BLOCKCHAINS AS INFRASTRUCTURE AND SEMICOMMONS

JAMES GRIMMELMANN*

A. JASON WINDAWI**

ABSTRACT

Blockchains are not self-executing machines. They are resource systems designed by people, maintained by people, and governed by people. Their technical protocols help to solve some difficult problems in shared resource management, but behind those protocols there are always communities of people struggling with familiar challenges in governing their provision and use of common infrastructure.

In this Article, we describe blockchains as shared, distributed transactional ledgers using two frameworks from commons theory. Brett Frischmann's theory of infrastructure provides an external view, showing how blockchains provide useful, generic infrastructure for recording transactions and why that infrastructure is most naturally made available on common, nondiscriminatory terms. Henry Smith's theory of semicommons provides an internal view, showing how blockchains intricately combine private resources (such as physical hardware and on-chain assets) with common resources (such as the shared transactional ledger and the blockchain protocol itself). We then detail how blockchains struggle with many of the governance challenges that these frameworks predict, requiring blockchain communities to engage in extensive off-chain governance work to coordinate their uses and achieve consensus. Blockchains function as

* Tessler Family Professor of Digital and Information Law, Cornell Tech and Cornell Law School.

Our thanks to Aislinn Black, Tyler Kell, and Yan Ji.

** Ph.D., Sociology, Princeton University.

infrastructure and semicommons not in spite of the human element, but because of it.

TABLE OF CONTENTS

INTRODUCTION

Blockchains are black boxes—at least as far as legal scholarship is concerned. Large and growing bodies of literature discuss the potential applications of blockchains in fields including antitrust,[1] contracts,[2] commercial law,[3] corporate law,[4] financial regulation,[5] property,[6] securities law,[7] and more.[8] This scholarship largely takes blockchains themselves as given and instead asks whether and how law should regulate the various uses people make of blockchains.

When legal scholarship does discuss the inner workings of a blockchain, the details are treated primarily as a technical question. The computer science of consensus protocols, cryptographic signatures, mining, and transactions are described in enough detail to explain how the underlying technology works and then set to one side. This is the ambit of computer science, not of law. On this view,

1. *See, e.g.*, THIBAULT SCHREPEL, BLOCKCHAIN + ANTITRUST: THE DECENTRALIZATION FORMULA (2021) (ebook).

2. *See, e.g.*, Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 322 (2017).

3. *See, e.g.*, Heather Hughes, *Blockchain and the Future of Secured Transactions Law*, 3 STAN. J. BLOCKCHAIN L. & POL'Y 21, 22-23 (2020); Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 WASH. & LEE L. REV. 1521 (2021); Kevin V. Tu, *Perfecting Bitcoin,* 52 GA. L. REV. 505, 545-46, 555 (2018); Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIA. BUS. L. REV. 1 (2016).

4. *See, e.g.*, Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679 (2019); Alexandra Andhov, *Corporations on Blockchain: Opportunities & Challenges*, 53 CORNELL INT'L L.J. 1 (2020); Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373 (2019); Kevin V. Tu, *Blockchain Stock Ledgers*, 96 IND. L.J. 223 (2020); George S. Geis, *Traceable Shares and Corporate Law*, 113 NW. U. L. REV. 227 (2018).

5. *See, e.g.*, Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919 (2023).

6. *See, e.g.*, Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607 (2022); Joshua A.T. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261 (2022); Eric D. Chason, *How Bitcoin Functions as Property Law*, 49 SETON HALL L. REV. 129 (2018).

7. *See, e.g.*, Yuliya Guseva, *A Conceptual Framework for Digital-Asset Securities: Tokens and Coins as Debt and Equity*, 80 MD. L. REV. 166 (2021); Jonathan Rohr & Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, 70 HASTINGS L.J. 463 (2019).

8. *See, e.g.*, Bridget J. Crawford, *Blockchain Wills*, 95 IND. L.J. 735 (2020) (trusts and estates). For general analyses of the relationship of blockchains to law, see KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018); AARON WRIGHT & PRIMAVERA DE FILIPPI, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).

legal scholars should care about *what blockchains enable* rather than *how they work*.

We disagree. We believe that legal theory should pay close attention to the technical details of blockchains for two reasons.

First, what is inside the black boxes is interesting in its own right. Legal scholarship can illuminate *how blockchains work*. A blockchain is, at heart, a set of rules for how to use a shared resource, and this kind of coordination problem is a familiar subject for property theory and intellectual property theory. Similar to wikis and open-source software projects, blockchains are an important real-world example of collaboration in action.[9]

Second, black boxes do not always work. Legal scholarship can explain *how blockchains break*. Predicting blockchains' likely failure modes is a central question for regulating them. The same tools from legal theory that help explain when collaborations succeed can also help explain when they fail. The history of blockchain disasters—from the DAO hack to stolen apes—is most usefully explained in terms of their inner workings.[10]

In this Article, we give a careful description of blockchains as *infrastructural semicommons*.[11] Our description draws on two established lines of scholarship. First, we use Brett Frischmann's theory of infrastructure[12] to position blockchains in larger streams

9. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

10. Some legal scholarship examines blockchain failure modes to extract lessons for regulation. *See, e.g.*, Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019) (analyzing technical flaws in smart contracts); James Grimmelmann, *All Smart Contracts Are Ambiguous*, 2 J.L. & INNOVATION 1 (2019) (examining forks and other consensus breakdowns).

11. We presume familiarity with the technical fundamentals of blockchains. For references, see generally ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016); ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS (2019). For a gentle introduction, see generally Kevin Roose, *The Latecomer's Guide to Crypto*, N.Y. TIMES (Mar. 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/cryptocurrency-crypto-guide.html [https://perma.cc/RZ4Y-YEAZ]. For a critique, see Molly White, Matt Binder, Grady Booch, Amy Castor, Stephen Diehl, Dirty Bubble Media, Catherine Flick, David Gerard, Geoffrey Huntley, Bennett Tomlin, Neil Turkewitz & Ed Zitron, *The (Edited) Latecomer's Guide to Crypto*, MOLLYWHITE.NET (Mar. 25, 2022), https://www.mollywhite.net/annotations/latecomers-guide-to-crypto [https://perma.cc/WGU7-SCGP].

12. BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES,

of production.[13] On the one hand, blockchains are useful to their users because they provide an infrastructural service: users can record transactions and run sophisticated applications without needing to trust a single centralized service operator.[14] On the other hand, blockchains themselves depend on a set of underlying infrastructural resources.[15] Some of this infrastructure (for example, worldwide internet connectivity) is preexisting, but some of it (for example, protocols and software) must be specifically provisioned for a blockchain to function.[16]

This infrastructural framework foregrounds the functional roles that blockchain systems play but tells us relatively little about how they are constructed. We fill in these details using Henry Smith's semicommons theory, which highlights the complex balance of private (for example, individual computers, cryptocurrency tokens) and commons property (for example, the blockchain protocol, the history of blocks) that make the construction and ongoing functioning of a blockchain possible.[17] Semicommons theory directs attention to the boundaries between different resources, the mixed incentives of different participants, and governance institutions.[18]

The two frameworks are complementary. The infrastructure story is demand-side. It explains blockchains from the outside in: why they provide useful outputs and what inputs they require to function. The semicommons story is supply-side. It explains blockchains from the inside out: how they are structured to overcome coordination and cooperation problems.

---

at xiii (2012); *see also* Yochai Benkler, *Commons and Growth: The Essential Role of Open Commons in Market Economies*, 80 U. CHI. L. REV. 1499 (2013) (reviewing BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012)) (situating Frischmann's theory of infrastructure within commons theory more broadly).

13. *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 918-19 (2005); FRISCHMANN, *supra* note 12; GOVERNING KNOWLEDGE COMMONS (Brett M. Frischmann et al. eds., 2014); Michael J. Madison, Brett M. Frischmann & Katherine J. Strandburg, *Constructing Commons in the Cultural Environment*, 95 CORNELL L. REV. 657 (2010).

14. *See* Frischmann, *supra* note 13, at 956 (explaining what constitutes an infrastructural service).

15. *See id.* at 928 (discussing examples of infrastructural resources).

16. *See id.* at 1005-07.

17. *See* Henry E. Smith, *Exclusion Versus Governance: Two Strategies for Delineating Property Rights*, 31 J. LEGAL STUD. S453, S453-54 (2002).

18. *See id.* at S457.

Our analysis highlights the roles of different and overlapping governance institutions in blockchains.[19] Governance has long been recognized as a key feature of commons management.[20] An essential task in mapping a commons resource is describing how its governance institutions are constituted and the rules they develop and enforce.[21] Although the commons form is sometimes treated as the opposite of private property, recognizing commons governance and private exclusion as two strategies for resource management is more helpful.[22] Infrastructural blockchain semicommons use both governance and exclusion in complementary ways.[23] In particular, this perspective emphasizes that socially based "off-chain" governance plays an essential role in making technically based "on-chain" exclusion work at all.[24]

Part I of this Article gives a description of a blockchain as layered infrastructure. It describes the essential features of a transactional ledger and shows how Frischmann's theory of infrastructure elegantly captures these characteristics. Then, Part II shows how blockchains overcome the coordination and cooperation problems inherent in making a ledger distributed. Here, Smith's theory of semicommons succinctly describes the relevant moving parts. Next, Part III complicates the story by demonstrating that blockchains display precisely the tensions and instabilities that semicommons theory predicts. These challenges are serious, and whether a blockchain fails or succeeds often turns on whether its governance institutions are capable of rising to the occasion. Finally, a brief

19. We are not the first to consider blockchain governance. The most comprehensive theoretical framework is Enrico Rossi & Carsten Sørensen, Towards A Theory of Digital Network De/Centralization: Platform-Infrastructure Lessons Drawn from Blockchain (Dec. 13, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3503609 [https://perma.cc/C66S-SPC4]. *See also* Rowan van Pelt, Slinger Jansen, Djuri Baars & Sietse Overbeek, *Defining Blockchain Governance: A Framework for Analysis and Comparison*, 38 INFO. SYS. MGMT. 21, 21-22 (2021). *See generally* Yue Liu, Qinghua Lu, Liming Zhu, Hye-Young Paik & Mark Staples, A Systematic Literature Review on Blockchain Governance (Mar. 29, 2022) (unpublished manuscript), https://arxiv.org/abs/2105.054603 [https://perma.cc/2HY3-MG4T].

20. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 1-2 (1990).

21. *See, e.g.*, Rossi & Sørensen, *supra* note 19, at 18.

22. *See* Smith, *supra* note 17, at S454-55.

23. *See id.*

24. *See, e.g.*, van Pelt et al., *supra* note 19, at 22, 30.

conclusion reflects on the rhetoric of trust and community around blockchains—seeing them as infrastructural semicommons helps one understand what is really at stake in these conversations.

I. Infrastructure

A. Definition

In Frischmann's definition, a resource is infrastructure when it has three characteristics.[25] First, the resource is nonrival: it "may be consumed nonrivalrously for some appreciable range of demand."[26] Nonrivalrousness means that the resource is capable of serving multiple simultaneous uses.[27] Second, the resource is valuable as an input: demand for the resource "is driven primarily by downstream productive activities that require the resource as an input."[28] Input resources are valuable for what they enable rather than for direct consumption.[29] And third, the resource is generic: it "may be used as an input into a wide range of goods and services, which may include

25. Frischmann, *supra* note 12, at 61. A related but less precisely theorized concept is the "platform." *See, e.g.*, Vitalik Buterin, A Next-Generation Smart Contract & Decentralized Application Platform 13 (2014), https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [https://perma.cc/M5XE-6WJJ] (describing Ethereum as a platform). A definition from economics is that a (multisided) platform enables direct interactions between two or more distinct groups of users, each of which is affiliated with the platform. *See* Andrei Hagiu & Julian Wright, *Multi-Sided Platforms*, 43 Int'l J. Indus. Org. 162, 163 (2015). A technical definition is that a (computing) platform is standardized hardware, software, or service that provides functionality developers can write software to make use of. (Other definitions emphasize the presence of network effects. *See* Juan Manuel Sanchez-Cartas & Gonzalo León, *Multisided Platforms and Markets: A Survey of the Theoretical Literature*, 35 J. Econ. Survs. 452, 453-57 (2021) (discussing competing definitions)). Combining these two definitions recovers something that can function as a form of infrastructure in Frischmann's sense. *See* Ben Thompson, *A Framework for Regulating Competition on the Internet*, Stratechery (Dec. 9, 2019), https://stratechery.com/ 2019/a-framework-for-regulating-competition-on-the-internet/ [https://perma.cc/M2LV-JSCJ]. *See generally* Tarleton Gillespie, *The Politics of 'Platforms,'* 12 New Media & Soc'y 347 (2010) (discussing ambiguities of "platform" terminology); Rossi & Sørensen, *supra* note 19, at 8-10 (discussing platform/infrastructure distinction and reviewing literature).

26. Frischmann, *supra* note 12, at 61.

27. *See id.* at 62.

28. *Id.* at 61.

29. *See id.* at 61, 63.

private goods, public goods, and social goods."[30] Genericity means that analysis of the resource cannot be assimilated to the analysis of its sole productive use.[31] Classic examples of infrastructure include roads and other transportation networks, telecommunications networks, the natural environment, ideas, and languages.[32]

But Frischmann also points to a pervasive dilemma of infrastructure. Many of the downstream uses that infrastructure supports create positive spillovers that have social benefit exceeding their private value to the user.[33] Many of these spillovers go beyond the consumer surplus that attaches to any good in a world without perfect price discrimination.[34] Some uses have network effects. For example, each additional user of a currency standard reduces the average information costs of pricing in a way that benefits all existing users. Other uses are true public goods that benefit everyone, whether or not they also use the infrastructure.[35] New ideas are public goods in this sense.[36]

The problem is that the infrastructure users who create positive spillovers cannot and will not pay for all of the value they confer on society.[37] This means that the traditional property strategy of treating a resource as a private good, with a price based on a user's willingness to pay, fails for infrastructure.[38] Users will pay for the private value they individually realize from using the infrastructure, but that is less than the full social value their use creates.[39] The private owner of the infrastructure will price access above the point that would be efficient for society overall, resulting in underuse.[40] Some of the uses that the infrastructure *could* support (because it is nonrival) will be lost because the private infrastructure

30. *Id.* at 61.
31. *See id.* at 64-65.
32. *Id.* at 3-4.
33. *Id.* at 63-64; Brett M. Frischmann & Mark A. Lemley, Essay, *Spillovers*, 107 COLUM. L. REV. 257, 257 (2007).
34. *See* Frischmann & Lemley, *supra* note 33, at 262.
35. *See id.* at 259.
36. *See id.* at 259 n.4.
37. *See id.* at 271-74.
38. *See id.* at 258.
39. *See id.*
40. *See* FRISCHMANN, *supra* note 12, at 66.

owner has too weak an incentive to allow them (because of uninternalized spillovers).[41]

Frischmann's solution to this dilemma is commons management, "in which a resource is shared among members of a community on nondiscriminatory terms ... *that do not depend on the users' identity or intended use*."[42] Anyone within the relevant community who wants to use the infrastructure can, and they can do so on substantially the same terms as anyone else.[43] Treating infrastructure as a commons encourages wider use, including publicly valuable uses that cannot pay their own way.[44] Frischmann traces the commons-management strategy in numerous infrastructural resources, including communications networks and knowledge resources.[45]

Commons governance of infrastructure faces two characteristic challenges. On the demand side, it must prevent congestion due to overuse.[46] While pure public goods, such as ideas, are inexhaustible, other kinds of infrastructure, such as roads and telephone networks, have limited capacity.[47] When that capacity is reached or exceeded, their quality degrades and users suffer.[48] So some kind of mechanism should deter use beyond the point at which the use's marginal value is exceeded by the negative spillovers it causes for other users. On the supply side, governance must create sufficient incentives to provision the resource in the first place.[49] For ideas, this is the intellectual property problem of incentives for creation.[50] For tangible infrastructure such as roads and communications networks, someone must physically create and maintain the infrastructure. So somehow compensation should flow to those who do the work of creation and maintenance.

---

41. *See* Frischmann & Lemley, *supra* note 33, at 265-66.

42. FRISCHMANN, *supra* note 12, at 92.

43. *See id.* at 91-114; Frischmann, *supra* note 13, at 926; GOVERNING KNOWLEDGE COMMONS, *supra* note 13, at 29-30. *See generally* James Grimmelmann, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42 (2015) (giving taxonomy of management strategies in the context of content moderation).

44. *See* Frischmann, *supra* note 13, at 975-78.

45. *See* FRISCHMANN, *supra* note 12, at 61.

46. *See* James Grimmelmann, *The Internet Is a Semicommons*, 78 FORDHAM L. REV. 2799, 2806-10 (2010) (discussing overuse challenges).

47. *See id.* at 2806, 2810-12.

48. *See id.* at 2806-10.

49. *See id.* at 2810-12 (discussing provisioning challenges).

50. Frischmann & Lemley, *supra* note 33, at 266.

There are two traditional solutions to these challenges. One is direct public provisioning, in which the government pays for the infrastructure out of general tax revenues.[51] This is how roads work, for example, and as a result, they are typically free to users.[52] The other is public utility regulation, in which the infrastructure is privately provided, but the government regulates the terms on and prices at which it is provided to users to ensure nondiscriminatory access at a price that maximizes overall social value.[53]

B. Ledgers as Infrastructure

Transactional ledgers are infrastructure under Frischmann's definition. Consider a county land title office for recording deeds and other documents. First, up to the capacity of the ledger, its use is nonrival. One person filing a deed does not interfere with anyone else's ability to file one.[54] Second, the ledger is useful as an input. Other than historians and property scholars, few people enjoy browsing through land title records for its own sake. Rather, the records are useful for facilitating secure land transactions. And third, the ledger is generic. It helps support all uses of land. The ledger is an input into home purchases, into factory construction, into secured lending, into environmental studies, and more.

It is important to distinguish between four related resources in a ledger, which can be illustrated using the traditional land title office. First, there is the physical hardware on which the ledger operates: the paper files or digital computers that tangibly and persistently store property records. These are private resources—one cannot just walk into a land title office and walk out with the file cabinets. Second, there is the ledger itself: the recording service the office provides. This is the infrastructural resource itself, and it is managed as a commons.[55] Third, there is the information on the ledger: the details of who owns what, who sent what to whom, and what computations have taken place. This information is a pure

51. *See* FRISCHMANN, *supra* note 12, at 196.

52. *See id.*

53. *See id.* at 108-14.

54. *See* Frischmann, *supra* note 13, at 942 (describing nonrivalry as a situation in which one individual's consumption does not hinder consumption opportunities for others).

55. *See* FRISCHMANN, *supra* note 12, at 92-93.

public good: it is nonrival and nonexcludable.[56] And fourth, there are the assets tracked on the ledger: legal interests in land, easements, and mortgages. These assets are private goods.[57] To summarize, private hardware is used to construct a common ledger that records common information about private assets.

The relationship between these resources can be usefully described in terms of modularity and layering. A modular system is one in which individual components can be divided into distinct modules—"specialized units that operate semi-autonomously from other specialized units."[58] Each module is tightly coupled internally, but loosely coupled to other modules.[59] In a modular system, a module serving a particular function can be swapped out for one performing the same or a similar function without significantly affecting the other modules in the system.[60] Replacing one computer with another in the recording office is invisible to users; they will not notice that the office has migrated its database from Oracle to MySQL.

Layering is a specific, and highly fruitful, type of modularity.[61] In a layered system, components are divided into distinct layers based on their functions, interactions, and dependencies.[62] In its ideal-typical form, each layer interacts only with the layers immediately above and beneath it and depends only on the layer immediately beneath it.[63] For example, the internet is commonly divided into a physical layer (hardware), a link layer (protocols designed for

---

56. *See id.* at 62.

57. *See id.* at 24-25.

58. Thomas W. Merrill, Response, *Property as Modularity*, 125 HARV. L. REV. F. 151, 155 (2012); *see also* Henry E. Smith, *Property as the Law of Things,* 125 HARV. L. REV. 1691, 1700-01 (2012) (presenting a modular theory of property); Henry E. Smith, *Modularity in Contracts: Boilerplate and Information Flow*, 104 MICH. L. REV. 1175, 1180-81 (2006) (applying modularity to boilerplate contracts).

59. *See* Merrill, *supra* note 58, at 155.

60. *See id.*

61. *See generally* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815 (2004) (describing the internet as a layered system); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008) (analyzing layering within networks); BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010) (explaining layering in internet architecture).

62. See generally VAN SCHEWICK, *supra* note 61, for a description of the internet as a layered system.

63. *See id.* at 47.

specific kinds of hardware), a network layer (internet protocol, which is universal across the internet, and from whence the "IP" in "IP address" derives), a transport layer (for example, protocols such as HTTP that are optimized for classes of applications), and an application layer (for example, Skype, Netflix, or Facebook).[64] In the ideal form, applications do not deal directly with the physical, link, or hardware layers; instead, they make requests of and receive information back from the transport layer.[65] Facebook does not know and does not care whether it is running on a DOCSIS-based cable network or a 4G-based wireless network.[66]

From a layers perspective, the recording office resource system has three layers. There is a physical-hardware layer, which supports a ledger-service layer, which records information about a property-interests layer. The hardware is private, the ledger service is managed as a commons, and the property interests are private.

C. Blockchains as Infrastructure

Blockchains are ledgers, and as such they are infrastructure.[67] One of the reasons for the widespread interest in blockchains is that they can be particularly generic as ledgers. Blockchains support cryptocurrencies such as Bitcoin and Ether.[68] Blockchains support asset-ownership tokens, such as Bored Apes, corporate shares, and titanium cubes.[69] And blockchains support smart-contract-based applications: games such as *Axie Infinity*,[70] investment schemes

---

64. *See* Solum & Chung, *supra* note 61, at 839-40.

65. *See id.* at 840.

66. *Cf.* BUTERIN, *supra* note 25, at 13 (describing Ethereum as "essentially the ultimate abstract foundational layer").

67. *See, e.g.*, Chason, *supra* note 6, at 135-37, 147, 156 (comparing traditional recording system and blockchain); Benito Arruñada, *Blockchain's Struggle to Deliver Impersonal Exchange*, 19 MINN. J.L. SCI. & TECH. 55, 58-60 (2018).

68. *See* Arruñada, *supra* note 67, at 58.

69. *See id.* at 61.

70. *See* Joshua Brustein, *A Billion-Dollar Crypto Gaming Startup Promised Riches and Delivered Disaster*, BLOOMBERG (June 10, 2022, 5:00 AM), https://www.bloomberg.com/news/features/2022-06-10/axie-infinity-axs-crypto-game-promised-nft-riches-gave-ruin [https://perma.cc/6LGU-NU6C].

such as SpiceDAO,[71] and economic exchanges such as prediction markets.[72]

A (public) blockchain is also a commons in Frischmann's sense.[73] It has no restrictions on who can record transactions in its ledger or who can read them.[74] While some blockchains have transaction fees, such as paying for gas on Ethereum, those fees are nondiscriminatory.[75] The pricing is based entirely on the intensity of one's use (for example, how much work the Ethereum Virtual Machine must do for one's transaction) rather than on the identity of the user or on how much value they are extracting from the use.[76]

One of the salient points about blockchains—which puts the "crypto" in "cryptocurrency"—is that the ledger entries are secured with digital signatures. Only a user who knows the private key to the address associated with a blockchain asset can create a transaction that uses or transfers that asset.[77] As long as users are able to keep their private keys secret, this makes these assets both rival and excludable: true private goods.[78] Thus, a blockchain can be used not just to record information about property rights in already-existing, off-chain assets but to create and enforce property rights in new on-chain assets.

D. Decentralization

Public provision of ledgers can be an attractive strategy because a ledger database is not especially costly. Publicly provisioned ledgers include land records and ownership of intellectual property

---

71. *See* Adi Robertson, *They Spent $3 Million on a Dune Script Bible—Now What?*, THE VERGE (Feb. 28, 2022, 9:07 AM), https://www.theverge.com/2022/2/28/22950868/spice-dao-crypto-jodorowsky-dune-bible-collective-writing-contest [https://perma.cc/JY2V-UEDG].

72. Clay Graubard & Andrew Eaddy, Opinion, *Forecasting, Prediction Markets and the Age of Better Information*, COINDESK (June 5, 2022, 3:47 PM), https://www.coindesk.com/layer2/2022/06/04/forecasting-prediction-markets-and-the-age-of-better-information/ [https://perma.cc/LL66-436X].

73. *See* Frischmann, *supra* note 13, at 933-37.

74. *See generally* Chason, *supra* note 6 (comparing blockchain with traditional property recording).

75. *See* GAVIN WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER 7, https://gavwood.com/paper.pdf [https://perma.cc/K65U-JDXB].

76. *See id.*

77. *See id.* at 17.

78. *See* FRISCHMANN, *supra* note 12, at 24-25.

assets, such as copyrights and patents.[79] While there are often fees to *record* a transaction in these ledgers, equally often they are free to *read*—in other words, the information in them is treated as the public good it is.[80]

But while centralized ledgers are straightforward and can be inexpensive, they have their own serious problems. For one thing, a centralized administrator has the power to discriminate among users, undoing the benefits of managing the ledger as a commons.[81] While a commons ledger with nondiscrimination rules may be better for society, the administrator may be better off treating it as a private resource and raising prices. For another thing, the administrator could corruptly manipulate the ledger for their own benefit—by transferring assets to themselves, or by taking bribes to modify the records in ways that benefit the parties paying them off.[82] Most severely, the administrator could lie about the ledger's contents, throwing the integrity of the ledger itself into question.[83]

A ledger is centralized when a single party controls the hardware the ledger operates on.[84] This physical control of the embodiment of the ledger gives them the power to control use of and access to the ledger as a resource and thus to control the informational contents of the ledger.[85] That is, corruption becomes possible when the administrator's *private* control over the hardware lets them manipulate the *common* ledger in a way that diverts the *private* assets tracked by the ledger to their own benefit.[86]

The fear of corruption in centralized ledgers is the impetus for *distributed* ledgers, in which numerous maintainers *collectively* maintain a ledger. Each maintainer contributes its own private hardware and effort to maintain a copy of the ledger.[87] No single

---

79. *See* Chason, *supra* note 6, at 163.

80. *See id.*

81. *See* PRIMAVERA DE FILIPPI & GREG MCMULLEN, COALA & BLOCKCHAIN RSCH. INST., GOVERNANCE OF BLOCKCHAIN SYSTEMS: GOVERNANCE *OF* AND *BY* DISTRIBUTED INFRASTRUCTURE 22 (June 2018), https://hal.archives-ouvertes.fr/hal-02046787/document [https://perma.cc/V7K8-5MLM] (explaining the "curator" role).

82. *See id.* at 5.

83. *See id.*

84. *See id.* at 22.

85. *See id.*

86. *See generally id.* (explaining how curators vetted submissions to the DAO).

87. *See* Bronwyn E. Howell, Petrus H. Potgieter & Bert M. Sadowski, Governance of

participant can exclude a user; no single participant can enter transactions on their own; no single maintainer can successfully lie about the ledger's contents; no single maintainer can corruptly transfer assets to themselves.[88] Dividing the administration among numerous maintainers can preserve the infrastructural benefits of commons management while avoiding the dangers of centralized corruption.

II. SEMICOMMONS

Decentralization raises its own new challenges. One is the challenge of creating appropriate incentives. Why should a maintainer contribute its resources and effort to supporting the infrastructure? This is a collective action problem. It would be easier and cheaper not to participate and instead free ride on the resources and effort contributed by other maintainers.[89] Another pervasive challenge is governance. In all but the simplest cases, the maintainers will have to make contestable decisions about how the infrastructure should be managed.[90] And even in simple cases, they must still monitor each other to be sure that they are acting in accordance with their agreed-upon rules.[91] Building a sustainable commons on top of privately contributed resources is a hard problem.[92]

A. Definition

However, it is a problem that has been solved before. In the Western European medieval open-field system, farmers held individual private plots of land.[93] But livestock were grazed on the

---

Blockchain and Distributed Ledger Technology Projects 2-3 (May 13, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3365519 [https://perma.cc/DC95-VERL].

88. *See generally id.*

89. *See* Henry E. Smith, *Governing the Tele-Semicommons*, 22 YALE J. ON REGUL. 289, 297 (2005).

90. *See generally* Howell et al., *supra* note 87, at 3, 5-6.

91. *See* DE FILIPPI & MCMULLEN, *supra* note 81, at 19.

92. *Cf.* Howell et al., *supra* note 87, at 11-12.

93. *See* Smith, *supra* note 17, at S459.

whole field in common during fallow seasons.[94] The farmers literally reaped the private rewards of their individual strips, but they also benefitted from the use of the open field for pasturage.[95]

Henry Smith generalized the open-field example into a broader definition of a semicommons.[96] In his theory, a resource is a semicommons when it satisfies three conditions. The resource must be held privately with respect to some substantial uses, it must be held in common with respect to some other substantial uses, and the private and common uses must substantially affect each other.[97]

At first glance, the semicommons form appears to be strictly worse than a pure commons. Similar to the commons form, the semicommons form suffers from the challenge of overuse by commons users.[98] This is the classic tragedy of the commons: peasants will overgraze their sheep on the open field because it is costless for them to do so.[99] And similar to a commons, a semicommons suffers from the challenge of underprovisioning by private users.[100] A farmer will be tempted to withdraw their plot from the common open field, perhaps to devote it to more intensive cultivation.[101] In addition to these commons challenges, the semicommons also faces the challenge of targeting by commons users who can choose which private users their use affects.[102] A shepherd can pick whose plot the sheep trample on (bad for the crops) and whose plot the sheep defecate on (good for the crops).

The semicommons form is valuable when the gains from participating in the common use outweighs these costs.[103] In the open field, the semicommons made sense as long as the value of the commons use (wool and mutton) and the benefits conferred by the commons use on the private use (manure as fertilizer) exceeded the costs imposed by the commons use on the private use (trampling of crops)

94. *See id.*
95. *See id.* at S457.
96. Henry E. Smith, *Semicommon Property Rights and Scattering in the Open Fields*, 29 J. LEGAL STUD. 131, 132 (2000).
97. *Id.* at 138.
98. *Id.*
99. *See id.* at 140.
100. *See id.*
101. *See id.*
102. *Id.* at 139.
103. *Id.* at 132.

and the various governance and monitoring costs (keeping an eye on the shepherd).[104] Under those circumstances, each farmer was better off participating than not, and the semicommons was stable.[105] For a more modern example, the internet semicommons makes sense as long as the value to a user of online news, video games, social media, shopping, memes, and the other uses of an internet-connected computer exceeds the price of a computer and an internet connection. The resource-management question is whether and how the distinctive costs of a semicommons—overuse, underprovision, targeting, governance, and monitoring—can be kept sufficiently small that they are less than the benefits of the semicommons form.

Thus, semicommons theory describes a series of characteristic mechanisms employed as semicommons to modulate resource use appropriately. One is compensation, to reward private users for participating in provisioning the common uses.[106] Some compensation is explicit: your monthly bandwidth bill compensates your internet service provider (ISP) for connecting its network cables to the rest of the internet.[107] Other compensation is implicit: farmers who participated in the open-field system were rewarded in mutton from their own sheep and manure of others' sheep.[108] Another is boundary-setting so that private users can defend themselves against targeted overuse and abuse.[109] In the internet semicommons, the Computer Fraud and Abuse Act[110] and the trespass to chattels tort defend the boundaries around individual computers by protecting owners against attacks that impair the functioning of their computers.[111] A third is scattering so that commons users cannot target the costs and benefits of their uses to particular

104. *See id.*

105. *See id.* at 141-42.

106. *See generally* Howell et al., *supra* note 87 (describing miners being rewarded for participating).

107. DE FILIPPI & MCMULLEN, *supra* note 81, at 11-12.

108. *See* Smith, *supra* note 96, at 135-36.

109. *Id.* at 162; *see also* Grimmelmann, *supra* note 46, at 2827-41 (discussing "defensible borders" around internet resources).

110. 18 U.S.C. § 1030.

111. *See, e.g.*, Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016); Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677 (2009); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395 (2007).

private users.[112] In the open-field system, individual plots were held as long, thin strips.[113] This made it impracticable for a shepherd to park a flock over a specific farmer's plot, ensuring that both the trampling and the defecating were spread more evenly over different farmers' land.[114] And finally, as in a pure commons, governance institutions resolve disputes and adjust rules in light of experience in a way that is broadly acceptable to participants.[115]

Not many resources are held as semicommons, but for those that are, it is an essential analytical framework.[116] Robert Heverly and Lydia Pallas Loren have shown that intellectual property law has the structure of a semicommons, combining private and common uses in a mutually overlapping way.[117] In other work, Smith has analyzed water rights as a semicommons, arguing that the literal fluidity of water as it flows above and beneath different owners' land makes the semicommons form appropriate.[118] Telecommunications networks are another good example. Smith has applied semicommons theory to analyze equipment sharing under the Telecommunications Act of 1996,[119] and one of the authors of this Article has

---

112. Smith, *supra* note 96, at 133. Smith treats scattering as a form of boundary-setting, and in a literal and important sense, it is. However, disaggregating the two roles that boundary-setting can play is useful. One, which is typified by scattering, makes targeting by commons more difficult. The other, which is typified by purely private property, makes it easier for private owners to prevent, detect, and take action against intrusions. Note that scattering in the open fields made boundary enforcement *harder*; one point of Smith's argument is that scattering's benefits in preventing targeting outweighed those costs. *See id.* at 156-60 (discussing competing theories).

113. *See id.* at 146.

114. *See id.* at 146-54.

115. *See generally id.* (explaining farmers' governance of a semicommons).

116. For more on semicommons theory in general, see Lee Anne Fennell, *Commons, Anticommons, Semicommons*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF PROPERTY LAW 35 (Kenneth Ayotte & Henry E. Smith eds., 2011).

117. *See* Robert A. Heverly, *The Information Semicommons*, 18 BERKELEY TECH. L.J. 1127, 1164 (2003); Robert A. Heverly, *Revisiting "The Information Semicommons,"* 59 IDEA 137, 151 (2018) [hereinafter Heverly, *Revisiting the Information Semicommons*]; Lydia Pallas Loren, *Building a Reliable Semicommons of Creative Works: Enforcement of Creative Commons Licenses and Limited Abandonment of Copyright*, 14 GEO. MASON L. REV. 271, 295 (2007).

118. Henry E. Smith, *Governing Water: The Semicommons of Fluid Property Rights*, 50 ARIZ. L. REV. 445, 475-77 (2008); Henry E. Smith, *Semicommons in Fluid Resources*, 20 MARQ. INTELL. PROP. L. REV. 195, 206-08 (2016).

119. Smith, *supra* note 89, at 291-93, 300, 302.

previously argued that the internet as a whole is a semicommons.[120] The internet is a particularly apt example because similar to a blockchain, it is layered: a globally connected common network layer sits atop a layer of private hardware.[121]

B. Blockchains as Semicommons

Seen through this lens, the system of mining rewards for maintainers is the necessary glue that holds a blockchain semicommons together. In Bitcoin, for example, the first miner who successfully completes a block of transactions and adds it to the chain receives transaction fees offered by users whose transactions are in that block.[122] By compensating miners, these rewards give them an incentive to contribute their (private) resources to the blockchain: specialized hardware, electricity, network connectivity, and maintenance.[123] At the same time, transaction fees limit overuse by (common) ledger users by pricing access.[124] Users who pay larger fees get their transactions processed faster, and the higher the fee, the less attractive it is to use the blockchain at all.[125] Moreover, transaction fees are broadly nondiscriminatory: they change based on the intensity of use rather than on the user's identity or the value of the use.[126]

Mining rewards are also a form of scattering. Under Bitcoin's proof-of-work algorithm, a miner's chances of finding a nonce that

120. Grimmelmann, *supra* note 46.

121. *See generally* Solum & Chung, *supra* note 61 (explaining that the internet's architecture is layered); ZITTRAIN, *supra* note 61 (describing the modularity of the internet's design).

122. There are also mining rewards, which allocate previously unallocated Bitcoins to the miner who successfully mines a block, according to a schedule that will gradually decrease to zero over time. *See* Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, 12TH WORKSHOP ON ECON. INFO. SEC., 2013, at 5-6. In a sense, because mining rewards dilute the supply of Bitcoin, they function as a tax paid by all users to miners, in which each user's contribution is proportional to their holdings of Bitcoin. We will not further discuss this complication in this Article.

123. *Cf.* Howell et al., *supra* note 87 (describing how incentives and rewards impact contributions).

124. *See id.* at 8-9.

125. *See* David Easley, Maureen O'Hara & Soumya Basu, *From Mining to Markets: The Evolution of Bitcoin Transaction Fees*, 134 J. FIN. ECON. 91, 92, 97-100 (2019).

126. *See* WOOD, *supra* note 75, at 7 (describing usage-based pricing in the Ethereum protocol).

makes a block of transactions hash correctly scales with the number of possible nonces they are able to test.[127] This means that, in expectation, the mining rewards to participants are exactly in proportion to the computational resources that those participants contribute to maintaining the blockchain.[128] This is statistically perfect scattering: a miner's rewards increase with the effort they contribute, and nothing else.[129] In particular, there is no way to corruptly steer the fees from a transaction to any particular miner—a user cannot collude with a miner to pocket those fees.[130] All transaction fees go into a common pool, which is then probabilistically scattered out among participating miners.[131]

This is exactly the necessary link required between the private assets *on top* of the common ledger and the private resources that *maintain* it. The link is tight enough to get the incentives against overuse and for provisioning right: the rewards flow from blockchain *users* to blockchain *providers*, exactly as needed.[132] But at the same time, the two are not so tightly coupled as to vitiate the important commons features of layers between them.[133] Access remains open to all users on nondiscriminatory terms. Rewarding miners using on-chain assets holds the whole thing together.

The other characteristic technical innovation of blockchains—the convention that the state of the ledger is defined by the longest chain—is a governance mechanism.[134] The convention forces

---

127. *See generally* NARAYANAN ET AL., *supra* note 11.

128. *See, e.g.*, *id.*

129. *See* DE FILIPPI & MCMULLEN, *supra* note 81, at 14.

130. *See* E. Napoletano & Benjamin Curry, *Proof of Work Explained*, FORBES ADVISOR (Apr. 8, 2022, 3:06 PM), https://forbes.com/advisor/investing/cryptocurrency/proof-of-work [https://perma.cc/8JHQ-NEL2].

131. The process is a little different in proof-of-stake blockchains. Here, users participate by temporarily locking up (or "staking") their cryptocurrency and receive rewards proportional to the amount they stake rather than to the computational effort they expend. *See, e.g.*, Vitalik Buterin, *Proof of Stake FAQ*, VITALIK (Dec. 31, 2017), https://vitalik.ca/general/2017/12/31/pos_faq.html [https://perma.cc/E8H9-S6EA] (providing an accessible overview of proof of stake, its advantages, and its challenges). *See generally* Phil Daian, Rafael Pass & Elaine Shi, *Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake*, 23D INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SEC. 23 (2019) (providing an overview of design requirements for proof-of-stake systems). This, too, is a form of scattering; the strips are on-chain assets rather than off-chain computers.

132. *See* Easley et al., *supra* note 125.

133. *See generally* Solum & Chung, *supra* note 61.

134. *See* DE FILIPPI & MCMULLEN, *supra* note 81, at 14.

consensus on what the state of the ledger actually is by giving participants a powerful incentive to agree with each other.[135] It is rational for any given participant to settle on the chain that all the *other* participants regard as authoritative, and the convention that the authoritative chain is the longest one is a game-theoretic focal point. Observing which candidate chain is longest is easy, and any situation with multiple competing chains will tend to resolve itself quickly as one or the other pulls ahead.[136]

A participant who dissents about the state of the ledger effectively forfeits their on-chain assets because no one else will trade with them.[137] That participant also has nothing to gain from mining work.[138] Other participants will not accept the new blocks they propose.[139] Nakamoto consensus is a governance mechanism that strongly incentivizes agreement.[140] The proposal's rules are normative: they give participants reason to accept the verdict of the longest chain.[141] That normative force is what holds a blockchain together.

III. Governance

The picture sketched in Part II is striking in its elegance. The key technical features of a blockchain—cryptographic verification, block rewards to participants, and longest-chain consensus—fit together similar to the parts of a finely engineered watch. Driven by their own private incentives, participants collaborate to produce a common ledger.[142] The protocol itself appears to be the only enforcement mechanism needed. The blockchain governs itself.

But that is not the end of the story. It never is. Just as infrastructural ledgers face challenges that distributed ledgers help solve, and distributed ledgers face challenges that blockchain

135. *See* Howell et al., *supra* note 87, at 15.
136. *See generally* Daian et al., *supra* note 131.
137. *See* Howell et al., *supra* note 87, at 12.
138. *See* De Filippi & McMullen, *supra* note 81, at 14.
139. *See id.*
140. *See generally* Bruno Biais, Christophe Bisière, Matthieu Bouvard & Catherine Casamatta, *The Blockchain Folk Theorem*, 32 Rev. Fin. Stud. 1662 (2019) (discussing the degree to which the Bitcoin protocol creates incentives against forks).
141. *See id.* at 1664.
142. *See id.*

semicommons help solve, blockchain semicommons face their own challenges.

Blockchain governance looks automated, but it is not.[143] The formal, technical mechanisms embedded in a blockchain protocol are just one facet of the governance work required to keep a blockchain functioning as infrastructure.[144] Semicommons theory directs our attention to the ways in which collaboration among blockchain participants and users can break down and to the governance institutions that guard against these breakdowns and deal with their consequences.[145] This Part describes six challenges that compel blockchain participants and users to engage in governance.

A. Protocols and Software

The first challenge is that blockchains do not spring full-blown like Athena from the minds of their creators. A blockchain's protocol, which describes the format of entries on its ledger, the messages participants and users exchange with each other, and the rules for achieving consensus, is a complicated thing.[146] The document defining the semantics of the Ethereum virtual machine is a forty-one-page PDF, and that is just a small part of the Ethereum protocol.[147] There are also highly detailed documents defining the data structures maintained by clients to describe the state of the ledger, the messages exchanged among clients, and much more.[148] Similarly, a blockchain requires software—actual clients that implement the protocol as runnable code.[149] For a complicated

143. Primavera De Filippi and Greg McMullen have usefully described this distinction as one between "governance *by* the infrastructure" (that is, rules embedded in the technical protocols and enforced by software) and "governance *of* the infrastructure" (that is, rules that "operate at the social or institutional level"). DE FILIPPI & MCMULLEN, *supra* note 81, at 17-18.

144. *See id.* at 16-20.

145. *See id.* at 23 (offering the DAO as an example of the limitations of on-chain governance).

146. *See generally id.* (explaining the interaction between blockchain's hard-coded rules and governance by individual users).

147. *See* WOOD, *supra* note 75.

148. *See Geth Documentation*, GETH, https://geth.ethereum.org/docs/ [https://perma.cc/5HV9-DM3V] (directory of Ethereum specifications and resources).

149. *See* DE FILIPPI & MCMULLEN, *supra* note 81, at 19 (explaining institutional rules within technical protocols software enforces).

blockchain such as Ethereum, this is an immense, complicated piece of software.[150]

There is good news and bad news. The good news is that protocols and software are information, and as such, they are pure public goods, so there is no risk of overuse.[151] Indeed, blockchain software is typically open-sourced to induce greater adoption and to attract greater participation in developing it.[152] The bad news is that protocols and software are information, and as such, they are pure public goods, so they are at risk of being underprovisioned.[153] This is the classic challenge of information production. Everyone involved in a blockchain ecosystem benefits from the existence of a rock-solid protocol and high-quality software, but everyone is also better off free riding on someone else's work to develop them.[154] In this respect, blockchain development raises governance challenges similar to other open-source projects.[155]

One typical solution in the blockchain space is to add private incentives. For example, a new blockchain's developers will reserve some on-chain assets for themselves or for the investors who have funded the development.[156] The idea is that once the blockchain is up and running, those on-chain assets will become valuable, so the development work can be repaid out of this new store of value.[157] One way of doing so, which was particularly faddish a few years ago,

150. As of June 27, 2022, the Linux version of Geth (the official and most popular Ethereum client) was a 42.8-megabyte executable. *Download Geth—Camaraon (v.1.10.19)*, GETH, https://geth.ethereum.org/downloads/ [https://perma.cc/ZXM6-KV5S]. To get a more visceral sense of Geth's complexity and scale, go to its official source code repository, *Go-Ethereum*, GITHUB, https://github.com/ethereum/go-ethereum/ [https://perma.cc/R27X-QZF7], and browse through its source code. This is by no means large by the standards of modern software, but it is hardly trivial, either: this is not something a programmer could dash off in a couple of weeks.

151. *See* Grimmelmann, *supra* note 46, at 2810.

152. *See* Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer & Nelson M. Rosario, *Blockchain Development and Fiduciary Duty*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 139, 156 (2019).

153. *See* Grimmelmann, *supra* note 46, at 2811.

154. *See* Madison et al., *supra* note 13, at 666.

155. Haque et al., *supra* note 152, at 154-55; Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, *in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 58, 58 (Philipp Hacker et al. eds., 2019).

156. *See* Haque et al., *supra* note 152, at 156.

157. *See id.*

was the Initial Coin Offering (ICO), in which the developers directly sell on-chain tokens to the investing public.[158]

However, these on-chain asset-based incentives create their own governance issues. For example, a large stock of reserved tokens creates the risk that the developers who are hoarding them could liquidate their positions, flood the market, and undercut the value of others' investments. Or the developers could sneak in protocol changes or software backdoors that primarily benefit themselves.[159] For this reason, it is also common to set up a foundation or other governance institution to steward these assets and to coordinate development of protocol and software for the benefit of the community around the blockchain.[160] In this way, blockchains strongly resemble previous software-governance efforts, such as those responsible for major open-source projects.[161]

B. Turtles All the Way Up

Another complication is that on-chain assets are not always purely private goods. They can be infrastructure too.[162] The most obvious example is smart contracts. A smart contract is software, which means someone needs to design, program, and debug it.[163] Once a smart contract is created, however, it is an information good.[164] If the source code is shared, then others can reuse it, creating their own instantiations of the same functionality—or they

---

158. Rohr & Wright, *supra* note 7, at 463-65.

159. *See* DE FILIPPI & MCMULLEN, *supra* note 81, at 21.

160. *See, e.g.*, Carla L. Reyes, *(Un)Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875, 1896 (2020).

161. *Cf. id.* at 1895-96 (discussing governance and regulation of blockchain protocol and software development); *see also* Haque et al., *supra* note 152, at 146-47. This connection also highlights the ways in which blockchain communities inherit the governance challenges of online communities such as wikis and open-source development efforts because whatever else it is, a blockchain community *is also by necessity* a software-development community. *See generally* Nicolas Auray, *Online Communities and Governance Mechanisms*, *in* GOVERNANCE, REGULATION AND POWERS ON THE INTERNET 211 (Eric Brosseau et al. eds., 2012) (discussing online governance challenges); Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*, 5 INTERNET POL'Y REV., Sept. 30, 2016, at 10-15 (analyzing online governance challenges in Bitcoin).

162. *See supra* Part I.

163. *See* Werbach & Cornell, *supra* note 2, at 365.

164. *See* Heverly, *Revisiting the Information Semicommons*, *supra* note 117, at 138-42.

can modify and extend it to produce derivative smart contracts with different functionality.

Thus, the software *above* a blockchain clearly raises some of the same resource-governance issues as the software *beneath* it. Who pays for the effort invested in design, programming, and debugging? Should the code be free for reuse by the creators' competitors? Can participants in the smart-contract ecosystem trust the creators of the contract?

Answers to these and many other questions must be sought, and solutions come from many of the same mechanisms we have already seen at a lower level of the blockchain stack. Thus, for example, a number of smart-contract designs have their own consensus mechanisms that reuse and recombine consensus mechanisms developed to achieve consensus within a blockchain.[165]

C. Resource Consumption

Bitcoin-style proof-of-work consensus mechanisms are inefficient in a subtle but massive way. As long as the reward for generating a block times the probability of winning the nonce lottery is greater than the cost of mining (in hardware, electricity, et cetera), more miners will enter.[166] They will push the probability of winning down until the net marginal reward from additional mining effort equals exactly zero.[167]

But if users highly value the ledger the blockchain provides, then they will be willing to spend highly to have their transactions carried out. Users will push up the transaction fees—and hence the

---

165. *E.g.*, JACK PETERSON, JOSEPH KRUG, MICAH ZOLTU, AUSTIN K. WILLIAMS & STEPHANIE ALEXANDER, GITHUB, AUGUR: A DECENTRALIZED ORACLE AND PREDICTION MARKET PLATFORM (V2.0) (2022), https://github.com/AugurProject/whitepaper/releases/latest/download/augur-whitepaper-v2.pdf [https://perma.cc/B3ZY-QWCS]; LORENZ BREIDENBACH, CHRISTIAN CACHIN, BENEDICT CHAN, ALEX COVENTRY, STEVE ELLIS, ARI JUELS, FARINAZ KOUSHANFAR, ANDREW MILLER, BRENDAN MAGAURAN, DANIEL MOROZ, SERGEY NAZAROV, ALEXANDRU TOPLICEANU, FLORIAN TRAMÈR & FAN ZHANG, CHAINLINK, CHAINLINK 2.0: NEXT STEPS IN THE EVOLUTION OF DECENTRALIZED ORACLE NETWORKS (2021), https://research.chain.link/whitepaper-v2.pdf [https://perma.cc/H67P-2XP8]; *DAO User Guide*, DECENTRALAND, https://docs.decentraland.org/decentraland/dao-userguide/ [https://perma.cc/3NMP-33WZ].

166. *See* Gur Huberman, Jacob D. Leshno & Ciamac Moallemi, *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, 88 REV. ECON. STUD. 3011, 3020 (2021).

167. *See id.* at 3021-22.

rewards to miners—until the marginal value of having one's transaction processed faster exactly equals the additional fee one must pay to achieve it.[168] In equilibrium, therefore, the value the blockchain collectively delivers for users determines the level of effort miners collectively expend.[169] High prices for on-chain assets and high transaction fees induce a high level of mining.[170]

The result is that the most popular blockchains are immensely, inefficiently, wastefully *over*provisioned. A single entry-level laptop computer drawing perhaps fifty watts is easily able to store and maintain a modern blockchain.[171] And yet Bitcoin mining consumes 122 terawatt hours per year of electricity, about 0.5 percent of the world's entire electricity production, which is as much as Sweden or Norway.[172] The environmental consequences are catastrophic.[173]

Unfortunately, *some* redundancy is essential to trustworthiness. A centralized database is far more resource efficient, but it sacrifices the benefits of distributing ledger control among many participants.[174] Thus, a great deal of effort has been put into developing alternative "proof-of-stake" mechanisms, in which mining rewards are distributed to participants in proportion to how many on-chain assets they have at "stake" in the system.[175] Ethereum has been gearing up for a transition from proof-of-work to proof-of-stake for years,[176] and made the leap during the editing of this Article.[177]

This, too, is a governance problem. The previous Sections discussed the problem of *developing* protocols, but the process of

168. *See* Easley et al., *supra* note 125, at 106.

169. *See id.*

170. *See id.* at 99, 106.

171. *See* Alisa DiCaprio & Maya Marie, *Just How Energy Efficient Is Your Blockchain?*, R3 (Oct. 21, 2021), https://www.r3.com/blog/just-how-energy-efficient-is-your-blockchain/ [https://perma.cc/L8WJ-EDQQ].

172. *See Cambridge Bitcoin Electricity Consumption Index*, UNIV. OF CAMBRIDGE, https://ccaf.io/cbeci/index/comparisons [https://perma.cc/5J98-CDWS].

173. *See* Michaela Stones, *The Environmental Consequences of Cryptocurrency Mining*, N.Y. LEAGUE OF CONSERVATION VOTERS (Nov. 4, 2021), https://nylcv.org/news/the-environmental-consequences-of-cryptocurrency-mining/ [https://perma.cc/T88L-6H5B].

174. *See, e.g.*, Buterin, *supra* note 131.

175. *See id.*

176. *See Upgrading Ethereum to Radical New Heights*, ETHEREUM, https://ethereum.org/en/upgrades/ [https://perma.cc/M9EN-KN6M].

177. *See* David Yaffe-Bellany, *Crypto's Long-Awaited 'Merge' Reaches the Finish Line*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/ethereum-merge-crytpo.html [https://perma.cc/4GFJ-53TT].

debating and deciding which protocols to use is also governance. In blockchain communities, these debates take place across a riotous collection of mailing lists, blogs, news sites, and Discord servers.[178]

D. Tyranny of the Majority

In a "51% attack," a majority of the mining power on a proof-of-work blockchain collusively hijacks the ledger.[179] One way to do so is by ignoring proposed blocks that come from outside their cartel and accepting only proposed blocks from members.[180] If a cartel with more than half the mining power does so, then more than half the proposed new blocks will come from the cartel's efforts, which means that given long enough, the cartel is overwhelmingly likely to win the mining race against all possible competitors. Thus, all of the block rewards accrue to cartel members. The cartel can also collectively manipulate the contents of the ledger—for example, by refusing to recognize certain transactions from nonmembers or by changing the semantics of the protocol in self-favoring ways.[181]

Although the core idea of Nakamoto consensus is elegantly simple, it only holds under restrictive hypotheses. The game theory of 51-percent attacks gets very complicated, very quickly. For example, some results show that groups with *less* than a majority of mining power can still extract more than their proportional share in mining rewards.[182] Another point is that participants who are subject to a 51-percent attack can retaliate by withdrawing from the blockchain entirely, which functions as a threat to reduce the value of on-chain assets and potentially deter attacks in the first place.[183] In practice, the political maneuvering around mining pools and transaction processing is far more complicated than the simple picture of a single focal point suggests.

---

178. *See, e.g.*, Richard Yan, *The Blockchain Debate Podcast*, BUZZSPROUT, https://blockdebate.buzzsprout.com/ [https://perma.cc/6ZNM-T2GR].

179. *See* Kroll et al., *supra* note 122, at 11-12.

180. *See* Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, 18TH INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SEC. 436, 441-42 (2014).

181. *See* Kroll et al., *supra* note 122, at 11-12.

182. Eyal & Sirer, *supra* note 180, at 447.

183. *See* Kroll et al., *supra* note 122, at 11-12.

From a resource-governance perspective, what happens in a 51-percent attack is that the proof-of-work protocol's antitargeting properties break down. A cartel with more than half the mining power can prevent mining rewards from being scattered onto non-members.[184] Therefore, the cartel's members are able to connect private on-chain assets to their own private hardware in a way that disproportionately benefits themselves.

Another example of clever targeting involves "miner extractable value" (MEV), in which a clever miner can modify the contents of the ledger in a way that remains acceptable to other participants under the longest-chain convention but diverts some resources to themselves.[185] One type of MEV attack involves front-running proposed transactions so that the miner can capture for themselves value that a user intended to.[186] Another, called a "time-bandit attack," involves rolling back transactions already recorded in the blockchain to capture MEV from previous blocks.[187]

These are governance problems that no protocol can fully resolve. 51-percent attacks are inherent to the design of the Bitcoin proof-of-work consensus mechanism.[188] Different consensus mechanisms create their own opportunities for strategic behavior. For example, proof-of-stake mechanisms can display rich-get-richer phenomena, in which whales with large holdings are best able to and most incentivized to stake their holdings for additional rewards.[189] Blockchain-mechanism design is an area of immense practical and theoretical interest, but there is no silver-bullet protocol design that is fully incentive-compatible under all circumstances. The governance of a blockchain semicommons cannot be fully embedded in its protocol.

---

184. *See id.*

185. *See* Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach & Ari Juels, *Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability*, 2020 IEEE SYMP. ON SEC. & PRIV. 910, 911.

186. *See id.* at 912.

187. *See id.* at 921.

188. *See* Kroll et al., *supra* note 122, at 11-12.

189. *See, e.g.*, Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath & Gerui Wang, *Compounding of Wealth in Proof-of-Stake Cryptocurrencies*, 23D INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SEC. 42, 42-43 (2019); Yuming Huang, Jing Tang, Qianhao Cong, Andrew Lim & Jianliang Xu, *Do the Rich Get Richer? Fairness Analysis for Blockchain Incentives*, ACM SIGMOD INT'L CONF. ON MGMT. DATA 790 (2021).

E. Consensus Breakdown

A more fundamental governance issue is that blockchain protocols are not natural laws of the universe.[190] Protocols are creatures of consensus, and they last only as long as that consensus endures.[191] A nation's people can always scrap their constitution and write a new one, regardless of what the old one said. Similarly, a blockchain community can always collectively decide to modify its protocol. The old protocol does not have the power to stop them.[192]

Thus, the longest-chain convention, the semantics of a virtual machine, and other details of a protocol are not inviolate. Sometimes the community collectively decides to change; sometimes an influential participant steps in and persuades others to go along.[193] After the infamous "DAO Hack," for example, the Ethereum blockchain adopted a new one-off modification that unwound a particularly large transaction that many felt had been misappropriated.[194] Vitalik Buterin, the creator and visionary of Ethereum, presented this change as a necessary compromise to ensure the blockchain's long-term stability and acceptance.[195]

---

190. Another way of making this point is that the technical "decentralization" of a blockchain as a distributed system with a consensus protocol does not necessarily mean that a blockchain is decentralized in the sense of not having concentrations of power. *See* Angela Walch, *Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 39, 40-41 (Chris Brummer ed., 2019).

191. *See* Grimmelmann, *supra* note 10, at 17.

192. *See* Karen Yeung & David Galindo, *Why Do Public Blockchains Need Formal and Effective Internal Governance Mechanisms?*, 10 EUR. J. RISK REGUL. 359, 374-75 (2019) (arguing that off-chain consensus is necessary to serve as a Hartian rule of recognition making the state of a blockchain authoritative); *cf.* Wessel Reijers, Iris Wuisman, Morshed Mannan, Primavera De Filippi, Christopher Wray, Vienna Rae-Looi, Angela Cubillos Vélez & Liav Orgad, *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, 40 TOPOI 821 (2021) (describing on-chain governance as a Kelsenian positivist legal order and subjecting it to the Schmittian critique of the state of exception).

193. *See, e.g.*, Haque et al., *supra* note 152, at 156-66 (describing social process by which protocol changes are proposed, agreed to, and made); Sarah Azouvi, Mary Maller & Sarah Meiklejohn, *Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance*, 2018 FIN. CRYPTOGRAPHY & DATA SEC. 127 (analyzing distribution of contributions to code and discussions).

194. *See* Grimmelmann, *supra* note 10, at 17-19.

195. *See* Vitalik Buterin, *Onward from the Hard Fork*, ETHEREUM FOUND. BLOG (July 26, 2016), https://blog.ethereum.org/2016/07/26/onward-from-the-hard-fork [https://perma.cc/AYC4-GQMU].

The debates over whether to make these changes are inherently political.[196] Unwinding the DAO Hack required taking a large quantity of Ether from one user's address and returning it to other users' addresses.[197] *Not* unwinding the hack was equivalent to saying that the user who found and exploited a bug in a smart contract's design was entitled to keep all of the Ether they drained from an investment club's joint account.[198]

These, too, are governance disputes. The work required to achieve blockchain consensus becomes most visible in the cases where it breaks down, where people genuinely argue over what the blockchain ledger ought to say. In the DAO Hack case, the dispute was serious enough that the Ethereum blockchain forked into two mutually incompatible communities.[199] One of the communities unwound the hack in its version of the ledger; the other did not.[200]

F. Inherent Instability

A pervasive source of instability in blockchain resource systems is that they are built using software. No large software project is ever completely finished or free of bugs. In particular, blockchains have seen so many bugs and exploits that entire websites are dedicated to tracking them.[201] The need to modify and upgrade blockchain protocols and software to bring them into line with the intended design never goes away, and neither does the need to reconsider the design itself in light of bitter experience. Therefore, every blockchain is always and forever in motion; it evolves over time as part of the normal lifecycle of software. This evolution requires governance work, even if it takes place stably and invisibly—*especially* to make it take place stably and invisibly.

---

196. *See* Barton E. Lee, Daniel J. Moroz & David C. Parkes, An Analysis of Blockchain Governance via Political Economics (Sept. 8, 2021) (unpublished manuscript), https://www.dropbox.com/s/adfvbeslt20hqpq/Lee_Moroz_Parkes-2019.pdf [https://perma.cc/2FTA-LNUW] (analyzing blockchain forks using tools from economics and political science).

197. *See* Grimmelmann, *supra* note 10, at 18.

198. *See id.*

199. *See id.*

200. *See id.*

201. *See, e.g.*, Molly White, WEB3 IS GOING JUST GREAT, https://web3isgoinggreat.com [https://perma.cc/TV6B-RFZA]; *Documented Timeline of Exchange Hacks*, CRYPTOSEC, https://cryptosec.info/exchange-hacks/ [https://perma.cc/Z2S4-CA4U] (last updated Jan. 9, 2022).

Similarly, using on-chain assets as incentives creates complex and poorly understood reward systems that depend on emergent social behavior. For example, the Terra algorithmic stablecoin depended on user perception that the on-chain assets being exchanged for each other would retain enough value that Terra's governance foundation could always successfully defend its peg.[202] After the stablecoin briefly broke a buck, the confidence deflated like a popped balloon.[203] It hovered very slightly under a dollar for several days before collapsing completely.[204] The crowd dynamics that at first maintained, and then destroyed, the Terra peg cannot be captured in its protocol, and yet they are essential to understanding Terra as a resource system. The massive price volatility of Bitcoin and other cryptocurrencies similarly means that these resource systems are coupled to the broader economy in ways that can both promote and undermine their governance mechanisms.[205]

Even functioning semicommons are vulnerable to changes in prices or production technology. Landlords ultimately enclosed the open-field semicommons.[206] In a blockchain, the temptation is always to add more epicycles to the protocol: new staking mechanisms, new abuse mitigations, et cetera. But no protocol can solve all governance problems. Constant technological and social change mean that the incentives, threats, and design alternatives for blockchains are always shifting. The design parameters that make sense for a low-transaction-volume store of value for people distrustful of governmental authority are completely inappropriate for a system for low-risk, high-volume international remittances, and neither of them is well suited to a general-purpose distributed computer intended to provide a platform for worldwide collaboration.[207] The shifting mix of private and public values means that no blockchain

---

202. *See* Matt Levine, Opinion, *Terra Flops*, BLOOMBERG (May 11, 2022, 1:44 PM), https://www.bloomberg.com/opinion/articles/2022-05-11/terra-flops [https://perma.cc/S3C5-LXSP].

203. *See id.*

204. *See id.*

205. *See* Nicole Lapin, *Explaining Crypto's Volatility*, FORBES (Dec. 23, 2021, 6:00 AM), https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/?sh=5f885a997b54 [https://perma.cc/W7WB-HEDK].

206. *See* Smith, *supra* note 96, at 160-61.

207. *See* BUTERIN, *supra* note 25, at 13 (defining goals for Ethereum).

resource system instantiates the right governance institution for all places and all times.

CONCLUSION

Blockchains are not just scams, hype, and carbon emissions. There is something novel, nonobvious, and possibly useful here. Blockchains are a clever new way of providing ledger infrastructure. Their decentralization avoids some familiar corruption problems. And semicommons mechanisms address some familiar incentive problems of decentralization. But as we have shown, blockchains face governance and incentive challenges of their own—challenges that can be appreciated and confronted by thinking about blockchains as infrastructural resource systems.

Our description of blockchain governance helps make sense of a paradox in blockchain rhetoric. On the one hand, blockchain advocates proudly point to the "trustless" nature of blockchains: participants supposedly can rely on technical features of blockchains to protect them, rather than on social relations.[208] On the other hand, blockchain advocates also proudly point to the importance of blockchain communities; they celebrate the social relations participants forge by joining with each other to promote the blockchain vision.[209] Which is it, skeptics ask? Are blockchains about individuals who are perfectly independent of one another, or are they about communities richly bound together by social ties? Why does a trustless world need blockchain communities?

---

208. *See, e.g.*, SATOSHI NAKAMOTO, BITCOIN, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1, https://bitcoin.org/bitcoin.pdf [https://perma.cc/344A-D9DU] ("What is needed is an electronic payment system based on cryptographic proof instead of trust."); Nick Szabo, *Trusted Third Parties Are Security Holes*, NAKAMOTO INST. (2005), https://nakamotoinstitute.org/trusted-third-parties/ [https://perma.cc/S3SY-DCG3]. For sophisticated analyses of what "trust" means in this context, see Rebecca M. Bratspies, *Cryptocurrency and the Myth of the Trustless Transaction*, 25 MICH. TECH. L. REV. 1 (2018); WERBACH, *supra* note 8; Bill Maurer, Taylor C. Nelms & Lana Swartz, *"When Perhaps the Real Problem Is Money Itself!": The Practical Materiality of Bitcoin*, 23 SOC. SEMIOTICS 261 (2013).

209. *See, e.g.*, Mia Sato, *A Trip to the GaryVee Convention, Where Everyone Is Part of Crypto's 1 Percent*, THE VERGE (June 10, 2022, 9:00 AM), https://www.theverge.com/23160201/gary-vaynerchuk-veecon-veefriends-nfts-web3-conference-crypto [https://perma.cc/FEY4-D2UV]; Kevin Roose, *Crypto Is Cool. Now Get on the Yacht*, N.Y. TIMES (Nov. 5, 2021), https://www.nytimes.com/2021/11/05/technology/nft-nyc-metaverse.html [https://perma.cc/KCR2-QMWS].

The paradox dissolves when one realizes that purely technical descriptions of how blockchains "work" cannot be taken at face value. Blockchains are technosocial systems, not just technologies. On-chain stability is possible only because participants engage in extensive off-chain governance work. The crowds of blockchain believers encouraging each other to HODL on Discord, or milling along listlessly while LCD Soundsystem plays at the NFT.NYC conference, are central to blockchains, not peripheral to them.[210] What participants do off-chain matters just as much as what they do on-chain.

Scholars and developers must pay close attention to *actual* blockchain governance mechanisms, not just the ones formally instantiated in protocols and code. Collective community governance decisions are routine, not exceptions. They are a feature, not a bug. And they make blockchains work.

210. *See* Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, 62 TECH. SOC'Y, Aug. 2020, at 7-8.