Bitcoin Governance as a Decentralized Financial Market Infrastructure

Nabilou, H.

Publication date
2021

Document Version
Final published version

Published in
Stanford Journal of Blockchain Law & Policy

License
CC BY

Citation for published version (APA):
Nabilou, H. (2021). Bitcoin Governance as a Decentralized Financial Market Infrastructure. *Stanford Journal of Blockchain Law & Policy, 4*(2), 177-202.
https://heinonline.org/HOL/P?h=hein.journals/sjblp4&i=239
BITCOIN GOVERNANCE AS A DECENTRALIZED FINANCIAL MARKET INFRASTRUCTURE

Hossein Nabilou*

ABSTRACT

Bitcoin is the oldest and most widely established cryptocurrency network with the highest market capitalization among all cryptocurrencies. Although bitcoin (with lowercase b) is increasingly viewed as a digital asset belonging to a new asset class, the Bitcoin network (with uppercase B) is a decentralized financial market infrastructure (“dFMI”) that clears and settles transactions in its native asset without relying on the conventional financial market infrastructures (“FMIs”). To be a reliable asset class as well as a dFMI, however, Bitcoin needs to have robust governance arrangements; whether such arrangements are built into the protocol (i.e., on-chain governance mechanisms) or relegated to the participants in the Bitcoin network (i.e., off-chain governance mechanisms), or are composed of a combination of both mechanisms (i.e., a hybrid form of governance).

This paper studies Bitcoin governance with a focus on its alleged shortcomings. In so doing, after defining Bitcoin governance and its objectives, the paper puts forward an idiosyncratic governance model whose main objective is to preserve and maximize the main value proposition of Bitcoin, i.e., its censorship-resistant property, which allows participants to transact in an environment with minimum social trust. Therefore Bitcoin governance, including the processes through which Bitcoin governance crises have been resolved and the standards against which the Bitcoin Improvement Proposals (“BIPs”) are examined, should be analyzed in light of the prevailing narrative of Bitcoin as a censorship-resistant store of value.

* Assistant Professor of Law & Finance, University of Amsterdam, Amsterdam Law School; UNIDROIT - Bank of Italy Chair, The International Institute for the Unification of Private Law (UNIDROIT). The author is grateful to the fellow participants in the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law Conference on Blockchain and Procedural Law: Law and Justice in the Age of Disintermediation (Nov. 15, 2019) held in Luxembourg for their comments and feedback. All errors are those of the author. The views expressed are those of the author and do not necessarily reflect the views of the institutions with which he is affiliated.
and payment infrastructure. Within such a special governance model, this paper seeks to identify the potential shortcomings in Bitcoin governance by reference to the major governance crises that have posed serious threats to Bitcoin in the last decade. It concludes that the existing governance arrangements in the Bitcoin network have been largely successful in dealing with Bitcoin’s major crises that would have otherwise become existential threats to the network.

INTRODUCTION

Bitcoin is a distributed peer-to-peer (“P2P”) system that brings together a decentralized P2P network (the Bitcoin Protocol), a public transaction ledger (the blockchain), a set of consensus rules for independent transaction validation and native asset issuance, and a mechanism for reaching global consensus on the valid chain in a decentralized manner, i.e., the Proof-of-Work Algorithm (hereinafter “PoW”). The popularity of bitcoin as a medium of exchange and a unit of account in the Bitcoin network overshadows its rather complex, innovative and transformative aspects, i.e., establishing the first dFMI. It is important to highlight that the Bitcoin network functions as infrastructure, while bitcoin (i.e., the token) functions as a medium of exchange in the Bitcoin network. Following convention in the computer science literature, hereinafter uppercase-B Bitcoin refers to the network and lowercase-b bitcoin refers to the unit of account. Needless to say, this paper is concerned with the governance of Bitcoin as a network or infrastructure.

Governance is a system that shapes coordination between various participants in an enterprise. As such, it refers to the processes that enable an organization to set its objectives, identify the means of achieving them, and monitor the performance of the organization against those objectives. In traditional corporate law, the main governance objective is to design incentive mechanisms that optimally allocate ownership rights, ownership structures, and define control, while aligning the interests of owners

---

1 Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system* (2008), https://bitcoin.org/bitcoin.pdf. *See also* Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* 2 (2017).

2 Philipp Hacker, *Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations*, in *Regulating Blockchain: Techno-Social and Legal Challenges* 140, 140-146 (Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich eds., 2019).

3 Comm. on Payment and Settlement Sys. & Technical Comm. of the Int’l Org. of Sec. Comm’ns, *Principles for Financial Market Infrastructures* 26 (2012), https://www.bis.org/cpmi/publ/d101a.pdf.
In the FMI context, governance is defined as “the set of relationships between an FMI’s owners, board of directors (or equivalent), management, and other relevant parties, including participants, authorities, and other stakeholders (such as participants’ customers, other interdependent FMI s, and the broader market).”

Issues relating to control take center stage in defining governance. Questions of control in corporations often arise when there is a need for change in ownership, business model, structure of the firm, or long-term strategic goals. In this sense, governance should be separate from the law or regulations applicable to the governance of a firm in that it is internal to the firm, whereas law and regulations are external to the firm or organization.

In the past decade, several critical developments in the Bitcoin ecosystem have thrown governance issues into the spotlight. As such crises could not be resolved simply by relying on the Nakamoto consensus, they highlighted the central role of human discretion in the governance of Bitcoin and other cryptocurrencies.

These incidents were as follows:

1. The integer overflow incident (2010) involving an integer overflow bug that created more than 184 billion bitcoin: This bug was discovered on October 15, 2010 at block 74,638. Once it was reported in the Bitcoin Forum, within 3 hours, Satoshi published a new Bitcoin client and rewound the hyper-inflated chain. Nearly two hours later Satoshi released version 0.3.1 of the Bitcoin client where the hacked coins were erased. It took 19 hours for the good chain to prevail and become the dominant chain.

---

4 Eugene F. Fama & Michael C. Jensen, Separation of Ownership and Control, 26 J. L. & ECON. (1983); Brian L. Connelly, et al., Ownership as a Form of Corporate Governance, 47 J. OF MGMT. STUD. (2010). See also Michael C. Jensen & William H. Meckling, Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, 3 J. OF FIN. ECON. (1976). In other words, governance refers to the dynamics of power and influence that shape decision-making within a firm and delineate the rights and responsibilities of various stakeholders towards the firm. See Ruth V. Aguilera & Gregory Jackson, Comparative and International Corporate Governance, 4 THE ACAD. OF MGMT. ANNALS, 489-90 (2010); Ying-Ying Hsieh et al., The Internal and External Governance of Blockchain-Based Organizations: Evidence From Cryptocurrencies, in BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 48 (Malcom C. Verduyn ed., 2018).

5 COMM. ON PAYMENT AND SETTLEMENT SYS. & TECHNICAL COMM. OF THE INT’L ORG. OF SEC. COMM’NS, supra note 3.

6 This important point seems to be overlooked in many discussions regarding Bitcoin governance. See Vlad Zamfir, Against Szabo’s Law, For a New Crypto Legal System, MEDIUM (Jan. 26, 2019).

7 Aaron van Wirdum, A Primer on Bitcoin Governance, or Why Developers Aren’t in Charge of the Protocol, BITCOIN MAGAZINE (Sept. 7, 2016).
2. An erroneous upgrade to the Bitcoin protocol and its rollback via coordination between developers and miners: On March 11, 2013, there was an erroneous upgrade to the Bitcoin protocol that led to two sets of miners mining the legacy protocol and the updated protocol separately. A chain-split of at least 24 blocks occurred with the new chain having a maximum lead of 13 blocks. Two separate chains were mined for several hours, and there was a successful double-spend. This incident caused the price of bitcoin to sink by one-third. However, the fork was rolled back via coordination between developers and miners who decided to ignore the longest chain, an apparent violation of the Nakamoto consensus. This resulted in some transactions being voided, and raised questions not only about settlement finality, but also about Bitcoin governance: who decides on issues concerning upgrades, and how such critical issues should be managed in the future.

3. The debate about Bitcoin scaling that reached its zenith in 2017 and led to extremely polarizing controversies in the Bitcoin community, forming the epitome of the governance crisis in Bitcoin: Two main camps emerged on this dividing issue; one supporting vertical scaling solutions, or second-layer solutions, and the other supporting horizontal scaling solutions, or increasing the block size. Ultimately, the dispute was settled by hard-forking. This crisis raised questions regarding transparency, power asymmetry, censorship, and more importantly, the very nature and purpose of Bitcoin.

4. The discovery of an inflation bug in the Bitcoin protocol allowing for potential double-spends in September 2018: The manner in which this bug was addressed raised questions about transparency in Bitcoin governance, because the discovery of the bug was

---

8 BitMEX Research, *A Complete History of Bitcoin’s Consensus Forks*, BITMEX BLOG (Dec. 28, 2017), https://blog.bitmex.com/bitcoins-consensus-forks. See also Bank for International Settlements, *Cryptocurrencies: Looking Beyond the Hype*, ANN. ECON. REP. (2018).

9 Id. See also Bank for International Settlements, *supra* note 8, at 102-103. See also macbook-air, *A successful DOUBLE SPENT US$10000 against OKPAY this morning*, BITCOIN FORUM (Mar. 12, 2013, 6:22 PM), http://archive.is/64Rkj.

10 ANTONPOULOS, *supra* note 1, at 300-321.

11 Joseph Poon & Thaddeus Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* (2016), http://lightning.network/lightning-network-paper.pdf. See also Aaron van Wirdum, *The History of Lightning: From Brainstorm to Beta*, BITCOIN MAGAZINE (Apr. 4, 2018); Tom E. Jedusor, *Mimblewimble*, (July 19, 2016), https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin; Aaron van Wirdum, *Mimblewimble: How a Stripped-Down Version of Bitcoin Could Improve Privacy, Fungibility and Scalability All At Once*, BITCOIN MAGAZINE (Aug. 12, 2016).

12 See BitcoinCore, *CVE-2018-17144 Full Disclosure (Notice)* (Sept. 20, 2018), https://bitcoincore.org/en/2018/09/20/notice.
publicly disclosed only after the inflation bug was discovered by other non-core developers and after the news made it to the public.

These developments have brought forth a serious governance question as to who controls changes to the Bitcoin network and, specifically, to the protocol. The current literature on Bitcoin governance is far from thorough in providing answers to such questions. More importantly, as Bitcoin does not entirely rely on on-chain mechanisms to resolve governance issues, the censorship-resistant property of Bitcoin ultimately relies on its off-chain governance which eventually depends on the power dynamics and interactions of the participants in the Bitcoin network. A broken governance framework can easily become prone to censorship due to centralization.

This paper proceeds as follows. Firstly, it briefly discusses the objectives of Bitcoin governance by highlighting the differences between objectives pursued in Bitcoin governance and those pursued in other governance schemes. In so doing, it also briefly compares Bitcoin governance with conventional governance in constitutional systems, corporate governance and internet governance, and highlights the idiosyncrasies in Bitcoin governance objectives. Secondly, after briefly sketching the built-in governance mechanisms in Bitcoin, the paper proceeds to identify the potential market failures in its governance. Having discussed the potential market failures and the potential market-driven and decentralized forms of governance mechanisms that would remedy such governance weaknesses in Bitcoin, the paper finally concludes that at the time of writing, there has been no serious market failure that could necessitate third-party intervention in the governance framework of Bitcoin as it has managed to resolve some of its most pressing concerns with relative success in the last decade.

Bitcoin governance vs. constitutional, corporate, and internet governance

In the literature on Bitcoin governance, several analogies have been made between Bitcoin governance and governance in other disciplines, spanning from constitutional law (i.e., analogies to separation of powers and}

\[13\] van Wirdum, supra note 7. See also Matthew A. Zook & Joe Blankenship, New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance, 96 GEO FORUM (2018); MICHELE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE (2019); Philipp Paech, The Governance of Blockchain Financial Networks, 80 THE MODERN L. REV. (2017); Primavera De Filippi & Benjamin Loveluck, The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure, 5 INTERNET POL’Y REV. (2016); Sinclair Davidson et al., Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995; Hacker, supra note 2.
checks and balances systems and corporate governance to internet governance. One such analogy draws parallels between Bitcoin nodes and the executive branch, the miners and the judiciary, the developers and the Senate, and finally, the business and infrastructure community and the House of Representatives. In this analogy, the users, who may also be node operators, often use businesses to interact with the network. However, the analogy to the constitutional checks and balances system remains misleading at best. In the Bitcoin ecosystem, there is neither a clear separation of powers/roles nor even a clear division of labor. For example, a Bitcoin user can be a developer, may run a fully validating node, and at the same time be a miner or engage in other Bitcoin related businesses. The same applies to other participants in Bitcoin governance. As the constitutional checks and balances system is heavily built on the idea of separation of powers, in the absence of such separation, a checks and balances system would be at best dysfunctional, and at worst redundant. The second problem with such analogies is that there is no real representation or agency relationship between the user community and developers, miners, or node operators. For example, when a developer writes a piece of code, or otherwise contributes to the protocol, one could hardly imagine that she is acting on behalf of or as an agent to users. Therefore, such analogies fail to convey any meaningful message about Bitcoin governance.

Parallels have also been drawn between Bitcoin governance and corporate governance. This parallelism is either implicit or explicit. Some studies have explicitly advocated the application of corporate governance standards to the governance in cryptocurrency ecosystems. In contrast, other studies do not explicitly refer to corporate governance. However, their treatment of Bitcoin governance, conclusions, and policy recommendations seem to be rooted in the corporate governance literature. Further studies have highlighted the role of Bitcoin as FMI and whether Bitcoin is compliant with the current legal and regulatory and governance requirements applicable to conventional FMIs. This latter approach should also be viewed in the shadow of the Bitcoin-governance-as-corporate-
governance thesis, in which there is an implicit or explicit assumption of agency problems or trust relationships, and the assumption that the Bitcoin blockchain and its function is a (semi-) public one as market infrastructure.

However, a quick overview of the corporate governance literature clearly demonstrates that the drawing of parallels between corporate governance and Bitcoin governance is misleading. Since the seminal work of Berle and Means, *The Modern Corporation and Private Property*, it is believed that the separation of ownership and control in large corporations results in managerial autonomy, because diffused share ownership would prevent shareholders from effectively monitoring the managers. The entire corporate governance literature has been developed on this simple but powerful insight. This is why shareholders select board members to monitor managerial activities. However, the main difference between such a governance scheme built on the premises of agency relationship and information asymmetry which could give rise to opportunistic behavior, and Bitcoin governance, is that in the Bitcoin ecosystem, there does not seem to be any meaningful separation between ownership and control, and hence no agency relationship. Furthermore, Bitcoin blockchain transparency minimizes the information asymmetry between various Bitcoin stakeholders such that most of the venues for opportunistic behavior are practically closed off. In addition, Bitcoin has successfully decreased the role of intermediaries and has given birth to a trust-minimized ecosystem. Such an achievement is what sets Bitcoin governance apart from conventional corporate governance.

One of the major implications of this analogical reasoning based on the seeming resemblance between Bitcoin governance and corporate governance has been the suggestion that certain fiduciary duties should be imposed on Bitcoin coders or developers, a proposal that can have a significant impact on Bitcoin governance. However, it seems that such a proposal is based on the assumption that there exists an agency and trust relationship between Bitcoin developers and users, and that developers can effect changes either by themselves or on behalf of other network participants. The problem with fiduciary duties in Bitcoin governance is that developers can only *propose* changes to the protocol, whereas the implementation of a Bitcoin Improvement Proposals (“BIPs”) requires a

---

19 ADOLF A. BERLE JR. & GARDINER C. MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY (1933).
20 Walch, supra note 17. See also Hacker, supra note 2. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. (2016). For a different view see van Wirdum, supra note 7. See also Jerry Brito & Peter van Valkenburgh, *Writing and Publishing Code Alone Cannot Be a Crime*, COINCENTER.ORG (Oct. 29, 2018); Raina Haque et al., *Blockchain Development and Fiduciary Duty*, STAN. J. BLOCKCHAIN L. & POL’Y (2019).
consensus to be reached by other participants, especially Bitcoin users. In this respect, it is not clear how such fiduciary duties are to be designed if the developers do not have the authority or power to implement and impose that implementation on other network participants. In this sense, developers are said to be one of the least powerful major Bitcoin stakeholders.  

Furthermore, the imposition of fiduciary duties should be commensurate to the extent of the agent’s authority to exert a meaningful influence on behalf of the principal that could bind her. If no such authority exists, imposition of the duty would go far beyond the long-established legal principle that no one should be held liable for that which is beyond her control. Moreover, if such duties are to be imposed, it is not very obvious to whom those duties should be owed. Ideally, the majority of Bitcoin users should be anonymous, which makes the identification of the persons to whom the duty is owed an arduous task.

A third approach to Bitcoin governance draws parallels between Bitcoin governance and internet governance. The main focus of this approach is to discern whether it is appropriate to follow the internet governance model and apply similar mechanisms to Bitcoin governance. The literature on internet governance has always been a battleground of two opposing forces: government-centric multilateral governance model and the private-sector-led multi-stakeholder governance model (or distributed governance model). Indeed, Bitcoin governance shares many common features with internet governance, in particular that both governance models deal with governance in relatively decentralized systems. This indeed makes internet governance the closest model that could be analogized to Bitcoin governance.

Bitcoin governance is similar to internet governance in that it is concerned with the governance of a distributed system. The emphasis on decentralization in earlier days in internet governance is what makes it especially similar to Bitcoin governance. In this sense, Bitcoin governance has already benefited from the governance mechanisms present in internet governance. For example, the process that is used to make updates to Bitcoin protocol follows the Request for Comments (“RFC”) format created in 1969 for the ARPANET. However, the promise of decentralization in

21 Jeffery Atik & George Gerro, Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice, STAN. J. BLOCKCHAIN L. & POL’Y 7 (2018).
22 De Filippi & Loveluck, supra note 13. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).
23 See generally Glob. Comm’n on Internet Governance, WHO RUNS THE INTERNET? THE GLOBAL MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE (2017), https://issuu.com/cigi/docs/gcig_volume_2/4.
24 In the same vein, the analogies to the internet can be useful in analyzing certain aspects of Bitcoin governance, such as the analogy made between Bitcoin layers and layers of the internet. DE FILIPPI & WRIGHT, supra note 22; Eric Lombrozo, BIP 123 (Aug. 26, 2015),
the internet largely faded away with the passage of time, and other issues such as access to internet, net neutrality, data protection, and the role of governments in regulating the internet have taken center stage in its governance.

In addition to the decentralized nature of the internet and Bitcoin, Bitcoin governance diverges from the internet governance in some other key respects. For example, some of the market failures in the governance of the internet have been designed out through various innovations in Bitcoin. In particular, embedding the digitally scarce native asset is one such innovation that motivates stakeholders, including miners, users and developers to play an active role in securing the Bitcoin network and contributing to the maintenance of the network. In addition, embedding the PoW algorithm in the Bitcoin network shields it against various attacks and spamming activities and indirectly encourages cooperative behavior on the part of the participants in the ecosystem. Furthermore, the direct compensation of miners through block rewards ensures that the miners have enough at stake not only to behave cooperatively to secure the system, but also to contribute to the governance of Bitcoin. Embedding such incentive-compatible mechanisms in the design of the Bitcoin network mitigates concerns about positive externalities, or the potential tragedy of the commons, expressed where governance is seen as a public good—or commons. In other words, such built-in incentive mechanisms that promote an active role for participants in Bitcoin governance differentiate the governance model of Bitcoin from that of the internet.

To summarize, in spite of the similarities to constitutional, corporate and internet governance, Bitcoin possesses features that differentiate it from all three governance models. Therefore, as enlightening as such broad analogies may seem, they remain misleading to varying degrees. By highlighting the idiosyncrasies of Bitcoin and its governance mechanisms, the next section argues for an idiosyncratic governance model for Bitcoin that maximizes its unique value proposition and hence benefits the entire population of its constituents and stakeholders.

---

https://github.com/bitcoin/bips/blob/master/bip-0123.medawiki; Aaron van Wirdum, *Why Some Changes to Bitcoin Require Consensus: Bitcoin’s 4 Layers*, BITCOIN MAGAZINE (Feb. 26, 2016). By slicing the Bitcoin network to many layers similar to that of the internet, this provides an analytical view of the governance of Bitcoin that is essential to both understanding the Bitcoin network and potential regulatory measures for minimizing the risks stemming from the network. For example, an indirect regulatory approach to regulating Bitcoin can be advocated for based on such an analogy. See Hossein Nabilou, *How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency*, INT’L J. L. & INFO, TECH (2019), for more details on the indirect regulation of Bitcoin.

25 The heavy capital investment by miners in the mining infrastructure highly increases their incentives to act cooperatively rather than attack the network. See Hasu, *No, Concentration Among Miners Isn’t Going to Break Bitcoin*, COINDesk (Feb. 20, 2020).
Towards an idiosyncratic governance model for Bitcoin

The governance framework of an organization or network is a function of governance objectives. Different organizational structures require different sets of governance mechanisms based on their idiosyncratic features. Given the importance of certain firms such as those providing conventional FMI services, a formal governance framework is a necessity for them. For example, Principle 2 of the Principles for Financial Market Infrastructures states that “[a]n FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.” But the question is whether a formal governance framework for FMIs is also suitable for Bitcoin as a dFMI.

In this regard, it is important to make a distinction between permissioned and permissionless blockchains. Thanks to their decentralization, in permissionless networks no entity could be identified to have meaningful control of the network such that it would be granted specific powers and burdened with equivalent responsibilities in the governance of a distributed network. In this sense, unlike the mainstream perception of Bitcoin governance, this paper argues that Bitcoin’s current governance framework is suited for the purpose that it is created to serve, i.e., establishing a censorship-resistant store of value and medium of exchange. From this perspective, the importance of Bitcoin manifests itself in providing optionality for those who do not have access to the conventional financial markets or whose access has been revoked.

Censorship resistance as the unique value proposition of Bitcoin is reflected in the Bitcoin whitepaper\textsuperscript{26} as well as in Satoshi Nakamoto’s communications with early bitcoin adopters. Given the fate of Bitcoin’s predecessors such as Digicash and American Liberty Dollar (“ALD”)\textsuperscript{27} whose centralization was their undoing, the creator or creators of Bitcoin had the understanding that permissionless innovative payment systems have to be decentralized, otherwise those innovations will face the same fate as

\textsuperscript{26} Nakamoto, supra note 1.
\textsuperscript{27} Aaron van Wirdum, The Genesis Files: How David Chaum’s eCash Spawned a Cypherpunk Dream, BITCOIN MAGAZINE (Apr. 24, 2018). See also Aaron van Wirdum, The Genesis Files: If Bitcoin Had a First Draft, Wei Dai’s B-Money Was It, BITCOIN MAGAZINE (June 15, 2018); Nick Bilton, American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road (2017).
Bitcoin’s ancestors. This is also clear from the chronology of the technological breakthroughs that led to the birth of Bitcoin.\(^{28}\)

More importantly, the censorship-resistant property of Bitcoin manifests itself in the design of the Bitcoin network. The clearest manifestation of this property is in the trade-off between efficiency and censorship resistance. Rather than opt for fast and efficient payments, Bitcoin goes a long way to create extreme inefficiencies by introducing a distributed ledger that should be maintained, updated and validated by all fully validating nodes, only to make sure that no single or a small group of participants violates the rules of the Bitcoin protocol, modifies the ledger arbitrarily, or censors other stakeholders from participating in the Bitcoin network. Within the Bitcoin network, the objective of becoming a fast and efficient global settlement layer is secondary and should yield if conflicting with the objective of censorship resistance.

It is indeed difficult not to notice that the censorship-resistant property of Bitcoin drives the entire mechanism design embedded in the Bitcoin network. Since Bitcoin is designed to operate outside the legal framework, it assumes an adversarial environment and prepares to defend itself against various attack vectors using a variety of ex-ante built-in mechanisms within the Bitcoin network rather than rely on the external legal system for ex-post remedies. To this end, the PoW security and consensus mechanism and various other incentive mechanisms are embedded to align the often varied and divergent interests of network participants and discourage uncooperative behavior that could result in attacks on the network.\(^{29}\)

More importantly, it seems that pursuing censorship resistance is the single use case that could bring the interests of users, investors, miners, and other actors in the ecosystem together. As other properties of Bitcoin could easily be replicated and conducted more efficiently within the traditional banking, financial, and payment institutions, without its censorship-resistant property, Bitcoin would be redundant.\(^{30}\) In this sense, if Bitcoin network were just a normal payment system without any censorship-resistant property, its native token would have had virtually no value at all. Therefore, compromising this core feature would render the entire network useless.

Having said so, the failures or shortcomings of Bitcoin governance should be analyzed in light of the objectives of Bitcoin governance. If Bitcoin governance is to maximize its value as an uncensorable dFMI, one

\(^{28}\) See generally Arvind Narayanan & Jeremy Clark, *Bitcoin’s Academic Pedigree*, 15 COMMS. OF THE ACM (2017).

\(^{29}\) De Filippi & Loveluck, *supra* note 13, at 5-6.

\(^{30}\) For a similar view, see Gabriel Shapiro, *In Defense of Szabo’s Law: For a (Mostly) Non-Legal Crypto System: A Lawyer’s Response to Vlad Zamfir’s “Against Szabo’s Law, For A New Crypto Legal System,” MEDIUM (Jan. 26, 2019).
could issue a different verdict on Bitcoin governance compared to the scenario in which the objective of Bitcoin governance is to maximize its value proposition as a payment mechanism to compete with established payment infrastructures such as Visa, Mastercard, or other wholesale and retail payment infrastructures. In the latter case, one could concede that the governance of Bitcoin is broken, because it is unlikely for a decentralized organization to reach the level of efficiency that exists in the centralized systems due to the resources needed to overcome coordination problems in PoW-based decentralized systems. The rest of this paper will gauge the success or failure of Bitcoin governance in light of the fact that it is designed to be a censorship-resistant network.

**Is Bitcoin governance broken?**

Various governance crises in Bitcoin thus far have highlighted the role of governance and its importance in the Bitcoin ecosystem. One of these crises was the famous scaling crisis that led certain well-known figures in the cryptocurrency ecosystem to declare that Bitcoin governance is broken, and that the Bitcoin project should be liquidated. Despite said protestations and doomsday predictions, the Bitcoin network has continued to grow. However, the legitimate question remains as to whether there are deficiencies in Bitcoin governance that could warrant interventions by third parties, such as private sector stakeholders or governments. As the classic reason for third-party intervention in free markets is to establish a case for market failures, the starting point for the investigation is to fathom whether Bitcoin governance works or there are market failures that would necessitate remedial actions.

The theory of market failure suggests that markets fail due to externalities, imperfect competition, and imperfect information which give rise to agency costs and coordination problems. The rest of this paper identifies the potential market failures in Bitcoin governance by reference to its four major governance crises. These crises include the value overflow incident (2010), the erroneous upgrade and double spend in Bitcoin network (2013), the discovery of an inflation bug (2018), and the Bitcoin scalability debate (2015-2017). The first three of these crises highlight the coordination problems arising from imperfect information (i.e., information asymmetry) in the maintenance of code and the fixing of bugs. The first two of these incidents highlight coordination problems in the maintenance of code, whereas the third put a spotlight on the potential opportunistic behavior that such information asymmetries could give rise to in the relationship between developers and users (and even miners). The third important issue giving

---

31 Mike Hearn, *The Resolution of the Bitcoin Experiment*, MEDIUM (Jan. 14, 2016).
rise to market failures originates from the problems associated with imperfect competition. The fourth major Bitcoin crisis (i.e., the scalability debate) highlights the role of competition and fork-choice rule and foot voting in resolving governance disputes in the Bitcoin ecosystem.

Information asymmetry could give rise to either coordination problems, that might hinder effective governance and maintenance of Bitcoin, or to opportunistic behavior, including adverse selection (such as the classic Lemons problem à l’Akerlof) that might hinder bitcoin adoption. The latter also includes the adverse selection problem that may emerge if certain participants who have private information about the Bitcoin network, such as the knowledge of an existing bug, engage in selling bitcoins to less informed market participants. In this section, this potential opportunistic behavior is studied first prior to investigating the coordination problems.

**Agency costs and opportunistic behavior in Bitcoin governance**

One of the main objectives of conventional corporate law and governance is to remedy the agency costs in a corporation. In traditional corporate governance, information asymmetry between principals (shareholders) and agents (managers or officers) increases the agency costs, e.g., chances of engaging in opportunistic behavior such as looting by managers. The early literature has recognized this problem by focusing on the separation of ownership and control and highlighting that the diffuse

---

32 See George A. Akerlof, *The Market for “Lemons”: Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECONOMICS 488 (1970).
33 George A. Akerlof et al., *Looting: The Economic Underworld of Bankruptcy for Profit*, 1993 BROOKINGS PAPERS ON ECON. ACTIVITY (1993).
share ownership would eventually lead to managerial autonomy.\textsuperscript{34} To mitigate the agency costs, principals often use various mechanisms, such as the board of directors to monitor the performance of those who are in control (management). Combined with various other mechanisms, conventional corporate governance has only been relatively successful in controlling managers and protecting shareholders, especially the minority shareholders.

The question is whether the conventional corporate governance paradigm can be applied to Bitcoin. It appears that such a transplant remains dubious at best. Firstly, as the agency relationships (both in the legal and economic sense) do not exist between various participants in the Bitcoin network, traditional mechanisms of corporate governance can hardly be applicable to Bitcoin governance. Agency relationships and the protections that are in place for both principals and agents, such as fiduciary duties and duties of care and loyalty,\textsuperscript{35} are traditionally established where there is a relationship of trust between the parties to a relationship. However, central to the idea of Bitcoin is the creation of an alternative decentralized network that could compete with traditional economic organizations by proposing a different form of organizational governance.\textsuperscript{36} In other words, the main idea of having Bitcoin in place is to use a trustless or trust-minimized socially scalable system for transacting or reaching consensus in an adversarial environment.\textsuperscript{37} This applies in particular to those who run fully validating nodes and hence participate in the Bitcoin network directly and without the intermediary role of third parties. In this sense, Bitcoin has tried to remove the principal-agent problem by replacing humans with machines at the center of the network and moving human discretion to the periphery.\textsuperscript{38}

Secondly, since the Bitcoin network is highly transparent about its protocol, blockchain, and methods of effecting change in the protocol, it is difficult to establish a clear-cut informational asymmetry between various participants in the network. Such a difficulty is exacerbated by the fact that various participants in the network can assume different roles. For example, a developer can simultaneously be a user and can be employed by a mining company or other Bitcoin businesses. Furthermore, she can operate a fully validating node and can run her own Bitcoin business. This muddies the traditional information asymmetry framework in conventional organizations.

\textsuperscript{34} BERLE JR. & MEANS, supra note 19. See also Brian R Cheffins, The Rise and Fall (?) of the Bearle-Means Corporation, 42 SEATTLE U. L. REV. (2018).
\textsuperscript{35} See Balkin, supra note 20.
\textsuperscript{36} Davidson et al., supra note 13; ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016).
\textsuperscript{37} Nick Szabo, Money, Blockchains, and Social Scalability, UNENUMERATED (Feb. 9, 2017).
\textsuperscript{38} Hsieh et al., supra note 4, at 51; Vitalik Buterin, DAOs, DACs, Das and More: An Incomplete Terminology Guide, ETHEREUM BLOG (May 6, 2014).
where there is a relatively clear division of labor and separation of roles and powers that make it possible to define various conflict-of-interest rules for participants.

Finally, it appears that in the Bitcoin network, participants are symmetrically informed about all aspects of the Bitcoin network, or where there is a hidden aspect to the network (e.g., unknown unknowns) that information is hidden symmetrically.\(^3\) To be clear, this does not mean that there is complete information, but there is no \textit{asymmetric} information. One might argue that there are influential figures—constituting a small fraction of participants in the Bitcoin network whose decisions can affect the network disproportionately—who may have some inside information that would create information asymmetry. Although information asymmetries might exist outside of the technical environment of the Bitcoin network and in the allegedly closed circles of a few prominent participants such as miners, developers and investors,\(^4\) there are mechanisms embedded in the Bitcoin network that can remedy such informational asymmetries. For example, the mere fact that the decisions made by so-called insiders cannot be imposed on other participants due to the possibility of forking and creating the version of Bitcoin that best serves the interests of the broader community of the users makes such informational asymmetry largely inconsequential.\(^5\)

Thus far, there is no publicly-known evidence that any of the core developers or their close relatives, or those endowed with the private information about potential bugs in the Bitcoin protocol, have engaged in opportunistic behavior and abused their special status by trading on such private information. Though the possibility of such a phenomenon cannot be entirely disregarded, Bitcoin’s checks and balances system thus far has largely dealt with this problem. Therefore, as of this writing, there seems to be no need for imposing potential liability rules on Bitcoin network participants above and beyond the existing general liability rules that would nevertheless be applicable to anyone irrespective of being active in the cryptocurrency ecosystem or in the real economy.

\(^3\) Hossein Nabilou & André Prüm, \textit{Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies}, \textit{J. of Fin. Regul.} (2019).

\(^4\) Hsieh et al., \textit{infra} note 4.

\(^5\) Even if there were consequential information asymmetries in the Bitcoin network, imposition of traditional conflict-of-interest rules, including fiduciary duties on developers, could not be justified, mainly because the core development team is not an official designation that could grant rights to or impose responsibilities on the developers. In addition, having such designations as official Bitcoin developer risks a level of centralization in Bitcoin network that a truly decentralized and censorship-resistant network cannot afford. Furthermore, as mentioned earlier, an additional problem with assigning liability to protocol developers is that they cannot force software changes and updates to other participants in the network. See Haque et al., \textit{infra} note 20, at 11.
Coordination problems in Bitcoin governance

Information asymmetries may give rise to coordination problems among participants in the Bitcoin network, especially among Bitcoin developers, and may eliminate any incentives for their contribution to protocol improvements and maintenance, particularly in times of crisis. First, the developers are dispersed and relatively decentralized, meaning the coordination for fixing bugs and adding patches can take a substantial amount of time. Due to this operational risk, the very existence of Bitcoin could be put at risk. Second, information asymmetry can also be present where there is a major impending event that could fork Bitcoin. Such informational asymmetry can create standoffs of the sort that were seen in the debate about scaling Bitcoin. Third, information asymmetry in distressed times can also give rise to runs on Bitcoin. If participants in the Bitcoin network would come to the conclusion that there is an epsilon of material information that is unevenly distributed in the network, each and every participant in the network is better off selling their holdings and only afterwards investigating the nature of the piece of information hidden from them.

The Bitcoin network mitigates some of the coordination problems that exist among users, nodes, miners and other direct participants in the Bitcoin network. For example, the Nakamoto consensus is embedded in the Bitcoin network to make it Byzantine fault tolerant and resilient to Sybil attacks, which in itself encourages coordination among network participants. However, the governance of the network, as it is indirect and exercised at a different level (off-chain), remains subject to coordination problems, especially where there would be a need for maintenance, upgrade, or otherwise making changes to the protocol, or when there is an urgent need to effectively respond to an attack on the network in a timely manner.

Various governance mechanisms attempt to reduce these coordination problems. For example, making upgrades to the Bitcoin protocol follows the tradition of open source software, i.e., the Request for comments format, created in 1969 for the ARPANET. To further reduce coordination problems, various channels of communication such as BitcoinTalk Forum and Bitcoin Core GitHub repository are set up, and relatively informal processes for upgrading Bitcoin’s protocol, such as BIP—which is a standardized process for proposing, testing and peer review of the new proposals for effecting changes to the protocol—are established. The latter

42 De Filippi & Wright, supra note 22.
43 See Atik & Gerro, supra note 21, at 4.
procedure is to ensure that innovation is not hindered while the improvements are implemented through consensus and collaboration.

In the early days of Bitcoin, there was no specific framework for improving Bitcoin protocol. Satoshi created the code and simply made improvements. He used to solicit feedback from the Cryptography Mailing List, and eventually decided to create the BitcoinTalk Forum. At the time, Satoshi alone was in charge of effecting any changes or upgrades to Bitcoin. In 2011, Nakamoto left the Bitcoin project and handed it over to Gavin Andresen. As Gavin did not want to accept the responsibility alone, he in turn enlisted four other developers[^44] who became known as Bitcoin Core developers (“Core Devs”). Bitcoin Core Devs have commit access to the Bitcoin Core GitHub repository and maintain the Bitcoin codebase. They are the only developers who have the ability to push live code to the Bitcoin Core client. Therefore, although hundreds of developers have contributed to the code, only a few of them have commit access to the code base.[^45]

Having only a few Core Devs with commit access to the code may give the impression of significant centralization. However, these Core Devs are not unconstrained and changes to the code follow a process of rough consensus that determines which proposed changes are to be merged into the protocol.[^46] In deciding whether to merge a proposal or a patch, Bitcoin Core Devs will take the followings into account:

- Whether the patch is in line with the general principles of the project;
- Whether it meets the minimum standards required for inclusion; and
- Whether it aligns with the general consensus of contributors.[^47]

Such broad language grants a great deal of informal powers to Bitcoin Core Devs. In addition, it is even theoretically possible for maintainers to organize a coup to hijack the GitHub repository and censor the dissenting developers, or even hijack the brand name of Bitcoin (core). However, those powers are again constrained by at least two factors; first, that Bitcoin developers are not a homogenous pool of developers, which makes it unlikely for them to hijack the project, and second, the fact that dissenting developers can always fork the code and shift their work to a different repository that is not controlled or otherwise influenced by Bitcoin Core

[^44]: These core maintainers include Pieter Wuille, Wladimir van der Laan, Gregory Maxwell, and Jeff Garzik.
[^45]: SFOX, *Bitcoin Governance: What are BIPs and How Do They Work?*, MEDIUM (Apr. 16, 2019).
[^46]: See CONTRIBUTING TO BITCOIN CORE, GITHUB, https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md.
[^47]: SFOX, *supra* note 45.
maintainers.\(^{48}\) Again, the threat of forks, especially hard forks, to which the developers have expressed aversion, presents a strong check over the potential abuse of powers by developers.

**The impact of competition on Bitcoin governance**

Zooming in on various competitive forces in Bitcoin, three forms of competition with Bitcoin Core can be identified: competition between chains, competition between independent implementations, and competition between Bitcoin and other competing software projects (which neither change the consensus rules nor reimplement the codebase).\(^{49}\) These competitive forces may be best classified as internal and external competition. Internal competition refers to the ability for each individual to fork Bitcoin’s codebase and blockchain and create their competing network or chain. External competition, similar to the market for corporate control, refers to the competitive pressures exerted by other cryptocurrency projects that would put substantial pressure on Bitcoin to improve its governance model. Unlike the market for corporate control for certain institutions (e.g., banks) in certain jurisdictions (e.g., Europe) that are somewhat paralyzed by extensive regulatory requirements,\(^{50}\) Bitcoin faces cut-throat competition in a market for cryptocurrencies without any entry or exit restrictions and no regulatory barriers to competition.\(^{51}\)

The most important governance mechanism in Bitcoin is provided by its open-source software that can be tweaked and forked. One method of making a change in Bitcoin is through hard forks. A hard fork is a backward-incompatible change to the rules of the consensus. For example, increasing the block size of Bitcoin can be seen as a hard fork, in the sense that if a fully validating node would receive blocks with sizes higher than one megabyte, it will reject the block as it violates the rules of the consensus. Once the block height, where a specific hard fork is scheduled to activate, hits, each individual miner and user can determine which set of rules to follow and enforce.

There may be several methods for resolving a hard fork. First, if one chain accumulates a lower hash rate than its competing chain, it would take

\(^{48}\) See also Jameson Lopp, *Who Controls Bitcoin Core?*, Cypherpunk Cogitations (Dec. 15, 2018); Jameson Lopp, *Nobody Understands Bitcoin (And That’s OK)*, CoinDesk (Mar. 11, 2017).

\(^{49}\) BitMEX Research, *Competing with Bitcoin Core* BitMEX Blog (Oct. 15, 2018), https://blog.bitmex.com/bitcoin-cores-competition.

\(^{50}\) For the regulatory limitations imposed on the corporate takeover of banks in the EU see Georgina Tsagas, *The Market for Corporate Control in the Banking Industry*, in *The Law on Corporate Governance in Banks* (Iris H-Y Chiu & Michael McKee eds., 2015).

\(^{51}\) Lawrence H. White, *The Market for Cryptocurrencies*, 35 CATO Journal 383, 384-386 (2015).
longer for it to reach the 2016 block cycle for the readjustment of mining difficulty. However, the chain with the higher hash rate would continue building its blocks regularly and accumulating more PoW. In this case, following Nakamoto consensus, users opt for following the chain with the most accumulated PoW. The second way to solve the hard fork is for the users/full nodes to decide to follow the chain that has the lower amount of accumulated PoW. This may render the chain with the higher PoW irrelevant. The third method of resolving the hard fork is for two independent networks to run independently using replay protection. Indeed, nothing can prevent the two resulting chains from being mined by miners or validated by full node operators. This can result in two competing chains running in parallel, which could cause a great deal of uncertainty that often receives lukewarm reception as the dispute resolution mechanism of last resort in the Bitcoin ecosystem. An extraordinary example of resolving disputes through hard forks in the Bitcoin ecosystem occurred in 2017, which came to be known as the scaling crisis of 2017.

Scholars have argued that the scaling crisis of 2017 and the failure in conflict resolution illustrate a fragile decision-making mechanism within the Bitcoin network. However, with the benefit of hindsight and the fact that the narrative of Bitcoin has shifted from being a payment system to becoming a store of value and a digital infrastructure for clearing and settling transactions without being subject to censorship, Bitcoin’s adversarial governance mechanisms have in fact contributed to its long-term goal of establishing this image of Bitcoin as a censorship-resistant network.

In addition to the role of the aforementioned internal competition in Bitcoin governance, Bitcoin faces external competitive forces from both competing cryptocurrencies as well as fiat currencies. As there are virtually no barriers to entry and exit, Bitcoin—to the extent that it is used as a substitute for other currencies—competes with currencies in the forex markets. In addition, to the extent that Bitcoin is viewed as a store of value, it competes with traditional commodities used as stores of value such as gold. Such competitive forces have indeed huge implications for Bitcoin’s governance and push Bitcoin to continuously improve itself to stay relevant.

52 For more technical details see Antonopoulos, supra note 1, at 253.
53 See Laura Shin, Will This Battle For The Soul Of Bitcoin Destroy It?, FORBES (Oct. 23, 2017). See also Poon & Dryja, supra note 11; van Wirdum, supra note 11; Jedusor, supra note 11; van Wirdum, supra note 11; Eric Lombrozo, Forks, Signaling, and Activation, MEDIUM (June 18, 2017).
54 De Filippi & Loveluck, supra note 13, at 9.
55 Albert O. Hirschman, Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States (1970). See also Atik & Gerro, supra note 21.
Externalities and public goods nature of Bitcoin governance

Although there is no general agreement on whether law and governance constitute public goods, governance exhibits many properties of a public good insofar that it is non-excludible and non-rivalrous. In the same vein, to the extent that it is non-excludible and non-rivalrous, Bitcoin governance possesses the properties of a public good. Although bitcoin, as a unit of account in the Bitcoin network, is not a public good as it is both excludible and rivalrous, the Bitcoin network, and in particular, the maintenance and governance of the protocol, could be said to be a public good. As the benefits of good governance in Bitcoin are shared by everyone, and use by one participant does not decrease such benefits to other participants, Bitcoin network participants face collective action and free-rider problems. Therefore, it is likely that maintenance and governance of Bitcoin would be under-provided if left to the markets.

Despite public-good designation of Bitcoin governance, upon closer inspection, the main market failure in Bitcoin governance may be due to the classic commons property of Bitcoin governance. The permissionless nature of Bitcoin means that no one can be excluded from either participating in Bitcoin governance or from consuming the benefits of good governance in Bitcoin. However, since the use of block space by one user reduces the amount of space left to other users, Bitcoin can be said to be a rivalrous good or service. The classic problem of commons is that no one has adequate incentives to contribute to its governance, because the benefits of such contributions cannot be fully captured by the contributors, and the overuse of common resources often leads to the tragedy of the commons and the eventual depletion of common resources.

Market failure as a result of the commons nature of Bitcoin may be derived especially from fully validating nodes. Such node operators, which are the watchdogs of miners, may have no incentive to operate a fully validating node in the absence of proportionate reward for their operation due to the free-rider problem. The same applies to developers whose contribution to the code is voluntary, reputation-based, or in some instances market driven, i.e., financed by start-ups or corporations. Such collective action problems may be addressed using a variety of mechanisms. Various mechanisms embedded in the Bitcoin network have incentivized participants to contribute to Bitcoin governance and to maintenance of the code. For

56 Compare Tyler Cowen, Law as a Public Good: The Economics of Anarchy, 8 ECON. & PHILOSOPHY (1992) with David D. Friedman, Law as a Private Good: A Response to Tyler Cowen on the Economics of Anarchy, 10 ECON. & PHILOSOPHY (1994).

57 See Charlotte Hess & Elinor Ostrom, Understanding Knowledge as a Commons: From Theory to Practice 4 (2007). See generally Garrett Hardin, The Tragedy of the Commons, 162 SCIENCE 1243 (1968).
example, using bitcoin for payments involves fees that discourage spamming and the overuse of the network. In the future, it is likely that the industry would provide financial incentives for contribution to Bitcoin development. In certain other cryptocurrencies, there have been suggestions to provide subsidies for cryptocurrency developers by taxing miners.\(^5\) Though the dislike for compulsory taxation would make the realization of such proposals in the Bitcoin ecosystem very unlikely, more market-based and voluntary incentive mechanisms could likely emerge.

Despite the fact that Bitcoin governance is prone to the free-rider problem, thus far, its governance has proven to be both effective and relatively successful. This is puzzling as insights from economic literature, such as public goods, club goods,\(^5\) the tragedy of the commons,\(^6\) and game theory\(^6\) suggest that free-rider problems would result in a failed and broken governance model in Bitcoin. Perhaps the solution to this puzzle should be sought after in different schools of thought. For example, in contrast to the standard economic theory that predicts the tragedy of the commons and over-exploitation and depletion of the common resource, certain studies—pioneered by Elinor Ostrom—have found that such mainstream economic thought has not been entirely accurate, and where common resources exist, a variety of bottom-up mechanisms have emerged to address the issue.\(^6\)

Therefore, it is not clear whether the tragedy of the commons is a reality or a myth.

On the other hand, deriving evidence from the pattern of social production on the internet (e.g., Wikipedia), some scholars suggest that new patterns of production are emerging that are based on different incentive mechanisms than those studied under the classical economic theory. The theory of commons-based social production, put forward by Yochai Benkler, is a prominent example of this approach.\(^6\) Yet another way to

\(^{5}\) Jiang Zhuoer, *Infrastructure Funding Plan for Bitcoin Cash*, MEDIUM (Jan. 22, 2020).
\(^{5}\) RICHARD CORNES & TODD Sandler, *The Theory of Externalities, Club Goods, and Public Goods* (1996).
\(^{6}\) Hardin, *supra* note 57. See also Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (1990); Elinor Ostrom, *Coping With the Tragedies of the Commons*, 2 ANNALS REV. POL. SCI. (1999); Francesco Parisi & Ben Depoorter, *Commons and Anticommons*, in *The Encyc. of Public Choice* (Charles K. Rowley & Friedrich Schneider eds., 2004); Francesco Parisi et al., *Simultaneous and Sequential Anticommons*, 17 EUR. J. OF L. & ECON. (2004).
\(^{6}\) Stephen Morris & Hyun Song Shin, *Global Games: Theory and Applications*, in *Advances in Economics and Econometrics: Theory and Applications, Eighth World Congress* (Lars P. Hansen et al. eds., 2003). See also Joseph Abadi & Markus Brunnermeier, *Blockchain Economics* (Nat’l Bureau of Econ. Rsch., Working Paper No. 25407, 2018).
\(^{6}\) Ostrom, *supra* note 60. See also Ostrom, *supra* note 60; Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. (2010).
\(^{6}\) Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (2006).
explain the success of the Bitcoin community in maintaining the code and resolution of disputes without resorting to external factors or third parties is by reference to the literature on law without order, which highlights the insignificance of the law and formal mechanisms in social coordination and dispute resolution, instead emphasizing the importance of unwritten social norms. Irrespective of the reasons, Bitcoin seems to be like the proverbial Bumblebee that in theory would not fly, but in practice does. The three aforementioned non-mainstream theories may be helpful in shedding some light on how Bitcoin governance works and manages to encourage the community to maintain the code and resolve disputes.

**Bitcoin governance and downward accountability**

It is argued that Bitcoin governance, similar to other governance models, needs legitimacy. Although at first glance, Bitcoin governance seems ambivalent regarding the concept of legitimacy, this paper argues that legitimacy in Bitcoin governance stems from its downward or market accountability, meaning that users are afforded with mechanisms that enable them to exert a significant influence on Bitcoin governance. Among others, users may employ a variety of mechanisms to participate in governance of the network. Firstly, users may threaten not to run the software proposed by developers. Secondly, those users running fully validating nodes may threaten not to validate certain blocks broadcasted by miners. Thirdly, users may vote *with their feet* by abandoning the project, i.e., its usage, mining, or development of Bitcoin altogether.

The importance of network effects in Bitcoin renders foot voting a very powerful mechanism in Bitcoin governance because abandoning the project by its users could amount to its immediate demise. Although foot voting is available to all participants in Bitcoin governance with varying degrees of costs and benefits, it seems to be the cheapest option for users, compared to miners or developers. This enables users to leverage this powerful device in any dispute over Bitcoin governance, ultimately resulting in a market-driven, bottom-up, decentralized form of governance for Bitcoin.

---

64 ROBERT C. ELICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).
65 This metaphor is expressed by the former president of the European Central Bank (“ECB”) about the euro. See Mario Draghi, President of the European Central Bank, Speech at the Global Investment Conference in London (July 26, 2012) (transcript available at https://www.ecb.europa.eu/press/key/date/2012/html/sp120726.en.html).
66 Colin Scott, Accountability in the Regulatory State, 27 J. L. & Soc’y (2000). See also Colin Scott, Regulation in the Age of Governance: The Rise of the Post-Regulatory State, in THE POLITICS OF REGULATION: INSTITUTIONS AND REGULATORY REFORMS FOR THE AGE OF GOVERNANCE (Jacinta Jordana & David Levi-Faur eds., 2004).
67 For the concept of polycentric governance model see David Zaring, Financial Regulation’s Overlooked Networks, in RECONCEPTUALISING GLOBAL FINANCE AND ITS REGULATION (Ross
In addition, users, especially those running fully validating nodes, have considerable leverage against miners, because Bitcoin governance largely relies on the emergent consensus through a network-wide agreement of rules ultimately enforced by the users running full nodes. In Bitcoin, miners have to create blocks according to these rules and submit them to the network of full nodes for validation. Then, full nodes validate the block by downloading the block and verifying if those blocks match the consensus rules of the client. The nodes will not reject any block that is considered valid in terms of the most accumulated PoW. However, if the block does not match the criteria of a valid block or does not have the most accumulated PoW, it will be rejected by the nodes. In sum, miners are bound by the rules of the network and have to implement them, otherwise, those blocks will be rejected by the full nodes, which take on the role of watchdogs, constantly monitoring miners for their compliance with Bitcoin’s consensus rules.

Although miners may use the threat of forks (Miner Activated Soft Forks (“MASFs”) or hard forks) or may even use the threat of a 51% attack after the fork to kill the parallel chain as a mechanism to exert influence on Bitcoin governance, ultimately, it is the user community which decides whether to use the fork supported by a subset of miners. For example, in the Bitcoin scaling saga and the activation of the User Activated Soft Fork (“UASF”), some nodes made a commitment to represent the views of users as well as some segments of the business community by advocating a soft fork implementation of Segregated Witness (“SegWit”), in which both SegWit and non-SegWit compliant blocks could be processed. As the majority of the miners did not adopt the SegWit update for a long time after the release of the code, certain Bitcoin users installed a client that threatened to suspend the Nakamoto consensus by ignoring the blocks relayed by the miners refusing SegWit after a specific date. If this situation had dragged on, that soft fork would have resulted in a contentious fork. The mere threat to Bitcoin utility and value from such a contentious fork and hence the miners’ business model finally persuaded miners to stop resisting the SegWit update and acquiesce to the users’ intended result.

The same applies to the powers of developers who can propose software rule changes.

---

P. Buckley et al. eds., 2016). See also David Zaring, *International Law by Other Means: The Twilight Existence of International Financial Regulatory Organizations*, 33 Tex. Int’l L. J. (1998); Anne-Marie Slaughter, *A New World Order* (2004); Anne-Marie Slaughter, *Global Government networks, Global Information Agencies, and Disaggregated Democracy*, 24 Mich. J. Int’l L. 1041 (2003); Finck, *supra* note 13, at 172-8.

68 ecurrencyhodler, *Bitcoin Governance*, MEDIUM (Feb. 5, 2019).

69 Aaron van Wirdum, *The Latest Twist to the Block Size Debate is Called a “UASF,”* BITCOIN MAGAZINE (Mar. 2, 2017).

70 Atik & Gerro, *supra* note 21, at 7. See also Alyssa Hertig, *UASF Revisited: Will Bitcoin’s User Revolt Leave a Lasting Legacy?*, COINDesk (Aug. 3, 2017).
If changes proposed or even implemented by developers are not supported by a significant number of users, those changes eventually will be doomed.

Precedent in Bitcoin’s history shows that users have decided to even ignore Nakamoto consensus due to the fact that the longer chain, or the chain with the most accumulated PoW, did not represent the social contract that users perceived they were parties to. As explained before, this happened in the 2010 integer overflow bug where within 3 hours, Satoshi published a new Bitcoin client and rewound the hyperinflated chain. Similarly, in the 2013 inflation bug incidents, the 0.7/0.8 consensus bug split the blockchain into two separate chains for several hours. In this case, the incident could only be resolved when developers and the mining pools suspended the fork-choice rule temporarily, by supporting the 0.7 fork and abandoning the 0.8 chain. Although this required some miners to forgo the block rewards form the 0.8 chain, they did so with the expectation that it would eventually maximize the overall value of the network.

Ultimately, the key takeaway in Bitcoin governance is that users are not bound to follow miners or developers if a majority of the users do not share the same ideas about the future of the network. In addition, if there is a disagreement over how to maximize network utility, users can suspend Nakamoto consensus and disempower miners. This also applies to any attacker of the Bitcoin network; because users may stop following the chain with the most accumulated PoW, the attacker must take this into account before spending resources on attacking.

CONCLUSION

Bitcoin’s main value proposition is its censorship-resistant property, which is backed by a technological innovation that allows participants to transact in a trust-minimized environment. To retain and maintain such a property, it is highly important for Bitcoin to remain decentralized. Decentralization entails that various participants in the Bitcoin network, in particular its users, have an effective voice in Bitcoin governance. Although

---

71 Hasu et al., A Model for Bitcoin’s Security and the Declining Block Subsidy, UNCOMMONCORE (2019), https://uncommoncore.co/research-paper-a-model-for-bitcoins-security-and-the-declining-block-subsidy.  
72 Charlie Shrem, Bitcoin’s Biggest Hack In History: 184.4 Billion Bitcoin from Thin Air, HACKERNOON (Jan. 11, 2019).  
73 This incident related to the 0.8 update to the Bitcoin, which was the most popular Bitcoin implementation. The new software had an unintended change to the consensus rules causing the block 225,430 to become incompatible with older clients. See Vitalik Buterin, Bitcoin Network Shaken by Blockchain Fork, BITCOIN MAGAZINE (Mar. 13, 2013).  
74 Id.  
75 Hasu et al., supra note 71.  
76 Id.
a variety of stakeholders in the Bitcoin network take part in Bitcoin governance, and there is no single or group of homogenous participants that has the final say, it appears that the ultimate decision is principally made by those who can successfully fork Bitcoin and convince the majority of users to shift to the new chain. In this regard, users of the Bitcoin network seem to possess the ultimate authority to decide which software to install and run, or which implementation to follow. The possibility of forking means that unlike many other ways to resolve societal collective action problems, including a reliance on coercion, Bitcoin governance is based on deliberation, persuasion, volition, and choice.

To resolve disputes in the Bitcoin network and unlike other political decision-making processes, in addition to open and free entry and exit, each and every participant can fork the codebase or the blockchain and create their own version of Bitcoin and try to persuade other users to follow their version of the chain or code. By providing for the technical possibility that the new chain maintains the history of the blockchain going back to the genesis block, as well as the fact that the holders of the legacy coins receive the new coins proportionate to their holdings in the legacy chain, Bitcoin is most open to competition provided by forks. To make a comparison, there is also foot voting in corporate law; however, the act of forking is more than mere foot voting. Forking is similar to incorporating a new company with the same brand name and certain tangible and intangible assets without any new capital expenditure—the only limitation being convincing the greater number of participants to follow the new forked chain. This significantly lifts the barriers to entry and invites even more competition.

There are additional factors that strengthen the position of users as the ultimate decision-makers in the Bitcoin network. For example, users may decide not to install and run the particular software created by developers. Furthermore, they may decide not to validate the blocks broadcasted by certain miners. Last but not least, they have their own mechanisms of forking Bitcoin (e.g., UASF). Contrary to a popular belief that miners and developers control Bitcoin, the history of forks in Bitcoin and the constraints that developers and miners face in influencing the protocol or users confirms that the ultimate decision-makers are users and markets, rather than a relatively centralized groups of developers or miners. Given the multiparty decision-making process in Bitcoin, as well as its reliance on users at the apex of decision-making processes, Bitcoin governance remains decentralized, and it is unlikely that any single actor could have a disproportionate impact over the protocol.

Thus far, Bitcoin governance has worked well in addressing its potential market failures. However, potential challenges lie ahead, and it is not clear whether Bitcoin’s decentralized governance mechanisms can deal with all future crises. One of the issues that is likely to give rise to
governance crises is the declining block reward or subsidy, and its implications for the Bitcoin security model. Various proposals for dealing with such an issue have been put forward, such as improving block space, perpetual issuance, crowdfunding, and adapting the supply of the block space. Another hurdle may arise from discussions regarding a change in security and consensus mechanisms, and a potential shift from PoW to proof of stake (“PoS”), or other mechanisms of securing and reaching consensus in Bitcoin. Governance crises are also likely to emerge if the tamper-resistance property of Bitcoin is called into question. For example, in the immediate aftermath of the Binance hack in 2019, there have been discussions about Bitcoin blockchain reorganization to reverse transactions and undo the damage. Although such discussions faced immediate and strong resistance from users and developers, leading to the concession by miners and exchanges not to pursue the proposal, such issues are likely to bring the question of governance to the forefront again. Only time will tell whether Bitcoin and its governance model can address these critical governance issues.

77 Raphael Auer, Beyond the Doomsday Economics of “Proof-of-Work” in Cryptocurrencies 8-10 (BIS Working Paper No. 765, 2019), https://www.bis.org/publ/work765.pdf.

78 Hasu et al., supra note 71.