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 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 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 Bitcoin network.

Keywords: *Bitcoin, Cryptocurrency, Blockchain, Governance, Censorship resistance*

JEL classification: *E42, E51, E58, G01; G23; G28; K22; K23, K24*

* Postdoctoral researcher in Banking and Financial Law, University of Luxembourg, Faculty of Law, Economics and Finance. Research Associate at the University College London, UCL Centre for Blockchain Technologies (UCL CBT), and the Amsterdam Center for Law and Economics (ACLE), University of Amsterdam Law School. E-mail: hossein.nabilou@uni.lu
The author is grateful to the 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 (15 November 2019) held in Luxembourg for their comments and feedback. All errors are those of the author.

Introduction

In November 2018, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) - a financial market infrastructure (FMI) institution that provides secure messaging for international payments - suspended certain Iranian banks' access (including that of the Central Bank of Iran) to its messaging system. This step was seemingly taken to protect the stability and integrity of the global financial systems.[1] However, the reluctant tone of the announcement could hardly disguise the reality that SWIFT took such an action conceding to the US government push to expand the secondary sanctions on financial messaging services to the Central Bank of Iran. Although the US did not have jurisdiction over SWIFT, which is a cooperative company incorporated under the Belgian law and is owned and controlled by its shareholders (financial institutions), after months of intense negotiations about the US demands and irrespective of the dismay expressed by European officials, SWIFT had to acquiesce.[2] In making SWIFT to yield to US demands, the US government apparently went to such an extent as to threaten the SWIFT's twenty five board members (which include two US bankers from Citi Bank and JPMorgan) with visa bans and asset freezes, and its member banks with charges and fines.[3]

The intrusion of considerations beyond the scope of financial regulation in the operation and risks management of Financial Market Infrastructures (FMIs),[4] was of such proportions that triggered radical proposals for reforming and restructuring the international FMI institutions. The recent calls for establishing international payment rails independent of the US have shown the frustration with the hegemony of a single dominant player having formal (i.e., through extraterritorial application of its laws or through secondary sanctions) and informal dominance over international payment infrastructures.[5] For example, German foreign minister Heiko Maas proposed that Europe could create its own SWIFT rival based on the euro rather than the US dollar (USD).[6] More recently, speculations about Synthetic Hegemonic Currency (SHC),

---

[1] Michael Peel, "SWIFT to Comply with US Sanctions on Iran in Blow to EU," *Financial Times* November 5, 2018.; SWIFT, "Update: Iran Sanctions Agreement," (17 January 2016). This was not the first time that SWIFT cut access to the Central Bank of Iran (CBI). CBI's access was cut in 2012. *See* "Swift Instructed to Disconnect Sanctioned Iranian Banks Following Eu Council Decision," (15 March 2012).

[2] "Compliance: How Is Swift Governed?," (Undated).

[3] Katrina Manson, "Europe Steps up Drive to Exempt Swift from Iran Sanctions," *Financial Times* Octover 9, 2018.

[4] Klaus Löber, "Extraterritorial Application or Regulation in the Area of Financial Market Infrastructure: The Case for Cross-Border Cooperative Oversight," in *European Financial Infrastructure in the Face of New Challenges*, ed. Franklin Allen, et al. (San Domenico di Fiesole (FI): European University Institute (EUI), 2019), 54.

[5] Guy Chazan, "Germany Calls for Global Payments System Free of Us," *Financial Times*, August 21, 2018 August 21, 2018.; Yves Mersch, "Strengthening the European Financial Industry Amid Disruptive Global Challenges," *Speech by Yves Mersch, Member of the Executive Board of the ECB, at the European Institute of Financial Regulation (EIFR), Paris, 3 September 2018* (September 3, 2018).; JP Koning, "Monetary Exclusion," *American Institute for Economic Research* (July 26, 2018).
For the first practical steps taken at the EU level, *see* European Union External Action - European External Action Service, "Implementation of the Joint Comprehensive Plan of Action: Joint Ministerial Statement," news release, September 24, 2018, September 24, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/51036/implementation-joint-comprehensive-plan-action-joint-ministerial-statement_en.; *See also* Esfandyar Batmanghelidj and Axel Hellman, "Europe, Iran, and Economic Sovereignty: A New Banking Architecture in Response to Us Sanctions," (2018).

[6] Manson, "Europe Steps up Drive to Exempt Swift from Iran Sanctions."

which would be provided by the public sector through a network of central bank digital currencies (CBDCs),[7] could also be viewed as a mechanism that could - in the long run - lead to decentralization in a multipolar international monetary and financial system.[8] However, it is unlikely that a system, which is based on fiat money, issued and controlled by states, could stand tall against the pressures exerted by one or more groups of hegemonic governments.

These developments have also highlighted the need for a truly decentralized uncensorable FMI on which one or a group of coordinated actors could not exert arbitrary influence. Such a value proposition requires a settlement asset that is denationalized, decentralized (peer-to-peer), divisible, digital, and globally transferable, and that provides certain levels of anonymity to its users. Bitcoin, which is built upon an open-source protocol, a distributed tamper-resistant timestamped globally synchronized ledger, and embeds a native digital asset is an obvious candidate to play such a role, despite its shortcomings in terms of price volatility.[9] In spite of its currently predominant use as a speculative asset, Bitcoin and its underlying technology can be viewed as a new model for a parallel decentralized FMI (dFMI) for clearing and settling obligations in its unanchored native settlement asset (i.e., bitcoin). In addition to clearing and settling its native asset, Bitcoin can be used to transfer the title to tangible or intangible assets on top of the Bitcoin blockchain. This is made possible because Bitcoin's scripting language allows embedding metadata in bitcoin transactions. For example, colored coins allow for recording the creation, ownership, transfer, and tracking of extrinsic digital and physical assets other than bitcoin.[10]

Whether a parallel dFMI relying on a settlement asset other than fiat currencies can alleviate the issues of financial exclusion and payment censorship remains to be seen. In particular, because the reason that the US possesses disproportionate influence over payment infrastructures is not entirely due to the reserve currency status of the USD, which is predominantly used in international FMIs, but also it is because the US has a large and attractive economy the benefits of which are hard to forgo for market participants in the face of a threat of being cut out of the US markets.[11] But it seems that decentralized financial technologies (FinTech), in particular, their structural architecture, which is built upon decentralized or distributed,[12]

---

[7] For the notion, potential design features, and legal issues concerning CBDCs, *see* Hossein Nabilou, "Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies," *Journal of Banking Regulation* (2019).; Hossein Nabilou and André Prüm, "Central Banks and Regulation of Cryptocurrencies," *Review of Banking & Financial Law (forthcoming)* (2019).

[8] Mark Carney, "The Growing Challenges for Monetary Policy in the Current International Monetary and Financial System," (Jackson Hole Symposium 2019: Bnak of England, 23 August 2019).

[9] For potential shortcomings of Bitcoin businesses to be recognized as a payment institution in terms of compliance with the existing regulations, *see* Hossein Nabilou, "The Dark Side of Licensing Cryptocurrency Exchanges as Payment Institutions," *Law and Financial Markets Review* 13, no. 4 (2019).

[10] Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchian* (Sebastopol, CA: O'Reilly Media, Inc.,, 2017), 278.

[11] *See* Koning, "Monetary Exclusion."

[12] For the distinction between decentralized and distributed systems in the context of Bitcoin, *see* William J. Luther and Sean Stein Smith, "Is Bitcoin a Decentralized Payment Mechanism?," *SSRN Working Paper Series* (2020). Under his definition of

consensus-based and censorship-resistant mechanisms without relying on centralized third parties can help shield such infrastructures from undue political influence.

A reflection on the history of Bitcoin shows that censorship-resistance considerations was central to its creation.[13] Although censorship resistance in Bitcoin has been achieved through a combination of technological innovations hardcoded in the Bitcoin network, preserving and maintaining such properties ultimately depend on the participants' consensus (i.e., judgment and discretion) in the Bitcoin network. In other words, preserving and enhancing or otherwise dispensing and undermining the censorship-resistant property of Bitcoin relies on its governance, which encompasses the processes and procedures for effecting changes in the rules governing the Bitcoin network.[14]

This study has been motivated by the recent developments concerning the censorship of the international FMI institutions, which have highlighted the vulnerabilities in the governance of the conventional FMIs. It will explore the governance of Bitcoin in the shadow of its censorship-resistant property and will discuss whether its governance mechanisms have been successful in addressing Bitcoin governance crises. This paper proceeds as follows. *Firstly*, it briefly discusses the objectives of Bitcoin governance by highlighting the differences in the objectives pursued in Bitcoin governance from those pursued in other governance schemes. In so doing, it also briefly compares Bitcoin governance with the 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-parity 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: What is it and what is it for?

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

decentralization, Bitcoin is best described as a distributed system. This paper uses the terms *decentralized* and *distributed* interchangeably.

[13] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008).

[14] Such changes may include changes to the size of each block, the number of block rewards, and even smaller changes to unlock or enable new features in Bitcoin such as SegWit activation.

valid chain in a decentralized manner, i.e., the Proof-of-Work (PoW) Algorithm.[15] 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 the infrastructure, while bitcoin (i.e., the token) functions as a medium of exchange in the Bitcoin network. Following the convention in the computer science literature, throughout this paper uppercase-B Bitcoin refers to the network and lowercase-b bitcoin refers to the unit of account. Needless to say, this paper concerns with the governance of Bitcoin as a network or infrastructure.

Governance is a system that shapes coordination between various participants.[16] 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.[17] In the 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 (principals) and managers (agents).[18] 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 FMIs, and the broader market)."[19]

From the above-mentioned definitions of governance, one can surmise that issues relating to *control* takes the center stage in defining governance. The questions of control in corporations often arise when there is a need for change in ownership, business model, structure of the firm, or its 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 the law and regulations are external to the firm or organization.[20]

---

[15] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."; Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (Sebastopol, CA: O'Reilly Media, Inc.,, 2017), 2.

[16] Philipp Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations," *Forthcoming in: Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, Oxford University Press, 2019* (2018): 10.

[17] Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, "Principles for Financial Market Infrastructures," (Basel, Switzerland: Bank for International Settlements and International Organization of Securities Commissions, April 2012), 26.

[18] Eugene F. Fama and Michael C. Jensen, "Separation of Ownership and Control," *The Journal of Law and Economics* 26, no. 2 (1983).; Brian L. Connelly et al., "Ownership as a Form of Corporate Governance," *Journal of Management Studies* 47, no. 8 (2010).; Michael C. Jensen and William H. Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *Journal of Financial Economics* 3, no. 4 (1976).; In other words, governance refers to the dynamics of power and influence that shapes decision making within a firm and delineates the rights and responsibilities of various stakeholders towards the firm. *See* Ruth V. Aguilera and Gregory Jackson, "Comparative and International Corporate Governance," *The Academy of Management Annals* 4, no. 1 (2010): 489-90.; Ying-Ying Hsieh, Jean-Philippe (JP) Vergne, and Sha Wang, "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies," in *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, ed. Malcolm Campbell-Verduyn (New York: Routledge, 2018), 48.

[19] Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, "Principles for Financial Market Infrastructures," 26.

[20] 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* (Janauray 26, 2019).

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.[21] Those incidents were as follows:

1. Integer overflow incident (2010) involving an integer overflow bug that created 184,467 *billion* bitcoins: This bug was discovered on October 15, 2010 at the block 74,638. Once this bug 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.
2. An erroneous upgrade to Bitcoin protocol and its rollback by coordination between developers and miners:[22] On March 11, 2013, there was an erroneous upgrade to Bitcoin protocol that led to two sets of miners mining legacy protocol and the updated one 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 has been a successful double-spend. This incident caused bitcoin price to sink by one third. However, the fork was rolled back by 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,[23] and raised concerns not only about settlement finality, but also about Bitcoin governance and who decides about issues concerning upgrades, and how such critical issues should be managed in the future.
3. The epitome of the governance crisis in Bitcoin was the debate about Bitcoin scaling that reached its zenith in 2017 and led to extremely polarizing controversies in the Bitcoin community.[24] Two main camps emerged on this dividing issue; one supporting vertical scaling solutions or second-layer solutions,[25] the other camp supporting horizontal scaling solutions or increasing the block

[21] Aaron van Wirdum, "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol," *Bitcoin Magazine*Sept. 7, 2016.
[22] BitMEX Research, "A Complete History of Bitcoin's Consensus Forks," (28 December 2017).; Bank for International Settlements, "Cryptocurrencies: Looking Beyond the Hype," in *Annual Economic Report* (Basel2018), 102-03.
[23] Research, "A Complete History of Bitcoin's Consensus Forks."; Settlements, "Cryptocurrencies: Looking Beyond the Hype," 102-03. *See also* macbook-air, "A Successful Double Spent Us$10000 against Okpay This Morning," *Bitcoin Forum* (March 12, 2013). Available at: http://archive.is/64Rkj
[24] Bitcoin itself can be viewed as an invention that emerged to overcome social scalability problem in the first place. Although the discussion of this paper is limited to technological scalability, the problem of social scalability stands at the core of the scalability issues in Bitcoin. Indeed, the perceived inefficiencies in the PoW can be understood in the balance struck between social scalability and computational scalability. In the Bitcoin Blockchain the latter is sacrificed to improve the former. For more details, *see* Nick Szabo, "Money, Blockchains, and Social Scalability," *Unenumerated* (February 09, 2017).
[25] Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchian*, 300-21.

size.[26] Ultimately, the dispute was settled by hard-forking. This crisis raised questions about 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 of handling this bug[27] raised questions about transparency in Bitcoin governance, because the discovery of the bug was publicly disclosed only after the inflation bug was discovered by other non-core developers and after the news made it to the public.

It is asserted that the Bitcoin blockchain by design is a technology that embeds governance and makes the rules-based economic order possible.[28] In the same vein, it is argued that within public blockchains in general, cryptocurrencies enable the creation and execution of rule-based systems that harbinger new institutional forms of economic governance, amounting to a new form of rule-system for economic coordination besides firms, markets, clubs, commons and governments.[29] However, as the above-mentioned instances of Bitcoin crises demonstrate, on-chain governance mechanisms have proved to be insufficient for its long-term viability. In addition to a need for constant intervention for protocol maintenance and improvements by developers, human intervention in the Bitcoin's open or permissionless blockchain has proved that Bitcoin governance is not immune to human discretion[30] and that the code-as-law narrative, put forward by the early proponents of such innovations, is far from accurate. In addition, these developments have put forward a serious governance question about who controls the changes to the Bitcoin network and specifically to the protocol.[31] The current literature on Bitcoin governance is far from thorough in providing answers to such questions.[32] More importantly, as Bitcoin does not entirely rely on on-chain mechanisms

[26] Joseph Poon and Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (2016).; Aaron van Wirdum, "The History of Lightning: From Brainstorm to Beta," *Bitcoin Magazine* (4 April 2018).; Tom Elvis Jedusor, "Mimblewimble," (19 July 2016).; Aaron van Wirdum, "Mimblewimble: How a Stripped-Down Version of Bitcoin Could Improve Privacy, Fungibility and Scalability All at Once," *Bitcoin Magazine* (12 August 2016).

[27] *See* BitcoinCore (September 20, 2018), CVE-2018-17144 Full Disclosure (Notice), available at: https://bitcoincore.org/en/2018/09/20/notice/

[28] Sinclair Davidson, Primavera De Filippi, and Jason Potts, "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology," *SSRN Working Paper Series* (2016).

[29] "Economics of Blockchain," *SSRN Working Paper Series* (2016): 6-7.

[30] Research, "A Complete History of Bitcoin's Consensus Forks."; Bank for International Settlements, "Cryptocurrencies: Looking Beyond the Hype," in *Annual Economic Report* (Basel, SwitzerlandJune 2018), 102.; Aaron van Wirdum, "The Good, the Bad and the Ugly Details of One of Bitcoin's Nastiest Bugs Yet," *Bitcoin Magazine* (September 21, 2018).

[31] Although governance in dFMIs, can be in the form of on-chain governance, off-chain governance or a combination of both, most projects opt for a hybrid form of governance. Bitcoin has already embedded certain technical features, such as monetary policy, in its protocol. However, this does not mean that such rules are not subject to change. Therefore, Bitcoin governance, within the meaning of the governance adopted in this paper, remains to be off-chain.

[32] van Wirdum, "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol."; Matthew A. Zook and Joe Blankenship, "New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance," *Geoforum* 96 (2018).; Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge: Cambridge University Press, 2019).; Philipp Paech, "The Governance of Blockchain Financial Networks," *The Modern Law Review* 80, no. 6 (2017).; Primavera De Filippi and Benjamin Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," *Internet Policy Review* 5, no. 3 (2016).; Davidson, De Filippi, and Potts, "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology."; Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations."

to resolve governance issues, the censorship-resistant property of Bitcoin ultimately relies on its off-chain governance that eventually depend 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 is why the importance of governance framework cannot be overstated. Having said so, the next section studies the analogies made between Bitcoin governance, constitutional arrangements, corporate governance, and internet governance, and will show why there is a need for an idiosyncratic governance model for Bitcoin.

Bitcoin governance vs. constitutional, corporate, and internet governance

In the relatively nascent literature on Bitcoin governance, several analogies have been made between Bitcoin governance and the governance in other disciplines spanning from constitutional law (i.e., analogies to separation of powers and checks and balances systems),[33] 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 the 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 or 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 can be a miner or can have other Bitcoin related businesses. The same applies to other participants in the Bitcoin governance. As constitutional checks and balances system is heavily built on the idea of separation of powers, in the absence of such a separation, checks and balances system would at best be dysfunctional and at worst redundant. The second problem with such analogies is that there is no real representation or agency relationships 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.[34] Some studies have explicitly advocated the application of corporate governance standards to the governance in cryptocurrency ecosystems.[35] In contrast, other studies do not explicitly refer

[33] Buck Perley, "Crypto-Governance and the Dangers of Faction: Lessons from the 18th Century for Designing a Decentralized Future," *Medium* (October 27, 2017).; TwoBitIdiot, "Bitcoin's Constitutional Crisis & Why I Support the Uasf," ibid. (June 21, 2017).; Fred Ehrsam, "Blockchain Governance: Programming Our Future," ibid. (November 27, 2017).
[34] For an example of explicit application of the corporate governance principles to cryptocurrencies, *see* Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations."
[35] Ibid.

to corporate governance, however, their treatment of Bitcoin governance, conclusions and policy recommendations seem to be rooted in the corporate governance literature.[36] 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.[37] 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 function as market infrastructure.

However, a quick overview of the corporate governance literature would clearly demonstrate that the drawing parallels between corporate governance and Bitcoin governance is misleading. Since the seminal work of Berle and Means entitled *the modern corporation and private property*,[38] it is believed that the separation of ownership and control in large corporations results in the managerial autonomy, because diffuse 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 premise 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 in a way that most of the venues for opportunistic behavior are practically closed. In addition, Bitcoin has successfully decreased the role of intermediaries and gave 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,[39] a proposal that can have a significant impact on Bitcoin

[36] Angela Walch, "In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains," in *Regulating Blockchain: Techno-Social and Legal Challenges*, ed. Philipp Hacker, et al. (Oxford: Oxford University Press, Forthcoming 2019).;
[37] "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," *N.Y.U. Journal of Legislation & Public Policy* 18 (2015).
[38] Adolf A. Berle JR. and Gardiner C. Means, *The Modern Corporation and Private Property* (New York: The Macmillan Company, 1933).
[39] Walch, "In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains."; Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations."; Jack M. Balkin, "Information Fiduciaries and the First Amendment," *UC Davis Law Review* 49 (2016). For an different view, *see* Aaron van Wirdum, "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol," *BITCOINMAGAZINE*Sept. 7, 2016.; Jerry Brito and Peter van Valkenburgh, "Writing and Publishing Code Alone Cannot Be a Crime," *CoinCenter.org* (Octover 29, 2018).; Raina Haque et al., "Blockchain Development and Fiduciary Duty," *Stanford Journal of Blockchain Law & Policy* (2019).

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 (BIP) requires a 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, the developers are said to be one of the least powerful of major Bitcoin stakeholders.[40] 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.[41] 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 battle ground of two opposing forces: government-centric multilateral governance model as opposed to the private-sector-led multi-stakeholder governance model (or distributed governance model).[42] Indeed, the Bitcoin governance shares many common features with internet governance, in particular in that both governance models deal with the governance in relatively decentralized systems. This indeed makes internet governance the closest model that can be followed in studying 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 its especially similar to Bitcoin governance. In this sense, Bitcoin governance has already benefited from the governance mechanisms 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.[43]

---

[40] Jeffery Atik and George Gerro, "Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice," ibid. (2018): 7.
[41] De Filippi and Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure."; Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Massachusetts: Harvard University Press, 2018).
[42] Global Commission on Internet Governance, "Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance," (Waterloo, Ontario; London: Centre for International Governance Innovation and the Royal Institute of International Affairs, 2017), 2-4.
[43] In the same vein, the analogies to internet can be useful in analyzing certain aspects of Bitcoin governance, such as the analogy made of Bitcoin layers to the layers of the internet. *See* De Filippi and Wright, *Blockchain and the Law: The Rule of Code*.;

However, as it is well known, the promise of decentralization in 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 the center stage in its governance.

In addition to the decentralized aspect 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* with various innovations in Bitcoin. In particular, embedding the digitally scarce native asset is one such innovation that motivates the 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.[44] Embedding such incentive-compatible mechanisms in the design of the Bitcoin network mitigates the concerns about positive externalities, or 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 the active role for participants in Bitcoin governance differentiate the governance model of Bitcoin from that of the internet.

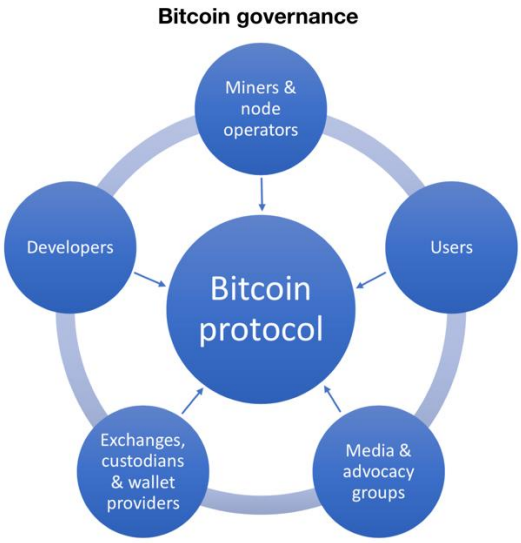
To summarize, in spite of the similarities to constitutional, corporate and internet governance, Bitcoin possesses features that differentiate it from all those three governance models. Therefore, as much as enlightening such analogies are, they remain misleading to varying degrees. By highlighting the 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.

Lombrozo, BIP 123. https://github.com/bitcoin/bips/blob/master/bip-0123.mediawiki; Aaron van Wirdum, "Why Some Changes to Bitcoin Require Consensus: Bitcoin's 4 Layers," *Bitcoin Magazine* (February 26, 2016). By slicing the Bitcoin network to many layers similar to that of the internet, this provides an analytical view for 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 based on such an analogy. For more details on the indirect regulation of Bitcoin, *See* Hossein Nabilou, "How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency," *International Journal of Law and Information Technology* (2019).

[44] 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* (February 20, 2020). In addition, the fact that selling freshly minted bitcoins (block rewards) by miners require 100 confirmations, also provide another incentive-compatible mechanism for securing the system against the miners misbehavior and spending the coins on orphaned blocks.

Towards an idiosyncratic governance model for Bitcoin

Economic organizations have various actors, stakeholders or constituents, each with oft-divergent interests. Aside from shareholder value maximization, one of the main objectives of corporate governance is to create an institutional or otherwise streamlined framework for resolution of disputes stemming from those conflicting interests inside an ecosystem, organization or network. In conventional corporate governance, there are internal actors including owners (shareholders), managers, and the board members, and external actors or constituents such as customers, the media, government, and the broader community.[45] In Bitcoin governance, it is equally important to discern who the main stakeholders of Bitcoin network are and what Bitcoin can uniquely offer to maximize their payoffs. In the Bitcoin ecosystem, various actors such as mining pools, node operators, users, developers, exchanges, custodians and wallet providers, and eventually the media and advocacy groups have their say and they ultimately decide over critical governance issues either by reaching a consensus or by forking. It appears that it is the very unique value proposition of Bitcoin as censorship-resistant store of value and value transfer infrastructure that is likely to maximize value for all Bitcoin stakeholders. This paper analyzes Bitcoin governance in light of this unique value proposition.



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. For example, bank governance is often deemed different from the governance of other financial and non-financial institutions due to the idiosyncrasies in banking.[46] Similarly, the governance of dFMIs

[45] Hsieh, Vergne, and Wang, "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies," 51.

[46] John Armour, "Bank Governance," in *The Oxford Handbook of Corporate Law and Governance*, ed. Jeffrey Gordon and Wolf-George Ringe (Oxford: Oxford University Press, 2015).; Klaus J. Hopt, "Corporate Governance of Banks after the Financial Crisis," in *Financial Regulation and Supervision: A Post-Crisis Analysis*, ed. Eddy Wymeersch, Klaus J. Hopt, and Guido Ferrarini (Oxford: Oxford University Press, 2012).; Jakob de Haan and Razvan Vlahu, "Coroporate Governance of Banks: A Survery,"

should be different from the governance models of conventional centralized businesses and organizational structures, mainly due to their decentralization.[47] Given the importance of certain firms such as those providing conventional FMI services, a formal governance framework is mandatory 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 are also suitable for Bitcoin as a dFMI.

In this regard, it is important to make a distinction between permissioned and permissionless blockchains. The governance of a permissioned network, though has its unique challenges, can be straightforward and could be similar to the governance of conventional FMIs, mainly because their value proposition is very similar to that of conventional businesses, and more impotently because there is no need for minimizing trust by relying on decentralized technologies. However, the governance in permissionless decentralized networks can be extremely challenging mainly due to their unique value proposition. In addition, thanks to their decentralization, no entity could be identified to have a meaningful control on the network so 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 on 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. In 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 for legitimate or illegitimate reasons.

Censorship resistance as the unique value proposition of Bitcoin is very much reflected in the Bitcoin whitepaper[48] as well as Satoshi Nakamoto's communications with early bitcoin adopters. Given the fate of Bitcoin's predecessors such as Digicash and American Liberty Dollar (ALD),[49] 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 Bitcoin's

Journal of Economic Surveys 30, no. 2 (2016).; Kern Alexander, "Bank Corporate Governance: Law and Regulation," in *Principles of Banking Regulation* (Cambridge: Cambridge University Press, 2019), 128.

[47] For an attempt to apply the traditional corporate governance to the cryptocurrencies and blockchain-based technologies, *see* Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations."

[48] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

[49] Aaron van Wirdum, "The Genesis Files: How David Chaum's Ecash Spawned a Cypherpunk Dream," *Bitcoin Magazine* (24 April 2018).; "The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It," *Bitcoin Magazine* (15 June 2018).; Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (New York: Portfolio/Penguin, 2017).

ancestors. This is also clear from the chronology of the technological breakthroughs that led to the birth of Bitcoin.[50]

More importantly, censorship-resistant property of Bitcoin is reflected 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 violate the rules of the Bitcoin protocol, modify the ledger arbitrarily or censor other stakeholders from participating in the Bitcoin network. Such a tradeoff has been made because the unique value proposition of Bitcoin and blockchain technology is not to replicate the functions of centralized technologies in a faster or cheaper fashion. Indeed, as blockchain technology is one of the least efficient technologies for payments and data storage, and as virtually everything that can be done on blockchain can also be performed on a network that uses a client-server or master-slave architecture, the very use of blockchain technology creates inefficiencies that are absent in centralized systems.[51] As the client-server architecture uses a centralized coordination mechanism, it is much faster, cheaper and efficient than the systems relying on blockchain technology. However, blockchain technology can be suitable for use-cases such as creating an asset that would give its owner near-full control so that she could hold and transact with the asset using a secure and trust-minimized network.[52] In this perspective, the objective of becoming a fast and efficient global settlement layer is secondary and should yield when conflicted with the objective of censorship resistance.

It is indeed hard not to notice that the censorship-resistant property of Bitcoin drives the entire mechanism designs embedded in the Bitcoin network. Since Bitcoin is designed to operate outside the legal framework (i.e., alegality), 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.[53]

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

[50] Arvind Narayanan and Jeremy Clark, "Bitcoin's Academic Pedigree," *Communications of the ACM* 60, no. 12 (2017).
[51] Szabo, "Money, Blockchains, and Social Scalability."; *See also* Gabriel Shapiro, "Tokenizing Corporate Capital Stock," *ZERO_LAW* (October 28, 2018).
[52] "Tokenizing Corporate Capital Stock."
[53] De Filippi and Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," 5-6.

and payment institutions, without its censorship-resistant property, Bitcoin would be redundant.[54] 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. As protecting censorship resistance would entail a decent amount of decentralization, to make the system resilient against the attacks aimed at the central point of failure, decentralization and censorship-resistant property go hand in hand and should be given equal weight in Bitcoin governance. Having said so, the ultimate goal of Bitcoin governance should be retaining its censorship-resistant property through boosting its decentralization.

Not only does decentralization makes Bitcoin censorship resistant, but also it ensures that Bitcoin's other important features, including bitcoin issuance or emission rate, cannot be easily manipulated by one or coordinated groups of related parties. If for example, bitcoin issuance would have been subject to change by a few players who could be able to coordinate easily, it would have been unlikely for Bitcoin to retain the value that it has retained so far. As my coauthor and I have argued elsewhere, partly due to decentralized architecture of Bitcoin, which begets potential endogenous information insensitivity, Bitcoin has a good shot at becoming a safe asset.[55] Gaining such a status ultimately depends on the governance of Bitcoin. Meaning that if the governance of Bitcoin makes it malleable to changes that can be easily incorporated into the Bitcoin protocol and allows for information asymmetries, Bitcoin would lose its potential to become endogenously information insensitive.

This paper is written under the assumption that for the foreseeable future, Bitcoin will continue its role as a niche medium of exchange and dFMI. Under this assumption, the greatest value proposition of Bitcoin would be its censorship-resistant property. Therefore, the efficiency and effectiveness of governance arrangements in Bitcoin should be tested against this important criterion. This acknowledgement will constitute a point of departure from the governance models in other types of organizations in that Bitcoin governance should lean towards protecting that censorship resistance even at the expense of creating inefficiencies for other perceived use-cases of Bitcoin. This assumption, in turn, means that the application of the stringent governance standards as applied to conventional organizations and FMIs to Bitcoin is misguided, not only because the application of the centralized governance models to decentralized models can be counterproductive, but also because for a censorship resistant network to remain so, it needs to be regulation-resistant too. In this sense, it appears that the external regulation by governments of the

[54] 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* (January 26, 2019).
[55] Hossein Nabilou and André Prüm, "Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies," *Journal of Financial Regulation* 5, no. 1 (2019).; *See also* David Andolfatto, "Is Bitcoin a Safe Asset?," *MacroMania* (March 27, 2016).

governance of the Bitcoin protocol, even if feasible, is likely to undermine Bitcoin's core value proposition.[56]

Having said so, the question on the failure or the 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 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?

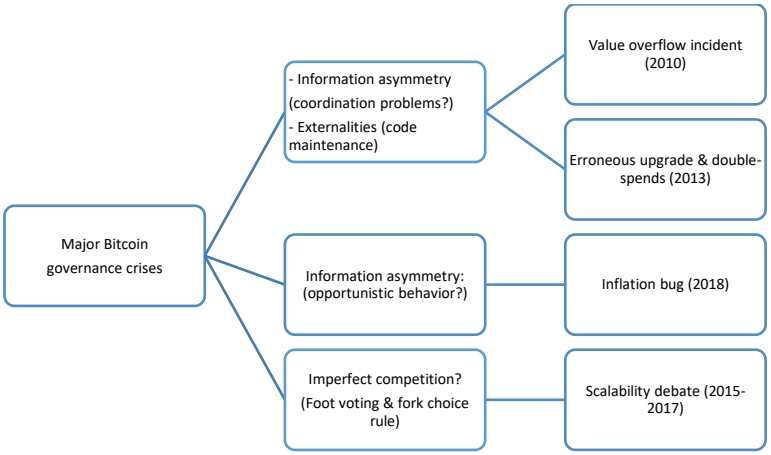
Various governance crises in Bitcoin thus far have highlighted the role of governance and its importance in the Bitcoin ecosystem. One of these crises was the famous scaling crisis that led certain well-known figures in the cryptocurrency ecosystem to declare that Bitcoin governance is broken, and that Bitcoin project should be liquidated.[57] Despite those protestations and doomsday predictions, the Bitcoin network has continued to grow. However, the legitimate question remains to be 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 gives rise to agency costs and coordination problems. The rest of this paper is to identify 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).

[56] Jameson Lopp, "Nobody Understands Bitcoin (and That's Ok)," *Coindesk* (March 11, 2017).; to Cypherpunk Cogitations: Jameson Lopp's thoughts on Bitcoin, Privacy, and Freedom, 2018, https://blog.lopp.net/who-controls-bitcoin-core-/
[57] Mike Hearn, "The Resolution of the Bitcoin Experiment," *Medium* (January 14, 2016).

Three such crises highlight the coordination problems arising from imperfect information (i.e., information asymmetry) in the maintenance of the code and dealing with the bugs. Such crises include the value overflow incident (2010), an erroneous upgrade and double spends (2013), and the inflation bug (2018). The first two of these incidents highlight the coordination problems in the maintenance of the code, whereas the latter put the spotlight on the potential opportunistic behavior that such information asymmetries would give rise to in the relationship between developers and users (and even miners). The third most important issue giving rise to market failures originate from the problems associated with imperfect competition. The fourth major Bitcoin crisis (i.e., 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.[58] 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, the potential opportunistic behavior is studied first and then the coordination problems will be investigated.



Agency costs and opportunistic behavior in Bitcoin governance

One of the main objectives of the 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

[58] George A. Akerlof, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics* 84, no. 3 (1970).

opportunistic behavior such as looting[59] by managers. The early literature has recognized this problem by focusing on the separation of ownership and control and highlighting that the diffuse share ownership would eventually lead to managerial autonomy.[60] To mitigate the agency costs, the principals often use various mechanisms. Central to such mechanisms are the board of directors to monitor the performance of those who are in control (management).[61] 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 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 its legal and economic sense) do not exist between various participants in the Bitcoin network, the 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,[62] 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.[63] 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.[64] 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 the human discretion to the periphery.[65]

Secondly, since the Bitcoin network is highly transparent about its protocol, blockchain and methods of effecting a change in the protocol, it is hard to establish a clear-cut informational asymmetry between various participants in the network. Such a difficulty is exacerbated by the problem that various participants

[59] George A. Akerlof et al., "Looting: The Economic Underworld of Bankruptcy for Profit," *Brookings Papers on Economic Activity* 1993, no. 2 (1993).
[60] Berle JR. and Means, *The Modern Corporation and Private Property*.; John Armour and Jeffrey N Gordon, "The Berle-Means Corporation in the 21st Century," (2009).; Brian R Cheffins, "The Rise and Fall (?) of the Bearle-Means Corporation," *Seattle University Law Reveiw* 42 (2018).
[61] However, the management has wielded considerable influence on the board members making such monitoring ineffective. The increasing emphasis on the use of independent board members has been a response to such unfettered influence.
[62] For more details on such duties, *see* Balkin, "Information Fiduciaries and the First Amendment."
[63] Davidson, De Filippi, and Potts, "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology."; Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, 2016).
[64] Szabo, "Money, Blockchains, and Social Scalability."
[65] Hsieh, Vergne, and Wang, "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies," 51.; Vitalik Buterin, "Daos, Dacs, Das and More: An Incomplete Terminology Guide," *Ethereum Blog* (May 6, 2014).

in the network can assume different roles. For example, a developer can simultaneously be a user and/or can be employed by a mining company or other Bitcoin businesses. Furthermore, she can operate a fully validating node or can run her own Bitcoin business. This muddies the traditional information asymmetry framework in conventional organizations 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, as my coauthor and I have argued elsewhere,[66] 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. To be clear, this does not mean that there is complete information, but there is no *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, may have some inside information that would create information asymmetry. Although information asymmetries might exist outside the technical environment of the Bitcoin network and in the allegedly closed circles of a few prominent participants such as miners, developers and investors,[67] 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.[68]

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 has 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, the 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.

---

[66] Nabilou and Prüm, "Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies."

[67] Hsieh, Vergne, and Wang, "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies."

[68] 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., "Blockchain Development and Fiduciary Duty," 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, in particular in times of crises. *First*, the developers are dispersed and relatively decentralized, the coordination for fixing bugs and adding patches can take substantial amount of time. Due to this operational risk, the very existence of Bitcoin could be put at risk. *Second*, the 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 her holdings and only afterwards investigating into the nature of the piece of information hidden from her.

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 is exercised at a different level (off-chain), remains to be 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.[69] 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 BIP, which is a standardized process for proposing, testing and peer review of the new proposals for effecting changes to the protocol, are established.[70] The latter procedure is to ensure that innovation is not hindered while the improvements are implemented through consensus and collaboration.

[69] De Filippi and Wright, *Blockchain and the Law: The Rule of Code*.

[70] In addition, there are several mechanisms that are hardcoded to the bitcoin network to reduce or eliminate coordination problems. For example, the programmability of Bitcoin allows several other mechanisms to be embedded into the transactions that could function as a signal by Bitcoin network participants such as miners in crucial decision-making processes (i.e., miner signaling). In this regard, BIP 9 has been introduced to function as a signaling mechanism that allows miners to indicate whether they are ready

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 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 his turn, enlisted four other developers,[71] 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 that 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 has the commit access to the code base.[72]

Having only a few Core Devs with commit access to the code would give the impression of significant centralization. However, these Core Devs are not unconstrained and the changes to the code follows a process of rough consensus that determines what proposed changes to be merged in the protocol.[73] 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.[74]

Such a 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 highjack the brand name of Bitcoin (core). However, those powers are again constrained by at least two factors. *First*, the fact that Bitcoin developers are not a homogenous pool of developers, which makes it unlikely for them to highjack the project. *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 maintainers.[75] 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.

In closing this section, it is important to note that the difficulty in the coordination in Bitcoin should not always be viewed as a negative feature. A truly decentralized cryptocurrency network will inevitably face

to implement a particular change. Some BIPs require the signaling of a super majority of miners to be activated. *See* Atik and Gerro, "Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice," 4.

[71] These core maintainers include Pieter Wuille, Wladimir van der Laan, Gregory Maxwell, and Jeff Garzik.

[72] SFOX, "Bitcoin Governance: What Are Bips and How Do They Work?," *Medium* (April 16, 2019).

[73] See Contributing to Bitcoin Core, GitHub, available at: https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md

[74] SFOX, "Bitcoin Governance: What Are Bips and How Do They Work?."

[75] Ibid.; *See also* Lopp Who Controls Bitcoin Core?; "Nobody Understands Bitcoin (and That's Ok)."

certain levels of disagreements at every level of coordination. Therefore, slow and laggard nature of decision-making and resolving disputes in a decentralized fashion should not be viewed as a problem for a decentralized network, unless where there is a critical issue that poses an existential threat to the network. A parallel can be made between the evolution of dispute resolution mechanisms in the common law countries through a network of distributed courts as opposed to contriving dispute resolution methods through codification across the board. In the former, although the emergence of standards can take decades or ages, giving the impression of inefficiency, the ultimate outcome often benefits from the dispersed knowledge and experience of the vast number of participants and only afterwards becomes the law, which is likely to last for decades or centuries. In contrast, codification either dictates the law or codifies the preferences of limited number of participants into the law, which may entail the creation of economic rents. It seems that the first approach, despite being slow, is more sustainable. By the same token, dispute resolution in Bitcoin would benefit from the slow process of deliberation that distills the decentralized knowledge dispersed among various economic participants to overcome the Hayekian knowledge problem.[76] This may eventually turn the threat of coordination problem to an opportunity for long-term sustainability of decision making and governance for the Bitcoin network. In this sense, it seems that there would be a last-mover advantage in Bitcoin governance, which seems particularly true where there is a need for tweaking the protocol layer rather than higher levels of the Bitcoin network.

The impact of competition on Bitcoin governance

Zooming 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 reimplements the codebase).[77] These competitive forces may best be classified as internal and external competition. Internal competition refers to the ability of each individual to fork Bitcoin's codebase and blockchain and create her 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

[76] F. A. Hayek, "The Use of Knowledge in Society," *The American Economic Review* 35, no. 4 (1945).
[77] Bitmex Research, "Competing with Bitcoin Core," (2018).

paralyzed by extensive regulatory requirements,[78] Bitcoin faces a cut-throat competition in a market for cryptocurrencies without any entry or exit restrictions and no regulatory barriers to competition.[79]

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 lower amount of hash rate than its competing chain, it would take longer for it to reach the 2016 block cycle for the readjustment of the mining difficulty.[80] However, the chain with 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 most accumulated PoW. The second way to solve the hard fork is for the users/full nodes to decide to follow the chain having the lower amount of accumulated PoW. This may render the chain with higher PoW irrelevant. The third method of resolving the hard fork is that two independent networks would 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 the last resort* in the Bitcoin ecosystem.

An extraordinary example of resolving disputes through hard forks in the Bitcoin ecosystem occurred in 2017 that came to be known as scaling crisis of 2017.[81] Bitcoin's block size limit is set at one megabyte by

[78] For the regulatory limitations imposed on the corporate takeover of banks in the EU, *see* Georgina Tsagas, "The Market for Coporate Control in the Banking Industry," in *The Law on Corporate Governance in Banks*, ed. Iris H-Y Chiu and Michael McKee (Cheltenham, UK: Edward Elgar Publishing Limited, 2015).

[79] Lawrence H. White, "The Market for Cryptocurrencies," *CATO Journal* 35, no. 2 (2015).; In addition to such competition, the second dimension of competition that contributes to the healthy level of governance is the competition among each category of participants in the Bitcoin network. For example, miners competing for the block reward and fees, despite being resource intensive, provides a strong security for Bitcoin network. In addition, there is competition among users for block space. In the future, where there would be no block reward to be distributed to the miners, such competition would be essential for the security model of Bitcoin as it would incentivize miners to divert substantial resources to mining bitcoin and, hence securing the network. At this stage, where the transaction fees play a less important role on the security model of Bitcoin, the participation of the majority of users remains passive. This may be attributed to rational ignorance or user apathy, similar to the well-known phenomenon in the voting systems, which would result in citizens not participating in elections.

[80] For more technical details, see: Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 253.

[81] Bitcoin itself can be viewed as an invention that emerged to overcome social scalability problem in the first place. Although the discussion of this paper is limited to technological scalability, the problem of social scalability stands at the core of the scalability issues in bitcoin. Indeed, the perceived inefficiencies in the PoW can be understood in the balance struck between social scalability and computational scalability. In the Bitcoin Blockchain the latter is sacrificed to improve the former. For more details, see: Szabo, "Money, Blockchains, and Social Scalability."

Satoshi Nakamoto in 2010 using a soft fork.[82] As the demand for using Bitcoin increased, so did the competition for block space on the Bitcoin blockchain and consequently the blocks were nearing their full capacity. This higher demand for block space sharply increased transaction fees in the Bitcoin network, which priced out many earlier use cases of Bitcoin, especially those involving micropayments. Such a development increased the demand for increasing the block size, in particular from the Bitcoin business community.

Various proposals were put forward for resolving the problem, ranging from increasing the block size from one megabyte to 2 megabytes or even to 8 megabytes to having a dynamic block size limit for Bitcoin. The first of such proposals were put forward in August 15, 2015 by the introduction of Bitcoin XT that was released by Gavin Andresen and Mike Hearn as a soft fork that could be turned into a hard fork down the road. This marked the beginning of a protracted dispute within the Bitcoin community. The opponents, such as Gregory Maxwell and Nick Szabo, argued that increasing the block size would lead to centralization, security risks, and variable and delayed confirmation times. Two main camps emerged on this dividing issue; one supporting vertical scaling solutions or second-layer solutions,[83] the other camp supporting horizontal scaling solutions or increasing the block size.[84] There has been various allegation of censorship by Bitcoin XT supporters claiming that Bitcoin core team had censored them. After much debate, Hearn resigned,[85] and Bitcoin XT had eventually been abandoned. Later projects were launched to increase the block size, such as Bitcoin Unlimited, Bitcoin Classic, and BitPay Core with very limited success. Some intermediate proposals, such as SegWit2X, were put forward, but failed to gather momentum. The protracted *civil war* within the Bitcoin community eventually resulted in the failed SegWit2X, and a hard fork leading to the creation of bitcoin cash (BCH) and subsequent user-activated soft fork (UASF) and the activation of SegWit on the legacy chain.[86]

Scholars have argued that this governance crisis and failure in conflict resolution amount to a fragile decision-making mechanism within the Bitcoin network.[87] However, with the benefit of hindsight and the

---

[82] *See* Eric Lombrozo, "Forks, Signaling, and Activation," *Medium* (June 18, 2017).; *See also* https://github.com/bitcoin/bitcoin/commit/f1e1fb4bdef878c8fc1564fa418d44e7541a7e83#diff-118fcbaaba162ba17933c7893247df3aR1422

[83] Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchian*, 300-21.

[84] Poon and Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments."; Wirdum, "The History of Lightning: From Brainstorm to Beta."; Jedusor, "Mimblewimble."; Wirdum, "Mimblewimble: How a Stripped-Down Version of Bitcoin Could Improve Privacy, Fungibility and Scalability All at Once."

[85] Hearn, "The Resolution of the Bitcoin Experiment."

[86] Laura Shin, "Will This Battle for the Soul of Bitcoin Destroy It?," *Forbes*Oct. 23, 2017. Similar controversies happened on the Ethereum's blockchain due to the loss of funds associated with DAO project, resulting in a chain split and the creation of Ethereum and Ethereum Classic. *See* Quinn DuPont, "Experiments in Algorithmic Governance: A History and Ethnography of "the Dao," a Failed Decentralized Autonomous Organization," in *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, ed. Malcolm Campbell-Verduyn (New York: Routledge, 2018).; Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The Dao," (Washington, DCJuly 25, 2017).

[87] De Filippi and Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," 9.

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 in fact have contributed to its long-term goal of establishing such an image of Bitcoin as a censorship-resistant network.

In addition to role of the above-mentioned 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 to 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 store of value such as gold. Such competitive forces have indeed huge implications for Bitcoin's governance and pushes Bitcoin to continuously improve itself to stay relevant.[88]

Externalities and public goods nature of Bitcoin governance

Although there is no general agreement on whether the law and governance belong to the category of public goods,[89] governance exhibits many properties of public goods in so far as it is non-excludible and non-rivalrous. In the same vein, to the extend it is non-excludible, and non-rivalrous,[90] Bitcoin governance possess the properties of public goods. 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 the use by one participant, does not decrease such benefits to other participants, Bitcoin network participants face the 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 the Bitcoin governance may be due to classic commons property of Bitcoin governance. The permissionless nature of Bitcoin means that no one can be excluded from either participating in the Bitcoin governance or from consuming the benefits of good governance in Bitcoin, however, as the use of block space by one user

[88] However, one would expect that an easy exit enabled by both internal and external competitive forces in Bitcoin governance would lead to the tendency of having less voice being raised by stakeholders in Bitcoin, as evidenced by some prominent Bitcoin developers leaving the project rather than staying and engaging in the long-term development of the project. For an excellent backgrounder, see Albert O. Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Cambridge, Massachusetts: Harvard University Press, 1970).; Atik and Gerro, "Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice."

[89] *See* Tyler Cowen, "Law as a Public Good: The Economics of Anarchy," *Economics and Philosophy* 8, no. 02 (1992).; David D. Friedman, "Law as a Private Good: A Response to Tyler Cowen on the Economics of Anarchy," ibid.10, no. 2 (1994).

[90] Commons are goods that are non-excludible in the sense that others cannot be excluded from its consumption, but they are rivalrous, meaning that its consumption by one individual will decrease its availability for others. In contrast, public goods are both non-excludible and non-rivalrous.

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,[91] and the overuse of the common resource often leads to the tragedy of the commons and its eventual depletion.

The market failures due to the commons nature of Bitcoin especially applies to 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 incentive mechanisms embedded in the Bitcoin network have incentivized participants to contribute to Bitcoin governance and to the maintenance of the code. For 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.[92] 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 are likely to emerge.

Despite the fact that Bitcoin governance is prone to the free-rider problem, thus far, its governance proved to be both effective and relatively successful. This is puzzling as insights from the economic literature, such as public goods, club goods,[93] the tragedy of the commons,[94] and game theory[95] suggest that free-rider problems would result in a failed and broken governance model in Bitcoin. Perhaps the solution to this puzzle should be found 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

[91] The term "tragedy of the commons" coined by Garret Hardin in his famous article in 1968 indicates a source shared by a group of people, in which individuals are granted the right to use that given resource without any cost-efficient way of monitoring or limiting each other's use. This will lead to the depletion of that resource. *See* Garrett Hardin, "The Tragedy of the Commons," *Science* 162, no. 3859 (1968).; Charlotte Hess and Elinor Ostrom, *Understanding Knowledge as a Commons: From Theory to Practice* (Cambridge, Massachusetts: MIT Press, 2007), 4.

[92] Jiang Zhuoer, "Infrastructure Funding Plan for Bitcoin Cash," *Medium* (January 22, 2020).

[93] Richard Cornes and Todd Sandler, "The Theory of Externalities, Club Goods, and Public Goods," (Cambridge: Cambridge University Press, 1996).

[94] Hardin, "The Tragedy of the Commons."; Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (New York: Cambridge university press, 1990).; "Coping with the Tragedies of the Commons," *Annual Review of Political Science* 2, no. 1 (1999).; Franciesco Parisi and Ben Depoorter, "Commons and Anticommons," in *The Encyclopedia of Public Choice*, ed. Charles K. Rowley and Friedrich Schneider (Boston, MA: Springer US, 2004).; Francesco Parisi, Norbert Schulz, and Ben Depoorter, "Simultaneous and Sequential Anticommons," *European Journal of Law and Economics* 17, no. 2 (2004).

[95] Stephen Morris and Hyun Song Shin, "Global Games: Theory and Applications," in *Advances in Economics and Econometrics: Theory and Applications, Eighth World Congress*, ed. Lars Peter Hansen, Mathias Dewatripont, and Stephen J. Turnovsky, Econometric Society Monographs (Cambridge: Cambridge University Press, 2003).; Joseph Abadi and Markus Brunnermeier, "Blockchain Economics," *National Bureau of Economic Research Working Paper 25407* (2018).

resource, 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 been emerged to address the issue.[96] 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 in the internet (e.g., Wikipedia), some scholars suggest that the 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.[97] Yet another way to explain the success of the Bitcoin community in maintaining the code and resolution of disputes without any resort to external factors or third parties is by reference to the literature on *law without order* that highlights the insignificance of the law and formal mechanisms in social coordination and dispute resolution, and instead puts the spotlight on the importance of unwritten social norms.[98] Irrespective of the reasons, Bitcoin seems to be like the proverbial Bumblebee that in theory it would not fly, but in practice it does.[99] The above mentioned three non-mainstream theories may be helpful in shedding some light on how Bitcoin governance and several other phenomena that rely on the cooperation and collaboration in distributed systems work and manage 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 the first blush, Bitcoin governance seems to be ambivalent about the concept of legitimacy, this paper argues that legitimacy in Bitcoin governance stems from its downward or market accountability,[100] meaning that the users are afforded with the mechanisms that enable them to exert a significant influence on Bitcoin governance. Among others, users may employ a variety of mechanisms to participate in the governance of the network. *Firstly*, users may threaten not to run the software proposed by developers. *Secondly*, those

[96] Ostrom, "Coping with the Tragedies of the Commons."; *Governing the Commons: The Evolution of Institutions for Collective Action*.; "Beyond Markets and States: Polycentric Governance of Complex Economic Systems," *The American Economic Review* 100, no. 3 (2010).
[97] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006).
[98] Robert C. Ellickson, *Order without Law: How Neighbors Settle Disputes* (Cambridge, Massachusetts: Harvard University Press, 1991).
[99] This metaphor is expressed by the former president of the European Central Bank (ECB) about the euro. *See* Mario Draghi, "Speech by Mario Draghi, President of the European Central Bank at the Global Investment Conference in London 26 July 2012," (2012).
[100] Colin Scott, "Accountability in the Regulatory State," *Journal of Law and Society* 27, no. 1 (2000).; "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*, ed. Jacint Jordana and David Levi-Faur (Northampton, Massachusetts: Edward Elgar Publishing, Inc., 2004).

users running fully validating nodes may threaten not to validate certain blocks broadcast by miners. *Thirdly*, users may vote with their feet.

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 it is 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.[101]

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 that are ultimately enforced by the users running full nodes.[102] 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, who take on the role of watchdogs, constantly watch miners for their compliance with Bitcoin's consensus rules.[103]

Although miners may use the threat of forks (Miner Activated Soft Forks (MASFs) or hard forks) or they 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 who 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 the users as well as some segments of the business community by advocating a soft fork implementation of Segregated

[101] Given the roles of other stakeholders such as miners and developers, this renders Bitcoin governance to a strong governance framework for dFMIs similar to what is sometimes dubbed as polycentric or networked governance framework in conventional governance studies. For the concept of polycentric governance model, *see* David Zaring, "Financial Regulation's Overlooked Networks," in *Reconceptualising Global Finance and Its Regulation*, ed. Ross P. Buckley, Emilios Avgouleas, and Douglas W. Arner (New York: Cambridge University Press, 2016); "International Law by Other Means: The Twilight Existence of International Financial Regulatory Organizations," *Texas International Law Journal* 33 (1998). Anne-Marie Slaughter, *A New World Order* (Princeton, New Jeresey: Princeton University Press, 2004).; "Global Government Networks, Global Information Agencies, and Disaggregated Democracy," *Michigan Journal of International Law* 24 (2003).; Finck, *Blockchain Regulation and Governance in Europe*, 172-78.

[102] Although users' contribution to Bitcoin governance could be hampered by collective action problems, the technological means, which are embedded in the Bitcoin network, such as the ability to signal one's preferences via the network itself, would help alleviate coordination problems.

[103] ecurrencyhodler, "Bitcoin Governance," *Medium* (February 5, 2019).

Witness (SegWit), in which both SegWit and non-SegWit compliant blocks could be processed.[104] 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 the SegWit after a specific date. If this situation would have dragged on, that soft fork would have been 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 the miners to stop resisting the SegWit update and acquiesce to the users' intended result.[105] The same applies to the powers of developers who can propose software rule changes. If changes proposed or even implemented by developers would not be supported by significant number of users, those changes are eventually doomed.

The 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 the users were perceived to be parties to.[106] 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.[107] Similarly, in 2013 inflation bug incidents, where the 0.7/0.8 consensus bug split the blockchain into two separate chains for several hours.[108] 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.[109]

Ultimately, the key takeaway in Bitcoin governance is that users are not bound to follow the miners or developers if a majority of the users do not share the same ideas about the future path of the network. In addition, if there is a disagreement over how to maximize network utility, users can suspend Nakamoto consensus and *disempower* miners.[110] This also applies to any attacker to the network, as the users may stop following the chain with the most accumulated PoW, the attacker must take this into account before spending resources on attacking the Bitcoin network.[111]

---

[104] Aaron van Wirdum, "The Latest Twist to the Block Size Debate Is Called a "Uasf"," *Bitcoin Magazine* (March 2, 2017).
[105] Atik and Gerro, "Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice," 7. *See also* Alyssa Hertig, "Uasf Revisited: Will Bitcoin's User Revolt Leave a Lasting Legacy?," *Coindesk* (August 3, 2017).
[106] Hasu, James Prestwich, and Brandon Curtis to Uncommoncore, 15 October, 2019, https://uncommoncore.co/research-paper-a-model-for-bitcoins-security-and-the-declining-block-subsidy/.
[107] Charlie Shrem, "Bitcoin's Biggest Hack in History: 184.4 Billion Bitcoin from Thin Air," *Hackernoon* (January 11, 2019).
[108] This incident related to the 0.8 update to the Bitcoind, 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. For more details, *see* Vitalik Buterin, "Bitcoin Network Shaken by Blockchain Fork," *Bitcoin Magazine* (March 13, 2013).
[109] Ibid.
[110] Hasu, Prestwich, and Curtis A Model for Bitcoin's Security and the Declining Block Subsidy.
[111] Ibid.

Conclusion

Bitcoin's main value proposition is its censorship-resistant property, which is backed up 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 users, have an effective voice in Bitcoin governance. Although 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, the 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 modes of resolving the societal collective action problems, which ultimately relies on coercion, Bitcoin governance is based on deliberation, persuasion, volition, and choice.

To resolve disputes in the Bitcoin network, 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 her own version of Bitcoin and try to persuade other users to follow her 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.[112] To make a comparison, there is also foot voting in corporate law, however, forking is something more than 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 (good will) to follow the new forked chain. This significantly lifts the barriers to entry and invites even more competition.

There are other 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 developed by developers. Furthermore, they may decide not to validate the blocks broadcast by certain miners. Last but not least, they have their own mechanisms of forking Bitcoin (e.g., UASF). Contrary to the popular belief that the miners and developers control Bitcoin, the history of forks in Bitcoin and the constraints that the developers and miners face in influencing the protocol or users confirm that the ultimate decision makers

[112] In other words, in addition to various types of foot-voting mechanisms, the Bitcoin network is welcome to forking, despite the natural aversion and dislike expressed by some participants against forking Bitcoin. However, if forking is frequently used and become widespread, it may lead to market fragmentation and present a risk to users, consumers or investors. *See* Financial Stability Board, "Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications," (Basel, Switzerland6 June 2019), 23.

are users and markets rather than a relatively centralized groups of developers or miners. Give 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 the potential market failures. However, potential future challenges lie ahead, and it is not clear whether Bitcoin's decentralized governance mechanisms would be able to deal with 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 Bitcoin security model.[113] Various proposals or mechanisms 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.[114] Another important issue would be the discussions about a change in security and consensus mechanisms and 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 would be 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, which led to the concession by miners and exchanges not to pursue such a proposal, such issues are likely to bring the question of governance to the fore again. Only time will tell whether Bitcoin and its governance model can address those critical governance issues.

[113] Raphael Auer, "Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies," *BIS Working Papers No 765* (2019).;
[114] Hasu, Prestwich, and Curtis A Model for Bitcoin's Security and the Declining Block Subsidy.

Bibliography

Abadi, Joseph, and Markus Brunnermeier. "Blockchain Economics." *National Bureau of Economic Research Working Paper 25407* (2018).

Aguilera, Ruth V., and Gregory Jackson. "Comparative and International Corporate Governance." *The Academy of Management Annals* 4, no. 1 (2010/01/01 2010): 485-556.

Akerlof, George A. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84, no. 3 (1970): 488-500.

Akerlof, George A., Paul M. Romer, Robert E. Hall, and N. Gregory Mankiw. "Looting: The Economic Underworld of Bankruptcy for Profit." *Brookings Papers on Economic Activity* 1993, no. 2 (1993): 1-73.

Alexander, Kern. "Bank Corporate Governance: Law and Regulation." Chap. 5 In *Principles of Banking Regulation*, 127-61. Cambridge: Cambridge University Press, 2019.

Andolfatto, David. "Is Bitcoin a Safe Asset?". *MacroMania* (March 27, 2016).

Antonopoulos, Andreas M. *Mastering Bitcoin: Programming the Open Blockchain.* Sebastopol, CA: O'Reilly Media, Inc.,, 2017.

———. *Mastering Bitcoin: Programming the Open Blockchian.* Sebastopol, CA: O'Reilly Media, Inc.,, 2017.

Armour, John. "Bank Governance." In *The Oxford Handbook of Corporate Law and Governance*, edited by Jeffrey Gordon and Wolf-George Ringe. Oxford: Oxford University Press, 2015.

Armour, John, and Jeffrey N Gordon. "The Berle-Means Corporation in the 21st Century." (2009).

Atik, Jeffery, and George Gerro. "Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice." *Stanford Journal of Blockchain Law & Policy* (2018).

Auer, Raphael. "Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies." *BIS Working Papers No 765* (2019).

Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UC Davis Law Review* 49 (2016): 1183-234.

Bank for International Settlements. "Cryptocurrencies: Looking Beyond the Hype." In *Annual Economic Report*. Basel, Switzerland, June 2018.

Batmanghelidj, Esfandyar, and Axel Hellman. "Europe, Iran, and Economic Sovereignty: A New Banking Architecture in Response to Us Sanctions." 2018.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven: Yale University Press, 2006.

Berle JR., Adolf A., and Gardiner C. Means. *The Modern Corporation and Private Property*. New York: The Macmillan Company, 1933.

Bilton, Nick. *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road.* New York: Portfolio/Penguin, 2017.

Brito, Jerry, and Peter van Valkenburgh. "Writing and Publishing Code Alone Cannot Be a Crime." *CoinCenter.org* (Octover 29, 2018).

Buterin, Vitalik. "Bitcoin Network Shaken by Blockchain Fork." *Bitcoin Magazine* (March 13, 2013).

———. "Daos, Dacs, Das and More: An Incomplete Terminology Guide." *Ethereum Blog* (May 6, 2014).

Carney, Mark. "The Growing Challenges for Monetary Policy in the Current International Monetary and Financial System." Jackson Hole Symposium 2019: Bnak of England, 23 August 2019.

Chazan, Guy. "Germany Calls for Global Payments System Free of Us." *Financial Times*, August 21, 2018 August 21, 2018.

Cheffins, Brian R. "The Rise and Fall (?) of the Bearle-Means Corporation." *Seattle University Law Reveiw* 42 (2018): 445.

Committee on Payment and Settlement Systems, and Technical Committee of the International Organization of Securities Commissions. "Principles for Financial Market Infrastructures." Basel,

Switzerland: Bank for International Settlements and International Organization of Securities Commissions, April 2012.
Connelly, Brian L., Robert E. Hoskisson, Laszlo Tihanyi, and S. Trevis Certo. "Ownership as a Form of Corporate Governance." *Journal of Management Studies* 47, no. 8 (2010): 1561-89.
Cornes, Richard, and Todd Sandler. "The Theory of Externalities, Club Goods, and Public Goods." Cambridge: Cambridge University Press, 1996.
Cowen, Tyler. "Law as a Public Good: The Economics of Anarchy." *Economics and Philosophy* 8, no. 02 (1992): 249-67.
Davidson, Sinclair, Primavera De Filippi, and Jason Potts. "Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology." *SSRN Working Paper Series* (2016).
———. "Economics of Blockchain." *SSRN Working Paper Series* (2016).
De Filippi, Primavera, and Benjamin Loveluck. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure." *Internet Policy Review* 5, no. 3 (2016): 1-28.
De Filippi, Primavera, and Aaron Wright. *Blockchain and the Law: The Rule of Code.* Cambridge, Massachusetts: Harvard University Press, 2018.
de Haan, Jakob, and Razvan Vlahu. "Coroporate Governance of Banks: A Survery." *Journal of Economic Surveys* 30, no. 2 (2016): 228-77.
Draghi, Mario. "Speech by Mario Draghi, President of the European Central Bank at the Global Investment Conference in London 26 July 2012." (2012).
DuPont, Quinn. "Experiments in Algorithmic Governance: A History and Ethnography of "the Dao," a Failed Decentralized Autonomous Organization." Chap. 8 In *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, edited by Malcolm Campbell-Verduyn, 157-77. New York: Routledge, 2018.
ecurrencyhodler. "Bitcoin Governance." *Medium* (February 5, 2019).
Ehrsam, Fred. "Blockchain Governance: Programming Our Future." *Medium* (November 27, 2017).
Ellickson, Robert C. *Order without Law: How Neighbors Settle Disputes.* Cambridge, Massachusetts: Harvard University Press, 1991.
European Union External Action Service - European External Action. "Implementation of the Joint Comprehensive Plan of Action: Joint Ministerial Statement." news release, September 24, 2018, September 24, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/51036/implementation-joint-comprehensive-plan-action-joint-ministerial-statement_en.
Fama, Eugene F., and Michael C. Jensen. "Separation of Ownership and Control." *The Journal of Law and Economics* 26, no. 2 (1983): 301-25.
Financial Stability Board. "Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications." Basel, Switzerland, 6 June 2019.
Finck, Michèle. *Blockchain Regulation and Governance in Europe.* Cambridge: Cambridge University Press, 2019.
Friedman, David D. "Law as a Private Good: A Response to Tyler Cowen on the Economics of Anarchy." *Economics and Philosophy* 10, no. 2 (1994): 319-27.
Global Commission on Internet Governance. "Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance." Waterloo, Ontario; London: Centre for International Governance Innovation and the Royal Institute of International Affairs, 2017.
Hacker, Philipp. "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations." *Forthcoming in: Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, Oxford University Press, 2019* (2018).
Haque, Raina, Rodrigo Seira, Brent Plummer, and Nelson Rosario. "Blockchain Development and Fiduciary Duty." *Stanford Journal of Blockchain Law & Policy* (2019).
Hardin, Garrett. "The Tragedy of the Commons." *Science* 162, no. 3859 (1968): 1243-48.
Hasu. "No, Concentration among Miners Isn't Going to Break Bitcoin." *Coindesk* (February 20, 2020).

Hasu, James Prestwich, and Brandon Curtis. "A Model for Bitcoin's Security and the Declining Block Subsidy." In *Uncommoncore*, 2019.
Hayek, F. A. "The Use of Knowledge in Society." *The American Economic Review* 35, no. 4 (1945): 519-30.
Hearn, Mike. "The Resolution of the Bitcoin Experiment." *Medium* (January 14, 2016).
Hertig, Alyssa. "Uasf Revisited: Will Bitcoin's User Revolt Leave a Lasting Legacy?". *Coindesk* (August 3, 2017).
Hess, Charlotte, and Elinor Ostrom. *Understanding Knowledge as a Commons: From Theory to Practice.* Cambridge, Massachusetts: MIT Press, 2007.
Hirschman, Albert O. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.* Cambridge, Massachusetts: Harvard University Press, 1970.
Hopt, Klaus J. "Corporate Governance of Banks after the Financial Crisis." Chap. 11 In *Financial Regulation and Supervision: A Post-Crisis Analysis*, edited by Eddy Wymeersch, Klaus J. Hopt and Guido Ferrarini, 337-67. Oxford: Oxford University Press, 2012.
Hsieh, Ying-Ying, Jean-Philippe (JP) Vergne, and Sha Wang. "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies." Chap. 3 In *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, edited by Malcolm Campbell-Verduyn, 48-68. New York: Routledge, 2018.
Jedusor, Tom Elvis "Mimblewimble." (19 July 2016).
Jensen, Michael C., and William H. Meckling. "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure." *Journal of Financial Economics* 3, no. 4 (1976/10/01/ 1976): 305-60.
Koning, JP. "Monetary Exclusion." *American Institute for Economic Research* (July 26, 2018).
Löber, Klaus. "Extraterritorial Application or Regulation in the Area of Financial Market Infrastructure: The Case for Cross-Border Cooperative Oversight." In *European Financial Infrastructure in the Face of New Challenges*, edited by Franklin Allen, Elena Carletti, Mitu Gulati and Jeromin Zettelmeyer, 47-56. San Domenico di Fiesole (FI): European University Institute (EUI), 2019.
Lombrozo, Eric. "Forks, Signaling, and Activation." *Medium* (June 18, 2017).
Lopp, Jameson. "Nobody Understands Bitcoin (and That's Ok)." *Coindesk* (March 11, 2017).
———. "Who Controls Bitcoin Core?" In *Cypherpunk Cogitations: Jameson Lopp's thoughts on Bitcoin, Privacy, and Freedom*, 2018.
Luther, William J., and Sean Stein Smith. "Is Bitcoin a Decentralized Payment Mechanism?". *SSRN Working Paper Series* (2020).
macbook-air. "A Successful Double Spent Us$10000 against Okpay This Morning." *Bitcoin Forum* (March 12, 2013).
Manson, Katrina. "Europe Steps up Drive to Exempt Swift from Iran Sanctions." *Financial Times*, Octover 9, 2018.
Mersch, Yves. "Strengthening the European Financial Industry Amid Disruptive Global Challenges." *Speech by Yves Mersch, Member of the Executive Board of the ECB, at the European Institute of Financial Regulation (EIFR), Paris, 3 September 2018* (September 3, 2018).
Morris, Stephen, and Hyun Song Shin. "Global Games: Theory and Applications." Chap. 3 In *Advances in Economics and Econometrics: Theory and Applications, Eighth World Congress*, edited by Lars Peter Hansen, Mathias Dewatripont and Stephen J. Turnovsky. Econometric Society Monographs, 56-114. Cambridge: Cambridge University Press, 2003.
Nabilou, Hossein. "The Dark Side of Licensing Cryptocurrency Exchanges as Payment Institutions." *Law and Financial Markets Review* 13, no. 4 (2019): 1-9.
———. "How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency." *International Journal of Law and Information Technology* (2019).
———. "Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies." *Journal of Banking Regulation* (2019).
Nabilou, Hossein, and André Prüm. "Central Banks and Regulation of Cryptocurrencies." *Review of Banking & Financial Law (forthcoming)* (2019).

———. "Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies." *Journal of Financial Regulation* 5, no. 1 (2019): 1-35.
Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.
Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press, 2016.
Narayanan, Arvind, and Jeremy Clark. "Bitcoin's Academic Pedigree." *Communications of the ACM* 60, no. 12 (2017): 36-45.
Ostrom, Elinor. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *The American Economic Review* 100, no. 3 (2010): 641-72.
———. "Coping with the Tragedies of the Commons." *Annual Review of Political Science* 2, no. 1 (1999): 493-535.
———. *Governing the Commons: The Evolution of Institutions for Collective Action.* New York: Cambridge university press, 1990.
Paech, Philipp. "The Governance of Blockchain Financial Networks." *The Modern Law Review* 80, no. 6 (2017): 1073-110.
Parisi, Francesco, Norbert Schulz, and Ben Depoorter. "Simultaneous and Sequential Anticommons." *European Journal of Law and Economics* 17, no. 2 (March 01 2004): 175-90.
Parisi, Franciesco, and Ben Depoorter. "Commons and Anticommons." In *The Encyclopedia of Public Choice*, edited by Charles K. Rowley and Friedrich Schneider, 426-28. Boston, MA: Springer US, 2004.
Peel, Michael. "Swift to Comply with Us Sanctions on Iran in Blow to Eu." *Financial Times*, November 5, 2018.
Perley, Buck. "Crypto-Governance and the Dangers of Faction: Lessons from the 18th Century for Designing a Decentralized Future." *Medium* (October 27, 2017).
Poon, Joseph, and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." (2016).
Research, Bitmex. "Competing with Bitcoin Core." 2018.
———. "A Complete History of Bitcoin's Consensus Forks." (28 December 2017).
Securities and Exchange Commission. "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The Dao." Washington, DC, July 25, 2017.
Scott, Colin. "Accountability in the Regulatory State." *Journal of Law and Society* 27, no. 1 (2000): 38-60.
———. "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*, edited by Jacint Jordana and David Levi-Faur, 145-74. Northampton, Massachusetts: Edward Elgar Publishing, Inc., 2004.
———. "Cryptocurrencies: Looking Beyond the Hype." In *Annual Economic Report*. Basel, 2018.
SFOX. "Bitcoin Governance: What Are Bips and How Do They Work?". *Medium* (April 16, 2019).
Shapiro, Gabriel. "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* (January 26, 2019).
———. "Tokenizing Corporate Capital Stock." *ZERO_LAW* (October 28, 2018).
Shin, Laura. "Will This Battle for the Soul of Bitcoin Destroy It?" *Forbes*, Oct. 23, 2017.
Shrem, Charlie. "Bitcoin's Biggest Hack in History: 184.4 Billion Bitcoin from Thin Air." *Hackernoon* (January 11, 2019).
Slaughter, Anne-Marie. "Global Government Networks, Global Information Agencies, and Disaggregated Democracy." *Michigan Journal of International Law* 24 (2003): 1041-75.
———. *A New World Order.* Princeton, New Jeresey: Princeton University Press, 2004.
SWIFT. "Compliance: How Is Swift Governed?". (Undated).
———. "Swift Instructed to Disconnect Sanctioned Iranian Banks Following Eu Council Decision." 15 March 2012.

———. "Update: Iran Sanctions Agreement." (17 January 2016).
Szabo, Nick. "Money, Blockchains, and Social Scalability." *Unenumerated* (February 09, 2017).
Tsagas, Georgina. "The Market for Coporate Control in the Banking Industry." Chap. 9 In *The Law on Corporate Governance in Banks*, edited by Iris H-Y Chiu and Michael McKee, 285-336. Cheltenham, UK: Edward Elgar Publishing Limited, 2015.
TwoBitIdiot. "Bitcoin's Constitutional Crisis & Why I Support the Uasf." *Medium* (June 21, 2017).
van Wirdum, Aaron. "The Genesis Files: How David Chaum's Ecash Spawned a Cypherpunk Dream." *Bitcoin Magazine* (24 April 2018).
———. "The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It." *Bitcoin Magazine* (15 June 2018).
———. "The Good, the Bad and the Ugly Details of One of Bitcoin's Nastiest Bugs Yet." *Bitcoin Magazine* (September 21, 2018).
———. "The Latest Twist to the Block Size Debate Is Called a "Uasf"." *Bitcoin Magazine* (March 2, 2017).
———. "Why Some Changes to Bitcoin Require Consensus: Bitcoin's 4 Layers." *Bitcoin Magazine* (February 26, 2016).
van Wirdum, Aaron "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol." *Bitcoin Magazine*, Sept. 7, 2016.
———. "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol." *BITCOINMAGAZINE*, Sept. 7, 2016.
Walch, Angela. "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk." *N.Y.U. Journal of Legislation & Public Policy* 18 (2015): 837-93.
———. "In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains." In *Regulating Blockchain: Techno-Social and Legal Challenges*, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos and Stefan Eich. Oxford: Oxford University Press, Forthcoming 2019.
White, Lawrence H. "The Market for Cryptocurrencies." *CATO Journal* 35, no. 2 (Spring/Summer2015 2015): 383-402.
Wirdum, Aaron van. "The History of Lightning: From Brainstorm to Beta." *Bitcoin Magazine* (4 April 2018).
———. "Mimblewimble: How a Stripped-Down Version of Bitcoin Could Improve Privacy, Fungibility and Scalability All at Once." *Bitcoin Magazine* (12 August 2016).
Zamfir, Vlad. "Against Szabo's Law, for a New Crypto Legal System." *Medium* (Janauray 26, 2019).
Zaring, David. "Financial Regulation's Overlooked Networks." Chap. 5 In *Reconceptualising Global Finance and Its Regulation*, edited by Ross P. Buckley, Emilios Avgouleas and Douglas W. Arner, 67-90. New York: Cambridge University Press, 2016.
———. "International Law by Other Means: The Twilight Existence of International Financial Regulatory Organizations." *Texas International Law Journal* 33 (1998): 281.
Zhuoer, Jiang. "Infrastructure Funding Plan for Bitcoin Cash." *Medium* (January 22, 2020).
Zook, Matthew A., and Joe Blankenship. "New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance." *Geoforum* 96 (2018/11/01/ 2018): 248-55.