Influential Article Review - How the Bitcoin Caused the Emergence of Autonomous Organizations

Carmen Ferguson

Floyd Buchanan

Wayne Barnett

This paper examines technology. We present insights from a highly influential paper. Here are the highlights from this paper: 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. For our overseas readers, we then present the insights from this paper in Spanish, French, Portuguese, and German.

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

SUMMARY

- 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 subculture 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 . 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 ; 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. 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.

HIGHLY INFLUENTIAL ARTICLE

We used the following article as a basis of our evaluation:

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design, 7(1), 1–16.

This is the link to the publisher's website:
https://jorgdesign.springeropen.com/articles/10.1186/s41469-018-0038-1

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.Footnote1

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).Footnote2 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).Footnote3 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 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 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 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.

CONCLUSION

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.

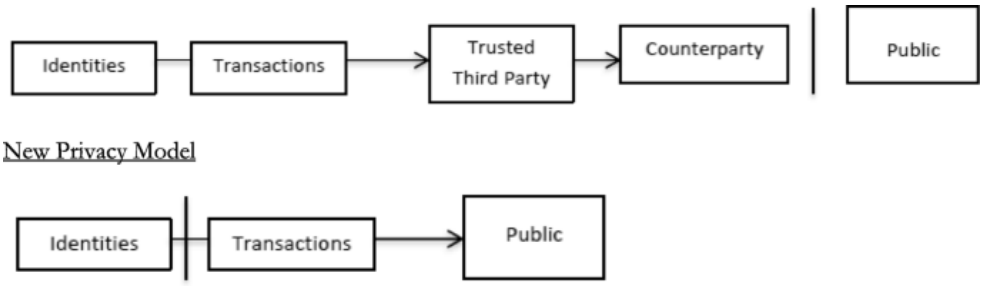
Finally, we cannot but agree with commentator #3 and commentator #1 that "distributed ledgers enable DAOs but will also find many applications inside more traditional organizations." In fact, as we write these lines, decentralized public blockchains like Bitcoin already co-exist with private distributed 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.

APPENDIX

FIGURE 1
TRADITIONAL PRIVACY MODEL VS. THE BITCOIN PRIVACY MODEL



(Adopted from Nakamoto 2008)

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.

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.

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
O'Mahony S, Ferraro F (2007) The emergence of governance in an open source community. Acad Manag J 50(5):1079–1106
O'Mahony S, Lakhani KR (2011) Organizations in the shadow of communities. In: Communities and organizations. Emerald Group Publishing Limited, pp 3–36
Okhuysen GA, Bechky BA (2009) Coordination in organizations: an integrative perspective. Acad Manag Ann 3(1):463–502

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

TRANSLATED VERSION: SPANISH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUCIDA: ESPAÑOL

A continuación se muestra una traducción aproximada de las ideas presentadas anteriormente. Esto se hizo para dar una comprensión general de las ideas presentadas en el documento. Por favor, disculpe cualquier error gramatical y no responsabilite a los autores originales de estos errores.

INTRODUCCIÓN

¿Qué es Bitcoin?

Bitcoin es un código de software de código abierto que implementa un sistema de pago en efectivo digital descentralizado, punto a punto que no requiere ningún intermediario de confianza para operar (por ejemplo, bancos o compañías de pago). El Libro Blanco Bitcoin fue publicado en 2008 por un desarrollador (o equipo de desarrollo) bajo el seudónimo Satoshi Nakamoto, y pronto fue seguido por la primera "moneda" creada en forma de un registro digital en 2009. En el momento de la escritura (octubre de 2017), Bitcoin alcanzó otro precio récord de más de $4400, formando una economía de $73 mil millones.

Inicialmente, el diseño de Bitcoin tenía como objetivo resolver las ineficiencias inherentes y los problemas de agencia derivados del modelo bancario intermedio y centralizado. Por lo general, para realizar una transferencia bancaria internacional entre, por ejemplo, Canadá y China, el dinero pasa por cuatro bancos diferentes (incluidos dos bancos "corresponsales"), dos sistemas nacionales de pagos y un servicio de liquidación internacional (por ejemplo, SWIFT). Un pago internacional estándar tarda entre 3 y 15 días hábiles en completarse, dependiendo del país de destino, e involucra a múltiples agentes como cajeros bancarios, empleados y gerentes de las instituciones financieras mencionadas anteriormente. Se aplican tasas bancarias y tipos de cambio caros.

Por el contrario, Bitcoin se distribuye en el ciberespacio a través de miles de nodos de red, y es inherentemente sin fronteras. Los pagos son validados y actualizados por la red cada 10 min. No se requieren intermediarios (por ejemplo, no se requieren bancos corresponsales). No hay comisiones bancarias para las transacciones, pero los usuarios normalmente pagan una pequeña cuota a los validadores de pago (conocidos como "mineros", que se discutirán más adelante). Mientras que para una transferencia internacional de $5000, un cableado bancario cobraría una tarifa de alrededor de $125, se esperaría una tarifa de alrededor de $1 por una transferencia Bitcoin. No es de extrañar, que Bitcoin es visto como un disruptor potencialmente significativo del sistema financiero actual basado en la banca. Nota al pie de página1

Bitcoin como un Decentralizado Unaoonía Organización

Bitcoin "ejecuta un sistema de pago... Emplea subcontratistas que son mineros... Pagado con las acciones de bitcoin recién emitidas en sí misma" (Vigna y Casey 2015, p. 229, citando a Larimer 2013). Footnote2 El sistema Bitcoin comparte así las cuatro características principales comunes a todas las conceptualizaciones de "organizaciones": es un "sistema multiagente [...] Con límites identificables y [un] propósito [...] Hacia el cual los esfuerzos de los agentes constituyentes hacen una contribución" (Puranam 2017, p. 6). Pero a diferencia de las organizaciones tradicionales, Bitcoin no tiene un CEO o un equipo de alta dirección, sino desarrolladores que "escriben el reglamento", es decir, definen reglas de gobierno para el programa (Narayanan et al. 2016, págs. 173–175). Bitcoin no tiene sedes, subsidiarias o empleados, sino una red distribuida de usuarios y mineros que recopilan, verifican y actualizan transacciones en un libro mayor público compartido que es públicamente auditable. Las decisiones sobre las modificaciones de código se toman a través de procesos de votación democrática basados en la comunidad, respaldados por la potencia informática de los mineros para su implementación (Narayanan et al. 2016, págs. 173 a 175).

Dos innovaciones significativas sustentan Bitcoin: una tecnológica, a saber, la tecnología de contabilidad pública y distribuida llamada "blockchain", que mantiene de forma segura un registro inmutable de todas las transacciones de los usuarios, y una innovación organizativa, a saber, la existencia de una red abierta de usuarios con roles y derechos especiales llamados "mineros", que prestan poder informático para asegurar la red a cambio de bitcoins recién acuñados y derechos de voto con respecto a futuras revisiones de protocolos (Davidson et al. , 2016b).

Estas innovaciones han llevado a algunos expertos de la industria a concebir el sistema Bitcoin como la primera implementación real de un nuevo tipo de organización llamada "organización autónoma descentralizada" (en adelante, DAO). Después de un trabajo previo, definimos a los daos como organizaciones no jerárquicas que realizan y registran tareas rutinarias en una red pública peer-to-peer, criptográficamente segura, y confiamos en las contribuciones voluntarias de sus partes interesadas internas para operar, administrar y evolucionar la organización a través de un proceso de consulta democrática (Valkenburgh et al. 2015; Dietz et al. 2016). Los DAO de Footnote3 coordinan tareas rutinarias a través de rutinas criptográficas (a diferencia de las rutinas humanas). El código abierto define reglas para que los mineros acuerden un historial compartido de transacciones registradas de forma segura y redundante entre nodos de red, con el fin de evitar tener un único punto de error (Nakamoto 2008). Mientras que Bitcoin fue la primera instancia en ser identificado como un DAO, unos pocos cientos más se han creado desde 2009 (por ejemplo, Ethereum, Litecoin).

Bitcoin vs. banks

Bitcoin representa un sustituto parcial de los bancos, aunque con diferencias notables.

En primer lugar, no se puede abrir una cuenta bancaria sin proporcionar una serie de documentos de identificación oficiales, que en el mundo en desarrollo a menudo impiden el acceso a la banca. Por el contrario, cualquier persona puede convertirse en un usuario de Bitcoin y obtener libremente una dirección Bitcoin seudónima (es decir, análoga a una cuenta bancaria) no vinculada ex ante a una identidad del mundo real. En esencia, una dirección Bitcoin es una clave pública vinculada criptográficamente a una clave privada que actúa como una contraseña para gastar fondos. Esto permite un nuevo modelo de privacidad que separa la identidad de las transacciones (Nakamoto 2008). La barra vertical de la Fig. 1 demuestra dónde Bitcoin rompe el flujo de información en comparación con los bancos.

En segundo lugar, a nivel agregado, los bancos tradicionales almacenan historiales de transacciones de manera centralizada. Los usuarios sólo pueden ver sus estados de cuenta personales y deben confiar en que su información está protegida de los ciberataques y la mala conducta de los empleados. Tradicionalmente, los bancos emplean a los empleados bancarios para procesar los pagos. Los agentes humanos son propensos a problemas de agencia que pueden conducir a mala conducta como el robo. El costo de pagar a los agentes humanos tampoco es trivial. Con Bitcoin, todas las transacciones se registran pública y electrónicamente en el "blockchain" inmutable almacenado de forma distribuida en miles de nodos de red, lo que facilita el mantenimiento de los registros y es poco probable que los ciberataques tengan éxito (porque la información sobre las transacciones en este caso no se mantiene en una ubicación central). La tecnología blockchain proporciona las copias multisédi de "ledgers", que son realmente agregaciones de transacciones anteriores (por ejemplo, como un extracto de cuenta bancaria). También proporciona cifrado para validar transacciones como válidas o no válidas (por ejemplo, como el dispositivo de seguridad personal que utilizamos actualmente para la banca en línea, que generan una firma específica de transacción única basada en una clave personal).

Mientras que los bancos evitan el doble gasto comprobando la suficiencia de fondos en un servidor centralizado, en un sistema peer-to-peer como Bitcoin, los beneficiarios no pueden verificar si los pagadores todavía tienen los fondos que dicen tener debido a retrasos impredecibles en la red (por ejemplo, un correo electrónico enviado ahora puede llegar a su destinatario antes de que otro correo electrónico se envíe un minuto antes). Para resolver este problema, Bitcoin se basa en rutinas criptográficas para verificar, marca de tiempo y ordenar transacciones de una manera no reversible, evitando así la necesidad de reconciliación humana. Este proceso se denomina "minería". La idea clave es que alguien en la red va a marcar legítimamente un bloque de transacciones, pero no podemos predecir quién será (por ejemplo, reemplazar a un empleado de banco, que puede ser corrompido a sellos de tiempo falsos, con un sistema que no se puede corromper).

Bitcoin "contrata" a los mineros para procesar transacciones de esta manera a través de un proceso de "contabilidad competitiva" (Yermack 2017). La minería es un proceso mediante el cual nodos de red específicos ("mineros") organizan nuevas transacciones en una secuencia, y las marca el tiempo resolviendo un rompecabezas: adivinando un número arbitrariamente largo después de hacer miles de millones de conjeturas aleatorias. El proceso de conjetura se puede hacer más rápido mediante la confirmación de más potencia de computación a la red. Por lo tanto, la probabilidad de un minero de ser capaz de proporcionar la "prueba de trabajo" necesaria para actualizar el libro mayor es proporcional a la potencia de cálculo que controla. La potencia informática comprometida cada 10 minutos a los bloques de transacciones registradas en el libro mayor se acumula y constituye una barrera para la piratería, lo que hace prácticamente imposible editar los registros de transacciones anteriores contenidos en la cadena de bloques (es decir, la prueba de trabajo tendría que ser completamente rehecho por cada bloque agregado después del editado, que es demasiado intensivo computacionalmente y demasiado costoso para lograr). Los mineros son recompensados en Bitcoin por su trabajo, que implica costos en hardware y electricidad, según el protocolo Bitcoin.

Mecanismos de consenso: soluciones novedosas a los problemas universales de organización

Mientras que la minería organiza el procesamiento de pagos Bitcoin, "los seres humanos primero deben decidir qué protocolo ejecutar antes de que las máquinas puedan hacerlo cumplir (Lopp 2016)". Para distinguir la lógica de la cadena de bloques de su proceso de gobierno y re-diseño, definimos el consenso de la máquina como el proceso por el cual blockchain produce un acuerdo (ayudado por los esfuerzos de los mineros) sobre el orden de las transacciones a través de la marca de tiempo creada por los mineros logrando adivinar un número aleatorio; y el consenso social como el proceso por el cual los mineros votan sobre las propuestas de actualización de protocolo introducidas por los desarrolladores voluntarios. El consenso de la máquina y el consenso social alimentan el novedoso modelo organizativo de Bitcoin y se integran a través del proceso de minería único basado en la provisión de potencia informática.

Consenso de la máquina: el sistema de pago bitcoin

La minería de prueba de trabajo es un proceso computacionalmente intensivo y altamente redundante que genera ineficiencias en términos de consumo de energía. Pero como resultado, el registro blockchain

no puede ser manipulado con un beneficio. Con el consenso de la máquina, las tareas se asignan en función de los compromisos en potencia informática y se recompensan competitivamente en función del resultado de la minería. Todos los datos relacionados con la minería son auditables públicamente para toda la red. La Tabla 1 muestra cómo Bitcoin como sistema de pago se organiza de manera diferente a los bancos y las organizaciones de pago.

Consenso social: actualizaciones de protocolo

Detrás del sistema de pago Bitcoin está el software blockchain soportado por actualizaciones de protocolo en curso (Wang y Vergne 2017). En términos de gobernanza, el voto de los mineros sobre las propuestas de actualización de protocolos se asemeja a la gestión basada en la comunidad del desarrollo de software de código abierto (OSSD) observado para proyectos como Linux. Alinea las expectativas de las partes interesadas (Lopp 2016) y facilita el intercambio de conocimientos, la resolución de problemas y la realización de resultados colectivos (O'Mahony y Lakhani 2011). Al igual que OSSD, el desarrollo de software Bitcoin también es de código abierto, descentralizado y basado en la comunidad. Las comunidades Bitcoin de desarrolladores de software voluntarios colaboran en una red no jerárquica y se auto-seleccionan en tareas y roles basados en la experiencia y las preferencias. Con el tiempo, un equipo de desarrolladores principales de Bitcoin se ha formado y se ha vuelto cada vez más influyente en la comunidad, a pesar de que su trabajo no es financiado por una organización centralizada, sino por un programa de patrocinio que se basa en donaciones.

La principal novedad organizativa de Bitcoin en comparación con OSSD es que además de los desarrolladores, los mineros juegan un papel igualmente importante en las modificaciones de protocolo. Específicamente, el software Bitcoin se actualiza a través de propuestas de mejora de Bitcoin (bips), que son documentos de diseño que proponen nuevas características, cambios o procesos para el protocolo. Los BIP permiten a los desarrolladores hacer propuestas sobre las actualizaciones de software que los mineros deben votar para desencadenar la implementación. Las propuestas son revisadas primero por los editores del BIP, y los mineros luego incluyen un voto "sí" o "no" en un bloque durante el período de votación (por ejemplo, 100 bloques a partir de hoy, a saber, un período de 1000 minutos). El poder de votación es proporcional a la potencia informática que un minero contribuye a la red. Un cambio de código sólo se implementará cuando se obtenga una mayoría del 55% para una propuesta determinada (Franco 2014, p. 90). La Tabla 2 compara el desarrollo de software Bitcoin con OSSD a lo largo de cuatro dimensiones principales de organización: división de tareas, asignación de tareas, distribución de recompensas y flujo de información (Puranam et al. 2014).

La verdadera novedad organizativa de Bitcoin radica en cómo la minería determina la división de tareas (basada en la contribución de potencia informática), la asignación de tareas y la distribución de recompensas (a través de la contabilidad competitiva) y los flujos de información (en la cadena de bloques y en la red). Mientras que la integración de tareas en entornos tradicionales se centra en reglas y procesos diseñados en gran parte por los gerentes (Okhuysen y Bechky 2009), con Bitcoin, el consenso de la máquina (por ejemplo, la contabilidad competitiva) y el consenso social (por ejemplo, la votación) se coordinan a través de los mineros, una nueva clase de partes interesadas.

Los mineros consienten jugar por el libro de reglas, pero pueden votar para cambiarlo usando la influencia derivada de su poder de computación. Sin embargo, es importante tener en cuenta que el código Bitcoin no asume el problema de los costos de la agencia. Más bien, Bitcoin se ocupa explícitamente de estos problemas de larga data mediante la incorporación de incentivos de contrapeso en el código, haciendo que el sistema de pago sea incorruptible.

A diferencia de los contextos de OSSD, Bitcoin se basa en una comunidad mixta de desarrolladores voluntarios y mineros pagados que revisan conjuntamente el diseño de la organización a través de bips. En pocas palabras, Bitcoin ofrece una solución novedosa a "los problemas universales de organización" (Puranam et al. 2014) al involucrar a una nueva clase de partes interesadas, incentivada tanto por algoritmos de consenso de máquinas como por rutinas de consenso social, con el diseño de una organización cuyos parámetros no pueden ser cambiados unilateralmente por ningún grupo de partes interesadas, y cuyas operaciones rutinarias no pueden ser descarriladas por la mala conducta encubierta de los expertos.

Implementaciones de blockchain similares: criptomonedas

Bitcoin es el primer y más establecido DAO implementado hasta la fecha. Desde Bitcoin, ha habido más de 800 otros daos creados sobre la base de diseños similares, la mayoría de los cuales se consideran "criptomonedas" (es decir, como Bitcoin, permiten el intercambio de valor). En el momento de la escritura, las criptomonedas forman una economía de 110.000 millones de dólares y tienen un impacto real en el mundo. Algunas criptomonedas se desarrollan sobre la base del código fuente Bitcoin (por ejemplo, Litecoin, Namecoin, Dash), mientras que otros comenzaron desde cero con su propio protocolo (por ejemplo, Monero, Ethereum). También han surgido variaciones para abarcar una gama más amplia de aplicaciones que no sean solo pagos, como el registro de dominios descentralizados (Namecoin), los contratos inteligentes (Ethereum) y la privacidad (Monero). La minería de prueba de trabajo ya no es la única manera de lograr el consenso de la máquina, ya que se han desarrollado e implementado en los últimos años esquemas alternativos o complementarios, como la prueba de participación (por la que la prueba de seguridad se basa en la cantidad de criptomonedas que tienen los validadores de pago) o la prueba de quemado (por lo que la red está protegida por validadores que asignan monedas a una dirección insaluable) en los últimos años. Las investigaciones preliminares sugieren que el desempeño de DAO varía con el grado de descentralización de la gobernanza (Hsieh et al. 2018), por lo que comprender cómo diversas formas de consenso entre máquinas y sociales contribuyen al éxito y el fracaso de los daos representa una vía emocionante para futuras investigaciones organizativas.

¿Empresas del futuro?

Las investigaciones indican que el potencial de innovación tecnológica detrás de las criptomonedas se erige como el motor clave de su valor de mercado (Wang y Vergne 2017). Pero, como the Economist (2015) señala con razón, la tecnología blockchain tiene aplicaciones de gran alcance más allá de las criptomonedas y los pagos. De hecho, la organización basada en blockchain y los daos resultantes tienen la capacidad de reemplazar intermediarios centralizados en otras aplicaciones que requieren una coordinación compleja, como el seguimiento de la propiedad de activos, el financiamiento comercial, la provisión de identidad digital, la trazabilidad de la cadena de suministro y más. Además, en los últimos 3 años, más de 50 nuevas empresas recibieron financiación semilla utilizando "ofertas iniciales de monedas" impulsadas por blockchain, evitando así, al menos en parte, el uso de intermediarios capitalistas de riesgo para obtener financiación más rápido y en valoraciones más favorables (por ejemplo, en 2014, Ethereum recaudó $18.4 millones en pocos días y ahora está valorado en $34 mil millones). Los daos están en aumento, y es un momento emocionante para los académicos de la gerencia y la organización para abordar este fenómeno emergente con nueva teoría e investigación empírica sólida.

CONCLUSIÓN

En consonancia con el espíritu de la serie Organization Zoo, examinamos las características de diseño desconcertantes e innovadoras de una organización muy especial (Bitcoin) y argumentamos que allanarán el camino para nuevas formas de organización. Tentativamente, propusimos la etiqueta "organización autónoma descentralizada" (DAO) para caracterizar teóricamente lo que está en juego con Bitcoin y otras organizaciones comparables. Agradecemos la oportunidad de poner en primer plano lo que bien podría ser la innovación organizativa más emocionante del siglo XXI (daos) y por los comentarios perspicaces proporcionados por los tres comentaristas.

Estamos de acuerdo con el comentarista #1 que, desde la perspectiva de la beca de gestión, "cryptocurrencies [...] Están en la raíz de la organización, no de dinero. Y, como señaló el comentarista #2, Bitcoin y su blockchain "proporcionan una visión del futuro de nuevas formas organizativas que podrían ser altamente descentralizadas y diseñadas sobre diferentes principios." Pero matiza su afirmación esbozando tres advertencias: la concentración observada de las operaciones mineras, la dificultad práctica de descentralizar la gobernanza de DAO y el riesgo de monopolización que normalmente se observa en las industrias de la información sujetas a fuertes efectos de la red: piense en AT&T, Microsoft, Google o Facebook (véase Wu 2011 y Durand y Vergne 2013 para obtener perspectivas históricas complementarias sobre este fenómeno). La comunidad es muy consciente de estas limitaciones, y ya se están desarrollando soluciones para abordarlas: la sustitución de la minería de prueba de trabajo por mecanismos de consenso

alternativos para mitigar la concentración no deseada, la implementación de la gobernanza directamente en la cadena de bloques para evitar la aparición de una autoridad externa con demasiada influencia en la evolución del protocolo blockchain (un fenómeno llamado "gobernanza en cadena"), y la creación de protocolos de interoperabilidad para facilitar la comunicación a través de blockchains y prevenir un efecto ganador. Tenga en cuenta, sin embargo, que el dominio de una sola cadena de bloques no sería demasiado problema, siempre y cuando esa cadena de bloques permanezca descentralizada por el diseño.

Estamos de acuerdo con el comentarista #3 que la novedad tecnológica que sustenta Bitcoin es un fenómeno más matizado que lo que normalmente se representa en cuentas de medios exageradas. Como lo demostraron Narayanan y Clark (2017), "Bitcoin fue inusual y exitoso no porque estuviera a la vanguardia de la investigación sobre cualquiera de sus componentes, sino porque combinaba viejas ideas de muchos campos previamente no relacionados", es decir, marca de tiempo vinculada, dinero digital, prueba de trabajo, tolerancia a errores bizantinos y uso de claves públicas como identidades. Tomados por separado, cada uno de estos bloques de construcción había estado en desarrollo desde la década de 1980, pero nadie había pensado en juntarlos de una manera tan creativa para resolver problemas que los estudiosos de la informática, la ingeniería de redes y la criptografía habían estado luchando durante décadas. Por lo tanto, argumentamos que Bitcoin constituye una forma de innovación arquitectónica (Henderson y Clark 1990) y representa una situación típica en la que se logra un avance mediante la recombinación de componentes existentes de maneras anteriormente imprevistas, en lugar de llegar a un componente independiente radicalmente nuevo (Hargadon y Sutton 1997).

Sin embargo, a diferencia de los #3 comentaristas, creemos que los DAO permiten nuevas formas de división de tareas (por ejemplo, dado que Bitcoin no tiene gerentes, la toma de decisiones se modulará y distribuye en su lugar), nuevas formas de asignación de tareas (por ejemplo, difuminando la "distinción entre 'propietarios', 'colaboradores' y 'usuarios'", como explican los comentaristas #1), y nuevas formas de recompensar a los miembros (por ejemplo, eliminando la evaluación subjetiva y la promoción por parte de los gerentes, y en su lugar haciendo que las reglas relacionadas con las recompensas sean transparentes en el código de software).

Como señaló el comentarista #1, es poco probable que Bitcoin se convierta en el diseño dominante para los futuros daos. No es más que la primera instancia de un paradigma tecnológico en etapa temprana, y las oleadas de innovación ya están mejorando en sus elementos de diseño iniciales (por ejemplo, gráficos acíclicos dirigidos, Lee 2018). El comentarista #1 añade que los daos de hoy en día están "compitiendo para institucionalizar formas de crear confianza entre extraños que no dependen de intermediarios de confianza". Estamos de acuerdo y contendríamos que esto representa un cambio importante del tipo de capitalismo que surgió en el siglo XVII en torno a la creación de poderosos intermediarios centralizados como la bolsa de valores, el banco central y varias organizaciones de compensación y liquidación. Fundamentalmente, la tecnología blockchain podría perder gran parte de su potencial de desintermediación si no estuviera organizada dentro de un entorno distribuido como un DAO. Creemos que los daos, a nivel estructural, son organizacionalmente diferentes de las empresas que hemos encontrado en el pasado y tienen el potencial de alterar la naturaleza del capitalismo corporativo tal como lo hemos conocido durante los últimos 400 años.

Por último, no podemos sino estar de acuerdo con los #3 comentaristas y comentaristas #1 que "los libros de contabilidad distribuidos permiten a los DAO, pero también encontrarán muchas aplicaciones dentro de las organizaciones más tradicionales". De hecho, a medida que escribimos estas líneas, blockchains públicas descentralizadas como Bitcoin ya coexisten con libros de contabilidad distribuidos privados implementados dentro y a través de las empresas tradicionales: la plataforma tradelens, lanzada por el gigante naviero Maersk con IBM, es un ejemplo (Allison 2018). Por analogía, lo que vemos ahora, y seguiremos viendo en un futuro previsible, es la coexistencia de una "Internet" de cadenas de bloques públicas, por así decirlo, y de varias "Intranets" hechas de libros de contabilidad corporativas privadas. Y veremos que los daos compiten contra las empresas tradicionales, al igual que Bitcoin ha estado compitiendo con Western Union en la industria global de las remesas.

Para concluir, nos gustaría señalar que el auge de los daos en el mundo real está acompañado, en los círculos académicos, por el auge de la "criptoeconomía", una naciente (inter)disciplina que examina cómo

las redes descentralizadas y los tokens pueden incentivar la creación de valor colectivo. Imagine, por ejemplo, que los usuarios de una red social tenían que apostar tokens que representaban valor para poder publicar un vídeo. Si ese video resulta ser noticias falsas o discursos de odio, el usuario pierde su apuesta. Si resulta ser contenido valioso para otros y se vuelve viral, el usuario recibe recompensas con tokens adicionales. Del mismo modo, los usuarios que ayudan a controlar la red marcando el discurso de odio se recompensan, y los usuarios que actúan como observadores de tendencias al notar contenido viral antes de que se vuelva viral también se recompensan. El uso de tokens criptomoneda para crear este tipo de incentivos podría ayudar a mitigar algunos de los problemas a los que se enfrentan actualmente, por ejemplo, Facebook, desincentivando el comportamiento dañino y dando a los usuarios la propiedad de sus datos personales (Naughton, 2018). Determinar las reglas criptográficas, de gobierno y económicas para crear, distribuir e intercambiar los tokens para obtener los resultados colectivos deseados es objeto de criptoeconomía. Se basa en varias disciplinas, incluyendo economía conductual, psicología social, teoría de juegos, ingeniería de redes e informática, y criptografía.

El auge de la criptoeconomía representa un desarrollo emocionante. Dará a los académicos de la dirección y de la organización un conjunto de herramientas complementarios para investigar el mundo de los daos con la precaución y el escepticismo necesarios que deben acompañar las futuras investigaciones académicas de este fascinante fenómeno.

TRANSLATED VERSION: FRENCH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUITE: FRANÇAIS

Voici une traduction approximative des idées présentées ci-dessus. Cela a été fait pour donner une compréhension générale des idées présentées dans le document. Veuillez excuser toutes les erreurs grammaticales et ne pas tenir les auteurs originaux responsables de ces erreurs.

INTRODUCTION

Qu'est-ce que Bitcoin?

Bitcoin est un code logiciel open source qui implémente un système de paiement en espèces numérique décentralisé et peer-to-peer qui n'exige aucun intermédiaire de confiance pour fonctionner (par exemple, les banques ou les sociétés de paiement). Le Bitcoin Whitepaper a été publié en 2008 par un développeur (ou une équipe de développement) sous le pseudonyme de Satoshi Nakamoto, et a été bientôt suivi par la toute première « pièce » créée sous la forme d'un disque numérique en 2009. Au moment d'écrire ces lignes (octobre 2017), bitcoin a atteint un nouveau record de plus de 4400 dollars, formant une économie de 73 milliards de dollars.

Initialement, la conception de Bitcoin visait à résoudre les inefficacités inhérentes et les problèmes d'agence découlant du modèle bancaire intermédiaire et centralisé. En règle générale, pour effectuer un virement international entre, disons, le Canada et la Chine, l'argent passe par quatre banques différentes (dont deux banques « correspondantes »), deux systèmes de paiement nationaux et un service de règlement international (p. Ex., SWIFT). Un paiement international standard prend entre 3 et 15 jours ouvrables, selon le pays de destination, et implique plusieurs agents tels que les caissiers de banque, les employés et les gestionnaires des institutions financières susmentionnées. Des frais bancaires et des taux de change coûteux s'appliquent.

En revanche, Bitcoin est distribué dans le cyberespace à travers des milliers de nœuds réseau, et est intrinsèquement sans frontières. Les paiements sont validés et mis à jour par le réseau toutes les 10 minutes. Les intermédiaires ne sont pas requis (p. Ex., aucune banque correspondante n'est requise). Il n'y a pas de

frais bancaires pour les transactions, mais les utilisateurs paient généralement une petite taxe aux validateurs de paiement (connus sous le nom de « mineurs » — à discuter plus loin ci-dessous). Alors que pour un virement international de 5000 $, un câblage bancaire exigerait des frais d'environ 125 $, des frais d'environ 1 $ seraient attendus pour un transfert bitcoin. Il n'est pas étonnant que Bitcoin soit considéré comme un perturbateur potentiellement important du système financier actuel basé sur les banques. Note de bas de page1

Bitcoin comme un Decentralisé Autonomie O Organization

Bitcoin « gère un système de paiement... Emploie des sous-traitants mineurs... Payé avec des actions bitcoin nouvellement émises en soi » (Vigna et Casey 2015, p. 229, citant Larimer 2013). Note de bas de page2 Le système Bitcoin partage ainsi les quatre caractéristiques de base communes à toutes les conceptualisations des « organisations » : il s'agit d'un « système multi-agents [...] Avec des limites identifiables et [un] but [...] Vers lequel les efforts des agents constitutifs contribuent » (Puranam 2017, p. 6). Mais contrairement aux organisations traditionnelles, Bitcoin n'a pas de PDG ou d'équipe de direction, mais plutôt de développeurs qui « écrivent le règlement », c'est-à-dire définissent les règles de gouvernance du programme (Narayanan et al., 2016, pp. 173–175). Bitcoin n'a pas de siège social, de filiales ou d'employés, mais un réseau distribué d'utilisateurs et de mineurs qui collectent, vérifient et mettent à jour les transactions sur un registre public partagé qui est publiquement vérifiable. Les décisions relatives aux modifications du code sont prises par le biais de processus de vote démocratique communautaire, appuyés par le pouvoir de calcul des mineurs pour la mise en œuvre (Narayanan et al., 2016, p. 173 à 175).

Deux innovations importantes sous-tendent Bitcoin : une technologie technologique, à savoir la technologie des registres publics et distribués appelée « blockchain », qui maintient en toute sécurité un dossier immuable de toutes les transactions des utilisateurs, et une innovation organisationnelle, à savoir l'existence d'un réseau ouvert d'utilisateurs ayant des rôles et des droits spéciaux appelés « mineurs », qui prêtent un pouvoir de calcul pour sécuriser le réseau en échange de bitcoins nouvellement frappés et de droits de vote en ce qui concerne les futures révisions de protocole (Davidson et coll. , 2016b).

Ces innovations ont conduit certains experts de l'industrie à concevoir le système Bitcoin comme la première mise en œuvre réelle d'un nouveau type d'organisation appelée « rréation autonome décentralisé » (ci-après, DAO). À la suite de travaux antérieurs, nous définissons les DAO comme des organisations non hiérarchiques qui exécutent et enregistrent des tâches courantes sur un réseau public de pair à pair, cryptographiquement sécurisé, et qui comptent sur les contributions volontaires de leurs parties prenantes internes pour exploiter, gérer et faire évoluer l'organisation par le biais d'un processus de consultation démocratique (Valkenburgh et al., 2015; Dietz et coll. 2016). Les DAO de Bassy3 coordonnent les tâches courantes par le biais de routines cryptographiques (par opposition aux routines humaines). Le code open source définit les règles pour que les mineurs s'entendent sur un historique partagé des transactions enregistrées en toute sécurité et redondantes sur les nœuds réseau, afin d'éviter d'avoir un seul point d'échec (Nakamoto 2008). Alors que Bitcoin a été le premier exemple à être identifié comme un DAO, quelques centaines d'autres ont ensuite été créés depuis 2009 (par exemple, Ethereum, Litecoin).

Bitcoin vs Banks

Bitcoin représente un substitut partiel pour les banques, mais avec des différences notables.

Premièrement, on ne peut pas ouvrir un compte bancaire sans fournir un certain nombre de documents d'identité officiels, ce qui, dans les pays en développement, empêche souvent l'accès aux services bancaires. En revanche, n'importe qui peut devenir un utilisateur de Bitcoin et obtenir librement une adresse Bitcoin pseudonyme (c'est-à-dire analogue à un compte bancaire) non liée ex ante à une identité du monde réel. Essentiellement, une adresse Bitcoin est une clé publique cryptographiquement liée à une clé privée agissant comme mot de passe pour dépenser des fonds. Cela permet un nouveau modèle de confidentialité qui sépare l'identité des transactions (Nakamoto 2008). La barre verticale de la fig. 1 montre où Bitcoin brise le flux d'informations par rapport aux banques.

Deuxièmement, à un niveau global, les banques traditionnelles stockent les historiques des transactions de façon centralisée. Les utilisateurs n'ont qu'à consulter leurs relevés bancaires personnels et doivent avoir confiance que leurs renseignements sont protégés contre les cyberattaques et les inconduites des employés. Traditionnellement, les banques emploient des commis de banque pour traiter les paiements. Les agents

humains sont sujets à des problèmes d'agence qui peuvent conduire à une inconduite comme le vol. Le coût de payer les agents humains n'est pas non plus négligeable. Avec Bitcoin, toutes les transactions sont enregistrées publiquement et électroniquement sur la « blockchain » immuable stockée de manière distribuée sur des milliers de nœuds réseau, ce qui rend les enregistrements plus faciles à entretenir et les cyberattaques peu susceptibles de réussir (parce que les informations sur les transactions dans ce cas ne sont pas conservées dans un seul emplacement central). La technologie blockchain fournit les copies multi-sites de « ledger », qui sont en fait des agrégations de transactions passées (par exemple, comme un relevé de compte bancaire). Il fournit également le chiffrement pour valider les transactions comme valides ou non valides (par exemple, comme le dispositif de sécurité personnelle que nous utilisons actuellement pour les services bancaires en ligne, qui génèrent une signature spécifique à une transaction unique basée sur une clé personnelle).

Alors que les banques empêchent les doubles dépenses en vérifiant la suffisance des fonds dans un serveur centralisé, dans un système peer-to-peer comme Bitcoin, les bénéficiaires ne peuvent pas vérifier si les payeurs ont encore les fonds qu'ils prétendent avoir en raison de retards de réseau imprévisibles (par exemple, un e-mail envoyé maintenant peut atteindre son destinataire avant un autre e-mail envoyé une minute plus tôt). Pour résoudre ce problème, Bitcoin s'appuie sur des routines cryptographiques pour vérifier, horodatager et commander les transactions d'une manière non réversible, évitant ainsi la nécessité d'une réconciliation humaine. Ce processus est appelé « exploitation minière ». L'idée clé est que quelqu'un dans le réseau sera légitimement horodatage un bloc de transactions, mais nous ne pouvons pas prédire qui ce sera (par exemple, le remplacement d'un commis de banque, qui peut être corrompu à de faux horodatages, avec un système qui ne peut pas être corrompu).

Bitcoin « engage » les mineurs pour traiter les transactions de cette manière par le biais d'un processus de « comptabilité compétitive » (Yermack 2017). L'exploitation minière est un processus par lequel des nœuds réseau spécifiques (« mineurs ») organisent de nouvelles transactions en une séquence, et les horodatage en résolvant un puzzle de toutes sortes : en devinant un nombre arbitrairement long après avoir fait des milliards de suppositions aléatoires. Le processus de devinettes peut être rendu plus rapide en consacrant plus de puissance de calcul au réseau. Ainsi, la probabilité d'un mineur de pouvoir fournir la « preuve de travail » requise pour mettre à jour le registre est proportionnelle à la puissance de calcul qu'il contrôle. La puissance de calcul engagée toutes les 10 minutes pour bloquer les transactions enregistrées dans le registre s'accumule et constitue un obstacle au piratage, ce qui rend pratiquement impossible la modification des enregistrements de transactions passés contenus dans la blockchain (c'est-à-dire que la preuve de travail devrait être entièrement refaite pour chaque bloc ajouté après celui modifié, ce qui est trop intensif sur le plan informatique et trop coûteux à réaliser). Les mineurs sont récompensés en Bitcoin pour leur travail, qui implique des coûts dans le matériel et l'électricité, selon le protocole Bitcoin.

Mécanismes de consensus : nouvelles solutions aux problèmes universels de l'organisation

Alors que l'exploitation minière organise le traitement des paiements Bitcoin, « les humains doivent d'abord décider quel protocole fonctionner avant que les machines puissent l'appliquer (Lopp 2016) ». Pour distinguer la logique de la blockchain de son processus de gouvernance et de refonte, nous définissons le consensus machine comme le processus par lequel la blockchain produit un accord (aidé par les efforts des mineurs) sur l'ordre des transactions par le biais de l'horodatage créé par les mineurs réussissant à deviner un nombre aléatoire; et le consensus social comme processus par lequel les mineurs votent sur les propositions de mise à jour du protocole introduites par les développeurs bénévoles. Le consensus des machines et le consensus social alimentent le nouveau modèle organisationnel de Bitcoin et s'intègrent grâce au processus d'exploitation minière unique basé sur la fourniture de puissance de calcul.

Consensus machine : le système de paiement bitcoin

L'exploitation minière de la preuve de travail est un processus intensif et très redondant qui génère des inefficacités en termes de consommation d'énergie. Mais en conséquence, l'enregistrement blockchain ne peut pas être trafiqué à un profit. Avec le consensus des machines, les tâches sont réparties sur la base d'engagements en matière de puissance de calcul, et récompensées de manière compétitive en fonction des résultats de l'exploitation minière. Toutes les données relatives à l'exploitation minière sont publiquement

vérifiables pour l'ensemble du réseau. Le tableau 1 montre comment Bitcoin en tant que système de paiement s'organise différemment des banques et des organisations de paiement.

Consensus social : mises à niveau du protocole

Sous-jacent au système de paiement Bitcoin est le logiciel blockchain pris en charge par les mises à jour du protocole en cours (Wang et Vergne 2017). En termes de gouvernance, le vote des mineurs sur les propositions de mise à jour du protocole ressemble à la gestion communautaire du développement de logiciels open source (OSSD) observée pour des projets tels que Linux. Il aligne les attentes des parties prenantes (Lopp 2016) et facilite le partage des connaissances, la résolution de problèmes et la réalisation des résultats collectifs (O'Mahony et Lakhani 2011). Comme OSSD, le développement de logiciels Bitcoin est également open source, décentralisé et communautaire. Les communautés Bitcoin de développeurs de logiciels bénévoles collaborent dans un réseau non hiérarchique et s'auto-choisissent dans les tâches et les rôles basés sur l'expertise et les préférences. Au fil du temps, une équipe de développeurs Bitcoin de base s'est formée et est devenue de plus en plus influente dans la communauté, même si leur travail n'est pas financé par une organisation centralisée, mais par un programme de parrainage qui repose sur des dons.

La principale nouveauté organisationnelle de Bitcoin par rapport à OSSD est qu'en plus des développeurs, les mineurs jouent un rôle tout aussi important dans les modifications de protocole. Plus précisément, le logiciel Bitcoin est mis à jour par le biais de propositions d'amélioration Bitcoin (BIP), qui sont des documents de conception proposant de nouvelles fonctionnalités, modifications ou processus pour le protocole. Les BIP permettent aux développeurs de faire des propositions sur les mises à jour logicielles sur lesquelles les mineurs doivent voter pour déclencher la mise en œuvre. Les propositions sont d'abord examinées par les rédacteurs en chef du BIP, et les mineurs incluent ensuite un vote « oui » ou « non » dans un bloc pendant la période de vote (p. Ex., 100 blocs à partir d'aujourd'hui, soit une période de 1000 minutes). La puissance de vote est proportionnelle à la puissance de calcul qu'un mineur contribue au réseau. Une modification de code ne sera mise en œuvre que lorsqu'une majorité de 55 % sera obtenue pour une proposition donnée (Franco 2014, p. 90). Le tableau 2 compare le développement de logiciels Bitcoin avec l'ossd dans quatre dimensions essentielles de l'organisation : la division des tâches, l'attribution des tâches, la distribution des récompenses et le flux d'information (Puranam et al., 2014).

La véritable nouveauté organisationnelle de Bitcoin réside dans la façon dont l'exploitation minière détermine la division des tâches (basée sur la contribution de puissance de calcul), l'allocation des tâches et la distribution de récompenses (par le biais d'une comptabilité compétitive) et les flux d'information (sur la blockchain et dans le réseau). Alors que l'intégration des tâches dans les contextes traditionnels se concentre sur les règles et les processus conçus en grande partie par les gestionnaires (Okhuysen et Bechky 2009), avec Bitcoin, le consensus machine (par exemple, la comptabilité concurrentielle) et le consensus social (par exemple, le vote) sont coordonnés par les mineurs, une toute nouvelle classe d'intervenants.

Les mineurs consentent à jouer selon le règlement, mais ils peuvent voter pour le modifier en utilisant l'influence dérivée de leur puissance de calcul. Toutefois, il est important de noter que le code Bitcoin n'assume pas le problème des coûts d'agence. Bitcoin traite explicitement ces problèmes de longue date en incorporant des incitations à contrebalancer dans le code, rendant le système de paiement incorruptible.

Contrairement aux contextes OSSD, Bitcoin s'appuie sur une communauté mixte de développeurs bénévoles et de mineurs rémunérés qui révisent conjointement la conception organisationnelle par le biais de BIP. En d'autres termes, Bitcoin offre une solution nouvelle aux « problèmes universels d'organisation » (Puranam et al.) En impliquant une nouvelle classe d'intervenants, encouragés à la fois par les algorithmes de consensus des machines et les routines de consensus social, avec la conception d'une organisation dont les paramètres ne peuvent être modifiés unilatéralement par aucun groupe d'intervenants, et dont les opérations courantes ne peuvent être déraillées par l'inconduite secrète des initiés.

Implémentations de blockchain similaires : crypto-monnaies

Bitcoin est le premier et le plus établi DAO mis en œuvre à ce jour. Depuis Bitcoin, il y a eu plus de 800 autres DAO créés sur la base de conceptions similaires, dont la plupart sont considérées comme des « crypto-monnaies » (c'est-à-dire, comme Bitcoin, elles permettent l'échange de valeur). Au moment d'écrire ces lignes, les crypto-monnaies forment une économie de 110 milliards de dollars et ont un impact réel sur le monde. Certaines crypto-monnaies sont développées à partir du code source Bitcoin (p. Ex., Litecoin,

Namecoin, Dash), tandis que d'autres ont commencé à partir de zéro avec leur propre protocole (par exemple, Monero, Ethereum). Des variantes ont également émergé pour englober un plus large éventail d'applications autres que les paiements, tels que l'enregistrement de domaine décentralisé (Namecoin), les contrats intelligents (Ethereum), et la vie privée (Monero). L'exploitation minière de la preuve de travail n'est plus le seul moyen d'atteindre un consensus machine, car des régimes alternatifs ou complémentaires tels que la preuve de participation (par lequel la preuve de sécurité est basée sur le montant des crypto-monnaies valides de paiement détiennent) ou la preuve de brûlure (par lequel le réseau est sécurisé par des validateurs allouant des pièces à une adresse non pendable) ont été développés et mis en œuvre ces dernières années. Des recherches préliminaires suggèrent que le rendement du DAO varie en fonction de l'ampleur de la décentralisation de la gouvernance (Hsieh et coll. 2018), de sorte que la compréhension de la façon dont diverses formes de machine et de consensus social contribuent au succès et à l'échec des CAO représente une avenue passionnante pour la recherche organisationnelle future.

Les entreprises du futur ?

La recherche indique que le potentiel d'innovation technologique derrière les crypto-monnaies est le principal moteur de leur valeur marchande (Wang et Vergne 2017). Mais, comme le souligne à juste titre The Economist (2015), la technologie blockchain a des applications de grande envergure au-delà des crypto-monnaies et des paiements. En fait, l'organisation basée sur la blockchain et les ADO qui en résultent ont la capacité de remplacer les intermédiaires centralisés dans d'autres applications nécessitant une coordination complexe telles que le suivi de la propriété des actifs, le financement du commerce, la fourniture d'identité numérique, la traçabilité de la chaîne d'approvisionnement, et plus encore. En outre, au cours des trois dernières années, plus de 50 nouvelles entreprises ont reçu des fonds de démarrage à l'aide d'« offres initiales » alimentées par la blockchain, contournant ainsi, au moins en partie, l'utilisation d'intermédiaires de capital-risque pour obtenir des financements plus rapidement et à des valorisations plus favorables (par exemple, en 2014, Ethereum a levé 18,4 millions de dollars en quelques jours et est maintenant évaluée à 34 milliards de dollars). Les DAO sont à la hausse, et c'est un moment passionnant pour les chercheurs en gestion et en organisation pour aborder ce phénomène émergent avec de nouvelles théories et des recherches empiriques solides.

CONCLUSION

Conformément à l'esprit de la série Organization Zoo, nous avons examiné les caractéristiques de conception déroutantes et novatrices d'une organisation très spéciale (Bitcoin) et avons fait valoir qu'elles ouvriraient la voie à de nouvelles formes d'organisation. Provisoirement, nous avons proposé l'étiquette « organisation autonome décentralisée » (DAO) pour caractériser théoriquement ce qui est en jeu avec Bitcoin et d'autres organisations comparables. Nous sommes reconnaissants de l'occasion qui nous a donné l'occasion de mettre en avant ce qui pourrait bien être l'innovation organisationnelle la plus excitante du xxie siècle (DAO) et pour les commentaires perspicaces fournis par les trois commentateurs.

Nous sommes d'accord avec le commentateur #1 que, du point de vue de la bourse de gestion, « crypto-monnaies [...] Sont à la racine sur l'organisation, pas sur l'argent. Et, comme l'a noté le commentateur #2, Bitcoin et sa blockchain « donnent un aperçu de l'avenir de nouvelles formes organisationnelles qui pourraient être hautement décentralisées et conçues sur des principes différents ». Mais il nuance sa prétention en exposant trois mises en garde : la concentration observée des opérations minières, la difficulté pratique de décentraliser la gouvernance du DAO, et le risque de monopolisation généralement observé dans les industries de l'information soumises à de forts effets de réseau — pensez AT&T, Microsoft, Google ou Facebook (voir Wu 2011 et Durand et Vergne 2013 pour des perspectives historiques complémentaires sur ce phénomène). La communauté est bien consciente de ces limites, et des solutions sont déjà en cours d'élaboration pour y remédier : remplacer l'exploitation minière par des mécanismes de consensus alternatifs pour atténuer les concentrations indésirables, mettre en œuvre la gouvernance directement dans la blockchain pour éviter l'émergence d'une autorité externe ayant trop d'influence sur l'évolution du protocole blockchain (phénomène appelé « gouvernance en chaîne »), et création de protocoles

d'interopérabilité pour faciliter la communication à travers les blockchains et empêcher un effet gagnant-gagnant. Notez, cependant, que la domination d'une blockchain unique ne serait pas trop d'un problème tant que cette blockchain reste décentralisée par la conception.

Nous sommes d'accord avec le commentateur #3 que la nouveauté technologique qui sous-tend Bitcoin est un phénomène plus nuancé que ce qui est généralement représenté dans les comptes de médias surhyped. Comme l'ont démontré Narayanan et Clark (2017), « Bitcoin a été inhabituel et réussi non pas parce qu'il était à la fine pointe de la recherche sur l'un de ses composants, mais parce qu'il combinait de vieilles idées de nombreux domaines auparavant indépendants », à savoir, le timestamping lié, l'argent numérique, la preuve de travail, la tolérance aux défauts byzantins et l'utilisation des clés publiques comme identités. Pris séparément, chacun de ces blocs de construction était en cours de développement depuis les années 1980, mais personne n'avait jamais pensé à les réunir d'une manière si créative pour résoudre des problèmes que les chercheurs de l'informatique, l'ingénierie des réseaux, et la cryptographie avait été aux prises avec des décennies. Ainsi, nous soutiendrons que Bitcoin constitue une forme d'innovation architecturale (Henderson et Clark, 1990) et représente une situation typique dans laquelle une percée est réalisée en recombinant les composants existants de manière imprévue auparavant, plutôt qu'en proposant une composante autonome radicalement nouvelle (Hargadon et Sutton, 1997).

Contrairement aux #3 commentateurs, nous croyons que les DAO permettent de nouvelles formes de division des tâches (p. Ex., Comme Bitcoin n'a pas de gestionnaires, la prise de décision est plutôt modularisée et distribuée), de nouvelles formes d'attribution des tâches (par exemple, en brouillant la « distinction entre les propriétaires », les « contributeurs » et les « utilisateurs », comme l'explique le commentateur #1), et de nouvelles façons de récompenser les membres (par exemple, en supprimant l'évaluation subjective et la promotion par les gestionnaires, et en rendant les règles relatives aux récompenses transparentes dans le code logiciel).

Comme l'a noté le commentateur #1, Bitcoin est peu susceptible de devenir la conception dominante pour les futurs DAO. Ce n'est que le premier exemple d'un paradigme technologique à un stade précoce, et les vagues d'innovation s'améliorent déjà sur ses éléments de conception initiale (par exemple, graphiques acycliques dirigés, Lee 2018). Le commentateur #1 ajoute que les DAO d'aujourd'hui « rivalisent pour institutionnaliser les moyens de créer la confiance entre les étrangers qui ne dépendent pas d'intermédiaires de confiance ». Nous sommes d'accord et nous prétendrions qu'il s'agit d'un changement majeur par rapport au type de capitalisme qui a émergé au xviie siècle autour de la création de puissants intermédiaires centralisés tels que la bourse, la banque centrale et diverses organisations de compensation et de règlement. Fondamentalement, la technologie blockchain pourrait perdre une grande partie de son potentiel de désintermédiation si elle n'était pas organisée dans un cadre distribué comme un DAO. Nous croyons que les DAO, au niveau structurel, sont essentiellement différents des entreprises que nous avons rencontrées dans le passé et ont le potentiel de modifier la nature du capitalisme d'entreprise tel que nous le connaissons depuis 400 ans.

Enfin, nous ne pouvons qu'être d'accord avec le commentateur #3 et commentateur #1 que « les registres distribués permettent aux DAO, mais trouveront également de nombreuses applications au sein d'organisations plus traditionnelles ». En fait, au moment où nous écrivons ces lignes, les blockchains publiques décentralisées comme Bitcoin coexistent déjà avec des registres privés distribués mis en œuvre au sein et à travers les entreprises traditionnelles — la plate-forme tradelens, lancée par le géant du transport maritime Maersk avec IBM, en est un bon exemple (Allison 2018). Par analogie, ce que nous voyons maintenant, et que nous allons continuer à voir dans un avenir prévisible, c'est la coexistence d'un « Internet » de blockchains publiques, pour ainsi dire, et de divers « intranets » faits de registres d'entreprises privés. Et nous verrons les APO concurrencer les entreprises traditionnelles, tout comme Bitcoin a été en concurrence avec Western Union dans l'industrie mondiale des envois de fonds.

Pour conclure, nous tenons à souligner que la montée des AO dans le monde réel s'accompagne, dans les milieux universitaires, de la montée de la « cryptoéconomie », une (inter)discipline naissante qui examine comment les réseaux décentralisés et les jetons peuvent encourager la création de valeur collective. Imaginez, par exemple, que les utilisateurs d'un réseau social ont dû jalonner des jetons représentant la valeur pour être en mesure de poster une vidéo. Si cette vidéo s'avère être de fausses nouvelles ou des

discours de haine, l'utilisateur perd son pieu. S'il s'avère être un contenu précieux pour les autres et devient viral, l'utilisateur est récompensé par des jetons supplémentaires. De même, les utilisateurs qui aident à la police du réseau en signalant les discours haineux sont récompensés, et les utilisateurs qui agissent comme des observateurs de tendance en remarquant le contenu viral avant qu'il ne devienne viral obtenir récompensé aussi. L'utilisation de jetons de crypto-monnaie pour créer ce genre d'incitations pourrait aider à atténuer certains des problèmes auxquels sont actuellement confrontés, par exemple, Facebook, en dissuasiveant les comportements nuisibles et en donnant aux utilisateurs la propriété de leurs données personnelles (Naughton, 2018). La détermination des règles cryptographiques, de gouvernance et économiques pour la création, la distribution et l'échange des jetons pour obtenir les résultats collectifs souhaités fait l'objet de la cryptoéconomie. Il s'appuie sur diverses disciplines, y compris l'économie comportementale, la psychologie sociale, la théorie des jeux, l'ingénierie des réseaux et de l'informatique, et la cryptographie.

L'essor de la cryptoéconomie représente un développement passionnant. Il donnera aux chercheurs en gestion et en organisation une boîte à outils complémentaire pour la recherche dans le monde des AO avec la prudence et le scepticisme nécessaires qui devraient accompagner les futures recherches savantes de ce phénomène fascinant.

TRANSLATED VERSION: GERMAN

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

ÜBERSETZTE VERSION: DEUTSCH

Hier ist eine ungefähre Übersetzung der oben vorgestellten Ideen. Dies wurde getan, um ein allgemeines Verständnis der in dem Dokument vorgestellten Ideen zu vermitteln. Bitte entschuldigen Sie alle grammatikalischen Fehler und machen Sie die ursprünglichen Autoren nicht für diese Fehler verantwortlich.

EINLEITUNG

Was ist Bitcoin?

Bitcoin ist ein Open-Source-Software-Code, der ein dezentrales, Peer-to-Peer-Digital-Cash-Payment-System implementiert, das keine vertrauenswürdigen Vermittler erfordert (z. B. Banken oder Zahlungsunternehmen). Das Bitcoin Whitepaper wurde 2008 von einem Entwickler (oder Entwicklungsteam) unter dem Pseudonym Satoshi Nakamoto veröffentlicht und wurde bald von der ersten "Münze" gefolgt, die 2009 in Form einer digitalen Aufzeichnung erstellt wurde. Zum Zeitpunkt des Schreibens (Oktober 2017) erreichte Bitcoin einen weiteren Rekordpreis von über 4400 US-Dollar und bildete eine Wirtschaft von 73 Milliarden US-Dollar.

Ursprünglich zielte Bitcoins Design darauf ab, die inhärenten Ineffizienzen und Agenturprobleme zu lösen, die sich aus dem zwischengeschalteten und zentralisierten Bankmodell ergeben. In der Regel, um eine internationale Überweisung zwischen, z. B. Kanada und China, zu tätigen, fließt das Geld über vier verschiedene Banken (darunter zwei "Korrespondentenbanken"), zwei nationale Zahlungssysteme und einen internationalen Abwicklungsdienst (z. B. SWIFT). Eine standardinternationale Zahlung dauert je nach Zielland zwischen 3 und 15 Werktagen und umfasst mehrere Agenten wie Bankangestellte, Mitarbeiter und Manager der oben genannten Finanzinstitute. Es gelten teure Bankgebühren und Wechselkurse.

Im Gegensatz dazu wird Bitcoin im Cyberspace über Tausende von Netzwerkknoten verteilt und ist von Natur aus grenzenlos. Zahlungen werden alle 10 Min. Vom Netzwerk validiert und aktualisiert. Intermediäre sind nicht erforderlich (z.B. Sind keine Korrespondenzbanken erforderlich). Es gibt keine Bankgebühren für Transaktionen, aber Benutzer zahlen in der Regel eine kleine Gebühr an Zahlungsprüfer

(bekannt als "Miners" – weiter unten diskutiert werden). Während für eine internationale Überweisung von 5000 US-Dollar eine Banküberweisung eine Gebühr von etwa 125 US-Dollar erheben würde, würde für eine Bitcoin-Überweisung eine Gebühr von etwa 1 US-Dollar erwartet. Es ist kein Wunder, dass Bitcoin als potenziell signifikanter Disruptor des aktuellen Finanzsystems auf der Grundlage des Bankwesens angesehen wird. Fußnote1

Bitcoin als Dezentralisierte Autonomous Organization

Bitcoin "läuft ein Zahlungssystem ... Beschäftigt Subunternehmer, die Bergleute sind... Mit neu ausgegebenen Bitcoin-Aktien an sich bezahlt" (Vigna und Casey 2015, S. 229, zitiert Larimer 2013). Footnote2 Das Bitcoin-System teilt somit die vier Kernfunktionen, die allen Konzeptualisierungen von "Organisationen" gemeinsam sind: Es ist ein "Multi-Agent-System [...] Mit identifizierbaren Grenzen und einem Zweck ,,zu dem die Bemühungen der konstituierenden Vertreter einen Beitrag leisten" (Puranam 2017, S. 6). Aber im Gegensatz zu traditionellen Organisationen hat Bitcoin kein CEO oder Top-Management-Team, sondern Entwickler, die "das Regelwerk schreiben", d.h. Governance-Regeln für das Programm definieren (Narayanan et al. 2016, S. 173–175). Bitcoin verfügt nicht über Hauptsitze, Tochtergesellschaften oder Mitarbeiter, sondern über ein verteiltes Netzwerk von Benutzern und Bergleuten, die Transaktionen in einem freigegebenen öffentlichen Ledger sammeln, überprüfen und aktualisieren, das öffentlich überprüfbar ist. Entscheidungen über Codeänderungen werden durch gemeinschaftsbasierte demokratische Abstimmungsverfahren getroffen, die durch die Rechenleistung der Bergleute für die Umsetzung unterstützt werden (Narayanan et al. 2016, S. 173–175).

Zwei bedeutende Innovationen untermauern Bitcoin: eine technologische Technologie, nämlich die öffentliche und distributed ledger Technologie namens "Blockchain", die sicher eine unveränderliche Aufzeichnung aller Benutzertransaktionen aufrechterhält, und eine organisatorische Innovation, nämlich die Existenz eines offenen Netzwerks von Nutzern mit speziellen Rollen und Rechten, die als "Miner" bezeichnet werden, die Rechenleistung verleihen, um das Netzwerk im Austausch für neu geprägte Bitcoins und Stimmrechte in Bezug auf zukünftige Protokollrevisionen zu sichern (Davidson et al. , 2016b).

Diese Innovationen haben einige Branchenexperten dazu gebracht, das Bitcoin-System als die erste reale Implementierung einer neuen Organisationsart namens "dezentralisierte autonome Organisation" (im Folgenden DAO) zu konzipieren. Nach vorheriger Arbeit definieren wir daos als nicht-hierarchische Organisationen, die Routineaufgaben in einem Peer-to-Peer-, kryptographisch sicheren öffentlichen Netzwerk ausführen und aufzeichnen und sich auf die freiwilligen Beiträge ihrer internen Stakeholder verlassen, um die Organisation durch einen demokratischen Konsultationsprozess zu betreiben, zu verwalten und weiterzuentwickeln (Valkenburgh et al. 2015; Dietz et al. 2016). Footnote3 daos koordinieren Routineaufgaben durch kryptografische Routinen (im Gegensatz zu menschlichen Routinen). Open-Source-Code definiert Regeln für Bergleute, um eine gemeinsame Historie von Transaktionen zu vereinbaren, die sicher und redundant über Netzwerkknoten aufgezeichnet werden, um einen einzigen Fehlerpunkt zu vermeiden (Nakamoto 2008). Während Bitcoin die erste Instanz war, die als DAO identifiziert wurde, wurden seit 2009 ein paar hundert weitere erstellt (z.B. Ethereum, Litecoin).

Bitcoin vs. Banks

Bitcoin stellt einen teilweisen Ersatz für Banken dar, wenn auch mit bemerkenswerten Unterschieden.

Erstens kann man kein Bankkonto eröffnen, ohne eine Reihe von amtlichen Ausweisdokumenten vorzulegen, die in den Entwicklungsländern oft den Zugang zum Bankwesen verhindern. Im Gegensatz dazu kann jeder Bitcoin-Nutzer werden und frei eine pseudonyme Bitcoin-Adresse (d. H. Analog zu einem Bankkonto) erhalten, die nicht ex ante an eine reale Identität gebunden ist. Im Wesentlichen ist eine Bitcoin-Adresse ein öffentlicher Schlüssel, der kryptographisch mit einem privaten Schlüssel verknüpft ist, der als Passwort für die Verwendung von Geldern fungiert. Dies ermöglicht ein neues Datenschutzmodell, das Identität von Transaktionen trennt (Nakamoto 2008). Der vertikale Balken in Abb. 1 zeigt, wo Bitcoin den Informationsfluss im Vergleich zu Banken bricht.

Zweitens speichern traditionelle Banken die Transaktionshistorie auf aggregierter Ebene zentralisiert. Benutzer können nur ihre persönlichen Kontoauszüge einsehen und müssen darauf vertrauen, dass ihre Informationen sowohl vor Cyberangriffen als auch vor Fehlverhalten von Mitarbeitern geschützt sind. Traditionell beschäftigen Banken Bankangestellte, um Zahlungen zu verarbeiten. Menschliche Agenten

sind anfällig für Agenturprobleme, die zu Fehlverhalten wie Diebstahl führen können. Die Kosten für die Bezahlung der menschlichen Agenten sind auch nicht trivial. Mit Bitcoin werden alle Transaktionen öffentlich und elektronisch auf der unveränderlichen "Blockchain" aufgezeichnet, die auf verteilte Weise über Tausende von Netzwerkknoten gespeichert wird – wodurch die Verwaltung von Datensätzen und Cyberangriffe unwahrscheinlich sind (weil die Informationen über Transaktionen in diesem Fall nicht an einem zentralen Ort gespeichert sind). Die Blockchain-Technologie liefert die Multi-Site-Kopien von "Ledgern" – die wirklich Aggregationen vergangener Transaktionen sind (z. B. Ein Kontoauszug). Es bietet auch Verschlüsselung, um Transaktionen als gültig oder ungültig zu validieren (z. B. Wie persönliche Sicherheitsgeräte, die wir derzeit für Online-Banking verwenden, die eine eindeutige transaktionsspezifische Signatur basierend auf einem persönlichen Schlüssel generieren).

Während Banken Doppelausgaben verhindern, indem sie in einem zentralisierten Server auf Geldtilgung prüfen, können die Zahlungsempfänger in einem Peer-to-Peer-System wie Bitcoin nicht überprüfen, ob die Zahler noch über die Mittel verfügen, die sie angeblich aufgrund unvorhersehbarer Netzwerkverzögerungen haben (z. B. Kann eine E-Mail, die jetzt gesendet wird, ihren Empfänger erreichen, bevor eine andere E-Mail eine Minute zuvor gesendet wird). Um dieses Problem zu lösen, verlässt sich Bitcoin auf kryptografische Routinen, um Transaktionen auf nicht reversible Weise zu überprüfen, zu benachlässigen und zu bestellen, wodurch die Notwendigkeit einer menschlichen Versöhnung vermieden wird. Dieser Prozess wird als "Mining" bezeichnet. Der Schlüsselgedanke ist, dass jemand im Netzwerk legitimerweise einen Block von Transaktionen abstempeln wird, aber wir können nicht vorhersagen, wer das sein wird (z. B. Einen Bankangestellten ersetzen, der mit gefälschten Zeitstempeln korrumpiert werden kann, durch ein System, das nicht korrumpiert werden kann).

Bitcoin "vermietet" Bergleute, um Transaktionen auf diese Weise durch einen "wettbewerbsfähigen Buchhaltungsprozess" zu verarbeiten (Yermack 2017). Mining ist ein Prozess, bei dem bestimmte Netzwerkknoten ("Miner") neue Transaktionen in einer Sequenz anordnen und sie durch das Lösen eines Rätsels mit einem Zeitstempel versehen: indem sie eine willkürlich lange Zahl erraten, nachdem sie Milliarden von zufälligen Vermutungen gemacht haben. Der Rateprozess kann schneller durchgeführt werden, indem mehr Rechenleistung in das Netzwerk übertragen wird. Somit ist die Wahrscheinlichkeit eines Bergmanns, den "Proof-of-Work" zur Verfügung stellen zu können, der für die Aktualisierung des Ledgers erforderlich ist, proportional zur Rechenleistung, die er kontrolliert. Die Rechenleistung, die alle 10 Minuten an Die im Ledger aufgezeichneten Transaktionsblöcke gebunden wird, akkumuliert und stellt ein Hindernis für Hacking dar, was es praktisch unmöglich macht, vergangene Transaktionsdatensätze zu bearbeiten, die in der Blockchain enthalten sind (d.h. Der Proof-of-Work müsste für jeden Block, der nach dem bearbeiteten blockiert wird, vollständig neu erstellt werden, was zu rechenintensiv und zu teuer ist, um ihn zu erreichen). Bergleute werden in Bitcoin für ihre Arbeit belohnt, die Kosten für Hardware und Strom nach dem Bitcoin-Protokoll beinhaltet.

Konsensmechanismen: neue Lösungen für die universellen Probleme der Organisation

Während Das Mining die Bitcoin-Zahlungsverarbeitung organisiert, "müssen die Menschen zuerst entscheiden, welches Protokoll ausgeführt werden soll, bevor die Maschinen es durchsetzen können (Lopp 2016)". Um die Logik der Blockchain von ihrem Governance- und Redesign-Prozess zu unterscheiden, definieren wir den Maschinenkonsens als den Prozess, bei dem Blockchain eine Vereinbarung (unterstützt durch Bergarbeiterbemühungen) über die Reihenfolge von Transaktionen durch die von Bergleuten erstellte Zeitstempel erzeugt, die es gelingt, eine Zufallszahl zu erraten; und gesellschaftlicher Konsens als Prozess, bei dem Bergleute über Vorschläge zur Protokollaktualisierung abstimmen, die von freiwilligen Entwicklern eingeführt wurden. Maschinenkonsens und gesellschaftlicher Konsens befeuern Bitcoins neuartiges Organisationsmodell und werden durch den einzigartigen Mining-Prozess integriert, der auf der Bereitstellung von Rechenleistung basiert.

Maschinenkonsens: das Bitcoin-Zahlungssystem

Proof-of-Work-Mining ist ein rechenintensiver und hochredundanter Prozess, der Ineffizienzen in Bezug auf den Energieverbrauch erzeugt. Aber als Ergebnis kann der Blockchain-Datensatz nicht mit Gewinn manipuliert werden. Mit dem Maschinenkonsens werden Aufgaben auf der Grundlage von Verpflichtungen in der Rechenleistung zugewiesen und auf der Grundlage des Ergebnisses des Bergbaus

wettbewerbsfähig belohnt. Alle Mining-bezogenen Daten sind für das gesamte Netzwerk öffentlich überprüfbar. Tabelle 1 zeigt, wie sich Bitcoin als Zahlungssystem anders organisiert als Banken und Zahlungsorganisationen.

Sozialer Konsens: Protokoll-Upgrades

Dem Bitcoin-Zahlungssystem liegt die Blockchain-Software zugrunde, die von laufenden Protokollaktualisierungen unterstützt wird (Wang und Vergne 2017). In Bezug auf governance ähnelt die Abstimmung von Bergleuten über Protokollaktualisierungsvorschläge dem community-basierten Management der Open-Source-Softwareentwicklung (OSSD), die für Projekte wie Linux beobachtet wird. Es richtet die Erwartungen der Stakeholder aus (Lopp 2016) und erleichtert den Wissensaustausch, die Problemlösung und die Realisierung kollektiver Ergebnisse (O'Mahony und Lakhani 2011). Wie OSSD ist auch die Entwicklung von Bitcoin-Software Open Source, dezentral und communitybasiert. Bitcoin-Gemeinschaften von freiwilligen Software-Entwicklern arbeiten in einem nicht-hierarchischen Netzwerk zusammen und wählen sich auf der Grundlage von Fachwissen und Präferenzen selbst in Aufgaben und Rollen aus. Im Laufe der Zeit hat sich ein Team von Bitcoin-Kernentwicklern gebildet und wird zunehmend einflussreich in der Community, obwohl ihre Arbeit nicht von einer zentralisierten Organisation finanziert wird, sondern von einem Sponsoring-Programm, das auf Spenden angewiesen ist.

Die wichtigste organisatorische Neuheit von Bitcoin im Vergleich zu OSSD ist, dass neben Entwicklern, Bergleute spielen eine ebenso wichtige Rolle bei Protokolländerungen. Insbesondere wird die Bitcoin-Software durch Bitcoin-Verbesserungsvorschläge (bips) aktualisiert, bei denen es sich um Designdokumente handelt, die neue Funktionen, Änderungen oder Prozesse für das Protokoll vorschlagen. Bips ermöglichen es Entwicklern, Vorschläge zu Softwareupdates zu machen, über die Bergleute abstimmen müssen, um die Implementierung auszulösen. Die Vorschläge werden zuerst von BIP-Redakteuren geprüft, und die Bergleute schließen dann während des Wahlzeitraums ein "Ja" oder "Nein" in einen Block ein (z. B. 100 Blöcke ab heute, nämlich eine 1000-Minuten-Periode). Die Stimmleistung ist proportional zur Rechenleistung, die ein Bergmann zum Netzwerk beisteuert. Eine Codeänderung wird nur umgesetzt, wenn für einen bestimmten Vorschlag eine Mehrheit von 55 % erreicht wird (Franco 2014, S. 90). Tabelle 2 vergleicht die Entwicklung von Bitcoin-Software mit OSSD entlang vier Kerndimensionen des Organisierens: Aufgabenteilung, Aufgabenzuweisung, Prämienverteilung und Informationsfluss (Puranam et al. 2014).

Bitcoins wahre organisatorische Neuheit liegt darin, wie Mining die Aufgabenteilung (basierend auf Rechenleistungsbeitrag), Aufgabenzuweisung und Prämienverteilung (durch wettbewerbsfähige Buchhaltung) und Informationsflüsse (auf der Blockchain und im Netzwerk) bestimmt. Während sich die Aufgabenintegration in traditionellen Umgebungen auf Regeln und Prozesse konzentriert, die zu einem großen Teil von Managern (Okhuysen und Bechky 2009) entworfen wurden, werden mit Bitcoin, Maschinenkonsens (z. B. Wettbewerbsfähige Buchhaltung) und sozialer Konsens (z. B. Abstimmung) durch Bergleute – eine brandneue Klasse von Stakeholdern – koordiniert.

Die Bergleute stimmen dem Spiel nach dem Regelwerk zu, aber sie können abstimmen, um es unter Verwendung des Einflusses zu ändern, der von ihrer Rechenleistung abgeleitet wird. Es ist jedoch wichtig zu beachten, dass der Bitcoin-Code das Problem der Agenturkosten nicht wegnimmt. Vielmehr befasst sich Bitcoin explizit mit diesen seit langem bestehenden Problemen, indem es Ausgleichsanreize in den Code einbezieht, wodurch das Zahlungssystem unbestechlich wird.

Im Gegensatz zu OSSD-Kontexten verlässt sich Bitcoin auf eine gemischte Gemeinschaft von freiwilligen Entwicklern und bezahlten Bergleuten, die gemeinsam das Organisationsdesign über bips überarbeiten. Vereinfacht gesagt bietet Bitcoin eine neuartige Lösung für "die universellen Probleme der Organisation" (Puranam et al. 2014), indem es eine neue Klasse von Stakeholdern einbezieht, die sowohl durch Maschinenkonsensalgorithmen als auch durch gesellschaftliche Konsensroutinen mit dem Entwurf einer Organisation, deren Parameter nicht einseitig von einer Stakeholder-Gruppe geändert werden können, und deren Routineoperationen nicht durch verdecktes Fehlverhalten von Insidern entgleist werden können.

Ähnliche Blockchain-Implementierungen: Kryptowährungen

Bitcoin ist der erste und etablierteste DAO, der bisher implementiert wurde. Seit Bitcoin wurden über 800 andere daos auf der Grundlage ähnlicher Designs erstellt, von denen die meisten als

"Kryptowährungen" gelten (d.h. Wie Bitcoin ermöglichen sie den Wertaustausch). Zum Zeitpunkt des Schreibens bilden Kryptowährungen eine Wirtschaft von 110 Milliarden Dollar und haben einen echten Einfluss auf die Welt. Einige Kryptowährungen werden auf Basis des Bitcoin-Quellcodes entwickelt (z.B. Litecoin, Namecoin, Dash), während andere mit ihrem eigenen Protokoll (z.B. Monero, Ethereum) von Grund auf neu begannen. Es haben sich auch Variationen herausgebildet, die eine breitere Palette von Anwendungen umfassen, die nicht nur Zahlungen sind, wie die dezentrale Domainregistrierung (Namecoin), Smart Contracts (Ethereum) und Datenschutz (Monero). Proof-of-Work-Mining ist nicht mehr der einzige Weg, um einen Maschinenkonsens zu erzielen, da alternative oder ergänzende Systeme wie Proof-of-Stake (wobei der Sicherheitsnachweis auf der Höhe der Kryptowährungen basiert, die Zahlungsprüfer halten) oder Proof-of-Burn (wobei das Netzwerk durch Validatoren gesichert ist, die Münzen einer nicht auswertbaren Adresse zuordnen) in den letzten Jahren entwickelt und implementiert wurden. Vorläufige Untersuchungen deuten darauf hin, dass die DAO-Leistung mit dem Ausmaß der Governance-Dezentralisierung variiert (Hsieh et al. 2018), so dass das Verständnis, wie verschiedene Formen des maschinellen und gesellschaftlichen Konsenses zum Erfolg und Misserfolg von daos beitragen, einen spannenden Weg für zukünftige Organisationsforschung darstellt.

Unternehmen der Zukunft?

Untersuchungen zeigen, dass das technologische Innovationspotenzial hinter Kryptowährungen der Haupttreiber ihres Marktwerts ist (Wang und Vergne 2017). Doch wie der Economist (2015) zu Recht hervorhebt, hat die Blockchain-Technologie weit reichende Anwendungen jenseits von Kryptowährungen und Zahlungen. Tatsächlich haben Blockchain-basiertes Organisieren und die daraus resultierenden daos die Möglichkeit, zentralisierte Intermediäre in anderen Anwendungen zu ersetzen, die eine komplexe Koordination erfordern, wie z. B. Asset Ownership Tracking, Handelsfinanzierung, digitale Identitätsbereitstellung, Rückverfolgbarkeit der Lieferkette und vieles mehr. Außerdem erhielten in den letzten 3 Jahren mehr als 50 neue Unternehmen Startkapital mittels Blockchain-betriebener "Anfangsmünzangebote" und umgingen damit zumindest teilweise den Einsatz von Risikokapitalgebern, um schneller und zu günstigeren Bewertungen Finanzmittel zu erhalten (z. B. Sammelte Ethereum 2014 innerhalb weniger Tage 18,4 Millionen DOLLAR ein und wird nun mit 34 Milliarden Dollar bewertet). Daos sind auf dem Vormarsch, und es ist eine aufregende Zeit für Management- und Organisationswissenschaftler, dieses aufkommende Phänomen mit neuer Theorie und solider empirischer Forschung anzugehen.

SCHLUSSFOLGERUNG

Im Einklang mit dem Geist der Organisation Zoo Serie, untersuchten wir die rätselhaften und innovativen Design-Features einer ganz besonderen Organisation (Bitcoin) und argumentierten, dass sie den Weg für neue Formen der Organisation ebnen werden. Vorläufig schlugen wir das Label "decentralized autonomous organization" (DAO) vor, um theoretisch zu charakterisieren, was mit Bitcoin und anderen vergleichbaren Organisationen im Spiel ist. Wir sind dankbar für die Gelegenheit, die wohl spannendste organisatorische Innovation des 21. Jahrhunderts (daos) in den Vordergrund zu rücken und für die aufschlussreichen Kommentare der drei Kommentatoren.

Wir stimmen mit Kommentator #1, dass aus der Perspektive der Management-Stipendium, "Kryptowährungen [...] Sind an der Wurzel der Organisation, nicht über Geld." Und wie der Kommentator #2 bemerkte, bieten Bitcoin und seine Blockchain "einen Blick in die Zukunft neuer Organisationsformen, die stark dezentralisiert und nach verschiedenen Prinzipien gestaltet werden könnten." Aber er summiert seine Behauptung, indem er drei Vorbehalte umreißt: die beobachtete Konzentration von Bergbauoperationen, die praktische Schwierigkeit der Dezentralisierung der DAO-Governance und das Risiko der Monopolisierung, die typischerweise in Informationsbranchen beobachtet werden, die starken Netzwerkeffekten ausgesetzt sind – denken Sie an AT&T, Microsoft, Google oder Facebook (siehe Wu 2011 und Durand und Vergne 2013 für ergänzende historische Perspektiven dieses Phänomens). Die Community ist sich dieser Einschränkungen sehr wohl bewusst, und es werden bereits Lösungen entwickelt, um sie anzugehen: die Ersetzung von Proof-of-Work-Mining durch alternative Konsensmechanismen zur

Minderung unerwünschter Konzentration, die Implementierung von Governance direkt in die Blockchain, um das Entstehen einer externen Behörde mit zu viel Einfluss auf die Entwicklung des Blockchain-Protokolls (ein Phänomen namens "On-Chain-Governance") zu vermeiden, und die Erstellung von Interoperabilitätsprotokollen, um die Kommunikation über Blockchains hinweg zu erleichtern und einen Gewinner-Take-all-Effekt zu verhindern. Beachten Sie jedoch, dass die Dominanz einer einzelnen Blockchain kein allzu großes Problem wäre, solange diese Blockchain durch Design dezentralisiert bleibt.

Wir stimmen mit Kommentator #3 überein, dass die technologische Neuheit, die Bitcoin zugrunde liegt, ein nuancierteres Phänomen ist, als das, was typischerweise in überbewerteten Medienberichten dargestellt wird. Wie Narayanan und Clark (2017) zeigten, "war Bitcoin ungewöhnlich und erfolgreich, nicht weil es auf dem neuesten Stand der Forschung an einem seiner Komponenten war, sondern weil es alte Ideen aus vielen bisher nicht verwandten Bereichen kombinierte" – nämlich verknüpfte Zeitstempel, digitales Bargeld, Proof-of-Work, byzantinische Fehlertoleranz und die Verwendung von öffentlichen Schlüsseln als Identitäten. Getrennt betrachtet, war jeder dieser Bausteine seit den 1980er Jahren in der Entwicklung, aber niemand hatte jemals daran gedacht, sie so kreativ zusammenzustellen, um Probleme zu lösen, mit denen Wissenschaftler der Informatik, Netzwerktechnik und Kryptographie seit Jahrzehnten zu kämpfen hatten. So würden wir argumentieren, dass Bitcoin eine Form architektonischer Innovation darstellt (Henderson und Clark 1990) und eine typische Situation darstellt, in der ein Durchbruch erreicht wird, indem bestehende Komponenten auf bisher unvorhergesehene Weise neu kombiniert werden, anstatt eine radikal neue eigenständige Komponente zu finden (Hargadon und Sutton 1997).

Im Gegensatz zu Kommentator #3 jedoch, wir glauben, dass daos neue Formen der Aufgabenteilung ermöglichen (z. B. Da Bitcoin keine Manager hat, die Entscheidungsfindung stattdessen modularisiert und verteilt wird), neue Formen der Aufgabenzuweisung (z. B. Durch Verwischung der "Unterscheidung zwischen 'Eigentümern', 'Mitwirkenden' und 'Nutzern'), wie von Kommentator #1 erklärt), und neue Möglichkeiten, Mitglieder zu belohnen (z. B. Indem sie subjektive Bewertung und Förderung durch Manager entfernen und stattdessen Belohnungen vornehmen).

Wie von Kommentator #1 festgestellt, Bitcoin ist unwahrscheinlich, das dominierende Design für zukünftige daos zu werden. Es ist nur der erste Fall eines technologischen Paradigmas in der Frühphase, und Innovationswellen verbessern sich bereits bei ihren ursprünglichen Designelementen (z. B. Gerichtete azyklische Graphiken, Lee 2018). Kommentator #1 fügt hinzu, dass daos heute "konkurrieren, um Wege zu institutionalisieren, um Vertrauen unter Fremden zu schaffen, das nicht von vertrauenswürdigen Vermittlern abhängt." Wir stimmen zu und behaupten, dass dies eine große Abkehr von der Art von Kapitalismus darstellt, die im siebzehnten Jahrhundert um die Schaffung mächtiger zentralisierter Intermediäre wie der Börse, der Zentralbank und verschiedener Clearing- und Abrechnungsorganisationen entstanden ist. Grundsätzlich könnte die Blockchain-Technologie einen Großteil ihres Disintermediationspotenzials verlieren, wenn sie nicht innerhalb einer verteilten Umgebung wie einem DAO organisiert wäre. Wir glauben, dass sich DIE daos auf struktureller Ebene organisatorisch von den Unternehmen unterscheiden, denen wir in der Vergangenheit begegnet sind, und das Potenzial haben, das Wesen des Unternehmenskapitalismus, wie wir ihn seit 400 Jahren kennen, zu verändern.

Schließlich können wir mit Kommentator #3 und Kommentator #1 zustimmen, dass "verteilte Ledger daos ermöglichen, aber auch viele Anwendungen in traditionelleren Organisationen finden werden." In der Tat, während wir diese Zeilen schreiben, existieren dezentrale öffentliche Blockchains wie Bitcoin bereits mit privaten verteilten Ledgern, die innerhalb und über traditionelle Unternehmen implementiert sind – die tradelens-Plattform, die vom Versandriesen Maersk mit IBM ins Leben gerufen wurde, ist ein Beispiel dafür (Allison 2018). Analog dazu sehen wir jetzt und werden es auch in absehbarer Zukunft sehen, ist die Koexistenz eines "Internets" öffentlicher Blockchains sozusagen und verschiedener "Intranets" aus privaten Unternehmens-Ledgern. Und wir werden sehen, wie daos mit traditionellen Unternehmen konkurrieren, ähnlich wie Bitcoin mit Western Union in der globalen Überweisungsbranche konkurriert hat.

Abschließend möchten wir darauf hinweisen, dass der Aufstieg von daos in der realen Welt in akademischen Kreisen mit dem Aufstieg der "Kryptoökonomie" einhergeht, einer aufkeimenden (Inter-)Disziplin, die untersucht, wie dezentrale Netzwerke und Token Anreize für die kollektive Wertschöpfung schaffen können. Stellen Sie sich beispielsweise vor, dass Nutzer eines sozialen Netzwerks Token setzen

müssen, die einen Wert darstellen, um ein Video posten zu können. Wenn sich dieses Video als Fake News oder Hassrede entpuppt, verliert der Nutzer seinen Einsatz. Wenn es sich als Inhalt wertvoll für andere und wird viral, wird der Benutzer mit zusätzlichen Tokens belohnt. In ähnlicher Weise werden Nutzer, die helfen, das Netzwerk zu polizeien, indem sie Hassreden kennzeichnen, belohnt, und Benutzer, die als Trend-Spotter fungieren, indem sie virale Inhalte bemerken, bevor sie viral werden, werden ebenfalls belohnt. Die Verwendung von Kryptowährungstoken zur Schaffung dieser Art von Anreizen könnte dazu beitragen, einige der Probleme zu mildern, mit denen beispielsweise Facebook derzeit konfrontiert ist, indem schädliches Verhalten entminiert und Den Nutzern das Eigentum an ihren persönlichen Daten gegeben wird (Naughton, 2018). Die Bestimmung der kryptografischen, Governance- und wirtschaftlichen Regeln für das Erstellen, Verteilen und Austauschen der Token, um die gewünschten kollektiven Ergebnisse zu erzielen, ist Gegenstand der Kryptoökonomie. Es stützt sich auf verschiedene Disziplinen, einschließlich Verhaltensökonomie, Sozialpsychologie, Spieltheorie, Netzwerk- und Computertechnik und Kryptographie.

Der Aufstieg der Kryptoökonomie stellt eine spannende Entwicklung dar. Es wird Management- und Organisationswissenschaftlern ein ergänzendes Instrumentarium geben, um die Welt der daos mit der notwendigen Vorsicht und Skepsis zu erforschen, die zukünftige wissenschaftliche Untersuchungen dieses faszinierenden Phänomens begleiten sollte.

TRANSLATED VERSION: PORTUGUESE

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSÃO TRADUZIDA: PORTUGUÊS

Aqui está uma tradução aproximada das ideias acima apresentadas. Isto foi feito para dar uma compreensão geral das ideias apresentadas no documento. Por favor, desculpe todos os erros gramaticais e não responsacule os autores originais responsáveis por estes erros.

INTRODUÇÃO

O que éitcoina B?

O Bitcoin é um código de software de código aberto que implementa um sistema de pagamento em dinheiro digital descentralizado, peer-to-peer, que não requer que quaisquer intermediários de confiança operem (por exemplo, bancos ou empresas de pagamento). O Bitcoin Whitepaper foi publicado em 2008 por um desenvolvedor (ou equipa de desenvolvimento) sob o pseudónimo Satoshi Nakamoto, e logo foi seguido pela primeira "moeda" criada sob a forma de um recorde digital em 2009. Na altura da escrita (outubro de 2017), a Bitcoin atingiu outro preço recorde superior a 4400 dólares, formando uma economia de 73 mil milhões de dólares.

Inicialmente, o desenho da Bitcoin visava resolver as ineficiências inerentes e os problemas de agência decorrentes do modelo bancário intermédio e centralizado. Normalmente, para fazer uma transferência bancária internacional entre, digamos, o Canadá e a China, o dinheiro passa por quatro bancos diferentes (incluindo dois bancos "correspondentes"), dois sistemas nacionais de pagamentos e um serviço internacional de liquidação (por exemplo, SWIFT). Um pagamento internacional padrão demora entre 3 a 15 dias úteis para ser concluído, dependendo do país de destino, e envolve vários agentes, como caixas bancárias, funcionários e gestores das referidas instituições financeiras. Aplicam-se taxas bancárias caras e taxas de câmbio.

Em contraste, o Bitcoin é distribuído no ciberespaço através de milhares de nós de rede, e é inerentemente sem fronteiras. Os pagamentos são validados e atualizados pela rede a cada 10 minutos. Não são necessários intermediários (por exemplo, não são necessários bancos correspondentes). Não há

comissões bancárias para transações, mas os utilizadores normalmente pagam uma pequena taxa aos validadores de pagamento (conhecidos como "mineiros" — a serem discutidos mais abaixo). Enquanto que para uma transferência internacional de $5.000, uma cablagem bancária cobraria uma taxa de cerca de $125, uma taxa de cerca de $1 seria esperada para uma transferência de Bitcoin. Não é de admirar que o Bitcoin seja visto como um potencial disruptor do sistema financeiro atual baseado na banca. Nota de rodapé1

Bitcoin como um Decentralizado Umarganização**utonomous Organization**

Bitcoin "gere um sistema de pagamento... Emprega subempreiteiros que são mineiros... Pagos com ações bitcoin recentemente emitidas em si" (Vigna e Casey 2015, p. 229, citando Larimer 2013). Nota de rodapé2 O sistema Bitcoin partilha assim as quatro características fundamentais comuns a todas as conceptualizações de "organizações": é um "sistema multi-agente [...] Com limites identificáveis e [a] propósito [...] Para o qual os esforços dos agentes constituíveis dão um contributo" (Puranam 2017, p. 6). Mas, ao contrário das organizações tradicionais, a Bitcoin não tem um CEO ou uma equipa de gestão de topo, mas sim os desenvolvedores que "escrevem o livro de regras", ou seja, definem as regras de governação para o programa (Narayanan et al. 2016, pp. 173-175). A Bitcoin não tem sede, subsidiárias ou funcionários, mas uma rede distribuída de utilizadores e mineiros que recolhem, verificam e atualizam transações num livro público partilhado que é publicamente auditável. As decisões sobre as modificações de código são tomadas através de processos de votação democráticas baseados na comunidade, apoiados pelo poder de computação dos mineiros para a sua implementação (Narayanan et al. 2016, pp. 173-175).

Duas inovações significativas sustentam o Bitcoin: uma tecnológica, nomeadamente a tecnologia de contabilidade pública e distribuída chamada "blockchain", que mantém seguramente um registo imutável de todas as transações de utilizadores, e uma inovação organizacional, nomeadamente, a existência de uma rede aberta de utilizadores com papéis e direitos especiais chamados "mineiros", que emprestam poder de computação para garantir a rede em troca de bitcoins recém-cunhadas e direitos de voto no que diz respeito a futuras revisões do protocolo (Davidson et al 2016. , 2016b).

Estas inovações levaram alguns especialistas do setor a conceber o sistema Bitcoin como a primeira implementação real de um novo tipo de organização chamada "organização autónoma descentralizada" (doravante, DAO). Após trabalhos anteriores, definimos os daos como organizações não hierárquicas que executam e registam tarefas rotineiras numa rede pública peer-to-peer, criptograficamente segura, pública, e contamos com as contribuições voluntárias dos seus stakeholders internos para operar, gerir e evoluir a organização através de um processo de consulta democrática (Valkenburgh et al. 2015; Dietz et al. 2016). Os daos de notas de rodapé 3 coordenam tarefas de rotina através de rotinas criptográficas (em oposição às rotinas humanas). O código open source define regras para os mineiros acordarem numa história partilhada de transações registadas de forma segura e redundante através dos gândes de rede, a fim de evitar ter um único ponto de falha (Nakamoto 2008). Embora o Bitcoin tenha sido a primeira instância a ser identificada como DAO, mais algumas centenas foram criadas desde 2009 (por exemplo, Ethereum, Litecoin).

Bitcoin vs. Banks

A Bitcoin representa um substituto parcial para os bancos, embora com diferenças notáveis.

Em primeiro lugar, não se pode abrir uma conta bancária sem fornecer uma série de documentos oficiais de identificação, que no mundo em desenvolvimento muitas vezes impedem o acesso à banca. Em contraste, qualquer pessoa pode tornar-se um utilizador bitcoin e obter livremente um pseudónimo endereço Bitcoin (isto é, análogo a uma conta bancária) não ligado ex ante a uma identidade real. No fundo, um endereço Bitcoin é uma chave pública criptograficamente ligada a uma chave privada agindo como uma senha para gastar fundos. Isto permite um novo modelo de privacidade que separa a identidade das transações (Nakamoto 2008). A barra vertical na Fig. 1 demonstra onde o Bitcoin quebra o fluxo de informação em comparação com os bancos.

Em segundo lugar, a nível agregado, os bancos tradicionais armazenam histórias de transações de forma centralizada. Os utilizadores só podem ver os seus extratos bancários pessoais e devem confiar que as suas informações estão protegidas tanto de ciberataques como de má conduta dos funcionários. Tradicionalmente, os bancos empregam funcionários bancários para processar pagamentos. Os agentes humanos são propensos a problemas de agências que podem levar a condutas impróprias, como roubo. O custo do pagamento aos agentes humanos também não é trivial. Com o Bitcoin, todas as transações são

registadas publicamente e eletronicamente no imutável "blockchain" armazenado de forma distribuída em milhares de nós de rede , tornando assim os registos mais fáceis de manter e os ciberataques improváveis de serem bem sucedidos (porque as informações sobre transações neste caso não são realizadas numa localização central). A tecnologia blockchain fornece cópias multi-sites de "livros", que são realmente agregações de transações passadas (por exemplo, como um extrato de conta bancária). Também fornece encriptação para validar transações como válidas ou inválidas (por exemplo, como dispositivo de segurança pessoal que utilizamos atualmente para o banco online, que geram uma assinatura específica de transação única baseada numa chave pessoal).

Enquanto os bancos impedem a dupla despesa verificando a suficiência de fundos num servidor centralizado, num sistema peer-to-peer como o Bitcoin, os beneficiários não conseguem verificar se os pagadores ainda têm os fundos que alegam ter devido a atrasos imprevisíveis na rede (por exemplo, um e-mail enviado pode agora chegar ao seu destinatário antes de outro e-mail enviado um minuto antes). Para resolver este problema, a Bitcoin baseia-se em rotinas criptográficas para verificar, marcar tempo e encomendar transações de forma não reversível, evitando assim a necessidade de reconciliação humana. Este processo chama-se "mineração". A ideia-chave é que alguém na rede irá legitimamente carimbar um bloco de transações, mas não podemos prever quem será (por exemplo, substituir um funcionário bancário, que pode ser corrompido em carimbos de tempo falsos, com um sistema que não pode ser corrompido).

A Bitcoin "contrata" mineiros para processar transações desta forma através de um processo de "contabilidade competitiva" (Yermack 2017). A mineração é um processo pelo qual os nós de rede específicos ("mineiros") organizam novas transações numa sequência, e carimbam-nas através da resolução de um enigma: adivinhando um número arbitrariamente longo depois de fazer biliões de palpites aleatórios. O processo de adivinhação pode ser feito mais rapidamente comprometendo mais poder de computação para a rede. Assim, a probabilidade de um mineiro ser capaz de fornecer a "prova de trabalho" necessária para atualizar o livro é proporcional aos controlos de poder de computação. O poder de computação comprometido a cada 10 minutos a blocos de transações registadas no livro-razão acumula-se e constitui uma barreira à pirataria, tornando praticamente impossível a edição de registos de transações anteriores contidos na blockchain (ou seja, a prova de trabalho teria de ser inteiramente refeita para cada bloco adicionado após o editado, que é demasiado intensivo computacionalmente e demasiado dispendioso para ser alcançado). Os mineiros são recompensados em Bitcoin pelo seu trabalho, que envolve custos em hardware e eletricidade, de acordo com o protocolo Bitcoin.

Mecanismos de consenso: novas soluções para os problemas universais da organização

Enquanto a mineração organiza o processamento de pagamentos Bitcoin, "os humanos devem primeiro decidir qual o protocolo a executar antes que as máquinas possam aplicá-lo (Lopp 2016)". Para distinguir a lógica do blockchain do seu processo de governação e de redesensoamento, definimos o consenso da máquina como o processo pelo qual blockchain produz acordo (ajudado pelos esforços dos mineiros) na ordenação de transações através da estampagem temporal criada pelos mineiros que consegue adivinhar um número aleatório; e o consenso social como o processo pelo qual os mineiros votam sobre propostas de atualização do protocolo introduzidas pelos desenvolvedores voluntários. O consenso da máquina e o consenso social alimentam o novo modelo organizacional da Bitcoin e tornam-se integrados através do processo de mineração único baseado na oferta de energia computacional.

Consenso da máquina: o sistema de pagamento de bitcoin

A exploração mineira de prova de trabalho é um processo computacionalmente intensivo e altamente redundante que gera ineficiências em termos de consumo de energia. Mas como resultado, o registo da blockchain não pode ser adulterado com lucro. Com o consenso da máquina, as tarefas são atribuídas com base em compromissos no poder de computação, e recompensadas competitivamente com base no resultado da mineração. Todos os dados relacionados com a mineração são publicamente auditáveis para toda a rede. O quadro 1 mostra como o Bitcoin como sistema de pagamentos se organiza de forma diferente dos bancos e das organizações de pagamentos.

Consenso social: atualizações do protocolo

Subjacente ao sistema de pagamento Bitcoin está o software blockchain suportado por atualizações de protocolo em curso (Wang e Vergne 2017). Em termos de governação, a votação dos mineiros sobre

propostas de atualização de protocolos assemelha-se à gestão comunitária do desenvolvimento de software de código aberto (OSSD) observada para projetos como o Linux. Alinha as expectativas das partes interessadas (Lopp 2016) e facilita a partilha de conhecimentos, a resolução de problemas e a realização de resultados coletivos (O'Mahony e Lakhani 2011). Tal como o OSSD, o desenvolvimento de software Bitcoin também é de fonte aberta, descentralizado e baseado na comunidade. As comunidades de bitcoin de desenvolvedores de software voluntário colaboram numa rede não hierárquica e auto-selecionam em tarefas e funções baseadas em conhecimentos e preferências. Com o passar do tempo, uma equipa de desenvolvedores de Bitcoin formou-se e tornou-se cada vez mais influente na comunidade, embora o seu trabalho não seja financiado por uma organização centralizada, mas por um programa de patrocínios que se baseia em doações.

A principal novidade organizacional do Bitcoin em comparação com a OSSD é que, além dos desenvolvedores, os mineiros desempenham um papel igualmente importante nas modificações do protocolo. Especificamente, o software Bitcoin é atualizado através de propostas de melhoria de Bitcoin (bips), que são documentos de design que propõem novas funcionalidades, alterações ou processos para o protocolo. Os bips permitem que os desenvolvedores façam propostas sobre atualizações de software que os mineiros devem votar para desencadear a implementação. As propostas são primeiramente revistas pelos editores do BIP, e os mineiros incluem um voto "sim" ou "não" num bloco durante o período de votação (por exemplo, 100 blocos a partir de hoje, nomeadamente um período de 1000 minutos). O poder de voto é proporcional ao poder de computação que um mineiro contribui para a rede. Uma alteração de código só será implementada quando for obtida uma maioria de 55% para uma determinada proposta (Franco 2014, p. 90). O quadro 2 compara o desenvolvimento do software Bitcoin com o OSSD ao longo de quatro dimensões fundamentais da organização: divisão de tarefas, atribuição de tarefas, distribuição de recompensas e fluxo de informação (Puranam et al. 2014).

A verdadeira novidade organizacional da Bitcoin reside na forma como a mineração determina a divisão de tarefas (baseada na contribuição de poder de computação), a atribuição de tarefas e distribuição de recompensas (através de contabilidade competitiva) e fluxos de informação (na blockchain e na rede). Embora a integração de tarefas em configurações tradicionais se centre em regras e processos desenhados em grande parte pelos gestores (Okhuysen e Bechky 2009), com Bitcoin, o consenso da máquina (por exemplo, a contabilidade competitiva) e o consenso social (por exemplo, votação) são coordenados através de mineiros - uma nova classe de stakeholders.

Os mineiros concordam em jogar pelo livro de regras, mas podem votar para mudá-lo usando a influência derivada do seu poder de computação. No entanto, é importante notar que o código Bitcoin não assume o problema dos custos da agência. Pelo contrário, a Bitcoin lida explicitamente com estes problemas de longa data, incorporando incentivos de contrabalançamento no código, tornando o sistema de pagamento incorruptível.

Em contraste com os contextos OSSD, o Bitcoin conta com uma comunidade mista de desenvolvedores voluntários e mineiros pagos que reveem conjuntamente o design organizacional através de bips. Simplificando, o Bitcoin oferece uma nova solução para "os problemas universais de organização" (Puranam et al. 2014) envolvendo uma nova classe de stakeholders, incentivado por algoritmos de consenso de máquinas e rotinas de consenso social, com o desenho de uma organização cujos parâmetros não podem ser alterados unilateralmente por qualquer grupo de interessados, e cujas operações de rotina não podem ser descarriladas por conduta imprópria de insiders.

Implementações semelhantes em blockchain: criptomoedas

Bitcoin é o primeiro e mais estabelecido DAO implementado até à data. Desde o Bitcoin, houve mais de 800 outros daos criados com base em designs semelhantes, a maioria dos quais são considerados "criptomoedas" (ou seja, como o Bitcoin, permitem a troca de valor). No momento da escrita, as criptomoedas formam uma economia de 110 mil milhões de dólares e têm um impacto real no mundo. Algumas criptomoedas são desenvolvidas com base no código fonte bitcoin (por exemplo, Litecoin, Namecoin, Dash), enquanto outras começaram do zero com o seu próprio protocolo (por exemplo, Monero, Ethereum). Também surgiram variações para abraçar um leque mais alargado de aplicações que não apenas pagamentos, tais como registo de domínio descentralizado (Namecoin), contratos inteligentes (Ethereum)

e privacidade (Monero). A exploração mineira de prova de trabalho já não é a única forma de alcançar o consenso das máquinas, uma vez que foram desenvolvidos e implementados nos últimos anos sistemas alternativos ou complementares que atribuem moedas a um endereço não autilizável. Pesquisas preliminares sugerem que o desempenho do DAO varia com a extensão da descentralização da governação (Hsieh et al. 2018), pelo que compreender como várias formas de máquina e consenso social contribuem para o sucesso e o fracasso dos daos representa uma excitante via para a investigação organizacional futura.

Empresas do futuro?

A investigação indica que o potencial de inovação tecnológica por trás das criptomoedas é o principal motor do seu valor de mercado (Wang e Vergne 2017). Mas, como o Economist (2015) assinala com razão, a tecnologia blockchain tem aplicações de longo alcance para além das criptomoedas e dos pagamentos. Com efeito, a organização baseada em blockchain e os daos resultantes têm a capacidade de substituir intermediários centralizados noutras aplicações que requerem uma coordenação complexa, como o rastreio da propriedade de ativos, o financiamento do comércio, a disponibilização de identidade digital, a rastreabilidade da cadeia de abastecimento, entre outros. Além disso, nos últimos 3 anos, mais de 50 novos empreendimentos receberam financiamento de sementes usando "ofertas iniciais de moedas" movidas a blockchain, contornando, pelo menos em parte, o uso de intermediários capitalistas de risco para obter financiamento mais rápido e com avaliações mais favoráveis (por exemplo, em 2014, o Ethereum angariou 18,4 milhões de dólares em poucos dias e está agora avaliado em 34 mil milhões de dólares). Os daos estão em ascensão, e é um momento emocionante para os estudiosos da gestão e da organização abordarem este fenómeno emergente com uma nova teoria e uma investigação empírica sólida.

CONCLUSÃO

De acordo com o espírito da série Organization Zoo, examinámos as características intrigantes e inovadoras de um design muito especial (Bitcoin) e argumentámos que abrirão caminho para novas formas de organização. Provisoriamente, propusemos o rótulo de "organização autónoma descentralizada" (DAO) para caracterizar teoricamente o que está em jogo com a Bitcoin e outras organizações comparáveis. Estamos gratos pela oportunidade de trazer à toa o que poderia muito bem ser a mais excitante inovação organizacional do século XXI (daos) e pelos comentários perspicazes fornecidos pelos três comentadores.

Concordamos com o comentador #1 que, do ponto de vista da bolsa de gestão, "criptomoedas [...] Estão em raiz sobre a organização, não sobre o dinheiro. E, como nota o comentador #2, a Bitcoin e a sua blockchain "proporcionam um vislumbre do futuro de novas formas organizacionais que poderiam ser altamente descentralizadas e desenhadas com diferentes princípios". Mas matiza a sua afirmação delineando três ressalvas: a concentração observada das operações mineiras, a dificuldade prática de descentralizar a governação do DAO, e o risco de monopolização tipicamente observado nas indústrias da informação sujeitas a fortes efeitos de rede — pensem AT&T, Microsoft, Google ou Facebook (ver Wu 2011 e Durand e Vergne 2013 para perspetivas históricas complementares sobre este fenómeno). A comunidade está bem ciente destas limitações, e já estão a ser desenvolvidas soluções para as resolver: substituir a mineração à prova de trabalho por mecanismos de consenso alternativos para mitigar a concentração indesejada, implementar a governação diretamente na blockchain para evitar o surgimento de uma autoridade externa com demasiada influência na evolução do protocolo blockchain (um fenómeno chamado "governação em cadeia"), e a criação de protocolos de interoperabilidade para facilitar a comunicação através de blockchains e prevenir um vencedor.todos os efeitos. Note-se, no entanto, que o domínio de uma única blockchain não seria um problema muito grande, desde que a blockchain permaneça descentralizada pelo design.

Concordamos com o comentador #3 que a novidade tecnológica subjacente ao Bitcoin é um fenómeno mais matizado do que o que é tipicamente retratado em contas mediáticas exageradas. Como demonstrado por Narayanan e Clark (2017), "O Bitcoin foi invulgar e bem-sucedido não porque estava na vanguarda da investigação sobre qualquer um dos seus componentes, mas porque combinava ideias antigas de muitos campos anteriormente não relacionados"— nomeadamente, o timestamping ligado, o dinheiro digital, a prova de trabalho, a tolerância à falha bizantina, e o uso de chaves públicas como identidades. Tomados

separadamente, cada um destes blocos de construção estava em desenvolvimento desde a década de 1980, mas nunca ninguém tinha pensado em juncá-los de uma forma tão criativa para resolver problemas que os estudiosos da ciência da computação, engenharia de redes e criptografia tinham lutado durante décadas. Assim, argumentamos que o Bitcoin constitui uma forma de inovação arquitetónica (Henderson e Clark 1990) e representa uma situação típica em que se consegue uma descoberta através da recombinação dos componentes existentes de formas anteriormente imprevistas, em vez de criar uma componente autónoma radicalmente nova (Hargadon e Sutton 1997).

No entanto, ao contrário do comentador #3, acreditamos que os daos permitem novas formas de divisão de tarefas (por exemplo, uma vez que o Bitcoin não tem gestores, a tomada de decisão é, em vez disso, modularizada e distribuída), novas formas de atribuição de tarefas (por exemplo, ao esbater a "distinção entre 'proprietários', 'contribuintes' e 'utilizadores'", como explica o comentador #1), e novas formas de recompensar os membros (por exemplo, removendo a avaliação subjetiva e a promoção por parte dos gestores, e, em vez disso, tornando as regras relacionadas com as recompensas transparentes no código do software).

Como nota o comentador #1, é pouco provável que o Bitcoin se torne o design dominante para futuros daos. É apenas a primeira instância de um paradigma tecnológico em fase inicial, e as ondas de inovação já estão a melhorar nos seus elementos de design iniciais (por exemplo, gráficos acíclicos direcionados, Lee 2018). O comentador #1 acrescenta que os daos de hoje estão "a competir para institucionalizar formas de criar confiança entre estranhos que não dependem de intermediários de confiança". Concordamos e defendemos que isto representa uma grande mudança para o tipo de capitalismo que surgiu no século XVII em torno da criação de poderosos intermediários centralizados, como a bolsa de valores, o banco central, e várias organizações de compensação e liquidação. Fundamentalmente, a tecnologia blockchain poderia perder grande parte do seu potencial de desintermediação se não fosse organizada dentro de um ambiente distribuído, como um DAO. Acreditamos que os daos, a nível estrutural, são organizacionalmente diferentes das empresas que encontrámos no passado e têm o potencial de alterar a natureza do capitalismo corporativo, como o conhecemos há 400 anos.

Por fim, não podemos deixar de concordar com o comentador #3 e comentador #1 que "os livros distribuídos permitem os daos, mas também encontrarão muitas aplicações dentro de organizações mais tradicionais". De facto, à medida que escrevemos estas linhas, blockchains públicos descentralizados como o Bitcoin já co-existem com livros privados distribuídos implementados dentro e em todas as empresas tradicionais — a plataforma tradelens, lançada pelo gigante do transporte de mercadorias Maersk com a IBM, é um caso em destaque (Allison 2018). Por analogia, o que vemos agora, e continuaremos a ver num futuro previsível, é a coexistência de uma "Internet" de blockchains públicos, por assim dizer, e de várias "Intranets" feitas de livros corporativos privados. E veremos os daos competirem contra as empresas tradicionais, tal como a Bitcoin tem competido com a Western Union na indústria global de remessas.

Para concluir, gostaríamos de salientar que a ascensão dos daos no mundo real é acompanhada, nos círculos académicos, pela ascensão da "criptoeconomia", uma disciplina nascente (inter)que examina como redes e fichas descentralizadas podem incentivar a criação de valor coletivo. Imaginem, por exemplo, que os utilizadores de uma rede social tinham de apostar fichas que representassem valor para poderem publicar um vídeo. Se o vídeo se revelar notícias falsas ou discurso de ódio, o utilizador perde a sua participação. Se se revelar um conteúdo valioso para os outros e se tornar viral, o utilizador é recompensado com fichas adicionais. Da mesma forma, os utilizadores que ajudam a policiar a rede, assinalando discursos de ódio, são recompensados, e os utilizadores que atuam como observadores de tendências, notando conteúdos virais antes que se tornem virais, também são recompensados. Usar fichas de criptomoedas para criar este tipo de incentivos poderia ajudar a mitigar alguns dos problemas atualmente enfrentados pelo Facebook, por exemplo, ao desincentivar comportamentos prejudiciais e dar aos utilizadores a propriedade dos seus dados pessoais (Naughton, 2018). Determinar as regras criptográficas, governativas e económicas para criar, distribuir e trocar os tokens para obter os resultados coletivos desejados é objeto de criptoeconomia. Baseia-se em várias disciplinas, incluindo economia comportamental, psicologia social, teoria dos jogos, engenharia de redes e computadores, e criptografia.

A ascensão da criptoeconomia representa um desenvolvimento excitante. Dará aos estudiosos da administração e da organização um kit de ferramentas complementar para pesquisar o mundo dos daos com a necessária cautela e ceticismo que devem acompanhar futuras investigações académicas deste fenómeno fascinante.