BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS

TREVOR I. KIVIAT†

ABSTRACT

The buzz surrounding Bitcoin has reached a fever pitch. Yet in academic legal discussions, disproportionate emphasis is placed on bitcoins (that is, virtual currency), and little mention is made of blockchain technology—the true innovation behind the Bitcoin protocol. Simply, blockchain technology solves an elusive networking problem by enabling "trustless" transactions: value exchanges over computer networks that can be verified, monitored, and enforced without central institutions (for example, banks). This has broad implications for how we transact over electronic networks.

This Note integrates current research from leading computer scientists and cryptographers to elevate the legal community's understanding of blockchain technology and, ultimately, to inform policymakers and practitioners as they consider different regulatory schemes. An examination of the economic properties of a blockchain-based currency suggests the technology's true value lies in its potential to facilitate more efficient digital-asset transfers. For example, applications of special interest to the legal community include more efficient document and authorship verification, title transfers, and contract enforcement. Though a regulatory patchwork around virtual currencies has begun to form, its careful analysis reveals much uncertainty with respect to these alternative applications.

† Duke University School of Law, J.D. / LL.M. expected 2016; Syracuse University, B.S. 2011. I have no financial interest in bitcoin. My thanks in completing this Note are many: to Sheldon Thomas, for introducing me to bitcoin and for many lively conversations on this topic; to Professor Campbell R. Harvey, for inviting me to workshop early versions of this Note in his Cryptoventures course; to Reuben Grinberg and John Weinstein, for insightful comments and mentorship; to the Bluebook ninjas of the *Duke Law Journal*, for their outstanding contributions; and to my family, for their endless love, patience, and support.

The circulation of confidence is better than the circulation of money.

– James Madison[1]

INTRODUCTION

On December 26, 2014, three million homes nationwide tuned in to watch the North Carolina State Wolfpack take on the University of Central Florida Knights in the Bitcoin St. Petersburg Bowl—the first of several bitcoin-branded, postseason college bowl games.[2] ESPN's online presale, held open to sports fans across the nation, involved one catch: prospective attendees could only purchase the tickets with bitcoin.[3] This episode was the first of many that collectively exemplify the mainstreaming of virtual currencies—an atmosphere most recently dominated by the acts of financial players,[4] such as the New

1. Statement of James Madison at the Virginia Convention (June 20, 1788), *in* 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 538 (Jonathan Elliot ed., 2d ed. 1836). As this Note illustrates, Bitcoin's core innovation is not the controversial "virtual currency"; rather, it is the facilitation of "trustless" electronic transactions. In other words, blockchain transactions allow each party to independently verify that it is not being defrauded, without the involvement of a trusted intermediary, such as a bank or other financial institution. This is the circulation of confidence.

2. Tony Gallippi, *ESPN and BitPay Enter 3-Year Deal To Produce NCAA Bowl Game*, BITPAY BLOG (June 18, 2014), http://blog.bitpay.com/2014/06/18/espn-and-bitpay-enter-3-year-deal-to-produce-ncaa-bowl-game.html [http://perma.cc/9RAT-WMDS].

3. Tony Gallippi, *Get Ready for the Bitcoin Bowl*, BITPAY BLOG (Oct. 15, 2014), https://blog.bitpay.com/get-ready-for-the-bitcoin-bowl [http://perma.cc/H6QF-GQLB].

4. *See, e.g.*, Clint Boulton, *BNY Mellon Explores Bitcoin's Potential*, WALL ST. J. (Apr. 5, 2015, 6:19 PM), http://blogs.wsj.com/cio/2015/04/05/bny-mellon-explores-bitcoins-potential [http://perma.cc/9NQL-N9FV] (describing how Bank of New York Mellon is experimenting with blockchain technology); Grace Caffyn, *Barclays Trials Bitcoin Tech With Pilot Program*, COINDESK (June 22, 2015, 3:32 PM), http://www.coindesk.com/barclays-trials-bitcoin-tech-with-pilot-program [http://perma.cc/DDH2-J5ZU] (detailing Barclay's signing off on a proof-of-concept to trial blockchain technology); Grace Caffyn, *RBS Trials Ripple as Part of £3.5 Billion Tech Revamp*, COINDESK (June 26, 2015, 2:03 PM), http://www.coindesk.com/rbs-trials-ripple-part-3-5-billion-tech-revamp [http://perma.cc/PZS8-5NK8] (describing Royal Bank of Scotland's efforts to integrate blockchain-based technology as part of a technological revamp); *Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative*, NASDAQ (May 11, 2015), http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196 [http://perma.cc/GH2Z-KQGZ] (detailing Nasdaq's blockchain technology initiative); Nathanial Popper, *When Goldman Sachs Began Flirting with Bitcoin*, AM. BANKER (May 21, 2015), http://www.americanbanker.com/bankthink/when-goldman-sachs-began-flirting-with-bitcoin-1074472-1.html [http://perma.cc/3CBJ-7AUY] (profiling Goldman Sachs's interest in blockchain technology).

York Stock Exchange (NYSE), and state regulators,[5] such as New York's Department of Financial Services (NYDFS).

Bitcoin discussions largely focus on the technology's well-publicized growing pains: wild price volatility;[6] fraudulent investment schemes;[7] multimillion dollar hacks;[8] and the infamous Silk Road case[9]—an episode that resulted in a life sentence for Ross Ulbricht,[10] drug kingpin of the deep web,[11] and the indictment of two federal agents.[12] Accordingly, some intelligent and well-respected detractors

5. New York was first. The list now includes California and North Carolina. Additionally, legislators in Connecticut, New Hampshire, New Jersey, and Pennsylvania are considering various proposals. Peter Van Valkenburgh, *Tracking Bitcoin Regulation State by State*, COIN CENTER (June 2, 2015), https://coincenter.org/2015/06/tracking-bitcoin-regulation-state-by-state [https://perma.cc/U646-8K59].

6. *See Market Price (USD)*, BLOCKCHAIN.INFO, https://blockchain.info/charts/market-price [http://perma.cc/JPQ9-AZNR] (providing historical and real-time price data).

7. *See, e.g.*, SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *14, *21–25 (E.D. Tex. Sept. 18, 2014) (finding an interest in a bitcoin-based Ponzi scheme to be an "investment contract" for purposes of U.S. securities laws and imposing civil monetary penalties under the Securities Act); Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Charges Against Two Florida Men For Operating An Underground Bitcoin Exchange (July 21, 2015), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-two-florida-men-operating-underground [https://perma.cc/T3QF-D97T] (describing charges brought against defendants who operated a federal credit union as a captive bank for their illegal business).

8. *See, e.g.*, Robert McMillan, *$1.2m Hack Shows Why You Should Never Store Bitcoins on the Internet*, WIRED (Nov. 7, 2013, 3:49 PM), http://www.wired.com/2013/11/inputs [http://perma.cc/FD5L-2ZCU] (reporting on a hack suffered by inputs.io, a wallet software provider); Amir Mizroch, *Large Bitcoin Exchange Halts Trading After Hack*, WALL ST. J.: DIGITS BLOG (Jan. 6, 2015, 4:13 AM), http://blogs.wsj.com/digits/2015/01/06/large-bitcoin-exchange-halts-trading-after-hack [http://perma.cc/5L8K-LZZX] (reporting on a hack on "[o]ne of the largest bitcoin exchanges").

9. *See generally* Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [http://perma.cc/LE7G-HM6T] (detailing the Silk Road case); 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/9XH5-XFLK] (same).

10. Press Release, Dep't of Justice, Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), http://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison [http://perma.cc/9LBY-X8XF].

11. The deep web is a "portion of the Internet that is hidden from conventional search engines, as by encryption," such as the Tor network, often used for illegal or criminal activity. *See Deep Web*, DICTIONARY.COM, http://www.dictionary.reference.com/browse/deep-web?s=t [http://perma.cc/2KMN-B42K]. For an interactive, nautical-themed representation of this concept, see *What Is the Deep Web?*, CNN MONEY (Mar. 10, 2014, 9:18 AM), http://money.cnn.com/infographic/technology/what-is-the-deep-web [http://perma.cc/8R3B-4ECT].

12. Press Release, Dep't of Justice, Former Federal Agents Charged with Bitcoin Money Laundering & Wire Fraud (Mar. 30, 2015), https://www.fbi.gov/sanfrancisco/press-releases/2015/former-federal-agents-charged-with-bitcoin-money-laundering-and-wire-fraud [https://perma.cc/

have called it a "bubble,"[13] and others have gone so far as to call it "evil."[14] Nevertheless, technologists and business leaders have declared it "better than currency,"[15] citing its promise to lower transaction costs,[16] transform developing economies,[17] and generally "reshape [the financial] system."[18] Simply put, sensationalism in this area is high.[19] Perhaps this is encouraged by the facts, which read like a science fiction novel, blurring the physical and digital worlds:[20] A pseudonymous inventor[21] releases a cryptographic[22] technology that

---

4J3P-V248].

13. Robert J. Shiller, *In Search of a Stable Electronic Currency*, N.Y. TIMES, Mar. 1, 2014, at BU4. Professor Shiller was awarded the 2013 Nobel Prize in Economic Sciences along with Professors Eugene Fama and Lars Peter Hansen for their research into market prices and asset bubbles. *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2013*, NOBELPRIZE.ORG (Oct. 28, 2015), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2013 [http://perma.cc/6XEW-GUG6].

14. Paul Krugman, *Bitcoin is Evil*, N.Y. TIMES: CONSCIENCE OF A LIBERAL (Dec. 28, 2013, 2:35 PM), http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil [http://perma.cc/8K5G-W62Y].

15. Kim Lachance Shandrow, *Bill Gates: Bitcoin is 'Better than Currency'*, ENTREPRENEUR (Oct. 3, 2014), http://www.entrepreneur.com/article/238103 [http://perma.cc/LTM4-UUJJ].

16. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 23 (2014).

17. *See* JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 14–15 (2013) (describing bitcoin's potential to improve the lives of the world's most impoverished individuals); Kyle Torpey, *Five Economies that Could Actually Use Bitcoin*, VICE: MOTHERBOARD (Apr. 30, 2014, 1:30 PM), http://motherboard.vice.com/blog/five-economies-that-could-actually-use-bitcoin [http://perma.cc/G34G-QCV9] (profiling prospects for bitcoin to support financial modernization in developing countries).

18. Marc Andreesen, *Why Bitcoin Matters*, N.Y. TIMES: DEALBOOK (Jan. 21, 2014, 11:54 AM), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters [http://perma.cc/HW64-THPB].

19. Here is a sampling of the "greatest hits" of sensationalist headlines: John Mauldin, *Is Bitcoin the Future?*, FORBES (Dec. 1, 2014, 11:29 AM), http://www.forbes.com/sites/johnmauldin/2014/12/01/is-bitcoin-the-future/ [https://perma.cc/LJ97-FZEJ]; Jose Pagliery, *Ron Paul: Bitcoin Could 'Destroy the Dollar'*, CNN MONEY (Dec. 4, 2013, 12:01 PM), http://money.cnn.com/2013/12/04/technology/bitcoin-libertarian [http://perma.cc/4D2X-V6MW]; Jonathan M. Trugman, *Welcome to 21st-Century Ponzi Scheme: Bitcoin*, N.Y. POST (Feb. 15, 2014, 5:08 PM), http://nypost.com/2014/02/15/welcome-to-21st-century-ponzi-scheme-bitcoin [http://perma.cc/R8FP-9ZRH]; Tim Worstall, *So, That's the End of Bitcoin Then*, FORBES (June 20, 2011, 4:42 AM), http://www.forbes.com/sites/timworstall/2011/06/20/so-thats-the-end-of-bitcoin-then [http://perma.cc/3AE4-9L4L].

20. For a particularly entertaining work blending the real and synthetic, see PHILIP K. DICK, DO ANDROIDS DREAM OF ELECTRIC SHEEP? (1968).

21. *See* Hiroko Tabuchi, *Will the Real Satoshi Nakamoto Please Stand Up?*, N.Y. TIMES: DEALBOOK (Mar. 11, 2014, 3:57 PM), http://dealbook.nytimes.com/2014/03/11/will-the-real-satoshi-nakamoto-please-stand-up [https://perma.cc/5739-DSVB] (exploring the intrigue regarding the true identity of the Bitcoin architect).

incentivizes armies of supercomputers[23] to mine digital assets[24] that can be traded for real-world goods and services.[25]

Further, authors almost exclusively focus on bitcoin as a currency system. For example, authors have weighed the costs and benefits of transacting with virtual currencies,[26] considered the sustainability of virtual currencies,[27] and contemplated the application of existing regulatory schemes to virtual currency.[28] Missing from the dialogue is a deeper perspective on the technology.

This Note offers that perspective. Primarily, it expands on contemporary academic literature by highlighting the conceptual distinction between bitcoins (that is, virtual currency) and the "blockchain,"[29] the Bitcoin platform's key technological innovation. It

---

22. Cryptography is "the scientific study of techniques for securing digital information, transactions, and distributed computations." JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY: PRINCIPLES AND PROTOCOLS 3 (2007).

23. *Bitcoin: The Magic of Mining*, THE ECONOMIST, Jan. 10, 2015, at 58, http://www.economist.com/node/21638124 [http://perma.cc/UB2F-2EL7]; Ashlee Vance & Brad Stone, *The Bitcoin-Mining Arms Race Heats Up*, BLOOMBERG BUSINESSWEEK (Jan. 9, 2014), http://www.businessweek.com/articles/2014-01-09/bitcoin-mining-chips-gear-computing-groups-competition-heats-up [http://perma.cc/6XK3-KVYJ].

24. A digital asset is essentially any digital file with economic properties that generate value, such as consumption or transfer rights. TOBIAS BLANKE, DIGITAL ASSET ECOSYSTEMS: RETHINKING CROWDS AND CLOUDS 8 (2014).

25. Over 100,000 merchants accept payments in bitcoin as of the publication of this Note. Anthony Cuthbertson, *Bitcoin Now Accepted by 100,000 Merchants Worldwide*, INT'L BUS. TIMES (Feb. 4, 2015, 3:34 PM), http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613 [http://perma.cc/Y26K-FMCB].

26. *See, e.g.*, Joshua J. Doguet, Comment, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1130 (2013) (arguing that bitcoin benefits users by cutting out financial intermediaries—that is, lowers transaction costs—which makes possible even smaller transactions).

27. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 174–81 (2012) (considering the sustainability of bitcoin and concluding that bitcoin is not doomed).

28. *See, e.g.*, Ruoke Yang, *When is Bitcoin a Security Under U.S. Securities Law?*, 18 J. TECH. L. & POL'Y 99, 99 (2014) (federal securities regulation); Kelsey L. Penrose, Note, *Banking On Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. J. 529, 529 (2014) (anti-money-laundering schemes); *see also* Paul H. Farmer, Jr., Comment, *Speculative Tech: The Bitcoin Legal Quagmire & The Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 86 (2014) (exploring the appropriate legal definition for "bitcoins," based upon their intended and actual use); Matthew Kien-Meng Ly, Note, *Coining Bitcoin's "Legal-Bits": Examining The Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 596 (2014) (contemplating whether and which existing legal frameworks may be used to regulate bitcoin).

29. The blockchain is also referred to as the "Bitcoin protocol." *Drawing Distinction Between the Uppercase "B" and Lowercase "b" in Bitcoin*, BLOCKCHAIN (Dec. 29, 2014), http://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-

does this by integrating current research from leading computer scientists and cryptographers.[30] And its ultimate aim is to elevate the legal community's understanding of blockchain technology and, ultimately, to inform policymakers and practitioners as they consider different regulatory regimes.

In short, the blockchain is a "trustless" technology.[31] "Trustless" means—for the first time in history—exchanges for value over a computer network can be verified, monitored, and enforced without the presence of a trusted third party or central institution.[32] Because the blockchain is an authentication and verification technology,[33] it can enable more efficient title transfers and ownership verification.[34] Because it is programmable, it can enable conditional "smart" contracts.[35] Because it is decentralized, it can perform these functions with minimal trust without using centralized institutions.[36] Because it is borderless and frictionless, it can provide a cheaper, faster infrastructure for exchanging units of value.[37]

Simply, blockchain technology has broad implications for how we transact, and the potential for innovation is hard to overstate.[38] Regardless of one's opinion on the merits of virtual currencies, financial regulators must develop a better understanding of blockchain technology's impact potential as they continue to engage in its pragmatic regulation.

---

lowercase-b-in-bitcoin [http://perma.cc/6TGY-9P6W]. A capital "B" is associated with the protocol and the community; for example, "The Bitcoin ecosystem consists of a wide swath of activities, businesses, and services." A lowercase "b" is associated specifically with the virtual currency; for example, "My favorite local coffee shop now accepts payments in bitcoin."

30. *See supra* note 22 (defining cryptography).

31. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 8 (2009), https://bitcoin.org/bitcoin.pdf [https://perma.cc/MW6Y-WSCR].

32. *Id*.

33. ADAM BACK ET AL., ENABLING BLOCKCHAIN INNOVATIONS THROUGH PEGGED SIDECHAINS 7 (2014), http://www.blockstream.com/sidechains.pdf [http://perma.cc/995Y-ALF8].

34. *Id*. at 4, 15–16.

35. *Id*. at 4.

36. NAKAMOTO, *supra* note 31, at 1.

37. *See* TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 67 (2014) (describing math-based "cryptocurrencies" such as bitcoin as an alternative to the often slow and expensive money transfers).

38. One might use venture capital investment data as a rough proxy for perceived innovation opportunities in this area. Total investments in the technology—both venture capital and strategic—are estimated to be over $1 billion. Jose Pagliery, *Record $1 Billion Invested in Bitcoin Firms So Far*, CNN MONEY (Nov. 3, 2015, 12:56 PM), http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested [http://perma.cc/88HT-GGKB].

This Note proceeds in three Parts. Part I introduces blockchain technology and its most widely understood application: money transfers and payments with bitcoin. First, it explains how blockchain transactions occur and why this technology is highly innovative. Second, it explores bitcoin's economic properties and situates the currency within the long evolution of monetary technology. Drawing on economic perspectives, it highlights the benefits and drawbacks of a blockchain-based currency like bitcoin. Part I concludes that the technology's most valuable utility lies beyond bitcoin—in other words, not as a currency but as an exchange medium for digital-asset transfers.

Part II surveys the emerging regulatory landscape, which is heavily premised on the technology's singular application as a virtual currency. First, it explains the current federal scheme—a patchwork of bitcoin-specific guidance and rulings from the Financial Crimes Enforcement Network (FinCEN), paired with the Commodity Futures Trading Commission's (CFTC) oversight authority and the Securities and Exchange Commission's (SEC) enforcement capabilities, which both apply in highly limited circumstances. Next, it explores recent state action—namely, New York's BitLicense, with special attention to its key provisions and ambiguities.[39] At each layer of regulation, it examines open issues that present uncertainty and opportunity for further clarification.

Part III raises issues presented by blockchain technology beyond virtual currency—beyond bitcoin. It covers applications of special interest to the legal community including more efficient contracts, document and authorship verification, and title transfers. It also explores more advanced aspects of the technology, an understanding of which is essential for sensible policy making in this area. After exploring the vistas beyond bitcoin, this Note concludes by offering thoughts on how caution and restraint might be exercised in the law to facilitate technological and economic growth.

39. As this Note goes to press, other states are taking significant steps—most notably, California and North Carolina. Valkenburgh, *supra* note 5. For timely updates relating to regulation of bitcoin and other virtual currencies, see *Virtual Currency Regulation Resources*, DAVIS POLK & WARDWELL LLP, http://bitcoin-reg.com [http://perma.cc/RAY6-4QGJ].

I. THE BLOCKCHAIN, PART 1: BITCOIN, A BLOCKCHAIN-BASED CURRENCY

Experiments in currency are as old as commerce and civilization itself.[40] Today, most currencies—the U.S. dollar included—are fiat currencies.[41] Fiat currencies are not backed by physical assets;[42] rather, they are backed by the promise of their issuing government.[43] Commodity monies, by contrast, are backed by a tradable, naturally scarce resource with value beyond its use in trade.[44] Gold or silver, for example, backed the U.S. dollar for much of our nation's history.[45] This Section explains why bitcoin, the blockchain-based "virtual currency," does not fit comfortably into either of these traditional categories.

First, this Section answers the fundamental question, "What is bitcoin?" by explaining the lifecycle of a blockchain transaction. Second, it examines the economic properties of an artificial commodity like bitcoin as compared to well-known and widely traded physical commodities and traditional fiat currencies. Finally, it highlights the special properties of this technology—core features that not only enable blockchain-based currencies but also hold vast potential for applications beyond bitcoin.

---

40. *See generally* GLYN DAVIES, A HISTORY OF MONEY: FROM ANCIENT TIMES TO MODERN DAY (3d ed. 2002) (documenting the history of currency).

41. *Id*. at 355.

42. In other words, the holder of a paper Federal Reserve Note does not have the right to any amount of an asset—for example, gold or silver, from the government. *Id*. at 642.

43. *See* 31 U.S.C. § 5103 (2012) ("United States coins and currency . . . are legal tender for all debts, public charges, taxes, and dues.").

44. 1 JOHN MAYNARD KEYNES, A TREATISE ON MONEY: THE PURE THEORY OF MONEY 14 (1930). Monetary economists sometimes refer to this as "intrinsic value"—think gold, silver, tobacco, and cocoa beans. ARTHUR O'SULLIVAN & STEVEN M. SHEFFRIN, ECONOMICS: PRINCIPLES IN ACTION 246 (2003).

45. *See generally* George Selgin, *The Rise and Fall of the Gold Standard in the United States*, CATO INST. POL'Y ANALYSIS (June 20, 2013), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa729_web.pdf [http://perma.cc/C3YT-WT4Y] (reviewing the history of the gold standard in the United States).

A. *The Blockchain: "Triple-Entry Accounting"*[46] *on a Transparent, Public Ledger*

In the physical world, security requires locks, vaults, and signatures; in the digital world, it requires cryptography, or techniques for securing digital information and transactions.[47] The blockchain is a cryptographic technology.[48] It is the core innovation driving the bitcoin currency system, and it solves an important technological problem. For the first time ever, secure electronic transfers of value can occur without the presence of a trusted third party.[49] By contrast, outside of the blockchain, electronic transfers of value require financial intermediaries—for example, commercial banks, brokerages, or PayPal—to establish trust and security in the transaction.[50] Such institutions establish trust and security by preserving a centralized ledger[51] to track account holders' balances and, ultimately, vouch for a transaction's authenticity.[52] Without intermediaries, electronic units of value—dollars, for instance—can be copied and spent twice, just as any digital document can be copied ad infinitum.[53] This "double spending problem"[54] has riddled programmers for decades.[55]

---

46. Modern financial accounting is a double-entry system—a system of recordkeeping that allows firms to maintain records of what the firm owns and owes and what the firm has earned and spent over any given period of time. Triple-entry accounting refers to the idea that transactions on the blockchain are essentially accounting entries that are cryptographically sealed, preventing tampering and enabling near-real-time auditing.

47. KATZ & LINDELL, *supra* note 22, at 3.

48. NAKAMOTO, *supra* note 31, at 1.

49. *Id*. at 8.

50. *See* ORG. FOR ECON. CO-OPERATION & DEV., THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES 173–83 (2011) (chronicling the development and growth of online payment intermediaries).

51. This used to be a physical ledger; now it is a centralized server network. *See* BRIJENDRA SINGH, NETWORK SECURITY AND MANAGEMENT 323 (3d ed. 2012) (describing how centralized server networks are utilized for Internet banking).

52. *Id*.

53. The recorded music industry is still recovering from the painful implications of this fact. *See* David Byrne, *David Byrne's Survival Strategies for Emerging Artists—and Megastars*, WIRED (Dec. 18, 2007), http://archive.wired.com/entertainment/music/magazine/16-01/ff_byrne?currentPage=all [http://perma.cc/7EPD-Q8L9] (explaining how peer-to-peer file sharing transformed the economic model of the recorded music industry).

54. The double-spending problem is also referred to as the "Two Generals' Problem," and is illustrated best through the following hypothetical: Imagine two generals, each preparing his troops to attack a common enemy. Each squadron is situated on separate hills, flanking the enemy. The generals can communicate only by courier. Each message sent carries a risk of interception by the enemy. While the two generals have agreed to attack, they have not agreed

Blockchain technology enables secure electronic transactions without a centralized ledger and without double spending.[56] Instead of a centralized ledger, it makes a collective accounting by distributing a shared (that is, decentralized) public ledger—a complete record of all past transactions on the network.[57] This ledger is the blockchain.[58] When two parties wish to engage in a transaction, they must broadcast it to the entire network,[59] effectively asking network participants to determine its authenticity.[60] The following example illustrates this process.

Party A begins by broadcasting a message to the network signaling the terms of the agreement.[61] For example, "I, Party A, am giving Party B one bitcoin." Next, Party B accepts the transaction by broadcasting its acceptance to the entire network[62] and asking network participants to determine the authenticity of the transaction.[63] The network automatically validates the transaction—or guards against the threat of double spending—through a "proof-of-work" validation system.[64] If the transaction is validated, the ledger is

---

upon a time. Assume that a successful attack requires both squadrons to attack the city simultaneously. The issue, then, is that the two generals must agree on an attack time, and each general must know that the other general knows they have agreed. This is difficult because acknowledgement of receipt can be lost as easily as the original message. Thus, a potentially infinite chain of messages is required to reach consensus. *See* Jim Gray, IBM RES. LABORATORY, *Notes on Data Base Operating Systems*, *in* LECTURE NOTES IN COMPUTER SCIENCE 394, 465 (G. Goos & J. Hartmanis eds., 1978), http://research.microsoft.com/en-us/um/people/gray/papers/DBOS.pdf [http://perma.cc/C5ZV-RZ7C] (coining the name "Two Generals' Problem"); *see also* E. A. Akkoyunlu, K. Ekanadham & R. V. Huber, *Some Constraints and Tradeoffs in the Design of Network Communications*, *in* PROCEEDINGS OF THE FIFTH ACM SYMPOSIUM ON OPERATING SYSTEMS PRINCIPLES 67, 73 (J.C. Browne & Juan Rodriguez-Rosell eds., 1975) (documenting the problem for the first time).

55. *See* Gray, *supra* note 54, at 466 (describing the problem as having no solution in 1978).

56. NAKAMOTO, *supra* note 31, at 8.

57. *Id*. at 3.

58. *See id*. (explaining that transactions are recorded in a series of blocks). Although the term "blockchain" was not used in Nakamoto's original paper, it has become synonymous with this technology because transaction data is encoded in blocks that, together, make a chain of all past transactions. BACK ET AL., *supra* note 33, at 3.

59. BACK ET AL., *supra* note 33, at 3–4.

60. *Id*.

61. *Id.*

62. NAKAMOTO, *supra* note 31, at 3. "Broadcasting," in telecommunication and information theory, refers to the method of transferring a message to all recipients or network participants simultaneously. ANDREW S. TANENBAUM & DAVID J. WETHERALL, COMPUTER NETWORKS 17 (5th ed. 2012). In this case, that message is, "I accept the transaction."

63. NAKAMOTO*, supra* note 31, at 4.

64. *Id*. at 3–4.

updated[65] and network users' blockchain records are collectively updated.[66] In other words, once a transaction has been recorded in this transparent public ledger, that transaction cannot be changed after the fact (unless it is matched with a second offsetting transaction).[67]

The proof-of-work validation system is essentially a competition among network participants to validate transactions.[68] Network users participate in this competition by exercising computational power.[69] Under this system, a user's ability to improperly influence validation—to double spend—is limited by the total proportional computation power he can harness.[70] Users are incentivized to bear the computational costs of validation because successful participants are rewarded with new bitcoin.[71] Accordingly, new bitcoins are said to have been "mined," with the "[computational] time and electricity that is expended" as "analogous to gold miners expending resources to add gold to circulation."[72] Eventually there will be nothing left to mine because the total outstanding supply is limited.[73] When that

65. Alternatively, a request for a dishonest transaction falls off the chain and therefore the transaction never occurs.

66. BACK, *supra* note 33, at 3–4. In this respect, the blockchain can be thought of as a historical record of all transactions that have occurred on the network.

67. *Id*. at 1. *But see Stop Saying Bitcoin Transactions Aren't Reversible*, ELI DOURADO (Dec. 4, 2013), https://elidourado.com/blog/bitcoin-arbitration [https://perma.cc/5XW3-YU5Y] (describing advanced features of blockchain technology that may essentially provide users with the ability to encode transactions to include arbitration and similar dispute-resolution services).

68. NAKAMOTO, *supra* note 31, at 3. The transactions are time-stamped to ensure validity. *Id.* at 2.

69. *Id*. at 2.

70. "Computation power" essentially refers to how fast a machine can perform an operation. *See generally* AKEO ADACHI, FOUNDATIONS OF COMPUTER THEORY (1990). The merits of this validation scheme are apparent when compared to a hypothetical alternative. Imagine a scheme in which validation is influenced by the number of network identities the user controls instead of his computational power. Although the marginal cost of acquiring more identities is nearly zero, the marginal cost of amassing greater computational power is quite significant. Accordingly, the scheme that properly deters participants from cheating, or double spending, is the one that raises the costs of cheating to a point of impracticability. *See* NAKAMOTO, *supra* note 31, at 4, 8 (asserting that the structure of Bitcoin makes cheating "computationally impractical").

71. NAKAMOTO, *supra* note 31, at 4. Similarly, users are disincentivized from double spending because the economic cost of doing so, as measured by the computation power required, outweighs the benefits that could be gained in a given transaction.

72. *Id.*

73. Grinberg, *supra* note 27, at 163 (explaining that the rate of bitcoins issued declines by half every four years and that the number of bitcoins approaches but never reaches the total supply of 21 million).

happens, the incentive to validate transactions will likely be transaction fees.[74] Importantly, this is an open-source protocol, meaning open innovation can occur around the technology's various parameters.[75]

In sum, the blockchain establishes trust between two parties to a transaction through both a decentralized public ledger and a cryptographic mechanism that ensures transactions cannot be changed after the fact.[76] One can easily see why the creator of this technology called it "purely peer-to-peer . . . electronic cash."[77] Leaving aside counterfeiting, physical transactions—routine cash transactions, for instance—have never quite suffered from these acute problems of trust and assurance.[78] Yet for the reasons described above,[79] simple two-party exchanges of value over electronic networks could not occur prior to the blockchain innovation.

B. The Economic Properties of a Blockchain-Based Currency

This Section now explores the economic properties of a blockchain-based currency like bitcoin. It examines its basic economic qualities, as compared to commodity money (like gold) and fiat money (like banknotes). It summarizes the key arguments for and against a blockchain-based currency and concludes that, whatever one's normative views regarding the desirability of such a currency, the technology's distinctive features indisputably hold potential for the efficient transfer of all sorts of digital value.

Innovation and disruption in the "technology of money"[80] is not new;[81] this competitive landscape has existed for thousands of years.

---

74. *See* Kerem Kaşkaloğlu, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, INT'L CONF. ON DIGITAL SECURITY & FORENSICS 91, 91–93 (June 2014), http://sdiwc.us/digitlib/request.php?article=96cd6f6067fcbaf5e3947d071aa688fb [https://perma.cc/HAE4-CYU2] (arguing that zero or infinitesimal transaction fees will not be sustainable, given characteristics of mining, securing the network from dishonest users, and the scarce supply).

75. *See infra* notes 240–44 and accompanying text.

76. *See* NAKAMOTO, *supra* note 31, at 8 (concluding that the proposed system for electronic transactions works without relying on trust because it uses a public history of transactions, which makes it impractical for them to be changed later on).

77. *Id.* at 1.

78. "Show me the money," an in-person seller could say.

79. *See supra* notes 54–55 and accompanying text.

80. I use the term "technology of money" to refer to the idea that money, in whatever the currently accepted form may be, represents a particular society's "practical . . . use of scientific and mathematical discoveries." *See Technology*, BLACK'S LAW DICTIONARY (10th ed. 2014).

81. And neither are unregulated currencies. *See generally* DAVIES, *supra* note 40 (tracing

For any technology—be it gold, banknotes, or bitcoin—to be accepted as a monetary standard, it must perform three important functions especially well: it must be (1) a medium of exchange,[82] (2) a store of value,[83] and (3) a unit of account[84] (collectively the functions of money). When a new standard comes along that performs the functions of money better than the incumbents, a platform shift occurs, and the old standard is replaced.[85]

Once upon a time, commodities—shells, grain, and metals—operated as primitive monetary technologies.[86] Among these early prototypes, gold reigned supreme because, of all the naturally occurring elements, its physical properties made it most suitable to perform the functions of money.[87] Despite its first-mover advantage of more than 4000 years,[88] gold was eventually disrupted by the next

---

the development of money and currencies).

82. *See id.* at 13–18 (explaining that in the barter system, goods could not as easily be bought and sold because of valuation and exchange-rate problems). A good monetary platform provides users with liquidity and trade efficiency. In other words, it eliminates the problems that make a pure barter system inefficient. For example, say you have three chickens; all I have is a cow. I need one dozen eggs—a task for which my cow is obviously unfit. If my cow cannot produce anything you need, we are out of a deal. This problem is called the "double coincidence of wants." *Id.* at 15. Second, even if you decide you could use some milk, we are faced with the problems of valuation and exchange rate. *Id.* What is my cow's milk worth as to your chickens' eggs?

83. A good monetary platform provides users with wealth stability—safety, storage, and retrieval features, for example. N. GREGORY MANKIW, PRINCIPLES OF MACROECONOMICS 643 (5th ed. 2008).

84. A good monetary platform provides users with a standardized unit of measurement, meaning users can track the value of economic items such as assets, liabilities, income, and expenses. *Id*.

85. *See generally* George Selgin, *Adaptive Learning and the Transition to Fiat Money*, 113 ECON. J. 147, 162 (2003) (examining how the exchange medium effects influenced the development of money and when and how the transition from a barter to a money system occurs).

86. *See* DAVIES, *supra* note 40, at 35–45 (tracing the evolution of commodities used as primitive money).

87. It is dense, meaning a lot of value can be held in a little space; it is light enough to transport with relative ease; it does not corrode or decay; it is easily divisible into smaller pieces; and it is very hard to counterfeit. *Why Gold?*, NPR: PLANET MONEY (Nov. 16, 2010), http://www.npr.org/blogs/money/2011/02/07/131363098/the-tuesday-podcast-why-gold [http://perma.cc/A9QG-49C7].

88. Many historians claim the first coins containing gold were struck in Lydia, Asia Minor (modern-day Turkey), around 600 B.C. *See, e.g.*, DAVIES, *supra* note 40, at 61–65 (recounting the development of the first bimetallic coinage in Lydia); *see also generally* Robert A. Mundell, *The Birth of Coinage* (Columbia Univ. Dept. of Econ. Discussion Paper Series, Paper No. 0102-08, Feb. 2002) (tracing the development of coinage in the first millennium B.C. in Asia Minor and examining the evidence that they were invented in Lydia).

innovation in monetary technology, government-backed banknotes.[89] Though still a physical technology, banknotes offered streamlined features: portability, divisibility, storability, and fungibility.[90] Soon after, another fundamental shift—this time digital—in monetary technology occurred: electronic deposits and transfers.[91]

1. *Bitcoin's Downside: Blockchain-Based Currencies are a Poor Store of Value*. Gold and paper money have worked as monetary platforms because these technologies perform the functions of money especially well. Gold worked as a store of value due to its physical characteristics.[92] The move away from gold was brought on by the realization that commodity money ties a country's economy to a scarce natural resource, and this can have destabilizing effects.[93] In other words, when Mother Nature controls the supply, shocks can occur that are beyond control.[94] By contrast, fiat currency's supply—and thus its value—is protected by regulation.[95] It is the only platform

89. In 1870, the Supreme Court struck down the Legal Tender Act of 1862, 12 Stat. 345, the first legislation aimed at creating paper money under Article I of the Constitution. Hepburn v. Griswold, 75 U.S. (8 Wall.) 603, 624 (1870). The very next year, a new Court overturned this decision, reasoning that the Civil War was a crisis that necessitated Congress's power to declare paper money to be legal tender and that it was not forbidden by the Constitution. Knox v. Lee (Legal Tender Cases), 79 U.S. (12 Wall.) 457, 540–47 (1871) ("Whatever power there is over the currency is vested in Congress. If the power to declare what is money is not in Congress, it is annihilated."). Finally, the Court extended *Knox* to uphold the validity of legal-tender laws during peacetime in *Juilliard v. Greenman*, 110 U.S. 421, 450 (1884). Indeed, one court has gone so far as to declare, "Article I, section 8 of the United States Constitution clearly gives the United States Congress the power to make *anything it wishes* legal tender." Lowry v. State, 655 P.2d 780, 782 (Alaska Ct. App. 1982) (emphasis added). For an extended discussion, see generally JAMES WILLARD HURST, A LEGAL HISTORY OF MONEY IN THE UNITED STATES, 1774–1970 (1973).

90. *See* WILLIAM STANLEY JEVONS, MONEY AND THE MECHANISM OF EXCHANGE 30–31 (1875) (explaining the ideal properties in choosing the material of money, in particular portability and divisibility); SWANSON, *supra* note 37, at 12–13 (describing the differences in storability and portability, among other factors, between gold, banknotes, and bitcoin).

91. *See* DAVIES, *supra* note 40, at 649 (arguing that this innovation is second only to the printing of paper money in the history of monetary technology).

92. *See supra* note 87.

93. EDWARD B. BARBIER, SCARCITY AND FRONTIERS 238 (2011).

94. *See id*. The Panic of 1857, for example, was triggered when a hurricane off the coast of the Carolinas sunk the S.S. Central America, a vessel carrying thirty thousand pounds of gold. This sum represented the money supply of many East Coast banks. William J. Broad, *X Still Marks the Sunken Spot, and Gold Awaits*, N.Y. TIMES, May 4, 2014, at A1.

95. *See* DONALD R. WELLS, THE FEDERAL RESERVE SYSTEM: A HISTORY 19–20 (2004). Fiat systems rest on the generally accepted premise that a country's citizens are better off when their federal government controls the money supply. *Id*. at 195.

recognized as legal tender,[96] the government is obliged to accept it for tax payment,[97] the central bank has monopoly control over supply,[98] and it is often backed by indirect collateral[99] and insurance.[100] These characteristics allow greater price stability.[101] For example, the Federal Reserve can adjust supply to navigate macroeconomic and financial policy issues.[102]

On the issue of value, a blockchain-based currency such as bitcoin is an imperfect substitute for fiat currency in much the same way gold is. The mathematic rules governing the bitcoin mining process[103] are designed to mimic gold.[104] So just as the laws of nature govern the gold supply, the laws of math govern the bitcoin supply.[105] In both cases, supply cannot be adjusted "to deal with recessions or to counteract destabilizing periods of inflation or deflation."[106] This might explain why the market has experienced wild price volatility.[107]

---

96. *See* 31 U.S.C. § 5103 (2012) ("United States coins and currency . . . are legal tender for all debts, public charges, taxes, and dues. Foreign gold or silver coins are not legal tender for debts.").

97. *Id*.

98. *See* 12 U.S.C. § 411 (2012) (directing that Federal Reserve Notes are to be issued at the discretion of the Board of Governors of the Federal Reserve System).

99. *See* 12 C.F.R. § 9.10(b) (2012) (clarifying that acceptable collateral may be direct obligations or other obligations guaranteed by the United States as to principal and interest).

100. U.S. bank accounts are often insured by the Federal Deposit Insurance Corporation (FDIC). *See* 12 C.F.R. § 330.3 (2012) (explaining the general principles of the insurance coverage).

101. *See* WELLS, *supra* note 95, at 127, 190, 195. The Federal Reserve does this through a combination of lowering and stabilizing inflation, limiting fluctuation in the business cycle, and standing as a lender of last resort during periods of turmoil. *Id.*

102. *See id.* at 150 (discussing various normative perspectives on the Federal Reserve's proper role in setting monetary policy).

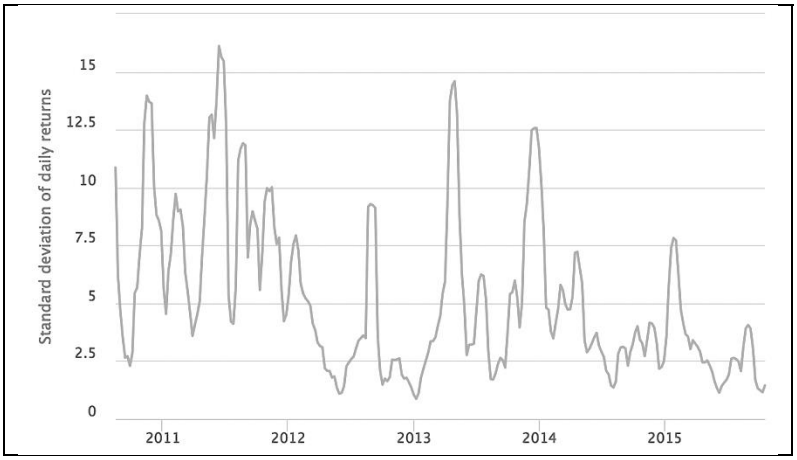
103. *See supra* notes 56–77 and accompanying text.

104. *See supra* notes 72–74 and accompanying text.

105. *See id.* This rule has one important caveat. Although initial distribution is fixed, its parameters can be altered through a majoritarian process. *An Interview with Eric Posner*, *in* 21 GOLDMAN SACHS GLOBAL MACRO RESEARCH 4, 5 (2014). Commentators find this unsettling because it means "technology and programming experts" wield control over a money supply, rather than "economists or monetary experts." *E.g.*, *id.* At least one commentator has explored the possibility of managing the money supply to create a stable blockchain-based currency without the need for intermediation at all. *See* Cameron Harwick, Cryptocurrency and the Problem of Intermediation 12–15 (May 31, 2015) (unpublished manuscript), http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2612727_code2326669.pdf?abstractid=2523771&mirid=1 [http://perma.cc/XZ9V-E72D]. However, since these parameters are fixed at the outset and bitcoin is very widely held, problems of coordination and collective action make it highly unlikely, as a practical matter, that any of the initial parameters will ever be altered.

106. David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* 7 (Coase-Sandor Institute Inst. for L. & Econ., Working Paper No. 685,

Figure 1. Bitcoin Volatility Time Series from Aug. 16, 2010 to Oct. 20, 2015.[108]



Over its history, bitcoin's exchange rate against the U.S. dollar has frequently jumped or crashed over 20 percent (sometimes nearly 50 percent) in the course of a single day.[109] By contrast, over the same period, the U.S. dollar-to-euro exchange rate has never changed more than 2.5 percent in one day.[110] Even a casual observer can recognize that such instability is not a desirable currency trait because its

2014), http://www.law.uchicago.edu/files/file/685-dse-economic.pdf [http://perma.cc/3NET-EYEB].

107. *See infra* Figure 1. Liquidity and pricing issues also exist. Bitcoin is a relatively illiquid asset. *See Illiquid asset*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining illiquid asset as "[a]n asset that is not readily convertible into cash, usu. because of (1) the lack of demand, (2) the absence of an established market, or (3) the substantial cost or time required for liquidation" (alteration in original)). Accordingly, relatively small trades can move these thin markets. 2 JOHN MAYNARD KEYNES, A TREATISE ON MONEY: THE APPLIED THEORY OF MONEY 67 (1930). And prices are different across different exchanges, indicating that some markets carry a liquidity premium—for example, ones that allow users to more readily convert their holdings to fiat. All bitcoin-to-fiat trades are liquidity trades because the asset lacks underlying fundamentals. To attract business, payment processors such as BitPay must guarantee the price for a period of time so businesses may accept bitcoin payments without the corresponding price risk. *See Bitcoin Exchange Rates*, BITPAY, https://bitpay.com/bitcoin-exchange-rates [https://perma.cc/4EUZ-YJH3] (listing the exchange rates).

108. THE BITCOIN VOLATILITY INDEX, https://btcvol.info [http://perma.cc/XTF5-4B3G]. Volatility in this figure is represented by the standard deviation of daily returns for the preceding thirty-day window over the past five years. *Id.*

109. Harwick, *supra* note 105, at 6.

110. *Id.*

holder's purchasing power can increase or decrease drastically and suddenly.[111]

2. *Bitcoin's Upside: A More Efficient Medium of Exchange*. Though the technology fails as a store of value for reasons described above, the blockchain could play an integral role in the next phase of the financial-technology (fintech) revolution. Given its features, it is a technology uniquely capable of performing several key components of a transaction—recordkeeping, auditing, monitoring, enforcement, or asset custody (that is, escrow)—in addition to facilitating the trade itself. This is important because the global movement of value can be quite cumbersome.[112]

For example, gold and fiat currency have always had high transportation costs, involving security, armored cars, and insurance.[113] In fact, the simple laws of physics limited the Federal Reserve's original structure; the number and locations of the Reserve Banks are such that "no bank [was] more than an overnight's train ride from its [Federal Reserve]."[114] These restraints were shattered by the first wave of the digital revolution, in which electronic transfers greatly reduced the cost of moving value.[115]

Yet the movement of value along these electronic systems is still costly. First, moving value—actually clearing and settling a transaction—takes time. For example, on January 26, 2015, the Federal Reserve issued a call to action for all stakeholders in the U.S.

111. For an extended discussion of bitcoin's volatility problem, see generally Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto & Kenji Saito, *Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money* (Hitotsubashi Univ. Inst. of Econ. Research, Discussion Paper Series A No. 617, 2014) (suggesting an amendment to the Bitcoin protocol to set monetary policy without a central bank).

112. *See* DAVIES, *supra* note 40, at 596–602 (describing the "poverty trap" faced by many countries, despite the rapid increase of wealth in many others).

113. *See id.* at 606 (describing, for example, the prohibitive costs of transporting silver in rural Africa).

114. U.S. GEN. ACCOUNTING OFFICE, FEDERAL RESERVE SYSTEM: CURRENT AND FUTURE CHALLENGES REQUIRE SYSTEMWIDE ATTENTION 83 (1996).

115. As early as 1984, banks recognized that "[i]nformation about money" is "almost as important as money itself." Thomas A. Bass, *The Future of Money*, WIRED (Oct. 1996), http://archive.wired.com/wired/archive/4.10/wriston_pr.html [http://perma.cc/98R4-L9RQ]. Today, "[d]igitization is challenging the very way banks operate." Somesh Khanna, *The Bank of the Future*, MCKINSEY & CO. (Nov. 2014), http://www.mckinsey.com/insights/financial_services/the_bank_of_the_future [http://perma.cc/U8ST-J8XH].

payments system[116] to increase end-to-end payment speed, among other things.[117] Currently, the Automated Clearing House[118] (ACH) system supports more than 20 percent of all electronic payments in the United States—these transactions, to a great extent, relate to consumer and small-business transactions.[119] More than $40 trillion moves through the ACH network each year in nearly 23 billion electronic transactions.[120] Nearly all consumer transactions on the ACH network take two to three days.[121] Second, moving money takes money. For example, an estimated $600 billion in principal will be sent in the remittance[122] market in 2015.[123] Companies like Western Union and MoneyGram traditionally provide this service and enjoy an average fee (or "take rate") of 6 percent, though this rate can run as high as 9 percent.[124] This translates to roughly $36 billion in fees in 2015.

---

116. *See* FED. RESERVE SYS., STRATEGIES FOR IMPROVING THE U.S. PAYMENT SYSTEM 6–7 (2015), https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf [https://perma.cc/GL6W-PR4S] (calling all stakeholders to seize the opportunity of the current critical juncture and improve the U.S. payment system).

117. *Id.* at 7.

118. Created in 1974, ACH is an electronic network of U.S. financial institutions. It was designed to reduce the need for paper checks in making "routine payments." *Automated Clearing Houses (ACHs)*, FED. RESERVE BANK OF N.Y., http://www.ny.frb.org/aboutthefed/fedpoint/fed31.html [http://perma.cc/66MX-K3CK].

119. *History and Network Statistics*, NACHA—THE ELEC. PAYMENTS ASSOC., https://www.nacha.org/ach-network/timeline [https://perma.cc/5T2B-7KPE]. The other major electronic-value transfer systems, Fedwire and CHIPS—sometimes called "large-value payment systems"—are primarily used by financial institutions to settle large financial-market and other transactions. *See* COMM. ON PAYMENT & SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS, *Payment, Clearing and Settlement Systems in the United States*, *in* 2 PAYMENT, CLEARING AND SETTLEMENT SYSTEMS IN THE CPSS COUNTRIES 471, 487 (2012).

120. NACHA—THE ELEC. PAYMENTS ASSOC., ACH VOLUME INCREASES 5.3 PERCENT IN 1ST QUARTER 2015, at 1, https://www.nacha.org/system/files/resources/1st%20Quarter%202015.pdf [https://perma.cc/5533-CRZM].

121. Although transactions can technically clear overnight on the ACH network, they are generally subject to batch processing, a process whereby a large volume of transactions is aggregated for simultaneous movement through the network.

122. Remittances are money transfers by (typically foreign) workers to other individuals (typically relatives in their home country). *See Remittance*, WEBSTER'S UNABRIDGED DICTIONARY 1630 (2d ed. 2014) (defining the term as "money or its equivalent sent from one place to another").

123. Mark Scott, *Remittances at the Click of a Smartphone Button*, N.Y. TIMES: BITS (June 7, 2015, 9:00 AM), http://bits.blogs.nytimes.com/2015/06/07/remittances-at-the-click-of-a-smartphone-button [http://perma.cc/V6PG-2AZN] (citing a study by the World Bank).

124. DILIP RATHA ET AL., THE WORLD BANK, MIGRATION AND DEVELOPMENT BRIEF 23, at 12 (2014), http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief23.pdf [http://perma.cc/RS2L-58AM].

Blockchain technology is uniquely positioned to tackle the problems of both speed and cost. For example, Coinbase, a prominent bitcoin company, provides a service called Instant Exchange.[125] This service facilitates instantaneous cross-border money transfers with bitcoin as the intermediary for a total transaction cost of 2 percent.[126] As applied to the $600 billion principal figure above (today's remittance market), a potential cost savings of $24 billion might pass through directly to the consumers of such a service.[127]

For these reasons (and many more that are beyond the scope of this Note), the financial-services sector is in the midst of a digital revolution.[128] Of the $23.5 billion invested in fintech ventures between 2013 and 2014, 23 percent ($5.4 billion) was invested in payments technology.[129] As illustrated above, one critical aspect of payments technology is infrastructure. Payments-infrastructure initiatives are emerging in many countries across the world, driven by both public and private actors.[130] Many players—from bootstrapping startups to large, incumbent financial institutions—believe blockchain technology will play an integral role.[131]

In sum, blockchain technology solves an important problem in electronic value transfers. The blockchain does not only move value; it also integrates several components of the trading-clearing-settlement value chain in an elegant, efficient, and mathematical way.

---

125. *Instant Exchange*, COINBASE, https://www.coinbase.com/instant-exchange [http://perma.cc/D9DE-TFB6].

126. *What is Instant Exchange?*, COINBASE, https://support.coinbase.com/customer/portal/articles/2021569-what-is-instant-exchange [http://perma.cc/Z8TK-8RAR] (noting that Coinbase's standard 1 percent fee is applied on both sides of the transaction).

127. This amount is calculated as follows: First, solve for the difference between the average prevailing rate (that is, 6 percent) and Coinbase's low-cost position (that is, 2 percent) to arrive at 4 percent. Second, solve for 4 percent of the $600 billion principal figure. The amount is $24 billion.

128. *See* ACCENTURE, THE FUTURE OF FINTECH AND BANKING: DIGITALLY DISRUPTED OR REIMAGINED? 3 (2015), https://www.accenture.com/t20150707T195228__w__/lven/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf [https://perma.cc/3QL2-567B] (reporting a 201 percent increase in fintech investments from 2013 to 2014); *see also* MARIANO BELINKY, EMMET RENNICK & ANDREW VEITCH, THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERVICES (2015), http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/The_Fintech_2_0_Paper_Final_PV.pdf [http://perma.cc/9LMK-XQ4U] (discussing the significant changes in the policy and technology surrounding fintech).

129. BELINKY ET AL., *supra* note 128, at 4.

130. *See* Rob Hayden, *Transforming National Payments Systems*, 20 MCKINSEY ON PAYMENTS 23, 24 (Sept. 2014).

131. For articles on bank innovation around blockchain technology, see *supra* note 4.

To be sure, these facts neither imply nor foreclose on the desirability of a blockchain-based currency. They simply indicate that blockchain technology should be of interest to any industry engaged in the digital transfer of value. For example, instead of being used as an alternative currency, it might facilitate the transfer of traditional units of value—U.S. dollars or euros for example. In other words, incumbent firms in the payments-and-transfer space can co-opt it to gain efficiencies systems, lower fee structures, and provide more competitive services.[132]

II. THE DEVELOPING LEGAL FRAMEWORK FOR BLOCKCHAIN TRANSACTIONS

Part I explained how money has evolved over time, both as a technology and as a concept. Specifically, it has shifted from a store of value in itself to a medium of exchange. As the role of cash diminishes in favor of electronic deposits and transfers,[133] many wonder about the extent to which blockchain-based currencies will influence the next phase of this global payment revolution. Indeed, entrepreneurial ventures—some backed by considerable human and financial resources—are building a vibrant ecosystem of complementary products and services around this vision.[134] One view, hailing the virtues of a free, open currency market is that transactions in this space should be entirely deregulated.[135] This Part concludes at

132. One prominent example in this space is Ripple, a company that has designed a protocol similar to Bitcoin for routing payments and settling funds. Designed to simplify interbank payments at the infrastructure level, Ripple has end users in the financial industry, including banks, governments, and clearinghouses. RIPPLE, EXECUTIVE SUMMARY FOR FINANCIAL INSTITUTIONS 2 (2015), https://ripple.com/files/ripple_executive_summary.pdf [https://perma.cc/W83S-8XSF]. For a note on the technical distinction between Bitcoin and Ripple, see *infra* note 170. For a discussion on Ripple's recent settlement agreement with FinCEN, see *infra* notes 171–74 and accompanying text.

133. *See* DAVIES, *supra* note 40, at 649–52 (discussing the global move toward electronic transactions).

134. *See* Grinberg, *supra* note 27, at 165 ("A growing ecosystem surrounds Bitcoin, including exchanges, transaction services providers, market information and chart providers, escrow providers, joint mining operations and so on."); *see also* Michael A. Cusumano, *The Bitcoin Ecosystem*, COMM. OF THE ACM, Oct. 2014, at 22, https://www.deepdyve.com/lp/association-for-computing-machinery/the-bitcoin-ecosystem-fUAzCpWvpD [https://perma.cc/PE6T-NV6W] ("[B]itcoins are a complex platform technology that requires the help of intermediaries—an ecosystem of 'complementary' product and service providers that charge fees.").

135. *See* Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 171 (2012) (arguing that "bitcoins should be treated as an unregulated community currency under the

the outset without further discussion that such a view is neither realistic nor desirable, given a compelling policy interest in preventing abuse and misuse.[136] Examples of such abuses include bitcoin's potential to facilitate black-market transactions,[137] tax evasion,[138] money laundering,[139] and terrorist financing.[140]

This Part explores the emerging legal framework around virtual currencies and serves as a practical guide for policymakers and innovators trying to both shape and navigate it. Both federal and state regulators have identified some basic risks around blockchain-based currencies and begun staking jurisdictional claims. Policymakers are currently revisiting complex, interwoven regulatory frameworks—primarily banking laws, commodities laws, and securities laws—to shoehorn the technology into existing frameworks and consider where new ones might be appropriate. This Part presents a patchwork that is continuing to emerge,[141] with special attention on areas posing uncertainty for innovators.

A. Federal Regulation of Blockchain-Based Currencies

No comprehensive federal regulation exists for virtual currencies. Many government bodies—specifically, FinCEN, the Internal Revenue Service (IRS), SEC, CFTC, and Consumer Financial Protection Bureau (CFPB)—have offered guidance and taken limited action. This Section summarizes the most significant federal developments to date—FinCEN's guidance, administrative rulings, and enforcement against Ripple Labs, Inc. (Ripple)[142]—and explains the likely implications for innovators. Finally, it notes the

law").

136. For a thoughtful discussion on normative and logistical issues in regulating Internet activity, see generally LAWRENCE LESSIG, CODE VERSION 2.0 (2d ed. 2006).

137. Ly, *supra* note 28, at 595 (discussing Silk Road).

138. *Id*. at 595–96.

139. *Id*. at 594.

140. *See* SWANSON, *supra* note 37, at 28 (mentioning terrorist financing and money laundering as two of the possible pitfalls of Bitcoin).

141. Given the fixed nature of print publication, readers should visit DAVIS POLK & WARDWELL LLP, *supra* note 39, for the latest developments on regulation of Bitcoin and other virtual currencies.

142. The IRS has also issued a notice declaring that virtual currencies should be treated as property for federal tax purposes. *See IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, INTERNAL REVENUE SERV. (Mar. 25, 2014), http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance [http://perma.cc/3F4A-KHLA]. For an extended discussion of the implications of this rule for the bitcoin economy, see Ly, *supra* note 28, at 606–08.

limited scenarios in which the other agencies have jurisdiction over blockchain activities.

1. *FinCEN Guidance, Rulings, and Enforcement*. Under the Bank Secrecy Act (BSA),[143] banks and other financial institutions are subject to various registration and recordkeeping requirements.[144] All "money service businesses"[145] are required to register with the Department of the Treasury[146] and develop anti-money-laundering[147] and customer identification programs.[148] In March 2013, FinCEN[149] extended these rules to cover certain participants who transact in "convertible virtual currencies."[150] It defined this term to include any medium of exchange that "operates like a currency in some environments," and "has an equivalent value in [or acts as a substitute for] real currency," but does not have "legal tender status in any jurisdiction."[151]

Under FinCEN's guidance, "exchangers" and "administrators" are possibly subject to regulation.[152] Exchangers are persons or businesses that exchange virtual currency for real currency, funds, or other virtual currency.[153] Administrators are persons or businesses engaged in the business of "issuing (putting into circulation) a virtual currency" who also have "the authority to redeem (to withdraw from

143. Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified at 12 U.S.C. §§ 1829b, 1951–59 and 31 U.S.C. §§ 5311 et seq.).

144. Courtney J. Linn, *Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring*, 50 SANTA CLARA L. REV. 407, 412–20 (2010) (providing an overview of the registration and record-keeping requirements for banks and other "money transmitters").

145. The term "money services business" includes "money transmitters," defined as a person that accepts and transmits currency, funds, or other value that substitutes for currency. 31 C.F.R. § 1010.100(ff) (2015).

146. *Id.* § 1022.380(a).

147. *Id.* § 1022.210(a).

148. *Id.* § 1022.210(i).

149. Established in 1990, the Financial Crimes Enforcement Network, or FinCEN, is a bureau of the Department of the Treasury that combats domestic and international money laundering, terrorist financing, and other financial crimes. *What We Do*, FinCEN, http://www.fincen.gov/about_fincen/wwd/ [http://perma.cc/S72W-VBJE].

150. FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013), http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [http://perma.cc/5XAF-PAFC] [hereinafter FINCEN GUIDANCE].

151. *Id*.

152. *Id*. at 2.

153. *Id*.

circulation) such virtual currency."[154] An exchanger or administrator becomes a "money transmitter" subject to these registration and recordkeeping requirements when they either "accept[] and transmit[]" convertible virtual currency or "buy[] or sell[]" convertible virtual currency.[155] "Users" are explicitly carved out.[156]

In 2014, FinCEN issued four rulings under this guidance[157] that, together with existing BSA laws, provide some key insights. First, any blockchain transaction is likely a virtual-currency transaction, because even nonfinancial uses require a de minimis amount of currency (that is, a fraction of a penny of bitcoin). However, such activity must also be performed by an "exchanger" or "administrator" to trigger BSA requirements.[158] End users, such as merchants or consumers, are likely to be exempted.[159]

Second, a user who mines virtual currency (miner-user) is not a money transmitter, even if he uses the bitcoin to purchase goods and services.[160] Further, miner-users converting virtual currencies to real or other virtual currencies are not subject to BSA requirements, so long as their conversion is for personal use.[161] Therefore, miner-users

---

154. *Id*.

155. *Id*. at 3.

156. "Users" are persons who obtain virtual currency "to purchase goods and services." *Id*. at 2.

157. FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R001, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (2014) [hereinafter FINCEN RULING 1], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf [http://perma.cc/Q4PL-F92L]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY (2014) [hereinafter FINCEN RULING 2], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf [http://perma.cc/P8K4-WTQQ]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R011, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM (2014) [hereinafter FINCEN RULING 3], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf [http://perma.cc/HL78-LDHQ]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R012, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM (2014) [hereinafter FINCEN RULING 4], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf [http://perma.cc/NZA9-WLTR].

158. *See supra* text accompanying notes 152–55.

159. *See* FINCEN GUIDANCE, *supra* note 150, at 1 ("A user of virtual currency is *not* an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations.").

160. FINCEN RULING 1, *supra* note 157, at 3.

161. This conclusion is grounded in the "end user" exemption. *See supra*, note 159 and accompanying text. It is supported by FINCEN GUIDANCE. *See supra* note 157, at 3. ("What is

should not be seen as money transmitters subject to the BSA's registration and recordkeeping requirements unless they are selling bitcoin as a business.[162]

Third, a company that mines virtual currency (miner-company) is not a money transmitter in certain instances. Specifically, miner-companies are not money transmitters when convertible virtual currency is used (1) to pay for goods or services, (2) to pay debts previously incurred, (3) to make distributions to owners, (4) to purchase real or other virtual currency specifically for any of the previous three purposes, or (5) for the company's own investment account.[163]

Fourth, a company is an "exchanger" regardless of whether it acts as a broker (by matching two simultaneous, offsetting transactions) or as a dealer (by transacting on its own account).[164] At least three U.S.-based exchanges have shut down in the wake of this guidance.[165]

Finally, two important exemptions (that predate both the guidance and the rulings) carve out certain activities from the definition of money transmitter: the "integral" exemption and the

---

material to the conclusion . . . is not the mechanism by which person obtains the convertible virtual currency, but what the person uses the convertible virtual currency for, and for whose benefit.").

162. FINCEN GUIDANCE, *supra* note 150, at 2 & n.7.

163. FINCEN RULING 1, *supra* note 157, at 3; FINCEN RULING 2, *supra* note 157, at 4.

164. FINCEN RULING 3, *supra* note 157, at 3; FINCEN RULING 4, *supra* note 157, at 3.

165. Jon Matonis, *Fincen's New Regulations are Choking Bitcoin Entrepreneurs*, AM. BANKER: THE MONETARY FUTURE (Apr. 25, 2013), http://www.americanbanker.com/bankthink/fincen-regulations-choking-bitcoin-entrepreneurs-1058606-1.html [http://perma.cc/5ADR-M5FH]. The force of these regulations is compounded by the fact that, a few months after the FinCEN issued its guidance, the Office of the Comptroller of the Currency (OCC) issued guidance effectively raising the cost for banks and other financial institutions for conducting business with any blockchain-based currency companies. OCC Bulletin 2013–29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013). To be sure, the guidance does not specifically address bitcoin or blockchain-based currencies; however, it refers to certain third-party relationships that involve "critical activities" and merit enhanced risk measures. *Id.* Specifically, the guidance requires the adoption of "risk-based processes" for third-party relationships commensurate with the level of risk and complexity inherent in those relationships. *Id.* With bitcoin businesses considered high risk due to their potential for money laundering and other illicit uses, this guidance means banks will have to conduct enhanced due diligence on any blockchain-based company. *Id.* Accordingly, many U.S. companies and entrepreneurs have had trouble accessing basic banking services. *See* Kashmir Hill, *Bitcoin Companies and Entrepreneurs Can't Get Bank Accounts*, FORBES (Nov. 15, 2013, 3:23 PM), http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts [http://perma.cc/CY76-ADVY] (reporting on the U.S.-based bitcoin exchanges that have shut down).

"payment processor" exemption. First, BSA legislation provides an exemption for entities that accept and transmit funds "only integral to the [entity's] sale of goods or the provision of [other, nonmoney transmission] services."[166] In other words, ordinary merchants and service providers who merely accept bitcoin as a convenience to customers are not money transmitters. Second, BSA legislation provides an exemption for any entity acting as a "payment processor to facilitate the purchase of . . . a good or service through a clearance and settlement system by agreement with the creditor or seller."[167] One condition necessary for this exemption is that the entities operate only through clearance and settlement systems that admit BSA-regulated financial institutions.[168] Accordingly, bitcoin-based payment processors will have a difficult time availing themselves of this exception because the virtual-currency leg of the transaction will always settle on the blockchain[169]—a system that inherently allows participation by non-BSA-regulated members.[170]

On May 5, 2015, in its first civil enforcement action against a virtual-currency business, FinCEN announced a $700,000 fine against

166. 31 C.F.R. § 1010.100(ff)(5)(ii)(F) (2015). FinCEN has specified a three-prong test for this exemption: (1) the money-transmission component must be part of the provision of goods or services distinct from money transmission itself, (2) the exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission, and (3) the money transmission component must be necessary for the provision of the goods and services. FINCEN RULING 3, *supra* note 157, at 4; FINCEN RULING 4, *supra* note 157, at 4.

167. 31 C.F.R. § 1010.100(ff)(5)(ii)(B) (2015).

168. FinCEN has specified a four-prong test for this exemption: (1) the entity providing the service must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself), (2) the entity must operate through clearance-and-settlement systems that admit only financial institutions regulated under the BSA, (3) the entity must provide the service pursuant to a formal agreement, and (4) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds. FINCEN RULING 3, *supra* note 157, at 4–5; FINCEN RULING 4, *supra* note 157, at 4.

169. *See supra* Part I.A.

170. This exemption implicates an important distinction between "permissionless" networks (like Bitcoin) and "permissioned" networks (like Ripple). A permissionless network, such as the Bitcoin blockchain, is fully decentralized—in other words, participants may join the network, process transactions, and fully participate without any previous relationship with the ledger. *See* TIM SWANSON, CONSENSUS-AS-A-SERVICE: A BRIEF REPORT ON THE EMERGENCE OF PERMISSIONED, DISTRIBUTED LEDGER SYSTEMS 5 (2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf [http://perma.cc/A2GA-SUQH]. Such a network will never meet the "payment processor" exemption because non-BSA-regulated entities cannot be screened out. By contrast, on permissioned networks, participants are whitelisted through some type of know-your-customer procedure. *Id*. Such a network may be designed to accommodate regulatory exemptions of this nature.

Ripple and a simultaneous settlement agreement.[171] Ripple was selling XRP, a virtual currency similar to bitcoin, that it designed for the purpose of creating a real-time settlement infrastructure.[172] In its negotiated settlement with the U.S. Attorney's Office in the Northern District of California, Ripple admitted to violating several BSA requirements in its "exchange" and "transmission" of XRP for fiat currency.[173] Though Ripple had registered its subsidiary as a money-services business in accordance with FinCEN's guidance, it sold XRP for several months without a proper anti-money-laundering (AML) program in place, failed to designate a compliance officer, and did not solicit an independent review of its practices and procedures.[174]

Two lessons can be learned from FinCEN's enforcement against Ripple. First, FinCEN is clearly taking a hard stance, per its 2013 guidance, that AML programs are a necessity from the very moment a business begins "exchang[ing]" or "transmi[tting]" customer funds.[175] Second, distributed-ledger businesses that operate outside of the traditional Bitcoin blockchain will not escape FinCEN's scrutiny.

2. *CFTC Jurisdiction over Bitcoin Derivatives and Market Manipulation Oversight.* As noted above,[176] blockchain-based currencies share some economic properties with commodity money,[177] and legal definitions support their characterization as a commodity in some instances. The Commodity Exchange Act (CEA)[178] broadly defines a "commodity" to include "all services, rights and interests . . . in which contracts for future delivery are presently or in the future

171. Press Release, Fin. Crimes Enf't Network, U.S. Dep't of the Treasury, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), http://www.fincen.gov/news_room/nr/pdf/20150505.pdf [http://perma.cc/T6WU-55Z4].

172. Does this sound familiar? *See supra* Part I.B.2.

173. U.S. DEP'T OF JUSTICE, SETTLEMENT AGREEMENT WITH RIPPLE LABS, INC., at app. A 4–6 (May 5, 2015), http://www.justice.gov/file/421626/download [http://perma.cc/DPD5-P8Q9].

174. *Id.* at app. A 5–6.

175. *See supra* text accompanying notes 152–56 (discussing exchangers and transmitters).

176. *See supra* Part I.B.1.

177. Indeed, one monetary economist established the term "synthetic commodity money" to describe the unique economic properties of a blockchain-based currency, such as bitcoin. *See* George Selgin, Synthetic Commodity Money 7–8 (Apr. 10, 2013) (unpublished manuscript), http://ssrn.com/abstract=2000118 [http://perma.cc/G2GY-BSNH].

178. Commodity Futures Trading Commission Act of 1974, Pub. L. No. 93-463, 88 Stat. 1389, 1395 (codified as amended at 7 U.S.C. §§ 1 et seq.) (defining the term "commodity" and providing for CFTC jurisdiction over all options and futures trading in commodities); *see also* William L. Stein, *The Exchange-Trading Requirement of the Commodity Exchange Act*, 41 VAND. L. REV. 473, 485–86 (1988) (discussing the meaning of "commodity" under the CEA).

dealt in."[179] Accordingly, the CFTC has jurisdiction over derivatives contracts[180] related to interests not traditionally thought of as commodities—Treasury securities, stock-market indices, and currencies, for example. Under this analysis,[181] the CFTC concluded that bitcoin and other virtual currencies are "properly defined as commodities."[182] And in September 2014, the agency oversaw the launch of the first bitcoin swap execution facility (SEF).[183]

Bitcoin derivatives—for example, a swap contract pegged to the U.S.-dollar-bitcoin exchange rate—are exotic instruments at this stage.[184] The more pressing question, then, is the extent to which the

---

179. 7 U.S.C. § 1a(9) (2012); *see also* 17 C.F.R. § 1.3 (2015) (codifying CFTC Final Rule 1.3(e)).

180. Derivatives contracts are agreements between two parties, the value of which is determined by the price of something else, such as a changing interest rate, financial index, or market price. *See generally* ROBERT L. MCDONALD, DERIVATIVES MARKETS 1 (2d ed. 2006) ("Derivatives [contracts] can be thought of as bets on the price of something.").

181. More accurately, it was a legal conclusion lacking any analysis. It can only be assumed, however, that analysis was driving the conclusion, and this analysis would be a proper line of reasoning if the CFTC's position is challenged. Indeed, CFTC Chairman Timothy Massad has used similar reasoning in contending that "[d]erivative contracts based on a virtual currency represent one area within [the CFTC's] responsibility." *Testimony of Chairman Timothy Massad Before the U.S. Senate Committee on Agriculture, Nutrition & Forestry*, U.S. COMMODITY FUTURES TRADING COMM'N (Dec. 10, 2014), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 [http://perma.cc/9LNA-NQVM].

182. Coinflip, Inc., Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions at 3, CFTC Docket No. 15-29 (Sept. 17, 2015), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf [http://perma.cc/5B4W-PJ3G].

183. *See* Press Release, TeraExchange, TeraExchange Launches First Regulated Bitcoin Derivatives Trading (Sept. 12, 2014), http://www.teraexchange.com/news/2014_09_12_Launches%20First%20Regulated%20Bitcoin%20Derivatives.pdf [http://perma.cc/B3DG-3ACQ] (announcing the first regulated trading platform for bitcoin derivatives). An SEF is a type of regulated marketplace under Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Specifically, it is a platform for swap trading that provides pretrade information—a spot-market index, bids, and offers—and an execution mechanism for swap transactions. *See* 7 U.S.C. § 1a(50) (2012) (defining "swap execution facility"). Swaps are agreements for parties to exchange cash flows over time, with one party paying the other based on the actual price in reference to the contractually specified price. MCDONALD, *supra* note 180, at 247. The first recorded swap in this space involved the sale of a multimillion-dollar Stradivarius violin to a wealth-management company. The buyer wanted to use bitcoins in consideration for the purchase, but the seller was worried about exchange-rate risk over the period of the contract, given wild price fluctuations. TeraExchange worked with the buyer to structure a deal that would protect both parties from losses, and it became the prototype for this SEF. *See* Paul Vigna & Michael J. Casey, *BitBeat: Bitcoin, Stradivarius Make Beautiful Music Together*, WALL ST. J.: MONEY BEAT (Mar. 28, 2014, 7:26 PM), http://blogs.wsj.com/moneybeat/2014/03/28/bitbeat-bitcoin-stradivarius-make-beautiful-music-together [http://perma.cc/A728-RC4D].

184. Currently, payment processors assume the exchange-rate risk from merchants. For

CFTC can exercise jurisdiction over spot-market transactions[185] under its anti-manipulation authority.[186] In other words, the CFTC has enforcement authority over spot transactions in certain instances because spot-market manipulation can affect derivatives market prices.[187] Thus, in certain cases the CFTC may regulate bitcoin pursuant to its anti-manipulation rules.[188] While manipulation oversight would bring some regulation to the spot market, one issue is whether manipulation oversight alone is sufficient, even under the broad anti-manipulation rules of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[189]

Dodd-Frank extended the CEA's anti-manipulation rules to cover swaps and clarified that "manipulation" under the CEA includes not only "actual manipulation"[190] but also an intent-based "attempted manipulation."[191] This new authority was first exercised in

---

example, merchants typically utilize a payment-processing service, such as BitPay, to convert bitcoin-denominated payments to fiat currency almost immediately. *See Getting Started: Accepting Bitcoin Payment*, BITPAY, https://bitpay.com/docs [https://perma.cc/KHB2-UY6X]. One way payment processors may consider hedging this risk would be through derivatives.

185. A "spot transaction" is simply the current sale or purchase for immediate settlement. *Spot transaction*, BLACK'S LAW DICTIONARY (10th ed. 2014).

186. The CEA makes it a felony "to manipulate or attempt to manipulate the price of . . . any commodity." 7 U.S.C. § 9 (2012). The CEA also creates a private right of action to accompany the government's civil and criminal enforcement capabilities. *Id*. § 22(a); *see also id*. § 25(a)(1) ("Any person . . . who violates this chapter or who willfully aids . . . a violation of this chapter shall be liable for actual damages resulting from . . . such violation."). The exact meaning of "manipulation" has been debated, as is not statutorily defined. Broadly stated, manipulation is an intentional exaction of a price determined by forces other than supply and demand.

187. *See* Jerry W. Markham, *Manipulation of Commodity Futures Prices—The Unprosecutable Crime*, 8 YALE J. REG. 281, 283 (1991) (describing "market power manipulation"); *see also* JOSEPH M. BURNS, A TREATISE ON MARKETS: SPOTS, FUTURES, AND OPTIONS 93–94 (1979) (describing the CFTC's "preventive and punitive approaches for dealing with temporary monopolies").

188. *See* 7 U.S.C. § 9(3) (2012) ("In addition to the prohibition in paragraph (1), it shall be unlawful for any person, directly or indirectly, to manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity.").

189. Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, tit. VII, 124 Stat. 1376, 1641–1802 (2010). Section 753 of Dodd-Frank amends section 6(c) of the CEA (codified at 7 U.S.C. §§ 9, 15 (2012)).

190. Before Dodd-Frank, "manipulation" generally required "actual manipulation," proven by a well-established four-prong test: (1) the ability to influence market prices, (2) the intent to create or affect prices not reflecting legitimate forces of supply and demand, (3) the existence of artificial prices, and (4) the accused caused such artificial prices. 2 THOMAS A. RUSSO, REGULATION OF THE COMMODITIES FUTURE AND OPTIONS MARKETS § 12.11 (1983).

191. 7 U.S.C. § 9(3) (2012) ("It shall be unlawful for any person, directly or indirectly, to

CFTC v. Atlantic Bullion & Coin, Inc.[192] In *Atlantic Bullion*, the CFTC brought a civil action against the coordinators of a Ponzi scheme involving spot-market silver contracts.[193] Over an eleven-year period, the defendants fraudulently sold silver contracts in a nationwide scheme.[194] The defendants never supplied any silver; instead, they misappropriated all the funds and issued false account statements.[195] Under a similar analysis, the CFTC could bring investor-protection measures to the spot market for blockchain-based currencies and derivative products.[196]

B. State Regulation of Blockchain-based Currencies

On June 3, 2015, New York's Department of Financial Services issued its final "BitLicense" framework for regulating "virtual currency businesses."[197] Over a period of almost one year, BitLicense went from its initial proposal[198] to reproposal[199] to final rule. The process gave rise to two comment periods that elicited thousands of letters[200] expressing a wide range of opinions. And although it is too

---

manipulate or attempt to manipulate the price of any swap, or of any commodity."). The CFTC implemented this provision in Final Rule 180.2. 17 C.F.R. § 180.1 (2012).

192. U.S. Commodity Futures Trading Comm'n v. Atl. Bullion & Coin, Inc., [2012–2013 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 32,551 (D.S.C. June 6, 2012).

193. Complaint at 1, *Alt. Bullion & Coin, Inc.*, No. 8:12-cv-01503-JMC.

194. *Id*.

195. *Id*. at 2.

196. Similarly, investors have at least some protection under U.S. securities laws, to the extent they are dealing in interests in bitcoin-related investment vehicles. *See* SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *6 (E.D. Tex. Sept. 18, 2014) (finding an interest in a bitcoin-based Ponzi scheme to be an "investment contract" for purposes of U.S. securities laws and imposing civil monetary penalties under the Securities Act). For an extended analysis of market manipulation at the infamous and ill-fated Mt. Gox exchange, see *The Willy Report: Proof of Massive Fraudulent Trading Activity at Mt. Gox, and How it has Affected the Price of Bitcoin,* THE WILLY REP. (May 25, 2014), https://willyreport.wordpress.com/2014/05/25/the-willy-report-proof-of-massive-fraudulent-trading-activity-at-mt-gox-and-how-it-has-affected-the-price-of-bitcoin [http://perma.cc/N59G-BSMC].

197. N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015).

198. N.Y. Dep't of Fin. Servs., Notice of Proposed Rulemaking on the Regulation of the Conduct of Virtual Currency Businesses, 36 N.Y. Reg. 14 (July 23, 2014) [hereinafter BitLicense Proposal]. The full text of the BitLicense Proposal is available from the NYDFS's website at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf [http://perma.cc/38SU-8XDB].

199. N.Y. Dep't of Fin. Servs., Notice of Proposed Rulemaking on the Regulation of the Conduct of Virtual Currency Businesses, 37 N.Y. Reg. 8 (Feb. 25, 2015) [hereinafter BitLicense Reproposal]. The full text of the BitLicense Reproposal is available at http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf [http://perma.cc/VR2p-KCCU].

200. Nearly 4,000 comments were received over the course of this eleven-month period. *See Comments Regarding the Proposed Virtual Currency Regulatory Framework*, N.Y. DEP'T OF

early to draw any empirical conclusions on BitLicense's long-term market impact,[201] it has certainly raised the cost of entry for certain participants and will likely pave a smoother path to integration with the established banking system.

New York's regime covers most business activities[202] involving (1) "virtual currencies," defined to include decentralized blockchain-based currencies,[203] and (2) New York or New York customers.[204] Much of the uncertainty around BitLicense lurks in its protracted definition of "virtual currency business activities," which breaks down into five major prongs: (1) transmitting virtual currency; (2) holding virtual currency on behalf of others; (3) buying and selling virtual currency as a customer business; (4) providing exchange services as a customer business; and (5) controlling, administering, or issuing virtual currency.[205]

First, the "transmission" prong presents some uncertainty in the statutory language itself. For example, the definition includes "the transfer, by or through a third party, of Virtual Currency from a Person to a Person."[206] Imagine a business that simply transfers virtual

---

FIN. SERVS., http://www.dfs.ny.gov/legal/vcrf_comments.htm [http://perma.cc/J7H3-KANH] (collecting comments).

201. The application deadline passed only four months prior to this Note's publication. *See BitLicense Frequently Asked Questions*, N.Y. DEP'T OF FIN. SERVS., http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm [http://perma.cc/972V-5Q3A] ("[A]pplicants must apply by August 10, 2015.").

202. Exemptions are provided for approved exchange service providers chartered under New York Banking Law and mere merchant/consumer activities. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.03(c) (2015).

203. *Id.* § 200.02(m). This includes:

> Any type of digital unit used as a medium of exchange or form of digitally stored value [and is] broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.

DAVIS POLK & WARDWELL LLP, NEW YORK'S FINAL "BITLICENSE" RULE: OVERVIEW AND CHANGES FROM JULY 2014 PROPOSAL 9 (2015), http://www.davispolk.com/sites/default/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf [http://perma.cc/V5KG-C9ZJ]. It does not include digital units that are used (i) solely within online-gaming platforms, such as Nintendo Wii Points; (ii) in connection with a customer-affinity or rewards program, such as Delta SkyMiles; or (iii) used as part of fiat prepaid cards. *Id.*

204. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.02(n) (2015). The extent of New York jurisdiction is very broad. It likely includes businesses that serve or solicit New York customers through web-based services when such businesses do not take adequate precautions to exclude such customers. However, because no prohibition precludes dividend distributions, businesses may choose to limit New York–facing activity to limited-purpose subsidiaries.

205. *Id.* § 200.02(q)(1)–(5).

206. *Id.* § 200.02(o).

currency internally between proprietary accounts. In such a case, the transmission prong rightly is not triggered because the business does not interact with any third parties. However, what if that same business also transfers virtual currency to third parties, but not for goods or services—for example, to pay dividend distributions or salaries? The statutory language does not resolve whether the business, by virtue of that fact alone, must carry a BitLicense.

Another wrinkle in the "transmission" prong is the explicit exception for transactions "undertaken for non-financial purposes" that do not involve "more than a nominal amount" of virtual currency.[207] "Non-financial" is not a statutorily defined term. Blockchain technology can be used in a number of ways that are clearly "non-financial"—for example, to facilitate identity verification,[208] digital-document verification,[209] or peer-to-peer transfers of digital assets.[210] In other cases, however, it is less clear whether this exception applies. For example, how would a smart contract[211] transferring a right to payment from financial assets using a nominal amount of virtual currency be treated?

Second, the "holding" prong presents uncertainty with respect to its scope. Though the draft language includes the word "securing," that word is absent from the final rule.[212] "Securing" virtual currency likely refers to multi-signature ("multi-sig") transactions. Multi-sig transactions involve more than two parties.[213] For example, a two-of-three multi-sig transaction is a transaction between three parties that requires the approval of two parties prior to settlement.[214] One implication of this feature is cryptographic escrow. For example,

---

207. Importantly, based on the structure of the rule itself, this is an exception from the "transmission" prong, not from the entire rule. *See id.* § 200.02(q)(1) (exempting this transaction from the definition of transmission).

208. *See, e.g.*, ONENAME, https://onename.com [https://perma.cc/9YZV-G5NK] (allowing users to sign their blockchain transactions with a verifiable personal identity).

209. *See, e.g.*, BLOCK NOTARY, http://www.blocknotary.com [http://perma.cc/KD26-F2F2] (allowing users to securely and digitally sign documents via blockchain transactions, performing a notary-like function).

210. For more examples of potential innovative applications of blockchain technology, see *infra* Part III.

211. For a discussion of smart contracts, see *infra* Part III.B.

212. *Compare* BitLicense Proposal, *supra* note 198, § 200.2(n)(2) (defining "Virtual Currency Business Activity" to include "securing . . . Virtual Currency on behalf of others), *with* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q) (2015) (omitting the word "securing").

213. ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 129 (2014).

214. *Id.* at 129–30.

Party A and Party B enter a contract with payment provisions contingent on an objectively verifiable event. They enlist Party M as a mediator who will sign the transaction in favor of the appropriate party upon the occurrence or nonoccurrence of such event. Removing Party M from the scope of this prong is probably appropriate because Party M never actually takes custody of the assets.

Third, the "buying and selling" prong presents uncertainty in the statutory language. Specifically, this prong is triggered by the buying and selling of virtual currency "as a customer business"[215]—a phrase that, read broadly, could likely encompass a wide range of activity. The best way to view this prong seems to be that it refers to buying virtual currency from customers and selling virtual currency to customers on a principal or agency basis. Under this interpretation, sales of virtual currency to third parties that are not part of the customer-facing business should fall beyond the provision's scope.

Both the fourth and fifth prongs (that is, the "exchange services" and "controlling or administering" prongs) overlap with FinCEN's definitions of "exchangers" and "administrators" under FinCEN's 2013 guidance.[216] Likewise, the same analysis that applies under FinCEN's 2013 guidance would apply to covered activities under both prongs.[217] Miners and creators of decentralized virtual currencies likely would be excluded under the same reasoning, assuming their activities extend no further.[218]

Lastly, two exemptions are worth noting.[219] First, the "merchant/consumer" exemption is fairly straightforward. Like FinCEN's 2013 guidance,[220] it carves out merchants or consumers who use virtual currency solely for purchasing or selling goods or services, or solely for investment purposes. Second, a more ambiguous "software developer" exemption applies to individuals and businesses that engage solely in the development and dissemination of

215. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q)(3) (2015).

216. *See supra* notes 152–56 and accompanying text.

217. *See supra* notes 160–63 and accompanying text.

218. *Id.*

219. The "non-financial purposes" exception to the "transmission" prong would not be considered an exemption here because it only operates as an exclusion to that specific element of "virtual currency business activity." *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q)(1) (2015) (excluding non-financial purposes from this definition). In other words, a business may satisfy the "non-financial purposes" exception yet still be subject to the rule by means of one of the other four prongs.

220. *See supra* note 156 and accompanying text.

software.[221] NYDFS has consistently asserted that it is regulating financial intermediaries, not software developers.[222] However, the line between the two may not always be clear.

Consider a business that develops wallet software—mobile applications that allow users to view and manage their virtual-currency balance.[223] On one hand, the developer does not take custody of the user's virtual currency at any point, and it does not transmit or exchange virtual currency.[224] Instead, it simply provides the user with a blockchain access point. On the other hand, the software stores the user's private key—the secret mathematical code necessary for the user to access his holdings on the blockchain. This weighs against the exemption's application, because access to a user's private key is the functional equivalent of access to the user's holdings tied to that key. Accordingly, a security compromise in the wallet software could cause users to lose all or part of their virtual-currency holdings.[225]

In light of the prior analysis, it seems fair to say that the law will have at least two short-term consequences. First, it will raise the cost of entry for market participants by mandating various programs—cybersecurity,[226] consumer protection,[227] financial reporting,[228] and AML.[229] Indeed, many businesses have already chosen to exit New

---

221. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.02(q) (2015).

222. *See, e.g.*, *NYDFS Announces Final Bitlicense Framework for Regulating Digital Currency Firms*, N.Y. DEP'T OF FIN. SERVS. (June 3, 2015), http://www.dfs.ny.gov/about/speeches/sp1506031.htm [http://perma.cc/9Y8C-3BYS] ("[W]e have no intention of being a regulator of software developers—only financial intermediaries.").

223. *See Some Bitcoin Words You Might Hear: Wallet,* BITCOIN.ORG, https://bitcoin.org/en/vocabulary#wallet [https://perma.cc/SS6R-9MNC] (defining "wallet").

224. This assumes the service is purely a wallet provider and does not provide additional value-added services, such as an exchange of U.S. dollars to virtual currency.

225. *See, e.g.*, McMillan, *supra* note 8 (reporting on a digital attack in which $1.2 million in bitcoins were stolen from online virtual wallets).

226. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.16 (2015). Cybersecurity requirements would include board-approved cybersecurity policy and a program to protect electronic systems and sensitive data, qualified chief information security officer, annual reports to NYDFS, annual penetration testing and audits, and maintenance of a business-continuity and disaster-recovery plan, to be independently tested annually. *Id.* § 200.16(b); *id.* § 200.17.

227. *Id.* § 200.19. Consumer-protection requirements include the disclosure of material risks, including certain minimum disclosures: virtual currency is not legal tender, transactions are generally irreversible, and the risk of fraud, cyberattack, and total loss of value, among other risks. *Id*.

228. *Id.* § 200.14. Reports and financial disclosures

229. *Id.* § 200.15. AML requirements include initial and annual risk assessments, ten-year records of all transactions, suspicious activity reports, a customer identification program, Office

York, citing total compliance implementation costs between $50,000 and $100,000.[230] Second, the certainty of licensure decreases legal risk of companies operating in this space, so a smoother path will likely emerge for blockchain businesses to integrate with the established banking system.

III. THE BLOCKCHAIN REVISITED: THE SHAPE OF TRANSACTIONS TO COME

This Part builds on the explanation of blockchain technology set forth in Part I and illustrates why regulations designed to "broadly construe[]"[231] the definition of "virtual currency" may unintentionally engulf an entire realm of activities. First, it explains the concepts of "scripting" and "sidechains"[232]—innovations that could spawn additional applications for blockchain technology. Second, it surveys current research and experimentation at the cutting edge of cryptography and computer science that could impact commerce and on a similar order of magnitude as the Internet did. It closes by circling back to themes raised in Part II, exploring the challenge that regulators face as they seek to understand this technology.

A. The Blockchain Revisited: Scripting and Sidechains

Potential applications of blockchain technology are not limited to money transfers and payments. At its core, this protocol facilitates more than the exchange of "bitcoins"; it facilitates the exchange of *value*.[233] Part I established a series of important mathematical rules

---

of Foreign Asset Control (OFAC) checks and compliance, annual internal or external audits, and no structuring to evade reporting, or obfuscating identity. *Id.*

230. Daniel Roberts, *Behind the "Exodus" of Bitcoin Startups from New York*, FORTUNE (Aug. 14, 2015, 11:19 AM), http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense [http://perma.cc/T3WF-QEHE] (citing at least ten companies that chose to exit New York, rather than incur the costs of compliance).

231. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(p) (2015) ("Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.").

232. *See* BACK ET AL., *supra* note 33, at 5 (introducing the term "sidechain," and describing it as a blockchain that is interoperable with the main Bitcoin blockchain).

233. *Id.* at 4 ("There are assets besides currencies that may be traded on blockchains, such as IOUs and other contracts, as well as smart property."); Evans, *supra* note 106, at 1 (defining the blockchain as a "protocol for sending, receiving, and recording value securely"); *see also infra* Part III.B (describing some alternative applications of blockchain technology); *see generally* SWANSON, *supra* note 37 (discussing ways in which blockchain technology can be utilized to exchange things of value).

that govern the network. Fundamentally, transactions have a three-part structure: (1) Party A sends a message to the network declaring the transaction; (2) Party B accepts the transaction by broadcasting its acceptance; and (3) the network participants verify the transaction's authenticity.[234] To be sure, this basic structure was designed for transferring ownership of bitcoins. But when people send and receive bitcoins, those bitcoins are best thought of as containers for value.[235] Like a digital envelope, these containers can carry "coins" across the network; but they can also transmit richer forms of information, holding promise for many compelling applications beyond bitcoin.[236]

A typical transaction follows a simple script—a set of instructions—that adheres to the three-part structure described above.[237] If the script were amended to contain additional conditions, users could engage in more sophisticated transactions. For instance, consider that Party A and Party B may want to add a fourth condition to that script structure: they only want the transaction to occur at a certain time, or upon the occurrence or nonoccurrence of a conditional event. Many possibilities branch out from this basic idea, and it has sparked much discussion around "smart" contracts.[238]

As a practical matter, developers cannot currently implement scripts like this in bitcoin transactions because protocol amendments require a majority consensus.[239] Similar to a corporate charter, default rules are easy to establish at the outset and much harder to change later on. This fact, paired with the open-source nature of the Bitcoin platform, has inspired dozens of "altcoins," or alternative-utility iterations on blockchain technology.[240] In other words, developers

234. *See supra* notes 61–66 and accompanying text.

235. Evans, *supra* note 106, at 4 ("Calling the container a coin causes confusion because, at least at the start of the platform, the container is not a currency, since it is not widely used, and because the public ledger platform could be viable even if the container did not evolve into being a general-purpose currency.").

236. SWANSON, *supra* note 37, at n.55.

237. *Id*.

238. *See, e.g.*, Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST CO. LABS (Sept. 17, 2014), http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app [https://perma.cc/YU3Y-MLKP] (explaining how smart-contract projects such as Ethereum and Codius are aimed at decreasing the monitoring and enforcement costs inherent in contracting).

239. This is an economic majority of 51 percent. *See supra* note 105; *see also* SWANSON, *supra* note 37 at 18, 28 (explaining that Bitcoin Improvement Proposals require community consensus in order to be implemented).

240. *See* SWANSON, *supra* note 37, at 13 ("An altcoin means 'alternate coin' – which commonly means any cryptocoin or cryptoledger that is not Bitcoin.").

with a novel vision for the ideal blockchain parameters set their own rules at the outset, according to a desired set of economic properties.[241] Some examples are Litecoin, a platform similar to Bitcoin but with faster transaction confirmations, an ideal feature for high-volume merchants;[242] Viacoin, a "notary" platform that time-stamps, transfers, and verifies ownership of documents;[243] and Storjcoin, a platform much different from Bitcoin that allows for a decentralized cloud storage system.[244]

Despite the excitement of this unbounded innovation, a system of parallel blockchains is inefficient and undesirable. They also pose significant risks to the sustainability and goodwill of the blockchain experiment. Although a full discussion of these risks exceeds the scope of this Note, they generally fall into one or more of the following categories: problems of initial distribution and valuation, liquidity shortages, adverse network effects, market fluctuations, fragmentation, security breaches, pump-and-dump market games, and plain fraud.[245] The good news, however, is that a recent development has shown these "worlds" of alternative-utility blockchains can coexist without the exchange-rate risk and other factors that make the current altcoin system unworkable.[246]

In October 2014, a group of leading developers introduced the concept of "sidechains."[247] Unlike altcoins, which require users to leave the Bitcoin platform, exposing them to significant risks,[248] sidechains are blockchains that are interoperable with one another and, most importantly, interoperable with the Bitcoin blockchain.[249]

---

241. *Id*.

242. LITECOIN, http://www.litecoin.org [http://perma.cc/SVYS-9DEN].

243. VIACOIN, http://viacoin.org [http://perma.cc/AGT6-6EHP].

244. STORJ, http://www.storj.io [http://perma.cc/WD67-FV5L].

245. *See* BACK ET AL., *supra* note 33, at 5 (describing these as problems with bitcoin and other cryptocurrencies); *see also* William J. Luther, *Cryptocurrencies, Network Effects, and Switching Costs* (Kenyon Coll., Mercatus Center Working Paper No. 13-17) (July 17, 2013) (on file with the *Duke Law Journal*) (analyzing the adverse impact of network effects and switching costs with respect to blockchain-based currencies like bitcoin). Given the legitimate policy issues around such "vaporware"—technology that is promised, but never fully developed—future scholarship in this area might consider whether the federal securities laws provide an appropriate mechanism for investor protection, particularly when such technology is centrally administered.

246. *See generally* BACK ET AL., *supra* note 33 (suggesting "sidechains" as a tool for avoiding these problems).

247. *Id*. at 1.

248. *See supra* text accompanying note 245.

249. BACK ET AL., *supra* note 33, at 5, 8.

By integrating with Bitcoin's blockchain, sidechains provide the benefits of altcoins without the accompanying risks. Such purpose-specific scripting will encourage further innovation[250] by allowing for a network of "distributed trust systems."[251]

B. Decentralized Smart Contracts and the Shape of Transactions to Come

Sidechains and scripting are changing how people think about blockchain technology. One broad area of innovation around these features is decentralized smart contracts.[252] Smart contracts are "computer protocols that facilitate, verify, execute and enforce the terms of a commercial agreement."[253] This concept is not new and is not unique to the blockchain. One primitive example is digital rights management (DRM), a technology developed to fight copyright infringement.[254] DRM technology essentially embedded U.S. copyright law into digital files by limiting the user's ability to view, copy, play, print, or otherwise alter the works.[255] In other words, digital audio files encrypted with DRM technology were not subject to the double-spending problem because they contained a basic smart contract, one that referenced a centralized network, (that is, Apple's server programmed to enforce the iTunes Store Terms and Conditions).[256]

The blockchain enables decentralized smart contracts—in other words, smart contracts that leverage a secure public ledger as an enforcement mechanism.[257] In contrast to the iTunes example, these

---

250. *See id*. at 7 ("[B]ecause sidechains are still blockchains independent of Bitcoin, they are free to experiment with new transaction designs, trust models, economic models, asset issuance semantics, or cryptographic features.").

251. *Id*. at 7. One expansive way to conceptualize the blockchain innovation is through the concept of "trustlessness"—the property of enabling all parties to verify on their own that information is correct without relying on trusting external parties for correct operation. *Id*.

252. *See* SWANSON, *supra* note 37, at 15–16 (introducing the concept of smart contracts and discussing their potential usefulness).

253. *Id*. at 11.

254. ROSS ANDERSON, SECURITY ENGINEERING 679 (2d ed. 2008); *see also* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 60 (2008) (explaining the evolution of DRM technology).

255. Armstrong, *supra* note 254, at 60.

256. In 2009, Apple changed its policy and no longer provides DRM-encrypted digital files in its iTunes store. *See* Ruth Suehle, *The DRM Graveyard: A Brief History of Digital Rights Management in Music*, OPENSOURCE.COM (Nov. 3, 2011), http://opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music [http://perma.cc/F94Q-3JDK].

257. For an extended discussion on decentralized smart contracts, see SWANSON, *supra* note

contracts do not rely on a third-party institution or server for centralized recordkeeping and enforcement. Because blockchain transactions are programmable and self-enforcing, parties might use smart contracts to design contractual relationships that are automatically executed without the additional costs of monitoring or enforcement.

This fact is significant. Intermediaries typically establish trust and reduce risk between counterparties to a transaction.[258] But with decentralized smart contracts, parties may transact at arms length, with total strangers, without the worry of fraud, and without the cost of third-party enforcement (that is, recordkeeping costs, mediation costs, and other administrative and operational costs). In other words, decentralized smart contracts allow for new markets to develop: disintermediated contract markets in which parties do not have concern for counterparty risk.[259]

Consider a smart-contracts market for futures trading.[260] Smart contracts in this market would be simple for two reasons. First, futures agreements involve objectively verifiable conditions about the state of the world—for example, the price of crude oil at a given time on the New York Mercantile Exchange. And second, futures agreements are highly standardized to ensure that contracts can be easily traded and priced.[261] Such an agreement would be self-

---

37, at 15–30.

258. DOUGLAS NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 6 (1990).

259. Counterparty risk is the risk arising from the possibility that the counterparty may default on amounts owed on a transaction. THE NEW PALGRAVE DICTIONARY OF MONEY & FINANCE 502 (John Eatwell, Murray Milgate & Peter Newman eds., 1992).

260. For an extended analysis of smart contract markets and futures trading, see generally Trevor I. Kiviat, "Smart" Contract Markets: Trading Derivatives on the Blockchain (Apr. 2015) (unpublished manuscript), https://www.academia.edu/10766594 [http://perma.cc/2K8A-4HAW].

261. CME GROUP, A TRADER'S GUIDE TO FUTURES 4 (2013), https://www.cmegroup.com/education/files/a-traders-guide-to-futures.pdf [http://perma.cc/7ASG-6G3T]; *see also* Stephen G. Cecchetti, Jacob Gyntelberg & Marc Hollanders, *Central Counterparties for Over-the-Counter Derivatives*, BIS Q. REV., Sept. 2009, at 45, 49 ("[D]erivatives contracts have in many cases become more standardised. For example, over the years, *interest rate swaps* and foreign exchange derivatives have become highly standardised through voluntary industry initiatives."). This model is based on a hypothetical developed by Professor Houman B. Shadab in his remarks to the CFTC's Global Markets Advisory Committee. Houman B. Shadab, Professor of Law, New York Law School, Regulating Bitcoin and Block Chain Derivatives: Written Statement to the Commodity Futures Trading Commission 15 (Oct. 9, 2014), http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf [http://perma.cc/XL9G-5WXU].

monitoring and self-enforcing through a combination of scripting,[262] multi-sig,[263] and oracles, systems set up to monitor off-blockchain information and data that is essential to the effective execution of the smart contract's terms.[264]

In sum, the technology's potential to lower transaction costs with respect to contracting and transferring title to physical and personal property should generate special interest in the legal community. To be sure, there are challenges. First, the task of encoding the legal subtleties and nuances that underlie even the most basic contract poses significant programming challenges. And second, it is not clear whether and how smart contracts fit within the legal frameworks of the Uniform Commercial Code and general common law. Although an extended discussion of these two issues is beyond the scope of this Note, their serious analysis would add much to this nascent field.

CONCLUSION

Blockchain technology is adaptable and policymakers must view it as such. Regulation designed to mitigate the risks of such a powerful technology should be encouraged. However, policymakers should exercise caution and precision in tailoring the scope of regulation. As illustrated above, blockchain technology has utility beyond transmitting value in the traditional money-transmitter sense. Regulation aimed at the blockchain's money-transfer and payment functionalities must not create an unintentional chilling effect on this second category of functionalities.

States should monitor New York's BitLicense experiment and consider the issues raised in this Note as they consider their own models.[265] .For example, the NYDFS has recognized that BitLicense is

---

262. *See supra* Part III.A.

263. *See supra* note 213 and accompanying text.

264. "Off-blockchain" events are any measurable events that occur outside of the blockchain and thus cannot be monitored by an on-blockchain script. The current temperature in Durham, North Carolina; the spot price of Brent crude at a particular time in the future; and the results of the 2015 NCAA Men's Basketball Tournament are all off-blockchain events that could be referenced in a smart contract and enforced by an oracle.

265. It is likely that many such codes will be based on the Conference of State Bank Supervisors Draft Model Regulatory Framework for Virtual Currency Activities. *See* CONF. STATE BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES: CSBS MODEL REGULATORY FRAMEWORK (Sept. 15, 2015), https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf [http://perma.cc/USP3-U5WX].

intended only to apply to financial intermediaries.[266] This Note highlighted some ambiguity around "nonfinancial" use language.[267] Further, depending on particular alternative applications of blockchain technology, some additional guidance and regulation may need to occur outside of the BSA and state banking frameworks. For example, smart contracts that enable equity crowdfunding[268] should fit squarely in the domain of federal securities law, triggering registration and disclosure requirements and subjecting participants to SEC enforcement rules. In other words, policymakers must carefully define the specific activities that they seek to regulate. A basic understanding of the concepts set forth in this Note would be a strong starting point. To borrow from technologist Mark Stefik's words on the Internet, blockchain technology can support different kinds of dreams: "We choose, wisely or not."[269]

266. DAVIS POLK & WARDWELL LLP, *supra* note 39.

267. *Id*.

268. *See* SWANSON, *supra* note 37, at 83 (describing "crowdequity" as a potential tool for incentivizing early adoption by giving an equity stake to early users).

269. Mark J. Stefik, *Epilogue: Choices and Dreams*, *in* INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 390 (Mark J. Stefik ed. 1996).