Western University
Scholarship@Western

Business Publications | Business (Richard Ivey School of Business)

2017

Bitcoin and the Rise of Decentralized Autonomous Organizations

Ying-Ying Hsieh
Western University

Jean-Philippe Vergne
Western University

Follow this and additional works at: https://ir.lib.uwo.ca/iveypub

 Part of the Business Commons

Citation of this paper:
Hsieh YY & Vergne JP. Forthcoming. Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design, Organization Zoo Series.

BITCOIN AND THE RISE OF DECENTRALIZED AUTONOMOUS ORGANIZATIONS[1]

Ying-Ying Hsieh
PhD Candidate in Strategy
Ivey Business School
Western University
1255 Western Road
London, Ontario, Canada N6G 0N1
yhsieh@ivey.ca

Jean-Philippe Vergne
Associate Professor of Strategy
Ivey Business School
Western University
1255 Western Road
London, Ontario, Canada N6G 0N1
jvergne@ivey.ca

Citation: Hsieh YY & Vergne JP. *Forthcoming*. Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, Organization Zoo Series.[2]

[1] Acknowledgements: This work was supported by the Social Sciences and Humanities Research Council (grant# 430-2015-0670), the Ontario Government (grant# R4905A06), and the Scotiabank Digital Banking Lab at Ivey Business School.
[2] We thank Associate Editors Dr. Phanish Puranam and Dr. Dorthe Døjbak Håkonsson for providing constructive feedback throughout the revision process.

BITCOIN AND THE RISE OF DECENTRALIZED AUTONOMOUS ORGANIZATIONS

"[I]t makes most sense to see Bitcoin […] as a decentralized autonomous organization."
Vitalik Buterin, Industry Expert, Co-founder of Ethereum and Co-founder of Bitcoin Magazine

ABSTRACT

Bitcoin represents the first real-world implementation of a "decentralized autonomous organization" (DAO) and offers a new paradigm for organization design. Imagine working for a global business organization whose routine tasks are powered by a software protocol instead of being governed by managers and employees. Task assignments and rewards are randomized by the algorithm. Information is not channelled 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 invite commentaries from renowned organization scholars to share their views on this intriguing phenomenon.

Keywords: Decentralized autonomous organization; blockchain; consensus mechanisms; new forms of organizing; organizational forms

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 $4,400, 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 minutes. 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 $5,000, 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.[3]

BITCOIN AS A "DECENTRALIZED AUTONOMOUS ORGANIZATION" (DAO)

Bitcoin "runs a payment system…employs subcontractors who are miners… paid for with newly issued bitcoin shares in itself" (Vigna & Casey, 2015:229, quoting Larimer, 2013)[4]. 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: 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, Bonneau, Felten, Miller & Goldfeder, 2016: 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: 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, De Filippi & Potts, 2016a; 2016b).

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

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

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* (Van Valkenburgh, Dietz, De Filippi, Shadab, Xethalis & Bollier, 2015; Dietz, Xethalis, De Filippi & Hazard, accessed 2016)[5]. 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 Figure 1 demonstrates where Bitcoin breaks the information flow as compared to banks.

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

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 ten minutes to blocks of transactions recorded in the ledger accumulates and forms a barrier to hacking, making it practically impossible to edit past transaction records contained in the blockchain (i.e. the proof-of-work would have to be entirely redone for every block added after the edited one, which is too computationally intensive and too costly to achieve). 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 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 & 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 & Lakhani, 2009). 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 1,000 minutes 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: 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, Alexy & Reitzig, 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 & 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, Vergne & Wang, 2017), 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 & 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 three years, more than fifty new ventures received seed funding using blockchain-powered "initial coin offerings", thereby bypassing, at least partly, the use of venture capitalist intermediaries to obtain funding faster and at more favorable valuations (e.g. in 2014, Ethereum raised $18.4 million in a few days and is now valued at $34 billion). 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.

FIGURE AND TABLES

Figure 1 Traditional Privacy Model vs. the Bitcoin Privacy Model (adopted from Nakamoto, 2008)

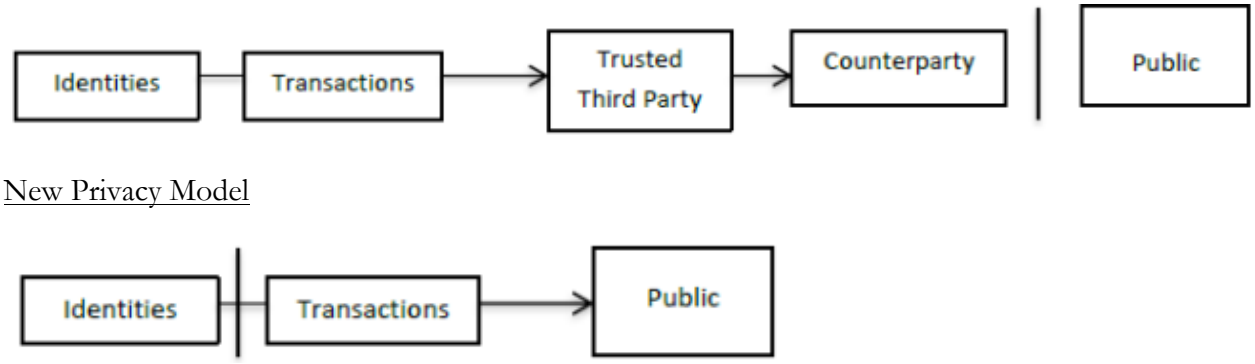

Table 1 Banks and Payment Organizations vs. Bitcoin on their Forms of Organizing

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 payment 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

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

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

Davidson, S., De Filippi, P. & Potts, J. 2016a. Disrupting governance: The new institutional economics of distributed ledger technology. SSRN: http://ssrn.com/abstract=2811995

Davidson, S., De Filippi, P. & Potts, J. 2016b. Economics of blockchain. SSRN: http://ssrn.com/abstract=2744751.

Dietz, J., Xethalis, G., De Filippi, P. & Hazard, J. Model distributed collaborative organizations. Stanford Working Group. [Accessed August 2016].

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 April 2017].

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

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

Hsieh, YY., Vergne, JP. & Wang, S. 2018 *Forthcoming*. The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In Campbell-Verduyn M (ed.**),** ***Bitcoin and Beyond: Blockchains and Global Governance***. RIPE/Routledge Series in Global Political Economy.

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

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

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

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

Okhuysen, G. A. & Bechky, B. A. 2009. Coordination in organizations: An integrative perspective. ***Academy of Management Annals***, 3(1): 463-502.

Orlikowski, W. J. 2002. Knowing in practice: Enacting a collective capability in distributed organizing. ***Organization science***, 13(3): 249-273.

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

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

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 2016].

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

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

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance*, p.rfw074.