DOI: 10.1002/jsc.2150

RESEARCH ARTICLE

WILEY

Disrupting governance with blockchains and smart contracts*

Voshmgir Shermin

BlockchainHub, Berlin, Germany

Correspondence
Alte Schönhauserstrasse 9, 19119 Berlin, Germany

Email: shermin@blockchainhub.net

Abstract

Blockchain as an engine for auto-enforceable smart contracts could disrupt traditional governance structures by reducing bureaucracy through lower transaction costs, solving principal–agent issues, and subsequent moral hazard. While machine consensus can radically reduce transaction costs and disrupt traditional governance structures, there is a gap between initial conceptualizations of blockchains and their first instantiations. First use cases show that as circumstances change, protocols can become inappropriate for the new environment and require modification. Modification of blockchain code happens through majority consensus, but reaching consensus in a distributed multi-stakeholder network with sometimes unaligned interests is complex, potentially introducing new agency issues.

1 | INTRODUCTION

Blockchain is a novel solution to the age-old human problem of trust. Blockchain provides an architecture for so-called *trustless trust* that allows us to trust the outputs of a system without trusting any actor within it (Werbach, 2016). The promise, or threat, of blockchain is to challenge centralized, top-down decision-making through radical transparency and auto-enforceable code. The claim of many early blockchain advocates has therefore been "money without banks, companies without managers, countries without politicians."

Drawing on organizational and political theories of how society organizes itself, this article explores the extent to which these claims are valid, and what the potentials and challenges to such new forms of decentralized governance are. Could companies, nations, and other kinds of top-down managed organizations really become obsolete?

The purpose of this article is to explain how blockchains and smart contracts bypass traditional principal–agent dilemmas of organizations, and radically reduce transaction costs, thus creating the emergence of new decentralized organizational structures—*decentralized governance*—that were not feasible before.

This disruptive potential is explored through the cases of Bitcoin, *TheDAO*, and Ethereum, chosen for the revelatory insights they offer as early and extreme exemplars of blockchain use cases (Eisenhardt & Graebner, 2007). In particular, analysis draws on auto-ethnographic insights (Empson, 2012) from the author's direct personal experience as a curator within the *TheDAO* project (May–August 2016).

Analysis demonstrates that while ideals like *trustless trust*, *decentralization*, and *governance by code* sound simple and promising in theory, the reality of early use cases paints a more complex picture. The use cases of Bitcoin and *TheDAO* demonstrate that for the moment, these ideals are partially aspirational rather than a reality. All of which raises certain issues, including: (1) while machine consensus through auto-enforceable code running on a P2P network can radically reduce transaction costs and solve certain principal–agent problems, the question of how such pre-defined auto-enforceable code can withstand time has not been resolved; (2) centralization and the requirement to trust experts will prevail around expert opinion, thus creating new principal–agent problems that have yet to be addressed; (3) the need for development of decentralized information, communication, and transparency tools as a basis for decentralized consensus-reaching.

Assuming that blockchain protocols could become the constitutional layer for all our future transactions, the article argues that in addition to existing automated consensus rules, further exploration of additional governance and communication structures is required to maintain systems flexible enough to endure over time, as well as cope with unforeseen edge cases.

* JEL classification codes: C70, D20, D23, D70, M15.

2 | BLOCKCHAIN, SMART CONTRACTS, AND DAOS

Blockchain currently seems to be a driving technology behind the next-generation Internet, referred to by some as the "decentral web" or Web 3.0 (Wood, 2014). It relies on a P2P network of computers, where all the members of the network maintain a distributed, shared, trusted, public ledger of transactions which everyone can inspect, but that no single user controls. Distributed consensus based on game-theoretical incentive mechanisms, combined with cryptography, allows for anonymous yet secure P2P validation of transactions, thus bypassing the need for traditional trusted third parties (Nakamoto, 2008).

Blockchain can record transactions between two parties efficiently and in a verifiable and permanent way (Iansiti & Lakhani, 2017). Instead of a single trusted third party validating transactions through their servers with authority, a peer-to-peer network of computers running the blockchain protocol validates transactions by consensus. These formalized, pre-defined governance rules are stored in the consensus layer (see Figure 1 later) that manages and auto-enforces the transactions of all participants in the network. Blockchain first came to prominence in October 2008 as part of a proposal for Bitcoin (Nakamoto, 2008), a digital currency without the need for banks.

It is important to note that while Bitcoin refers to the Bitcoin protocol and the Bitcoin P2P network of participating computers, it is also the name of a native token of transaction, the Bitcoin token (BTC), which can be exchanged for fiat currency like USD or EUR. Native blockchain tokens represent assets, and are an integral part of the governance rules embedded in the consensus layer. Tokens are designed as part of an incentive scheme to manage the behavioral rule-set of all stakeholders in the blockchain network offering (1) financial rewards for correctly validating transactions on the blockchain according to the consensus rules defined in the protocol and (2) spam prevention through transaction fees (Nakamoto, 2008). Given that tokens can be endowed with certain attributes, other blockchains with other token governance rule-sets can be envisaged and have, indeed, emerged over time (e.g. Taghiyeva, Abdu, Mellish, & Ta'eed, 2017). Ethereum is one example of a blockchain with an alternate set of governance rules, and its native token Ether (ETH) has quite different properties from Bitcoin.

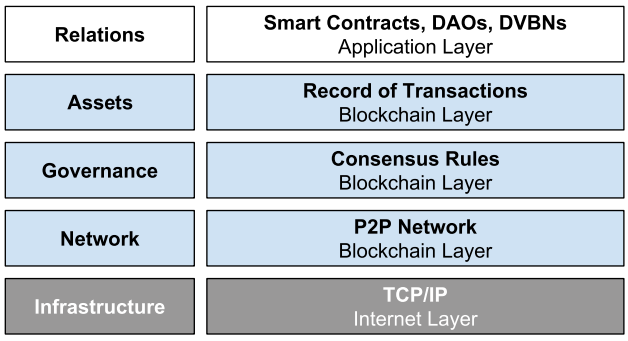

FIGURE 1 Blockchain technology stack of Ethereum and similar blockchains [Color figure can be viewed at wileyonlinelibrary.com]

While Bitcoin was originally designed for P2P money only, it soon became apparent that the underlying blockchain technology could be used for any kind of P2P value transaction on top of the Internet. The Ethereum project thus introduced the idea of decoupling the smart contract layer from the blockchain layer, where the ledger itself is used by smart contracts that trigger transactions automatically when certain pre-defined conditions are met (Buterin, 2013). By decoupling the smart contract layer from the blockchain layer, blockchains like Ethereum aim to provide a more flexible development environment than the Bitcoin blockchain. In such a setup, the governance rules of transactions can now be flexibly defined by the parties to a smart contract, instead of defining all governance rules directly in the consensus layer of the blockchain (**Figure 1**).

The most complex form of a smart contract is a decentralized autonomous organization (DAO), governing a group of people who share the same interests and goals. DAOs run according to a set of token governance rules written in code of the application layer, obviating the need for human management involvement. These token governance rules, of the blockchain layer and the application layer alike, have the potential to disrupt governance as we know it.

3 | DISRUPTING GOVERNANCE WITH BLOCKCHAIN

Governance refers to the way rules, norms, and actions of how people interact with each other are structured, sustained, regulated, and held accountable. It is about regulating decision-making processes among actors involved in a collective problem, leading to the creation, reinforcement, or reproduction of social norms and institutions (Bevir, 2013). The degree of formality depends on the internal rules of a given organization and, externally, with its business partners. As such, governance may take many forms, driven by different motivations and with different results (Hufty, 2011). In the context of this article, governance refers to the processes of governing, whether by a government, market, organization, network, family, or tribe—formal or informal—through laws, norms, power, or language.

A traditional view of organizational and political governance structures emphasizes centralization and hierarchy, with various degrees of rigid top-down command and control decisions making rule-sets. Blockchain promises more decentralized and spontaneous coordination by addressing two problems of traditional centralized governance structures: the *principal–agent dilemma* and high *transaction costs of coordination*.

The *principal–agent* dilemma occurs when the agent (a person or entity) is empowered to make decisions on behalf of, or impacting, a so-called principal (another person or entity): the agent is assumed to be a self-interested utility maximizer who will pursue their own self-interests over and above the wishes of the principal in the absence of threats, sanctions, or inducements (Eisenhardt, 1989). In such setups, moral hazard occurs if one person takes more risks because someone else bears the cost of those risks, usually when underlying information asymmetry is at play. In the context of governance, examples of

the principal–agent dilemma include the relationship between corporate management and shareholders, or that between a political and bureaucratic elite and voters (Jensen & Meckling, 2009). Various mechanisms have been devised to align the interests of principals and agents, such as profit-sharing models for employees. Blockchain and smart contracts introduce new ways of aligning interests and governing groups of people in a much more decentralized way (Tapscott & Tapscott, 2016).

Furthermore, blockchains and smart contracts reduce *transaction costs* of reaching an agreement, formalization and enforcement of relationships between people, institutions, and the assets they own, by standardizing transaction rules (Glatz, 2014). The transaction rule-sets (agreement) of the smart contract define the conditions—rights and obligations—to which parties are bound by a smart contract consent. They are often pre-defined, and agreement is reached by simple opt-in actions. They are formalized in digital form, in machine-readable code (formalization). These rights and obligations established in the smart contract can now be automatically executed by a computer or a network of computers as soon as the parties have come to an agreement and met the conditions of the agreement (enforcement) (Glatz, 2014).

This auto-enforceable code of the blockchain layer, as well as the smart contract layer, radically reduces bureaucracy and thus transaction costs, replacing traditional middle men with machine consensus. Furthermore, token governance rule-sets of permissionless public blockchains, powered by game-theoretical incentive schemes, provide simple opt-in and opt-out mechanisms rather than traditional top-down structured organizations. These token governance rule-sets of the consensus layer allow for much simpler coordination of a disparate group of people who do not know or trust each other.

At a conceptual level, blockchains, smart contracts, and DAOs can therefore eradicate the agency problem and reduce transaction costs. An examination of pioneering blockchain applications permits insight into how the technology might be used in the future to disrupt governance in organizational and political domains. The following sections showcase first use cases, analyze learnings, and outline a future roadmap to decentralized governance.

4 | ORGANIZATIONAL GOVERNANCE

According to economist Ronald Coase (1937), individuals choose to form companies, partnerships, and other business entities only if it is more efficient for them to do so than to engage in bilateral trading in the marketplace. He argues that firms arise when they can arrange to produce what they need internally more cheaply than through outsourcing, taking into account all costs like search, information acquisition, bargaining, policing, and implementation (Dahlman, 1979). His theories explain the concentration of economic production, through vertical integration of production, and the subsequent rise of multinational corporations, from the Industrial Revolution until the late twentieth century.

Organizations can be structured and governed in different ways, expressing the allocation of responsibilities for different purposes, functions, and processes to different entities such as the branch, department, workgroup, or individual (Feldman & Miller, 1986). Organizational structures have been a dynamic phenomenon since at least the Industrial Revolution (Giddens, 1984). The highly structured, centralized, and bureaucratic organizations of the twentieth century have, in recent decades, given way to looser, flatter organizational forms such as Holacracy, which is organized around autonomous and self-reliant units, that also depend on the greater whole of which they are part, with iterative governance, adaptive decision processes, and high self-organization (Robertson, 2007). However, traditional organizational structures always require some form of management, even if they are flatter, as in the case of Holacracy, where the decision-making process is more distributed, but still highly centralized around each holon, with rigid and programmatic communication rules.

The Internet, as an information-sharing technology, has facilitated much of this organizational innovation, but while Web 2.0 has enabled the emergence of new forms of organizing around, for example, the prosumer (Toffler, 1984), there remains one powerful intermediary, a giant trusted third party—like Amazon, eBay, Zalando, Uber, Airbnb, Facebook, Twitter, and so on—providing a trusted platform for A and B, who mostly don't know each other, to interact. While products and services around those platforms have become more and more unbundled, bringing producers and consumers closer to each other, the terms of service are always dictated by that one trusted third party in the middle.

Blockchain and smart contracts can disintermediate these platforms, introducing new ways of coordinating activities such as task allocation, coordination, and supervision of a group of people who share common economic interests, but are geographically distributed, without the necessity of a centrally managed organization. This could be possible with DAOs, or through automatic self-alignment around Schelling points.

4.1 | Blockchain solution 1: DAOs

DAOs are the most complex form of a smart contract on a blockchain, where its governance is embedded into the code of the smart contract using complex token governance rules. Historically, the Bitcoin network is considered the first truly autonomous organization governed solely through a distributed consensus protocol, which anybody is free to adopt. Today, DAOs are moving up the technology stack, thereby becoming fully virtualized through software, code executed on top of an increasingly opaque stack of distributed networking, and consensus technology such as the Ethereum blockchain or similar.

As governance rules are defined in the code and automatically executed, mundane central coordination and administrative and executive functions can be automated. Expert know how, on the other hand, has to be replaced with subcontractors serving the specific needs of the DAO. Token holders of a DAO can now appoint such subcontractors based on the token governance rules defined in the smart contract of the DAO (Buterin, 2014).

Blockchain therefore represents an incentive network, powered by the governance rules tied to its cryptographic tokens. These tokens

are for people what code is for machines—a means of programming their behavior. Since these tokens have a monetary value tied to them, they have proved to be effective motivators, triggering basic survival instincts. We will likely see many more DAOs, with a wide range of purposes, evolve on top of the technology that Bitcoin once pioneered (Olpinski, 2016b).

In this context, Bitcoin can be regarded as the first use case of blockchain, just like email was one of the first killer applications of the early Internet. Blockchain and other decentralized protocols could be seen as an operating system for the *economic web* (Olpinski, 2016b).

4.2 | Blockchain solution 2: Automatic coordination and Schelling points

Schelling points are named after economist Thomas Schelling, who was researching coordination of multiple parties in the absence of communication with economic game theory. He identified focal points—later referred to by others as Schelling points—as a solution that participants to a coordination game are drawn to use because it seems special to them. Schelling points are similar to social norms, which can be regarded as *appropriate* behavior adopted by most members of a society without the use of explicit laws and legislation. It is an agreement over "what people expect that others expect them to be expected" (Schelling, 1960).

Schelling points allow people to converge on a mutually consistent decision framework, in the absence of direct communication and centralized coordination (management). In the context of Web 2.0, social media, and e-commerce platforms, Schelling points can describe how users self-coordinate through the mechanisms of ratings and reputation systems, as well as through likes, shares, and follows on social networks to achieve community consensus.

However, rather than being wholly community-derived, the consensus reached on Web 2.0 platforms is driven by algorithms that are determined centrally by the engineers and managers of the "trusted intermediary," the organizational owner of the platform. Furthermore, the process is paid for largely by the provision of online advertising and the monetization of private user data through big data analytics (George, Haas, & Pentland, 2014). Until the emergence of blockchains, an alternative model in which users were directly rewarded for their participation in a network was unavailable due to the expectation of free content and the psychological barrier to online paywalls; unaffordable transaction costs for micro-payments; and intellectual property uncertainties of shared and modified content.[†]

However, blockchains—as an operating system for smart contracts—create novel opportunities for economic alignment, shared purpose, and coordination between distributed, trustless individuals, at negligible cost. It can be envisaged that, through the shared use of the tokens of a particular blockchain, users have a vested interest in the success of that token. They are economically aligned proportionally to their stake in whichever token they commonly hold. Economic networks, or Web 3.0 (**Figure 2**), consist of networks of people linked by ownership of the same tokens (Olpinski, 2016b). On this basis, blockchain can provide an economic transaction layer: a web of humans transacting as economic agents using the blockchains as the interaction mechanism, with their underlying cryptographic tokens

[†] For example, a Facebook user cannot be paid for content she/he uploads and shares that was created by a third party (say user-generated YouTube videos to a *CNN* news piece) which is stored on the platform, in this case Facebook's servers, that she/he does not own and has consented to cease all right to uploaded, often third-party, content. Even though a Facebook user creates value by aggregating content and becoming a focal point of interest for their followers, the current model does not compensate them economically for the value they are providing, and it is not rewarding the consumer who is paying attention to that shared content. Furthermore, the user has no certainty over intellectual property rights claims of the content users shared, as they are not transparently communicated. On the blockchain, through smart contracts, the IP of content can easily be managed and auto-executed, without any uncertainties.

	Network	Graphs	Connection	Relationships	Discovery	Platform
Web1	**Document Network**	Web of **Static Pages**	**Hyperlinks**	**Semantic** (shared keywords)	**Keyword Search**	**Google**
Web2	**Social Network**	Web of **People**	**Social Links** (likes, shares, upvotes, follows, etc.)	**Social** (shared friends)	**Social Feeds**	**Facebook**
Web3	**Incentive Network**	Web of **Economic Transactions**	**Economic Links** (Bitcoin, Ether, etc.)	**Economic** (shared interests)	**?**	**?**

FIGURE 2 The economic web matrix

Source: Olpinski (2016a).

serving as a critical component of the emerging economic web built on top of the blockchain.

Blockchain and token-based incentives of the economic web are still in the very early stages of development. At such an early stage, it is unclear what kind of reward, attention, and coordination systems will evolve in a blockchain ecosystem. Will producers get compensated for providing information and services? Will aggregators be paid for filtering information and services by becoming focal points of interest? Or will users get rewarded for paying attention because information is vast and attention time is limited? Most likely it will be a mix of all, with attention becoming the more scarce resource.

At the birth of the Internet, developers sought methods to provide a discovery layer for web content, the search engines. Whereas Yahoo sought to catalogue content, Google exploited links between sites to underpin its approach to search: Yahoo missed critical signals that were native to the network they wanted to curate. Similarly, we currently lack a search facility native to the reputational signals of the token-based economic networks of the blockchain (Olpinski, 2016a). Solving that problem might be the answer to automatic alignment of interests and a completely new form of decentralized governance through automatic alignment, of an anonymous and distributed group of people, in a trustless trust environment, purely through reputational and economic incentive mechanisms.

5 | POLITICAL GOVERNANCE

Democracy is a system of governance where people who are affected by collective decisions of the group they belong to, should be able to participate in said decisions. The question of how individuals should participate is and has been the source of many debates and conflicts and evolved over time.

Direct democracy is a form of democracy in which people decide policy initiatives directly. Large societies make it impossible for citizens to participate in each and every decision-making process due to (1) the collective economic transaction costs of the voting process; (2) information asymmetries between specialists and average voters who would have to vote on issues they might not (fully) understand or would need to spend time to study and understand; (3) the time-consuming decision and voting process due to the sheer amount of decisions one would need to participate in. These transaction costs of coordinating large groups of people in a direct democratic manner have led to hierarchical top-down structures, similar to the ones we know in big corporations, with centralized institutions, bureaucratic organizational structures, that have emerged around modern representative democracies.

Modern representative democracy is a system of governance in which, typically, elected representatives govern on behalf of all the (eligible) members of a state. It provides: (1) a political system for choosing and replacing the government through free and fair elections; (2) a system of checks and balances; (3) protection of the human rights of all citizens; and (4) a rule of law, in which the laws and procedures apply equally to all citizens (O'Donnell, 2005).

Both systems, representative and direct democracies, have merits and deficiencies (Matsusaka, 2005). For example, voters may be irrational or ill-informed (Caplan, 2005); systems may be susceptible to the principal–agent problem, where political elites make decisions in their own not their constituents' best interests (Montesquieu, 2008), or run the risk of populism (Wright & De Filippi, 2015); in a majority system, it can be difficult to cater to and protect the rights of minorities (Fierlbeck, 1998).

Recent political history suggests high levels of disenchantment with established political governance systems, the emergence of a post-democratic system characterized by a growing and increasingly remote aristocratic governing elite, coupled with increased clamor from the citizenry to reclaim their place in decision-making (Crouch, 2000).

One suggested solution to this disenchantment is liquid democracy, a form of democratic governance whereby an electorate vests voting power in delegates rather than in representatives, and allows for differentiation in the powers delegated (Ford, 2014). In this way, liquid democracy is a way of making collaborative decisions, which does not depend on elected representatives, but rather on the transient delegation of votes (Paulin, 2014).

While liquid democracy may offer a solution to some of the problems of established democratic systems, the transaction costs of such systems can be high. The Internet, especially with the advent of blockchains, smart contracts, and Web 3.0, radically reduces transaction costs, possibly eliminates many of the above-mentioned agency problems, and offers the possibility of decentralized virtual borderless nations. Furthermore, the implementation of dominant assurance contracts may also offer a non-governmental solution to the provision of goods and services traditionally supplied by governments.

5.1 | Decentralized virtual borderless nations

The relative success of bitcoin challenges the notion, perhaps counter-intuitively, that national governments are a necessary condition to establish functioning currency systems. Applying the same principle to other services traditionally supplied by governments, BitNation proposes the notion of the decentralized virtual borderless nation (DVBN).

DVBNs are simply DAOs that coordinate the provision of (traditional) government services such as registration of births, marriages, and deaths, through smart contracts on top of a blockchain. By potentially programming laws, rules, and regulations into a smart contract on top of a blockchain, the traditional role of bureaucrats and politicians in executive roles as we know it is being challenged.

BitNation is a blockchain-based initiative proposing an alternative to the current status quo, where citizens are bound to the nation states and legal silo they are born into. BitNation assumes that citizens are simply consumers of government services, which are paid for with taxes. Government can therefore be seen as a big and complex public organization, a trusted third party that has a monopoly of provision of certain services for its citizens.

BitNation proposes providing the same services as traditional governments, with the difference of being geographically unbound,

decentralized, and voluntary, where anyone will be able to create their own virtual nation on top of what they call "Pangea blockchain jurisdiction." They are working on a DIY governance client that allows anyone to operationalize their own virtual nation on a smart contract-powered, peer-to-peer and end-to-end encrypted platform, the Ethereum blockchain. They purport to offer choice in the consumption of government services in the same way citizens have choice over which brand of breakfast cereal they buy. Through the offer of DIY DVBN building, users can overcome the constraints of "geographical apartheid" (Tarkowski Tempelhof et al., 2014) and move more freely than is possible within existing governance structures.

Much of BitNation's effort to date remains in proof-of-concept mode, but it has triggered widespread interest not least because it appears to resonate well with current political frustrations among many citizens worldwide, touching upon a desire to find new answers to the inefficiencies of existing political structures.

5.2 | Dominant assurance contracts

Tabarrok (1998) argues that some types of public good—traditionally those that are the preserve of government provision or protection—can be produced privately by profit-seeking entrepreneurs using a modified form of assurance contract, called a dominant assurance contract.

A simple assurance contract is a game-theoretic mechanism and a financial technology that facilitates the voluntary creation of public goods in the face of the free-rider problem. People pledge to fund a (public) good if and only if enough others pledge to fund the (public) good. Assurance contracts have become common in practice since the advent of Web 2.0 thanks to organizations like Groupon and Kickstarter that implemented business models using ideas of assurance contracts. Dominant assurance contracts introduce an additional feature: an entrepreneur agrees to produce a certain good if amount X is raised by date D. Further, he commits to pay a fee Y to each contributor if the desired amount X is not raised by date D, or to pay a fee Y if the originally envisioned amount X is raised but the entrepreneur fails to produce the good meeting pre-specified criteria.

Committing to the provision of public goods thus becomes a no-lose proposition: in game-theoretic terms, a "dominant strategy." If sufficient funds are pledged, the good is produced; if not, then those who have pledged are compensated with a prize. Thus, Tabarrok (1998) demonstrates theoretically that some types of public good can be produced privately by profit-seeking entrepreneurs. In such a setup, blockchains and smart contracts could radically reduce transaction costs of self-alignment amongst interested individuals who do not know or trust each other but share a common goal, and be a new possibility to funding the production of public goods.

However, Tabarrok's theories are based on invisible-hand explanations, assuming rational actors as economic agents to a game with incomplete information, and remain to be tested for large-scale projects.

6 | ANALYZING DAO USE CASES

Blockchains and smart contracts appear to have much promise to disrupt traditional governance. Their most disruptive influence may be in the reduction of transaction costs amongst disparate individuals, enabling them to align over shared interests through DAOs. Relatively few applications have actually been implemented so far. For the purpose of demonstration, this article presents the cases of (1) Bitcoin and (2) *TheDAO* and subsequent Ethereum hard fork.

These cases merely intend to give an insight into the possibilities and current limitations of DAOs. A simple comparison of these cases is not possible due to: technological differences, which are beyond the scope of this article to explain; differences of dominant blockchain philosophies of the core community of said blockchains; maturity of the technology and age of the network. While Bitcoin has existed since 2009, Ethereum went live mid-2015.

Furthermore, it is important to note that Bitcoin is the closest use case for a truly decentralized and autonomous organization to date, without any single legal entity in the background to be held accountable for its actions. While Bitcoin's development is driven by a leaderless open-source community, in a rather transparent way, with an anonymous creator who, as best we can tell, disappeared in the early stages of Bitcoin's creation, Ethereum remains led by its original creator, who is publicly known and outspoken, with a centralized institution in the background, the Ethereum Foundation, that can be held accountable by national regulators. Ethereum developers claim that development is consensus-driven, however internal communication as well as the decision-making process are not always fully transparent. The same applies to legal compliance, marketing, and other organizational decisions the foundation members execute.

Regardless of these differences, both cases paint a similar picture of the potentials and challenges around decentralized governance on the blockchain.

6.1 | Bitcoin use case

The aim of the Bitcoin network is to provide an operating system for money without banks. Historically, the Bitcoin network can be considered as the first truly autonomous organization governed solely through a distributed consensus protocol, which anybody is free to adopt.

The consensus rules of the Bitcoin network govern how the participants in the network interact with each other, defining among others: under which conditions Bitcoins are created; under which conditions sending money from A to B is valid; the transaction costs related to sending money from A to B; the incentive mechanism for validating transactions with a cryptographic token; and the implicit rules of how to change current consensus rules.

While, in traditional organizational models, the roles of the different stakeholders are well understood, reasonably stable, and often codified, in the Bitcoin model the role of stakeholders is more fluid. Any stakeholder of the network can opt-in and opt-out at any time, without permission of a central authority, but always within the

governance rule-sets of the underlying Bitcoin protocol. Stakeholders contribute to the Bitcoin network—the P2P Bitcoin organization—on an ad hoc basis depending on the levels of incentive available matched against their disposable resources. The nature of participation is transparent and regulated through auto-enforceable code.

Stakeholders of the Bitcoin network provide a range of services, including: provision of IT infrastructure (Bitcoin miners); writing code (Bitcoin developers); providing value-added services (Bitcoin exchanges); marketing (any stakeholder promoting the idea of Bitcoin through blogs, social media channels, private communication—online or offline). They perform actions in the physical world because Bitcoin's incentive mechanism makes it profitable for them to do so.

The existence of Bitcoin since 2009 has demonstrated the efficacy of blockchain technology in enabling economic coordination on a global scale while massively reducing prohibitively high transaction costs. The reduction in costs and the feasibility of automatically aligning interests of disparate individuals through governance rules at the consensus layer offer significant opportunities for business model innovation. However, there remain significant challenges related to the distillation of governance principles to lines of code at the consensus layer of the protocol. Some selected conflicts are outlined in **Box** 1.

6.2 | *TheDAO* and Ethereum use case

The most prominent DAO example on top of the Ethereum blockchain was *TheDAO*. The name is somewhat unfortunate and misleading, as *TheDAO* is a DAO with a specific purpose, and should not be confused with the general concept of DAOs that can have any kind of purpose.

BOX 1 BITCOIN'S CHALLENGES

The Bitcoin network faces something of a constitutional crisis as it seeks to address two barriers to its more widespread adoption: scalability, the speed of the network, or lack thereof, with only a handful of transactions getting verified per second, which is not enough for scalable business applications; and transaction fees, which are rising steadily, threatening to eliminate the competitive advantage that Bitcoin once had. While most people in the Bitcoin community acknowledge these problems as an obstacle to widespread adoption of the Bitcoin network, the solutions proposed vary greatly, the two most prominent being "segregated witness" (SegWit) and increasing Bitcoin's block size.

SegWit. This has been proposed by Bitcoin Core developers, who develop the market-dominant Bitcoin client, with over 90% market share, and who are funded by a private company called Blockstream. SegWit proposes to separate (seg) transaction signatures (witnesses) from the transactions, which would make them smaller in size and allow more transactions to be included in blocks, making the process more efficient. SegWit implementation would require a so-called *soft fork* of the network, which means that it needs a 95% approval rate of all Bitcoin miners over a 12-month period to upgrade the protocol to allow SegWit. The proposal remains contentious within the community.

Block size debate. Other, less market-dominant Bitcoin client developers, like Bitcoin XT and Bitcoin Classic, seem to favor on-chain scaling solutions like block size increase over SegWit. In Bitcoin Core, the market-dominant client, block size is limited to 1 MB. An outspoken critic of that block size limit has created his own full-node software client, Bitcoin Unlimited, where the hard limit is removed, allowing users to determine the block size by consensus (Hertig, 2016). Other mining pools with significant market shares, like ViaBTC with a network share of around 7.7%, also support the idea of increasing block size, a process named block size hard fork, over the SegWit option. From a current point of view, unless circumstances change drastically, SegWit seems unlikely (Caffyn, 2015).

Information and communication—the Bitcoin reddit problem. There are two important subreddits where information and discussion happen: r/Bitcoin and r/BTC. r/Bitcoin, with around 200,000 followers, is mainly controlled by the Bitcoin Core team. This subreddit has been criticized as it performs censorship as discussions about Bitcoin block size increases are not welcomed, and sometimes even deleted. r/BTC claims to be more open and has turned out to be the "block size increase subreddit," but has far fewer followers. It is doubtful whether enough people are aware of the smaller subreddit. Newcomers might be more likely to only read the r/Bitcoin subreddit, possibly getting influenced by the SegWit discussions that happen there.

Unaligned economic interests. The most powerful stakeholders with regard to change management on the Bitcoin blockchain are *miners* and *exchanges*. While the power of Bitcoin miners is hard coded in the consensus layer of the Bitcoin protocol, the power of exchange services is driven by market mechanisms. Miners seem to favor the status quo of the protocol, since users are currently paying the highest transaction fees since the creation of Bitcoin. While the network is still stable, miners are enjoying big profits. With a block size increase, the miners' fees will fall drastically. On the other hand, if SegWit gets deployed, miners might also face decreased transaction fees. Both scenarios are unfavorable for miners, who seem to have short-term economic interest in mind. Exchanges seem indifferent, since transactions on their platform happen off chain, and only deposits and withdrawals need the blockchain.

The initial creators of *TheDAO* code wanted to let the future token holders of *TheDAO* name the project once it went live after the initial cryptocurrency-based crowdfunding round, called a "crowdsale," but the naming never happened.

TheDAO was originally designed to be a decentralized and fully autonomous funding vehicle without fund managers for Ethereum-based projects. The idea was that anyone with an idea for a project related to the Ethereum ecosystem could submit proposals to *TheDAO*, and that token holders of *TheDAO* could decide, in proportion to the number of tokens they held, which projects they wanted to fund. To become a token holder, a four-week crowdsale in May 2016 was launched where anyone could obtain *TheDAO* tokens in exchange for the Ethereum token Ether. These *TheDAO* tokens were also later traded on cryptocurrency exchanges.

TheDAO token sale surpassed everyone's expectations, selling approximately USD$160m worth of Ether, with over 20,000 people participating, and became an unanticipated honeypot for hackers. Before operations could start, *TheDAO* smart contract was temporarily drained of roughly USD$50m by an unknown attacker. The *TheDAO* and Ethereum communities were faced with the decision of how to respond (see **Box** 2).

7 | DISCUSSION

Both cases, Bitcoin's "constitutional crisis" and the division of the Ethereum community over how to deal with the *TheDAO* "infiltration," are testament to the challenges of concepts like *trustless trust*, *decentralization*, and *governance by code*.

A smart contract simply checks whether participants in a transaction comply with the rules pre-defined in the smart contract. If they do, the transaction is validated, if not, the transaction is rejected. They are auto-enforceable, but are also only as smart as the people who developed and audited them, based on the information available to

BOX 2 ETHEREUM'S CHALLENGES

The Ethereum community, which was closely linked with the *TheDAO* community, was heavily affected by the consequences of the US$50m drain, and had to decide whether and how to respond.

Options to address the issue of the tokens taken included adhering to the letter and spirit of blockchain immutability and doing nothing, or acknowledging that this was a special case in the life of an immature technology and so legitimizing the conduct of a hard fork—the equivalent of going back in time to before the breach, thus denying the attacker the opportunity to realize the drained assets. The debate divided the community, which had 35 days to reach a conclusion, before the attacker—based on the governance rules specified by the smart contract—could withdraw the Ether from the child DAO that s/he or they had split to (Siegel, 2016).

The incident sparked a lively debate about how consensus in the Ethereum community should or should not work. Critics from within the *TheDAO* and Ethereum communities, as well as those from the wider Bitcoin community, noted that *TheDAO* token holders never got a direct vote in the decision on how to resolve the breach. The question was resolved at the blockchain level (Ethereum) instead of at the application level (*TheDAO*). Furthermore, advocates of the Ethereum hard fork were accused of trying to bail out *TheDAO* for being "too big to fail." Outspoken critics asked why the Ethereum Foundation was interfering with *TheDAO* at all, and compared it with a government bailout of banks. According to the critics, going back in history and reverting transactions killed the idea of an immutable blockchain, the very USP of a blockchain, thus introducing censorship to a system that has promised to be censorship-resistant (De Filippi, 2016).

Purists insisted on the rule of code. The so-called *attacker*, they claimed, was not attacker but merely an individual who used the possibilities of the code to recursively send funds to his/her own address, a bug in the code of the *TheDAO* smart contract. Since the *TheDAO* code was referred to on the website as the only source of truth, the attacker, from this perspective, was in fact not an attacker at all, and blame lay with the people who wrote the code and promoted *TheDAO* in the first place.

A heated discussion broke out on the Internet, spread over various social networks. Communication channels were not clear. While some developers were communicating on reddit only, others were using Twitter, and some communicated on "Medium" platform. Token holders were following one or the other channel, or none at all, and trying to find updates on a website that was not updated as it was not centrally run. Furthermore, it was unclear to the average token holder who was a social media troll, with personal interest not aligned with the community, and who was an expert. Even the developers had problems keeping up-to-date with who said what.

In the end, after the 35-day period, the majority of the Ethereum community decided to adopt the highly disputed hard fork. This allowed the Ethereum community, which was closely tied to the *TheDAO* community, to reverse the attack at a protocol level. The stolen funds could be reclaimed by the original token holders. A minority of the community remained on the old blockchain, did not fork, and decided to name that blockchain Ethereum Classic (ETC), claiming to be the true, original, and uncensored Ethereum chain.

these people at the time of coding. As currently enacted, they lack the flexibility to accommodate unforeseen eventualities that existing institutional infrastructures can provide. How should the so-called "unknown unknowns" in a trustless trust environment be handled?

The *TheDAO* incident showed that the absence of dispute settlement and governance mechanisms for edge cases divided the community, at a smart contract level (token governance rules of *TheDAO*) as well as at the blockchain level (Ethereum governance). This inability to foresee "unknown unknowns," as in the case of the *TheDAO* incident, showed that smart contracts can only be a default state, which might need to be overruled by supermajority consensus within the relevant community whenever deemed necessary.

How easy is it to pre-define and pre-regulate all possible human interactions, including potential attack vectors of bad actors, with complex lines of code? How can complex smart contracts like DAOs withstand time without decentralized governance rules that are triggered in case of edge cases, where defined stakeholders of the network fulfill certain roles and are accountable for necessary decision-making?

Code does not write itself. It is prone to human error. While so-called *formal verification* in software development can reduce human error, it cannot eradicate all errors, or short-sighted assumptions. The implicit community assumptions about the definitiveness of code and the feasibility of code to cover such eventualities have been severely tested. Artificial intelligence may have some impact here but, for the time being, while code can simplify transactions, it remains susceptible to human bias. Therefore code can only be a default state, based on which consensus happens if and when necessary.

Similarly, the Bitcoin scaling debate—which has been going on for several years without any consensus for a solution currently in sight—demonstrates how inertia can result from inadequate governance rules that account for large-scale decisions in a multi-stakeholder environment with unaligned interests at stake. While the blockchain consensus layer is a crucial aspect of blockchain governance, it does not yet seem to be the answer to all governance questions.

Both cases show that in the absence of more flexible governance structures, the "movers and shakers" of the community inadvertently become the thought leaders and quasi-agents of the principal (the token holder and other stakeholders). This might lead to inertia (in the case of Bitcoin) or the splitting of the network (in the case of Ethereum).

The *TheDAO* incident and subsequent Ethereum hard fork also raise questions about censorship-resistance and immutability, also core principles of blockchain technologies. Advocates of the Ethereum hard fork were accused of censoring the blockchain, by going back in time and invalidating the transaction of the attacker. Outspoken critics of the hard fork claimed that certain stakeholders in and around the Ethereum Foundation were contravening the immutability of the blockchain—a core value of early blockchain advocates and the basis of concepts like *trustless trust*—driving the decisions for the hard fork in a top-down way, making decisions in a centralized manner.

On the other hand, advocates of the hard fork claimed that in a decentralized community like *TheDAO* or Ethereum, no one single entity can make such a decision without the majority of the community agreeing. They argued that, if there is consensus about changing the current consensus, then this cannot be called censorship, but rather a community-driven natural evolution of the code or state of the blockchain.

Furthermore, the *TheDAO* incident showed that while one might be able to get rid of traditional gatekeepers and command and control managers found in top-down systems, there remains a need for experts. While the vision of many blockchain advocates is decentralizing control through trustless trust, the community of token holders, who make decisions based on pre-defined consensus rules, must still trust the design judgment of those experts who, to complicate things, might not always be of the same opinion. Thus the community, relying on expert opinion, will still need to trust the opinion of these experts.

In a decentralized architecture, whether at the application level (DAO) or the blockchain level (Ethereum), such experts are more distributed, and none have executive power to decide what to do. However, they do concentrate power around their expert knowledge. In a principal–agent setup, moral hazard only occurs when information asymmetries are at play. The question is whether these software developers, who have the necessary know how and insight, are the new "quasi-agents" in distributed systems where code is law. Currently, only a handful of software developers and system architects understand the ins and outs of Ethereum, and could make a fully educated decision about protocol upgrades.

Therefore, centralization will likely coalesce around experts, developers, and system architects. The system will only be more distributed, allowing more diversity of opinions, if and when more people understand the code.

The fact that Bitcoin and Ethereum are open source and run in a meritocratic way does not necessarily guarantee full decentralization. While it is true that whoever has the knowledge and motivation to contribute code can become a community developer and make their voice heard, in reality, the required programming experience and in-depth mathematical know how might be considered an entry barrier, creating new principal–agent problems around understanding code, from simple smart contract codes to complex blockchain protocols (Walport, 2015; Wright & De Filippi, 2015).

Lack of transparency in the decision-making process was a key critique of the Ethereum Foundation. While many of the developers involved in the process of responding to the *TheDAO* attack claimed that the process was much more decentralized than it might have seemed, apparent lack of transparency in the decision-making processes within the Ethereum Foundation became an issue for many. In decentralized organizations, expert opinion is distributed and it is often difficult for any single user to acquire an overview of the knowledge being shared.

While it might be expected that the early adopters of Bitcoin and Ether (and those who bought into the *TheDAO* project) are above average in their conversance with the principles, practices, and philosophy of the blockchain, it is difficult—even for many of those experts—to find a coherent, consistent, and trustworthy dialogic narrative relating to the attack. The distributed nature of expertise, the multiple

channels of communication, and the current lack of effective reputation systems make it hard for stakeholders to follow the discussion. Who wins the argument in a chatroom, the loudest voice or the most authoritative source?

While issues of communication and information dissemination are also concerns of contemporary (political) centralized governance systems, blockchain communities are even more susceptible to such concerns. How should distributed community members reach consensus relating to constitutional and governance issues when expert knowledge is also decentralized? Where does reliable information come from, and what tools—such as visualizations and decision trees—are required to facilitate such processes?

Both the Bitcoin use case as well as the Ethereum use case show that if issues of information, moderation, transparency, aggregation, and reputation are not resolved, decentralization might become a meaningless phrase.

8 | CONCLUSION

This article has explored how blockchain as an engine for auto-enforceable smart contracts could disrupt traditional governance structures by reducing transaction costs and solving the agency issue of moral hazard, at least to a certain extent. Drawing on pioneer use cases, it demonstrates an apparent gap between initial conceptualizations of the blockchain and its first instantiations, particularly around ideas like trustless trust, complete decentralization, and immutability. It is shown that, as circumstances change, protocols can become inappropriate for the new environment—whether at a protocol level or an application level—and require modification. Modification happens through majority consensus, but reaching consensus on the blockchain is not easy, as demonstrated by the challenges the Bitcoin and Ethereum communities are currently facing.

If blockchains become widely adopted in the future, as the economic layer on top of the Internet, they will affect all our daily operations as citizens and consumers of goods and services alike. Therefore, the underlying governance rules encoded in those blockchains may represent the constitutional foundation of our future transactions, which will be governed, executed, and resolved through smart contracts, DAOs, and DVBNs. Now is the time to ask whether we want to adapt to new social, economic, and political circumstances, if and when they emerge in the future.

As we enter the era of blockchains and the decentralized web, and before we start building the next killer applications on these blockchains, we need to start thinking about how flexible, transparent, and inclusive we want the protocols to be, as they might represent our future constitutions or quasi-legal operating systems.

Future research must turn its attention to a series of important questions around governance, beyond code, information dissemination, communication and transparency, and new forms of principal–agent problems and power concentration. What are the design parameters of flexible governance structures that incorporate and align the interests of stakeholders and are concurrently flexible enough to withstand future shocks? How decentralized is decentralized, and will we need to introduce tools like "decentralization metrics"? What set of decentralized communication and information tools on top of Web 3.0 will support transparency in the decision-making process and enable decentralized consensus that does not produce hidden gatekeepers? Finally, how can a majority-based consensus system adequately protect and provide for minority interests, in particular where voting influence is weighted in proportion to the number of tokens held?

REFERENCES

Bevir, M. (2013). *Governance: A very short introduction*. Oxford: Oxford University Press.

Buterin, V. (2013). *A next generation smart contract and decentralized application platform*. Ethereum White Paper.

Buterin, V. (2014). *DAOs, DACs, DAs, and more: An incomplete terminology guide*. Retrieved from https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Caffyn, G. (2015) What is the Bitcoin block size debate and why does it matter? *CoinDesk*. Retrieved from http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/

Caplan, B. (2005). From Friedman to Wittman: The transformation of Chicago political economy. *Econ Journal Watch*, *2*(1), 1–21.

Coase, R. (1937) *The nature of the firm*. Oxford: Blackwell Publishing.

Crouch, C. (2000). *Coping with post-democracy*. London: Fabian Society.

Dahlman, C. J. (1979). The problem of externality. *Journal of Law and Economics*, *22*(1), 141–162.

De Filippi, P. (2016). *A $50M hack tests the values of communities run by code*. Retrieved from http://motherboard.vice.com/read/thedao

Eisenhardt, K. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57–74.

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

Empson, L. (2012). My affair with the "other": Identity journeys across the research–practice divide. *Journal of Management Inquiry*, *22*, 229–248.

Feldman, P., & Miller, D. (1986). Entity model clustering: Structuring a data model by abstraction. *The Computer Journal*, *29*(4), 348–360.

Fierlbeck, K. (1998). *Globalizing democracy: Power, legitimacy and the interpretation of democratic ideas*. Manchester: Manchester University Press.

Ford, B. (2014). Delegative democracy revisited. Retrieved from http://bford.github.io/2014/11/16/deleg.html

George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. *Academy of Management Journal*, *57*, 321–326.

Giddens, A. (1984). *The constitution of society*. Berkeley, CA: University of California Press.

Glatz, F. (2014). *What are smart contracts? In search of a consensus*. Retrieved from https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad#.hbqzgm9hc

Hertig, A. (2016). *A controversial Bitcoin alternative is seeking a comeback*. Retrieved from http://www.coindesk.com/controversial-bitcoin-alternative-seeking-comeback/

Hufty, M. (2011). Investigating policy processes: The governance analytical framework (GAF). In U. Wiesmann & H. Hurni (Eds.), *Research for*

sustainable development: Foundations, experiences, and perspectives (pp. 403–424). Bern: Geographica Bernensia.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127.

Jensen, M., & Meckling, W. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360.

Matsusaka, J. G. (2005). Direct democracy works. *Journal of Economic Perspectives*, *19*, 185–206.

Montesquieu, C.-L. de Secondat Baron de (2008). *Stanford encyclopedia of philosophy*. Retrieved from Plato.stanford.edu

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. White Paper.

O'Donnell, G. (2005). Why the rule of law matters. In L. Diamond & L. Morlino (Eds.), *Assessing the quality of democracy* (pp. 3–17). Baltimore, MD: Johns Hopkins University Press.

Olpinski, M. (2016a). *Why I no longer explain Ethereum as a "world computer."* Retrieved from https://medium.com/@maciejolpinski/why-i-no-longer-explain-ethereum-as-a-world-computer-5adf7220b3eb#.smx6d7vm2

Olpinski, M. (2016b). *Building "Google for the economic web" on the Ethereum blockchain*. Retrieved from Blockchain.https://blog.userfeeds.io/building-google-for-the-economic-web-on-the-ethereum-blockchain-de27cb3d23b#.ski5jhoye

Paulin, A. (2014). Through liquid democracy to sustainable non-bureaucratic government. *Proceedings of the International Conference for E-Democracy and Open Government*, pp. 205–217.

Robertson, B. (2007). Evolving organization. *Integral Leadership Review*, 7(3), June.

Schelling, T. C. (1960). *The strategy of conflict*. Cambridge, MA: Harvard University Press.

Siegel, D. (2016). *Understanding the TheDAO attack*. CoinDesk. Retrieved from http://www.coindesk.com/understanding-dao-hack-journalists/

Tabarrok, A. (1998). The private provision of public goods via dominant assurance contracts. *Public Choice*, *96*, 345–362.

Taghiyeva, M., Abdu, S., Mellish, B., & Ta'eed, O. (2017). *Impacting with value: Capture-Translate-Transact-Report*. Northampton, UK: Centre for Citizenship, Enterprise and Governance.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. London: Portfolio.

Tarkowski Tempelhof, S. (2014). Document retrieved from https://bravenewcoin.com/assets/Whitepapers/BITNATIONWhitepaper-INCOMPLETE.pdf

Toffler, A. (1984). *The rise of the prosumer: The third wave*. New York, NY: Bantam Books.

Walport, M. (2015). *FinTech futures. The UK as a world leader in financial technologies*. A report by the UK Government Chief Scientific Adviser. Retrieved from www.gov.uk/go-science: Government Office for Science

Werbach, K. (2016). *Trustless trust*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409

Wood, G. (2014). *Apps: What Web 3.0 looks like*. Retrieved from http://opensecrecy.com/dappsweb3.html

Wright, A., & De Filippi, P. (2015). *Decentralized blockchain technology and the rise of Lex Cryptographia*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

AUTHOR BIOGRAPHY

Shermin Voshmgir is the founder of *BlockchainHub*, which started in Berlin and has since panned out internationally. It is a decentralized network of autonomous hubs that inform, analyze, and discuss interdisciplinary implications of blockchain and the decentralized web. She is on the advisory board of the Estonian e-residency program, a curator of *TheDAO*, and regularly speaks at conferences and consults on blockchains and smart contracts. She used to work as an assistant professor and currently lectures on blockchain-related topics at Vienna University of Economics.

How to cite this article: Voshmgir S. Disrupting governance with blockchains and smart contracts. *Strategic Change*. 2017;26:499–509. https://doi.org/10.1002/jsc.2150