect. Those who own tokens can use them to reward cooperation from others, or to exchange them for other things of value, such as vacation days. This could enable far more peer-to-peer collaboration among people who do not already know one another well, without needing a common supervisor as a trusted intermediary.

Transaction-cost economics suggests that the basic reason why organizations exist is to minimize transaction costs—if everybody could make, execute, and adjudicate contracts at low cost, that would be the most efficient way to manage the four basic functions of organization design. As the authors note, the rise of automated "smart contracts" can dramatically lower the cost of contracting and lessen the risk that people fail to deliver what they promise. Consequently, it is frequently conjectured that cryptocurrencies and distributed-ledger technology will lead to massive disintermediation and the supplanting of organizations with loose networks of contributors who are linked by contract. A DAO is an example *par excellence.*

Yet decades of research have explained why organizations arise and persist for reasons that go beyond minimizing transaction costs. Such factors as shared purpose, identity, collective reputation and status, and the ability to habituate pro-social behaviors help explain why organizations endure. Distributed-ledger technologies and tokens that ride on top of it will doubtless make a massive impact on organizations and exchange, and some DAO's will successfully supplant other ways to solve economic problems, as the authors suggest. Once a dominant design emerges and distributed ledgers become viable substitutes for other database architectures, tokens will also revolutionize the way organizations manage their routines while sustaining useful forms of central control. Bitcoin itself will likely become a historical artifact, but it has opened the door for a flood of organizational innovation that turns out to be far more important than the term "cryptocurrency" would suggest.

The decentralization mirage

Karim Lakhani

"Bitcoin and the Rise of Decentralized Autonomous Organizations" by the authors provides an intriguing snapshot of the rapidly evolving blockchain space for management and organizational studies scholars. I realized that something important was going on with Bitcoin when several Uber drivers mentioned that they were actively investing in Bitcoin. An obscure part of the internet sub-culture that had invented a new digital currency has now gone mainstream with stalwarts like Bloomberg News and Goldman Sachs now actively covering all the developments and the HBO show "Silicon Valley" featured the blockchain as an ongoing storyline for the imaginary startup Pied Piper.

As the authors point out, Bitcoin and blockchain not only demonstrate the creation and scaling of a decentralized currency but they also provide a glimpse into the future of new organizational forms that could be highly decentralized and designed on different principles than the ones we typically see around the world. In many ways, blockchain is a foundational technology that foreshadows significant economic, technological, and organizational change (Iansiti and Lakhani 2017). Tracking transactions between entities is a core organizational task and blockchain has reconceived this tracking function from being private and centralized to one that is public, decentralized, and potentially programmable. Just as packet switching and TCP/IP reconceived communications as a decentralized operation and then subsequently enabled the change in the economic, business, and social architecture of the world, it appears that blockchain may have the same potential for change by decentralizing how transactions get verified and recorded among parties.

I am however less sanguine than the authors as to the potential for the organizational architecture to mirror the decentralized blockchain technological architecture (Colfer and Baldwin 2016) as it comes to future decentralized autonomous organizations (DAO). In particular, I outline three concerns based on observed empirical regularities in Bitcoin and other distributed systems that point to the presence of centralized bottlenecks in the midst of decentralized architectures. First, bitcoin mining, although in theory can be decentralized, has emerged as a highly centralized operation requiring significant capital expenditure. Gencer et al. (2018) show that mining is highly concentrated, with the top four miners owning 53% of the average mining power for Bitcoin and only three miners holding 61% of the average mining power for Ethereum (a Bitcoin competitor). Analysis of mining power shows that the data fit an exponential distribution (0.21E^-19x and 0.35e^-30x in Bitcoin and Ethereum respectively) with 90% of the total mining power in the hands of only 16 miners in Bitcoin and just 11 miners in Ethereum. These highly centralized mining bottlenecks at the heart of Bitcoin raise serious questions regarding the concentration of power and authority in its DAO.

My second concern is that other forms of decentralized autonomous organizations, in particular open source software development, although it has decentralized participation, do not seem to exhibit decentralized governance. Authority to commit code and make it official tends to be limited to just a few individuals (Linus Torvalds has ultimate power as to what gets into the Linux kernel) or subject to some committee structure (von Krogh et al. 2003). Some communities even develop complex rules and regulations and related bureaucracies in the name of self-governance (O'Mahony and Ferraro 2007). The presence of a profit motive, in the form of a company-sponsored open source project further limits governance access and ultimate decision-making authority (West and O'Mahony 2008). If open source provides a roadmap for blockchain-enabled DAOs, then I expect centralized governance for these new organizations. Complicating matters is that DAOs are created in software, and thus those that can write and understand code will have inherently more access to influence the DAO versus those that do not.

My third concern is that the history of technology, particularly those involving network effects, shows that decentralization is often accompanied by centralization simultaneously. The personal computer revolution democratized computing power into the hands of ordinary citizens and workers and yet simultaneously created the Microsoft monopoly. The promise of the decentralized internet with distributed content creation and consumption has come true, yet search has become a significant bottleneck with Google currently acting as a centralized gateway. Similarly, in social media, Facebook has enabled disparate communities and individuals to connect and share information, yet it has centralized the matching of friends and the connections. Blockchain technology also exhibits network effects, and many of the novel applications being developed require ecosystem coordination (Iansiti and Lakhani 2017); thus I expect centralization also to emerge.

I agree with the authors that Bitcoin, the blockchain, and DAOs represent a new set of experiments in organizational design and management of complex activities. Studying the emergence, growth, sustainability, and failure of DAOs will offer greater insight into our literature and help us to understand better the changing landscape of knowledge workers and the organizations that support them. However, we should be cautious and skeptical about the mirage offered by many technologies that proport to decentralize. Instead, we should take our analytical toolkit and understand the contingencies under which the promise of decentralization takes hold and the circumstances that lead to even more concentration.

Bitcoin as DAO—between fascination and hype

Markus Reitzig

Little did Lamport, Shostak, and Pease know how their work would give rise to one of the truly radical business innovations of the past decade when they published their seminal piece on the fundamentals of blockchain algorithms in 1982. Wondering how to ascertain that malfunctioning components within a computer system would not pass on conflicting information to different parts of the system, in "The Byzantine Generals Problem",[5] the computer scientists from Menlo Park drew inspiration from an ancient military setting—the infamously fertile soil for so many innovative ideas. The question the authors posed was the following: how could a group of physically separated Byzantine divisions successfully coordinate on a concerted attack against their enemy in the presence of treacherous Albanian commanders and messengers within their own ranks? Communicating via forgeable oral messages would require truthful commanders to be in a serious majority. Communication using written, unforgeable messages, so Lamport et al. proved however, would enable coordination among commanding generals even in the presence of multiple traitors—commanders and messaging lieutenants alike, for as long as one lieutenant would be honest.

To this day, the signed message algorithm—the original idea behind the blockchain ledger—as well as Nakamoto's probabilistic solution to the Byzantine General Problem eventually deployed in Bitcoin continues to fascinate many who hear of it for the first time. And equally fascinating—at least in the eyes of an organizational scientist—seems the technology's widespread adoption across different sectors. Cryptocurrencies, digital voting, smart contracts—or any other thinkable application in which the technology alone can eliminate the risk of forgery—provide instances in which traditional forms of exchanging sensitive information, notably trust-based forms of exchange, face a modern substitute. The mushrooming of firms using blockchain technology testifies to the likely lasting impact it had on the variety of the organizational life that surrounds us.

All that being said, if nothing else, the sheer political incorrectness by modern standards regarding the use of national stereotypes in Lamport et al.'s work reminds us of how far the origins of blockchain technology date back already. By all measures of technological progress, it seems hard to still classify either their signed message algorithm or Nakamoto's proof-of-work as "novel" technologies in the eyes of an expert today. In fact, in the fast-paced life of information technology, one could argue that these would have assumed the status of "classics" rather than novice ideas. If that is so, however, it appears legitimate to ask if we can still expect it to be applied to business in hitherto unknown ways, or whether we may have seen all facets of its potential use being realized already.

For the sake of stimulating more debate, I lightheartedly propose that we may witness the birth of many more firms using blockchain technology, but that these ventures will be reminiscent of the ones we have seen to this day in one way or another. The reason being that blockchain ledgers—their fascination notwithstanding—really only provide novel solutions to one of the four fundamental problems of organizing; namely, to the way in which information is being exchanged. At the same time, they have little, if any, direct effect on the way in which tasks are being divided, let alone allocated, and on how members within an organization are being rewarded; and consequently can likely not give rise to forms of organizing which we would not have seen already.

Surprisingly enough, I believe it is the case of Bitcoin—arguably the most prominent blockchain-based venture—that supports my reasoning best. Undoubtedly, its functioning hinges on the functionality of the ledger and the possibility for individuals to exchange sensitive information in the absence of trust (worthy middlemen), as the authors neatly showed in their case description. The viability of its design, however, equally depends on its fully modular task divisibility, the feasibility of the self-selection mechanism, and a rather trivial rewards distribution challenge. Bitcoin's structure can be fully modular as gains from substitution, splitting, augmenting, or excluding individual tasks seem negligible. Task allocation can rely on self-selection as matching on skill is irrelevant. Reward distribution is obvious. These latter features, however, result from the very artifact that Bitcoin produces and do not require or preclude the use of the blockchain technology per se. Only jointly, however, will these solutions to the four fundamental problems of organizing render the workings of a "decentralized autonomous organization" viable. The parameter space for these specific combinations of organizational solutions seems limited to me, however, and is severely restricted by the artifacts that the organization seeks to produce.

Undeniably, Bitcoin's history so far has been captivating to say the least. However, it seems equally incontestable that the organization has a dangerous potential to be "over-hyped" by many actors—most prominently by late-bird financial investors in 2017 perhaps, but also by executives producing serious belly flops for their companies when changing their highly-valued corporate brand names into "blockchain" snippets of some kind, unsuccessfully attempting to dovetail on the Bitcoin success wave.[6] Finally, by ourselves, I believe that we, as organizational scholars, need to be wary not to fall for a similar trap of deriving undue generalizations from Bitcoin's account. In closing, let me thus make two claims by suggesting that blockchain technology will neither be a silver bullet to resolve an organization's overall decentralization challenge nor that blockchain technology is solely relevant to decentralized autonomous organizations. Bitcoin itself serves as a case in point supporting my first claim: both its architecture of participation and the blockchain ledger would appear to be necessary conditions for the organization's overall functioning. The Swedish e-krona project[7] may be seen as an example that lends credibility to my second claim: issued centrally by the Swedish Riksbank, this cryptocurrency could replace traditional coins and notes in the country in the foreseeable future. An all but decentralized venture…

Closing thoughts

The Authors

In keeping with the spirit of the *Organization Zoo* series, we examined the puzzling and innovative design features of a very special organization (Bitcoin) and argued that they will pave the way for new forms of organizing. Tentatively, we proposed the label "decentralized autonomous organization" (DAO) to theoretically characterize what is at play with Bitcoin and other comparable organizations. We are grateful for the opportunity to bring to the fore what could well be the most exciting organizational innovation of the twenty-first century (DAOs) and for the insightful commentaries provided by the three commentators.

We agree with commentator #1 that, from the perspective of management scholarship, "cryptocurrencies […] are at root about organizing, not about money." And, as noted by commentator #2, Bitcoin and its blockchain "provide a glimpse into the future of new organizational forms that could be highly decentralized and designed on different principles." But he nuances his claim by outlining three caveats: the observed concentration of mining operations, the practical difficulty of decentralizing DAO governance, and the risk of monopolization typically observed in information industries subject to strong network effects—think AT&T, Microsoft, Google, or Facebook (see Wu 2011 and Durand and Vergne 2013 for complementary historical perspectives on this phenomenon). The community is well aware of these limitations, and solutions are already being developed to address them: replacing proof-of-work mining with alternative consensus mechanisms to mitigate unwanted concentration, implementing governance directly into the blockchain to avoid the emergence of an external authority with too much influence on the evolution of the blockchain protocol (a phenomenon called "on-chain governance"), and the creation of interoperability protocols to facilitate communication across blockchains and prevent a winner-take-all effect. Note, however, that the dominance of a single blockchain would not be too much of an issue as long as that blockchain remains decentralized *by design*.

We concur with commentator #3 that the technological novelty underpinning Bitcoin is a more nuanced phenomena than what is typically depicted in overhyped media accounts. As demonstrated by Narayanan and Clark (2017), "Bitcoin was unusual and successful not because it was on the cutting edge of research on any of its components, but because it combined old ideas from many previously unrelated fields"—namely, linked timestamping, digital cash, proof-of-work, Byzantine fault tolerance, and using public keys as identities. Taken separately, each of these building blocks had been under development since the 1980s, but no one had ever thought of putting them together in such a creative way to solve problems that scholars of computer science, network engineering, and cryptography had been struggling with for decades. Thus, we would argue that Bitcoin constitutes a form of architectural innovation (Henderson and Clark 1990) and represents a typical situation wherein a breakthrough is achieved by recombining existing components in previously unforeseen ways, rather than by coming up with a radically new standalone component (Hargadon and Sutton 1997).

Unlike commentator #3 though, we believe that DAOs do enable new forms of task division (e.g., since Bitcoin has no managers, decision-making is instead modularized and distributed), new forms of task allocation (e.g., by blurring the "distinction between 'owners', 'contributors', and 'users'", as explained by commentator #1), and new ways of rewarding members (e.g., by removing subjective evaluation and promotion by managers, and instead making rewards-related rules transparent in the software code).

As noted by commentator #1, Bitcoin is unlikely to become the dominant design for future DAOs. It is but the first instance of an early-stage technological paradigm, and waves of innovation are already improving on its initial design elements (e.g., directed acyclic graphs, Lee 2018). Commentator #1 adds that DAOs today are "competing to institutionalize ways of creating trust among strangers that does not depend on trusted intermediaries." We agree and would contend that this represents a major shift away from the kind of capitalism that emerged in the seventeenth century around of the creation of powerful centralized intermediaries such as the stock exchange, the central bank, and various clearing and settlement organizations. Fundamentally, blockchain technology could lose much of its potential for disintermediation if it were not organized within a distributed setting such as a DAO. We believe that DAOs, at a structural level, are *organizationally* different from the firms we have encountered in the past and have the potential to alter the nature of corporate capitalism as we have known it for the past 400 years.

Finally, we cannot but agree with commentator #3 and commentator #1 that "distributed ledgers enable DAOs but will also find many applications inside more traditional organizations." In fact, as we write these lines, decentralized public blockchains like Bitcoin already co-exist with private distributed ledgers implemented within and across traditional firms—the TradeLens platform, launched by shipping giant Maersk with IBM, is a case in point (Allison 2018). By analogy, what we see now, and will keep seeing in the foreseeable future, is the co-existence of an "Internet" of public blockchains, so to speak, and of various "Intranets" made of private corporate ledgers. And we will see DAOs compete against traditional firms, much like Bitcoin has been competing with Western Union in the global remittances industry.

To conclude, we would like to point out that the rise of DAOs in the real world is accompanied, in academic circles, by the rise of "cryptoeconomics," a nascent (inter)-discipline examining how decentralized networks and tokens can incentivize collective value creation. Imagine, for instance, that users of a social network had to stake tokens representing value to be able to post a video. If that video turns out to be fake news or hate speech, the user loses her stake. If it turns out to be content valuable to others and becomes viral, the user gets rewarded with additional tokens. Similarly, users who help police the network by flagging hate speech get rewarded, and users who act as trend spotters by noticing viral content before it becomes viral get rewarded too. Using cryptocurrency tokens to create this kind of incentives could help mitigate some of the issues currently faced by, say, Facebook, by disincentivizing harmful behavior and giving users ownership of their personal data (Naughton, 2018). Determining the cryptographic, governance, and economic rules for creating, distributing, and exchanging the tokens to obtain the desired collective outcomes is the subject of cryptoeconomics. It draws on various disciplines, including behavioral economics, social psychology, game theory, network and computer engineering, and cryptography.

The rise of cryptoeconomics represents an exciting development. It will give management and organizational scholars a complementary toolkit to research the world of DAOs with the necessary caution and skepticism that should accompany future scholarly investigations of this fascinating phenomenon.

Endnotes

[1] Thus, the term "bitcoin" sometimes refers to the tokens, to the network, to the protocol/software, or to all three elements at once (i.e. the entire payment system).

[2] Daniel Larimer, founder of Bitshare, first coined the term "decentralized autonomous corporation" (DAC). The name DAC was later broadened as DAO by Vitalik Buterin (2014), co-founder of Ethereum and Bitcoin Magazine, to include varying forms of blockchain-based organizations.

[3] While some industry experts prefer the term "distributed organization" over DAO, we opted for DAO to avoid confusion, since "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).

[4] Miners compete to earn "free" tokens for their efforts, though Bitcoin is designed so that in the future they will be compensated more directly by transaction fees.

[5] Lamport, L., Shostak, R., Pease, M. (1982). "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems 4(3): 382–401.

[6] For the example of the "Long Island Ice Tea Company" changing their name to "Long Blockchain" See https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain (accessed 04 June 2018).

[7] See https://www.thelocal.se/20180115/sweden-predicted-to-become-first-country-with-own-cryptocurrency (accessed 04 June 2018).

Acknowledgements

We thank Associate Editors Dr. Phanish Puranam and Dr. Dorthe Døjbak Håkonsson for providing constructive feedback throughout the revision process. This work was supported by the Social Sciences and Humanities Research Council (grant# 430-2015-0670), the Ontario Government (grant# R4905A06), the CryptoEconomics Lab, and the Scotiabank Digital Banking Lab at Ivey Business School. Karim Lakhani gives thanks to Bunty Aggarwal, Helge Klapper, and Phanish Puranam for intellectual sparring. All remaining flaws are solely his.

Funding

This work was supported by the Social Sciences and Humanities Research Council (grant# 430-2015-0670), the Ontario Government (grant# R4905A06), the Scotiabank Digital Banking Lab, and the CryptoEconomics Lab (both at Ivey Business School).

Availability of data and materials

All data and material cited here are from publicly available sources.

Authors' contributions

YH was responsible for the conception, design, drafting, and revising of the manuscript. JV contributed to revising and editing the manuscript. All authors read and approved the final manuscript.

Authors' information

Dr. YH is an Assistant Professor of Innovation and Entrepreneurship at Imperial College Business School, Imperial College London, UK. Dr. JV is an Associate Professor of Strategy at Ivey Business School, Western University, Canada.

Competing interests

The authors declare that they have no competing interests. They only held negligible amounts of bitcoin at the time of writing, which they use primarily during teaching workshops.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Imperial College Business School, Imperial College London, South Kensington Campus, Exhibition Road, London SW7 2AZ, UK. [2]Ivey Business School, Western University, 1255 Western Road, London, ON N6G 0N1, Canada.

Received: 31 October 2018 Accepted: 8 November 2018
Published online: 30 November 2018

References

Allison, I (2018) 94 Companies join IBM and Maersk's blockchain supply chain. https://www.coindesk.com/90-companies-join-ibm-and-maersks-blockchain-supply-chain/. Accessed 12 Aug 2018

Buterin, V (2014) DAOs, DACs, DAs and more: An incomplete terminology guide. Available via Ethereum Blog. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. Accessed 15 Feb 2017

Colfer LJ, Baldwin CY (2016) The mirroring hypothesis: theory, evidence, and exceptions. Ind Corp Chang 25(5):709–738

Davidson S, De Filippi P, Potts J (2016a) Disrupting governance: the new institutional economics of distributed ledger technology. SSRN: http://ssrn.com/abstract=2811995. Accessed 01 Aug 2016

Davidson S, De Filippi P, Potts J (2016b) Economics of blockchain. Available via SSRN: http://ssrn.com/abstract=2744751. Accessed 01 Aug 2016

Dietz J, Xethalis G, De Filippi P, Hazard J (2016) Model distributed collaborative organizations. Stanford Working Group Accessed 01 Aug 2016

Durand R, Vergne JP (2013) The pirate organization: lessons from the fringes of capitalism. Cambridge: Wiley,

Franco P (2014) Understanding bitcoin: cryptography, engineering and economics. Wiley/the Wiley finance series (book), West Sussex, p 1

Gencer AE, Basu S, Eyal I, van Renesse R, Sirer EG (2018). Decentralization in Bitcoin and Ethereum Networks. *arXiv preprint arXiv:1801.03998*

Hargadon A, Sutton R (1997) Technology brokering and innovation in a product development firm. Adm Sci Q 42(4):716–749

Henderson R, Clark K (1990) Architectural innovation: the reconfiguration of existing product technologies and the failure of established firms. Adm Sci Q 35(1):9–30

Hinds PJ, Kiesler S (2002) Distributed work. MIT Press, Cambridge

Hsieh YY, Vergne JP, Wang S (2018) 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

Iansiti M, Lakhani KR (2017) The truth about blockchain. Harv Bus Rev 95(1):118–127

Larimer, D (2013) Overpaying for security: the hidden costs of Bitcoin. https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security#.UjtiUt9xy0w. Accessed 01 Apr 2017

Lee GK, Cole RE (2003) From a firm-based to a community-based model of knowledge creation: the case of the Linux kernel development. Organ Sci 14:633–649

Lee, S (2018) Explaining directed acylic graph (DAG), the real Blockchain 3.0. https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#16fa43d3180b. Accessed 14 Aug 2018

Lopp, J (2016) Bitcoin: the trust anchor in a sea of blockchains. Available vis Coindesk. http://www.coindesk.com/bitcoin-the-trust-anchor-in-a-sea-of-blockchains/. Accessed 02 Oct 2016

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. New York.

Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, New Jersey

Narayanan, A, Clark, J (2017) Bitcoin's academic pedigree. https://cacm.acm.org/magazines/2017/12/223058-bitcoins-academic-pedigree/fulltext#comments. Accessed 12 Aug 2018

Naughton, J (2018) How can Facebook change when it exists to exploit personal data? https://www.theguardian.com/commentisfree/2018/mar/25/forget-bit-players-facebook-brought-scandal-on-itself. Accessed 14 Aug 2018

Okhuysen GA, Bechky BA (2009) Coordination in organizations: an integrative perspective. Acad Manag Ann 3(1):463–502

O'Mahony S, Lakhani KR (2011) Organizations in the shadow of communities. In: Communities and organizations. Emerald Group Publishing Limited, pp 3–36

O'Mahony S, Ferraro F (2007) The emergence of governance in an open source community. Acad Manag J 50(5):1079–1106

Orlikowski WJ (2002) Knowing in practice: enacting a collective capability in distributed organizing. Organ Sci 13(3):249–273

Puranam P, Alexy O, Reitzig M (2014) What's "new" about new forms of organizing? Acad Manag Rev 39(2):162–180

The 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 15 April 2017

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 Accessed 01 Aug 2016

Vigna P, Casey MJ (2015) The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order. St. Martin's Press

Von Krogh G, Spaeth S, Lakhani KR (2003) Community, joining, and specialization in open source software innovation: a case study. Res Policy 32(7):1217–1241

Wang S, Vergne JP (2017) Buzz factor or innovation potential: what explains cryptocurrencies' returns? PLoS One http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0169556

West J, O'mahony S (2008) The role of participation architecture in growing sponsored open source communities. Ind Innov 15(2):145–168

Wu T (2011) The master switch: the rise and fall of information empires. Vintage Books, New York

Yermack D (2017) Corporate governance and blockchains. Rev Financ 21(1):7–31