Trust, but Verify

Author(s): Kevin Werbach

Source: *Berkeley Technology Law Journal*, 2018, Vol. 33, No. 2 (2018), pp. 487-550

Published by: University of California, Berkeley, School of Law

Stable URL: https://www.jstor.org/stable/10.2307/26533144

TRUST, BUT VERIFY: WHY THE BLOCKCHAIN NEEDS THE LAW

Kevin Werbach†

ABSTRACT

The blockchain could be the most consequential development in information technology since the Internet. Created to support the Bitcoin digital currency, the blockchain is actually something deeper: a novel solution to the age-old human problem of trust. Its potential is extraordinary. Yet, this approach may not promote trust at all without effective governance. Wholly divorced from legal enforcement, blockchain-based systems may be counterproductive or even dangerous. And they are less insulated from the law's reach than it seems. The central question is not how to regulate blockchains but how blockchains regulate. They may supplement, complement, or substitute for legal enforcement. Excessive or premature application of rigid legal obligations will stymie innovation and forego opportunities to leverage technology to achieve public policy objectives. Blockchain developers and legal institutions can work together. Each must recognize the unique affordances of the other system.

DOI: https://doi.org/10.15779/Z38H41JM9N.

† Associate Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania. Email: werbach@wharton.upenn.edu. Thanks to Dan Hunter for collaborating to develop the ideas that gave rise to this Article, and to Sarah Light, Patrick Murck, and participants in the 2017 Lastowka Cyberlaw Colloquium and 2016 TPRC Conference for comments on earlier drafts.

TABLE OF CONTENTS

I. INTRODUCTION: CODE'S REVENGE

The blockchain[1] has been called "[t]he technology most likely to change the next decade of business."[2] It has also been described as a haven for criminal activity,[3] a Ponzi scheme,[4] and a road both to anarchy[5] and to authoritarianism.[6] The root of this confusion is the blockchain's uncertain relationship to law. Proponents of blockchain technology describe it as a democratizing escape from the failings of territorial legal systems. Critics see it as a clever trick to avoid legal accountability. Neither is entirely correct…or entirely wrong. Both perspectives focus excessively on regulation of blockchains and not enough on how blockchains regulate. To achieve their monumental potential and avoid catastrophic failures, blockchain-based systems will need to integrate with the operations and institutions of the law.

From its roots in the Bitcoin cryptocurrency,[7] launched in 2009 by the pseudonymous Satoshi Nakamoto, the blockchain has rapidly taken hold around the world. The price of bitcoin jumped twenty-fold between late 2016 and the end of 2017, and other cryptocurrencies experienced similar appreciation.[8] Venture capitalists poured over $1 billion into blockchain-based

1. There is not yet agreement on terminology. Technically, a blockchain (sometimes written as "block chain") is a data storage system using sequentially signed blocks, as described in Part II. "The blockchain" may describe the universe of blockchains (similar to "the Internet"), the subset of public blockchains, or just the public ledger for Bitcoin.
Adding further confusion, some "blockchain" platforms use neither chains of blocks nor Bitcoin-like digital currencies. The more accurate term for this class of systems is distributed ledger technology (DLT).

2. *See* Don Tapscott & Alex Tapscott, *The Impact of the Blockchain Goes Beyond Financial Services*, HARV. BUS. REV. (May 10, 2016), https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services [https://perma.cc/7M3G-XUQY].

3. *See* Kim Zetter, *FBI Fears Bitcoin's Popularity with Criminals*, WIRED (May 9, 2012), https://www.wired.com/2012/05/fbi-fears-bitcoin/ [https://perma.cc/2LCF-XPQK].

4. *See* Matt O'Brien, *Bitcoin Isn't the Future of Money—It's Either a Ponzi Scheme or a Pyramid Scheme*, WASH. POST: WONKBLOG (June 8, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/ [https://perma.cc/6MDJ-U6PY].

5. *See* Matthew Sparkes, *The Coming Digital Anarchy*, TELEGRAPH (June 9, 2014), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html [https://perma.cc/T4LT-BXRK].

6. *See* Ian Bogost, *Cryptocurrency Might Be a Path to Authoritarianism*, ATLANTIC (May 30, 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/ [https://perma.cc/UU6F-7MFW].

7. A cryptocurrency is a form of digital money secured not through the backing of a state or financial institution, but through cryptography. *See infra* Section II.A. In this Article, the term Bitcoin is capitalized when describing the system as a whole, and lower case when referring to the unit of currency.

8. *See* Nathaniel Popper, *Bitcoin's Price Has Soared. What Comes Next?*, N.Y. TIMES (Dec.

startups between 2013 and 2016.[9] Blockchain projects themselves topped that in 2017, raising over $5 billion[10] selling digital tokens directly to users and investors.

The wave of blockchain adoption is not limited to entrepreneurial ventures. Technology giants such as IBM, Microsoft, and Intel are making major blockchain commitments,[11] as are leading professional services firms such as PwC and KPMG.[12] Directly or through consortia, virtually all the world's largest financial institutions are implementing distributed ledger technology based on similar principles.[13] Governments are getting into the act as well. Several are experimenting with distributed ledger platforms, and the world's central banks, from the Bank of England to the People's Bank of China, are studying the potential of issuing their own cryptocurrencies.[14] Even relatively sober observers such as Goldman Sachs see tens of billions of dollars in annual benefits just from low-hanging fruit opportunities.[15] While the near-

7, 2017), https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html [https://perma.cc/XW86-8AMW].

9. *See* Garrick Hileman, *State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin*, COINDESK (May 11, 2016), http://www.coindesk.com/state-of-blockchain-q1-2016/ [https://perma.cc/LC42-4Z7Y].

10. *See* Oscar Williams-Grut, *Only 48% of ICOs Were Successful Last Year—but Startups Still Managed to Raise $5.6 Billion*, BUS. INSIDER (Jan. 31, 2018), http://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1 [https://perma.cc/LP6N-U7H5].

11. *See* Anna Irrera, *Microsoft Unveils Technology to Speed Up Blockchain and Its Adoption*, REUTERS (Aug. 10, 2017), https://www.reuters.com/article/us-microsoft-blockchain-idUSKBN1AQ1KD [https://perma.cc/PV7M-SMB7]; Jeff John Roberts, *Can IBM Really Make a Business Out of Blockchain?*, FORTUNE (June 28, 2016), http://fortune.com/2016/06/28/ibm-blockchain/ [https://perma.cc/T6GH-VP6B].

12. *See Blockchain Services*, PRICEWATERHOUSECOOPERS, https://www.pwc.com/us/en/financial-services/fintech/blockchain.html [https://perma.cc/ND35-7P5T] (last visited Apr. 10, 2018); *Digital Ledger Services at KPMG: Seize the Potential of Blockchain Today*, KPMG, https://home.kpmg.com/xx/en/home/insights/2017/02/digital-ledger-services-at-kpmg-fs.html [https://perma.cc/8KLG-AUZM] (last visited Aug. 17, 2018).

13. *See* Nathaniel Popper, *Envisioning Bitcoin's Technology at the Heart of Global Finance*, N.Y. TIMES (Aug. 12, 2016), http://www.nytimes.com/2016/08/13/business/dealbook/bitcoin-blockchain-banking-finance.html [https://perma.cc/NT2P-P2CT] ("The report estimates that 80 percent of banks around the world could start distributed ledger projects by next year.").

14. *See* John Barrdear & Michael Kumhof, *The Macroeconomics of Central Bank Issued Digital Currencies* 3 (Bank of England, Staff Working Paper No. 605, 2016), http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf [https://perma.cc/QJV3-MNTT]; Chuan Tian, *China's Central Bank Opens New Digital Currency Research Institute*, COINDESK (June 30, 2017), https://www.coindesk.com/chinas-central-bank-opens-new-digital-currency-research-institute/ [https://perma.cc/3GRF-L7C3].

15. *See* James Schneider et al., *Blockchain: Putting Theory into Practice*, GOLDMAN SACHS EQUITY RES. 4 (May 24, 2016), https://www.scribd.com/doc/313839001/Profiles-in

term impacts of the blockchain may be overhyped, its long-term potential as a distributed foundation for the exchange of value is extraordinary.[16]

Blockchains use complex technology, but their basic function is simple: providing a distributed yet provably accurate record. Everyone can maintain a copy of a dynamically-updated ledger, but all those copies remain the same, even without a central administrator or master version.[17] This approach offers two basic benefits. First, one can have confidence in transactions without trusting the integrity of any individuals, intermediaries, or governments. Second, the single distributed ledger replaces many private ledgers that must be reconciled for consistency, thus reducing transaction costs. The software enabling this uses digital cryptography and game-theoretic incentives to make it difficult to cheat the system.

The initial interest in blockchains focused on Bitcoin as a private digital currency outside the control of territorial governments. Traditionally, currency transactions are heavily regulated to address concerns about fraud, money laundering, capital flight, currency manipulation, terrorist financing, and more.[18] Governments and powerful private interests have also prevailed on banks or payment processors to cut off services involved in gambling, distribution of copyrighted material, or dissemination of leaked government documents, even when such conduct was not clearly illegal in some jurisdictions. Bitcoin appears to operate as a store of value and a mechanism for transactions without any such constraints. It raises the tantalizing prospect (for some) of "censorship-proof" money.

On the other hand, unregulated currency can easily become a haven for lawlessness, consumer abuses, and financial speculation.[19] For some time, Bitcoin had a somewhat unsavory reputation. The early Bitcoin-based marketplace Silk Road, which was used primarily for drugs and other contraband, is the most spectacular example.[20] It was eventually shut down by

-Innovation-May-24-2016-1 [https://perma.cc/93FJ-EEDW].

16. *See* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Jan./Feb. 2017), https://hbr.org/2017/01/the-truth-about-blockchain [https://perma.cc/XEH4-YUE2] (describing the vast potential of the blockchain as a foundational technology, which will nonetheless take time to be realized fully).

17. A detailed explanation of how the blockchain achieves this paradoxical result is provided in Part II.

18. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 19 (2014); JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 43–47 (2013).

19. *See* HOMELAND SEC. STUDIES & ANALYSIS INST., RISKS AND THREATS OF CRYPTOCURRENCIES 2–3 (2014), https://www.anser.org/docs/reports/RP14-01.03.03-02_Cryptocurrencies 508_31Dec2014.pdf [https://perma.cc/6MYY-DLX5].

20. *See* David Yermack, *Is Bitcoin a Real Currency?* 6 (Nat'l Bureau of Econ. Research,

the FBI in 2013, and its operator, Ross Ulbricht, was sentenced to life in prison. However, during its three years of operation, Silk Road processed sales worth 9.5 million Bitcoin, or roughly $1.2 billion at the time.[21] Although legitimate applications have multiplied since then, the question whether Bitcoin and its progeny are the world's greatest gift to criminals remains.

While it seemingly precludes traditional legal enforcement, a blockchain-based system's software enforces its own rules in a manner analogous to the legal system. It thus illustrates the foundational insight of cyberlaw scholar Lawrence Lessig's 1999 book, *Code and Other Laws of Cyberspace*: code is law.[22] As in the 1990s, when peer-to-peer file sharing seemed on the verge of transforming copyright and free speech online seemed immune from government repression, those who seek to overturn existing power dynamics are invigorated. Legal scholars Aaron Wright and Primavera de Filippi, for example, argue that the blockchain "could make it easier for citizens to create custom legal systems, where people are free to choose and to implement their own rules within their own techno-legal frameworks."[23] Cyber-libertarianism remains a beautiful dream. But the idea that all online communities will successfully enforce their own rules, without regard for governments, will fare as poorly as it did the first time. It already has.

Over a few weeks in mid-2016, some 11,000 individuals worldwide committed Ether cryptocurrency worth roughly $150 million to a blockchain-based virtual company with no employees, no management, and no legal existence.[24] The DAO, short for "distributed autonomous organization," was

Working Paper No. 19747, 2013), http://www.nber.org/papers/w19747.pdf [https://perma.cc/Z53K-SG9T]; Joshuah Bearman, *The Rise and Fall of Silk Road: Part II*, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2 [https://perma.cc/L3G2-BUAG]; Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [https://perma.cc/5V47-EB6S].

21. Sealed Complaint at 15, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 14-cr-68), https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html [https://perma.cc/2FNK-F37V]. At that point, the total supply of Bitcoin was only about twelve million.

22. *See generally* LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999). Lessig published an updated version of the book in 2006, to incorporate new developments such as social media. *See generally* LAWRENCE LESSIG, CODE VERSION 2.0 (2006) [hereinafter CODE VERSION 2.0].

23. *See* Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia 40 (unpublished manuscript) (Mar. 12, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/3YUP-PNM4].

24. *See* Nathaniel Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, N.Y. TIMES (May 21, 2016), https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html [https://perma.cc/4DWV-VETX]; Joon Ian Wong, *The Price of Ether, a Bitcoin Rival, Is Soaring Because of a Radical, $150 Million Experiment*, QUARTZ (May

an online crowdfunding system built entirely out of self-executing software known as smart contracts.[25] It was hailed as "[a] new paradigm of economic cooperation . . . a digital democratization of business."[26] Autonomous code, running on a distributed platform with no central authority, took the place of law, intermediaries, and personal relationships as the instrument of trust. And then someone stole a third of the money overnight.[27]

That is when things got interesting.[28] According to The DAO's software, the siphoning off of funds was entirely legitimate. The blockchain had no way to distinguish between a thief and a customer.[29] More seriously, the immutability of blockchain records meant that no one had the power to stop or reverse the theft.[30] Eventually, the entire blockchain platform The DAO operated on had to be split in half in order to restore the funds.[31] A renegade group disagreed with this decision, so it began operating a duplicate currency

20, 2016), https://qz.com/688194/the-price-of-ether-a-bitcoin-rival-is-soaring-because-of-a-radical-150-million-experiment/ [https://perma.cc/UYM2-PVUX].

25. *See generally* Christoph Jentzsch, Decentralized Autonomous Organization to Automate Governance (unpublished manuscript) https://download.slock.it/public/DAO/WhitePaper.pdf [https://perma.cc/4B6L-BW68] (last visited Aug. 18, 2018) (describing the structure and functions of The DAO). For a more detailed discussion of smart contracts, see generally Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017); Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2017); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017).

26. Seth Bannon, *The Tao of "The DAO" or: How the Autonomous Corporation Is Already Here*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/ [https://perma.cc/V5Z3-B6JC].

27. *See* Klint Finley, *A $50 Million Hack Just Showed that the DAO Was All Too Human*, WIRED (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [https://perma.cc/4V66-8ARF]; Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html [https://perma.cc/QFQ5-B528].

28. One account described the subsequent events as "arguably the most philosophically interesting event to take place in your lifetime or mine." E.J. Spode, *The Great Cryptocurrency Heist*, AEON (Feb. 14, 2017), https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum [https://perma.cc/9HGW-9SEA].

29. *See* Vitalik Buterin, *Thinking About Smart Contract Security*, ETHEREUM BLOG (June 19, 2016), https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security/ [https://perma.cc/TP5M-SBPN] ("All instances of smart contract theft or loss—in fact, *the very definition* of smart contract theft or loss, is fundamentally about differences between implementation and intent.").

30. *See* Finley, *supra* note 27 ("If people can simply reverse transactions they didn't mean to make, it proves that people, not mathematics are really in charge of the system . . . .").

31. Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (July 20, 2016), http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/ [https://perma.cc/EK4R-XTAU].

where the thief kept the stolen funds.[32] The story sounds bizarre, but it is a harbinger of things to come. The DAO's software worked exactly as designed to replace legal enforcement and third-party intermediaries. Yet that created its own problems. There was verification, but a breakdown in trust. Users only got their money back because the supposedly immutable, unstoppable blockchain actually was not.

The DAO incident is emblematic of deeper issues. The reason the blockchain needs law is that both the blockchain and the law are, at their core, mechanisms of trust. Distributed ledger technology allows participants to trust the outcome of a system without trusting any individual participant. Yet trust implies uncertainty or vulnerability.[33] That is why President Reagan's favorite Russian proverb,[34] the title of this Article, is often criticized as meaningless: "If you trust, you won't insist on verifying, whereas if you insist on verifying, clearly you don't trust."[35] The blockchain is an ingenious solution for verification but to promote trust requires something more. That is where the legal system comes in play.

Even if the math works perfectly, blockchains are systems designed, implemented, and used by humans. Subjective intent remains relevant even when expressed through objective code. Blockchains are vulnerable to selfish behavior, attacks, and manipulation.[36] By 2016, there were already at least fifteen incidents in which cryptocurrency worth at least $1 million was stolen, with a total value exceeding $600 million.[37] And the scope of theft only

32. Paul Vigna, *The Great Digital-Currency Debate: 'New' Ethereum Vs. Ethereum 'Classic'*, WALL ST. J. (Aug. 1, 2016), http://blogs.wsj.com/moneybeat/2016/08/01/the-great-digital-currency-debate-new-ethereum-vs-ethereum-classic/ [https://perma.cc/D5CZ-DYUU].

33. *See* Roger C. Mayer et al., *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709, 712–14, (1995); Helen Nissenbaum, *Will Security Enhance Trust Online, or Supplant It*, *in* TRUST AND DISTRUST IN ORGANIZATIONS: DILEMMAS AND APPROACHES 155, 173 (Roderick M. Kramer & Karen S. Cook eds., 2004); Denise M. Rousseau et al., *Not So Different After All: A Cross-Discipline View of Trust*, 23 ACAD. MGMT. REV. 393, 394–95 (1998).

34. Reagan famously used this aphorism at the signing ceremony for the Intermediate-Range Nuclear Forces treaty with the Soviet Union in 1987. Soviet leader Mikhail Gorbachev remarked with exasperation, "You repeat that at every meeting." *See* DAVID E. HOFFMAN, THE DEAD HAND: THE UNTOLD STORY OF THE COLD WAR ARMS RACE AND ITS DANGEROUS LEGACY 295 (2009). The aphorism works better in the original Russian, because the two verbs rhyme and derive from the same root.

35. Barton Swaim, *'Trust, but Verify': An Untrustworthy Political Phrase*, WASH. POST (Mar. 11, 2016), https://www.washingtonpost.com/opinions/trust-but-verify-an-untrustworthy-political-phrase/2016/03/11/da32fb08-db3b-11e5-891a-4ed04f4213e8_story.html [https://perma.cc/QR8E-ZFMU].

36. *See infra* Section III.A (describing various attacks on blockchain systems or uses of the technology to commit fraud).

37. *See* Michael Matthews, *List of Bitcoin Hacks (2012-2016)*, STEEMIT (Aug. 20, 2016), https://steemit.com/bitcoin/@michaelmatthews/list-of-bitcoin-hacks-2012-2016

increased after that, as cryptocurrency prices skyrocketed in 2017.[38] The scope of legitimate practices for blockchain-based systems is fundamentally a governance question, not a computer science one. Without realizing it, blockchain developers have wandered into territories that legal scholars have fought over for centuries.

The challenge, therefore, is what happens when ledgers meet law? Legal structures such as contracts, property, corporations, and judicial enforcement replace interpersonal trust with more structured rights, expectations, and remedies. Yet there are places the legal system cannot go, and sometimes the very formalization that law imposes is an impediment to trust. The blockchain offers a tantalizing solution. Realizing its potential, however, will require a careful mapping of the respective roles of the "dry code" of cryptography and the "wet code" of law.[39] And surprisingly, developers of blockchain-based systems will often need to incorporate both. Even at this early stage, several hybrid solutions are under development, including regulatory mechanisms, technical approaches, and new dispute resolution techniques.[40] Some make legal institutions operate more like software code; others make the blockchain's code more consistent with law.

It is a mistake, therefore, to see law and the blockchain as necessarily enemies. Legal actors can make mistakes, but so can software designers. There have been many serious failures already in the blockchain's short history; The DAO is just one example. Developing the rules, norms, incentives, and technical architectures[41] for a well-functioning community is a very hard problem. There are points where law needs to adapt to recognize the potential of the blockchain, but the reverse is also true: the blockchain needs law. Its impact will depend on its developers' ability to connect Satoshi Nakamoto's cryptoeconomic trust model with the formal structures and institutions of legal enforcement.

[https://perma.cc/LK3V-8MJ5].

38. *See* Anna Irrera, *More Than 10 Percent of $3.7 Billion Raised in ICOs Has Been Stolen: Ernst & Young*, REUTERS (Jan. 22, 2018), https://www.reuters.com/article/us-ico-ernst-young/more-than-10-percent-of-3-7-billion-raised-in-icos-has-been-stolen-ernst-young-idUSKBN1FB1MZ [https://perma.cc/V3QG-D8CS]; Nathaniel Popper, *As Bitcoin Bubble Loses Air, Frauds and Flaws Rise to Surface*, N.Y. TIMES (Feb. 5, 2018), https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html [https://perma.cc/J4S4-PLKP].

39. The terms "wet code" and "dry code" come from smart contracts inventor Nick Szabo. *See* Nick Szabo, *Wet Code and Dry*, UNENUMERATED (Aug. 24, 2008), http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html [https://perma.cc/B8QB-YRMC].

40. *See infra* Sections IV.A, IV.B.

41. These represent the four "things that regulate" in Lessig's model. *See* CODE VERSION 2.0, *supra* note 22.

This Article defends the contrarian claim that law is the blockchain's destiny, not its undoing. Much of the legal scholarship in this area concentrates on regulation of cryptocurrencies.[42] While there are many challenges to resolve about the legal treatment of Bitcoin and its progeny, the more fundamental question is whether they can displace traditional law entirely. They cannot. Part II of this Article describes the technical features of the blockchain architecture and explains why it is seeing such rapid adoption. Part III shows how blockchain-based systems go wrong when they stray too far from legal enforcement. Part IV describes the emerging governance hybrids that connect cryptocurrency code with law. Part V concludes. The blockchain could indeed become a transformative technology for business, government, and society on the scale of the Internet, but only if it reaches accommodations with law.

II. HERE COMES THE BLOCKCHAIN

In just a few years, Bitcoin and the blockchain have sparked extraordinary excitement and activity in the technology world.[43] Leading figures equate them

42. *See generally* Jerry Brito et al., *Bitcoin Financial Regulation: Securities*, *Derivatives*, *Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144 (2015); Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441 (2014); Joshua J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119 (2013); Paul H. Farmer, Jr., *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85 (2014); Andres Guadamuz & Chris Marsden, *Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies*, 20 FIRST MONDAY (2015), http://firstmonday.org/ojs/index.php/fm/article/view/6198/5163 [https://perma.cc/QXC8-E5NU]; Nikolei M. Kaplanov, *Nerdy Money: Bitcoin*, *the Private Digital Currency*, *and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111 (2012); Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015); Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813 (2014); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015); Wright & De Filippi, *supra* note 23; Ruoke Yang, *When Is Bitcoin a Security Under U.S. Securities Law?*, 18 J.L. TECH. & POL'Y 99 (2013).

43. *See*, *e.g.*, Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters [https://perma.cc/RK6A-M5J4]; Amy Cortese, *Blockchain Technology Ushers in the "Internet of Value"*, CISCO (Feb. 10, 2016), https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1741667 [https://perma.cc/KX8X-P4V8]; Jerry Cuomo, *How Businesses and Governments Can Capitalize on Blockchain*, FORBES (Mar. 17, 2016), http://www.forbes.com/sites/ibm/2016/03/17/how-businesses-and-governments-can-capitalize-on-blockchain/ [http://archive.is/HYwR7] (calling the blockchain a "revolutionary technology"); Reid Hoffman, *Reid Hoffman: Why the Blockchain Matters*, WIRED (May 15, 2015), https://www.wired.co.uk/article/bitcoin-reid-hoffman [https://perma.cc/VU4U-LV5M]; MARK WALPORT, U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 4 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/

with nothing less than a new Internet: a radically powerful, open, and distributed platform that will enable a vast economy of new and enhanced digital services.[44] Some say they could prevent future financial crises[45] or even "transform business, government, and society."[46] Others suggest the blockchain heralds a new form of private law, which may supersede government-based institutions.[47] For libertarians, these technologies represent economic activity outside the bounds of sovereign state control. For progressives, they promise to undermine entrenched private power. For others, they are simply a huge opportunity to make money or solve problems.

The magic of distributed ledgers is to make certain activities trustworthy without the need to trust anyone in particular.[48] Billionaire entrepreneur and

gs-16-1-distributed-ledger-technology.pdf [https://perma.cc/X4C3-HQPV] ("In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation."); UBS, BUILDING THE TRUST ENGINE 5 (2016), https://www.ubs.com/microsites/blockchain-report/en/home/ [https://perma.cc/H66V-Q8DH] ("Like many of our peers, we at UBS believe the blockchain is a potentially transformative technology . . . ."); ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 2 (2016) ("Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world."); DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 8–9 (2016); Popper, *supra* note 13 ("A new report from the World Economic Forum predicts that the underlying technology introduced by the virtual currency Bitcoin will come to occupy a central place in the global financial system.").

44. *See* Cadie Thompson, *Bitcoin Transformative as the Web*, *Venture Capitalist Says*, CNBC (Jan. 28, 2014), http://www.cnbc.com/2014/01/28/bitcoin-transformative-as-the-web-venture-capitalist-says.html [https://perma.cc/K5D7-ET6W]; Scott Rosenberg, *How Bitcoin's Blockchain Could Power an Alternate Internet*, WIRED (Jan. 13, 2015), https://www.wired.com/2015/01/how-bitcoins-blockchain-could-power-an-alternate-internet/ [https://perma.cc/29VW-KCPD]; Peter Spence, *Bitcoin Revolution Could Be the Next Internet, Says Bank of England*, TELEGRAPH (Feb. 25, 2015), http://www.telegraph.co.uk/finance/currency/11434904/Bitcoin-revolution-could-be-the-next-Internet-says-Bank-of-England.html [https://perma.cc/WX5U-38EM]; Daniel Folkinshteyn, Mark Lennon & Tim Reilly, *A Tale of Twin Tech: Bitcoin and the WWW*, 10 J. STRATEGIC & INT'L STUD. 82 (2015).

45. *See Bring on the Blockchain Future*, BLOOMBERG (June 6, 2016), http://www.bloomberg.com/view/articles/2016-06-06/bring-on-the-blockchain-future [https://perma.cc/5D6X-JFDP] ("The blockchain really could change the world . . . .").

46. Tapscott & Tapscott, *supra* note 2. Going even further, Skype co-founder Jaan Tallinn believes the blockchain can be used to overcome the tragedy of the commons and solve some of humanity's greatest challenges. *See* Rebecca Burn-Callander, *Skype Inventor Jaan Tallinn Wants to Use Bitcoin Technology to Save the World*, TELEGRAPH (June 20, 2016), http://www.telegraph.co.uk/business/2016/06/20/skype-inventor-jaan-tallinn-wants-to-use-bitcoin-technology-to-s/ [https://perma.cc/GNT3-4KWM].

47. *See* Wright & De Filippi, *supra* note 23, at 40–41; Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 404 (2016).

48. *See* Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 814 (2015) ("Bitcoin

venture capitalist Reid Hoffman calls this "trustless trust."[49] Blockchain proponents argue that costly mechanisms of intermediation and legal enforcement can be dispensed with. Instead of trusting banks and courts and governments, proponents suggest that we can trust math and computation, in the form of open-source cryptographic protocols.

A. HOW THE BLOCKCHAIN WORKS

The blockchain was first described in a paper distributed online in late 2008 by someone (or some group) using the pseudonym Satoshi Nakamoto.[50] Many of the concepts in Nakamoto's paper were familiar to cryptographers, but the system was implemented in a novel and elegant way to create a private, decentralized form of digital cash, called bitcoin. The Bitcoin network was implemented in open source software in 2009 and has been operating ever since. Exchanges around the world sprung up to trade bitcoin for fiat currencies such as dollars or euros. A collection of developers works to improve the Bitcoin software—Nakamoto was last heard from in 2011—and "miners" around the world provide computing power to secure the network. One bitcoin now costs thousands of dollars to purchase on an exchange.[51]

Bitcoin was the first production of the blockchain system. In subsequent years, many others were created, differing from the Bitcoin network in various ways. Some of them, like Ripple, which facilitates cross-border currency exchange between financial services providers, are optimized for specific purposes.[52] Others, like Ethereum, are designed as general-purpose platforms.[53] These other blockchains still have a native cryptocurrency token that can be traded, but it is a means to an end. The primary purpose of their currencies is to incentivize activity. Another class of systems, called permissioned ledgers, have no cryptocurrency because they are designed for private groups of firms to share information or transactions. The leading two examples are Hyperledger—an open source project under the auspices of the

creates a manipulation-resistant solution to the problem of trust—a way of providing verification without centralization and its attendant risks and costs.").

49. *See* Hoffman, *supra* note 43.

50. *See generally* Satoshi Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System (unpublished manuscript), https://bitcoin.org/bitcoin.pdf [https://perma.cc/QGW4-W934] (last visited Aug. 18, 2018). Nakamoto's identity has never been conclusively identified.

51. *Bitcoin (USD) Price*, COINDESK, https://www.coindesk.com/price/ [https://perma.cc/X2FK-F47J] (last visited Sept. 3, 2018).

52. *See* Nathaniel Popper, *The Rush to Coin Virtual Money with Real Value*, N.Y. TIMES (Nov. 11, 2013), https://dealbook.nytimes.com/2013/11/11/the-rush-to-coin-virtual-money-with-real-value [https://perma.cc/5LMD-QNXC].

53. *See* Nathaniel Popper, *Move Over, Bitcoin. Ether Is the Digital Currency of the Moment*, N.Y. TIMES (June 19, 2017), https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html [https://perma.cc/26SC-PH9P].

Linux Foundation[54]—and the R3 financial services consortium.[55]

All the platforms use slightly different technical approaches. They make design tradeoffs to optimize for factors such as performance, decentralization, regulatory compliance, anonymity, security, and functionality. In the future, there may be only one blockchain of consequence, or there may be dozens of significant platforms and thousands of minor ones. Bitcoin today remains the biggest platform in terms of market capitalization of tokens, but its dominance appears to be waning. In twenty years, it could be worth several trillion dollars, or zero. However the market develops, the blockchain architecture that Bitcoin pioneered is now well-established. All systems of this type incorporate three primary features: distributed ledgers, consensus, and smart contracts.

1. *Ledgers*

A ledger is a record of accounts. Perhaps the most familiar ledgers are those used for double-entry bookkeeping, the foundation of accounting. However, ledgers are not limited to recording debits and credits for corporate balance sheets.[56] Real estate markets could not exist without land title registries. Democracy requires ledgers tallying votes. Copyright depends on both public and private records tracking the registration and assignment of rights. The modern firm depends on ledgers not just for its financials but for the relationships among its internal agents and external partners, as well as its supply chain, back-office, and customer-facing activities. Sociologists such as Max Weber and Werner Sombart argue that double-entry bookkeeping was the foundation of modern capitalism.[57]

54. *See* Cade Metz, *Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain*, WIRED (Dec. 17, 2015), https://www.hyperledger.org/news/2015/12/17/wired-tech-and-banking-giants-ditch-bitcoin-for-their-own-blockchain [https://perma.cc/KP2E-Z4BN].

55. *See* Paul Vigna, *Blockchain Firm R3 CEV Raises $107 Million*, WALL ST. J. (May 23, 2017, 6:37 PM), https://www.wsj.com/articles/blockchain-firm-r3-raises-107-million-1495548641 [https://perma.cc/G2CR-AXJP].

56. *See* Dominic Frisby, *In Proof We Trust*, AEON (Apr. 21, 2016), https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money [https://perma.cc/S6NH-YELA] (explaining the broader potential of distributed ledgers for all kinds of record-keeping).

57. *See* MAX WEBER, GENERAL ECONOMIC HISTORY 276 (Frank H. Knight trans., 1927) ("[T]he most general presupposition for the existence of . . . present-day capitalism is that of rational capital accounting . . . ."); WERNER SOMBART, DER MODERNE KAPITALISMUS 23 (1916) ("[C]apitalism and double entry bookkeeping are absolutely indissociable; their relationship to each other is that of form to content"); *see also* Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S REV. (June 23, 2016), http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/ [https://perma.cc/VA6B-W34B] (detailing the significance of ledgers and the implications for the blockchain). Going back even further, many of the earliest surviving written documents from antiquity, in Mesopotamian cuneiform, are ledgers of commercial transactions. *See* HANS

A blockchain is a kind of distributed ledger.[58] It is "distributed" in that there is no master copy. Any participant in the network can maintain an instantiation of the ledger, yet be confident it matches all the others. Venture capitalist Albert Wenger calls blockchains logically centralized (there is only one ledger), but organizationally decentralized (many entities maintain copies of that ledger).[59] Computers directly participating in a blockchain network, often called full nodes, are in constant communication to remain synchronized. Maintaining that synchronization, called consensus, is the hard part, because there is no canonical master copy.

Centralized ledgers have their own difficulties. If one entity keeps the master ledger, it becomes a single point of failure for the system. If, on the other hand, each organization or computer keeps its own ledger (as with most corporate financial records), every transaction is recorded independently at least twice. Whenever, for example, a company pays a vendor or a bank cashes a check from another bank's customer, their ledgers must be synchronized after the fact through a process of reconciliation. This introduces complexity, delay, and possibilities for error. Until the blockchain came along, these difficulties were thought to be necessary evils.[60]

2. *Consensus*

At the heart of the Bitcoin architecture is a set of software protocols often

J. NISSEN, PETER DAMEROW & ROBERT K. ENGLUND, ARCHAIC BOOKKEEPING: EARLY WRITING AND TECHNIQUES OF ECONOMIC ADMINISTRATION IN THE ANCIENT NEAR EAST (Paul Larsen trans., 1993).

58. *See* WALPORT, *supra* note 43; PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 124 (2015). Not all distributed ledgers are structured as blockchains. For example, the Corda system for financial agreements between regulated banks uses a different data structure. *See* Richard Gendal Brown, *Introducing R3 Corda(TM): A Distributed Ledger Designed for Financial Services*, GENDAL.ME (Apr. 5, 2016), https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/ [https://perma.cc/ES9K-8J9A]. Blockchains are the most common approach, especially for public ("permissionless") systems, so that is the term used here.

59. Albert Wenger, *Bitcoin: Clarifying the Foundational Innovation of the Blockchain*, CONTINUATIONS (Dec. 15, 2014), http://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of [https://perma.cc/8JXA-WRGN].

60. There has been extensive research and significant deployment of distributed database systems for many years. However, these systems generally assume all nodes will be controlled by a single company. They focus on the danger nodes that will fail, whereas blockchain systems protect against untrustworthy nodes that attack the system. *See* Rajesh Nair, *Why Aren't Distributed Systems Engineers Working on Blockchain Technology?*, PAXOS ENGINEERING BLOG (Aug. 1, 2017), https://eng.paxos.com/why-arent-distributed-systems-engineers-working-on-blockchain-technology [https://perma.cc/JG64-NRDC].

called Nakamoto Consensus.[61] Consensus means that participants in a network have confidence that their ledgers are both accurate and consistent.[62] Without a robust means of ensuring consensus, any Bitcoin participant could, for example, spend the same bitcoin multiple times (known as the double-spend problem), or claim it had more currency than it really did. The trouble with most approaches to consensus on digital systems is that it is easy to create multiple fake accounts. This is known as the "Sybil attack."[63] Even if most real users are honest, an attacker can dominate the network and impose its own false consensus on the system.

Nakamoto's response to Sybil attacks cleverly combined cryptographic[64] techniques with insights from game theory.[65] As a baseline, all Bitcoin transactions are cryptographically signed. It can be proven mathematically that only the possessor of the relevant private key (a secret string of letters and numbers) could have sent the relevant message. Next, Bitcoin and other consensus-based systems replace trust in individual actors with trust in networks of actors. Those actors—called "miners" in Bitcoin—are responsible for verifying transactions.[66] Anyone can be a miner. Even if some of them are

61. *See* Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, *in* PROCEEDINGS OF THE 36TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY 104, 106–07 (2015); Nick Szabo, *The Dawn of Trustworthy Computing*, UNENUMERATED (Dec. 11, 2014), http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html [https://perma.cc/Z7YL-F5XB].

62. For a more detailed discussion of the importance of consensus, see Casey Kuhlman, *What Are Ecosystem Applications*, MONAX (June 5, 2016), https://monax.io/2016/06/05/ecosystem-applications/ [https://perma.cc/MQ93-SKVU] ("The problem that blockchain technology solves is not electronic P2P cash, nor is it settlement latency, it is the problem of attribution and ordering of inbound events . . . .").

63. *See generally* John R. Douceur, *The Sybil Attack*, *in* PEER-TO-PEER SYSTEMS 251 (2002).

64. Cryptography is the use of mathematical techniques for secure communications. Encryption is a subset of cryptography used to make information unreadable without possession of a key. Bitcoin's core protocols use no encryption. Transactions are public but secure.

65. Others described similar approaches in the same time frame, although none achieved consensus in as robust a way. For example, cryptographer Nick Szabo propounded a system called Bit Gold. *See generally* Nick Szabo, *Liar-Resistant Government*, UNENUMERATED (May 7, 2009), http://unenumerated.blogspot.com/2009/05/liar-resistant-government.html [https://perma.cc/5BEZ-LM7T].

66. This approach is analogous to the republican form of government epitomized by the United States. Instead of empowering a king, power is decentralized to the people, who express it through voting. To mediate the potential for factionalism and mob rule, voters exercise power indirectly, by electing representatives. *See Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus*, 1 HYPERLEDGER ARCHITECTURE 4 (2017) [hereinafter HYPERLEDGER], https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf [https://perma.cc/Y97U-8XGP] (describing the advantages of voting-based systems for verifying transactions).

untrustworthy, the system holds so long as the majority is honest.[67] In Nakamoto's version, miners compete to validate groups of Bitcoin transactions, called "blocks."[68] The winner for each block earns a reward.

Sybil attacks are the major concern for such a system: if it is easy and rewarding to be untrustworthy, someone probably will be. Hence the second cryptographic technique in Bitcoin: proof of work.[69] Bitcoin's system requires miners who wish to earn the reward to solve cryptographic puzzles involving one-way functions known as "hashes."[70] Solutions require massive and growing computing power, which is sufficiently expensive to deter Sybil attacks.[71] The benefits of cheating are less than the costs. Other consensus systems include proof of stake, in which validators risk losing their existing currency if they attempt to cheat, and a variety of voting and lottery algorithms

67. Security researchers have identified scenarios in which dishonest miners that control more than one-third of the computing power in the network could attack the system successfully. *See* Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, *in* FINANCIAL CRYPTOGRAPHY & DATA SECURITY 436, 438 (2014).

68. *The Magic of Mining*, ECONOMIST (Jan. 10, 2015), https://www.economist.com/business/2015/01/08/the-magic-of-mining [https://perma.cc/9EQB-MA2W]; ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES (2014); *see also* Kevin Werbach, *Bitcoin Is Gamification*, MEDIUM (Aug. 5, 2014), https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22 [https://perma.cc/VX6X-2B8Z] (explaining the significance of the motivational system to Bitcoin).

69. *See* NARAYANAN ET AL., *supra* note 43, at 61. Not every blockchain implements proof of work in the same manner as Bitcoin. For example, Ethereum uses a modified algorithm so that miners do not gain an advantage from using custom chips known as ASICs. Other distributed ledger platforms such as Ripple and Tendermint do not employ proof of work at all, but instead implement alternate mechanisms to achieve the same goal. *See* Bonneau et al., *supra* note 61. It remains to be seen whether these other consensus protocols are as successful as Bitcoin's proof of work. *See id.*

70. A hash function takes some input string (such as a document file) and turns it into an output string—the hash—with a specified length. Although in theory multiple input strings could map to the same hash, cryptographic hash spaces are sufficiently large that such "collisions" are infinitesimally rare. It is easy to compute the hash function of any file. An input string will produce the same output string every time. However, there is no known way to go from a hash back to the input string other than trial and error. *See* NARAYANAN ET AL., *supra* note 43, at 23–24. Miners must attempt truly vast numbers of hashes to find the one that produced the specified output. *See id.* at 61–68.

71. The level of difficulty automatically adjusts as more computing power is added to the network. The Bitcoin network today is thousands of times more powerful than the world's 500 most powerful supercomputers combined. *See* Laura Shin, *Bitcoin Production Will Drop by Half in July, How Will that Affect the Price?*, FORBES (May 24, 2016), http://www.forbes.com/sites/laurashin/2016/05/24/bitcoin-production-will-drop-by-half-in-july-how-will-that-affect-the-price/ [https://perma.cc/XU65-KANQ]. The computing power involved is so vast that it raises concerns about the environmental impacts of the electricity required to power and cool the data centers involved. *See* TAPSCOTT & TAPSCOTT, *supra* note 43, at 259–63.

such as the Ripple Consensus Protocol, which do not require such "skin in the game."[72]

Consensus affirms the integrity both of each individual transaction and of the ledger as a whole. It does so by aggregating transactions together into blocks.[73] The proof of work system is tuned dynamically to generate a valid solution to the hashing puzzle for a block roughly once every ten minutes.[74] Each block thus validated is cryptographically signed with the hash of the prior block, creating an immutable chain of sequential blocks. The longest chain represents the consensus state of the system.[75] Only an attacker with a majority of total computing power in the entire network (known as a 51-percent attack) can "fork" the longest chain with a fraudulent block.[76] Doing so becomes increasingly difficult for blocks earlier in the chain.

A public blockchain, such as Bitcoin's, records all transactions on the network and is totally transparent to all participants.[77] Not only are the contents of the Bitcoin blockchain available to all, but the software involved is open source and freely available.[78] Bitcoin is also designed to be censorship- and tamper-resistant. There is no central control point or network that a government could manipulate or block. And once a transaction is recorded, it cannot easily be changed, a property known as immutability. For example, user A could send some bitcoin to user B, and then user B could send some or all of it back, but there is no way for user A, the miners, or anyone else to reverse the initial transfer.[79]

72. *See* HYPERLEDGER, *supra* note 66. There are various tradeoffs in the choice of consensus algorithm. For example, "permissioned" systems such as Ripple and Hyperledger Fabric only allow approved nodes to join the network. This largely prevents Sybil Attacks and improves transaction throughput but limits the scope of decentralization and the game -theoretic security guarantees of the Bitcoin approach. The security and performance of most consensus algorithms at scale are still open research questions. One approach might come to dominate, although it is more likely that different consensus systems will be used based on the category of application.

73. *See* NARAYANAN ET AL., *supra* note 43, at 88–90.

74. *See id.* at 65.

75. *See id.* at 59. More precisely, it is the chain with the most proof of work.

76. Although as noted above, some research suggests an attacker with over one-third of the mining power could disrupt the network. *See supra* note 67.

77. Users are identified on the blockchain through digital signatures, so the real-world identity of the parties to a transaction may be impossible to determine. For those desiring further anonymity, there are ways to break up transactions in order to obscure large transfers.

78. Alec Liu, *Who's Building Bitcoin? An Inside Look at Bitcoin's Open Source Development*, MOTHERBOARD (May 7, 2013), https://motherboard.vice.com/en_us/article/9aa4ae/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development [https://perma.cc/2A7U-N9KS].

79. The Bitcoin system records transactions, not asset holdings, using a mechanism called Unspent Transaction Output (UTXO). This makes it difficult to "walk back" account

These features suggest an inherent openness and decentralization more like the early Internet than today's more-controlled online environment.[80] They seem to fulfill the dreams of some Internet pioneers for a technology space that was not, in Lawrence Lessig's terminology, regulable.[81]

The final key piece of Nakamoto Consensus is the game-theoretic or psychological dimension: Why will miners bother? Proof of work is expensive, literally. It requires specialized computing hardware and large quantities of electricity. Miners will not be incentivized sufficiently out of altruism. Nakamoto's solution was supremely elegant. The miner who successfully validates a block receives a reward in a valuable currency: Bitcoin. This solves several problems, including how currency enters the money supply without a central bank. New bitcoin is only created through the reward mechanism, at a rate that declines over time.[82] Miners thus act purely out of self-interest, but in doing so, they fulfill a socially beneficial role.

Bitcoin is thus both the output and input of the system. One could equally well describe it as a trust infrastructure designed to support a digital currency, or a digital currency designed to support a trust infrastructure.

3. *Smart Contracts*

Distributed ledgers are active, not passive. In other words, they do not simply record information passed to them. They are part of a consensus system, so they must ensure that recorded transactions are actually completed to match the consensus.[83] For Bitcoin, that means the system self-enforces

balances even if a majority of miners change their Bitcoin software to unwind the validation of a particular block. Some other cryptocurrency platforms are easier to "hard fork" so as to revert prior transactions, because they operate on accounts rather than UTXO. The Ethereum community did so in July 2016 to address the theft of currency from a crowdfunding platform called The DAO. *See infra* notes 135–141. Such steps are controversial, because they call into question the censorship resistance and immutability of public blockchains.

80. *See* Andreessen, *supra* note 43; Morgen E. Peck, *The Future of the Web Looks a Lot Like the Bitcoin Blockchain*, IEEE SPECTRUM (July 1, 2015), http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin [https://perma.cc/Y2VT-D8V7].

81. Lawrence Lessig, *Deja Vú All Over Again: Thinking Through Law & Code, Again*, VIMEO (Dec. 11, 2015), https://vimeo.com/148665401 [https://perma.cc/C7DM-66XY].

82. Hence the analogy to mining for previous resources in the physical world. Eventually the block rewards will drop to zero. At that point, the number of Bitcoins in circulation will be fixed at twenty-one million. Nakamoto envisioned that voluntary transaction fees paid to miners by those seeking validation would gradually replace the rewards as adoption of the Bitcoin system grew. This remains to be seen.

83. Bitcoin actually uses a scripting language for transactions, meaning that every transfer is actually running software code on the blockchain. *See* NARAYANAN ET AL., *supra* note 43, at 79–88 (describing the Bitcoin scripting language and some applications beyond basic cash transfers).

financial transfers.[84] Someone cannot initiate a transaction promising to send bitcoin to another and then renege; the synchronization that reconciles and completes the transfer is part of the process. This mechanism is known as a "smart contract."[85] Both the specification of rights and obligations, and the execution of that contractual agreement, occur through the platform.

The idea of smart contracts was introduced independently from blockchains, and well before Bitcoin was developed.[86] Its practical relevance was limited, however, until Nakamoto's synthesis. Bitcoin takes advantage of smart contracts to execute transactions, and smart contracts take advantage of Bitcoin's distributed ledger to operate with autonomy. Smart contracts are essentially autonomous software agents.[87] With smart contracts, a distributed ledger becomes functionally a distributed computer. The same consensus algorithms that allow each node to have an identical copy of the ledger allow it to perform identical computations in the identical order. While Bitcoin operates based on smart contracts, it strictly limits their capabilities to basic fund transfers for security.

The most prominent platform for smart contracts today is Ethereum, which launched in 2015.[88] Ethereum offers a Turing-complete programming language, meaning that in theory, any application that runs on a conventional

84. To be precise, the blockchain records challenges and responses that either create or destroy Bitcoins, rather than transfers of discrete tokens as such. *See* NARAYANAN ET AL., *supra* note 43, at 75–76.

85. *See* TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 15–30 (2014). *See generally* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997) [hereinafter Szabo, *Public Networks*], http://ojphi.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/U2L2-B34P]; Nick Szabo, *The Idea of Smart Contracts*, *in* NICK SZABO'S ESSAYS, PAPERS, AND CONCISE TUTORIALS (1997) [hereinafter Szabo, *Smart Contracts*], http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html [https://perma.cc/YED2-ACVP]; Werbach & Cornell, *supra* note 25.

86. *See* Szabo, *Smart Contracts*, *supra* note 85.

87. *See generally* Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB (Aug. 20, 2018), https://github.com/ethereum/wiki/wiki/White-Paper [https://perma.cc/5DTZ-NEZ2].

88. *See generally id.*; Popper, *supra* note 53; D.J. Pangburn, *The Humans Who Dream of Companies that Won't Need Us*, FAST COMPANY (June 19, 2015), http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them [https://perma.cc/9GRQ-SPKS]; Jim Epstein, *Here Comes Ethereum, an Information Technology Dreamed Up By a Wunderkind 19-Year-Old That Could One Day Transform Law, Finance, and Civil Society*, REASON (Mar. 19, 2015), http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn [https://perma.cc/FH6S-4ZSS]; Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That Could Power the Internet of Things*, FAST COMPANY (May 21, 2015), http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could-power-the-Internet-of-things [https://perma.cc/NY3K-SBBY].

computer can be executed on the distributed computer of its consensus network.[89] Ethereum makes it easy for developers to code new kinds of applications on top, just as the web and various infrastructure tools such as application servers were the foundation for Google, Amazon, and eBay. Ether, Ethereum's cryptocurrency, is now easily the second most valuable after bitcoin.[90]

Generalized smart contracts platforms are the foundation for decentralized applications, or "DApps."[91] As with the financial uses of the blockchain, many decentralized applications mimic existing centralized applications. IPFS and Storj provide decentralized cloud storage, comparable to Dropbox or Apple's iCloud;[92] Steemit provides an open discussion platform, similar to Reddit;[93] Commuterz supports decentralized ridesharing, comparable to Uber or Lyft.[94]

Other DApps are more novel. For example, Goldman Sachs suggests that the blockchain might facilitate distributed markets for electricity.[95] Users could sell excess power generated through rooftop solar cells to local utilities. Such transactions are limited today due to the overhead of managing the volume of potential transactions among large numbers of individual customers and electric utilities.[96] A distributed ledger could track those transactions without the overhead of a central system. Goldman Sachs estimates a two and one-half

89. The overhead of distributed consensus means that such applications may run far slower than on a single computer or a cloud computing platform such as Amazon Web Services.

90. *See* Nathaniel Popper, *Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's*, N.Y. TIMES (Mar. 27, 2016), http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html?_r=1 [https://perma.cc/28VK-BQKQ].

91. One site lists nearly two thousand decentralized application projects at various stages of development as of August 2018. *See* STATE OF THE DAPPS, http://dapps.ethercasts.com/ [https://perma.cc/6N9A-LWME] (last visited Sept. 3, 2018).

92. *See* Gautham, *Storj, the New Decentralized Cloud Storage Platform Goes Live*, NEWSBTC (Apr. 10, 2016), http://www.newsbtc.com/2016/04/10/storj-new-decentralized-cloud-storage-platform-goes-live/ [https://perma.cc/DA2K-SDMP]; Ian Allison, *How IPFS Is Reimagining the Internet*, NEWSWEEK (Oct. 21, 2016), http://www.newsweek.com/how-ipfs-reimagining-Internet-512566 [https://perma.cc/6XGR-L54T].

93. *See* Andrew McMillen, *The Social Network Doling Out Millions in Ephemeral Money*, WIRED (Oct. 4, 2017), https://www.wired.com/story/the-social-network-doling-out-millions-in-ephemeral-money/ [https://perma.cc/R9CX-AWQ3].

94. COMMUTERZ, http://commuterz.io [https://perma.cc/E3HY-GSAE] (last visited Sept. 3, 2018).

95. *See* Schneider et al., *supra* note 15, at 4.

96. A trial program of this sort is underway in Brooklyn, New York. *See* Aviva Rutkin, *Blockchain-Based Microgrid Gives Power to Consumers in New Nork*, NEW SCIENTIST (March 9, 2016), https://www.newscientist.com/article/2079845-blockchain-based-microgrid-gives-power-to-consumers-in-new-york/ [https://perma.cc/H9M6-D2DU].

to seven-billion-dollar annual opportunity in the U.S. electricity industry by enabling distributed markets.[97]

A distributed autonomous organization, or "DAO," is an ambitious category of decentralized applications.[98] In a DAO, the standard corporate arrangements of equity, debt, and corporate governance could be encoded as a series of smart contracts.[99] Investors could contribute funds in the form of a cryptocurrency, and the distributed application would handle payment of salaries, dividends, proxy votes, and so forth. "The DAO," the crowdfunding system that was catastrophically hacked, was styled as the first implementation of the concept.[100]

B. REASONS FOR ADOPTION

If distributed ledgers did not solve real-world problems, they would be of interest only to cryptographers or philosophers. Some adoption is driven by ideological desire to circumvent state control. For the most part, however, the entrepreneurs, established corporations, major financial institutions, and governments investigating the blockchain today are pursuing tangible benefits. The blockchain's two primary value propositions are avoiding dependence on central actors and creating universal truth among untrusting parties.

1. Avoiding Problems with Central Authority

In 2016, authorities in Buenos Aires, Argentina forbade credit card companies from processing transactions for the ride-hailing company Uber, which was violating local regulations. Xapo, which offers a bitcoin-based debit card, was able to circumvent the ban[101] because it did not require a local

97. *See* Schneider et al., *supra* note 15, at 4.

98. *See* Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAG. (Sept. 19, 2013), https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/ [https://perma.cc/DZQ5-EUL5]; MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2015); Wright & De Filippi, *supra* note 23, at 17, 31–32.

99. The legal status of such virtual corporations as well as that of their investors, developers, and beneficiaries, is an open question. *See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U.L. REV. 1483, 1496–97 (2014); Tanaya Macheel, *The DAO Might Be Groundbreaking, But Is It Legal?*, AM. BANKER (May 19, 2016), http://www.americanbanker.com/news/bank-technology/the-dao-might-be-groundbreaking-but-is-it-legal-1081084-1.html [https://perma.cc/MND9-KMS2]; Peter Van Valkenburgh, *DAOs: the Internet Is Weird Again, and These Are the Regulatory Issues*, COIN CENTER (Jun. 2, 2016), https://coincenter.org/entry/daos-the-Internet-is-weird-again-and-these-are-the-regulatory-issues [https://perma.cc/JQ47-52JZ].

100. *See supra* notes 24–32 and accompanying text.

101. *See* Jamie Redman, *Uber Thriving in Argentina Once Again Thanks to Bitcoin*, BITCOIN NEWS (July 9, 2016), https://news.bitcoin.com/uber-thriving-argentina-bitcoin/ [https://perma.cc/8AL3-M6AS]; Joel Valenzuela, *Uber Switches to Bitcoin in Argentina After Govt*

connection to a traditional payment processor. Uber could continue operating despite the regulatory objections.

Whether routing around authority in this way is desirable or not depends on one's perspective. In at least some cases, however, avoiding dependence on central actors is clearly a valuable thing. This is the reason, for example, that Latin American countries have seen some of the most aggressive adoption of bitcoin for payments.[102] Citizens there are skeptical of the government and the financial system, after calamitous experiences with hyperinflation and currency devaluation. Bitcoin, perceived as immune from the vicissitudes of politics and the demands of international lenders, seems like a safer option. One of Bitcoin's value propositions is to serve as a residual store of value in many ways superior to gold, which today is a $7 trillion asset class.[103]

The same dynamic applies when central private actors are involved. Trust imposes risk. There is always the danger that the one you trust turns out to be untrustworthy. Investors in Bernie Madoff's Ponzi scheme lost their money because they trusted the wrong investment manager.[104] Law, regulation, and insurance are all mechanisms to limit such risks. The Madoff scenario is the exception rather than the rule, at least in the United States. For those at the mercy of loan sharks, payday lenders, or extortionate money transfer agents, however, the blockchain offers an appealing alternative.

Even when trusted authorities are not fundamentally untrustworthy, they are single points of failure that can be exploited. For example, access to websites is secured through cryptographic certificates that verify the user is connected to the correct site, with no interference in the middle. Those certificates are issued by central certificate authorities. In 2011, DigiNotar, a Dutch certificate authority, was hacked.[105] Fraudulent certificates were issued which allowed attackers to intercept and redirect traffic between users and Google's Gmail service. The damage was limited because Google and web

Blocks Uber Credit Cards, COINTELEGRAPH (July 6, 2016), http://cointelegraph.com/news/uber-switches-to-bitcoin-in-argentina-after-govt-blocks-uber-credit-cards [https://perma.cc/88VX-MVU6].

102. *See* Sonny Singh & Alberto Vega, *Why Latin American Economies Are Turning to Bitcoin*, TECHCRUNCH (Mar. 16, 2016), https://techcrunch.com/2016/03/16/why-latin-american-economies-are-turning-to-bitcoin/ [https://perma.cc/6H9C-MB29].

103. *See* Nathan Lewis, *Gold or Bitcoin? Gold and Bitcoin*, FORBES (June 30, 2017), https://www.forbes.com/sites/nathanlewis/2017/06/30/gold-or-bitcoin-gold-and-bitcoin/#3a6f0fe33e4b [http://perma.cc/GGT9-FDMQ].

104. A leading biography of Madoff is subtitled, "Bernie Madoff and the Death of Trust." DIANA B. HENRIQUES, THE WIZARD OF LIES (2011).

105. *See* Kim Zetter, *DigiNotar Files for Bankruptcy in Wake of Devastating Hack*, WIRED (Sept. 20, 2011), https://www.wired.com/2011/09/diginotar-bankruptcy/ [https://perma.cc/EG8W-XE99].

browser vendors acted quickly to invalidate the fraudulent certificates, but the incident shows the risk of centralized systems.[106] Projects such as Namecoin, Ethernet Name Service, and Blockstack are creating security frameworks for access to online resources that use blockchains to avoid this problem.[107]

Moreover, all intermediaries impose costs. When an intermediary is a private company, it expects to generate revenue in return for the value it provides. Google charges advertisers for exposing them to large number of users and for precisely targeting advertisements. Google's advertising revenues, now in the tens of billions of dollars annually, represent a direct cost of intermediation.[108] If the search engine advertising marketplace could exist without Google at the center, it would not have to bear those costs. And as the number of intermediaries multiplies, so do the costs. Search engine optimization firms, for example, are intermediaries that piggyback on Google. Those providers charge for their services, and Google has to expend resources to prevent excessive gaming of its search results.[109]

Intermediaries also shape markets to serve their own interests. They may restrict conduct or fail to innovate if they do not see the benefits. In 2017, the European Union imposed a $2.7 billion fine on Google for manipulating online shopping search results to benefit its affiliates.[110] In essence, being the trusted heart of a community conveys a kind of monopoly power. For example, many websites use Facebook's "social login" service to verify credentials for their users. It is more convenient to hand off to Facebook the process of identity management because Facebook is such a powerful trusted intermediary for online social interactions. Social login, however, entrenches Facebook's control.[111] It gives Facebook access to data from outside its own

106. *See* Josephine Wolff, *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure*, SLATE (Dec. 21, 2016), http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_Internet_s_infrastructure.html [https://perma.cc/LA57-EP2P].

107. *See* Michael del Castillo, *Blockstack Releases Blockchain-Powered, Tokenized Internet Browser*, COINDESK (May 23, 2017), https://www.coindesk.com/blockstack-blockchain-decentralized-browser/ [https://perma.cc/3GEJ-98ZG].

108. *See* Rani Molla, *Google Leads the World in Digital and Mobile Ad Revenue*, RECODE (July 24, 2017), https://www.recode.net/2017/7/24/16020330/google-digital-mobile-ad-revenue-world-leader-facebook-growth [https://perma.cc/YRR4-ZKDM] (stating that Google was expected to make $73.8 billion in net digital ad sales in 2017).

109. *See* David Kesmodel, *Sites Get Dropped By Search Engines After Trying to 'Optimize' Rankings*, WALL ST. J. (Sept. 22, 2015), https://www.wsj.com/articles/SB11271416978744925 [https://perma.cc/XWF4-49KY].

110. *See* Mark Scott, *Google Fined Record $2.7 Billion in E.U. Antitrust Ruling*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html [https://perma.cc/P574-QUA8].

111. *See generally* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133

boundaries and raises barriers to competition. Companies in Facebook's central position for long periods of time tend to, like any monopoly, raise prices and slow innovation. This monopoly is essentially cashing in on the gains it created. To the others in the network, however, the effect is a tax, and sometimes a significant one.

2. Shared Truth

The second appealing aspect of the blockchain model is its potential for speed and efficiency. At first glance, this sounds odd. Bitcoin validates a block roughly every ten minutes, and currently has a theoretical limit of seven transactions per second.[112] This is quite a small number: the Visa credit card network handles up to 10,000 transactions in the same period.[113] The overhead of synchronizing the distributed ledger is so great that, according to one estimate by cryptographer Nick Szabo, the process operates 10,000 times slower than a conventional computer.[114]

Yet there is a hidden advantage of removing the need to trust the specific actors with which you interact. Trust is not transitive. I may trust my bank, but that does not mean I trust yours. For me to cash your check, our banks must enter into their own trust relationship. With many thousands of financial institutions processing billions of transactions across hundreds of jurisdictions, this pairwise structure quickly bogs down. Or more accurately, it works only with huge inefficiencies and transaction costs. Much of the time, transaction costs become further value-extraction opportunities for the trusted actors. Hence the massive revenues for providers of remittances and credit cards.[115] The complexity of reconciling transactions between many interconnected trusted parties adds delay to the process. Stock trades, for example, typically settle after two days (a standard known as T+2).[116] This ties up capital that

(2017) (discussing how digital platforms have exploited the Internet environment to aggregate power).

112. *See* NARAYANAN ET AL., *supra* note 43, at 134 (validation every ten minutes), 95 (seven transactions per second limit).

113. *See* Timothy B. Lee, *Bitcoin Needs to Scale By a Factor of 1000 to Compete with Visa. Here's How to Do It*, WASH. POST (Nov. 12, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-to-compete-with-visa-heres-how-to-do-it/ [https://perma.cc/QXZ7-HJWC]. New technologies may greatly increase the speed of the Bitcoin transaction network. *See* Romain Dillet, *Blockchain Open Sources Thunder Network, Paving the Way for Instant Bitcoin Transactions*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/blockchain-open-sources-thunder-network-paving-the-way-for-instant-bitcoin-transactions/ [https://perma.cc/M4FX-DSRV].

114. *See* Szabo, *supra* note 61.

115. The remittance market generates $38 billion in annual fees worldwide. *See* TAPSCOTT & TAPSCOTT, *supra* note 43, at 183.

116. *See* SEC, *SEC Adopts T+2 Settlement Cycle for Securities Transaction*, (Mar. 22, 2017),

could otherwise be deployed more efficiently.

In the traditional system, every actor is individually responsible for keeping its ledger in sync with the virtual consensus. Yet it only has visibility (limited at that) into its direct partners. With the blockchain, every new block reconciles its transactions across the entire system. Each participant knows that its copy of the ledger is identical to every other. The truth—or what computer scientists call the network's "state"—is shared among them. Thus, while it may take much longer to record each transaction, the network as a whole updates more rapidly. Because this occurs through one synchronized process, rather than a potentially large number of separate transactions, costs may be significantly lower.[117] Goldman Sachs estimates that the blockchain could save $11–$12 billion annually in settlement and reconciliation fees, just for securities transactions.[118]

Bitcoin and other blockchain-based systems do face significant scaling challenges. The Bitcoin development community is engaged in debates about mechanisms such as increasing the size of each block to improve performance.[119] By contrast, the existing financial system has been optimized over an extended period for robust operation at massive scale. Predictions that the blockchain will soon sweep away the banking system as we know it are thus exaggerated. However, the potential for faster and more efficient reconciliation is a key reason major financial institutions are actively exploring permissioned blockchains.

Finally, there are different ways to structure a distributed ledger.[120] On public blockchains, such as Bitcoin and Ethereum, anyone can operate a mining node and maintain a copy of the shared ledger. Because there is no way to verify the integrity of network participants, elaborate protocols such as Nakamoto Consensus and high-overhead distribution of all transaction information are necessary. Permissioned ledgers can do away with those limitations and operate more efficiently, but at the cost of reintroducing elements of central control.[121] Different use cases will call for different

https://www.sec.gov/news/press-release/2017-68-0 [https://perma.cc/7DAW-Y7YH].

117. *See* BUILDING THE TRUST ENGINE, *supra* note 43, at 9, 18.

118. *See* Schneider et al., *supra* note 15, at 5.

119. *See* NARAYANAN ET AL., *supra* note 43, at 98.

120. *See* Nolan Bauerle, *What Is the Difference Between Public and Permissioned Blockchains?*, COINDESK, https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/ [https://perma.cc/A8E4-EE4N] (last visited Sept. 3, 2018); *see generally*, Swanson, *supra* note 85 at 4–5.

121. *See* Richard Gendal Brown, *Towards Deeper Collaboration in Distributed Ledgers: Thoughts on Digital Asset's Global Synchronisation Log*, GENDAL.ME (Jan. 24, 2017), https://gendal.me/2017/01/24/towards-deeper-collaboration-in-distributed-ledgers-thoughts-on-digital-assets-global-synchronisation-log/ [https://perma.cc/Q9BP-V8K2].

solutions.

As far as the world of distributed ledgers has come since the launch of Bitcoin in 2009, these are still early days. Vlad Zamfir, one of the core developers of Ethereum, created a stir when he tweeted in March 2017, "Ethereum isn't safe or scalable. It is immature experimental tech. Don't rely on it for mission critical apps unless absolutely necessary!"[122] He is correct. And not just for Ethereum. There are so many well-founded efforts underway, so many significant use cases, so much support from major enterprises, and so much capital flowing in that the blockchain is clearly more than a fad. Exactly how it will develop, though, remains uncertain. The blockchain offers tremendous potential benefits. It also poses very serious risks and public policy challenges.

III. LEDGERS MEET LAW

Distributed ledger technology gives users confidence that they can store and exchange valuable assets. However, that is not the same thing as finding a person or institution trustworthy.[123] If the blockchain entirely replaces reliance on people, companies, and governments with reliance on software code and cryptography, it will produce distrust. And this dissonance has real consequences. When the beautiful math of Satoshi Nakamoto meets the messy reality of real-world implementation, it turns out to be not so perfect. The limitations of the blockchain create problems when it is positioned as the sole guarantor of enforcement. Fortunately, there is a mechanism that can work alongside the technical trust architecture of the blockchain. That mechanism is the law.

A. WHAT COULD POSSIBLY GO WRONG?

The Bitcoin consensus ledger has not been successfully hacked since its

122. Vlad Zamfir (@VladZamfir), TWITTER (Mar. 4, 2017, 4:40 AM), https://twitter.com/vladzamfir/status/838006311598030848?lang=en [https://perma.cc/Z94J-VNDB]. Zamfir felt the need to explain himself the next day in a longer post. *See* Vlad Zamfir, *About My Tweet from Yesterday*.., MEDIUM (Mar. 5, 2017), https://medium.com/@Vlad_Zamfir/about-my-tweet-from-yesterday-dcc61915b572 [https://perma.cc/P6BL-ECND].

123. Agreement does not necessarily presume trust. An insight of game theory is that even non-communicating parties may converge on common points by independently choosing the most likely or familiar option. *See* THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 54–55 (1960). The creators of both smart contracts and Ethereum make reference to these Schelling Points. *See* Szabo, *Public Networks*, *supra* note 85; Vitalik Buterin, *SchellingCoin: A Minimal-Trust Universal Data Feed*, ETHEREUM BLOG (Mar. 28, 2014), https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/ [https://perma.cc/ZHA6-WSH9].

very early days. Sophisticated attackers have tried. Given that bitcoin is literally money, the ledger represented a bank vault storing over $300 billion at the 2017 peak. The best evidence that blockchain technology works is that this massive target remained secure. However, as successful as Bitcoin and other major blockchain systems have been in avoiding major security failures, the security of the cryptocurrencies is not a foregone conclusion. And as circumstances change, there is no guarantee it will continue. According to a group of leading researchers in 2015, "[w]e do not yet have sufficient understanding to conclude with confidence that Bitcoin will continue to work well in practice . . . ."[124]

Think of a blockchain network as a series of concentric circles. In the middle is the ledger, secured through robust decentralized consensus. At the next layer are the smart contracts, the software code that direct transactions on the network. Outside that are edge service providers like exchanges and wallet services, which interface between cryptocurrencies and the traditional world. Finally, there are coins that DApps and others sell directly to users. Each has weaknesses, but they are different weaknesses.

1. Trusting Ledgers

Blockchain-based systems are vulnerable. At the most general level, they depend on modern cryptographic techniques. Basic vulnerabilities in these mechanisms cannot be ruled out, especially with advances in computing power. Quantum computers, for example, might be able to break encryption methods that the most powerful conventional computers cannot crack.[125] If such flaws exist, however, they will apply at least as strongly to the existing online transactional systems, which rely on the same cryptography. And the blockchain world has attracted some of the world's foremost experts in cryptography, who are working actively to prevent such failures. A more likely danger is flawed implementation of cryptographic techniques, such as reliance on random number generators that are not actually random. Blockchain technology, like any system built on computer code, is not perfect. There have been significant bugs discovered in the open source Bitcoin code, although they were addressed prior to any lasting damage.

More serious vulnerabilities relate to the mining or proof of work process. Nakamoto's solution for consensus is remarkably robust, but it can be overcome by a 51% attack.[126] If someone controls more than half of the

124. Bonneau et al., *supra* note 61, at 104.

125. *See First Quantum-Secured Blockchain Technology Tested in Moscow*, MIT TECH. REV. (June 6, 2017), https://www.technologyreview.com/s/608041/first-quantum-secured-blockchain-technology-tested-in-moscow/ [https://perma.cc/B554-SYE8].

126. While the 51% attack is the most widely-discussed scenario, security researchers have

mining power in the network, they can validate blocks of their choosing, even if they involve double-spending. Bitcoin relies on the difficulty of amalgamating such enormous processing power. Today, that would be equivalent to several hundred of the world's fastest supercomputers, running non-stop.[127]

Nonetheless, because most mining is now handled through pools in which many participants aggregate their activity, it is not inconceivable that a pool could cross the threshold.[128] The danger of a 51% attack increases when mining network power decreases.[129] That tends to occur when the price of bitcoin falls, reducing the incentives for miners, or at the "halving" points when the algorithm automatically reduces the award to slow the flow of new currency into the system.[130] Other blockchain platforms such as Ripple use consensus approaches that do not involve mining rewards, and Ethereum plans to migrate to an alternate approach called "proof-of-stake."[131] However, these techniques have their own limitations and have survived less real-world exposure than Bitcoin.[132] And while permissioned blockchains, which have an additional layer of centralized trust over the participants in the network, may not need to worry about 51% of the attacks, they face more of the traditional information security concerns of centralized systems.

---

identified several other potential attack vectors against Bitcoin. *See* Bonneau et al., *supra* note 61, at 110–12.

127. *See* Reuven Cohen, *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!*, FORBES (Nov. 28, 2013), https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/ [https://perma.cc/7SYQ-E6YH].

128. *See* Jon Matonis, *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, COINDESK (July 17, 2014), http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/ [https://perma.cc/VK55-XRCQ] ("A forum for discussing these issues is critical to maintaining the integrity of the bitcoin network, as its overall health depends on smooth mining operations with a minimum amount of . . . players capable of executing a 51% attack.").

129. More generally, public blockchains must maintain sufficient scale and network effects to remain viable. *See* Fairfield, *supra* note 48, at 823–25.

130. *See* Fredrick Reese, *As Bitcoin Halving Approaches, 51% Attack Question Resurfaces*, COINDESK (July 6, 2016), http://www.coindesk.com/ahead-bitcoin-halving-51-attack-risks-reappear/ [https://perma.cc/UNV5-4YZU] (describing concerns about a 51% attack after the halving in July 2016). Adjusting to the expected scarcity, the price of Bitcoin tends to increase around these halving points, but equilibrium is not guaranteed. Other blockchains do not necessarily use the halving mechanism, but all those employing proof of work face the concern about incentives when the price of the cryptocurrency falls.

131. *See* Vlad Zamfir, *Introducing Casper "the Friendly Ghost"*, ETHEREUM BLOG (Aug. 1, 2015), https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ [https://perma.cc/6YH9-3JJA].

132. *See generally* Bonneau et al., *supra* note 61 (describing open research questions for cryptocurrencies).

Different levels of security and robustness will be needed depending on the context. A bank will be more concerned about certain risks than a merchant engaged in a small-value consumer transaction. Medical records on the blockchain will have different risk profiles than supply chain records for diamonds. Such variation is not unique to the blockchain; it is part of trust and security with existing centralized systems. Given the novelty of distributed ledgers, though, it will take some time to sort out the appropriate security models.

2. Trusting Smart Contracts

The next layer beyond the blockchain itself is the smart contract code that implements transactions.[133] A smart contract can have errors and security flaws, like any other software code. And indeed, vulnerabilities have already been identified in high-profile Ethereum smart contracts.[134] Errors or security exploits in smart contracts are particularly dangerous because the blockchain directly carries value or rights to assets. There are significant practical limitations in replacing human enforcement of agreements with software running on the blockchain. Things simply do not always go according to plan.

The collapse of The DAO, noted in the introduction, illustrated this vulnerability.[135] The transactions siphoning off funds were valid smart contracts according to the rules of The DAO, so they were subject to the same immutable execution as any others. Ethereum had to employ a "hard fork" to return the stolen Ether.[136] A hard fork creates two incompatible chains.[137] Although most miners adopted the new software without incident, the move was not without controversy.[138] It meant that Ethereum transactions were not

133. *See* Ari Juels, et al., *The Ring of Gyges: Investigating the Future of Criminal Smart Contracts*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 283, 285–87 (2016).

134. *See* Zikai Alex Wen & Andrew Miller, *Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug*, HACKING, DISTRIBUTED (June 16, 2016), http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/ [https://perma.cc/35M6-AGKL].

135. *See supra* notes 25–31 and accompanying text; *see generally* Jentzsch, *supra* note 25, at 1 (describing "the first implementation of Decentralized Autonomous Organization (DAO) code to automate organizational governance and decision-making.").

136. *See* Paul Vigna, *Ethereum Gets Its Hard Fork, and the 'Truth' Gets Tested*, WALL ST. J. (July 20, 2016), http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested/ [https://perma.cc/56WJ-8ANL].

137. Miners of one chain do not recognize the validity of blocks mined by the other clients, and vice versa, even though they may otherwise use exactly the same protocols. *See* Bonneau et al., *supra* note 61, at 112.

138. *See* Stan Higgins, *Will Ethereum Fork? DAO Attack Prompts Heated Debate*, COINDESK (June 17, 2016), http://www.coindesk.com/will-ethereum-hard-fork/ [https://perma.cc/8VD3-LUD2]; Michael del Castillo, *Specter of Ethereum Hard Fork Worries*

truly immutable, or immune from centralized interference. It also raised concerns about what might happen when governments or other central authorities became concerned about records stored on distributed ledgers.[139]

The assumption was that the pre-fork blockchain would wither away. That did not happen. A small but growing group of miners kept running the old software,[140] evidently dissatisfied with the Ethereum Foundation's willingness to break the ledger's immutability. A group of developers agreed to manage the software going forward, under the name "Ethereum Classic" (ETC). Ethereum core developer Peter Szilagyi summarized the experience with profound understatement: "The DAO has shown us that it takes much more effort to write smart contracts than we originally anticipated . . . ."[141]

The fallout of The DAO hack is still being felt. In May 2017, QuadrigaCX, the largest cryptocurrency exchange in Canada, announced it had lost Ether worth over $14 million.[142] There was no foul play involved. And the Ether did not disappear. It was permanently inaccessible because of an erroneous smart contract. The cause, it turned out, was a bug in code that was added to split Ethereum and Ethereum Classic balances after the hard fork.[143] Cryptographic immutability is a powerful thing. That power makes blockchain-based systems trustworthy, but it also leads to problems that code itself cannot solve.

3. Trusting Edge Services

Even when value is stored in decentralized systems, it is often accessed through centralized edge services. In theory, anyone can operate a full node with a complete copy of the blockchain on a public network such as Bitcoin or Ethereum. In practice, the technical and hardware requirements are prohibitive for ordinary users. Virtually all consumers use wallet services such as Coinbase or Xapo. Users must trust the wallet services in the same manner as a bank. A wallet provider stores the private cryptographic keys for its customers, which allows them to access their cryptocurrency through a standard username and password. However, if the wallet provider is hacked,

Australian Banking Group, COINDESK (June 29, 2016), http://www.coindesk.com/spectre-ethereum-hardfork-worries-anz-banking-group/ [https://perma.cc/8GTJ-Y23U].

139. Ethereum is a public blockchain, like Bitcoin. Permissioned blockchains do not provide the same assurance of non-interference because access is limited to identified parties.

140. *See* Vigna, *supra* note 32.

141. Peter Szilagyi, *DAO Wars: Your Voice on the Soft-Fork Dilemma*, ETHEREUM BLOG (June 24, 2016), https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/ [https://perma.cc/CSZ7-2WVY].

142. *See* Stan Higgins, *Ethereum Client Update Issue Costs Cryptocurrency Exchange $14 Million*, COINDESK (June 2, 2017), https://www.coindesk.com/ethereum-client-exchange-14-million/ [https://perma.cc/PJ2M-ER4W].

143. *See id.*

the keys are vulnerable. And given the novelty of cryptocurrencies, many are inexperienced or unsophisticated. As Nick Szabo tweeted, "Bitcoin is the most secure financial network on the planet. But its centralized peripheral companies are among the most insecure."[144]

A particular point of vulnerability lies in exchanges that trade cryptocurrencies for dollars or other government-backed fiat money. In proof of work systems like Bitcoin, the only two ways to obtain cryptocurrency are through mining or by exchanging with someone else. Most users are not miners, so at some point they have to buy their bitcoin. Exchanges make markets among various cryptocurrencies and dollars or other fiat currencies. Unfortunately, the exchanges sometimes prove insufficient to the task.

In 2014, the most prominent Bitcoin exchange, Mt. Gox, collapsed after hackers stole a significant amount of currency, then worth over $400 million.[145] Another major exchange, Bitfinex, was hacked in 2016, losing cryptocurrency valued at nearly $70 million.[146] And in early 2018, a Japanese exchange reported a theft of half a billion dollars of cryptocurrency.[147] Although there has been some effort to require licensing of cryptocurrency exchanges, the global nature of the market means many exchanges are effectively unregulated.[148]

Edge providers can also decide whether to police transactions. A Bitcoin transaction for drugs, gambling, or a contract killing will be processed on the ledger in the same way as one for a pizza. There is no bank or payment processor that governments can pressure to block the transaction. If, however, a user operates through an edge provider, it can be subjected to legal

144. Nick Szabo (@NickSzabo4), TWITTER (June 17, 2017, 6:05 PM), https://twitter.com/NickSzabo4/status/876244539211735041 [https://perma.cc/6ZE9-XYDR].

145. *See* Robin Sidel, Eleanor Warnock & Takashi Mochizuki, *Almost Half a Billion Worth of Bitcoins Vanish*, WALL ST. J. (Feb. 28, 2014) https://www.wsj.com/articles/mt-gox-to-hold-news-conference-1393579356 [https://perma.cc/C8E5-AG7A]; Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), http://www.wired.com/2014/03/bitcoin-exchange/ [https://perma.cc/6T7N-XD2H].

146. Josh Horwitz, *The $65 Million Bitfinex Hack Shows That It Is Impossible to Tell a Good Bitcoin Company From a Bad One*, QUARTZ (Aug. 9, 2016), https://qz.com/753958/the-65-million-bitfinex-hack-shows-that-it-is-impossible-to-tell-a-good-bitcoin-company-from-a-bad-one/ [https://perma.cc/XE5K-EYUP].

147. Evelyn Cheng, *Japanese Cryptocurrency Exchange Loses More Than $500 Million to Hackers*, CNBC (Jan. 26, 2018), https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html [https://perma.cc/DTA3-J2W3].

148. This may be changing. Bitfinex, one of the largest exchanges, announced in August 2017 that it would stop serving U.S. customers after the SEC suggested that it might be liable for trading tokens that are incorrectly failed to register as securities upon issuance. *See* Wolfie Zhao, *Bitfinex to Bar US Customers from Exchange Trading*, COINDESK (Aug. 11, 2017), https://www.coindesk.com/bitfinex-suspends-sale-select-ico-tokens-citing-sec-concerns/ [https://perma.cc/GE9L-GS2S].

enforcement. That might be difficult depending on where the service is located and whether it hides identities of its management. It is not impossible, as the Silk Road takedown and similar law enforcement actions illustrated.[149]

4. *Trusting Coin Issuers*

A final source of vulnerability involves the services built on top of blockchains. If these are centralized systems, they have the same issues as exchanges and other edge services. If they are decentralized, they operate based on vulnerable smart contracts. Many of them add an additional element, however, by offering their own cryptocurrency coins directly to users. These token sales create a further level of risk.

Just as a company can sell stock to the public to finance its operations, a distributed ledger network or DApp can sell cryptocurrency tokens. By analogy to an initial public offering (IPO) of stock, these token sales are often called initial coin offerings (ICOs). What rights the tokens grant depends on the associated smart contracts.[150] The first ICO was Mastercoin, a system for creating new application-specific "colored" coins on top of the Bitcoin network. Its 2013 ICO generated $5 million in bitcoin. Ethereum followed in 2014, raising approximately $18 million in bitcoin a year before it mined its first block of Ether. As the price of bitcoin surged in 2017, there was a flurry of ICOs raising over $5 billion.[151] The encrypted messaging application Telegram launched an ICO in early 2018 designed to raise $2 billion by itself, which is more than Google raised in its initial public offering.[152]

Token sales could offer a new means of funding innovative technologies that circumvents the limitations of the traditional venture capital model. They also offer an almost perfect way to cheat people out of their money.[153] Token purchasers today are generally contributing money to blockchain-based projects with virtually no way to guarantee they get anything in return, and very limited information about risks. The projects may be scams. The teams involved may try, but fail to build the application they described. The offering may be structured with unfair terms toward ordinary purchasers relative to the development team or their associates. The application may fail to attract

149. *See supra* note 20 and accompanying text.

150. Something they generally do not offer are the equity ownership rights in a corporate entity associated with stocks. Token holders own a share of the value of the network, but not a formal claim on any assets.

151. *See supra* note 10.

152. *See* Mike Orcutt, *Telegram's ICO: Give Us $2 Billion and We'll Solve All of Blockchain's Problems*, MIT TECH. REV. (Jan. 25, 2018), https://www.technologyreview.com/s/610055/telegrams-ico-give-us-2-billion-and-well-solve-all-of-blockchains-problems/ [https://perma.cc/U68E-32WR].

153. *See* Popper, *supra* note 38.

activity, depressing the value of the token.

Such risks overlap very significantly with those that produced the 1933 Securities Act and 1934 Securities Exchange Act.[154] Securities and Exchange Commission (SEC) rules require all securities offerings to be registered—triggering detailed disclosure and antifraud requirements—or subject to a specific exemption. Yet to this point, virtually no ICOs have attempted to register.[155]

The foundational principle of securities regulation is disclosure. Investment involves risks, and no one is entitled to legal protection against a bad decision. However, without regulation, there is a strong information asymmetry between investors, especially retail investors, and investment promoters. Token sales represent a sudden, grand experiment in *caveat emptor* securities offerings, targeting retail investors all around the world.[156] Given all the uncertainties and technical complexities of blockchain technology, most investors are unlikely to understand what they are getting into, even with extensive financial disclosure. Without disclosure, they are at the mercy of the offerors and investment promoters. A system that invites abuse on this scale will inevitably lead to scams.[157]

The potential abuses of ICOs do not mean that the entire enterprise should be banned or that all such offerings must be fit into the strictures of

154. *See* Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. §§ 77a et seq. (1982 & Supp. IV 1986)); *see also* SEC, *Registration Under the Securities Act of 1933*, https://www.sec.gov/fast-answers/answersregis33htm.html (last visited Sept. 3, 2018) [https://perma.cc/4G4W-X7Q5]; Securities Exchange Act of 1934, Pub. L. No. 73-291, § 78(b), 48 Stat. 881 (1934) (codified as amended at 15 U.S.C. §§ 78a–qq (1982 & Supp. IV 1986)).

155. A number of ICOs limit their offerings to wealthy "accredited" investors, which qualifies them for one of the registration exemptions under SEC rules. These are often structured using a framework called the Simple Agreement for Future Tokens (SAFT), under which purchasers hope to re-sell their tokens to the public once the application becomes operational. *See* Juan Batiz-Benet et al., *The SAFT Project: Toward a Compliant Token Sale Framework*, PROTOCOL LABS COOLEY (Oct. 2. 2017), https://saftproject.com/static/SAFT-Project-Whitepaper.pdf [https://perma.cc/AAX3-PE64]. The SEC has not passed judgment on the legality of this arrangement.

156. U.S. securities laws only apply when securities are marketed or sold to U.S. citizens. However, most other major jurisdictions have similar disclosure obligations. As the SEC affirmed in its investigative report on The DAO token offering, a foreign entity or even a virtual organization selling tokens to Americans is still subject to its rules. *See* SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 1–2 (2017) [hereinafter SEC DAO INVESTIGATION] https://www.sec.gov/litigation/investreport/34-81207.pdf [https://perma.cc/9X5T-DB44].

157. *See* David Z. Morris, *The Rise of Cryptocurrency Ponzi Schemes*, ATLANTIC (May 31, 2017), https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/ [https://perma.cc/4JH4-23AH].

U.S. securities laws. Not all token offerings are necessarily securities, for one thing. An SEC investigation concluded that The DAO tokens should have been classified as securities and therefore subject to the SEC's rules for public offerings.[158] However, it stopped short of declaring that all tokens would be.[159] Regulators around the world need to consider how to draw lines around token offerings that protect investors without chilling innovation. Without such efforts, investors will be hurt. And failures of ICOs could undermine confidence in the market as a whole. Blockchain effectively implements a decentralized security model, but this does not obviate the need for legal and regulatory involvement.

B. CODE VS. LAW

1. "No Sovereignty Where We Gather"

In the late 1990s, it was fashionable to see the Internet as a technology that undermined regulation through decentralization. Electronic Frontier Foundation co-founder John Perry Barlow's 1996 Declaration of the Independence of Cyberspace thundered that governments "have no sovereignty where we gather" and do not "possess any methods of enforcement we have true reason to fear."[160] This view captured the spirit of a cyber-libertarian movement that included not just traditional skeptics of state power, but also innovation-focused developers and legal experts. Scholars wrote of online communities freed from the strictures of territorial sovereigns.[161] Some cyber-activists went so far as to claim an abandoned British naval platform in international waters as the independent territory of Sealand, believing they could operate Internet servers completely outside of

158. *See* SEC DAO INVESTIGATION, *supra* note 156. The SEC concluded The DAO was an unauthorized, unregistered securities offering, but chose not to impose sanctions, "based on the conduct and activities known to the Commission at this time." *Id.* at 1. This apparently referred to the fact that, thanks to the hard fork, all investors received their money back, and The DAO subsequently shut down.

159. In February 2018 testimony before the Senate Banking Committee, SEC Chairman Jay Clayton stated that, "I believe every ICO I've seen is a security." However, he acknowledged that a token offering could conceivably be structured to avoid that classification. Jordan Pearson, *The SEC Is Mad About All These ICOs, Wants the Government to Regulate Cryptocurrency Trading*, MOTHERBOARD (Feb. 6, 2018), https://motherboard.vice.com/en_us/article/mb5anx/sec-regulate-cryptocurrency-icos-cftc-senate-hearing [https://perma.cc/59A7-LHJ3].

160. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. https://www.eff.org/cyberspace-independence [https://perma.cc/SF3L-Y7PX].

161. *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (discussing the need for new laws and legal institutions in Cyberspace that differ from those of the geographically-bound "real world").

legal restrictions.[162]

These visions of an unregulable cyberspace met the cold hard limits of reality. As Jack Goldsmith and Tim Wu explained in their 2006 book, *Who Controls the Internet*, governments around the world were able to impose their will on online activity.[163] Utopian initiatives like Sealand collapsed amid internal squab

bling, with little or no adoption.[164] China built a *Great Firewall* that allowed it to censor Internet traffic in and out of the country.[165] Geo-location technology allowed courts to impose sanctions on activity touching citizens of their jurisdictions.[166] Efforts to circumvent legal regimes, whether through peer-to-peer technology to hobble copyright enforcement or online gambling services located in island jurisdictions where the conduct was legal, were repeatedly shut down.[167] Authoritarian regimes discovered they could use the Internet as a tool for monitoring and repression.[168]

The Internet did represent something big and new. But the legal system was able to incorporate it, as it has incorporated every technology since at least the printing press. It turns out that while cyberspace is nowhere, the people and companies and systems that deliver Internet services are very much somewhere. There are any number of control points, from the Internet service and hosting providers that manage the flow of bits to the financial services firms that control the flow of money, which regulators can target to control online activity.[169] The Internet is a regulated space,[170] which is not to say, of course, that it is regulated the same way everywhere, or that online transactions are regulated identically to their offline analogues. Working through the practicalities of Internet regulation has been a twenty-year global process, with no end in sight. Yet a key point is incontestable: Internet regulation is not an

162. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 65 (Oxford Univ. Press, Inc., 2006), http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf [https://perma.cc/QSB5-G732].

163. *See id.* at 66.

164. *See id.*

165. *See id.* at 87–92.

166. *See id.* at 79–81.

167. *See id.* at 73–77.

168. *See generally* EVGENY MOROZOV, THE NET DELUSION (2011) (discussing the Internet's failed promise to aid the fight against authoritarianism, the global mindsets that allowed for it to fail, and policies that may be more successful).

169. *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 655–73 (2002) (discussing four different control points: the source, the source ISP, the destination, and the destination ISP).

170. Careful readers of Lawrence Lessig's *Code* knew this already. *See* CODE VERSION 2.0, *supra* note 22.

oxymoron.

The blockchain rekindled the cyber-libertarian flame. There are two ways to frame a discussion about blockchain and law: *Can* these technologies be subject to legal and administrative oversight? And *should* they be? Many blockchain developers and advocates, especially those who cut their teeth on Bitcoin in its earlier years, see the answer to the second question as obvious, and the first nearly so. Cryptocurrency, they argue, was created as a solution to the problem of government oversight of value-based transactions. Satoshi Nakamoto's breakthrough was to invent money that escaped the prison of regulation. On this view, the decentralized architecture of consensus computing is a firewall against government intervention. The blockchain is not just immutable; it is "censorship resistant." No higher authority can command a blockchain to do something any more than it can order around the Internet. There is no *there* to regulate. Regulation and the blockchain are antithetical.

Proponents of distributed ledgers are taking up this banner. Wright and De Filippi draw a direct connection between the blockchain's "Lex Cryptographia" and the "Lex Informatica" of software code described in a foundational 1997 article by Fordham law professor Joel Reidenberg.[171] Self-executing smart contracts and decentralized autonomous organizations could, they argue, implement private legal systems without regard to territorial states, much as Bitcoin created a private global currency.

The experience of the past twenty years suggests that governments and powerful private institutions will not so easily be disintermediated.[172] Where they had a strong desire to regulate online activity, they found ways to do so. A similar pattern seems likely for activity on the blockchain, where the stakes are high enough, governments will not simply defer their authority. Even when transactions are entirely digital, peer-to-peer, cross-border, and cryptographically secured, providers and users on the network can be identified and subject to territorial legal obligations.[173] Moreover, outside of

171. *See* Wright & De Filippi, *supra* note 23, at 48–51; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1997). Wright and De Filippi define Lex Cryptographia as "rules administered through self-executing smart contracts and decentralized (and potentially autonomous) organizations." Wright & De Filippi, *supra* note 23, at 48. Reidenberg's "Lex Informatica" and Lessig's "West Coast code" both involve regulations through computer processes rather than laws enacted by governments.

172. *See generally* Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, 69 FLA. L. REV. 887 (2017) (detailing how the vision of unregulated digital spaces failed); GOLDSMITH & WU, *supra* note 163, at 73–77 (showing how governments successfully imposed controls on online activity).

173. *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men With No Names*, *in* PROCEEDINGS OF THE 2013 CONFERENCE ON INTERNET MEASUREMENT, 127 (2013) (showing how seemingly anonymous Bitcoin transactions can be tied to users through

activity that is illegal or in need of extreme security, the incentives are lacking for most users to adopt custom legal systems where the existing ones are functional.[174] And as the creators of The DAO discovered, taking the place of law is not as easy as it may seem.

Wright and De Filippi acknowledge this fact. Yet they remain optimistic that the blockchain will dramatically expand the scope of regulation by code relative to other regulatory modalities.[175] Although ledgers based on Nakamoto Consensus are new, smart contracts and digital currencies are not. Nick Szabo described the mechanism for private regulation by smart contract in the early 1990s. There has not, however, been widespread adoption of cryptographically-based private law.

One reason is that immutable consensus appears to broach no half-measures. As one of the creators of OpenBazaar, a distributed eBay-like online marketplace based on cryptocurrency, put it, "if we allowed people to be accountable towards traditional courts and law, we're opening up [P]andora's box in letting governments interfere by making their own laws about what's 'cheating in a transaction' and what isn't, which leaves room for censorship . . . ."[176]

Many would cheer the use of blockchain technology by activists in China or North Korea to publish illegal pro-democracy manifestos, but it would not stop there. In a truly decentralized network, there is no way to impose limits on money transfers to known terrorists, transactions selling children into modern slavery, or laundering of funds known to be stolen. Universal freedom, at the limit, is tantamount to anarchy: Thomas Hobbes' war of all against all.[177]

---

forensic analytics). For further validation, consider the fate of Grokster, Kazaa, and Streamcast, the decentralized file-sharing services that were shut down when the U.S. Supreme Court declared them liable for contributory copyright infringement. *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). The courts cannot entirely prevent distribution or use of open-source peer-to-peer software, but they can impose liability on companies making money from that software. There is an important difference between fringe activities of bands of users, and substantial markets that can scale for the mainstream.

174. There are similar problems with Josh Fairfield's appealing argument that smart contracts could be used to negotiate terms of service with online sites, returning power to users. *See* Josh A.T. Fairfield, *Smart Contracts*, *Bitcoin Bots*, *and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 46–49 (2014), http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3 [https://perma.cc/YA7N-6XBT]. Service providers that benefit from the current system of clickwrap terms of service have no incentive to adopt an alternate legal regime.

175. *See* Wright & De Filippi, *supra* note 23, at 40–44.

176. Dionysis Zindros, *Trust Is Risk: A Decentralized Trust System*, OPENBAZAAR (Aug. 1, 2017), https://www.openbazaar.org/blog/trust-is-risk-a-decentralized-trust-system/ [https://perma.cc/Q9QW-3P2E].

177. THOMAS HOBBES, LEVIATHAN: OR, THE MATTER, FORME, & POWER OF A

The Augur prediction market illustrates this conundrum.[178] A prediction market allows participants to bet real money on the outcome of future events by "buying" or "selling" predictions like stocks.[179] Don and Alex Tapscott, in their best-selling book *Blockchain Revolution*, are enthusiastic about Augur's potential. After observing that centralized prediction markets such as Intrade were shut down, partly over concerns about "assassination markets and terrorism futures," they state briskly that this will not be a problem for the blockchain-based version: "Augur resolves the issue of unethical contracts by having a zero-tolerance policy for crime."[180]

That entirely begs the question: what is a crime, when laws governing the contracting parties, the developers, and the other participants in the prediction market disagree? Deciding what counts as unethical and what zero-tolerance means is even more difficult. The Augur developers do not control what questions can be posted on the prediction market. On Facebook or Reddit, administrators have the ability to delete illegal, offensive, or harassing material that users post. Not so on a distributed platform such as Augur. If someone lists a criminal contract such as one promoting an assassination, who is to stop it? There seems to be an inherent conflict between the innovative scope of something like Augur and legitimate public policy considerations.

2. Regulatory Debates

Regulatory skirmishes over blockchain-based systems are already being fought. Broadly speaking, there are three major types of controversies: illegality, classification, and legal validity.

The first involves using cryptocurrencies to break the law, or theft of cryptocurrencies through hacking and similar means. The fact that bitcoin can be used to pay for drugs does not by itself raise legal problems for the cryptocurrency; Russian rubles or bars of gold can do the same. The challenge is that a private, decentralized currency that is pseudonymous or anonymous makes it easier to engage in such illegal activity without consequence. Contrary

COMMON-WEALTH ECCLESIASTICALL AND CIVILL (1676). The "war of all against all" has been defined as "people living in a state of nature, without a common power over them to keep them in awe, are in a state of war of every person against every other." Gregory S. Kavka, *Hobbes's War of All Against All*, 93 ETHICS 291, 292 (Jan. 1983).

178. *See* Pete Rizzo, *Augur Bets on Bright Future for Blockchain Prediction Markets*, COINDESK (Mar. 1, 2015) http://www.coindesk.com/augur-future-blockchain-prediction-market/ [https://perma.cc/AH4F-V7DA] (Augur could " 'become one of the definitive prediction markets,' provided it can be maintained by its decentralized community.").

179. Prediction markets can produce highly accurate forecasts by aggregating the *wisdom of the crowd* based on financial incentives. *See* Kenneth J. Arrow et al., *The Promise of Prediction Markets*, 320 SCIENCE 877 (2008).

180. TAPSCOTT & TAPSCOTT, *supra* note 43, at 84.

to fears, no major Western government attempted to ban cryptocurrencies on this basis, and most of the nations that did have since recognized the basic legitimacy of bitcoin and similar currencies. That does not mean they are necessarily accepted as valid within the regulated banking system or for other particular purposes. It only means that transacting with cryptocurrencies in not *per se* prohibited.

The open question is how to deal with code that makes it quite difficult to engage in censorship or tampering, which also makes it easier to engage in terrorist financing or ransomware. A related concern is that code, by creating decentralized digital bearer instruments, creates an attractive target for thieves, both external and internal. These two problems, typified in Silk Road and Mt. Gox respectively, were the most prominent legal questions during the early years of Bitcoin. They remain central today.

A second category involves activity that is basically legitimate but not structured according to the legal requirements for the non-blockchain equivalent. Is a cryptocurrency exchange or a miner considered a money transfer agent or bank under state and federal laws in the United States? Is an issuance of tokens a securities offering under SEC rules, and are those doing the issuing investment managers?[181] Is a cryptocurrency exchange a derivatives marketplace subject to regulatory requirements issued by the Commodity Futures Trading Commission (CFTC)? [182] Should cryptocurrency service providers be required to obtain verified information about their customers and the destination of their transactions, as regulated financial institutions are under Anti-Money Laundering/Know Your Customer (AML/KYC) rules?

181. In testimony before the Senate Banking Committee in February 2018, SEC Chairman Jay Clayton argued that, "by and large, the structures of ICOs that I have seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws." SEC, *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC* (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission [https://perma.cc/JH4M-489Y]. However, he did acknowledge that, "there are cryptocurrencies that, at least as currently designed, promoted and used, do not appear to be securities," leaving open the question of how the SEC would distinguish close cases. *Id.*

182. CFTC Chairman Chris Giancarlo told the Senate Banking Committee in February 2018 that, "[i]n 2015, the CFTC determined that virtual currencies, such as Bitcoin, met the definition of 'commodity' under the [Commodity Exchange Act (CEA)]. Nevertheless, the CFTC does NOT have regulatory jurisdiction under the CEA over markets or platforms conducting cash or 'spot' transactions in virtual currencies . . . ." J. Christopher Giancarlo, Chairman, Commodity Futures Trading Comm'n, Written Testimony Before the Senate Banking Committee, Washington, D.C. (Feb. 6, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37 [https://perma.cc/YQ7R-EJBZ].

Are profits on appreciation in cryptocurrencies subject to income tax as assets, currencies, or neither? The list is long and growing.

Finally, there is the matter of how other legal structures recognize distributed ledgers. States are beginning to move toward treating blockchain-based information analogous to more traditional records. The State of Delaware adopted legislation authorizing distributed ledgers for both government records and regulatory functions such as tracking corporate shares and liens.[183] Arizona passed a law declaring blockchain-based digital signatures as legally enforceable.[184] Vermont made blockchain-based information admissible as evidence in court.[185] As with the classification issues, however, there are many specific questions to consider and many jurisdictions that must act.

3. Dumb Contracts

Smart contracts are another domain in which blockchain-based approaches cannot escape the law. Smart contracts seem to offer a superior alternative to the messy process of legal enforcement. When parties agree on contractual terms, why would they rely on slow, potentially inaccurate or biased, and jurisdictionally-limited courts, when a distributed network of machines can execute the agreement perfectly each time? This view is prevalent among blockchain promoters.[186] The flaw in this reasoning is the

183. *See* Jeff John Roberts, *Companies Can Put Shareholders on a Blockchain Starting Today*, FORTUNE (Aug. 1, 2017), http://fortune.com/2017/08/01/blockchain-shareholders-law/ [https://perma.cc/D89K-MJMH].

184. *See* Stan Higgins, *Arizona Governor Signs Blockchain Bill into Law*, COINDESK (Mar. 31, 2017), https://www.coindesk.com/arizona-governor-signs-blockchain-bill-law/ [https://perma.cc/T2JJ-RMAJ].

185. *See Vermont State to Recognize Blockchain Data in the Court System*, ECONOTIMES (May 18, 2016), http://www.econotimes.com/Vermont-State-to-recognize-blockchain-data-in-the-court-system-209803 [https://perma.cc/VGE2-C33X].

186. *See*, *e.g.*, TAPSCOTT & TAPSCOTT, *supra* note 43, at 109 ("[T]hrough smart contracts . . . [c]ompanies can program relationships with radical transparency . . . . And overall, like it or not, they must conduct business in a way that is considerate of the interests of other parties. The platform demands it."); Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST COMPANY (Sept. 17, 2014), http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app [https://perma.cc/4CUK-5JTY] ("Someday, these programs may replace lawyers . . . ."). Andrew Keys, *Memo from Davos: We Have a Trust Problem. Personal Responsibility and Ethereum Are the Solutions*, CONSENSYS (Jan. 19, 2017), https://media.consensys.net/memo-from-davos-we-have-a-trust-problem-personal-responsibility-and-ethereum-are-the-solutions-19d1104946d8#.c46zvkcks [https://perma.cc/5KKN-SAYH] ("It is early days, and there will surely be the need of attorneys, auditors, and regulators to learn, educate and facilitate smart contracts, but the process will become much more automated, intermediaries will be removed and the **cost of**

failure to distinguish contractual execution from enforcement. Carrying out the specified steps in an agreement is the easy part. It is not a particularly novel phenomenon. Billions of dollars of derivatives trades are executed each day with no human intervention. Computers are programmed with the contractual terms and perform the trades when specified circumstances occur.

The difference is that, with current "computable contracts" (to use a term from law professor and software engineer Harry Surden) execution of the agreement is automated but enforcement is not.[187] The parties involved can revise the agreement before performance, and a court can reverse it after. Smart contracts automate contractual enforcement by ceding all power to the decentralized network maintaining the ledger.[188] Everything beyond the code is just an explanation, or to quote The DAO's terms of service, it is "merely offered for educational purposes."[189]

Automating contractual enforcement is not as neat as automating execution. There are certainly large potential benefits to eliminating the legal system from the contractual process. An unstoppable contract does not operate at the whim of some confused judge, or corrupt local official, or greedy government, or deceitful counterparty. The potential efficiency and automation gains of taking lawyers out of the enforcement loop are great. Yet the same process allowed for the catastrophic failure of The DAO.

No matter how fast they calculate, there are some things computers cannot do as well as humans. The same is true for smart contracts.[190] There is no good way to represent terms such as "reasonable" or "best efforts" in code. And sometimes the meaning of the contract is best understood in terms of the intent of the parties rather than the precise meaning of the terms they used. The DAO was a perfect example. The only difference between the attacker who tried to steal the funds and the miners who took it back through the hard fork was their motivations.[191] That cannot be assessed by a computer.

Even when smart contracts fully execute agreements, parties aggrieved at the results will still resort to litigation.[192] Judges who believe an injustice or legally cognizable injury has occurred will not simply throw up their hands and

trust will plummet.")(emphasis in original).

187. Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012).

188. *See* Werbach & Cornell, *supra* note 25, at 344–48.

189. The DAO's terms of service page is no longer available. For a contemporaneous quotation, see Joel Ditz, *DAOs, Hacks and the Law*, MEDIUM (June 17, 2016), https://web.archive.org/web/20160622212443/https://daohub.org/explainer.html [https://perma.cc/SL53-WKLA].

190. Werbach & Cornell, *supra* note 25, at 365–66.

191. *See id.* at 360–63.

192. *See id.*

defer to a distributed ledger. There may be practical difficulties in identifying pseudonymous or anonymous counterparties, as well as in bringing legal actions against actors in other countries. On the former, there is almost always some known entity to sue, whether the action succeeds or not. Had contributors to The DAO not received their money back through the Ethereum hard fork, some of them doubtless would have sued Slock.it (the developers of the DApp) and the Ethereum Foundation. On the latter concern, cross-border contractual disputes are a staple of modern business among multi-national firms. There are certainly some parties to smart contracts who will refuse to appear in court but established firms are unlikely to do so. Issues of jurisdiction and choice of law are challenging but not insoluble.

C. REGULATION AND INNOVATION

1. Classifying Cryptoducks

Regulation is often posed as the antithesis of innovation. To many, it seems obvious that government involvement in the development of cryptocurrencies and blockchain-based systems will slow and corrupt the development of new systems. If government was only necessary because people could not trust each other without the fear of Thomas Hobbes' mythical Leviathan, then perhaps Satoshi Nakamoto solved that problem.

Here too, however, there is reason to question the old cyber-libertarian view. Regulation of the Internet was actually an important step in its widespread adoption.[193] Many things that "just worked" in the early days turned out to be consequences of a small, close-knit, homogeneous online community. As the Internet began to look more like society, it faced the same political and economic challenges as offline communities. For example, when Microsoft used its monopoly power in the late 1990s to threaten Internet-based startups, the U.S. Government intervened through antitrust enforcement to restrain it.[194] Moreover, the knowledge that governments were operating to police abusive practices helped promote trust in the new and unfamiliar word of virtual transactions. Internet advocates began to call for government intervention to enforce network neutrality rules and privacy protections.[195]

Something similar is likely to occur for distributed ledger technology. The notion that activity on a blockchain cannot be subject to legal enforcement died with the arrest of Ross Ulbricht, if not before. Alexander Vinnik, who allegedly masterminded the massive theft from Mt. Gox and hid his tracks

193. *See* Werbach, *supra* note 172, at 888–89.
194. *See id.* at 909–11.
195. *See id.* at 914–16.

through exchanges and mixer services that make it difficult to trace bitcoin transactions, was also eventually arrested.[196] Particularly with the rise of permissioned ledgers and enterprise-grade systems on top of public ledgers, regulation as a facilitator of blockchain development is gaining currency. Not that the path forward will be easy. The Internet offers a largely positive model of governments acting thoughtfully and nascent industries acting responsibly.[197] There are plenty of counter-examples, but there are enough cases of regulators and the regulated cooperating to allow growth and innovation. There is no guarantee the same will be true for the blockchain.

While Silk Road-like illicit cryptocurrency marketplaces still operate, as do non-blockchain "darknet" sites frequented by erstwhile criminal hackers, infringing content distributors, and identity thieves, such furtive activity is on a limited scale. Most people do not buy drugs online and pay to access streaming media services. The blockchain created a new challenge for law enforcement but so did the Internet. As did the development of strong encryption technology in the early 1990s and the spread of personal computers in the 1980s. The list goes on. The digital technology of the contemporary world is a double-edged sword, capable of good as well as evil. The blockchain adds a new chapter to this story, but does not fundamentally change the balance of power.

To be sure, there are important questions about where to draw lines around surveillance and permissible uses of technology. Criminals and terrorists will try to exploit the blockchain, just as they exploit other technologies whenever possible. Governments will overreact and propose rules with collateral damage to legitimate operations. The point is that these are not new questions. Nor should they be seen as evidence of some fundamental opposition between the blockchain and legality. The more interesting scenarios involve new services that do not set out to break the law. To what extent does the blockchain render superfluous existing legal regimes by interposing a powerful new mechanism for trust and compliance? And to what extent do those existing legal regimes necessarily impose excessive burdens on blockchain-based innovation?

As described in the previous section, much of regulation is a classification exercise. The rules establish status categories, and the regulators police who is subject to those categories. Sometimes the classification is obvious. Verizon

196. *See* Samuel Gibbs, *'Criminal Mastermind' of $4bn Bitcoin Laundering Scheme Arrested*, GUARDIAN (July 27, 2017), https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik [https://perma.cc/2EKW-KAH5].

197. *See* Werbach, *supra* note 172, at 916–17; Kevin Werbach, *The Federal Computer Commission*, 84 N.C. L. REV. 1, 63–65 (2005).

and AT&T do not dispute that in completing conventional circuit-switched landline telephone calls, they are operating as "telecommunications carriers" under the Communications Act of 1934.[198] Sometimes, though, the classification is more difficult. Does Comcast—which historically did not offer telephone service and now does so over specialized packet-switched data networks using Internet technologies—fit in that box? Does Vonage, which owns no network facilities itself and provides voice calling as an application for broadband users? Does Amazon, which now supports voice messages on its Echo personal assistant devices?

The simple answer is that services that look like ducks and quack like ducks should be regulated as ducks. The practical implications in the case of Internet telephony involved more than a decade of contentious debates.[199] That was not necessarily a bad thing. The FCC was sensitive to concerns about preemptive and over-expansive regulation dampening innovation.[200] There was no way the classification controversy could have been resolved quickly in the 1990s because the technology was too immature and its implementation too limited.

Regulators today face a similar challenge in classifying the flock of young "cryptoducks."[201] In 2015, FinCEN, the financial crimes enforcement office of the United States Treasury Department, announced a civil enforcement action against Ripple.[202] Ripple uses a blockchain to greatly reduce the cost of international money transfers, a multi-billion dollar annual market. The problem, in FinCEN's eyes, was that Ripple did so without registering as a regulated money services business.[203] There was nothing wrong with processing money transfers; the issue was doing so without the obligations of existing players in that industry. In particular, Ripple failed to follow the anti-money laundering and "know your customer" (AML/KYC) rules for its users. These are designed to prevent criminals and terrorists from using the banking system to support their activities. In response to the FinCEN action, Ripple

198. 47 U.S.C. § 153(51) (2018).

199. *See* Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED. COMM. L.J. 203, 207 (2013).

200. *See id.* at 231.

201. *See* Camila Russo, *Ethereum Co-Founder Says Crypto Coin Market Is a Time-Bomb*, BLOOMBERG (July 18, 2017), https://www.bloomberg.com/news/articles/2017-07-18/ethereum-co-founder-says-crypto-coin-market-is-ticking-time-bomb [https://perma.cc/H3ZB-6CPC] (quoting Ripple CEO Brad Garlinghouse, stating that, "If it talks like a duck and walks like a duck, the SEC will say it's a duck.").

202. *See* Sarah Todd, *Fincen Fines Ripple Labs Over AML, Says Firm 'Enhancing' Protocol*, AM. BANKER (May 5, 2015), https://www.americanbanker.com/news/fincen-fines-ripple-labs-over-aml-says-firm-enhancing-protocol [https://perma.cc/Q5B6-QRAB].

203. *See id.*

agreed to a $950,000 fine and committed to establish an AML/KYC compliance regime.[204]

The Ripple sanctions were a turning point for the cryptocurrency industry. Unlike Bitcoin, which is a protocol implemented on a distributed network, Ripple is a for-profit company. Its business model depends on its ability to develop partnerships with financial institutions around the world. For Ripple, FinCEN sanctions are a big deal. The AML/KYC process, which typically requires financial services operators to verify physical identity documents such as passports and check against blacklists of individuals, can be onerous, especially for fast-moving and highly-computerized service providers.

Some companies saw the FinCEN action as a signal that the U.S. was not a hospitable jurisdiction for cryptocurrency companies. Xapo, a venture-backed Bitcoin wallet startup, relocated its headquarters from California to Switzerland ten days after the decision.[205] A few months later, the New York State Department of Financial Services began requiring virtual currency businesses operating in the state to obtain a "BitLicense" from the agency.[206]

The idea behind the BitLicense—that financial exchanges transacting in cryptocurrencies should be treated similarly to comparable exchanges transacting in traditional currencies—was sound. However, the implementation was lacking. The requirements for covered entities were onerous. The regulations were drafted in a way that seemed to cover many cryptocurrency businesses other than custodial exchanges, and the certification process was cumbersome. As of early 2017, only three BitLicenses had been granted, despite dozens of applications.[207] The recipients—Circle, Ripple, and Coinbase—were three of the best-funded startups in the space, reinforcing concerns that BitLicense would crowd out innovative small players. At least ten Bitcoin companies announced they were ceasing business in New York as a direct result of the BitLicense.[208]

204. *See id.*

205. *See* Kia Kokalitcheva, *Switzerland is a Banking Capital. But a Bitcoin Capital?*, FORTUNE (May 15, 2015), http://fortune.com/2015/05/15/bitcoin-switzerland-privacy/ [https://perma.cc/JV4Q-B25N].

206. *See* Michael J. Casey, *NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms*, WALL ST. J. (June 3, 2015), https://www.wsj.com/articles/ny-financial-regulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396 [https://perma.cc/5AW4-DQZG].

207. *See* Michael del Castillo, *Bitcoin Exchange Coinbase Receives New York BitLicense*, COINDESK (Jan. 17, 2017), https://www.coindesk.com/bitcoin-exchange-coinbase-receives-bitlicense/ [https://perma.cc/TB5S-PBQM].

208. *See* Daniel Roberts, *Behind the "Exodus" of Bitcoin Startups from New York*, FORTUNE (Aug. 14, 2015), http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/ [https://perma.cc/RC8X-7UXX].

2. *Jurisdictional Competition*

One difference between the regulatory debates in the dot-com and distributed ledger eras is that the United States is no longer the dominant source of activity. The Internet today is highly globalized, but in the 1990s, usage and startup creation were heavily centralized in the United States. In contrast, there are concentrations of distributed ledger activity around the world. London, Berlin, Switzerland, and Singapore are major hubs, with significant centers in mainland China, Canada, South Korea, Japan, Estonia, Argentina, and Hong Kong.[209] Vitalik Buterin, leader of the Ethereum project, is a Russian who grew up in Canada, heads a foundation headquartered in Switzerland, and now lives in Singapore. If he had created an early Internet startup, he would have likely headed to Silicon Valley.

The global distribution of blockchain development activity encourages jurisdictional competition among regions. U.S. dominance of the early Internet industry produced major benefits, both economic and in terms of global soft power. Hoping to be the Silicon Valley of the crypto economy, countries ranging from tiny Gibraltar to Russia are creating new legal frameworks to attract blockchain startups, coin offerings, and other activity. The early leader is the canton of Zug, Switzerland, which combines a stable government, a central location in Europe, a welcoming environment for cryptocurrency companies, and very favorable tax policies.[210] It is bidding to be the cryptocurrency equivalent of Delaware for U.S. incorporation, although the real Delaware, among other locales, seems determined to compete.

The U.S. is still a very important driver of blockchain activity. A significant portion of core Bitcoin development occurs in the United States. New York is one of the primary centers for distributed ledger technology in financial services. Many of the most significant investors in blockchain startups are in the United States, including Digital Currency Group, Blockchain Capital, Andreessen Horowitz, and Union Square Ventures. U.S. technology and services firms such as IBM, Microsoft, and PwC are at the forefront of most large-scale enterprise implementations of distributed ledger applications. The technical talent and technology startup ecosystems in the United States remain unmatched.

It bears repeating that major Internet companies did not locate in Sealand or island tax havens; they went to where the developers and customers were.

209. *See* Richard Kastelein, *Global Blockchain Innovation: U.S. Lags, Europe and China Lead*, VENTUREBEAT (Apr. 16, 2017), https://venturebeat.com/2017/04/16/global-blockchain-innovation-u-s-lags-europe-and-china-lead/ [https://perma.cc/T6ST-QRLC].

210. *See* Kokalitcheva, *supra* note 205 (noting Switzerland's "regulatory stability, international neutrality and its deep-seated tradition in global finance").

Organizations do not just seek the least regulation; they seek the best regulation, among a slate of other factors. A reliable and stable regulatory environment will be important for building trust in blockchain platforms that seek a large user base. Similarly, even jurisdictions keen to attract entrepreneurial businesses in fields such as cryptocurrency do not simply engage in a race to the bottom. Singapore is a hotbed of blockchain activity, due in part to its permissive regulatory attitude. However, the Monetary Authority of Singapore made clear in an August 2017 announcement that initial coin offerings there would be subject to money laundering and terrorist financing restrictions.[211] They would also be regulated as securities offerings when they "represent ownership or a security interest over an issuer's assets or property."[212]

Some small territories focused on generating revenues may take an "anything goes" attitude, but ICOs based there will eventually be less trusted—and therefore less successful in attracting capital. Moreover, the countries where that capital comes from will not be shy about exercising jurisdiction. These are the same reasons why all companies today do not domicile in offshore tax havens.

While the BitLicense may have given the United States a poor regulatory reputation in some cryptocurrency circles, more recent initiatives were more thoughtfully drawn. The Uniform Law Commission, which creates model codes that are widely adopted by state legislatures, adopted a model cryptocurrency law in 2017 that limits the scope of regulation.[213] The CFTC created a LabCFTC group to study cryptocurrencies and engage with the nascent industry.[214] The SEC's investigative report on initial coin offerings and The DAO was widely praised as measured and technically knowledgeable.[215]

---

211. Monetary Auth. of Sing., MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore (Aug. 1, 2017), http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx [https://perma.cc/5RD2-T865].

212. *Id.*

213. Peter Van Valkenburgh, *The ULC's Model Act for Digital Currency Businesses Has Passed. Here's Why It's Good for Bitcoin*, COIN CENTER (July 19, 2017), https://coincenter.org/entry/the-ulc-s-model-act-for-digital-currency-businesses-has-passed-here-s-why-it-s-good-for-bitcoin?mc_cid=c93d4ad9d7&mc_eid=7845af7088 [https://perma.cc/D3E3-RMGA].

214. *See* J. Christopher Giancarlo, Acting Chairman, Commodity Futures Trading Comm'n, Address before the New York FinTech Innovation Lab: *LabCFTC: Engaging Innovators in Digital Financial Markets*, (May 17, 2017), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-23 [https://perma.cc/HF8W-NW8W].

215. *See*, *e.g.*, Kyle E. Mitchell, *Seven Takeaways from the SEC DAO Report*, /DEV/LAWYER, https://writing.kemitchell.com/2017/07/25/DAO-Report-of-Investigation.html

There is no certainty that the United States, or any jurisdiction, will strike the appropriate balance between flexibility and protection in its regulatory approaches to blockchain-based systems. The debates have just begun. Overall, though, regulators who do nothing will be a greater threat to the development of the market than those who engage in thoughtful and evolving efforts to address public policy considerations.

IV. CONNECTING LEGAL AND BLOCKCHAIN TRUST

One way for the blockchain to achieve more robust trust is, perhaps surprisingly, through the legal system. There are several mechanisms to hybridize the blockchain's distributed, algorithmic trust structures with the human-interpreted, state-backed institutions of law. In some contexts, no legal involvement will be needed. In others, where the blockchain is purely supplemental, existing legal arrangements function normally without any special integration. In many cases, however, affirmative steps must be taken to combine the best aspects of distributed ledgers and centralized law.

A. BLOCKCHAIN AND/OR/AS LAW

Lawrence Lessig's point in saying, "code is law," was that code—as well as markets and norms—is just one coequal modality of regulation.[216] Hence the title of his book, describing code "and other laws of cyberspace." Whether it is superior or inferior depends on the context. For example, digital rights management software limits use of content more tightly than copyright law, because it ignores safety valves such as fair use and the first sale doctrine.[217] If there is to be a Lex Cryptographia, therefore, the salient challenge is to identify its strengths and weaknesses, relative to those of traditional legal mechanisms.

Both the legal system and software code can promote trust. Both can also undermine it. As distributed ledgers become more prominent, the simplistic view that they obviate the need for law will become increasingly untenable. The Silk Road takedown showed that the blockchain is not an impermeable shield against legal enforcement, and the DAO attack showed the governance limitations of purely algorithmic systems. Yet the equally simplistic view that

[https://perma.cc/3Y3X-N4VM] (observing that the SEC "deploys the lingo of the industry like a native speaker"); Frances Coppola, *Digital Coins and Tokens Are Just Another Kind Of Security*, FORBES (July 31, 2017), https://www.forbes.com/sites/francescoppola/2017/07/31/sec-tells-digital-coin-and-tokens-issuers-to-comply-with-securities-laws/#19faf7953bb1 [https://perma.cc/B3YA-JUK8] (arguing that with ICOs, "it is the coders, not the investors, who run this show. The SEC has decided to call them to account, and rightly so.").

216. *See* CODE VERSION 2.0, *supra* note 22, at 1.

217. LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE, *supra* note 22.

regulators can and should direct these systems the way they manage centralized equivalents is equally misguided. Both legal actors and the technologists developing the new distributed platforms must take affirmative steps to promote trust. If governed properly, blockchain-based solutions can overcome some of the limitations of legal enforcement, and vice versa.

There are three primary ways the two systems can interact: blockchain as supplement, complement, or substitute.

1. Blockchain Supplements

Where the existing trust architecture is generally functional, the blockchain can operate as an additional layer subject to established legal rules. In such situations, the primary value proposition of the distributed ledger is the speed and efficiency gain of a single shared data record.[218] The blockchain replaces the error-prone messaging structures between participants but does not seek to upend industry structure.[219]

For example, in the United States, there are well-developed legal rules and established practices around real estate transactions. Title insurance is used to protect buyers against defects in land titles.[220] The combination of formal rules and solid norms produces a strong environment of trust. However, there are significant inefficiencies in the system. Title insurance is still largely based on paper records, which must be exchanged among multiple parties. Goldman Sachs estimates moving to distributed ledgers could reduce title insurance premiums in the United States and generate two to four billion dollars in cost savings, thanks to improved efficiency and reduced risk.[221]

In this scenario, the existing legal obligations and centralized business arrangements bear the primary trust burden for the transaction. The blockchain steps in as a potentially superior record-keeping mechanism. Trust in the integrity of the data on the shared ledger is sufficient. The buyer's trust relationships with the seller and various intermediaries such as banks and brokers remain unchanged. Systemic concerns about the technical viability of distributed ledgers remain relevant as trust considerations.[222] The other concerns and limitations of the blockchain as a trust infrastructure are less

218. *See* Schneider et al., *supra* note 15, at 4.

219. *Cf.* UBS, *supra* note 43, at 8 ("Instead of making them superfluous, the blockchain may very well make banks better at what they do.").

220. Title insurance is only necessary because the United States, unlike much of the world, has a system of "registration by title" instead of "title by registration." Valid recording of a title transfer does not guarantee indefeasible ownership. *See* Schneider et al., *supra* note 15, at 33–35.

221. *See* Schneider et al., *supra* note 15, at 4–5.

222. *See id.* at 4.

relevant because the shared ledger is not attempting to supplant legal recourse.

Another example is Corda, a project of the R3 financial industry consortium. It uses distributed ledger technology to manage agreements between financial institutions, thus avoiding the costs of reconciliation.[223] Only identified institutions can participate in the Corda network.[224] The data structure for recording transactions is actually not a blockchain and does not use proof of work, although it employs a consensus-based distributed ledger with smart contracts.[225]

Corda networks can explicitly invite in regulators, who can operate "supervisory observer nodes" with access to real-time information about transactions.[226] This is an important point. If designed to facilitate regulatory oversight, rather than to exclude government as with the original Bitcoin protocols, blockchain-based systems can actually support more effective regulation. The real-time transparency of the shared ledger could allow regulators to identify and respond to problems before the consequences become dire.[227] They could even build compliance mechanisms directly into the system.[228]

With supplementary distributed ledgers, all the work of establishing trust has already been done. The blockchain is used solely to protect the integrity of data on the shared ledger. This is the least ambitious mode of applying the blockchain and the least transformative. It is likely to be most comfortable for regulators and other government actors, because it does not ask them to change their roles or rules substantially. The risks are lower, but the benefits are concomitantly more limited. The blockchain as a supplement to existing legal regimes can promote efficiency and reduce transaction costs, but is unlikely to transform industry structures or produce breakthrough innovations.

2. Blockchain Complements

A second class of applications involves situations where trust based on the legal system is breaking down or insufficient. Distributed ledgers can complement and extend the existing trust architecture. Often the problem in the current environment is that centralized arrangements cannot scale

223. *See* Brown, *supra* note 58.

224. *See id.*

225. *See id.*

226. *Id.*

227. *See* UBS, *supra* note 43, at 24 ("In a blockchain-based system, where transactions are immediate and the ledger public, regulators could have a real-time view of what is transpiring in the system at all times.").

228. *See id.* at 25.

effectively enough, preventing desirable solutions. Where the blockchain powers new markets, it often does so in ways that are complementary to existing legal arrangements.

Consider the challenge of orphan works under copyright law.[229] These are works whose rights-holders cannot be located. Those who wish to use them, for example, documentary filmmakers wishing to incorporate archival footage, cannot negotiate a license even if they wanted to. Orphan works are thus in legal limbo. The risk of statutory damages for copyright infringement is a severe threat that scares away potential users of the material, even though in some cases it might actually be in the public domain. The marketplace envisioned by copyright law, in which authors can control and monetize their output, fails to develop.

Orphan works are a good opportunity to use a shared registry to create a new market.[230] A blockchain-based registry would be available to all and would not give excessive gatekeeper power to any intermediary. It could keep track of efforts to engage in the diligent search for rights-holders required under copyright law.[231] Smart contracts could be used to ensure that those who use orphan works pay licensing fees to legitimate rights-holders who come forward (most likely vetted by an arbitration mechanism). The distributed ledger here would not take the place of standard copyright law, but it would extend it in a direction that it cannot easily go today.[232]

A more ambitious version of a similar idea is to give artists and other content creators persistent control over rights associated with their creations. Today, digital rights management systems are controlled by intermediaries and distributors, not the creators themselves. As a result, many artists have difficulty receiving sufficient compensation. Initiatives are underway to decentralize control over digital rights using distributed ledgers, giving power back to artists, including Ujo Music, PeerTracks, and the Open Music

229. *See generally* Jerry Brito & Bridget Dooling, *An Orphan Works Affirmative Defense to Copyright Infringement Actions*, 12 MICH. TELECOMM. & TECH. L. REV. 75 (2005).

230. *See* Patrick Murck, *Waste Content: Rebalancing Copyright Law to Enable Markets of Abundance*, 16 ALB. L.J. SCI. & TECH. 383, 416–17 (2006) (discussing the potential new market if orphan works are liberated).

231. *See generally* Jake Goldenfein & Dan Hunter, *Blockchains*, *Orphan Works*, *and the Public Domain*, 41 COLUM. J.L. & ARTS 1, 22–25 (2017) (describing a blockchain-based system to solve the orphan works problem). The prohibition on formalities in international copyright agreements would make it difficult to establish a mandatory registry for orphan works.

232. Similarly, the blockchain could be used to create unique digital assets that allow for a digital version of copyright's longstanding first sale doctrine. *See* Patrick Murck, *The True Value of Bitcoin*, CATO UNBOUND (July 31, 2013), http://www.cato-unbound.org/2013/07/31/patrick-murck/true-value-bitcoin [https://perma.cc/Y28Q-4MD7].

Initiative.[233]

These ventures still face the challenge of entrenched power dynamics. Even if artists have the technical capacity to control their output, they may not have the practical ability to do without the marketing and distribution power of the music industry. In all likelihood, a limited segment of artists will be able to take advantage of distributed rights platforms, but this could still be an advance over the current artist-hostile system. As with the supplemental applications, these blockchain-based solutions leave conventional law (in this case, the copyright system) in place. However, they extend it to new applications that are untenable through existing trust architectures. As a result, there may need to be mappings between the apparatus of legal enforcement and the technical framework of distributed ledgers.

3. Blockchain Substitutes

The final category of blockchain legal applications involves no backstop of traditional legal enforcement. The saga of The DAO illustrates the dangers of this path.[234] However, where legal enforcement is weak, the blockchain can in some cases function as a substitute. If there is no workable rule of law to begin with, rule of blockchain may be a significant improvement. Several billion people in the developing world, for example, lack access to bank accounts and the opportunities for easy payments and credit they bring. Bitcoin and other cryptocurrencies offer a shortcut to address this challenge of the unbanked.[235] In 2017, the United Nations World Food Program conducted a successful trial using the Ethereum blockchain to track food aid distribution to 10,000 Syrian refugees in Jordan.[236] The program provided

233. *See* Gideon Gottfried, *How 'the Blockchain' Could Actually Change the Music Industry*, BILLBOARD (Aug. 5, 2015), http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry [https://perma.cc/84TX-3HGM]; Ian Allison, *Imogen Heap Shows How Smart Music Contracts Work Using Ethereum*, INT'L BUS. TIMES (Oct. 29, 2015), http://www.ibtimes.co.uk/imogen-heap-shows-how-music-smart-contracts-work-using-ethereum-1522331 [https://perma.cc/QP8L-BJRM]; Malcolm Gay, *Can Major Initiative Led by Berklee Solve Music-Rights Problems?*, BOSTON GLOBE (June 13, 2016), https://www.bostonglobe.com/arts/music/2016/06/12/berklee-lead-musical-rights-initiative/aXBXC8adJgXE4IRRt8dcKO/story.html [https://perma.cc/T6FJ-57J2].

234. *See supra* notes 135–139 and accompanying text.

235. *See* Mark S. Miller & Marc Stigler, *The Digital Path: Smart Contracts and the Third World*, *in* MARKETS, INFORMATION, AND COMMUNICATION: AUSTRIAN PERSPECTIVES ON THE INTERNET ECONOMY 63–88 (2003), http://www.erights.org/talks/pisa/paper/index.html [https://perma.cc/NFP8-R2J4]; Susan Athey, *5 Ways Digital Currencies Will Change the World*, WORLD ECON. FORUM (Jan. 22, 2015), https://agenda.weforum.org/2015/01/5-ways-digital-currencies-will-change-the-world/[https://perma.cc/Z8AU-8RF2].

236. *See* Leigh Cuen, *UN Using Blockchain Technology to Help Refugees, Fight World Hunger*, INT'L BUS. TIMES (May 4, 2017), http://www.ibtimes.com/un-using-blockchain-technology-help-refugees-fight-world-hunger-2534759 [https://perma.cc/Q2FG-VUJ2].

accountability in an environment where conventional legal enforcement is difficult.

In many parts of the world, land title records are incomplete and challenging for ordinary citizens to interact with. The Peruvian economist Hernando de Soto argues that the absence of well-functioning land registration systems in the developing world is a major impediment to economic development.[237] Initiatives are underway in various parts of the world to use the blockchain as a solution, including Ghana and the country of Georgia.[238]

The hurdle for these systems is the human actors outside the ledger. A corrupt local land office that refuses to record information accurately on a blockchain, or that disregards the information it reports, can still do so. One of the first initiatives to record land titles on a blockchain, an effort in Honduras involving the startup Factom, never got off the ground because of difficulties with the local partners.[239] For that reason, the initiatives likely to move forward first are in relatively stable countries such as Georgia, and very stable ones such as Sweden, even though the need might be greater in the developing world.

And of course, communities will use the blockchain to substitute for law when their goal is to evade legal responsibilities. Only when the point is to ensure honor among thieves in a dark marketplace such as Silk Road is the blockchain in opposition to legal enforcement. Recall the case of Uber in Buenos Aires. There, bitcoin was used to route around limits on payment processing at the behest of the city government; the transactions involved were not *per se* illegal.[240] The cryptocurrency gave Uber leverage by establishing a trusted payment option outside traditional centralized channels.[241] Such

237. *See* HERNANDO DE SOTO, THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE 15–28 (2000).

238. *See* Laura Shin, *Republic of Georgia to Pilot Land Titling on Blockchain With Economist Hernando De Soto, BitFury*, FORBES (Apr. 21, 2016), http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#5a2979f36550 [https://perma.cc/ZHW3-4JVL]; Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, FORBES (Apr. 5, 2016), http://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#59ee9ab11029 [http://perma.cc/99TT-4RYD].

239. *See* Pete Rizzo, *Blockchain Land Title Project 'Stalls' in Honduras*, COINDESK (Dec. 26, 2015), https://www.coindesk.com/debate-factom-land-title-honduras/ [https://perma.cc/MKJ8-ZM87].

240. *See supra* note 101.

241. The Buenos Aires government could not block the Uber riders from using the distributed Bitcoin network. However, it could probably issue an order against the Swiss firm, Xapo, that provides the debit cards which translate between Bitcoin and the local currency. *See* Valenzuela, *supra* note 101.

scenarios are real, but they occupy a relatively small and shrinking portion of the distributed ledger landscape.

B. MAKING LAW MORE CODE-LIKE

In any of the three scenarios just described, the relationship of blockchain-based systems and legal institutions can be smooth or rough. Blockchain developers cannot ignore the law, but neither can governments disregard the growing significance of the blockchain. One way to bridge the gap is for law to adapt. Some of that will happen naturally as regulators, legislators, and judges confront the challenges and opportunities this foundational new technology presents. More explicit steps can accelerate the process.

1. Safe Harbors and Sandboxes

A safe harbor is a regulatory provision formally limiting legal enforcement. When firms can take sufficient steps to police themselves, the safe harbor incentivizes them to do so. It also defines what specific conduct is necessary. Perhaps the best known safe harbor in the technology world is Section 230 of the Communications Act, which was adopted in 1996 as part of the Communications Decency Act (CDA).[242] It shields online intermediaries from liability for content flowing across their systems. The breadth of this safe harbor, created in the early days of the commercial Internet, is problematic. It shields intermediaries even when they ignore harmful activity, such as online harassment.[243] On the other hand, the CDA safe harbor was a significant factor in the rapid growth of online intermediaries.[244] It was particularly important to the spread of user-driven "Web 2.0" services and social media.[245]

Based on this history, Coin Center has proposed a new safe harbor for blockchain-based startups.[246] Specifically, it urges legislation stating that non-custodial services—those which do not obtain control over user funds—are exempt from rules governing money transmitters. This would acknowledge that distributed ledgers change the relationship between those who move

242. 47 U.S.C. § 230 (2018).

243. *See*, *e.g.*, Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 359 (2014).

244. *See*, *e.g.*, Derek Khanna, *The Law that Gave Us the Modern Internet—and the Campaign to Kill It*, ATLANTIC (Sept. 12, 2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-Internet-and-the-campaign-to-kill-it/279588/ [https://perma.cc/HG7W-VJEB].

245. *See id.* ("It was simple and intuitive to understand for entrepreneurs and . . . has functioned as a permission slip for . . . [e]ntrepreneurs [to found] the user-generated content sites we know and love today.").

246. *See* Peter Van Valkenburgh, *Bitcoin Innovators Need Legal Safe Harbors*, COIN CENTER (Jan. 24, 2017), https://coincenter.org/entry/bitcoin-innovators-need-legal-safe-harbors [https://perma.cc/C5ES-KZGN].

currencies and the users who own that currency.

Prior to Bitcoin, possessing money meant having the ability to do anything with it. An online service such as PayPal, where a user parks funds, has the power (absent legal or regulatory obligations) to steal it or send it to terrorists. On a blockchain, by contrast, many actors such as miners, DApps, and wallet software providers touch the records of transactions, but without the private keys governing user accounts, they lack any such capabilities. Only the custodial exchanges which users authorize to move funds operate like traditional money transmitters. Embedding the distinction between possession and control in a legal safe harbor would remove uncertainty from the market and make the legal regime more consistent with technical realities.

Sandboxes are similar to safe harbors but limited in time or scale. A regulatory sandbox exempts certain companies or activities from regulation as a means to foster experimentation and startup activity. Unlike a safe harbor, a sandbox is not necessarily permanent, and it usually only applies to new companies. One of the concerns about the Internet safe harbors is that they were designed to help nascent firms without the resources to police content on their platforms but wound up helping titans like Google and Facebook. A sandbox can be constructed to apply to organizations at early stages of development and disappear when they mature.

In the United Kingdom, the Financial Conduct Authority (FCA), the primary financial regulator, established a Fintech Sandbox program that allows companies to experiment with new services.[247] Companies apply to operate in the sandbox, and if approved, they receive individualized waivers and supervised special authorizations to engage in pilot projects without regulatory concerns. There is nothing quite comparable in the United States at this time, although the CFTC's LabCFTC program is designed to move in a similar direction.[248]

In contrast to the "prohibit if not permitted" approach of New York's BitLicense, a sandbox model would encourage the kind of "permissionless innovation" that was critical to the development of the Internet marketplace.[249] The ethos of software developers, including those building blockchain-based systems today, is reflected in the Internet Engineering Task Force motto that

247. *See Financial Conduct Authority Unveils Successful Sandbox Firms on the Second Anniversary of Project Innovate*, FIN. CONDUCT AUTH. (July 11, 2016), https://www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary [https://perma.cc/86BN-RSR7].

248. *See* Giancarlo, *supra* note 214.

249. *See generally* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2016).

decisions should be based on "rough consensus and running code."[250] Well-designed sandboxes can make it easier for startups to write that running code and give regulators visibility to understand the public policy concerns that may arise.

2. Modularizing Contracts

Private law can be made more code-like as well. Most business contracts are essentially modules that lawyers string together and customize. Some sections describe business terms and what should happen under defined circumstances. Such "operational" aspects are the kind that can often be automated in smart contracts.[251] Other parts of the contract are non-operational or legal terms, such as limitations on damages, indemnification, confidentiality, and choice of law or forum. Lawyers often re-use standard clauses, which they adapt and negotiate for the particular transaction.

To make this contract drafting process more analogous to the formalized coding that goes into a smart contract, the contractual clauses can be represented as components that are assembled into a digital document using a markup language. Templates could be created from these modules to provide baseline agreements for common scenarios. Lawyers would still have a role in customizing the templates, deciding which variations to use, and negotiating contentious terms. The skills required of lawyers would have to change, with the field becoming more like legal engineering.[252] Legal code audits could also be implemented to ensure the contracts match the parties' intent, analogous to the security audits widely used by firms engaged in software development.[253]

250. *See* Andrew L. Russell, *'Rough Consensus and Running Code' and the Internet-OSI Standards War*, *in* 28 IEEE ANNALS OF THE HIST. OF COMPUTING 48, 49 (2006).

251. Christopher D. Clack, et al., Smart Contract Templates: Foundations, Design Landscape and Research Directions 5 (Aug. 4, 2016) (unpublished manuscript), https://arxiv.org/pdf/1608.00771.pdf [https://perma.cc/PQW8-8GCJ] (defining operational aspect as "the parts of the contract that we wish to automate, which typically derive from consideration of precise actions to be taken by the parties and therefore are concerned with performing the contract.").

252. Or perhaps creating a new niche for legal hackers. Following the DAO attack, security expert Robert Graham suggested that, "in the past, people hired lawyers to review complicated contracts. In the future, they'll need to hire hackers. After a contract is signed, I'm now motivated to hire a very good hacker that will keep reading the code until they can find some hack to my advantage." Robert Graham, *Ethereum/TheDAO Hack Simplified*, ERRATA SEC. (June 18, 2016), http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html#.V2wGDOYrKV5 [https://perma.cc/9HLC-HRNM].

253. There are already technical auditing firms that review smart contract code for bugs or security vulnerabilities. *See* Alyssa Hertig, *Blockchain Veterans Unveil Secure Smart Contracts Framework*, COINDESK (Sept. 15, 2016), https://www.coindesk.com/blockchain-veterans-unveil-secure-smart-contracts-framework/ [https://perma.cc/L2MB-442J]. Traditional auditing firms are also considering how they might participate in this new world. As Grainne

Several initiatives are developing exactly this sort of system. These include Open Law, a project of Ethereum development studio Consensys;[254] the startups Clause.io and Agrello;[255] the smart contracts templates group of the R3 consortium;[256] and the CommonAccord and Legalese projects.[257] Some of these are focused more on the non-operational side, making the process of legal contract drafting more efficient. Others are concentrating more on operational templates that can be incorporated into smart contract systems. By standardizing and reviewing the elements of the smart contract ahead of time, such mechanisms should cut down on the errors that led to failures such as The DAO hack.

As the contractual mechanisms around blockchains become more standardized and modularized, the line between enforcement through law and code will blur. Something similar has already occurred in derivatives trading, where standardized master agreements and terminology under the International Swaps and Derivatives Association (ISDA) allows widespread automation of transactions even without the use of distributed ledgers.[258]

C. MAKING CODE MORE LAW-LIKE

Just as regulators and lawyers can adapt to the blockchain environment, distributed ledger systems can become more hospitable to legal enforcement. The three main pathways being explored are to integrate the terms of legal and smart contracts, to integrate traditional legal enforcement mechanisms into smart contracts, and to integrate law-like governance processes into

McNamara stated at a financial services conference, "we're looking at how to audit the technology using the technology." Grainne McNamara, Blockchain Strategist, PricewaterhouseCoopers, Address at the American Banker Blockchains + Digital Currencies Conference (June 13, 2017) (transcript on file with author).

254. *See Introducing OpenLaw*, CONSENSYS (July 25, 2017), https://media.consensys.net/introducing-openlaw-7a2ea410138b [https://perma.cc/T896-2LCU].

255. *See Clause.io Sets Out Strategy With Its Smart Contract Engine*, ARTIFICIAL LAW. (July 6, 2017), https://www.artificiallawyer.com/2017/07/06/clause-io-sets-out-strategy-with-its-smart-contract-engine/ [https://perma.cc/FE9J-VZVV]; *Agrello Becomes 1st LegalTech Co. To Launch Its Own Digital Currency*, ARTIFICIAL LAW. (July 17, 2017), https://www.artificiallawyer.com/2017/07/17/agrello-becomes-1st-legaltech-co-to-launch-its-own-digital-currency/ [https://perma.cc/578M-W5XQ].

256. *See generally* Clack, et al., *supra* note 251.

257. COMMONACCORD, http://commonaccord.org [https://perma.cc/D7LZ-BAYG] (last visited Sept. 2, 2018); LEGALESE, http://legalese.com [https://perma.cc/2TUM-7SXM] (last visited Sept. 2, 2018).

258. *See* INT'L SWAPS & DERIVATIVES ASS'N., The Future of Derivatives Processing and Market Infrastructure [hereinafter ISDA WHITE PAPER] (Sept. 2016), at 15, https://www2.isda.org/attachment/ODcwMA==/Infrastructure%20white%20paper.pdf [https://perma.cc/KE4P-BZDS].

blockchain platforms.

1. Contractual Integration

The simplest way to make blockchain-based systems more consistent with legal enforcement is literally to connect the two. Even if smart contracts can be enforced in court under basic principles of contract law, they serve a different function than the fundamentally remedial institution of contract.[259] Smart contracts are good at setting forth anticipated conditions and consequences *ex ante*, and then ensuring the consequences occur upon fulfillment of the conditions. Legal contracts are good at cleaning up the mess when, inevitably, things do not go according to plan. There is no reason, however, that the two mechanisms cannot coexist. Difficulties arise when the smart and legal contracts disregard one another, as in The DAO collapse.

The alternative approach is to pair smart contracts and legal contracts explicitly. Information security expert Ian Grigg first explored this idea in 2004, before the advent of cryptocurrencies, as part of the Ricardo digital transaction platform for financial instruments.[260] Ricardo defined its contracts as having three components: legal code (the human-readable text of a contract), computer code (the executable steps of s smart contract), and parameters (the variables that influence how the computer code executes). The legal code included the cryptographic hash string of the computer code, which guaranteed that it was referencing the proper smart contract. In parallel, the smart contract included the cryptographic hash string of the legal contract text. Thus, the two were definitely linked. If there was a problem with the smart contract, one could turn to the legal contract for resolution. Grigg called this structure the Ricardian contract because it was developed for the Ricardo system.[261]

Like Szabo's original notion of smart contracts, Ricardian contracts were largely a theoretical construct prior to the blockchain, and in particular, Ethereum's successful implementation of blockchain smart contracts.[262] The approach has since been rediscovered. Several groups are building solutions using the mutual hashing of smart and legal contracts, including a subgroup of the R3 consortium led by the British bank Barclays,[263] the Monax Burrow

259. *See* Werbach & Cornell, *supra* note 25, at 318.

260. *See generally* Ian Grigg, *The Ricardian Contract*, *in* PROCEEDINGS OF THE FIRST IEEE WORKSHOP ON ELECTRONIC CONTRACTING 25 (2004).

261. *See id.* at 25.

262. The Ricardo platform that Grigg was building never took off.

263. *See* Clack et al., *supra* note 251, at 12; Bailey Reutzel, *BNP Paribas Works With Blockchain Startup to Open Source Law*, COINDESK (May 5, 2016), http://www.coindesk.com/commonaccord-legal-smart-contracts-prove-beneficial-one-bank-veritcal/ [https://perma.cc/P23T-DS6N]; Ian Allison, *Barclays' Smart Contract Templates*

software now part of the Hyperledger open source project,[264] and OpenLaw.[265]

With this approach, the human and smart contracts explicitly reference one another through digital signatures. In contrast to The DAO terms of service, which privileged the algorithmic contract over the human-readable explanations, this approach makes each dependent on the other. A court or other decision-maker can use the conventional contract to understand the intent of the smart contract, which handles execution of the agreement.[266]

Every smart contract will not require a bespoke human-negotiated contract alongside it. As with the contract system today, forms will be widespread for business-to-consumer and low-value agreements. In many cases, the costs of dispute resolution will so far exceed the potential recovery that "quick-and-dirty" reliance on the naïve actions of machines will be sufficient. Regulation of intermediaries such as registries may obviate the need to specify legal terms for every associated smart contract. As blockchain-based systems become more familiar, a combination of customer, common law, and model legislation is likely to develop to address common situations.

2. Oracles and Computational Courts

Contractual integration links the substantive terms of a legal agreement with those of a smart contract. A different approach is to take some aspects of enforcement out of the automated system of the smart contract. In other words, a smart contract can be self-executing but not fully self-enforcing, thus avoiding the ambiguities and limitations of automated code-based enforcement.

Many smart contracts will already need to interface with the outside world. For example, a call option to buy a security at a certain price can be executed

Stars in First Ever Public Demo of R3's Corda Platform, INT'L. BUS. TIMES (Apr. 18, 2016), http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329 [https://perma.cc/5SFT-XLAY].

264. *See Putting the Contracts in Smart Contracts*, MONAX, https://monax.io/explainers/dual_integration [https://perma.cc/YQK4-43LS].

265. *See supra* note 254.

266. In the wake of the DAO attack, researchers have proposed technical mechanisms tantamount to rescission of smart contracts, without necessarily involving judicial actors. *See, e.g.*, Ittay Eyal & Emin Gun Sirer, *A Decentralized Escape Hatch for DAOs*, HACKING, DISTRIBUTED (July 11, 2016), http://hackingdistributed.com/2016/07/11/decentralized-escape-hatches-for-smart-contracts/ [https://perma.cc/6DBH-487G] (proposing an "escape hatch" mechanism in which all transactions would be buffered and subject to reversion based on a crowdsourcing mechanism); Bill Marino & Ari Juels, *Setting Standards for Altering and Undoing Smart Contracts*, *in* RULE TECHNOLOGIES. RESEARCH, TOOLS, AND APPLICATIONS: 10TH INTERNATIONAL SYMPOSIUM, RULEML 2016, STONY BROOK, NY, USA, JULY 6–9, 2016. PROCEEDINGS 151 (2016) (detailing scenarios for modifying or rescinding smart contracts).

algorithmically on the blockchain, with payment in bitcoin or another cryptocurrency. The blockchain, however, does not know stock prices. That information must be provided to the smart contract through an external connection, either to an automated data source or a human arbiter. Those external sources are called oracles.[267] Some oracles are just traditional data feeds designed with interfaces for smart contracts to process them in an automated way. Thomson Reuters, one of the largest business publishing firms, is making some of its data feeds available in a manner designed to function as smart contract oracles.[268] Oraclize is a startup focused entirely on turning data feeds into oracles.[269]

As Wright and De Filippi point out, oracles could be extended to dispute resolution by courts or private actors.[270] Oracles can also be humans. Consider a simple smart contract in which each of the parties has a private key and a third key is given to an expert arbitrator. The smart contract requires two of three keys in order to execute. If the parties agree the contract has been fully performed, they each provide their key and the smart contract executes. If there is a dispute, they turn to the arbitrator. She either provides her key along with that of the party seeking to enforce the contract or refuses it and therefore prevents completion of the transaction. This system mimics a legal arbitration process.

Smart contracts could by default incorporate arbitration mechanisms or rollback provisions. They could be designed to operate only in extreme cases, with high barriers through the design of the multisignature (or "multisig") process. This would help address extraordinary cases such as The DAO attack. Or they could be used to create a regular outlet for private dispute resolution, the way so many business-to-consumer form contracts today push disputes into arbitration. Balaji Srinavasan, a noted blockchain investor and founder of the startup 21, suggests that, "over time blockchains will provide 'rule-of-law-as-a-service' as an international, programmable complement to the Delaware Chancery Court."[271]

267. *See* Stefan Thomas & Evan Schwartz, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts* (July 17, 2014), https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts [https://perma.cc/S5TV-Q3JH].

268. *See* Maria Terekhova, *Thomson Reuters Is Making a Blockchain Push*, BUS. INSIDER (June 15, 2017), http://www.businessinsider.com/thomson-reuters-is-making-a-blockchain-push-2017-6 [https://perma.cc/P8HK-GV8L].

269. ORACLIZE, http://oraclize.it (last visited Sept. 3, 2018) [https://perma.cc/5CP7-VV8H].

270. *See* Wright & De Filippi, *supra* note 23, at 50.

271. Balaji S. Srinivasan, *Thoughts on Tokens*, MEDIUM (May 27, 2017), https://medium.com/@balajis/thoughts-on-tokens-436109aabcbe [https://perma.cc/NK5P-KNU6].

The distributed nature of the blockchain may call for new enforcement mechanisms that are themselves distributed.[272] For example, new international arbitration networks might need to be developed that were tuned to the needs of blockchain disputes, much as the World Intellectual Property Organization created the Uniform Dispute Resolution Process (UDRP) to handle trademark disputes over Internet domain names.[273] However, because arbitration decisions could, in some cases, be directly executed on the blockchain and would apply on a peer-to-peer basis, blockchain arbitration systems would be different than any current example.[274] Andreas Antonopoulos and Pamela Morgan proposed a decentralized arbitration and mediation network (DAMN) in 2016.[275]

Even more speculative—yet under development today in some blockchain-based projects—are computational courts, or as they are sometimes called, computational juries. Instead of arbitrators resolving disputes, these mechanisms employ the wisdom of the crowd through prediction markets.[276] The Augur Ethereum-based prediction market is developing this approach internally. One reason real-money prediction markets such as Intrade have been shut down by regulators is that they can be used in illegal or unethical ways. A prediction market for murder of one's mother-in-law, for example, would be troublesome.

Augur proposes to address such unethical markets through the same

272. Ethereum creator Vitalik Buterin has speculated about a regime of "decentralized courts" to resolve disputes. *See* Vitalik Buterin, *Decentralized Court*, REDDIT, https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/ [https://perma.cc/M5UY-5A39] (last visited Sept. 2, 2016); Izabella Kaminska, *Decentralised Courts and Blockchains*, FIN. TIMES (Apr. 29, 2016), http://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/ [https://perma.cc/BRV3-EBC6].

273. *See generally* Luke A. Walker, *ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY TECH. L.J. 289 (2000).

274. *See* Abramowicz, *supra* note 47, at 405.

275. *See* Michael del Castillo, *Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration With DAO Proposal*, COINDESK (May 26, 2016), http://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key/ [https://perma.cc/VW7G-E5FK]. It is based on the New York Convention, under which sixty-five countries agreed that their courts would enforce decisions of recognized arbitrators. The tradeoff of an arbitration regime is that it reintroduces intermediation to the decentralized blockchain environment. *See* James Grimmelmann & Arvind Narayanan, *The Blockchain Gang*, SLATE (Feb. 16, 2017), http://www.slate.com/articles/technology/future_tense/2016/02/bitcoin_s_blockchain_technology_won_t_change_everything.html [https://perma.cc/7RGA-YMAC] ("[A]n arbitrator who can give you back your car is also an arbitrator who can take your car away from you. He's an intermediary of precisely the sort the block chain was supposed to eliminate.").

276. *See* Rizzo, *supra* note 178.

reporting process it uses to verify outcomes of predictions. Augur uses a system in which participants in the marketplace purchase a token called Rep.[277] When someone creates a contract, such as a prediction that the President will be impeached within a certain period of time, they post a bond in Rep. They win additional Rep if the prediction is correct and lose the bond if incorrect. A randomly selected group of reporters (analogous to a jury) are tasked with verifying the outcome. Those reporters must also post a bond. The reports can be challenged, and if a second randomly selected jury agrees with the challenge, the reporter providing incorrect information loses her bond. This process is designed to produce verified outcomes without having to trust a specific central authority. It is admittedly complicated, and could fail. The process, though, illustrates a promising pathway to make decentralized blockchain-based technology operate more like the established institutions of the legal system.

Any of these voluntary mechanisms could be baked into blockchain applications, or even in some cases legally mandated. The full range of incentives and governance mechanisms could be used to encourage compliance with desirable approaches. Furthermore, just as the Federal Arbitration Act directs courts to accept private arbitration decisions when fraud is not involved, legislation could create similar legal force for appropriately designed blockchain dispute resolution systems.[278]

3. On-Chain Governance

One of the biggest problems with blockchain networks as governance institutions is that it is difficult to change their foundational rules. Systems that have well-structured mechanisms for considering and implementing changes to consensus rules or other technical attributes are not fundamentally decentralized. They may operate more like industry standards bodies or open source projects, where rule changes occur through collective agreement rather than the hierarchical edicts of corporate management.

Ethereum resembles Wikipedia more than General Electric. Wikipedia is a great example of how a novel organizational approach combined with massive user participation can transform a market.[279] It not only replaced other encyclopedias, it created perhaps the biggest open information resource in history. If Ethereum achieves as much, it will be a tremendous success story.

277. *See* Tony Sakich, Jeremy Gardner & Joey Krug, *What Is Reputation?* (June 18. 2015), http://augur.strikingly.com/blog/what-is-reputation [https://perma.cc/B35A-EAMS].

278. *See* Federal Arbitration Act, 9 U.S.C. § 10 (2012).

279. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); DON TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2008).

But the promise of Ethereum and other blockchain networks is greater still. To be truly transformative, these systems would have to evolve their governance using the same decentralized approach they use to enforce it.

Even though Bitcoin lacks a formal governance structure, its developers have rigged a voluntary signaling mechanism called BIP 9.[280] Under BIP 9, miners can broadcast their willingness and readiness to adopt changes. This process was used for the Segwit upgrade. Segwit is automatically activated on the Bitcoin network after a threshold of 80 percent network hashing power signaled for it.[281] While BIP 9 thus enables a crude voting mechanism for controversial Bitcoin protocol upgrades, it leaves much to be desired as on-chain governance. The thresholds for approval are arbitrary. They are set centrally by those who propose the upgrades. Even more important, BIP 9 only signals; it does not enforce policies. Debates about scaling Bitcoin still require agreement among a critical mass of network participants.

There are several efforts underway to create true on-chain governance. A project called Rootstock is trying to create a smart contracts layer on top of Bitcoin, with a built-in process giving both miners and users power to make binding votes on network changes. Decred and Tezos are building entirely new blockchains with governance mechanisms baked in. These systems use various algorithms to allow network participants to vote on changes to the protocol, which are automatically implemented when adopted. Decred successfully executed a change to its algorithm for allocating these voting tokens using the governance mechanism in Spring 2017.[282] Tezos, which raised $200 million in one of the largest initial coin offerings, has generated tremendous interest for its governance approach.[283]

There are limitations to these systems. They internalize many aspects of the rules governing distributed ledger systems. However, they rely on hard-coded rules for democratic voting to carry out changes. This may be a very good way to govern; it may even be, to paraphrase Winston Churchill, the best

280. BIP stands for Bitcoin Improvement Proposal. It is a mechanism to propose technical changes to Bitcoin for community review based on the Internet Engineering Task Force's "Request for Proposal" process.

281. This process was technically referred to as BIP 91.

282. *See* Christine Chiang, *Decred Launches Decentralized Voting Process for Blockchain Protocol Changes*, BRAVE NEWCOIN (June 17, 2017), https://bravenewcoin.com/news/decred-launches-decentralized-voting-process-for-blockchain-protocol-changes/ [https://perma.cc/9F8B-2F7L].

283. *See* Alice Lloyd George, *Behind the Scenes With Tezos, a New Blockchain Upstart*, TECHCRUNCH (July 12, 2017), https://techcrunch.com/2017/07/12/behind-the-scenes-with-tezos-a-new-blockchain-upstart/ [https://perma.cc/HTC6-H5D3].

possible among a set of bad options.[284] It is not perfect. Any governance structures that are imperfect will eventually need to be modified by someone. Moreover, humans need to define the rule changes that network participants vote on, and code the software to implement them if adopted. The on-chain governance systems make the blockchains operate more like a human-based legal or governance regime, but they still leave gaps that traditional institutions must fill.

V. CONCLUSION: STRANGE BLOCKFELLOWS

Distributed ledgers are the first foundational technology in twenty years whose potential impact matches that of the Internet. At a time when trust in centralized power structures is waning, the blockchain's "trustless trust" offers a compelling alternative. Further growth will depend partly on technical advances, partly on adoption patterns, partly on the business innovations built on top of distributed ledger platforms, and partly on resolution of the governance challenges to the blockchain's trust architecture. It is tempting to see law and regulation primarily as impediments to these processes, but that would be a mistake. Too much law could stifle the blockchain or drive it underground, yet so could too little law.

These are still early days for the blockchain. Satoshi Nakamoto's Bitcoin white paper was published less than a decade ago, and Ethereum just launched in 2015. As big as the market has grown, there is far less at stake, and therefore far less path dependence, than there will be in three, or five, or ten years. Now is the time to develop hybrids of law and code. Regulators, legislators, and courts can take the initiative to create both clarity and explicit spaces for experimentation. Blockchain developers must also take responsibility to find common ground.

Like the Internet, the blockchain is a foundational technology,[285] whose impacts could reach into every corner of the world. To move forward, though, law and distributed ledgers need each other.

284. *See* Winston S. Churchill, *The Worst Form of Government*, INT'L CHURCHILL SOC'Y (Nov. 11, 1947), https://winstonchurchill.org/resources/quotes/the-worst-form-of-government/ [https://perma.cc/XD75-Y7BB] ("No one pretends that democracy is perfect or all-wise. Indeed it has been said that democracy is the worst form of Government except for all those other forms that have been tried from time to time . . . .").

285. *See* Iansiti & Lakhani, *supra* note 16 (describing foundational technologies).