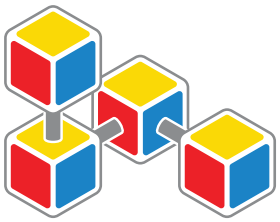
Governance of blockchain systems: Governance of and by Distributed Infrastructure

Primavera de Filippi, Greg Mcmullen



BLOCKCHAIN
RESEARCH
INSTITUTE

coala
COALITION OF AUTOMATED LEGAL APPLICATIONS

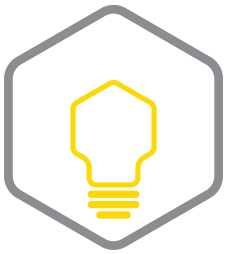
GOVERNANCE OF BLOCKCHAIN SYSTEMS

Governance *of* and *by* Distributed Infrastructure

Primavera De Filippi and Greg McMullen
Coalition of Automated Legal Applications

June 2018

A COALA + BLOCKCHAIN RESEARCH INSTITUTE BIG IDEA WHITEPAPER



Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, "the digital economy," with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights that will guide our members in achieving success.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the strategies, market opportunities, and implementation challenges of this nascent technology. Research projects are underway in the areas of financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as in the management of organizations and the transformation of the corporation.

Our findings, conclusions, and recommendations are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. Each research publication includes a video introduction by Don and an infographic for members' use in communicating these ideas throughout their organizations. To find out more, please visit www.blockchainresearchinstitute.org.

Management team

Don Tapscott – Co-Founder and Executive Chairman
Alex Tapscott – Co-Founder
Joan Bigham – Managing Director
Kirsten Sandberg – Editor-in-Chief
Jane Ricciardelli – Director of Marketing
Hilary Carter – Director of Research
Jenna Pilgrim – Director of Business Development
Maryantonett Flumian – Director of Client Experience
Luke Bradley – Director of Communications

Contents

Foreword 3

Idea in brief 4

Introduction 5

Unique features of blockchain systems 6

Decentralization 6

Cryptography and hashing functions 7

Immutability and auditability 8

The blockchain stack 9

The Internet layer 9

The role of Internet service providers 10

Barriers to participation: ISP data caps 11

Technical levers of influence: China's Great Firewall 12

Conclusion: Accounting for Internet-level governance 13

The blockchain layer 14

The application layer 15

Multiple layers of blockchain governance 16

Governance *by* the infrastructure 17

Governance *of* the infrastructure 18

Endogenous rules 18

Exogenous rules 20

Conclusion: Off-chain and on-chain governance 20

The DAO: A cautionary tale **21**

The smart contract, the attack, and the recovery 21

The limitations of on-chain governance 23

Lessons learned 25

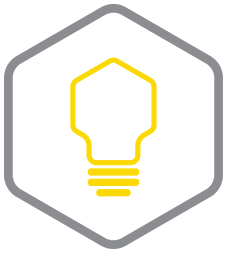
The distinctive features of blockchain governance **27**

Recommendations **29**

Appendix: Glossary **31**

About the authors **33**

Notes **34**



Foreword

As the foundational platform of the Fourth Industrial Revolution, blockchain technology enables such innovations as the Internet of things, robotics, artificial intelligence, machine learning, additive manufacturing, and smart supply chains so that more people can participate in the economy and benefit directly from the value they create.[1]

However, this extraordinary technology may be stalled, usurped, or otherwise suboptimized without governance. We do not mean government, regulation, or top-down, centralized control. Rather, we mean *stewardship*, a collaboration of stakeholders who are willing to identify their common interests and create incentives to align their behavior around blockchain systems as shared resources.

This research examines the impact of governance on blockchain systems. Specifically, it explores governance needs at three levels of the blockchain stack: the Internet layer, the blockchain layer, and the application layer. It is the third paper published in conjunction with Coalition of Automated Legal Applications, following its well-received papers on *Financing Open Blockchain Ecosystems: Toward Compliance and Innovation in Initial Coin Offerings* and *Regulatory Framework for Token Sales: An Overview of Relevant Laws and Regulations in Different Jurisdictions*.

The authors, Primavera De Filippi and Greg McMullen, share our view that, while decentralization is an advantageous design feature of blockchain systems, it requires the coordination of multiple and diverse actors with differing incentives to solve any problems that arise. They explain the difference between governance *by* the infrastructure and *of* the infrastructure. Given the state of the technology, they advocate for a hybrid approach that combines on-chain and off-chain elements rather than a code-only solution to stewardship.

Primavera has proven to be a very valuable and productive member of the Blockchain Research Institute. We are pleased that Greg signed on to co-author this report. He is a lawyer who investigates blockchain governance, privacy, intellectual property, and security. In addition to his legal practice, he is the co-founder of the Interplanetary Database Foundation and the former chief policy officer of ascribe.io and BigchainDB. Together they outline the lessons learned thus far and the work to be done, if we are to preserve and steward this nascent global resource so that it achieves its enormous potential.

DON TAPSCOTT
Co-Founder and Executive Chairman
Blockchain Research Institute

Idea in brief

Blockchain systems combine decentralized networks and cryptographic functions in novel ways, creating unique features that support the immutability and auditability of existing blockchain systems.

- *Blockchain governance* can refer to two concepts: either the governance of a blockchain system or the use of a blockchain system to govern an external organization or process. This report focuses on the former, the establishment and enforcement of rules and processes for the development and operation of blockchain systems.
- Blockchain systems combine decentralized networks and cryptographic functions in novel ways, creating unique features that support the immutability and auditability of existing blockchain systems. This report describes how these features present both opportunities and challenges for governing these systems.
- Any blockchain system is composed of multiple layers of technology forming a stack. Each layer brings additional capabilities to the previous layers and inherits their capabilities and limitations. Ultimately, all rules, policies, and constraints from the bottom layers determine what we can do in the layers built above them, in effect, forming a governance stack.
- Blockchain governance exists both on-chain and off-chain. On-chain rules are encoded directly into the underlying infrastructure of blockchain systems (governance *by* the infrastructure). Off-chain governance includes all other types of rules that might affect the operation or future development of a blockchain system (governance *of* the infrastructure).
- The distinctive characteristic of a blockchain system is that it is, by its very nature, decentralized and disintermediated. This stands in contrast with the other components of the technological stack, which have some characteristics of a decentralized system but are often controlled or governed by a centralized authority or intermediary operator.
- The hack of the DAO illustrates the dangers of favoring on-chain governance over off-chain governance. We need a more human-centric and hybrid approach that includes both on- and off-chain governance and preserves both the transparency and efficiency of on-chain governance and the flexibility and malleability of off-chain governance.

Introduction

Blockchain systems do not exist in a vacuum.

Blockchain systems do not exist in a vacuum. When we talk about blockchain governance, we need to think about the different layers of governance from the different layers of technology that both enable and constrain a particular blockchain system. The operations of a blockchain system—whether it is a blockchain network, framework, or application—are defined not only by the rules that govern that system but also by the underlying layers of Internet infrastructure, which both enable and constrain that particular blockchain system.

These multiple sets of rules ultimately fall into two fundamental categories—governance *by* the infrastructure and governance *of* the infrastructure—each of which is composed of endogenous rules, created internally by the community, and exogenous rules, imposed by third parties.

To illustrate the complexity inherent in blockchain governance, we first provide an overview of the multiple layers affecting the governance of a blockchain system, the characteristics of these different layers, and the possible interactions between them. We then look at how blockchain governance compares to or distinguishes itself from other forms of governance, with a particular focus on the distinction between the governance of centralized and decentralized systems, and the issues arising from the distinctive features of blockchain systems.

While centralized systems are subject to the whims of a central authority, which can exercise coercive force over the system, centralized systems are also much easier to regulate or govern. The central authority can easily modify or shut them down whenever a problem comes up. Conversely, decentralized blockchain systems operate peer to peer, without any central point of failure or control; and, therefore, no authority can alter it or shut it down. No one can exert influence except through the corruption or manipulation of a large quantity of network nodes.

On-chain *refers to rules encoded directly into the underlying infrastructure of blockchain systems.* Off-chain *refers to all other types of rules (endogenous or exogenous) that might affect these systems.*

Blockchain systems incorporate specific systems of rules and procedures that may be implemented both on-chain and off-chain. *On-chain* refers to rules that have been encoded directly into the underlying infrastructure of blockchain systems, whereas *off-chain* refers to all other types of rules (endogenous or exogenous) that might affect the operations and the future development of these systems. We will analyze the corresponding benefits and drawbacks of these two models as well as whether and when one model should prevail over the other.

We argue that the greatest benefit of each governance model also represents its greatest drawback. On-chain governance rules are more formal, strict, predictable, and often more efficient than their off-chain counterpart because they are clearly codified and automatically enforced by the underlying technology according to defined processes. However, on-chain rules are less adjustable to changing or unforeseen circumstances.

Conversely, off-chain governance rules are inherently ambiguous and malleable, but only the intervention of a third party authority can enforce—or attempt to enforce—them, case by case. Their advantage is that they can respond more humanely to edge cases, where a straightforward application of the rules would otherwise produce unfair outcomes. Off-chain rules can also evolve and adjust more easily to a changing environment. If necessary, we can use them to update or amend on-chain governance rules.

We emphasize the need for a more human-centric approach to blockchain governance that integrates on-chain and off-chain governance.

We conclude by highlighting the dangers of relying too heavily on on-chain governance at the expense of off-chain governance, and the dangers of focusing on endogenous rules while ignoring exogenous sources of authority and influence. We emphasize the need for a more human-centric approach to blockchain governance that integrates on-chain and off-chain governance, in ways that preserve the transparency and efficiency of on-chain governance rules, without foregoing the flexibility and malleability of off-chain governance rules.

Unique features of blockchain systems

Blockchain technology relies on a few core technological components—decentralized peer-to-peer networks, hashing functions, and public key cryptography—to create decentralized registries or databases whose content is largely immutable and readily auditable. This section will analyze the distinctive characteristics of these core components, along with their implications in the context of governance.

Decentralization

Advocates of decentralization hope it will lead to a more egalitarian society where power shifts from centralized authorities to a decentralized group of stakeholders, enabling a more even distribution of power and wealth. They believe decentralization will lead to increased participation and public engagement, and ultimately help people make decisions that promote the public interest rather than benefiting only a handful of powerful actors. However, the reality of decentralized governance is more complicated, in both theory and practice.

Advocates of decentralization hope it will lead to a more egalitarian society where power shifts from centralized authorities to a decentralized group of stakeholders.

From a theoretical perspective, the more people involved in the process of decision-making, the more difficult it becomes to agree on simple matters like what the group's goal should be. The level of difficulty increases for questions that are more complex. Numerous academic disciplines have thoroughly studied the problems of coordination and collective action in decentralization systems, and none has found a magic solution.[2]

Blockchain systems typically address the problem of distributed governance through cryptoeconomics, which combines cryptography with economics as its name suggests. Cryptoeconomics focuses on the design of specific incentives structures to reward the behavior that helps the network function properly, while discouraging behavior that leads to undesirable outcomes such as network congestion, overuse, or other forms of abuse. Yet these networks operate via traditional market dynamics, and unless there is an institution protecting them, they are likely to turn into highly concentrated and oligopolistic markets, dominated by a few powerful players.

Cryptoeconomics focuses on the design of specific incentives structures to reward the behavior that helps the network function properly, while discouraging behavior that leads to undesirable outcomes.

Besides, while cryptoeconomic incentives are useful to regulate the behavior of individuals interacting on a blockchain, there remains the question of who will be responsible for creating the incentive structure that defines the "rules of the game," and for embedding it into a particular blockchain system.

From a practical standpoint, we must address several technical problems for decentralized systems to work at scale. Theory and practice rarely align perfectly; emergent behavior or unanticipated situations can disrupt incentives and exacerbate tensions that the application of cryptoeconomics was meant to resolve. Moreover, as soon as we need to update or change the rules of the game—for example, to facilitate scaling or to resolve other technical challenges—the decision-making processes can devolve into contentious political questions related to the governance or design of the system.

One example that can illustrate both issues is the block size limit imposed in early versions of Bitcoin (discussed in more detail below), where an arbitrary technical limitation implemented during the early days of the network turned into a very contentious issue that, years later, ultimately led to the Bitcoin network splitting into several networks.

Cryptography and hashing functions

Blockchain systems leverage two key technological components to implement their novel features: cryptography and hashing functions.

Blockchain systems leverage two key technological components to implement their novel features: cryptography and hashing functions.

Hashing functions are algorithms that accept any data of any size as input, and then generate a fixed length string as an output. Hashing functions are deterministic: running the same hashing function on a particular input will always generate the same output. If even a single bit of the input is changed, then the output will be completely different. For example, providing the string "Hello world" as input to a common hashing function (MD5) will *always* generate a hash value of "3e25960a79dbc69b674cd4ec67a72c62"; but if we make the "h" lowercase instead of uppercase ("hello world"), the output hash is entirely different: "5eb63bbbe01eeed093cb22bb8f5acdc3" (see Figure 1, next page.)

This property makes the hashing function a powerful tool for verifying the integrity of data. In blockchain systems, each time a block is added to the chain, a hash of the previous block is included in the new block. By checking the recorded hash against the hash of the previous blocks, we can easily determine whether any data have been changed without verifying each transaction individually. If the hash does not match the expected value, then the data either are corrupted or have been tampered with.

In blockchain systems, each time a block is added to the chain, a hash of the previous block is included in the new block.

Public key cryptography is another important building block in any blockchain system. A public-private key pair defines ownership of assets (such as cryptocurrencies) on a blockchain network. Only the individual who controls the corresponding private key can use an asset associated with a specific public key. Because we can transact with an asset only after the relevant private key has signed the transaction, blockchain transactions are *non-repudiable*—that the transaction exists is proof that the agent who holds the corresponding private key has executed it.

Immutability and auditability

The combination of decentralized networks, hashing functions, and public key cryptography contributes to the immutability and auditability of blockchain systems.

The combination of decentralized networks, hashing functions, and public key cryptography contributes to the immutability and auditability of blockchain systems.

Immutability (or tamper-resistance) means that information written to the blockchain cannot be easily changed or deleted. The decentralized nature of a blockchain is such that the information it contains resides across a distributed network of computers, all of which store a copy of the blockchain. Because of this dispersion, no one can easily and unilaterally alter the stored data: all network participants will immediately detect and simply ignore any illegitimate modification.

Hashing functions enable us to determine easily whether the information recorded in a blockchain has been altered, because even the smallest change in any of the previous blocks would modify the hashes of all subsequent blocks, which would therefore need to be mined again. Therefore, while possible in theory, the cryptoeconomic incentives encoded into a blockchain network make tampering with a blockchain extremely difficult and costly in terms of money, energy, and time. Accordingly, unless someone controls more than

Figure 1: The difference an h makes

Input	Hello world (with capital H)	hello world (with lowercase h)
Output hash	3e25960a79dbc69b674cd4ec67a72c62	5eb63bbbe01eeed093cb22bb8f5acdc3

50 percent of the network, it is extremely unlikely that anyone can unilaterally modify the content of a blockchain.

Immutability presents novel challenges and opportunities. On the one hand, it means that no one has the power to censor specific transactions, thereby increasing both the transparency and auditability of blockchain-based applications. Blockchains provide a time-stamped record of events, visible to anyone who has access to that blockchain. In public blockchains, transactions can be accessed either by using an online blockchain explorer utility that displays the history of transactions (e.g., blockchain.info or etherscan.io) or by downloading the blockchain database.

Blockchains provide a time-stamped record of events, visible to anyone who has access to that blockchain.

On the other hand, to the extent that we can encode computer processes (known as *smart contracts* in blockchain parlance) into a blockchain system, these processes will continue to run as long as the blockchain network remains in operation; stopping such a program from executing on that network becomes extremely difficult. While bad actors cannot interfere with legitimate processes, good actors cannot halt harmful or dangerous processes.

Later in this paper, we look at the DAO, a *decentralized autonomous organization* designed for allocating venture capital; it was an immutable process that raised significant governance challenges. Use cases that are more dangerous, such as decentralized assassination markets, remain mostly hypothetical but exemplify the potential downfall of an immutable system.

The blockchain stack

Blockchain applications do not exist in a vacuum. They operate within a larger ecosystem of Internet applications that operate according to their own protocols and rules—a *stack* of applications and protocols that build on the layers (Figure 2, next page). Each new layer of the stack inherits the protocols and rules of the layer below, including the lower layers' governance. This section will describe the key elements of the blockchain stack and analyze the governance system that characterizes each of these elements. The next section will further break down these processes, exploring how the unique features of blockchain systems present unique opportunities and challenges for the governance of these systems.

Blockchain applications do not exist in a vacuum.

The Internet layer

Blockchain networks like Bitcoin and Ethereum exist at the bottom layer of the blockchain technology stack, but their operations depend on another technology stack: the Internet stack. Indeed, as a rule, blockchain networks are unable to operate without Internet connectivity. Because these networks operate on top of the Internet, their proper functioning is ultimately reliant on *transmission control*

protocol/Internet protocol (TCP/IP)—the protocols responsible for routing and transferring packets between nodes on the Internet. Accordingly, decisions at the Internet level can have a dramatic impact on the operation and governance of blockchain systems built on top of the Internet stack.

This section examines how choices made at the Internet level can affect critical factors related to the governance of blockchain networks, and even influence decisions regarding the development of those networks' protocols.

While blockchain systems are censorship-resistant, they are not entirely censorship-proof.

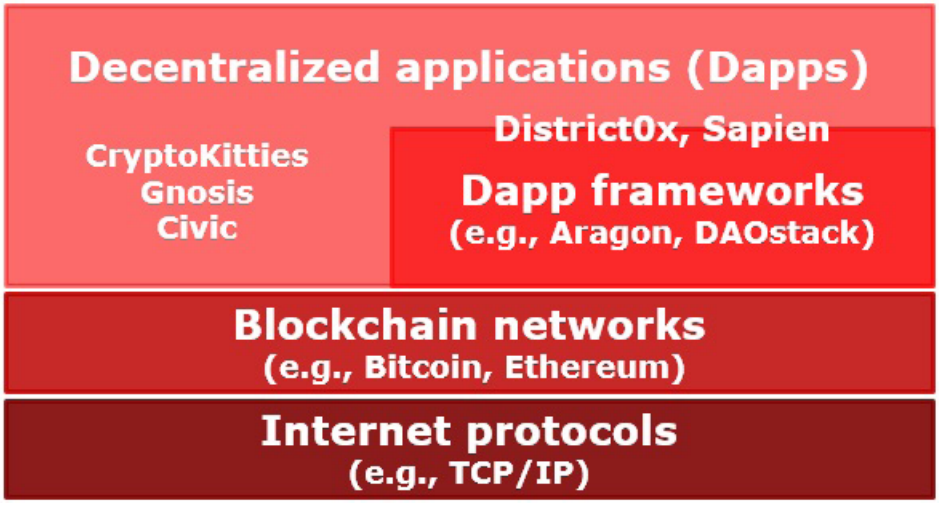
The role of Internet service providers

While blockchain systems are censorship-resistant, they are not entirely censorship-proof. In fact, because *Internet service providers* (ISPs) ultimately control the transportation layer of the Internet, they can discriminate against packets coming from or directed to any of these networks, if they so desire, thereby tampering with their operation. As a result, network management by ISPs or censorship by nation-states can influence the operation of blockchain systems, either by deliberately targeting their operation or as an unintended consequence of unrelated network management practices.

One of the foundational principles of the Internet is net neutrality, the idea that all traffic on the network should receive equal priority.

One of the foundational principles of the Internet is *net neutrality*, the idea that all traffic on the network should receive equal priority. Net neutrality states that information should be transmitted as it is received, no matter the sender or receiver, the port or protocol, the content type, or the application that created it. Net neutrality is critical for the operation of blockchain systems and other decentralized, peer-to-peer networks, as these networks rely on participants having unfettered access to the network.

Figure 2: The layers of the blockchain stack



Perhaps unsurprisingly, ISPs continue to push for an increased ability to offer paid priority services, prioritize their own bundled services, and downgrade or "throttle" content that competes with their offerings or that they deem to be too bandwidth-intensive. To protect Internet users against these practices and to encourage innovation and competition in network services, both the United States and the European Union had rules enshrining net neutrality in law, allowing only basic network management by ISPs when needed to keep the network running smoothly. However, in December 2017, the US Federal Communications Commission repealed its net neutrality rules, opening the door to increased interference at the Internet level.[3] Without these rules, ISPs are free to interfere in any number of ways: from slowing down or blocking network activity toward or from blockchain networks to prioritizing packets toward or from competing electronic payment services that are not subject to filtering.

Even if content is encrypted, analysis of multiple packets can often reveal their nature as well as the protocols or applications involved, and enable discrimination on this basis.

Let's consider *deep packet inspection* (DPI), a means for governments and ISPs to affect the operation of blockchain systems. TCP/IP routes data packets by looking at the address in the header of the packet and routing it along a particular path to its intended recipient. DPI examines the content of the packet: the network operator can determine the purpose of the packet and allow for content- or application-based discrimination. Even if content is encrypted, analysis of multiple packets can often reveal their nature as well as the protocols or applications involved, and enable discrimination on this basis.

Commercial vendors already offer products that use DPI to detect and block Bitcoin packets on corporate networks. There are rumors that China may be deploying similar technology to prevent connections to blockchain networks as part of a broader crackdown on cryptocurrencies. Governments and ISPs could apply DPI to restrict the use of cryptocurrencies or other blockchain systems, either within specific countries or around the world.

Governments and Internet service providers could apply deep packet inspection to restrict the use of cryptocurrencies or other blockchain systems, either within specific countries or around the world.

Barriers to participation: ISP data caps

Internet governance might also play a significant role in determining who is able to participate in the governance of specific blockchain networks. One clear example of Internet governance limiting participation in blockchain networks comes in the form of data caps imposed by ISPs. Many ISPs impose monthly caps on the amount of data customers can transfer in a given month.[4] Once customers exceed that cap, ISPs take a various approaches to recoup costs, including overage fees for data beyond the initial cap as well as reduced speed of service until the end of that billing period.

Active participation in the on-chain governance of a blockchain network is bandwidth-intensive. To vote as a miner, participants typically must download the entire blockchain and operate a full node. By May 2018, the full Ethereum blockchain was 575 gigabytes, and the full Bitcoin blockchain was 198 gigabytes (Figure 3, next page).[5] Both continue to grow with each new block, and the rate of

growth will increase as these blockchain networks scale up. Even after the initial blockchain download, nodes continue to send data to one another on a peer-to-peer basis to keep other nodes in sync and to process new transactions. The amounts of data involved can be considerable: operating a node involves monthly data transfers of between 70 and 140 gigabytes.[6]

Data caps raise the cost of participating in the operations of blockchain networks and, in some cases, may prevent participation entirely.

Data caps raise the cost of participating in the operations of blockchain networks and, in some cases, may prevent participation entirely. The result is a limitation on who can participate in blockchain governance. The limits are imposed not by the blockchain system itself but by choices made at the Internet level.

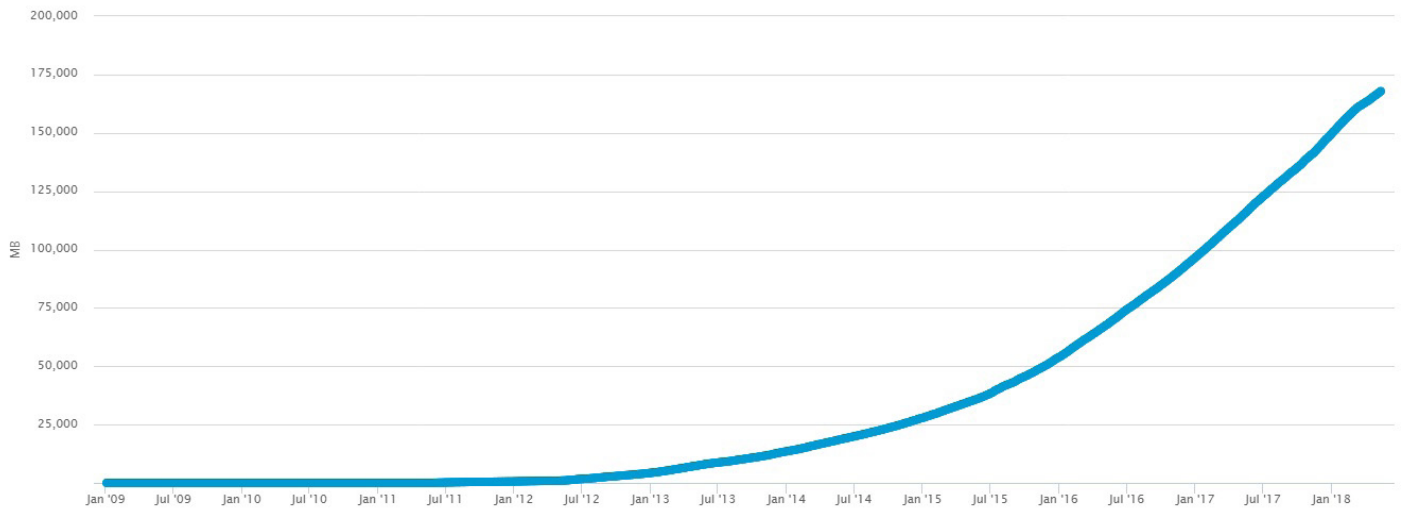
Technical levers of influence: China's Great Firewall

The national government's Internet policies on the governance of blockchain networks have already influenced the Bitcoin scaling debate. Bitcoin miners in China must consider the impact of the Great Firewall on their mining operations, bringing a nation-state censorship and surveillance regime into a debate that ostensibly was about reaching consensus on a particular protocol upgrade for Bitcoin. These nation-state policies played a significant role in hindering support for and implementation of a range of technical solutions.

The first implementation of Bitcoin capped the size of each block at one megabyte, which limited the number of transactions that could fit in each block. By 2015, the Bitcoin network reached a degree of saturation, as more transactions were undertaken every 10 minutes

Figure 3: Bitcoin blockchain size

The total size of all block headers and transactions excluding database indexes, as of 18 May 2018.



Source: blockchain.info, accessed 18 May 2018.

than what could effectively fit into a block. Efforts to increase the network's capacity took on a new sense of urgency.

A series of ongoing conferences titled *Scaling Bitcoin* launched in March 2015.[7] The conferences highlighted a number of proposals from Bitcoin developers to increase network capacity, some of which entailed a modification in the Bitcoin protocol to allow for an increased block size. For any technical upgrade to the Bitcoin network, a successful scaling solution would need to be adopted by a large majority of the network's mining power. It would require the support of miners based in China, who represent a large majority of the total processing power on the network.

Bitcoin mining is a highly competitive industry, and even the smallest advantage can make a big difference to large-scale mining farms.

Bitcoin mining is a highly competitive industry, and even the smallest advantage can make a big difference to large-scale mining farms. Latency and bandwidth are critical factors, since miners must learn a block has been completed and must download it before they can start working on the next block. Miners with high latency and limited bandwidth start late on the new block and waste valuable energy working on old, invalid blocks, while miners with lower latency and more bandwidth are already working on the next block.

While miners in China certainly wanted the Bitcoin network to keep growing and the value of bitcoin to appreciate further, they faced an issue that miners located outside of China did not have to address: the Great Firewall of China, through which all Internet traffic in China must pass. This extra technical overhead limits the bandwidth and increases the latency of packets transmission. Doubling the block size would effectively double the delay for miners to start mining on a new block, threatening to leave China-based mining operations unprofitable, despite their great investments in specialized mining devices. This concern was a major factor in the China-based miners' rejecting block size increases, even at the risk of decreasing the health of the network.[8] To a large extent, China's Internet governance system had indirectly and unintentionally shaped Bitcoin governance.

Conclusion: Accounting for Internet-level governance

Anyone building a blockchain system must consider the impact that Internet governance could have on the operations of that system.

Anyone building a blockchain system must consider the impact that Internet governance could have on the operations of that system. No system whose operations rely on the Internet network can ignore the implications of Internet-level governance. Hence, anyone designing a blockchain network or Dapp should understand and acknowledge the realities of the present-day Internet (e.g., data caps, DPI practices, etc.) and create a system that can accommodate them or perhaps work around them.

Blockchain systems should be designed so that they can respond to unforeseen circumstances at the level of the Internet network, which might significantly affect the continued operation of these systems. In some cases, stakeholders might even consider intervening and actively participating to influence the outcome of Internet governance (e.g., by advocating for net neutrality).

The blockchain layer

Blockchain systems operate on top of the Internet layer and, as discussed above, inherit the capabilities and limitations of that underlying layer, including its technical architecture and governance processes.

The higher the transaction fees paid to the network, the greater the chance miners will include these transactions in the next block.

Blockchain systems also introduce their own mechanisms of governance specific to each particular blockchain network. These mechanisms include the design of the underlying peer-to-peer network and the consensus protocol that facilitates agreement between the various nodes of the network. While ISPs are responsible for routing packets through the Internet according to specific protocols (e.g., TCP/IP and border gateway protocol or BGP), nodes in a blockchain network are responsible for validating and recording transactions into the underlying blockchain according to a particular set of rules. Each blockchain network implements its own protocols, consensus algorithms, and fork-choice. For example, Bitcoin miners operate according to the Bitcoin proof-of-work protocol, which stipulates that miners should always add to the "longest chain" as defined by the amount of hashing power required to compute the chain.

Despite their technical complexity, blockchain networks provide a relatively simple set of operational rules, which often leverage cryptoeconomics to encourage collaboration among participants to maximize the utility of the network, while punishing participants who try to cheat. As a result, the task of processing transactions is driven mostly by an economic incentive system, whereby the higher the transaction fees paid to the network, the greater the chance miners will include these transactions in the next block.

Transaction fees and mining rewards are a fundamental incentive for miners, but they are not the only factors that might influence the behavior of miners. Other levers might come into play, stemming from the outside of the blockchain infrastructure. Consider the following possibilities:

Transaction fees and mining rewards are a fundamental incentive for miners, but they are not the only factors that might influence the behavior of miners.

- A large mining pool might enter into an off-chain agreement with third parties to speed up the inclusion of certain transactions at the expense of others.
- Miners could collectively agree not to process specific transactions coming from or directed toward a criminal application in a block.
- Miners could agree to blacklist specific addresses.
- Regulators could prohibit all miners located in particular jurisdictions from validating transactions pertaining to a specific account.

These external forces exist beyond the control of any given blockchain system and could have significant consequences over the operations of these systems.

The application layer

Like the rest of the technology stack, the application system stack is not a unified whole. It consists of multiple layers, each inheriting from the one below. We distinguish here between two specific components that constitute the application layer:

- *Dapp frameworks* are built on top of a blockchain network and provide the basic building blocks for Dapps. Some are general purpose, with loosely defined logic that developers can repurpose in almost any Dapp (e.g., Open Zeppelin solutions). Others are more specific for certain kinds of Dapps (e.g., DAOstack and Aragon).

- *Dapps* are decentralized applications that may be built directly on top of a blockchain network or on an existing Dapp framework. Gnosis, Civic, and CryptoKitties are Dapps built directly on the blockchain network and implemented as smart contracts on Ethereum.[9] To streamline the creation of the Dapp, developers may choose to leverage Dapp frameworks (e.g., District0x built on top of Aragon and Sapien built on top of DAOstack).

Because hard forks have the power to change the balance or code of a particular Dapp, this level of intervention is extremely rare and has been used only in exceptional circumstances so far.

Even if Dapps can be designed to be completely decentralized and autonomous (in the sense that no single party has the power to control or influence their operations), they remain affected by the operations of their underlying blockchain network or Dapp framework. There are two ways to alter the operation of a Dapp:

- Change the state of the blockchain to overwrite the code of the Dapp.

- Change a small piece of the code it relies on, that is, a smart contract library or a *proxy contract,* a smart contract that delegates calls to other smart contracts.

The first case requires the participants of a blockchain network to intervene, with a coordinated action, to censor some of the transactions directed to a particular Dapp or perhaps even alter the code of a Dapp. For example, in response to the hack of the DAO, the Ethereum community implemented a *hard fork*, changing the protocol and state of the Ethereum blockchain so that users could withdraw their (stolen) funds. Yet, because hard forks have the power to change the balance or code of a particular Dapp, or even to delete the Dapp entirely, this level of intervention is extremely rare and has been used only in exceptional circumstances so far.

The second case arises whenever a Dapp is built upon or relies on a third-party smart contract for its operations. As a rule, in the context of software development, reusing well-established and tested code is good practice because it avoids duplication of effort. However, in the context of a blockchain system, if a Dapp makes an immutable reference to third-party code, it creates two kinds of risks.

One risk is that a flaw in one of these smart contracts libraries will affect all blockchain applications that rely on that third-party library. For example, the bug in Parity Technologies' multisignature (multisig) wallet smart contracts allowed the theft of over $30 million worth of ether.[10] In a subsequent attack on Parity's revised multisig smart contract code, the assailant forced the shared code to "self-destruct," thereby freezing the funds in all multisig wallets that depended on this code.[11]

One risk is that a flaw in one of these smart contracts libraries will affect all blockchain applications that rely on that third-party library.

Another problem emerges by construction, when platforms implement proxy contracts that delegate calls to other smart contracts, which platform developers can then update. While such practices are still uncommon, some platforms (e.g. Zeppelin Solutions) are starting to experiment with proxy libraries so that, whenever one of the underlying functions is changed, all Dapps relying on these libraries will automatically inherit those changes. This design provides many benefits in terms of flexibility and upgradability. However, it can be problematic if it relies on a trusted authority such as the smart contract platform operator, who might arbitrarily influence the operations of these so-called decentralized applications.

Multiple layers of blockchain governance

Building upon the information described above, this section provides an overview of the multiple layers of governance that might affect the operation of a blockchain system. It distinguishes between two distinct governance structures:

- Governance *by* the infrastructure
- Governance *of* the infrastructure

Depending on the focus of analysis, we can regard these two mechanisms as either *endogenous* to a particular community or *exogenous* to that community. Endogenous rules are elaborated *by* the community and *for* the community—a community's attempt at self-governance. Exogenous rules are established or imposed by a third party that is external to the community but nonetheless have the ability to influence it. We will explore each of these factors below.

The governance of most decentralized blockchain applications (Dapps) is split into different layers interacting with one another.

The governance of most decentralized blockchain applications (Dapps) is split into different layers interacting with one another:

- The Internet protocols layer (e.g., the TCP/IP protocol)
- The blockchain network layer (e.g., the Ethereum protocol)
- The Dapp framework (e.g., Aragon)
- The Dapp layer (e.g., District0x)

Each of these layers is designed and implemented by different people, with different purposes, and from separate communities that may or may not communicate with one another. Communities from the bottom layer of the stack often implement their own governance structure with little, if any, regard to the governance systems implemented at layers above. Despite this lack of regard, each one of these layers implements its own distinct governance structure, which remains interrelated with the governance structures of the other layers. The bottom layers play an especially important role, as they constitute the base on which everything else is built. They dictate how the applications deployed on the upper layers of the stack will operate and define what is possible to build at the highest levels.

The bottom layers play an especially important role, as they constitute the base on which everything else is built.

For instance, Aragon and DAOstack are Dapps built on top of the Ethereum blockchain and therefore subject to the governance rules of the Ethereum blockchain network. They are also Dapp frameworks in their own right and implement their own system of protocols and rules for how people can interact with their Dapp or create new Dapps on top of them. The Dapps deployed on these Dapp frameworks will, in turn, create their own protocols and rules to ensure their proper operation and management. Ultimately, a Dapp is directly subject to its own governance rules and indirectly affected by the rules of the blockchain network on which it operates, the rules of the Ethereum blockchain that ensures the proper execution of relevant smart contracts, and the rules of the Internet network that makes everything run.

Governance *by* the infrastructure

Governance by the infrastructure refers to governance by hard-coded rules embedded in a technological system—in our case, a blockchain system. It implies a narrow understanding of decision-making in terms of the process of rule enforcement, as opposed to the elaboration and development of these rules in the first place.

Governance by the infrastructure can include both *endogenous rules* that come from within the reference community and *exogenous rules* imposed from outside the reference community. As the definition hinges on a particular community, the question of whether a particular rule is endogenous or exogenous depends on the perspective of the community of consideration (i.e., a rule can be endogenous from one perspective but exogenous to another).

Ultimately, a Dapp is directly subject to its own governance rules and indirectly affected by the rules of the blockchain network on which it operates.

From the perspective of a particular blockchain network like Ethereum, endogenous rules are those codified directly into the network, such as the blockchain protocol and consensus algorithm. From the perspective of a Dapp deployed on top of Ethereum, endogenous rules include all the decision-making procedures and technical rules embodied in the smart contracts governing the Dapp—whereas the underlying protocol of the Ethereum network would qualify as exogenous. Both the blockchain network and the Dapp are affected by rules encoded into a system that is exogenous to the network's or Dapp's own governance structure. For instance, TCP/IP and other Internet protocols enable people to find and connect to the blockchain network.

When these rules are endogenous to a blockchain network, governance *by* the infrastructure is referred to as "on-chain governance" because the governance rules have been encoded directly into the blockchain itself. As such, these rules are generally considered immutable and self-executable since the normal operation of the blockchain network will guarantee their execution in a secure and decentralized manner.

Of course, on-chain governance rules can also specify procedures to amend themselves. Just as we can make laws that stipulate how to make, amend, or repeal laws, we can design protocol rules that define procedures to make, amend, or repeal other protocol rules. Tezos, for example, promises to build a self-amending blockchain and give participants the ability to change the protocol rules, including rules to change the rules.

On-chain governance presents both advantages and disadvantages. At its best, on-chain governance is predictable and fair in its execution. Because changing the process or the result of on-chain governance is extremely difficult, the entire system is fully transparent and auditable. Everyone can see why a particular decision was made; the whims of human decision makers cannot easily influence or alter the system's operations.

Flexibility can help a system avoid the execution of predetermined processes that might be fair in their execution but unjust in their outcomes.

However, given its resistance to change, on-chain governance may handle new and unexpected situations inadequately. In such cases, vagueness can be a feature, not a bug. Flexibility can help a system cope with unique circumstances that it was not built for, avoiding the execution of predetermined processes that might be fair in their execution but unjust in their outcomes. Hence, where possible, developers should provide on-chain governance with mechanisms similar to those proposed by Tezos, mechanisms that allow changes to the protocol rules underpinning the network.

Governance *of* the infrastructure

"Governance *of* the infrastructure" refers to all forces that subsist outside of a technological platform, but nonetheless influence its development and operations. These rules operate at the social or institutional level, rather than at the technical level. In blockchain systems, governance *of* the infrastructure is often referred to as "off-chain governance" because the governance rules subsist and operate outside of the blockchain infrastructure. These rules and procedures are not automatically executed, and a third-party authority might therefore be required for enforcement or oversight. Governance *of* the infrastructure comprises both endogenous and exogenous rules.

Endogenous rules

Endogenous rules consist of all the rules, social norms, customs, and other governance structures developed or endorsed by a particular community with a view to facilitate coordination within that community. For instance, developers in open source communities

have elaborated processes that codify the rules and procedures used to decide on the future development and evolution of an open source software project. These rules are usually norms or customs enforced via peer pressure, although the community might also implement formalized mechanisms of enforcement and oversight. Failure to follow these rules might lead to exclusion from the community, or other forms of social punishment.

Failure to follow these rules might lead to exclusion from the community, or other forms of social punishment.

In the context of a particular blockchain community, endogenous rules include the rules and procedures used to decide on changes to implement in the protocol, including the decision to fork. In Bitcoin, these decisions are mostly made via *Bitcoin improvement proposals* (BIPs)—an informal mechanism through which people can propose new features and improvements to the Bitcoin protocol. Ethereum implemented a similar system for people to submit *Ethereum improvement proposals* (EIPs), an informal procedure by which people can suggest or request changes to the Ethereum protocol or code.

Over time, informal practices have become norms within the development communities, although those practices are not well-documented or widely known. For example, EIPs must meet a certain technical standard and undergo peer review online before moving forward to the development team. From there, EIPs must be accepted unanimously by the core developers before they will be added to the development roadmap. However, there is no formal structure in place, and none of these conventions is binding.

The uncertainties around the EIP process and the role played by the development community have led to controversy over efforts to unlock the aforementioned Parity multisig wallets.[12] One of the volunteers responsible for bringing EIPs forward to the development team expressed his discomfort with the proposal and potential implications under Japanese law, while other members of the community called for his resignation. The volunteer ultimately stepped down, and the question of when legal or ethical concerns could block an otherwise valid EIP remains unanswered.

After the developers of a blockchain system put forth a proposal, there is typically a voting system to determine whether the community adopts it as a whole.

After the developers of a blockchain system put forth a proposal, there is typically a voting system to determine whether the community adopts it as a whole. For Bitcoin, miners vote by running new software with certain settings enabled or disabled, thereby indicating support or lack thereof. The recommendation of the lead developers is often very influential, but not determinative.

To the extent that these proposals are accepted and implemented into code, governance *of* the infrastructure has the ability to affect governance *by* the infrastructure. In other words, off-chain governance can shape or influence the on-chain governance of a particular blockchain-based network. Indeed, because off-chain governance is generally geared toward elaborating or changing the rules of a given blockchain protocol, it has the power to modify the on-chain governance structure specific to that blockchain.

Exogenous rules

Exogenous rules are all other rules that influence the activities of a community but that originate from outside that community. One prominent example of exogenous rules is the law. Although they may not apply directly to a blockchain network, national laws could nevertheless affect the operations of such a network and certainly apply to participants in the network. These laws do not stem from the community, nor are they chosen by it. They are imposed by a third-party authority, typically a government, to ensure public order and morality and to promote the interests of the public at large. Because they apply only in a given jurisdiction, only a national legal system can remediate the harm of any violations through law enforcement or court processes.

These two mechanisms—governance by the infrastructure and governance of the infrastructure—coexist more or less peacefully in the context of a blockchain system.

Conclusion: Off-chain and on-chain governance

These two mechanisms—governance *by* the infrastructure and governance *of* the infrastructure—coexist more or less peacefully in the context of a blockchain system. Together, they contribute to regulating a particular platform or infrastructure according to their own set of sometimes divergent or contradictory rules.

Both mechanisms present a series of benefits and drawbacks, which make them particularly suited for specific situations, but not for others.

- *Off-chain* governance is generally implemented through a system of rules, procedures, and social norms that are not as rigid and formalized as those of a code-based system. These systems are more informal and unstructured than their code-based counterpart, and are therefore more complex to oversee and control. As such, users can easily sidestep them because there is no automatic rule enforcement.

- *On-chain* governance systems, on the contrary, cannot be easily avoided or bypassed *sensu stricto*, because they operate according to a system of rules that have been encoded directly into the technological framework responsible for enforcing them. These systems are also more auditable and verifiable than their off-chain counterpart, because every transaction on a blockchain comes with irrevocable and non-repudiable proof of itself.

Yet, the main drawback of each system also and simultaneously constitutes its most powerful advantage, and vice versa.

Yet, the main drawback of each system also and simultaneously constitutes its most powerful advantage, and vice versa. While off-chain governance is difficult to enforce because of its social component, it also comes with a great deal of malleability, enabling the system to quickly and smoothly react to unforeseen circumstances, and easily adapt to changes in the environment.

Conversely, on-chain governance might excel at doing what it was expressly designed to do; yet, it is unable to cope with

unexpected situations and takes much longer to adjust to changing circumstances. Ultimately, the ambiguity of off-chain governance rules provides the necessary flexibility to shrink or expand the scope of these rules, case by case (albeit at the price of sometimes creating more uncertainty as to their application). In contrast, the rigidity of on-chain governance rules is such that—if there is a design flaw—malicious parties could potentially exploit them to subvert the system or simply mold it to their own benefit.

Today, much of the thinking on blockchain governance is mainly looking at endogenous rules, with regard to both on-chain and off-chain governance.

Today, much of the thinking on blockchain governance is mainly looking at endogenous rules, with regard to both on-chain and off-chain governance. Many projects and initiatives are trying to implement new mechanisms of governance *by* the infrastructure through a particular set of rules embedded in a blockchain protocol to ensure the proper governance thereof. Increasingly, people are identifying the need for blockchain networks and the communities around them to elaborate more precisely defined community rules, enabling better governance *of* the infrastructure. While endogenous rules have a crucial role to play in governance, stakeholders must also account for the impact of exogenous rules. Ultimately, the combination of endogenous and exogenous rules dictates the manner in which these blockchain systems will operate.

Now let's look at the interplay between the multiple layers of governance affecting particular blockchain applications—with regard to both their endogenous and exogenous rules—taking the DAO as our case study.

The DAO: A cautionary tale

A decentralized autonomous organization or DAO is a set of processes and rules encoded in smart contract code and operating autonomously on a blockchain network. A DAO can mimic the functions of more traditional organizations, like an association or corporation, without relying on a state-granted legal personality. Because they operate on top of a blockchain network, DAOs inherit the immutability and censorship-resistance of those networks. Once the code starts running, it is nearly impossible to stop or change its execution, because every node on the network runs the code.

Because they operate on top of a blockchain network, Decentralized Autonomous Organizations inherit the immutability and censorship-resistance of those networks.

The smart contract, the attack, and the recovery

The DAO was a smart contract deployed on the Ethereum blockchain network. The team at the start-up Slock.it designed the DAO to act as a decentralized investment fund that promised to operate with the "steadfast iron will of unstoppable code."[13] The DAO started with a fundraising phase, during which users could purchase TheDAO tokens by sending ether to the DAO smart contract. Following that initial phase, the general public could make proposals to the DAO community, and TheDAO token holders could vote on what projects

to fund. TheDAO token holders were entitled to a proportional share of the DAO's holdings, including returns from projects funded. Token holders who disagreed with the funding decisions could trigger a "split" function, which allowed them to move their funds out of the DAO to a newly formed "child" DAO.

Proposals submitted to the DAO had to be vetted by a group of "curators"—prominent members of the Ethereum community who volunteered to oversee submissions. Curators were originally expected to play a narrow oversight role, rejecting proposals that were technically flawed or fraudulent. Yet, different people had different understandings of the curator role.[14] Some thought the curators should assume an administrative role only, auditing the code of the smart contracts that would receive the funds and verifying the identities of the people behind these proposals to ensure that no one could abscond the funds. Others thought they should be more proactive in vetting the proposals, to promote the success of the DAO as a decentralized investment fund. As the governance issues related to the DAO's voting mechanisms started to emerge, some of the curators called for a moratorium and refused to accept proposals until the DAO governance was addressed.[15]

The attack on the DAO was spotted almost immediately, but there was no way to stop it.

The debate over curation soon took a back seat to more pressing concerns, which eventually led to the downfall of the DAO. Shortly after the end of fundraising, a serious flaw was identified in the DAO smart contract. This flaw enabled an attacker to drain funds by recursively calling the split function available to every token holder.[16] The attacker was able to withdraw funds repeatedly without updating the balance of the account held in the DAO. By exploiting this flaw, the attacker funneled one-third of the ether raised by the DAO into a child DAO controlled by the attacker.

The attack on the DAO was spotted almost immediately, but there was no way to stop it. The code was running on the Ethereum blockchain, and the attack went on for a few hours, draining 3.6 million ether (almost one-sixth of the total amount of ether available at the time) from the DAO.

Although forking was the only way to retrieve the funds, it was considered a highly controversial approach, as it would mean admitting that the Ethereum blockchain could, in fact, be altered.

The Ethereum community was left trying to decide how to respond. One alternative was to do nothing, allowing the attacker to keep the funds that had been illegitimately withdrawn from the DAO. Another alternative was to intervene with a network fork, modifying the Ethereum protocol to alter its state and course of operations. The decision was further complicated by the sense of urgency generated by the tight timeline imposed by the DAO contract: the funds were locked in the attacker's child DAO for only 21 days, after which they could be withdrawn; retrieving them would be impossible for the original owners.

Although forking was the only way to retrieve the funds, it was considered a highly controversial approach, as it would mean admitting that the Ethereum blockchain could, in fact, be altered. Besides, the process was not simple: any change in the protocol would require developers to figure out a fix, develop and test that fix,

and then convince a majority of the mining power on the network to install the new version of the software.

After much heated debate and several attempts at gauging the community consensus, leading Ethereum developers converged on a proposed solution: a hard fork that would transfer the funds of the attacker's child DAO into a new withdrawal smart contract that would only allow token holders to withdraw their funds. The proposal was implemented into code; members of the community then had to decide which network to support. While the hope was that everyone would switch to the new protocol and leave the old to die out, dissent within the Ethereum community led to the emergence of two blockchains that subsist today: Ethereum, which implemented the proposed change, and Ethereum Classic, which rejected it.

Beyond the issues internal to the Ethereum community, the DAO attack also brought considerable attention from litigators and regulators.

Beyond the issues internal to the Ethereum community, the DAO attack also brought considerable attention from litigators and regulators. There was a great deal of speculation over who might be liable for any wrongdoing caused by the DAO and who should respond to the investors who lost their funds in the attack. Meanwhile, the US Securities and Exchange Commission launched an investigation into the legal status of TheDAO tokens, and eventually issued a report concluding that the DAO had engaged in the unlicensed issuance of securities.[17]

The limitations of on-chain governance

The DAO exemplifies the limitations of on-chain governance. Despite the efforts of the DAO's developers to disclaim responsibility on the ground that the DAO operated solely according to its own code, the intervention of the Ethereum community in response to the attack has surfaced many other factors that stakeholders must take into account when governing the operation of a blockchain system. Table 1 breaks down these factors into categories: "governance by" refers to the rules and processes built into the blockchain network, whereas "governance of" describes the mechanisms by which people can control or influence its operation.

The DAO exemplifies the limitations of on-chain governance.

The DAO's founders described it as if it were predominantly operated through an on-chain governance structure, as if the smart contract code and the protocol of the underlying Ethereum network were the main elements determining the operations of the DAO. This was not the case. Even though smart contract code strictly defined the *modus operandi* (i.e., *how* the DAO operated), token holders and curators made the actual decisions concerning the DAO's operations (i.e., *which* actions the DAO could take) through a decision-making system that relied heavily on endogenous off-chain activities.

On one hand, the automation provided by the DAO could not replace the human side of governance, with activities such as voting, campaigning, keeping funded proposals accountable, and so forth. On the other hand, no proposals were put forward for a vote during the curator moratorium, thereby negating the token holder's ability to vote on proposals. The DAO's loosely defined on-chain rules spilled

out into the off-chain world: the curators *could* stop proposals, but *should* they? This question was never answered, as the DAO's attack became a more pressing concern.

Following the attack, the Ethereum community worked on understanding what it could do to fix the problem.

Following the attack, the Ethereum community worked on understanding what it could do to fix the problem. It had limited room for an endogenous response to the attack, as the DAO itself offered only limited tools. While Ethereum developers discussed technical fixes, some community members proposed a more immediate solution: staging a *denial of service* (DoS) attack on the Ethereum network to slow it down.[18] This approach failed, as the attacker continued to drain funds. Yet, it showed that, since the DAO's code could not be readily fixed, stakeholders had to move through the lower layers of the blockchain stack—the Ethereum network—to identify a possible fix.

Nevertheless, the DAO's code offered a temporary patch. After the attack ended, a small group of tech-savvy individuals formed the "Robin Hood Group" to prevent the attacker from withdrawing more ether. These "white hat" hackers exploited the same vulnerability to drain the remaining funds from the DAO—this time, with the intention of returning the ether to its rightful owners.

Ethereum developers came up with two possible fixes, each of which had to be implemented within a specified period, before the attacker could transfer the siphoned funds.

This solution, albeit useful to prevent additional harm, was unable to retrieve the ether that the attacker had already siphoned. Any solution would require the intervention of exogenous forces. Ethereum developers and the Ethereum community more broadly would have to engage in a combination of on-chain and off-chain governance efforts to mitigate and possibly undo the effects of the attack.

Ethereum developers came up with two possible fixes, each of which had to be implemented within a specified period, before the attacker could transfer the siphoned funds. One fix consisted in a *soft fork* that would prevent the attacker from spending the ether stored in the child DAO. Another fix required a *hard fork* that would transfer the child DAO's funds into a new withdrawal contract to allow the token holders to withdraw their funds.

Table 1: Categories of governance in blockchain systems

	Endogenous rules	**Exogenous rules** **Blockchain-level external to blockchain**	
Governance *by*	The DAO	Ethereum network protocol	TCP/IP, BGP, etc.
Governance *of*	Voting systems, quora upgradeContract()	Ethereum improvement proposals	National laws, regulatory findings, litigation

Both solutions were highly controversial, for different reasons. The hard fork was the more controversial of the two solutions, as it required an actual alteration of the blockchain's state. The soft fork did not go quite as far—it only blacklisted the child DAO's account so that the attacker could not transfer funds from it. Yet this approach was still controversial because it was regarded as a form of "transaction censorship." Eventually, the debate over the soft fork became moot when a security review showed that it would create a new attack vector, enabling malicious individuals to launch a potential DoS attack against the Ethereum network without incurring any cost.

The hard fork was the more controversial of the two solutions, as it required an actual alteration of the blockchain's state.

Following an intense debate over the merits of the proposed solution and whether intervention was appropriate in the first place, the developers decided to move ahead with the hard fork. They released a new version of the Ethereum client, with an option for miners to toggle in order to express whether they wanted to follow the hard fork. Through a "carbonvote," a makeshift polling tool devised after the DAO hack, ether holders could vote on their preferred outcome (to fork or not to fork, Figure 4, next page).[19] Although 97 percent of voters were in favor of the hard fork, only a tiny percentage (4.5%) of all ether holders actually voted, leading some people to question the legitimacy of the vote. Nonetheless, the developers released the new clients with the default set to accept the hard fork.

The hope was that the hard fork would proceed as planned, leaving the old blockchain to fade into obscurity as miners picked up the new forked chain. However, given the contentious nature of this fork, the community could not reach consensus. Those who believed that the principle of immutability was more important than the return of drained funds continued to mine on the old chain; they argued that the only legitimate Ethereum blockchain is the unaltered one. Perhaps because of their arguments or because of the potential economic gains from mining on a new, smaller network, this group successfully brought a significant amount of mining power to the old Ethereum blockchain, known as Ethereum Classic.

Lessons learned

The DAO has shown us how off-chain governance can influence the operation of on-chain governance rules. Developers usually introduce changes to a blockchain protocol to improve a network's functionalities or to fix technical issues that would otherwise jeopardize the whole network. However, they have used off-chain governance to update a blockchain's protocol in some exceptional situations, motivated not by technical reasons but by economic ones—thereby raising a series of questions as to the legitimacy of these interventions.

The DAO has shown us how off-chain governance can influence the operation of on-chain governance rules.

The DAO was the first major attack undertaken on a blockchain application, but it was definitely not the last one. More recently, an attacker exploited a flaw in the code operating Parity's multisig contracts. This flaw led to more than 500 million ether being frozen in a series of broken wallets, with no way for anyone to recover the funds without altering the state of the underlying blockchain—another

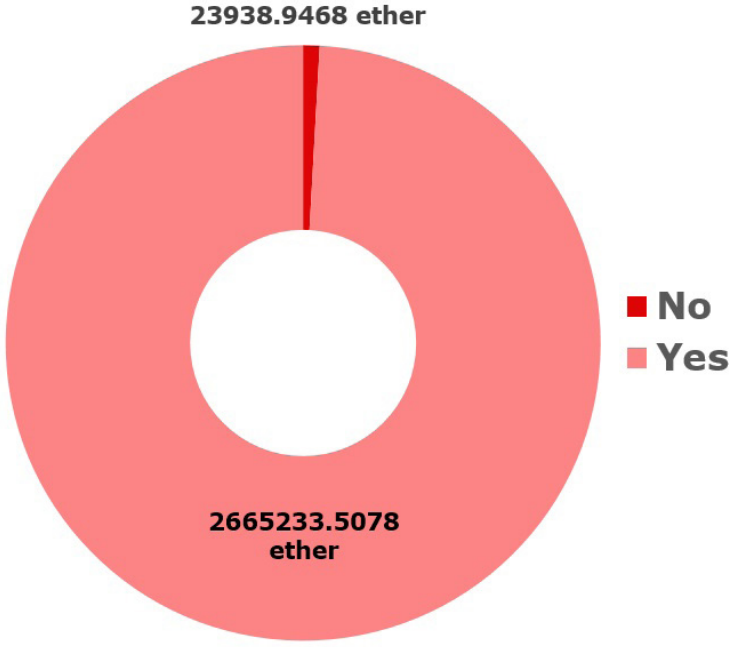
hard fork, which could be implemented only with the consensus of the whole Ethereum network.[20] Because of this incident, another call for action has been brought to the Ethereum community, requesting another protocol change to unfreeze the funds locked in the Parity multisig contracts.[21] It remains to be seen whether the Ethereum community will collectively agree to implement such a change.

There is a need for a mechanism to update the protocol of a blockchain network, if deemed necessary by relevant stakeholders.

This incident, like the DAO's incident, forces us to rethink what constitutes effective blockchain governance. On the one hand, it stresses out the limitations of endogenous on-chain governance. Even if we can codify specific governance rules into smart contract code, we cannot guarantee that these rules will execute as they were originally intended, or that a series of events will not render these rules obsolete or even undesirable.

As a result, there is a need for a mechanism to update the protocol of a blockchain network, if deemed necessary by relevant stakeholders. To do so, both the Bitcoin and Ethereum communities established a series of procedures that members must follow to update their respective blockchain (e.g., Bitcoin and Ethereum improvement proposals).[22] Yet, these procedures are sometimes criticized for being too slow and cumbersome, and empowering a small, centralized group of core developers who decide on the set of (limited) options to make available to the broader community.

Figure 4: To fork or not to fork Ethereum: The CarbonVote outcome



Source of data: CarbonVote.com, accessed 18 May 2018.

On the other hand, these incidents show that the governance of a blockchain system cannot rely, only and exclusively, on the traditional mechanisms of exogenous law enforcement. Traditionally, states can leverage their coercive power to enforce exogenous rules imposed by law. For example, if a court in a given jurisdiction ordered an injunction, people would need to comply with that injunction. If they refused, then such refusal could lead to the seizure of their assets or perhaps even jail.

Even if a court were to order the modification of a particular smart contract to meet legal requirements or remedy a wrong, it is unclear how such an order could be enforced and against whom.

Blockchain systems depart from this norm. Even if a court were to order the modification of a particular smart contract to meet legal requirements or remedy a wrong, it is unclear how such an order could be enforced and against whom. Even if the developers within the court's jurisdiction were forced to comply with the order, the smart contract would subsist as long as a majority of miners in the underlying blockchain network refused to accept the fork.

The distinctive features of blockchain governance

Blockchain systems present unique features in how they enforce the set of rules they embody. Traditionally, both in the online and offline worlds, a centralized authority (a *sovereign*) can intervene to stop or influence people's activities, either legitimately or illegitimately. For instance, in an attempt to stop Catalonia's independence referendum, Spain's government sent its police to seize ballot boxes from all Catalan polling stations.

Similarly, many authoritarian governments—such as China, Turkey, Iran, or Tunisia during the Arab Spring—have recurrently cut off access to certain news websites and social media during periods of social or political unrest. Some countries have even tried to shut down access to all Internet communication, as Egypt did in 2011 to contain the uprising against then-President Hosni Mubarak.[23] Even democratic governments often require online intermediaries to enforce rules and regulations against the dissemination of copyright infringement, hate speech, or obscene material.

Because of the disintermediated nature of a blockchain, the network operates autonomously, according to its own rules.

These particular kinds of interventions from an external force are more difficult to achieve in the context of a blockchain network. Because of the disintermediated nature of a blockchain, the network operates autonomously, according to its own rules. No one can exercise sovereign power to coerce the network into doing something that it was not programmed to do. The operations of most blockchain networks or decentralized applications are governed by a specific set of predefined rules that precisely stipulate the procedure that everyone must follow to participate in the governance of the system, and, in some cases, have the power to change or influence the decision-making process.

For most blockchain networks, decisions are taken via a consensus protocol (e.g., proof of work or proof of stake) that enable people (e.g., miners or validators) to vote (with their hashing power in the case of proof of work or with their tokens in the case of proof of stake) on which transactions to include into a block. New blockchains are exploring the possibility of token holders' relying on these same on-chain governance mechanisms to modify the rules of the underlying blockchain protocol in a fully automated way (e.g., Tezos). Yet, the implementations of most of the existing mechanisms of on-chain governance resemble plutocracies (i.e., "rule by the wealthy") rather than democracies.

The implementations of most of the existing mechanisms of on-chain governance resemble plutocracies (i.e., "rule by the wealthy") rather than democracies.

Similarly, in the context of Dapp, the decision makers are typically individual token holders who participate in governance either by burning some tokens or by casting a vote, the weight of which will depend on the number of tokens that each individual holds at any given time. A few heavily invested token holders (termed *whales*) will hold a disproportionate influence in the system at the expense of less wealthy users.

Because of these market forces, these systems are ultimately subject to potential manipulation. Certain parties might try to collude, or simply purchase the necessary resources (i.e., tokens or hashing power) to influence the vote in ways that will promote their own interests rather than those of the larger community. This is particularly problematic if the interests of token holders are not perfectly aligned with those of the users of a blockchain-based platform.

This kind of conflict is all too common in many Dapp designs: token holders are often more interested in seeing the price of their tokens rise, whereas users would rather see a decrease in price so as to reduce the costs of using the Dapp. As a result, on-chain governance suffers from the same problem that it was trying to solve: users acting in their own self-interest can exploit Dapp rules technically or economically, regardless of whether these users qualify as malicious.

On-chain governance is also not immune to outside influences. Entities not directly involved in the network could, for instance, try to shape the opinions of miners or large token holders through social networks or media campaigns. Alternatively or in addition, they could create incentives (i.e., benefits or bribes) or disincentives (i.e., sanctions or penalties) outside the system to change how participants exercise their rights inside the system.

On-chain governance is also not immune to outside influences.

Irrespective of the power dynamics that might come into play, the influence of off-chain governance rules on the operations of a blockchain network is limited because, to be effective, every protocol change must be accepted by all relevant stakeholders (i.e., active nodes and miners supporting the network, cryptocurrency exchanges, etc.). If some parties do not agree with these changes, they will refuse to update their software, causing the network to fork into separate networks.[24]

Forking illustrates one of the key features of the governance of blockchain systems: the ultimate governing power rests with individual miners or token holders. No centralized authority (or sovereign) can subvert the system using coercive force. Indeed, regardless of the system of rules in place to govern a particular blockchain network, no governance system can impose a protocol change that goes against the network's will. Whether this is dictatorial or democratic, the network still must approve any proposed changes: some parts of the network may approve them, whereas others may "exit" by forking into a new network.

Forking illustrates one of the key features of the governance of blockchain systems: the ultimate governing power rests with individual miners or token holders.

While this model presents many advantages—it ensures the autonomy and independence of blockchain systems—exogenous rules can be difficult to enforce on these systems without a formal or informal governance system in place, that is able and willing to account for and transpose these exogenous rules into its own system of endogenous or code-based rules.

Recommendations

Blockchain governance is a novel and complex issue, and there is still no consensus regarding the best ways to address it. Recent expert discussion has lauded the benefits of on-chain governance, but also highlighted its dangers and drawbacks.[25]

Each model of blockchain governance—on-chain and off-chain—presents its own set of benefits and drawbacks, which make it particularly well-suited for dealing with specific circumstances and much less for dealing with others. While some researchers have investigated the relationships between on-chain and off-chain governance rules, most have focused on determining how we can best replace slow and inefficient off-chain governance structures with fully automated on-chain governance systems. Only a small number of actors have been looking at how we can design off-chain mechanisms or processes capable of governing and regulating blockchain systems.

On-chain governance ultimately depends on off-chain governance rules to stipulate how a blockchain-based network will evolve over time.

As with many issues, the ideal solution is somewhere in the middle. Although they each rely on different rules and principles, the combination of on-chain and off-chain governance structures might lead to the most optimal outcome. To be sure, on-chain governance is more transparent and efficient than off-chain governance. However, when on-chain governance fails because of a technical issue or a lack of legitimacy, off-chain governance might be the only viable way out. On-chain governance ultimately depends on off-chain governance rules—especially endogenous ones—to stipulate how a blockchain-based network will evolve over time.

We need more research to bring about the integration of off-chain governance rules into a blockchain system without reducing the

ambiguity and flexibility of these rules into a set of algorithmically quantifiable and verifiable rules. Stakeholders could use on-chain governance not as a substitute for off-chain governance, but as a mechanism through which they could support and enhance off-chain decision-making processes characterized by subjective human judgment, political participation, and deliberation.

In some cases, on-chain governance could implement—at the protocol level—some of the rules and regulations that belong in the realm of off-chain governance. For instance, parts of a contractual agreement or legal provision could be codified into a smart contract, allowing it to be automatically executed and enforced by the underlying blockchain network. Or a variety of community rules and decision-making procedures could be enshrined in a blockchain system to ensure the transparency and verifiability of those procedures.

However, these mechanisms are inherently limited because no rule defined in natural language can be transposed into the strict language of code without losing some of its meaning or lessening the ability to expand or narrow its scope, case by case, depending on the circumstances at hand.

A variety of community rules and decision-making procedures could be enshrined in a blockchain system to ensure the transparency and verifiability of those procedures.

If we want to design new governance systems for more sophisticated blockchain applications—capable of accounting for the flexibility, ambiguity, and uncertainty of natural language and the subjectivity of human judgment—it is important that we incorporate some of the rules and procedures of off-chain governance when designing the on-chain governance structure of Dapp.

We have a number of ways to combine on- and off-chain governance. We could bring off-chain information into the blockchain. For example, we could use mechanisms like *oracles* to make new information available to a smart contract. By publishing data or decisions taken from the offline world onto a blockchain network, oracles provide the necessary link between on-chain and off-chain governance, so that a blockchain-based system can operate fairly and efficiently, without forfeiting the possibility to embed human appreciation and subjectivity into the execution of a smart contract.

Another possibility is to externalize on-chain governance rules into the offline world by integrating alternative dispute resolution and private arbitration systems into the code of smart contracts. These processes could ensure that, if a smart contract does not operate as planned, its execution would be subject to the judgment of external actors—private arbitrators, judges, or even a decentralized jury. These parties would be granted leeway to apply the most ambiguous pieces of the legal system such as the law of equity to a blockchain system. Such processes could ensure that the well-being of the people interacting these blockchain systems is not sacrificed in the name of efficiency and predictability.

Finally, new governance structures based on *global personas* or *reputation* could also be implemented into a blockchain-based

network or application. These could support the development of new decision-making processes that are more democratic or meritocratic than many of the plutocratic systems used in a large majority of blockchain applications. Specific institutions could be made to interface with the technology to ensure respect for endogenous community rules as well as for exogenous laws and regulations designed to preserve public order and morality.

While stakeholders debate how best to govern blockchain systems, we must start asking questions now, considering the implications of using on-chain and off-chain governance mechanisms.

While stakeholders debate how best to govern blockchain systems, we must start asking questions now, considering the implications of using on-chain and off-chain governance mechanisms, and the ways in which these mechanisms can interact with both endogenous and exogenous rules.

We are already building applications for blockchain systems that touch on the most important functions of government and business and their interactions with citizens and customers: identity, credit scores, healthcare, financial services, and credentialing. Blockchain governance, whether on-chain or off-chain, will need to be responsive to the needs of citizens and resilient in the face of unexpected challenges.

To that end, effective governance of blockchain systems must account for a variety of activities at different layers of the technological stack. Dapp frameworks will need to ensure that vulnerabilities at one level do not cascade through the system. Blockchain networks that operate on the Internet will need to guard against state and ISP filtering. Stakeholders of blockchain systems may need to engage relevant stakeholders in Internet governance to discuss the potential impact of their governance decisions on the operations of blockchain systems, rather than accepting trickle-down effects.

Stakeholders of blockchain systems may need to engage relevant stakeholders in Internet governance to discuss the potential impact of their governance decisions on the operations of blockchain systems.

Appendix: Glossary

To provide clarity and ease of reference, we prepared this list of definitions of terms used throughout this report. For some, there are still no standard definitions.

Blockchain network: A network of nodes that manages the recording of data into a blockchain data structure, according to a particular consensus protocol. Bitcoin and Ethereum are examples of blockchain networks.

Blockchain system: Any application or network that relies on blockchain technology. This can be a blockchain network like Ethereum or Bitcoin, a Dapp like Gnosis, or a Dapp framework like DAOstack or Aragon.

Border gateway protocol (BGP): BGP is a routing protocol used to transfer data among different host gateways, networks, or autonomous systems. As a path vector protocol (PVP), BGP "maintains paths to different hosts, networks, and gateway routers" and determines the best route.[26]

Dapp framework: A set of tools and resources that can be used in the creation of decentralized application.

Decentralized application (Dapp): An application that runs on a blockchain system.

Endogenous rules: Rules or processes coming from *within* the reference community of a particular layer in the technology stack.

Exogenous rules: Rules or processes coming from *outside* the reference community of a particular layer in the technology stack.

Governance infrastructure: Processes that are built into a technical infrastructure and define how that infrastructure will operate. Also known as governance *by* infrastructure.

Infrastructure governance: Processes that inform the development or operation of a technical infrastructure. Also known as governance *of* infrastructure.

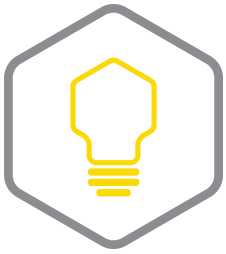
MD5 algorithm: A widely used hash function that produces a 128-bit hash value.

Multisig: multiple keys required to sign and approve a transaction.

Off-chain governance: Processes that are not encoded in a blockchain system and run outside that system. The design of a particular blockchain network is generally established through off-chain governance processes.

On-chain governance: Processes, often automated, that are encoded in a blockchain system. The Bitcoin or Ethereum consensus algorithms or reward mechanisms are part of the on-chain governance of these networks.

Technology stack (also known as *governance stack):* Layered view of a technological system, where each layer provides the infrastructure and tools for the layer above. Lower layers also provide rules and restrictions for the layers above.



About the authors

Primavera De Filippi is a researcher at the National Center of Scientific Research in Paris and a faculty associate at the Berkman Klein Center for Internet and Society at Harvard University. She is a member of the Global Future Council on Blockchain Technologies at the World Economic Forum and founder of the Internet Governance Forum's dynamic coalition on blockchain technology (Coalition of Automated Legal Applications). In 2018, Harvard University Press published her book, *Blockchain and the Law*, co-authored with Aaron Wright.

Greg McMullen is a lawyer, Internet advocate, and chief policy officer at BigchainDB, where he built the framework for the IPDB Foundation and helped bring together its founding caretakers. He is a leading member of the Coalition of Automated Legal Applications intellectual property (COALA IP) working group and co-authored the COALA IP specification and policy paper. Before joining BigchainDB and IPDB, Greg was a litigator at one of Canada's top class action law firms, where he worked on class actions involving privacy, copyright, competition law, and price fixing. He served on the board of directors of the British Columbia Civil Liberties Association (BCCLA), Canada's largest civil liberties organization, and authored the BCCLA's guide to privacy and security when crossing borders with electronic devices.

Notes

1. The Fourth Industrial Revolution is a concept developed by Klaus Schwab and the World Economic Forum. www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

2. See Jo Freeman, "The Tyranny of Structureless," *Berkeley Journal of Sociology* 17 (1972-73): 151-165. www.jofreeman.com/joreen/tyranny.htm; Carlisle Ford Runge, "Institutions and the Free Rider: The Assurance Problem in Collective Action," *The Journal of Politics* 46, no. 1 (Feb. 1984): 154-181, University of Chicago Press. doi.org/10.2307/2130438; Arun Agrawal and Sanjeev Goyal, "Group Size and Collective Action: Third-Party Monitoring in Common-Pool Resources," *Comparative Political Studies* 34, no. 1 (2001): 63-93. SAGE Publications, journals.sagepub.com/doi/10.1177/0010414001034001003; and Pranab Bardhan, "Distributive Conflicts, Collective Action, and Institutional Economics," eds. Gerald M. Meier and Joseph E. Stiglitz, *Frontiers of Development Economics: the Future in Perspective*, The International Bank for Reconstruction and Development/ The World Bank (New York: Oxford University Press, Dec. 2000): 269-290. World Bank documents, worldbank.org/curated/en/586861468762924370/pdf/multi0page.pdf, all accessed 15 May 2018.

3. Those rules are still in place as of 30 April 2018, but are expected to be repealed once replacement regulations are finalized. See Jon Brodkin, "Ajit Pai Hasn't Finalized Net Neutrality Repeal: Here's a Theory on Why," *Ars Technica*, WIRED Media Group, Condé Nast, 24 April 2018. arstechnica.com/tech-policy/2018/04/fcc-hasnt-finalized-net-neutrality-repeal-and-the-delay-might-be-strategic, accessed 12 May 2018.

4. Jon Brodkin, "Data cap analysis found almost 200 ISPs imposing data limits in the US," *Ars Technica*, WIRED Media Group, Condé Nast, 7 Aug. 2017. arstechnica.com/information-technology/2017/08/at-least-196-internet-providers-in-the-us-have-data-caps; "Blockchain Size," Bitcoin.com, Saint Bitts LLC, 2018. charts.bitcoin.com/chart/blockchain-size, both accessed 15 May 2018.

5. "Cryptocurrency statistics," BitInfoCharts, 19 May 2018. bitinfocharts.com, accessed 19 May 2018.

6. "Ethereum," Q&A site, Stack Exchange, Stack Exchange Inc., 20 May 2016, last modified 13 April 2017. ethereum.stackexchange.com/questions/4089/how-much-internet-bandwidth-does-keeping-a-ethereum-wallet-use, accessed 15 May 2018.

7. Scaling Bitcoin, "Scaling Bitcoin Workshops," Scaling Bitcoin Workshop Group, 2018. scalingbitcoin.org, accessed 15 May 2018.

8. Kyle Torpey, "Why the Great Firewall of China Is Causing Serious Issues for Bitcoin Miners," *Bitcoin Magazine*, BTC Media LLC, 26 Feb. 2016. bitcoinmagazine.com/articles/why-the-great-firewall-of-china-is-causing-serious-issues-for-bitcoin-miners-1456508966, accessed 15 May 2018.

9. Gnosis, Gnosis Ltd., last updated Jan. 2018. gnosis.pm; Civic, Civic Technologies, Inc., 2018. www.civic.com; and CryptoKitties, Axiom Zen, n.d. www.cryptokitties.co, all accessed 15 May 2018.

10. Wolfie Zhao, "$30 Million: Ether Reported Stolen Due to Parity Wallet Breach," *CoinDesk*, Digital Currency Group, 19 July 2017. www.coindesk.com/30-million-ether-reported-stolen-parity-wallet-breach, accessed 15 May 2018.

11. "A Postmortem on the Parity Multi-Sig Library Self-Destruct," Parity Technologies, 15 Nov. 2017. paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct, accessed 15 May 2018.

12. Adam Reese, "Ethereum Dev Yoichi Hirai Steps Away from Role as EIP Editor, Raises Questions about Process," *ETHNews.com*, Berns Inc., 15 Feb. 2018. www.ethnews.com/ethereum-dev-yoichi-hirai-steps-away-from-role-as-eip-editor-raises-questions-ab, accessed 15 May 2018.

13. Divisions of Corporation Finance and Enforcement, "Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on the DAO," public statement, US Securities and Exchange Commission, 25 July 2017. www.sec.gov/litigation/investreport/34-81207.pdf, accessed 18 May 2018.

14. Andrew Quentson, "Are the DAO Curators Masters or Janitors?" *Cointelegraph*, 12 June 2016. cointelegraph.com/news/are-the-dao-curators-masters-or-janitors, accessed 15 May 2018.

15. Dino Mark, Vlad Zamfir, and Emin Gün Sirer, "A Call for a Temporary Moratorium on the DAO," blog post, *Hacking*, *Distributed*, 27 May 2016. hackingdistributed.com/2016/05/27/dao-call-for-moratorium, accessed 15 May 2018.

16. A thorough technical analysis of how this occurred is not possible in this paper, but interested readers can find more information here: Phil Daian, "Analysis of the DAO Exploit," blog post, Hacking, Distributed, 18 June 2016. hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit, accessed 12 May 2018.

17. Divisions of Corporation Finance and Enforcement, "Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on the DAO," public statement, US Securities and Exchange Commission, 25 July 2017. www.sec.gov/news/public-statement/corpfin-enforcement-statement-report-investigation-dao, accessed 15 May 2018.

18. FelixA, "Update3: The DAO is under attack—but Vitalik saved us," *DAOhub*, Medium, 17 June 2016. blog.daohub.org/the-dao-is-under-attack-8d18ca45011b, accessed 15 May 2018.

19. "CarbonVote," Carbonvote.com, n.d. www.carbonvote.com, accessed 15 May 2018.

20. "A Postmortem on the Parity MultiSig Library Self-Destruct," ParityTech, Parity Technologies, 19 Dec. 2017. paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct, accessed 18 May 2018.

21. "Secure from scratch: our new smart contract development processes," *ParityTech*, Parity Technologies, 11 May 2018. paritytech.io/new-smart-contract-development-processes, accessed 18 May 2018.

22. "Bitcoin Improvement Proposals," GitHub, GitHub, Inc., last modified 7 April 2013. github.com/bitcoin/bips; "The Ethereum Improvement Proposal repository," GitHub, GitHub, Inc., last modified 15 May 2018. github.com/ethereum/EIPs, both accessed 15 May 2018.

23. "Internet Shutdowns: An Internet Society Public Policy Briefing," Internet Society, 13 Nov. 2017. cdn.prod.internetsociety.org/wp-content/uploads/2017/11/ISOC-PolicyBrief-Shutdowns-20171109-EN.pdf, accessed 18 May 2018.

24. This happened, for instance, with the Bitcoin community, whose discrepancy of opinions as to the best way to scale up the network has led to the Bitcoin network splitting into three separate networks—Bitcoin Core, Bitcoin Cash, and Bitcoin Gold—each implementing a different approach to scalability.

25. Fred Ehrsam, "Blockchain Governance: Programming Our Future," *Medium*, 27 Nov. 2017. medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74; Vlad Zamfir, "Against on-chain governance: Refuting (and rebuking) Fred Ehrsam's governance blog," *Medium*, 1 Dec. 2017. medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca; and Vitalik Buterin, "Notes on Blockchain Governance," Vitalik Buterin's website, 17 Dec. 2017. vitalik.ca/general/2017/12/17/voting.html, all accessed 15 May 2018.

26. "What Is Border Gateway Protocol (BGP)?" Techopedia.com, Techopedia Inc., n.d. www.techopedia.com/definition/6193/border-gateway-protocol-bgp, accessed 30 May 2018.

blockchainresearchinstitute.org