CRYPTOCURRENCY AND THE MYTH OF THE TRUSTLESS TRANSACTION

Rebecca M. Bratspies

"It's going to prevent wars, help the unbanked and bring honesty to financial systems."[1]

"It's worse than tulip bulbs. It won't end well. Someone is going to get killed,"[2]

Keywords: *bitcoin, smart contract, ICO, fraud, legitimacy, regulatory trust, blockchain, regulation, trust, cryptocurrency, technology.*

1. Kirsten Grind, *Let Me Tell You Some More About Bitcoin Hello? Hello?,* WALL ST. J. (Jan. 19, 2018, 11:02 AM), https://www.wsj.com/articles/mention-bitcoin-one-more-time-and-youre-sleeping-on-the-couch-1516377771 (quoting Doug Scribner, 50, of Edina, Minn.).

2. Fred Imbert, *JPMorgan CEO Jamie Dimon Says Bitcoin is a 'Fraud' that Will Eventually Blow Up*, CNBC (Sep. 12, 2017, 1:27 PM), https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html.

I. INTRODUCTION

Imagine a globally-accepted virtual currency able to facilitate virtually costless transactions[3] at near lightning speed.[4] Now imagine that this currency is open-source and decentralized.[5] Then add an unalterable, tamper-free recording feature to guarantee that every transaction 100% secure, and throw in anonymity to boot.[6] Finally, eliminate the need to trust third parties by making this currency independent of central banks or financial institutions.[7] This is the basic pitch for cryptocurrency—from Bitcoin to the thousands of alt-coins[8] that have followed in its wake. It is not hard to find true believers touting each of these supposed cryptocurrency traits as though they were gospel.

The term "*hodl*"[9] captures some of the evangelical fervor of bitcoin's proponents. An inside joke in the cryptocurrency world, *hodl* stands for long-term commitment to cryptocurrencies in the face of wild fluctuations.[10] These true believers posit a world with virtually limitless applications for the block chain—the technology at the core of cryptocurrencies. They suggest that these virtual cryptocurrencies[11] will replace fiat currencies, includ-

---

3. *See e.g.*, JERRY BRITO AND ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 13 (2016) (asserting that, "Because there is no third-party intermediary, bitcoin transactions can be cheaper and quicker than traditional payment networks").

4. *See* Felix Küster, *The War of Cryptocurrencies: Ripple vs. Ethereum vs. Bitcoin*, CAPTAINALTCOIN.COM (Dec. 8, 2017), https://captainaltcoin.com/ripple-vs-ethereum-vs-bitcoin/ (describing bitcoin as "frictionless, anonymous, and cryptographically astonishingly secure").

5. BITCOIN, https://bitcoin.org/en/ (last visited Oct. 26, 2018).

6. *Bitcoin for Individuals*, BITCOIN, https://bitcoin.org/en/bitcoin-for-individuals (last visited Oct. 26, 2018).

7. Patrick Mansfield, *A Bitcoin Guide: A Brief History, How to Buy, and the Latest Quote*, USCONSUMERFINANCE, https://www.usconsumerfinance.com/bitcoin-information (last visited Oct. 26, 2018).

8. Altcoins are cryptocurrencies other than Bitcoin, the first such digital currency. *See Altcoin: Definition of 'Altcoin'*, INVESTOPEDIA, https://www.investopedia.com/terms/a/altcoin.asp (last visited Oct. 26, 2018).

9. "Hodling" is an inside joke in the cryptocurrency world. It stems from a typo in a drunken rant by a user named GameKyuubi on the Bitcoin Forum in 2013. *See* GameKyuubi, *I am Hodling*, BITCOIN FORUM (Dec. 23, 2013, 10:03 AM), https://bitcointalk.org/index.php?topic=375643.0?red; *see also* rafaelnorman, *what's HODL?*, REDDIT (Jul. 20, 2014, 6:37 PM), https://www.reddit.com/r/Bitcoin/comments/2b8t78/whats_hodl/.

10. In comment after comment, "hodlers" advised the original poster to relax and wait for the inevitable bounce as the market returns to "normal." *See* Maxnilu, *Why Are All Cryptos Dropping In Price?*, BITCOIN FORUM (Feb. 01, 2018, 12:10 PM), https://bitcointalk.org/index.php?topic=2862588.0.

11. "The Financial Action Task Force defines 'virtual currency' as: a digital representation of value that can be digitally traded and functions as: (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from

ing the dollar, the yen and the euro. So far, the reality of cryptocurrency has not lived up to its hype. It turns out that cryptocurrency transactions can be slow[12] and expensive,[13] because the core technology, the blockchain,[14] scales poorly.[15] These technological issues may or may not be fixable. However, the most interesting divergence between this marketing pitch and cryptocurrency's actual track record have to do with the purported consequences of decentralization[16]—the claim that bitcoin obviates the need for trust.

In an increasingly volatile world, cryptocurrencies like Bitcoin purport to replace trust with technology. Indeed, Bitcoin founder, Satoshi Nakamoto described Bitcoin as an "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[17] In the 2008

---

fiat currency (a.k.a. 'real currency,' 'real money,' or 'national currency'), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency." Financial Action Task Force [FATF], Report on *Virtual Currencies—Key Definitions and Potential AML/CFT Risks*, at 4 (Jun. 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

12. In July 2017, the average transaction time was 116 minutes. *See*, Alex Lielacher, *How Long Should My Bitcoin Transaction Take?*, BITCOIN MKT. J. (Jul. 6, 2017, 11:00 AM), https://www.bitcoinmarketjournal.com/how-long-bitcoin-transactions/. In February 2017, transactions ranged from 14 minutes to 454 minutes, depending on the day. *See Average Confirmation Time*, BLOCKCHAIN, https://www.blockchain.com/charts/avg-confirmation-time?timespan=2years (last visited Oct. 26, 2018).

13. *See* Ryan Browne, *Big Transaction Fees are a Problem for Bitcoin—but There Could Be a Solution*, CNBC (Dec. 19, 2017), https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html. Bitcoin is what one user described as a "pay-to-play protocol." *See* brianddk, Comment to *Average Confirmation Times*, REDDIT (Mar. 2, 2016, 2:31 PM), https://www.reddit.com/r/Bitcoin/comments/48m9xq/average_confirmation_times/. Adding a fee to a bitcoin transaction bumps that transaction up in the queue. Those who do not pay a fee, or do not pay a sufficiently big fee, can wait hours or even days for their transaction to complete. *See e.g.*, fluffy1337, *PSA: Due to Delays, If you Buy Bitcoins Make Sure to Keep Them On An Exchange or They May Get Stuck in Transit for a While*, REDDIT (Mar. 2, 2016, 8:23 PM), https://www.reddit.com/r/btc/comments/48pkrw/psa_due_to_delays_if_you_buy_bitcoins_make_sure/; *see also*, caveman2, *I Have Issues With My Bitcoin Returned*, LOCALBITCOINS.COM (Mar. 2, 2016, 7:33 PM), https://localbitcoins.com/forums/#!/general-discussion:i-have-issues-with-my-bitco.

14. *See infra* pp. 19–29 for a detailed discussion of Blockchains.

15. Darryn Pollock, *SegWit2x's Failure Confirms Bitcoin's Status as Digital Gold,* COINTELEGRAPH (Nov. 14, 2017), https://cointelegraph.com/news/segwit2xs-failure-confirms-bitcoins-status-as-digital-gold (quoting Morgan Stanley analysts).

16. *See*, *What is Bitcoin?*, COINDESK (Jan. 26, 2018), https://www.coindesk.com/information/what-is-bitcoin/ ("Bitcoin's most important characteristic is that it is decentralized. No single institution controls the bitcoin network. It is maintained by a group of volunteer coders, and run by an open network of dedicated computers spread around the world.").

17. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008), https://bitcoin.org/bitcoin.pdf. The protocol behind the blockchain was first described in 1998 by Wei Dai. Wei Dai, *bmoney*, Wei Dai (1998), http://www.weidai.com/bmoney.txt.

whitepaper that launched Bitcoin, Satoshi Nakamoto criticized existing electronic payment systems for requiring a trusted third-party intermediary.[18] Nakamoto wrote the Bitcoin white paper during the depths of the 2008 financial crisis, when trust in the ability of governments and banks to manage the economy was at its nadir.[19] A decade later, the so-called "trustless" nature of cryptocurrency is still a big selling point. For example, the cryptocurrency news site Coindesk offers a Bitcoin 101 which touted that: "You don't need to trust anyone else."[20] Coindesk went on to explain that in the conventional banking system, there are multiple points at which trust comes into play: "You have to trust the bank, for example. You might have to trust a third-party payment processor. You'll often have to trust the merchant too. These organizations demand important, sensitive pieces of information from you."[21] With the blockchain, by contrast, cryptocurrency's boosters claim that trust, along with centralization, is no longer necessary.[22]

Depending on who you ask, Bitcoin, and cryptocurrencies more generally, are either "world-changing"[23] and "the wave of the future,"[24] or, alternatively, are a mania,[25] "more religion than asset,"[26] "rat poison squared"[27]

---

18. *See* NAKAMOTO, *supra* note 17, at 1.

19. *See* PEW RESEARCH CTR., THE PEOPLE AND THEIR GOVERNMENT: DISTRUST, DISCONTENT, ANGER AND PARTISAN RANCOR 4–5 (2010), http://www.pewresearch.org/wp-content/uploads/sites/4/legacy-pdf/606.pdf (noting that an October 2008 poll found that only 17% of respondents trusted the government to do what was right).

20. *Why Use Bitcoin?*, CYBER SECURITY INTELLIGENCE (Jun. 1, 2015), https://www.cybersecurityintelligence.com/blog/why-use-bitcoin-323.html.

21. *Id.*

22. *See e.g.*, Bryan Chia, *What is Cryptocurrency? (Part 2: Trustless, Decentralized & Immutable)*, MEDIUM (Nov. 27, 2017), https://medium.com/@dashrandom/what-is-cryptocurrency-part-2-trustless-decentralized-immutable-c6e82833bd5c.

23. *See generally* THE RISE AND RISE OF BITCOIN (Fair Acre Films & 44th Floor Productions 2014), https://bitcoindoc.com/.

24. Mike Ayers, *'Shark Tank' Investor Robert Herjavec Has a Bold Prediction for the Future of Cryptocurrency*, MONEY (Feb. 8, 2018), http://time.com/money/5137464/shark-tank-investor-robert-herjavec-has-a-bold-prediction-for-the-future-of-cryptocurrency/. A recent *New York Times* article quoted one enthusiast as proclaiming: "It's the entire world reorganizing itself. We could get rid of our armies because for the first time you'll have people saying, 'I want to vote for a global order.' It's the internet waking up — it's the internet grabbing its pitchfork. That's the blockchain." Nellie Bowles, *Everyone is Getting Hilariously Rich and You're Not*, N.Y. TIMES (Jan. 13, 2018), https://www.nytimes.com/2018/01/13/style/bitcoin-millionaires.html (quoting James Fickel).

25. Felix Allen, *'Absolutely Bananas' Bitcoin Bubble Fears as Cryptocurrency Soars Toward Record $10,000 with Half a Million New Investors a Day*, SUN (Nov. 28, 2017), https://www.thesun.co.uk/money/5016647/bitcoin-bubble-crash-price-record/.

26. A.J. Dellinger, *Bitcoin, Cryptocurrency Predictions 2018: What Mark Cuban Thinks About the Future of the Currency*, INT'L BUS. TIMES (Jan. 21, 2018), http://www.ibtimes.com/bitcoin-cryptocurrency-predictions-2018-what-mark-cuban-thinks-about-future-coins-2643150 (quoting Mark Cuban).

27. Paul R. La Monica, *Warren Buffett Says Bitcoin is "Rat Poison"*, CNN (May 8, 2018), https://money.cnn.com/2018/05/07/investing/warren-buffett-bitcoin/index.html.

or even a fraud.[28] Regardless of which camp one falls into, there is no question that the touted security of the blockchain has not prevented thieves and scam artists from stealing millions of dollars of cryptocurrency. Indeed, the combination of rapidly rising cryptocurrency values, anonymity, and lack of regulation make cryptocurrency platforms[29] "natural targets" for theft.[30] As of late 2017, Reuters estimated that 980,000 coins, worth up to $15 billion had been stolen between 2011 and 2017.[31] And that was before the January 2018, when hackers stole $534 million from Japanese cryptocurrency platform CoinCheck,[32] not to mention the June 2018 hacks of Korean cryptocurrency platforms Coinrail ($42 billion in market value loss)[33] and Bithumb ($30 million in coins stolen).[34]

This article interrogates the claim that trust can be replaced with blockchain technology. Part I begins with an introduction that provides an overview of the trust issues surrounding cryptocurrency. Part II then outlines the role that trust plays in a financial market more generally, focusing specifically on the trust embedded in what cryptocurrency supporters derogate as a 'fiat' currency. Part III introduces the blockchain, as well as Bitcoin and

---

28. Imbert, *supra* note 2. To be fair, Jamie Dimon has since said that he regrets calling bitcoin a fraud. Tae Kim, *J.P. Morgan CEO Jamie Dimon Says He Regrets Calling Bitcoin a Fraud*, USA TODAY (Jan. 9, 2018), https://www.usatoday.com/story/money/markets/2018/01/09/j-p-morgan-chase-ceo-jamie-dimon-says-he-regrets-calling-bitcoin-fraud/1016088001/. However, Dimon still refers to Bitcoin as a "scam." William Suberg, *JPMorgan CEO Jamie Dimon Returns to Bitcoin Bashing, Calls Cryptocurrency a Scam*, COIN TELEGRAPH (Aug. 8, 2018), https://cointelegraph.com/news/jpmorgan-ceo-jamie-dimon-returns-to-bitcoin-bashing-calls-cryptocurrency-a-scam.

29. Although cryptocurrency platforms are often called "exchanges," the SEC cautions investors that these platforms are unregulated, and "there is no reason to believe [that information provided by these platforms] has the same integrity as that provided by national securities exchanges." SEC, STATEMENT ON POTENTIALLY UNLAWFUL ONLINE PLATFORMS FOR TRADING DIGITAL ASSETS (2018), https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

30. *See* Steven Melendez, *Bitcoin Heist Adds $77 Million to Total Hacked Hauls of $15 Billion*, FASTCOMPANY (Dec. 7, 2017), https://www.fastcompany.com/40505199/bitcoin-heist-adds-77-million-to-hacked-hauls-of-15-billion.

31. Jim Finkle & Jeremy Wagstaff, *Hackers Steal $64 Million from Cryptocurrency Firm NiceHash*, REUTERS (Dec. 6, 2017), https://www.reuters.com/article/us.-cyber-nicehash/hackers-steal-64-million-from-cryptocurrency-firm-nicehash-idUSKBN1E10AQ.

32. Guarav Sharma, *'Crypto Heist': Coincheck Hack Could Be the World's Biggest Every CryptoCurrency Theft,* FORBES (Jan. 27, 2018), https://www.forbes.com/sites/gauravsharma/2018/01/27/crypto-heist-coincheck-hack-could-be-the-worlds-biggest-ever-cryptocurrency-theft/#6c99af91d583.

33. Eric Lam, Jiyuen Lee & Jordan Robertson*, Cryptocurrencies Lose $42 Billion After South Korean Bourse Hacked*, BLOOMBERG (June 10, 2018, 5:31 AM), https://www.bloomberg.com/news/articles/2018-06-10/bitcoin-tumbles-most-in-two-weeks-amid-south-korea-exchange-hack.

34. Saheli Roy Choudhury, *South Korean Cryptocurrency Exchange Bithumb Says It Was Hacked and $30 Million in Coins Was Stolen,* CNBC (June 19, 2018, 10:46 PM), https://www.cnbc.com/2018/06/19/south-korea-crypto-exchange-bithumb-says-it-was-hacked-coins-stolen.html.

cryptocurrency more generally. Part IV then tests the claims that Bitcoin eliminates the need for trust against real world experiences of Bitcoin holders and markets. This section disaggregates the blockchain technology itself from how actual people typically use Bitcoin or any of the follow-on cryptocurrencies. It documents the many points at which cryptocurrencies shifts the locus of embedded trust, rather than eliminating the need for such trust. Finally, Part V concludes that rather than replacing trust, cryptocurrencies instead require users to repose their trust in less transparent, less reliable and less accountable parties. The ultimate message is that *caveat emptor* should be a consumer watchword, and that users should understand that many legal protections they take for granted may not apply when purchasing cryptocurrency.

II. BEFORE CRYPTOCURRENCY: THE FIAT MONEY SYSTEM

The back of all United States currency carries the motto "In God We Trust." Yet people using that money often pay little attention to the many levels of earthly trust embedded in that currency. Money played a critical role in the rise of a division of labor, and the move from a subsistence to a market economy. The need for a "double coincidence of wants"[35] challenged the scope of barter systems, giving rise to the need for a more flexible unit of exchange.[36] At first salt, metals (like gold or silver), or wampum filled this need—serving as a store of value and a unit of exchange.[37] But the dangers and logistics associated with storage and transportation presented thorny problems that limited the utility of these items.[38] Traders shifted to receipts that could be exchanged as representatives of the underlying commodities.

The modern monetary system is dominated by fiat currencies regulated by national governments. Modern money is called "fiat money" because it has no intrinsic value. It is, instead, established by governmental decree—or fiat—and backed by the full faith and credit of that government. Until 1933, money issued by the United States was not fiat money, but was instead representative money, meaning that it was representative of a comparable amount of gold. The back of each such dollar read "this note is legal tender for all debts, public and private, and is redeemable in lawful money at the

35. Mike Moffatt, *The Double Coincidence of Wants*, THOUGHTCO. (Feb. 22, 2018), https://www.thoughtco.com/the-double-coincidence-of-wants-defintion-1147998.

36. *Id.*

37. *See generally* A. HINGSTON QUIGGIN, A SURVEY OF PRIMITIVE MONEY: THE BEGINNINGS OF CURRENCY (1947); JACK WEATHERFORD, A HISTORY OF MONEY 20-35 (2009).

38. WEATHERFORD, *supra* note 37, at 20-25.

United States Treasury or at any Federal Reserve Bank."[39] On June 5, 1933, President Roosevelt signed House Joint Resolution 192, the so-called "Gold Repeal Resolution" into law.[40] This Joint Resolution declared that obligations purporting to give the right to require payment in gold were against public policy.[41] The Resolution then went on to announce that any such debts would now be payable in "any coin or currency which at the time is legal tender for public and private debts."[42] By fiat, the United States changed the terms by which currency issued by the United States was held.[43]

To be considered money, a currency must fulfill three roles: it must serve as a store for value, be a unit of account, and function as a medium of exchange. Despite the changes wrought by the Gold Repeal Resolution, United States currency still fulfilled all three criteria. Comparing the fiat money, printed by the United States government, with Monopoly money, printed by the Parker Brothers[44], can help clarify how fiat money works. While the United States $100 bill is fancier than the Monopoly $100 bill (and has Benjamin Franklin on its front), the real difference has to do with its relationship to the government. You can pay your bills with the Benjamin Franklin $100 and not the Monopoly money because the United States government has, by fiat, declared its money to be "legal tender for all debts, public and private."[45] One of the Federal Reserve banks issues the currency, and a network of banks handle the transactions. The Benjamin Franklin $100 is not backed by gold, but by its power to purchase goods or services in the economy.[46] By contrast, the Monopoly money has value in the game, but nowhere else.

Law is the tool that government uses to regulate, and thus legitimate, a fiat currency. As one commenter noted, "[v]aults filled with gold have been

---

39. Lawful money in this context referred to gold. *See* Board of Governors of the Federal Reserve System, *FAQ: What Is Lawful Money? How Is It Different from Legal Tender?* https://www.federalreserve.gov/faqs/money_15197.htm (last updated Sept. 29, 2011). It was President Grant who put the country on a gold standard when he signed the Coinage Act of 1873, which ended gold/silver bimetallism in the United States and demonetizing silver. *See* Office of Corporate Communications, *U.S. Mint History: The "Crime of 1873*," U.S. MINT (Mar. 22, 2017), https://www.usmint.gov/news/inside-the-mint/mint-history-crime-of-1873.

40. H.R.J. Res. 192, 73d Cong. (1933).

41. *Id.* at § 1(a).

42. *Id.*

43. Subsequently, Congress enacted a law that prohibited the government from paying out gold, even in response to a gold clause in a public debt obligation. *See* Gold Clause and Consent to Sue, 31 U.S.C § 5118(b) (1997).

44. I am indebted to N. Gregory Mankiw for this example. *See* N. GREGORY MANKIW, BRIEF PRINCIPLES OF MACROECONOMICS 222 (2014).

45. This language, which is reproduced on all U.S. bills, comes from the Coinage Act of 1965, 31 U.S.C. § 5103, entitled "Legal tender," which states: "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues."

46. *See e.g.*, Stephanie Bell, *The Role of the State and the Hierarchy of Money,* 25 CAMBRIDGE J. ECON. 149, 153-57 (2001).

replaced by law and trust."[47] There is no question that trust in the law is an indispensable attribute of modern monetary systems. For example, a business willing to accept a check as payment for service does so in the context of fraud protection in the banking system, and the law of negotiable instruments. This remains true even though it is highly likely that the business representative does not consciously consider the soundness of the banking system or the Uniform Commercial Code when making this decision. Thus, an invisible edifice of law generates the trust that makes the individual transaction possible.[48] Without trust in the banking system, such transactions become extremely risky. The Federal Reserve Banks are tasked with maintaining the stability of the money supply in order to cultivate this trust.

Without trust in the legitimacy of a currency as a holder of value and a medium of exchange, a state's social institutions can disintegrate.[49] Indeed, collapse of trust in the monetary system is generally considered a sign of a social system under severe strain.[50] This was the situation after Lehman Brothers, Bear Stearns, and AIG imploded, and other major "too big to fail" banks needed a federal bailout.

During the depth of the resulting financial crisis, Satoshi Nokamoto wrote the Bitcoin White Paper.[51] He asserted that "[t]he root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."[52] Echoing this lament, cryptocurrency supporters like to claim that "the problem with regular fiat currency is that governments can print as much of it as they like, and they frequently do."[53] Unlike fiat currency, Nokamoto's Bitcoin is finite—the Bitcoin protocol was designed so that only 21 million Bitcoins can ever be

47. Markus Iofcea et al., *The Future of Currencies*, FORBES (Oct. 28, 2016, 10:08 AM), https://www.forbes.com/sites/ubs/2016/10/28/the-future-of-currencies/#551c41a623ef.

48. See Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 556 (2001) for a discussion advocating that "law cannot produce trust." Conversely, see Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. REV. 457, 459 (2001), for a discussion arguing that trust requires law.

49. The link between monetary instability, rampant inflation, and social unrest has long been recognized. See, for example, *The Political Cost of Inflation*, ECONOMIST (Apr. 4, 2008), https://www.economist.com/news/2008/04/04/the-political-cost-of-inflation.

50. See, for example, Matthew Boesler, *WEIMAR: The Truth About History's Most Infamous Hyperinflation Horror Story*, BUS. INSIDER (Sept. 20, 2013), https://www.businessinsider.com/weimar-germany-hyperinflation-explained-2013-9.

51. Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUNDATION (Feb. 11, 2009, 10:27 PM), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

52. *Id.*

53. *See Why Use Bitcoin?*, *supra* note 20.

created. Many cryptocurrency aficionados liken this fixed supply limitation to reinstating the gold standard, this time without banks or governments.[54]

There is no question that the 2008 financial crisis badly damaged trust in banks, and in the governmental regulators who oversee them.[55] Things have gotten worse. Since the Trump administration began, the United States has experienced the steepest decline of trust ever measured.[56] And, the more informed a member of the public is, the more his/her trust in this administration's handling of the United States government has plummeted.[57] Indeed, among the informed public, the United States has crashed from sixth place to dead last on the Edelman Trust Barometer, a global trust index that ranks 28 countries.[58] In comparison with the rest of the world, the United States has experienced a staggering and extreme loss of trust over a very short period of time.[59] While this recent decline in trust has been both steep and profound,[60] it is part of a larger trend. Over the past few decades, ever larger percentages of the United States population express a belief that the government is run for the benefit of a few big interests, rather than for the benefit of all.[61]

Many thinkers have emphasized the importance of trust for governance. For example, Sissela Bok argued that social trust is essential for an ethically grounded society.[62] Niklas Luhmann asserted that to trust is to organize

---

54. Fuathan, *Bitcoin as a Gold Standard*, BITCOIN FORUM (Jan. 10, 2016, 06:33 PM), https://bitcointalk.org/index.php?topic=1322343.0; Wences Cesares, *Bitcoin: The New Gold Standard*, YOUTUBE (Mar. 6, 2015), https://www.youtube.com/watch?v=yPIvqJsCOSo.

55. David Leonhardt, *Lesson from a Crisis: When Trust Vanishes, Worry*, N.Y. TIMES (Sept. 30, 2008), https://www.nytimes.com/2008/10/01/business/economy/01leonhardt.html; Sarah Knapton, *Financial Crisis: Home Safe Sales Soar as Trust in Banks Collapses*, TELEGRAPH (Oct. 9, 2008, 9:19 AM), http://www.telegraph.co.uk/finance/personalfinance/savings/3163645/Financial-crisis-Home-safe-sales-soar-as-trust-in-bankscollapses.html.

56. *2018 Edelman Trust Barometer*, EDELMAN INTELLIGENCE, 6 (Jan. 2018), https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf (reporting a decline of 9% in trust in the United States—by far the greatest decrease in the world).

57. *Id.* at 7 (reporting a 23% decline of the informed public's trust in the United States).

58. *Id.* at 11 (tallying responses to a question that asked: "Below is a list of institutions. For each one, please indicate how much you trust that institution to do what is right using a nine-point scale, where one means that you 'do not trust them at all' and nine means that you 'trust them a great deal.'").

59. *Id.* at 9 (reporting an aggregate loss of trust in the U.S. at 37%).

60. *Id.*

61. *The ANES Guide to Public Opinion and Electoral Behavior*, AM. NAT'L ELECTION STUDIES, http://anesold.isr.umich.edu/nesguide/text/tab5a_2.txt (last updated Nov. 11, 2015) (tallying responses to the question: "Would you say that the government is pretty much run by a few big interests looking out for themselves or that it is run for the benefit of all the people?").

62. SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 26-27 (1978).

one's world.[63] The growing lack of trust in the United States raises profound questions about the legitimacy of government decisions.[64] This crisis of trust poses special problems for currency markets. After all, the very idea of money as a unit of exchange is a social construct that relies on trust; fiat paper currency even more so. It works only because "everyone collectively agrees to participate in the fantasy that a dollar bill is worth a dollar, whatever that is."[65] As long as people believe in it, a currency will have value. A crisis in trust in the government or the banks can create a currency crisis.

All the conditions for such a crisis seem to be in place. Trust in the United States government has plummeted. At the same time, the financial sector is the least trusted sector of the global economy,[66] while technology is the most trusted sector.[67] In this context, it is perhaps not surprising to see the rise of cryptocurrency, which rejects the relationship between currency, government and trust, and seeks to replace the roles filled by both governments and trust with technology.[68] Indeed, cryptocurrency bull Tom Lee of Fundstrat Global Advisors explicitly ties falling trust in government to the growth of cryptocurrency.[69]

Even without cratering levels of trust, the rise of the internet, and the growth of digital transactions has challenged fiat currencies. Electronic payments, which typically exchange digital credits at blinding speed, have become the norm. For example, Visa processes an average of 150 million transactions each day, more than 24,000 per minute.[70] Mastercard claims to

---

63. *See* NIKLAS LUHMANN, TRUST AND POWER (1979). Similarly, Russell Hardin calls trust "a way of dealing with the risks inherent in complexity." Russell Hardin, *The Street-Level Epistemology of Trust*, 21 POL. & SOC'Y 505, 516 (1993).

64. For a theoretical exploration of this topic, *see generally* HAROLD D. LASSWELL & MYRES S. MCDOUGAL, JURISPRUDENCE FOR A FREE SOCIETY (1992); *see also*, Rebecca Bratspies, *Regulatory Trust*, 51 ARIZONA L. REV. 575, 580-82 (2009).

65. Lisa Wade, *Money is a Social Construct*, THE SOCIETY PAGES (Apr. 24, 2014), https://thesocietypages.org/socimages/2014/04/24/money-as-a-social-construction/.

66. *2018 Edelman Trust Barometer*, *supra* note 56 at 32, Sector and Home Country Provide Context for Business Leadership.

67. *Id.*

68. For a discussion of trust in the context of markets, see Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin and the Blockchain*, 17 NEVADA L. J. 139, 172-75 (2016).

69. Upfront Ventures, *Thomas Lee Presents The Economics of Cryptocurrenices*, YOUTUBE, (Feb. 21, 2018), https://www.youtube.com/watch?v=GGberGnxiJk&feature=youtu.be.

70. *Visa Acceptance for Retailers*, VISA, https://usa.visa.com/run-your-business/small-business-tools/retail.html (last visited Oct. 28, 2018) (citing 2010 testing). That works out to roughly 1667 transactions per second. However, Visa claims to be able to handle many more transactions—up to 56,000 transactions per second. Jan Vermulen, *VisaNet—Handling 100,000 Transactions Per Minute*, MYBROADBAND (Dec. 17, 2016), https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html.

be able to handle 65,000 transactions per minute.[71] Both payment networks achieve these processing speeds while navigating more than 150 currencies in more than 200 countries.[72] Handling these digital transactions is big business. In 2016 alone, global credit card issuers (Visa, Mastercard, American Express, DinersClub/Discover and JCB) handled purchases valued at $20.60 trillion.[73] The credit card companies serve as the trusted ledger-keeper to log these transactions. Their role is critical for ensuring that individuals do not "double-spend" digital credits by copying the information and sending it to two creditors at once, or by sending the copy to a creditor while retaining the original to use again in another transaction.[74]

By virtue of this role, the ledger keepers are privy to sensitive information about anyone using a credit card, a bank transfer, or a mobile payment system. This information, along with their gatekeeping function gives these companies tremendous power over consumers and allows them to dominate key points of the digital economy. Recently, a series of high profile hacks have soured the public on many formerly-trusted intermediaries.[75] Companies ranging from LinkedIn, to Target, to Experian have all reported massive data breaches that revealed private information from millions of people.[76] There is a growing perception that traditional data management practices have created an "architecture of vulnerability" that does not suffi-

---

71. Nikhal Subba, *MasterCard's Profits Beat Estimates as Card Spending Rises*, REUTERS (May 2, 2017), https://www.reuters.com/article/us-mastercard-results/mastercards-profit-beats-estimates-as-card-spending-rises-idUSKBN17Y1BQ.

72. MASTERCARD, ANNUAL REPORT 2016, 36 (2016), http://s2.q4cdn.com/242125233/files/doc_financials/supplemental/2016/Mastercard-2016-Annual-Report.pdf; VISA, ANNUAL REPORT 2017, 5 (2017), https://s1.q4cdn.com/050606653/files/doc_financials/annual/2017/Visa-2017-Annual-Report.pdf.

73. *Issue 1124*, THE NILSON REPORT (The Nilson Report), Jan. 2018, https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1124. This is just a small sliver of global commercial activity—Mastercard estimates that 85% of retail transactions involve cash currency or checks. MASTERCARD, *supra* note 72, at 12.

74. The role of the trusted intermediary, like Visa or Mastercard, is to keep track of the digital credits exchanged across multiple transactions in order to prevent this kind of double-spending. Physical money by and large does not share this problem. The parties to a transaction physically transfer the asset between themselves. While counterfeiting remains a possibility, it is difficult to replicate physical currency, and the parties can verify the bona fides of the currency before or immediately after the exchange. The big innovation of cryptocurrency is its proposal to replace the role of the trusted intermediary with cryptographic puzzles.

75. *See e.g.*, Selena Larson, *The Hacks that Left Us Exposed in 2017*, CNN (Dec. 20, 2017), http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html; Lily Hay Newman, *The Biggest Cybersecurity Disasters of 2017 So Far*, WIRED (July 1, 2017), https://www.wired.com/story/2017-biggest-hacks-so-far/.

76. Rajeev Dhir, *13 Recent Data Breaches, Hacks You Should Know About*, NJ.COM (Feb. 24, 2017), Eric Chabrow,_*Experian Hack Slams T-Mobile Customers*, BANK INFO SECURITY (Oct. 1, 2015), http://www.nj.com/news/index.ssf/2017/02/emails_credit_cards_biggest_data_breaches_affect_nj_residents.html; https://www.bankinfosecurity.com/experian-breach-a-8563.

ciently respect confidentiality.[77] In the United States, and other countries with extreme trust losses, the public clearly feels that business does not do enough to protect consumers, safeguard privacy, and guard information quality.[78]

III. ENTER CRYPTOCURRENCY

What happens when the ledger keepers of fiat currency can no longer be trusted? Supporters see cryptocurrency as the answer. They claim that the immutability and irreversibility of cryptocurrency transactions offers protection from data breaches,[79] and from untoward government meddling.

The key to understanding this claim is the distributed virtual ledger called the blockchain. Every cryptocurrency transaction is encrypted and recorded in the blockchain, and anyone can see that ledger. [80] Computers serve as a series interconnected "nodes" that maintain and verify the blockchain consensus record of transactions. The blockchain thus provides a publicly accessible system for participants to agree on a single history of transactions.[81] Because all full nodes in the network have a record of the complete blockchain, they all "have access to a shared, single source of truth."[82] The nodes can work together but do not need to trust each other. For cryptocurrency's most ardent supporters, the notion that "code is law,"[83] along with the purported immutability of the blockchain, replaces the need for trust.

The blockchain grows from the interaction between users, miners and nodes. Users contribute transactions by broadcasting them to nodes. To create a block to add to the Bitcoin blockchain, miners compete to solve a cryptographic puzzle, called a proof of work, in order to collect a reward in bitcoins.[84] The proof of work involves encrypting new transaction requests,

---

77. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L. J. 1227 (2003).

78. *2018 Edelman Trust Barometer*, *supra* note 56, at 33.

79. See Jonathan Keane, *Blockchain ID Schemes Could Kill the Data Breach, but How Soon?*, COINDESK (Nov. 11, 2017), https://www.coindesk.com/blockchain-id-schemes-could-kill-the-data-breach-but-how-soon/.

80. JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 4 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf.

81. NAKAMOTO, *supra* note 17, at 2.

82. Benjamin Quinlan & Yvette Kwan, *From KYC To KYT*, QUINLAN & ASSOCIATES, 24 (Nov. 2016), https://www.quinlanandassociates.com/wp-content/uploads/2018/03/Quinlan-Associates-From-KYC-to-KYT-new.pdf.

83. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999); Arvicco, *Code is Law and the Quest for Justice,* ETHEREUM CLASSIC BLOG (Sept. 8, 2016), https://ethereumclassic.github.io/blog/2016-09-09-code-is-law/.

84. *See* Georgios Konstantopoulos, *Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake*, MEDIUM (Dec. 8, 2017), https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-

along with information about the preceding block in the form of a 16-digit number called a "hash" that must be no greater than a target value (typically identified as starting by a certain number of zeros).[85] The block's hash serves as a digital fingerprint for the encrypted data, and a means to verify that the data has not been altered. That means that once a block is created, it can only be changed by redoing the entire calculation. And, as new, later blocks are chained to it, anyone seeking to alter a particular block, say to remove an included transaction, would also have to redo all the subsequent blocks. Thus, as blocks are added to the chain, the probability that anyone would succeed in redoing the work and altering the content of a transaction becomes very low. If there is a dispute, the longest chain, which represents the greatest proof-of-work effort invested, will be considered the valid chain, representing the "true" state of the world vis-à-vis past cryptocurrency transactions, and thus current ownership of the coins.[86]

Miners participate in this system in order to earn the reward for successfully adding a block to the blockchain. A new block is added to the Bitcoin blockchain roughly every 10 minutes. Currently the reward is 12.5 bitcoin per new block added. This reward creates an incentive for miners to spend their time and effort competing to complete each hash. The larger and more dispersed a cryptocurrency network's miner base is, the more secure it is. Thus, cryptocurrency holders want as many miners as possible competing to mine a block; more miners make the blockchain more decentralized and more secure. The block reward is intended to create an incentive for miners to add hash power to the network in order to increase their chances of winning the race to complete the puzzle and claim the reward.[87] This winner-takes-all approach to mining creates something akin to a digital arms race, with miners buying ever-more powerful and specialized equipment to increase their hash power, and thus their likelihood of obtaining the reward. A side effect of this arms race is a pressure on miners to centralize into mining

---

b6ae907c7edb. The reward for successfully generating a block is fixed by the system itself and divides in half after every 210,000 blocks. The reward is currently 12.5 coins per block. This reward will halve by approximately May 2020. *See* BITCOIN BLOCK REWARD HALVING COUNTDOWN, http://www.bitcoinblockhalf.com/ (last visited Nov. 23, 2018). Proof of work is not the only blockchain verification model, but for simplicity, this article will focus on proof of work verification.

85. A sample proof of work for the phrase "Hello World!," with an explanation of how such a hash is generated, can be found at *Proof of Work*, BITCOIN WIKI (last edited May 15, 2016), https://en.bitcoin.it/wiki/Proof_of_work. An excellent explanation can be found at antonylewis2015, *A Gentle Introduction to the Immutability of Blockchains*, BITS ON BLOCKS (Feb. 29, 2016), https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/. A more detailed, technical analysis is available from Campell R. Harvey, *Cryptofinance* (Jan. 14, 2016), https://ssrn.com/abstract=2438299.

86. *See generally*, NAKAMOTO, *supra* note 17.

87. For a good explanation accessible to users, see Ittay Eyal & Emin Gün Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, COMM. ACM, July 2018, at 95.

pools, which share hash power in exchange for a portion of the reward for a successfully mined block.

As a result of the distributed, and allegedly immutable nature of the blockchain, users purportedly "need trust no one when using it."[88] Indeed, cryptocurrency advocates have taken to heart the observation that Zbigniew Brzezinski, President Carter's National Security Advisor, reputedly made when asked before the 1985 arms talks in Geneva whether it made sense to trust the Russians. He replied that the point was "not to trust them" but "to find an agreement that is self-reinforcing."[89] The blockchain, and the ecosystem built around it, purports to provide that self-reinforcing legitimacy. Supporters make sweeping claims for the blockchain, suggesting that the technology will have "massive and cascading implications to the fundamentals of contract, public records of transaction, securities regulation and digital identity."[90]

A. *Cryptocurrency in the Marketplace*

Bitcoin was the first entrant into a field that has become known as cryptocurrency. As such, it is frequently touted as "the world's first completely decentralized currency."[91] Satoshi Nakamoto mined the first bitcoins, known as the genesis block in January 2009. It is no coincidence that cryptocurrency's meteoric rise began during the Great Recession—the largest global economic crisis since the Great Depression. Indeed, Bitcoin's genesis block underscored a profound disaffection with financial markets and regulators. Encoded in this very first Bitcoin block was the dire message "Chancellor on brink of second bailout of banks."[92] Bitcoin began as an oddity—a small niche product among tech geeks,[93] drug dealers,[94] and Hayek enthusi-

88. *See Why Use Bitcoin?*, *supra* note 20.

89. Geoffrey Hawthorne, *Three Ironies in Trust*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 111, 115 (Diego Gambetta ed., 1988).

90. Ed Sohn, *alt.Legal: Amy Wan is Making the Blockchain a Safer Place for Contracts*, ABOVE THE LAW (Jan. 19, 2018, 4:01 PM), https://abovethelaw.com/2018/01/alt-legal-amy-wan-is-making-the-blockchain-a-safer-place-for-contracts/.

91. JERRY BRITO & ANDREA CASTILLO, *supra* note 3, at 1, 47-48.

92. Joshua Davis, *The Crypto-Currency*, NEW YORKER (Oct. 10, 2011), https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency. Indeed, the essay by Satoshi Nakamoto bemoaned, "The central bank must be trusted not to debase the currency, but the fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve." *See* Nakamoto, *supra* note 51.

93. A Forbes headline labeled those who profited most from cryptocurrency as "freaks, geeks, and visionaries." Jeff Kauflin, *Forbes' First List of Cryptocurrency's Richest: Meet the Freaks, Geeks and Visionaries Minting Billions from Bitcoin Mania,* FORBES (Feb. 28, 2018), https://www.forbes.com/sites/jeffkauflin/2018/02/07/cryptocurrency-richest-people-crypto-bitcoin-ether-xrp/#163d15cf72d3. Crypto enthusiasts embrace a mantle of geekdom. For example, one group on the discord server Cryptoland dot tech, describes itself as "a bunch of blockchain hands-on tech geeks." Somewhat incongruously, this group's

asts.[95] Since then, cryptocurrency has gone mainstream. There are currently over 1500 different cryptocurrencies,[96] ten of which currently have market capitalizations above $1 billion.[97] New coins are launched almost daily. That said, the three largest cryptocurrencies, Bitcoin, Etherium, and Ripple, account for approximately 2/3 of the overall market,[98] with Bitcoin alone amounting to 40% of the cryptocurrency market currently.[99]

---

self-proclaimed mission is "to become a trustmark within blockchain ecosystem." CRYPTOLAND DOT TECH, https://cryptoland.tech/ (last visited Nov. 23, 2018).

94. Even as they have become more respectable, cryptocurrencies have not entirely shed their connections with crime. *See The U.S. Marshalls are Auctioning off $52 Million in Bitcoin Seized from Drug Dealers*, FORTUNE (Jan. 11, 2018), http://fortune.com/2018/01/11/bitcoin-drug-dealer-auction/; Rebecca Camber & Chris Greenwood, *Drug Dealers Use Bitcoin Cashpoints to Launder Money*, DAILY MAIL (Dec. 3, 2017), http://www.dailymail.co.uk/news/article-5142033/Drug-dealers-using-bitcoin-cashpoints-launder-money.html; Darryn Pollock, *Bitcoin at Center of Dark Web Drug Dealing Case in Holland*, COIN TELEGRAPH (Oct. 26, 2017), https://cointelegraph.com/news/bitcoin-in-center-of-dark-web-drug-dealing-case-in-holland; Joshua Althauser, *Why Cryptocurrencies are Increasingly Becoming A Favorite Among Criminals*, COIN TELEGRAPH (Oct. 5, 2017), https://cointelegraph.com/news/why-are-cryptocurrencies-increasingly-becoming-a-favorite-among-criminals; Andy Greenberg, *Monero, the Drug Dealer's Cryptocurrency of Choice, is on Fire*, WIRED (Jan. 25, 2017), https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/; *see also* Sanjana Varghese, *The Bitcoin Boom is a Surprise Windfall for Druggies*, THE NEW STATESMAN (Dec. 12, 2017) https://www.newstatesman.com/science-tech/future-proof/2017/12/bitcoin-boom-surprise-windfall-druggies.

95. According to the European Central Bank, the theoretical foundations for Bitcoin lie in the "Austrian School of economics and its criticism of the current fiat money system" specifically government and central bank monetary interventions into the economy, which the Austrian economists believe exacerbates inflation. EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES 22 (2012). For a description of these views, *see* FREDERICK A. HAYEK, DENATIONALIZATION OF MONEY (1976) (arguing for an end to the government monopoly over currency); *see also* Ferdinando M. Ametrano, *Hayek Money: The Cryptocurrency Price Stability Solution* (Aug. 13, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270.

96. The analysis offered in this article applies to bitcoin specifically. Much of the analysis also applies to other cryptocurrencies, but each coin has its own characteristics, which may make some of the points raised inapplicable.

97. *All Cryptocurrencies*, COINMARKETCAP, https://coinmarketcap.com/all/views/all/ (last visited Nov. 23, 2018). In March 2017, there were 1500 cryptocurrencies, twenty-five of which had market capitalizations above $1 billion. These statistics had to be continually revised downward during the writing and editing of this article to reflect the plummeting value of cryptocurrencies as a whole, and Bitcoin in particular.

98. Cryptocurrencies are extremely volatile. Cryptocurrency's total market capitalization peaked in January 2018 at over $825 billion. Andrew Marshall, *Combined Crypto Market Capitalization Races Past $800 Bln*, COINTELEGRAPH (Jan. 7, 2018), https://cointelegraph.com/news/combined-crypto-market-capitalization-races-past-800-bln. One month later, cryptocurrency's total market capitalization had fallen to $303 billion, *Total Market Capitalization*, COINMARKETCAP https://coinmarketcap.com/charts/ (last visited Dec. 18, 2018), and on August 14, it briefly dipped below $190 billion. Stan Higgins, *Below $200 Billion: Crypto Market Sinks to New 2018 Low*, COINDESK (Aug. 14, 2018), https://www.coindesk.com/below-200-billion-crypto-market-sinks-to-new-2018-low/.

99. Valued at roughly $180 billion on February 27, 2018, and $101 billion at the end of June. *Bitcoin Charts*, COINMARKETCAP, https://coinmarketcap.com/currencies/bitcoin/ (last

The first known commercial use of Bitcoin has become the stuff of legends. In 2010, a programmer and early Bitcoin miner offered 10,000 Bitcoins to anyone who would bring him two Papa John's pizzas.[100] The programmer, who valued those bitcoins at 0.003 cents apiece, thought buying two pizzas with $30 of found money was "cool."[101] By January 2013, that Bitcoin had an ascribed value of $13 per coin,[102] which translated into a per pizza purchase price of $65,000. By October of that year, Bitcoin was valued at $1000, or $5 million for each pizza. Since then, Bitcoin's value has gyrated wildly upwards, most recently rising to a peak of $19,783.06 on December 17, 2017.[103] At its peak, Bitcoin had an overall market valuation of over $300 billion (for perspective, that figure is equivalent to Bank of America's market capitalization in December 2017).[104] At that peak valuation, the Bitcoin paid for each pizza was worth nearly $99 million. The party was short-lived. Bitcoin ended 2017 at $14,290, down more than $5000 from its high of a few weeks earlier, but it still gained 1400% over the course of the year.[105]

---

visited Nov. 23, 2018). In February 2017, by contrast, Bitcoin had about 85% market share of the cryptocurrency sector. *Bitcoin Transaction Volume is Puzzling Investors*, FORTUNE (Mar. 2, 2018), http://fortune.com/2018/03/02/bitcoin-price-transaction-volume/.

100. Julie Bort, *May 22 is Bitcoin Pizza Day Thanks to these Two Pizzas Worth $5 Million*, BUS. INSIDER (May 21, 2014), https://www.businessinsider.com/may-22-bitcoin-pizza-day-2014-5. The pizzas were not actually purchased *with* Bitcoin, but were paid to someone who responded to an online posting offering to pay 10,000 bitcoin to anyone who brought the poster pizza. For a list of the companies that currently accept cryptocurrency, see Jonas Chokun, *What Accepts Bitcoins As Payment?*, 99BITCOINS (Sept. 13, 2018), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

101. Nick Bilton, *Disruptions: Betting On a Coin With No Realm*, N.Y. TIMES (Dec. 22, 2013), https://bits.blogs.nytimes.com/2013/12/22/disruptions-betting-on-bitcoin/.

102. *Bitcoin, The Nationless Electronic Cash Beloved by Hackers, Bursts into Financial Mainstream*, FOX NEWS (Apr. 11, 2013), http://www.foxnews.com/tech/2013/04/11/bitcoin-electronic-cash-beloved-by-hackers.html.

103. David Z. Morris, *Bitcoin Hits a New Record High But Stops Short of $20,000*, FORTUNE (Dec. 17, 2017), http://fortune.com/2017/12/17/bitcoin-record-high-short-of-20000/.

104. *Bank of America Corporation Market Cap*, YCHARTS, https://ycharts.com/companies/BAC/market_cap (last visited Nov. 23, 2018).

105. Adam Shell, *Bitcoin Price: Digital Currency Had Big Swings in 2017*, USA TODAY (Dec. 29, 2017), https://www.usatoday.com/story/money/2017/12/29/bitcoin-price-digital-currency-had-big-swings-2017/988544001/; Barbara Kollmeyer, *Bitcoin Futures Trade Near $20,000 in Debut on World's Biggest Exchange,* MARKETWATCH (Dec. 18, 2017), https://www.marketwatch.com/story/bitcoin-futures-debut-on-worlds-biggest-exchange-at-20000-then-pull-back-2017-12-18. That outsize gain did not even put Bitcoin on the Top 10 list for best cryptocurrency performers of 2017. Joon Ian Wong, *Here are the Top 10 CryptoAssets of 2017 (and Bitcoin's 1,000% Rise Doesn't Even Make the List*, QUARTZ (Jan. 1, 2018), https://qz.com/1169000/ripple-was-the-best-performing-cryptocurrency-of-2017-beating-bitcoin/. Over that same time period, 13 altcoins outpaced Bitcoin, with Ripple, the third-largest cryptocurrency gaining the most at 36,018%, and Ethereum, the second-largest cryptocurrency, gaining 9162%. *Id.*

On February 6, 2018 Bitcoin plummeted to $5920.[106] In the process, the total cryptocurrency market value fell more than $55 billion in ascribed value[107]—roughly the market capitalization of Aetna.[108] Bitcoin spent Spring 2018 bouncing around between $7500 and $10,000,[109] before falling below $6000 in late June.[110] This recent gyration was just one of many wild swings in value for the cryptocurrency. Just a few months earlier, in September of 2017, Bitcoin had experienced a similar wild ride, losing $30 billion in market cap.[111] In late June and early July of 2017, Bitcoin's valuation had plunged 36%.[112] Indeed, one self-described bitcoin bull admits that the currency is "prone to 40% corrections."[113]

Other cryptocurrencies are similarly volatile. The market valuation for cryptocurrencies as a class peaked on January 10, 2018 at $828 billion.[114] At the time, noted crypto-bull Tom Lee, bragged that "if crypto was a nation, . . . it [would be] the 19th largest country market . . . Its bigger than Brazil, and Spain, Ireland, and Greece."[115] He then went on to project that if cryptocurrencies reached his predicted target, they would become the 11th largest market.[116] Instead, just three weeks later, the combined market value of all cryptocurrencies had dropped by more than 50% to just under $360

106. Gertrude Chavez-Dreyfuss, *Bitcoin Bounces Back from Three-Month Low in Volatile Trade*, REUTERS (Feb. 6, 2018), https://www.reuters.com/article/us-markets-bitcoin/bitcoin-bounces-back-from-three-month-low-in-volatile-trade-idUSKBN1FQ0ZK; Evelyn Chang, *Bitcoin Continues To Tumble, Briefly Breaking Below $6000*, CNBC (Feb. 5, 2018), https://www.cnbc.com/2018/02/05/bitcoin-drops-more-than-14-percent-to-below-7000.html.

107. Arjun Kharpal, *Cryptocurrency Market Could Hit $1 Trillion This Year with Bitcoin Surging to $50,000, Experts Say*, CNBC (Feb. 7, 2018), https://www.cnbc.com/2018/02/07/bitcoin-price-could-hit-50000-this-year-experts-say.html.

108. *Aetna Inc Market Cap*, YCHARTS, https://ycharts.com/companies/AET/market_cap (last visited Oct. 28, 2018).

109. *Bitcoin Core (BTC) Price*, BITCOIN.COM, https://charts.bitcoin.com/btc/chart/ price (last visited Oct. 28, 2018).

110. *See* Jason Murdock, *Bitcoin Price: 'More Blood to Come' as Cryptocurrency Crashes Below $6000*, NEWSWEEK (June 29, 2018), https://www.newsweek.com/bitcoin-price-more-blood-come-cryptocurrency-falls-below-6000-1000867.

111. Jeff J. Roberts, *Five Big Bitcoin Crashes: What We Learned*, FORTUNE (Sept. 18, 2017), http://fortune.com/2017/09/18/bitcoin-crash-history/.

112. *Id.*

113. Shell *supra* note 105. For a tour of bitcoin's early wild swings in valuation, see Timothy Lee, *An Illustrated History of Bitcoin Crashes*, FORBES (Apr. 11, 2013), https://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/#6c6062d44039.

114. Vitalik Buterin, *Crypto, Blockchain Space Won't See '1,000-Times Growth' Again*, COINTELEGRAPH (Sept. 9, 2018), https://cointelegraph.com/news/vitalik-buterin-crypto-blockchain-space-wont-see-1-000-times-growth-again. For perspective, that is larger than the GDP of the Netherlands. *See* GDP: All Countries and Economies, THE WORLD BANK, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2016&start=2016&view=bar&year_high_desc=true (last visited Oct. 28, 2018).

115. Bloomberg, *How Fundstrat's Tom Lee Pegs a Value on Bitcoin*, YOUTUBE (Jan. 24, 2018), https://www.youtube.com/watch?v=otf3-x0pKhQ.

116. *Id.*

billion.[117] Six months later, that number had fallen another 35% to $236 billion, and in December 2018 the combined market value dipped to around $100 billion.[118] Ethereum, the second largest cryptocurrency, rose to $1302 in January 2018, before plummeting to $697.86 in early February,[119] $412 by late June,[120] and dropping well below $300 in August 2018.[121] In early September, Ethereum dropped below $200,[122] and as this article goes to print in December 2018, the price hovers around $90.[123] The volatility prompted Ethereum founder Vitalik Buterin to tweet a warning that "cryptocurrencies are still a new and hyper-volatile asset class, and could drop to near zero at any time."[124] Forbes routinely includes an editor's note in its cryptocurrency articles stating "Investing in cryptocoins or tokens is highly speculative and the market is largely unregulated. Anyone considering it should be prepared to lose their entire investment."[125] Nevertheless, cryptocurrency's most avid promoters routinely proclaim a new bull market that will see cryptocurrencies cross $1 trillion in valuation.[126]

IV. LAYERS OF TRUST EMBEDDED IN CRYPTOCURRENCIES

One of the key blockchain buzzwords is "trustless." It is not uncommon for those associated with cryptocurrency to claim that the blockchain replaces trust.[127] For many, the entire point of using a blockchain-based digital currency is to eliminate the need to trust actors with control over one's

117. *See Total Market Capitalization*, *supra* note 98. For perspective, this figure is slightly smaller than the GDP of the United Arab Emirates. *See* GDP: All Countries and Economies, *supra* note 114.

118. *See Total Market Capitalization*, *supra* note 98.

119. Ether/USD Coinbase, CNBC, https://www.cnbc.com/quotes/?symbol=ETH.CB%3D (last visited Feb. 7, 2018).

120. Ethereum Price, COINDESK (June 29, 2018), https://www.coindesk.com/ethereum-price/.

121. Ethereum Price, COINDESK (Aug. 15, 2018), https://www.coindesk.com/ethereum-price/.

122. Nick Chong, *Crypto Markets Continue Lower: ETH Falls Below $200, BTC at $6150*, ETHEREUM WORLD NEWS (Sept. 8, 2018), https://ethereumworldnews.com/crypto-market-lower-eth-200-btc-6150/.

123. Ethereum Price, COINDESK (Dec. 18, 2018), https://www.coindesk.com/ethereum-price/.

124. Vitalik Buterin (@VitalikButerin), TWITTER (Feb. 17, 2018, 7:25 AM), https://twitter.com/VitalikButerin/status/964838207215955969.

125. *See, e.g.*, Jesse Damiani, *Crypto Watch: Bitcoin, Ethereum, and Ripple Prices Continue to Plummet. Is the Bottom in Sight?*, FORBES (June 29, 2018), https://www.forbes.com/sites/jessedamiani/2018/06/29/crypto-watch-bitcoin-ethereum-and-ripple-prices-continue-to-plummet-is-the-bottom-in-sight/#7613270c2e31.

126. Kharpal, *supra* note 107.

127. *See, e.g.*, Nomad Wallet, *Blockchain—Believe in Cryptographic Proof Instead of Trust*, https://digitalnomad.community/believe-in-cryptographic-proof-instead-of-trust/; CRYPTOBITCLUB, https://cryptobitclub.co/.

wealth and how it may be used. More nuanced versions of this claim assert that "Blockchains don't actually eliminate trust. What they do is minimize the amount of trust required from any single actor in the system." [128]

When cryptocurrency advocates say that the blockchain replaces trust, what they really mean is that making a transaction on the blockchain involves shifting the trust that would otherwise repose in a specific trusted intermediary, like a bank, and instead placing that trust in the underlying blockchain system. The parties to such a transaction thus trust the blockchain to do the things that a bank would do in a more conventional transaction: to facilitate the transfer, to ensure sender authenticity, and to vouch for the validity of the currency exchanged. The blockchain purports to do this via cryptography (which validates sender authenticity) and a consensus mechanism which provides a probabilistic guarantee that transactions are valid.[129] As one blockchain expert stated: "when we transact with one another on the blockchain, we are anchoring our trust in the miners. . . ."[130] Because the blockchain assumes the nodes act independently and do not trust each other, each node demands proof that a transaction occurred. The theory is that whatever emerges from that decentralized, multi-directional proof demand can be trusted to be "true."[131]

Despite the extravagant rhetoric about trustless interactions, multiple layers of trust are built into cryptocurrencies.[132] With regard to the blockchain itself, users are 1) trusting developers to build secure software,[133] 2) trusting miners not to collude or attack the blockchain,[134] and 3) trusting the wider cryptocurrency governance process not to approve a malicious hard-fork.[135] With regard to using the currency, users are trusting 1) that markets

128. *See* Preethi Kasireddy, *ELI5: What Do We Mean by "Blockchains are Trustless,"* MEDIUM (Feb. 2, 2018), https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6.

129. *See* Nakamoto, *supra* note 17.

130. Kasireddy, *supra* note 128.

131. *See* Nakamoto, *supra* note 17 at 3 ("If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.").

132. *See* Hashib Qureshi, *Why Bitcoin is Not Trustless*, HACKERNOON (Dec. 18, 2017), https://hackernoon.com/bitcoin-is-not-trustless-350ba0060fc9.

133. For a discussion of bugs that called off the SegWit2x rollout, see Jimmy Song, *SegWit2x Bugs Explained,* BITCOIN TECH TALK (Nov. 20, 2017), https://bitcointechtalk.com/segwit2x-bugs-explained-8e0c286124bc (noting that the bugs could have allowed double-spending).

134. *See* Kwon et al., *Be Selfish and Avoid Dilemmas: Fork-After-Withholding Attacks on Bitcoin*, MORNING PAPER (Dec. 7, 2017), https://blog.acolyer.org/2017/12/07/be-selfish-and-avoid-dilemmas-fork-after-withholding-attacks-on-bitcoin/.

135. *See infra* pp. 33-38. For an in-depth consideration of DAOs as business entities, see generally Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. (forthcoming 2018).

are not being manipulated,[136] 2) that wallets will generate secure keys,[137] and 3) that trading platforms are using best security practices.[138] That is an awful lot of trust for a trustless system. The biggest differences with more conventional markets are that most of this trust is unspoken, and often unrealized by participants, and there is virtually no legal backstop should one or more of these trusts be broken.

A. *Trusting the Blockchain Itself*

The combination of difficulty in replacing a block and the distributed copies of the chain are what prompt claims about the immutability[139] and reliability of the blockchain. However, this scenario also gives rise to a major limiting factor: the blockchain's current inability to scale.[140] Each full node has an individual copy of the entire blockchain. That means that the blockchain as a whole is limited by the processing capacity of each single node. As the blockchain grows, the power needed to run a full node increases dramatically and it can take many hours to process a blockchain transaction. Under ordinary circumstances, confirmation takes 1-2 hours.[141] However, as traffic increases, processing times follow suit. For example, at the height of the December 2017 bitcoin frenzy, processing times rose from an average of 78 minutes to 1188 minutes (nearly 20 hours!).[142] As processing time shot up, fees increased as well. At the peak, average transaction fees topped $55

136. For a description of market manipulation, see J.P. Buntinx, *Who is Spoofy and How is He Manipulating Bitcoin's Price?*, NULLTX (Aug. 7, 2017), https://nulltx.com/who-is-spoofy/.

137. *See* Alex Hern, *Bitcoin App Issues Critical Update After Rare Bug Leads to Total Crypto Breakdown*, GUARDIAN (June 1, 2015), https://www.theguardian.com/technology/2015/jun/01/bitcoin-app-critical-update-bug-crypto-breakdown.

138. *See, e.g.*, Makiko Yamazaki, *Tokyo-based Cryptocurrency Exchange Hacked, Losing $530 million: NHK*, REUTERS (Jan. 26 2018), https://www.reuters.com/article/us-japan-cryptocurrency/tokyo-based-cryptocurrency-exchange-hacked-losing-530-million-nhk-idUSKBN1FF29C; Reuters, *Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong*, FORTUNE (Aug. 3, 2016), http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/; Robert McMillan, *The Inside Story of Mt. Gox Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), https://www.wired.com/2014/03/bitcoin-exchange/.

139. *See, e.g.*, Oscar L. Serrano, *Is the Blockchain Really Immutable?*, BLOCKCHAIN REVOLUTION (July 5, 2017), https://www.bbva.com/en/blockchain-really-immutable/.

140. Preethi Kasireddy, *Blockchains Don't Scale. Not Today, at Least. But There's Hope*, HACKERNOON (Aug. 23, 2017), https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a. The explanation in the rest of this paragraph is loosely based on Kasireddy's article.

141. Alex Lielacher, *How Long Should My Bitcoin Transaction Take?*, BITCOIN MKT. J. (July 6, 2017), https://www.bitcoinmarketjournal.com/how-long-bitcoin-transactions/.

142. Ryan Browne, *Big Transaction Fees are a Problem for Bitcoin - But There Could Be a Solution*, CNBC (Dec. 19, 2017), https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html.

dollars per transaction.[143] Indeed, *Bitcoin Marketing Journal*, the self-proclaimed "most trusted name in new finance," cautions, in bold, that "[t]he higher the fee you include with your transaction, the more likely it will be prioritized by bitcoin network participants, and the sooner it will be processed."[144] The problems got so bad that in January 2018, the North American Bitcoin Conference to refuse to accept cryptocurrency as payment, citing high fees and slow processing times.[145]

Because the system is decentralized, merely adding more nodes, unlike to the go-to solution of adding more servers in a traditional, centralized database, will not shorten processing time. Moreover, electricity demands associated with the Bitcoin blockchain alone has already reached unsustainable levels.[146] It seems clear that cryptocurrency proponents will have to address this complicated question and devise a mechanism that can both limit the number of nodes needed to validate each transaction while simultaneously maintaining the overall network trust that each transaction is valid. For that to happen, nodes will have to trust that blocks they did not validate are nevertheless secure.[147]

While the future of the blockchain will probably have to involve full nodes trusting each other in some fashion, the blockchain in its current state already explicitly incorporates trust in two very important respects. First, many cryptocurrency transactions use a simplified verification system, which

---

143. *Bitcoin Avg. Transaction Fee Historical Chart*, BIT INFO CHARTS (Oct. 27, 2018), https://bitinfocharts.com/comparison/bitcoin-transactionfees.html. Fees have fallen dramatically since then, but still average over $2.00 per transaction. This fee, paid by the transaction participants, is on top of the processing fee that merchants pay to bitcoin payment processers. Those merchant fees are frequently touted as much lower than credit card processing fees.

144. Lielacher, *supra* note 141.

145. Rob Price, *A Major Bitcoin Conference is No Longer Accepting Bitcoin Payments Because the Fees and Lag Have Gotten So Bad*, BUS. INSIDER (Jan. 10, 2018), http://www.businessinsider.com/bitcoin-conference-stops-accepting-bitcoin-network-fees-congestion-2018-1.

146. Bitcoin's energy footprint is already massive and far in excess of its ascribed value. Producing Bitcoin currently consumes more energy on a daily basis than the entire state of New York. *Energy Efficiency of Blockchain and Similar Technologies: Hearing Before the S. Comm. on Energy and Nat. Res.*, 115th Cong. (2018) (statement of Arvind Narayanan, Associate Professor, Princeton University), https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=8A1CECD1-157C-45D4-A1AB-B894E913737D. In 2017, Bitcoin mining consumed 54.2 TWh of energy, as much as the entire country of Bangladesh. *Bitcoin Energy Consumption Index*, DIGICONOMIST (Oct. 22, 2018), https://digiconomist.net/bitcoin-energy-consumption; *see also* Timothy B. Lee, *Bitcoin's Insane Energy Consumption Explained*, ARSTECHNICA (Dec. 6, 2017), https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/.

147. Some speculate that the process will eventually become so unwieldy that it will only be feasible for a few nodes to process a block—at which point, the trust based on decentralized, unanimous consensus will be called into question. Nodes will have to trust that blocks they did not validate. There are multiple proposed solutions to this conundrum that involve various verification methods. *See, e.g.*, Kassireddy, *supra* note 128, for an explanation of some of the possible solutions.

involves trusting full nodes. Second, blockchain users trust that built-in economic games will keep the miners honest.

1. Most Cryptocurrency Users Wind Up Trusting Individual Nodes

When Alice wants to pay Bob with Bitcoin or an altcoin, she broadcasts the transaction to all of the nodes that comprise the peer-to-peer network for the cryptocurrency in question.[148] Those nodes verify the block and the transactions within the block and then relay that block to other nodes. In theory, every node verifies every block by verifying every transaction within that block, before relaying that block to another node.[149] The transaction is considered confirmed when enough new blocks have been added to the chain on top of the particular block encoding that transaction. Because this consensus mechanism creates a single, global ledger, each node will use the identical agreed-upon history as it verifies the validity of any new block or transaction. This decentralized verification against an identical ledger is the source of cryptocurrency's much heralded security against hacking and double-spending. Every bitcoin is identifiable, allowing the payment system to confirm precisely which bitcoins are being sent, and from where, before the transaction is logged in the distributed ledger. Because each coin can only be in one place at a time, this system offers protection from an unscrupulous coin owner trying to game the system by spending the same coin twice. One can think of the blockchain as a decentralized, publicly accessible, virtual paper trail documenting the history of each coin—its past and current ownership and the journey the coin has taken from owner to owner.[150] The idea is that this decentralized process prevents forgery or double-spending, without the need for a trusted third party. As a result, "the majority of the participants on the network get to decide what version of the blockchain represents the truth."[151]

Most cryptocurrency participants do not run a full node (there are only about 10,000 full nodes in existence).[152] Instead, many cryptocurrency holders rely on so-called light nodes (also called light wallets), which use a simplified payment verification system (SPV). These SPV nodes connect with

148. Miners are full nodes, but full nodes need not be miners. Miners can create and propose blocks to the blockchain, but it is full nodes that determine the consensus for which blocks will be added to the blockchain.

149. *See* Danny Hamilton, *Difference Between Miners and Nodes*, BITCOIN FORUM (Dec. 31, 2016), https://bitcointalk.org/index.php?topic=1734235.0.

150. Catherine M. Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin and Blockchain*, 17 NEV. L.J. 139, 144-45 (2016).

151. Jimi S., *Blockchain: How a 51% Attack Works (Double Spend Attack)*, MEDIUM: COINMONKS (May 5, 2018), https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474.

152. *See* Jameson Lopp, *Bitcoin Nodes: How Many is Enough?*, MEDIUM (June 7, 2014), https://medium.com/@lopp/bitcoin-nodes-how-many-is-enough-9b8e8f6fd2cf.

one or more full nodes and ask that a cryptocurrency transaction be included in a block. The SPV wallet then receives confirmation from the full node that the transaction was included in a block, and that the block is part of a chain.[153] The SPV system trusts that a transaction followed by an adequate number of blocks would be too costly to forge. So long as a transaction is included in a block and that block is incorporated into a chain that is subsequently built upon, SPV wallets will accept the transactions as valid without checking further.[154] That means that a light wallet does not actually verify that the transaction was included in the correct chain—the one that is the single, agreed-upon history of all transactions.[155] Instead, the light nodes (and hence its user) trust one or more full nodes to verify transactions for them.[156]

SPV wallets are thus potentially at the mercy of rogue nodes, or even sloppy ones. Indeed, in July 2015, after a Bitcoin system upgrade, this vulnerability resulted in a crisis.[157] Despite a consensus to upgrade to a new process, roughly half the network was mining using the old protocol, which meant they were not fully vetting blocks.[158] Some of these miners produced invalid blocks that were accepted by SPV and old versions of the network software, while being rejected by the updated portion of the network. The invalid blocks showed transaction confirmations that were not real. There were at least three forks, one of which added six blocks before the valid chain reasserted itself.[159] SPV wallets were advised to wait for an additional

153. *See* Bisade Asolo, *Full Node and Lighweight Node*, MYCRYPTOPEDIA (Nov. 1, 2018), https://www.mycryptopedia.com/full-node-lightweight-node/. For a good description of the difference between light nodes and full nodes, see for example, AdminFrog, *What Are Full Nodes and Light Nodes of the Bitcoin BlockChain*, COIN FROG (Jan. 14, 2018), https://coinfrog.io/full-nodes-light-nodes/.

154. Many assert that SPV nodes are just as secure as full nodes. *See, e.g.*, Jonald Fyookball, *Why Every Bitcoin User Should Understand "SPV Security,"* MEDIUM (May 28, 2017), https://medium.com/@jonaldfyookball/why-every-bitcoin-user-should-understand-spv-security-520d1d45e0b9.

155. *See infra* p. 24, 26-27, 29-33. For an explanation of how a chain can be forked into two branches and then pruned, see Eyal & Sirer, *supra* note 87 (describing selfish mining). Transactions included in a pruned block are ignored, but can be resubmitted for processing. In the interim however, the possibility of double-spending arises.

156. Pwuille, Comment to *Full Node Question*, REDDIT (July 29, 2015, 7:24 AM), https://www.reddit.com/r/BitcoinBeginners/comments/3eq3y7/full_node_question/ctk4lnd/ ("SPV nodes . . . place a blind trust in the majority of miners, without checking validity of the blockchain they produce. It still requires a majority of miners to mislead an SPV node, but the can make it believe anything (including "You received 10000000 BTC!")").

157. *See Some Miners Generating Invalid Blocks*, BITCOIN, https://bitcoin.org/en/alert/2015-07-04-spv-mining (last updated July 15, 2018).

158. *See id.* The new rule was called BIP66. It was intended to remove OpenSSL from the consensus code for signature verification. *See generally Bip-0066.mediawiki*, GITHUB, https://github.com/bitcoin/bips/blob/master/bip-0066.mediawiki (last visited Nov. 1, 2018).

159. *See Some Miners Generating Invalid Blocks*, *supra* note 157.

thirty confirmations before assuming that their transactions had been correctly processed.[160]

Notice, this situation did not involve an invidious attack but sloppy execution of a consensus protocol upgrade. It took over an hour before it became clear which blockchain fork was growing longer, and therefore was the more valid chain. Users may have been surprised to discover that the fate of their crypto assets on the trustless blockchain hinged not on the much-touted unhackable cryptography but on software updates vulnerable to usual human error or laziness.

To avoid such a situation, the *Bitcoin Developers Guide* counsels that "block and transaction data should not be relied upon if it comes from a node that apparently isn't using the current consensus rules."[161] It advises SPV clients[162] to connect to several full nodes and ensure they are all "on the same chain with the same block height,[163] plus or minus several blocks to account for transmission delays and stale blocks."[164] It goes on to caution that if there is a divergence, it is up to the SPV clients to disconnect from nodes with weaker chains. Notice the layers of trust built into the transactions—that nodes are using appropriate software, that nodes are validly processing transactions, and that SPV wallets are monitoring the behavior of the full nodes they are trusting.

This vulnerability of light wallets is not a surprise. Satoshi Nakamoto himself noted that SPV verification "is reliable as long as honest nodes control the network, but is more vulnerable by an attacker . . . [t]he simplified method can be fooled by an attacker's fabricated transactions . . ."[165] Bitcoin developer Peter Todd puts it more bluntly, "a full node can lie about a lot of things to an SPV client and they'll be none the wiser."[166] In Todd's own

160. *Id.*

161. *Blockchain Guide*, BITCOIN, https://bitcoin.org/en/developer-guide#detecting-forks (last visited Nov. 2, 2018).

162. SPV stands for "simplified payment verification." It is a method for verifying transactions without downloading the entire blockchain.

163. An alert after the July 2015 fork advised SPV wallet users to wait until 30 blocks have been added to the chain before relying on a transaction confirmation. *Some Miners Generating Invalid Blocks*, *supra* note 157. At an average pace of 10 minutes per block, that would be a wait of 5 hours. *See* Alex Lielacher, *How Long Should My Bitcoin Transaction Take?*, BITCOIN MKT. J. (July 6, 2017), https://www.bitcoinmarketjournal.com/how-long-bitcoin-transactions/. The more usual wait was for six blocks, or an hour wait.

164. *Blockchain Guide*, *supra* note 161.

165. Nakamoto, *supra* note 17, at 5.

166. PeterTodd, Comment to *Bitnodes Recently Updated Their Node Counter Crawling Algorithm - Apparently the Old One Was Off by an Order of Magnitude*, REDDIT (Mar. 15, 2014, 2:30 PM), https://www.reddit.com/r/Bitcoin/comments/20hsql/bitnodes_ecently_updated_their_node_counter/cg3d1qy/?context=3. The Bitcoin wiki makes this point as well. *See Lightweight Node*, BITCOIN WIKI (last edited Jan. 15, 2018), https://en.bitcoin.it/wiki/Lightweight_node.

terms, using a light wallet is "just outsourc[ing] your trust to others."[167] Most of the people buying and selling cryptocurrency probably have no idea of the levels of trust they are placing in nameless, faceless full nodes. After all, they have been repeatedly assured that the blockchain replaces trust.

2. The Blockchain's Integrity Depends on the Honesty of Miners

Blockchains rely heavily on economic games that are intended to incentivize actors to cooperate. When the games work, the integrity of the blockchain is maintained. However, from the genesis block onward, it has been clear that the blockchain is secure only so long as honest miners control more computational power than a group of cooperating attackers.[168] The main caveat to the blockchain's probabilistic guarantee of validity is that it assumes no single miner controls a majority of the network. If a single miner or pool of miners were to control 51% of the nodes, (a so-called 51% attack) the system would cease to be decentralized. At that point, the majority miner could unilaterally control which blocks are added to the blockchain, enabling him/her to double-spend at will. Of course, theoretical vulnerability is not the same as an actual threat in the real world.[169] From time to time, scholars float the concern that a government might engage in a 51% attack in order to "destroy the Bitcoin economy in order to achieve utility outside the Bitcoin economy."[170]

The possibility of a 51% attack used to be considered more theoretical than actual, even though in 2016 there was a 51% attack against a smaller Ethereum chain.[171] Then, in the summer of 2018, at least five cryptocurrencies were subject to 51% attacks within the space of a single month.[172] The compromised currencies included: Zencash, Monacoin, Bitcoin gold, Verge and Litecoin.[173] There is even a website projecting the cost of acquiring the

---

167. PeterTodd, *supra* note 166.

168. Nakamoto, *supra* note 17, at 3.

169. For example, while it is theoretically possible to crack the encryption at the core of the blockchain, that risk is so improbable that it can safely be dismissed. Natalie Fratto, *Commentary: This New Technology Will Crack the Blockchain Like an Egg*, FORTUNE (Jan. 31, 2018), http://fortune.com/2018/01/31/commentary-this-new-technology-will-crack-the-blockchain-like-an-egg/.

170. Joshua A. Kroll et al., *The Economics of Bitcoin Mining or Bitcoin in the Presence of Adversaries* 1, 13 (2013), http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf.

171. *See* Rocky, *51% Crew Extorts and Hijacks Blockchains for Ransom*, CRYPTO HUSTLE (Sept. 3, 2016), https://cryptohustle.com/51-attack-crew-extorts-and-hijacks-blockchains-for-ransom.

172. Alyssa Hertig, *Blockchain's Once Feared 51% Attack is Now Becoming Regular*, COINDESK (June 8, 2018), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/.

173. *Id.*

mining power to enact a 51% attack on various cryptocurrencies.[174] To intentionally attack the Bitcoin blockchain in this fashion would require significant hashing power in order to control a majority of nodes. However, even Bitcoin has come close to this level of consolidation of mining power. In 2014, one mining pool, Ghash.io controlled around 50% of mining on the bitcoin blockchain.[175] In a statement that sounded perilously like "you can trust us," the CIO of the company hastened to assure the bitcoin community that "[w]e would never harm the community."[176] At the time of this writing, four mining pools, BTC.com, Antpool, BTC.Top, and Via.BTC together control roughly 70% of the bitcoin mining network.[177] BTC.com, which alone controls 25% of the network,[178] and Antpool, which controls 16% are both projects of the same China-based company, Bitman.[179] Bitman's founder Jihan Wu was a significant force behind the hard fork that created Bitcoin Cash.[180] The possibility that these nodes could collude to launch a 51% attack certainly exists. Overall, Chinese mining pools dominate bitcoin mining, controlling up to 80% of the network.[181] For a system that depends on decentralization for validity, that seems remarkably centralized.[182]

However, even putting aside the prospect of a 51% attack, there are multiple, profitable ways for miners to game the verification system and undermine the validity of the chain. A few of the best-known techniques are

---

174. *PoW 51% Attack Cost*, CRYPTO51, https://www.crypto51.app/ (last visited Nov. 23, 2018).

175. Roop Gill, *CEX.IO Slow to Respond as Fears of a 51% Attach Spread*, COINDESK (June 13, 2014), https://www.coindesk.com/cex-io-response-fears-of-51-attack-spread/.

176. *Id.*

177. *Hashrate Distribution*, BLOCKCHAIN, https://blockchain.info/pools?timespan=4days (last visited Nov. 23, 2018).

178. *Id.*

179. Jacob Donelly, *One of Bitcoin's Largest Miners Is Launching a Second Pool*, COINDESK (Sept. 14, 2016), https://www.coindesk.com/bitmain-bitcoin-mining-launch-second-mining-pool/. To get a sense of the scale of this operation, Bitman has 25,000 specialized machines continuously mining bitcoin. Joshua Althauser, *Jihan Wu of Bitman Confident that Bitcoin Will Be Valued at $100,000 in Five Years*, COINTELEGRAPH (Aug. 26, 2017), https://cointelegraph.com/news/jihan-wu-of-bitmain-confident-that-bitcoin-will-be-valued-100000-in-5-years.

180. Darryn Pollock, *Bitmans Mining Monopoly Compromises Bitcoin's Decentralized Nature*, COINTELEGRAPH (Aug. 30, 2017), https://cointelegraph.com/news/bitmains-mining-monopoly-compromises-bitcoins-decentralized-nature.

181. This may be changing. In 2018, China has cracked down on cryptocurrency, driving miners elsewhere. For example, Bitman has moved to Inner Mongolia. Rakesh Sharma, *China Intensifies Crackdown on Bitcoin Mining*, INVESTOPIA (Jan. 11, 2018, 5:05 PM), https://www.investopedia.com/news/china-intensifies-crackdown-bitcoin-mining/.

182. In general, Bitcoin holdings are astonishingly consolidated, with 95% of the wealth held by 4% of the owners. *See This Chart Reveals the Centralization of Bitcoin Wealth*, HOW MUCH (Sept. 12, 2017), https://howmuch.net/articles/bitcoin-wealth-distribution. Forbes reports that 94% of Bitcoin wealth is held by men. Jackie Lam, *Where Are the Women on the Blockchain Network?*, FORBES (Dec. 10, 2017), https://www.forbes.com/sites/lamjackie/2017/12/10/where-are-the-women-in-the-blockchain-network/#23ee1a2a530a.

Sybil attacks,[183] Block Withholding and Selfish Mining attacks, 184 and Fork After Withholding attacks.[185] These are maneuvers miners can use either to permit double-spending or to increase their share of the mining rewards at the expense of other miners. All of these attacks involve gaming the consensus mechanism for profit or to inflict harm. Moreover, these attacks can occur singly or in combination with a 51% attack.

These attacks are not merely hypothetical. At least one Block Withholding attack has been documented,[186] and scholars assert that the only defense against this attack is for mining pool managers to work with miners they know personally and trust.[187] Fork after Withholding attacks have been described by scholars as "always profitable" and "difficult to guard against."[188] Selfish Mining had traditionally been considered impractical because it was assumed that it required control of a majority of the network nodes. Howev-

183. Sybil attacks involve copying nodes to give the appearance that there are many different nodes verifying a transaction, when in fact all those pseudo-participants are really controlled by the same actor. Light wallets are particularly vulnerable to Sybil attacks. Moshe Babaioff, et al., *On Bitcoin and Red Balloons*, 10 ACM SIGECOM EXCHANGES 5, 7 (2011), http://www.sigecom.org/exchanges/volume_10/3/BABAIOFF.pdf.

184. Both Block Withholding and selfish mining involve withholding work. A selfish mining attack involves not immediately releasing a block but instead withholding it in an attempt to find a second or third block for the new, secret chain. If the miner does find a second block before the network has found the first, then it can work even farther ahead while the rest of the network pursues the wrong fork. As soon as a new block is found, the withholding miner can release its blocks. As the longer chain, the newly released blocks would immediately become the most valid chain. A miner can use withholding to double-spend or to undermine the validity of a mining pool's payment algorithm. *See* Eyal & Sirer, *supra* note 87 (describing a selfish mining attack); *but see* Nicholas T. Courtois & Lear Bahack, *On Subversive Miner Strategies and Block Withholding Attacks in Bitcoin Digital Currency*, ARXIV:1402.171 1, 6 (Dec. 2, 2014), https://arxiv.org/pdf/1402.1718/ (calling the selfish assumptions into question). *See also* Deepak K. Tosh, et al., *Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack*, IEEE COMPUTER SOC'Y 458, 461-62 (2017), https://www.researchgate.net/publication/317182715_Security_Implications_of_Blockchain_Cloud_with_Analysis_of_Block_Withholding_Attack.

185. A fork after withholding combines a block withholding attack with a selfish mining attack. Yujin Kwon, et al., *Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin*, ARXIV:1708.09790 1 (Aug. 31, 2017), https://arxiv.org/pdf/1708.09790.pdf.

186. The Block Withholding Attack occurred in the Eligius mining pool and reportedly cost the pool 300 Bitcoin. *See* Wizkid057, *Eligius: 0% Fee BTC, 105% PPS NMC, No registration, CPPSRB*, BITCOIN FORUM (June 13, 2014, 02:19:01 AM), https://bitcointalk.org/?topic=441465.msg7282674. The pool's response was to assure mining pool participants that any changes to the payment algorithms required the signatures of both Eligius pool founders, plus a disinterested third party. This announcement sought to leverage trust in the Eligius pool founders into trust in the validity of the mining pool payment algorithm.

187. Courtois & Bahack, *supra* note 184, at IX-A.

188. Kwon, *supra* note 185, at 3. Although this paper modeled the Fork After Withholding attack in bitcoin, the authors assert that other cryptocurrencies including Ethereum and Litecoin are also vulnerable.

er, recent research shows how such an attack could be successful even without controlling 51% of the network.[189]

The lesson from this should be that rhetoric about the trustless blockchain may have been overblown. From the earliest inception of cryptocurrency, it has been clear that the validity of the blockchain depends on there being sufficient honest miners to validate each block. If enough miners cease or reduce their operations, the blockchain becomes vulnerable. For a finite system, this dependence on miners poses a potential problem. Roughly 80% of the Bitcoin that will ever exist have already been mined.[190] Current estimates are that the last Bitcoin will be mined in 2140.[191] What will happen at that date adds uncertainty to Bitcoin.[192] Miners will still be needed to secure the integrity of the blockchain but will no longer obtain prizes for mining blocks. The system assumes (trusts?) that miners will continue to maintain the system to collect transaction fees.[193] Yet, once all the Bitcoin are mined, there will be no block reward. Thus mining will be less lucrative. This is also true on a smaller scale every time the value of Bitcoin falls. Since miners are paid in the cryptocurrency, any lowering of Bitcoin's value makes mining less lucrative, decreasing the incentive to mine. At some point this potentially becomes a death spiral, where the economic incentive for mining is not adequate to keep a sufficiently dispersed mining pool in place.[194]

Finally, it is worth noting that in contrast with cryptocurrency software developers, who tend to be well-known and trusted (that word again) public figures, miners are "an obscure group of anonymous people organized into a handful of pools."[195] Participants place a great deal of trust in nameless, faceless miners, and in the bitcoin incentive system that purports to align miner interests with those engaged in bitcoin transactions. Most cryptocurrency participants do not realize they are trusting miners in this fashion. Instead, they probably accept the oft-repeated assertions that the blockchain

189. Kevin Liao & Jonathan Katz, *Incentivizing Double-Spend Collusion in Bitcoin*, *in* FINANCIAL CRYPTOGRAPHY BITCOIN WORKSHOP (2017), https://www.cs.umd.edu/~gasarch/reupapers/katzbitcoin16.pdf (describing a so-called 'whale' attack that could feasibly permit double-spending on the blockchain).

190. *See* BITCOIN BLOCK REWARD HALVING COUNTDOWN, *supra* note 84.

191. *What Happens When All 21,000,000 Have Been Mined,* CRYPTOCOINMASTERY (Oct. 21, 2017), https://cryptocoinmastery.com/what-happens-when-all-bitcoins-have-been-mined/.

192. Evan Faggart, *What Happens to Bitcoin Miners When All Coins are Mined*, (Aug. 15, 2015), https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/.

193. *See* Comment *How Much Will Transaction Fees Eventually Be*, STACK EXCHANGE (Sept. 11, 2011, 11:02 PM) (detailing the possibilities and vulnerabilities of Bitcoin exchanges), https://bitcoin.stackexchange.com/questions/876/how-much-will-transaction-fees-eventually-be/895#895.

194. Kroll et al., *supra* note 170.

195. Courtois & Bahack, *supra* note 184, at I-A.

cannot be hacked[196] as a proxy for a system that does not place their interests in jeopardy. Thus we see a slew of articles unironically asking questions like "*Why do People Trust Bitcoin*."[197] These articles generally wind up explaining why Bitcoin, and cryptocurrency more generally, is trustworthy. Indeed, one commenter summed it up by saying "bitcoin is trust."[198] For a purportedly trustless technology, this claim is staggering.

B. *Trusting the Collective Governance Process*

At the same time that transactions require trust in the blockchain itself and in miners as a group, maintaining the blockchain system requires an additional kind of trust—trust in the integrity of the collective decision-making process that governs the blockchain. The need for consensus among the validating nodes is touted as the blockchain's insurance of validity.[199] Yet what happens when the consensus protocol is changed? If the changes are popular, the entire community adopts them. The old chain still exists, but all the users have migrated in unison to the new chain.[200] This is the ideal version of a hard fork, and results in adoption of the new protocol without creating a permanent fork in the blockchain.

Where things get tricky is when the new protocol is not unanimously accepted. If the community does not agree on the hard fork update path, it can get "very, very bad."[201] When the interested parties (which include, at a minimum, developers, users, miners, investors) cannot agree on a solution, the outcome can jeopardize trust in the cryptocurrency. Each stakeholder is forced to choose a side of the dispute, and commit to one version of the consensus protocol. This kind of hard fork, called a "contentious hard fork" splits the path of the blockchain—creating two separate chains running parallel to each other. Some nodes mine and verify following the old protocol

196. *See e.g.*, BittBurger, *Can the Blockchain Be Hacked*, BITCOIN FORUM (Dec. 5, 2013, 2:00AM), https://bitcointalk.org/index.php?topic=358039.0. In most cases, virtually nothing is known about who the miners are, even their country of residence is unknown. Moreover, miners have a real incentive to hide—they have realized billions of dollars of profits from mining, some or most of which is hidden from tax authorities.

197. *Why Do People Trust Bitcoin?*, BEST BITCOIN CASINOS, http://bitcoincasino.best/why-do-people-trust-bitcoin/ (last visited Nov. 1, 2018).

198. Tyler Willis, *Bitcoin is Trust*, BIG THINK (Dec. 7, 2013), http://bigthink.com/cue-the-future/bitcoin-is-trust.

199. SIGRID SEIBOLD & GEORGE SAMMAN, CONSENSUS: IMMUTABLE AGREEMENT ON THE BLOCKCHAIN 3 (KPMG ed., 2016), https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf.

200. Hard forks change block acceptance rules in a fashion that make previously invalid blocks valid. Users relying on older versions of the protocol will not accept the new blocks. As a result, users of the old protocol will remain on their own blockchain indefinitely.

201. Tanzeel Akhtar, *Understanding the Upcoming Ethereum Hard Fork*, THESTREET (Oct. 6, 2017), https://www.thestreet.com/story/14334000/1/understanding-the-upcoming-ethereum-hard-fork.html (quoting Cyrus Younessi, the Digital Currencies Investment Analyst at Cumberland Mining in Chicago).

and other nodes follow the new protocol. This situation creates permanently divergent chains—resulting in two distinct longest chains, both of which are considered valid by part of the network. Because the chains follow different validation rules, they are incompatible with each other. With no way to determine which chain was "valid" there would no longer be a shared, unambiguous blockchain history that represents something users agree on as the "truth." Users cannot send funds from one chain to the other because each chain uses a different, incompatible protocol.[202]

Experience on the Bitcoin blockchain underscores just how polarizing a contested hard fork can be, and highlights the role that trust plays in cryptocurrency more generally. In August 2017, the Bitcoin blockchain underwent the contentious hard fork that created Bitcoin Cash over a disagreement about how to handle congestion on the blockchain. A contentious fork is bad enough, but in this case, the circumstances surrounding the fork were rife with allegations of self-dealing and bad faith. As one commenter noted, the conflict "erode[d] trust within the community."[203] The commenter then went on to caution participants, seemingly without irony, that "[p]arties that don't trust each other have a difficult time compromising and meeting possible future challenges."[204]

The Bitcoin hard fork had its roots in the protocol's size limit of 1 MB per block. As Bitcoin gained popularity, users poured into the system. The size limit, combined with the decentralized nature of the network, led to major delays in processing transactions. Disagreement over how to respond to these delays split the Bitcoin community: specifically whether to increase the size of the blocks in the chain or make other operational changes to increase speed of processing.[205] A group of miners led by Bitman founder Jihan Wu[206] (remember Bitman—the force behind two of the major mining pools) pushed aggressively for increasing the size of each block added to the

202. *The Differences Between Hard and Soft Forks*, WEUSECOINS (Aug. 23, 2016), https://www.weusecoins.com/hard-fork-soft-fork-differences/.

203. David Dinkins, *Opinion: Collapse of Bitcoin's "New York Agreement" Would Have Long Term Consequences*, COINTELEGRAPH (Sept. 16, 2017), https://cointelegraph.com/news/opinion-collapse-of-bitcoins-new-york-agreement-would-have-long-term-consequences.

204. *Id.*

205. Because bitcoin blocks are 1MB in size and it takes 10 minutes to add a block, the chain can process only roughly 7 transactions per second. For comparison, Visa can process 2000 transactions per second. At peak times, bitcoin transactions can take hours to be filled. *Blockchain Scaling: Why PoW Networks Can't Scale*, COINMONKS (Aug. 31, 2018), https://medium.com/coinmonks/blockchain-scaling-30c9e1b7db1b.

206. Prableen Bajpai, *Who is Jihan Wu and Does He Basically Control Bitcoin?*, INVESTOPEDIA (May 1, 2017), https://www.investopedia.com/news/who-jihan-wu-and-does-he-basically-control-bitcoin-today/. Wu is a controversial figure because of allegations that he manipulated the cryptocurrency for his own gain. Jeff John Roberts, *Does Bitcoin Have a Mining Monopoly Problem?*, FORTUNE (Aug. 25, 2017), http://fortune.com/2017/08/25/bitcoin-mining/.

blockchain from 1 MB to 2 MB.[207] Others advocated a more permanent solution in the form of a code called Segregated Witness (SegWit).[208] This code separated the signatures from the transaction data in each block, then only counted the transaction data as subject to the 1 MB cap.

The debate over which solution to adopt raged on while the Bitcoin network got slower and slower. Finally a group of over 50 high profile companies met to resolve the situation, producing a compromise known as the New York Agreement.[209] This agreement resolved the debate by agreeing to do both proposals—to increase speed by segregating transaction signatures, and to subsequently increase in block size.[210] The companies signing the agreement represented 83.25% of the computing power on the bitcoin blockchain.[211]

It should have been simple. As designed by Nakamoro, the miners decide which code changes to accept. However, an entire economic ecosystem had grown up around the blockchain, and that ecosystem was not happy. Companies that provided cryptocurrency storage wallets aligned with the trading platforms to argue that the change should not proceed without support from an "economic majority" of the blockchain's users.[212] They offered an alternative proposal called BIP148, a user activated soft fork to comply with SegWit. This proposal would put blockchain users, rather than miners in the driver's seat. The stated goal was to avoid forcing users to upgrade their software unnecessarily.[213] But, what was really happening was a power struggle over who gets to make choices for the blockchain—the miners or the users. For example, the users proposed that "[u]sers that decide to enforce the new rules will only follow blocks that conform to the existing rules which will in turn cause miners to activate SegWit.[214] Their position was that the economic majority should signal support for the change, and the miners should follow along.[215] The threat was that if miners did not follow along with the user proposal, users would not recognize their coins as

---

207. *See* Laura Shin, *What Will Happen at the Time of the Bitcoin Hard Fork?*, FORBES (Oct. 31, 2017), https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#5ed3fddc337d.

208. This plan would increase processing speed by segregating transaction signatures (called "witnesses", hence the name "Segwit") from the blockchain. For an explanation of how Segwit works, see Kasireddy, *supra* note 140.

209. Digital Currency Group, *Bitcoin Scaling Agreement at Consensus 2017*, MEDIUM (May 23, 2017), https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77.

210. *Id.* SegWit supporters claimed their approach would save nearly 70% of the space in each block, and would thus be equivalent to a quadrupling of block size.

211. *Id.*

212. USAF Working Group, *BIP148 & UASF FAQ* (last visited Oct. 27, 2018), http://www.uasf.co/#bip148—uasf-faq.

213. *Id.*

214. *Id.*

215. *Id.*

Bitcoin—making sale of those coins more difficult. Yet, if users did not upgrade and the majority of the hash power switched to the new 2MB chain, there might not be enough miners to ensure the validity of the original 1MB blockchain. That would leave the original chain vulnerable to attack.[216] These twin threats highlighted the possibility of a split between a majority of the miners and an "economic majority" of the wallets and platforms, raising the question of whose consensus mattered for blockchain governance.[217]

Despite the agreement, the group of miners led by Jihan Wu decided to opt out of the SegWit debate and increase the size of bitcoin blocks on their own.[218] On August 1, 2017, they implemented a new consensus protocol that raised the block size from 1MB to 8 MB.[219] There were now two protocols, one that recognized only 1 MB blocks as valid, and one that recognized 8MB blocks. This resulted in two mutually incompatible chains—and thus a hard fork in the blockchain. Some miners stuck with the old protocol, while others moved to the new chain, resulting in two currencies: Bitcoin and Bitcoin Cash.[220] Akin to how shares are distributed after a corporate spin-off, *Hodlers* received one Bitcoin Cash for each Bitcoin they held on the day of the hard fork. Bitcoin Cash promoters claimed to be the true heir to Satoshi Nakamoto's vision and thus the true Bitcoin.[221] However, the market

---

216. *Id.*

217. Another group of miners decided to opt out of this debate entirely. They created a hard fork on August 1, 2017 by altering the consensus protocol to create blocks that were 8 MB rather than 1 MB.

218. Sudhir Khatwani, *Bitcoin Cash (BCH) - A New Feather in Bitcoin's Fork Cap*, COINSUTRA, https://coinsutra.com/bitcoin-cash-bch/ (last updated July 9, 2018).

219. Josiah Wilmoth, *The First 8MB Bitcoin Cash Block Was Just Mined*, CCN (Aug. 17, 2017), https://www.ccn.com/first-8mb-bitcoin-cash-block-just-mined/.

220. In an interesting coda to this story, one year after the contentious fork that created Bitcoin Cash, the cryptocurrency appears on the verge of another contentious hard fork, this time over how to treat noncash transactions in addition to disagreements over block size. *Bitcoin Cash Might Chain Split Fork As Tensions Rise with Jihan Wu Calling Craig Wright Fake Satoshi*, TRUSTNODES (Aug. 21, 2018), https://www.trustnodes.com/2018/08/21/bitcoin-cash-might-chain-split-fork-tensions-rise-jihan-wu-calling-craig-wright-fake-satoshi. Noting that the platforms are "kingmakers in these sorts of situations," TrustNodes unironically asks "Would any of them trust a Craig Wright chain?" *Id.* Another commenter sees the major mining pools as the key decisionmakers. Jeff Benson, *The Potential Bitcoin Cash Hard Fork, Explained*, ETHNEWS (Aug. 25, 2018), https://www.ethnews.com/the-potential-bitcoin-cash-hard-fork-explained. Both perspectives assume that the outcome will be the result of a relatively centralized decision-making process in which a few powerful interests dictate the outcome. A far cry from cryptocurrency's decentralized peer-to-peer rhetoric.

221. *See, e.g.*, Jonald Fyookball, *12 Reasons Bitcoin Cash Is the Real Bitcoin*, BITCOIN.COM (Feb. 2, 2018), https://news.bitcoin.com/12-reasons-bitcoin-cash-real-bitcoin/; Iyke Aru, *Roger Ver Declares Bitcoin Cash to Be True Bitcoin, Market Forces Bring More Attention*, (Nov. 20, 2017), https://cointelegraph.com/news/roger-ver-declares-bitcoin-cash-to-be-true-bitcoin-market-forces-bring-more-attention (quoting Ver as declaring "Bitcoin Cash is the Real Bitcoin and will have the bigger market cap, trade volume and user base in the future.").

generally did not accept this claim, and Bitcoin Cash trades for a fraction of the value of Bitcoin.

The saga did not end there. Bitcoin still had its own consensus protocol changes to implement. The first part of the New York Agreement went off as planned, and SegWit was adopted. However, Bitcoin's core development team still opposed doubling the block size.[222] Signatories to the New York Agreement began reneging on their support for the increased block size.[223] In November 2017, the block size increase (known as SegWit2x) was suspended for lack of support.[224] Outraged commenters lamented, apparently without irony, that "[w]ithdrawing one's support from important agreements erodes trust within the community."[225]

1. Lessons from The DAO Smart Contract

The core reason that Nakamoto declared Bitcoin to be a trustless system was that encryption could replace trust. He argued that with strong encryption, "[d]ata could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what."[226] For Nakamoto, cryptocurrency meant that "without the need to trust a third party middleman money can be secure and transactions effortless." [227] However, the halo of security extends well beyond the blockchain itself, inducing participants to trust a host of third parties who act as middlemen. Participants in cryptocurrency find themselves trusting exchanges, wallets, and smart contracts, all under the halo of the blockchain's immutability.

Under the Statute of Frauds, any contract for the sale of land, or that cannot be fully performed within one year, must be reduced to a writing. As per the Uniform Commercial Code, contracts that involve the sale of goods for more than $500 must similarly be memorialized in writing.[228] Thus, although oral contracts can be enforceable, most contracts are written down on

---

222. David Dinkins, *Bitcoin Developers Remain Adamant in Opposition to SegWit2x, Potential Showdown in November*, COINTELEGRAPH (Aug. 10, 2017), https://cointelegraph.com/news/bitcoin-core-developers-remain-adamant-in-opposition-to-segwit2x-potential-showdown-in-november.

223. Alyssa Hertig, *F2 Pool Reneges: Bitcoin Pool Pulls Segwit2x Support over Hard Fork*, COINDESK (Aug. 31, 2017), https://www.coindesk.com/f2pool-reneges-mining-pool-pulls-segwit2x-support-hard-fork/.

224. Posting of Michael Belshe, mike@bitgo.com, to bitcoin-segwit2x@lists.linuxfoundation.org (Nov. 8, 2017), https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html.

225. Dinkins, *supra* note 203.

226. Satoshi Nakamoro, *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUNDATION (Feb. 11, 2009), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

227. *Id.*

228. U.C.C. § 2-201 (AM. LAW INST. & UNIF. LAW COMM'N, amended 2012).

paper, and signed by the parties intending to be bound by the agreement. Smart contracts are a variation on this theme—with the agreement encoded on a blockchain rather than on paper. For technical reasons, most smart contracts to date have been designed for the Ethereum blockchain rather than the Bitcoin blockchain. The main attraction of these smart contracts is the claim that using a blockchain makes the deal immutable. The code *is* the contract. Neither party can renege "thanks to the remorseless logic-crunching of the machine, whose algorithm would execute, verify, and enforce itself."[229] This immutability is pitched as a means of replacing trust.[230] Because the execution of the agreement is no longer separate from the agreement itself, the idea is that trust becomes unnecessary. The touted advantage of these trustless, self-executing contracts is that they can reduce or eliminate the uncertainty and transactions costs associated with executing and/or enforcing a contract.

Yet, smart contracts also offer a good example of how participants can confuse their decision to trust the blockchain with trusting operations that use the blockchain. In particular, the saga of an Ethereum smart contract known as "The DAO"[231] shows how smart contracts can fail disastrously, with consequences that undermine the integrity of the blockchain itself. In 2016, an Ethereum startup called *Slock.it* created The DAO—a smart contract that was pitched as a distributed venture capital firm. It was intended to pool contributor money, and then distribute that money to projects the contributors voted to fund. On a now-deleted homepage, The DAO grandiosely proclaimed that it would "blaze a new path in business organization . . . operating solely with the steadfast iron will of unstoppable code."[232] The DAO launched a two-month investment window on April 30, 2016. By the end of May 2016, the DAO had collected roughly 12 million Ether ($150 million at the time) from investors.[233]

In early June, commenters began pointing out serious vulnerabilities in The DAO's code.[234] In response, on June 12, 2016, Slock.it founder Stephan

---

229. Kieron O'Hara, *Smart Contract – Dumb Idea*, 21 IEEE INTERNET COMPUTING 97, 97 (2017).

230. *Id.* (pointing out that this claim about smart contracts is particularly ironic because contracts are themselves a tool for *building* trust).

231. Distributed Autonomous Organizations (DAOs) is a term that describes smart contracts, generally. However, 'The DAO' was a specific smart contract on Ethereum. Other DAOs exist. *See e.g.*, DIGIX, https://digix.global (last visited Oct. 20, 2018) (Digix Global, a company that tokenizes gold on the Ethereum network, runs a DAO called DigixDAO that issues DGD tokens). Similarly, the cryptocurrency Dash is a DAO.

232. THE DAO, http://web.archive.org/web/20160622212302/https://daohub.org/ (last visited Oct. 31, 2018).

233. Christoph Jentzsch, *The History of the Dao and Lessons Learned*, MEDIUM: SLOT.IT BLOG (Aug. 24, 2016), https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5.

234. Peter Vessenes, *More Ethereum Attacks: Race-To-Empty is Real*, VESSENES (June 9, 2016), http://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/.

Tual took to social media to announce that no DAO funds were at risk,[235] essentially saying "trust us." Five days later, hackers diverted Ether worth nearly $60 million out of The DAO into a new account.[236] The hackers used a technique called a "recursive call exploit" in which they asked the smart contract to give back Ether invested in the DAO multiple times before the DAO updated the internal balances.[237] Observers watched the unknown hackers drain off funds, but because of The DAO's "unstoppable code" they could not do anything to stop it.

Smart contract advocates found themselves in a bind. The code that was supposed *to be* the contract allowed this conduct to occur. The point of a smart contract is that once entered, it is supposed to inviolable—even if circumstances change, or the parties change their minds. Yet faced with flawed code, those who had eagerly bought into an "unstoppable code" suddenly found that attribute far less desirable than they had imagined.[238]

In an extremely contentious move, the Ethereum community decided to create a hard fork to reverse the transfers out of The DAO. Hard Fork opponents argued vociferously against the decision on the ground that it would violate the immutability of the blockchain, thereby undermining the perception that blockchain contracts were permanent.[239] This excerpt of a *reddit* post by derrend is a fairly typical recap of this argument.

> Q: What makes a blockchain valuable?
> A: They are immutable and record an accurate version of history.
> Q: Is the ethereum blockchain immutable and does it represent an accurate version of history?
> A: No.
> Q: Was the integrity of the chain sacrificed in the interests of a small minority?

---

235. Stephan Taul, *No DAO Funds at Risk Following the Ethereum Smart Contract 'Recursive Call' Bug Discovery*, MEDIUM: SLOT.IT BLOG (June 12, 2016), https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b.

236. *See*, Ledgerwatch, *I Think TheDao is Getting Drained Right Now*, REDDIT (June 17, 2016, 3:10 AM), https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/; Vitalik Buterin, *Critical Update Re: DAO Vulnerability*, ETHEREUM BLOG (June 17, 2016), https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

237. Antonio Madera, *The DAO, the Hack, the Soft Fork and the Hard Fork*, CRYPTOCOMPARE (July 26, 2016), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/.

238. Subsequent forensic investigations found that a majority of Ethereum smart contracts ignore best-practices and are therefore vulnerable to hacks. *See* Zikai Alex Wen & Andrew Miller, *Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug*, HACKING, DISTRIBUTED (June 16, 2016), http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/ (calling Ethereum smart contracts "notoriously error-prone.").

239. Madera, *supra* note 237.

A: Yes
Q: If the NSA or the FBI demanded a transaction reversal on the ETH blockchain and ordered the foundation to do so, would they?
A: Yes, judging by precedent.[240]

Hard Fork opponents pointed out that altering the blockchain is a slippery slope[241] and once the blockchain is modified in this fashion, there will inevitably be further calls for other modifications.[242] More fundamentally, they argued that a hard fork to reverse this hack would violate the basic principle that "code is law."[243] Proponents of the hard fork retorted that the "code is law" approach lacks nuance and ignores the dynamic nature of law.[244] Instead, they offered a vision of decision-making in which human beings get to think and make choices that amount to a social consensus.[245]

Ultimately, the hard fork was put up for a vote. A supermajority of Ether holders approved the proposal, and the hard fork took place on July 20, 2016.[246] The hard fork created a new Ethereum chain. The first block on the new Ethereum chain deposited the funds lost from The DAO into an account available to The DAO's original investors.[247] However, a sizeable minority of users rejected the new chain, giving rise to two Ethereum chains—Ethereum and Ethereum Classic.

Note the ironic role that trust plays in this drama—the immutable blockchain was altered in the name of reinstating trust in the blockchain after a smart contract developer failed to live up to the trust placed in it. This decision unquestionably highlights the fragility of the much-touted immutability of the blockchain. It is demonstrably not accurate to say that a blockchain transaction cannot be reversed—an assertion that is the cornerstone for the notion that the blockchain can replace trust.[248] The DAO incident

240. derrend, Comment to *Code is Law*, REDDIT (Sept. 5, 2016, 7:45 PM), https://www.reddit.com/r/ethereum/comments/51bca4/code_is_law/#bottom-comments.

241. *Weaknesses*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Weaknesses (last visited Oct. 31, 2018) ("If it becomes possible for coins to be blacklisted in this way, then it is a slippery slope toward blacklisting of other 'suspicious' coins.").

242. For a sense of the content of these objections, see Arvicco, *Code is Law and the Quest for Justice*, ETHEREUM CLASSIC BLOG (Sept. 8, 2016), https://ethereumclassic.github.io/blog/2016-09-09-code-is-law/.

243. *See id.*; *see also* Lawrence Lessig, *Code is Law: On Liberty in Cyberspace*, HARV. MAG. (Jan. 1, 2000), https://harvardmagazine.com/2000/01/code-is-law-html.

244. *See* Madera, *supra* note 237.

245. *See id.*

246. *Id.*

247. Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (Jul. 20, 2016), https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/.

248. *See* Robert Graham, *Bitcoin: In Crypto We Trust,* ERRATA SECURITY: BLOG (Dec. 19, 2017), https://blog.erratasec.com/2017/12/bitcoin-in-crypto-we-trust.html (claiming that "the manifesto behind Bitcoin is that a transaction cannot be reversed—and thus, can always be trusted").

demonstrates that the blockchain is only as immutable as its community of users decides it is. That means that trusting that immutability is really trusting the community to make the right choice. If it happened once, it could happen again, including for far less savory reasons.

Indeed, Ethereum Hard Fork opponents were prescient in their assertion that The DAO hard fork would encourage others to request similar treatment. After a hacker exploited a vulnerability in wallets run by the company Parity, the company sought a hard fork to undo the hack.[249] The hacker took control of 587 wallets holding 513,774.16 Ether (worth roughly $300 million at the time.)[250] The user then destroyed the wallets, effectively freezing those coins.[251] Parity developers have requested another Ethereum hard fork to recover at least some of these coins.[252]

The decision of whether or not to accede to this request roiled the Ethereum network.[253] It turns out that stuck, non-recoverable Ether is a relatively common problem.[254] User error in the command line, software bugs,[255] and intentional hacks like the one at Parity have all created millions of dollars worth of "stuck" Ether, inaccessible to its owners.[256] Commenters have pointed out that having those coins taken out of circulation increases the value of the remaining Ether—creating a clear conflict of interest between those whose Ether is not locked and the unfortunate victims of the Parity hack or other stuck situations.[257]

---

249. *See* Parity Technologies, *A Postmortem on the Parity Multi-Sig Library Self-Destruct,* PARITY: BLOG (Nov. 15, 2017), https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/.

250. *Id.*; Alex Hern, *'$300m in Cryptocurrency' Accidentally Lost Forever Due to Bug*, GUARDIAN (Nov. 8, 2017), https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether.

251. *See* Parity Technologies, *supra* note 249.

252. *Id.* (conceding that "there is no timeline for when such an improvement proposal could be implemented.").

253. *See* Adam James, *Ethereum Community Votes Down $318 Million Parity Refund Request,* BITCOINIST.COM (April 25, 2018), https://bitcoinist.com/ethereum-community-votes-330-million-parity-refund-request/.

254. *See* Parity Technologies, *On Classes of Stuck Ether and Potential Solutions,* PARITY: BLOG (Dec. 11, 2017), https://paritytech.io/on-classes-of-stuck-ether-and-potential-solutions/.

255. Peter Vessenes, *Ethereum Contracts are Going to Be Candy for Hackers*, VESSENES.COM (May 18, 2016), http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/.

256. Parity Technologies, *supra* note 254.

257. *See* Editorial Team, *Parity to Ethereum Foundation: One Hard Fork, Please*, COINBUREAU (Dec. 14, 2017), https://www.coinbureau.com/smart-contracts/parity-ethereum-foundation-one-hard-fork-please/.

2. The Unrealized Vulnerabilities of Cryptokitties

The recent craze over Cryptokitties highlights another mistake of conflating the blockchain with smart contracts that use the blockchain. Cryptokitties are so-called non-fungible tokens. Each Cryptokitty is cartoon-like digital cat.[258] Users use Ether to purchase tokens that give them ownership of the virtual cats, each of which has a unique identity logged on the Ethereum blockchain. In late 2017, demand for these kitties nearly broke the Ethereum network.[259] At least one purchaser offered over $110,000 for a kitten, though most sell for far less.[260] The value proposition for these kittens as collectables rests on the immutable nature of the Ethereum blockchain. Promotional materials promise that "each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away or destroyed."[261] Yet, it is not clear that United States property law recognizes nonfungible tokens as property.[262]

The hype around these digital cats is an example of how the blockchain's aura of immutability spreads over related, but distinct entities, sweeping them within the halo of trust. All the Cryptokitties exist in one Ethereum smart contract.[263] As one commenter points out, "as far as Ethereum is concerned there is only a single version of the KittyOwnership contract, and that contract is owned by a single wallet. It doesn't get more centralized than this."[264] Indeed, the developers themselves acknowledged that their decentralized app had multiple centralized aspects.[265] This structure has practical implications that directly contradict the marketing language behind Cryptokitties. The contract holder retains near total control over the fate of the kittens. Should it choose to, the contract holder could

---

258. CRYPTOKITTIES, https://www.cryptokitties.co/ (last visited Oct. 31, 2018).

259. *See* Olga Kharif, *Cryptokitties Mania Overwhelms Ethereum Network's Processing*, BLOOMBERG (Dec. 4, 2017), https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app. Since then, demand has faded. Indeed, one analyst reports that by August 2018 Cryptokitty's user base had plummeted by 96%. *Decentralized Apps Facing Half-Life After Peak,* DIAR (Aug. 20-27, 2018), https://diar.co/decentralized-apps-facing-half-life-after-peak/.

260. Joseph Young, *Ethereum-Based Cryptokitten Sells for $117,712*, COINJOURNAL (Dec. 3, 2017), https://coinjournal.net/ethereum-based-cryptokitten-sells-117712/.

261. *Understanding CryptoKitties*, CRYPTO KITTY WORLD, http://cryptokittyworld.com/ (last visited Oct. 31, 2017).

262. Kyle Wood & Taylor Lindman, *Why the Next CryptoKitties Mania Won't Be About Collectables*, TECHCRUNCH (Aug. 21, 2018), https://techcrunch.com/2018/08/21/why-the-next-cryptokitties-mania-wont-be-about-collectables/.

263. Luke Zhang, *Your CryptoKitty Isn't Forever - Why DApps Aren't as Decentralized as You Think,* MEDIUM (Dec. 3, 2017), https://medium.com/loom-network/your-crypto-kitty-isnt-forever-why-dapps-aren-t-as-decentralized-as-you-think-871d6acfea.

264. *Id.*

265. David Floyd, *Decentralizing Popular Dapps Isn't Just a Scaling Problem,* COINDESK (June 28, 2018), https://www.coindesk.com/decentralizing-popular-dapps-isnt-just-scaling-problem/.

pause the contract—sending all Cryptokitties into permanent hibernation.[266] Moreover, Cryptokitties creator Axiom Zen retains total discretion to change the breeding algorithm, with the possibility of making previously rare (and expensive) kitten traits commonplace.[267] There is no reason to think that these things will happen, but they could. Purchasers dazzled by the blockchain do not even realize how much they are trusting Cryptokitties, Inc. to behave in a fashion that maintains the value, and indeed the very existence of their purchases. While posters on reddit express concern about the reliability of the wallets holding their expensive kittens,[268] they do not express the same concerns about the underlying contract. It is highly likely that they have no idea of the vulnerability built into their purchase. The levels of trust embedded in this trustless system are dangerous—lulling people into a false sense of security about transactions that are in fact quite vulnerable.

C. *Trusting Wallets and Platforms*

Most individuals do not interact directly on the blockchain. They instead interact through platforms or wallets or other intermediaries that purport to help them buy, sell, and hold cryptocurrencies. These interactions create a new set of trusted intermediaries. Nakamoro's vision for bitcoin of a peer-to-peer network with no need to trust third-parties has instead morphed into a system with multiple intermediaries, all of whom cloak themselves in the aura of the blockchain. His gripe that trusting banks meant "[w]e have to trust them with our privacy, trust them not to let identity thieves drain our accounts"[269] applies just as clearly to cryptocurrency third parties. It turns out that cryptocurrency requires the same trust, only this time it is placed in unregulated, non-transparent actors.

These cryptocurrency third parties have too often failed to live up to the trust placed in them. Even avid cryptocurrency supporters acknowledge that in the cryptocurrency universe, scandals and frauds are rampant.[270] Despite the purported immutable security of the blockchain, there are plenty of ways for thieves to steal cryptocurrency. Indeed, rapidly rising prices, anonymity,

---

266. In the Parity hack described above, this is what a malicious user did to the wallets.

267. Floyd, *supra* note 265.

268. *See e.g.,* kryptofan, Comment to *Where Exactly is my Kitty on the Blockchain*, REDDIT (Jan. 19, 2018, 10:05PM), https://www.reddit.com/r/CryptoKitties/comments/7rio31/where_exactly_is_my_kitty_on_the_blockchain/.

269. Satoshi Nakamoto, Comment to *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUNDATION (Feb. 11, 2009, 10:27PM), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

270. Coinbrief, *Bitcoin vs USD vs Gold—Here's Why Bitcoin Wins*, 99BITCOINS (Jan. 2, 2018), https://99bitcoins.com/bitcoin-gold-usd/. For a list of some of the scandals, see Coinbrief, *Mt. Gox, Mintpal, Hashfast, Butterfly Labs, and Robocoin: Blunders in Bitcoin Business*, 99BITCOINS (Feb. 22, 2018), https://99bitcoins.com/bitcoin-business-blunders/.

and lack of regulation make cryptocurrency exchanges "natural targets" for theft[271] and scams. Hacks and thefts are common occurrences. And because of cryptocurrency's decentralized, unregulated and irreversible nature, victims find themselves largely without recourse.[272] One major cryptocurrency investor summed up the situation clearly when he tweeted about one of the many cryptocurrency trading platform scandals: "Is it unfair? Of course. If you want fair, cryptocurrency isn't for you. Stick with assets that are based on trusting the regulatory and legal infrastructure."[273]

1. Hacks and Thefts

As of late 2017, Reuters estimated that 980,000 coins, worth up to $15 billion had been stolen in the prior six years from cryptocurrency wallets and platforms.[274] The following is a list of just a sampling of the most recent cryptocurrency hacks since then:[275]

- July 2018—Israeli platform Bancor was hacked. Cryptocurrency worth over $23 million stolen.[276]
- June 2018—South Korean platform Bithumb was hacked. Cryptocurrency worth $37 million stolen.[277]
- June 2018—South Korean platform Coinrail was hacked. Coins worth over $40 million stolen.[278]

---

271. Steven Melendez, *Bitcoin Heist Adds $77 Million to Total Hacked Hauls of $15 Billion*, FASTCOMPANY (Dec. 7, 2017), https://www.fastcompany.com/40505199/bitcoin-heist-adds-77-million-to-hacked-hauls-of-15-billion.

272. *See, e.g.*, Kai Sedgwick, *Cheated Cryptocurrency Investors are Taking Matters into Their Own Hands*, BITCOIN.COM (Dec. 21, 2017), https://news.bitcoin.com/cheated-cryptocurrency-investors-taking-matters-hands/ (describing various ineffectual self-help attempts by defrauded cryptocurrency investors).

273. Ari Paul (@AriDavidPaul), TWITTER (Dec. 20, 2017, 6:35 AM), https://twitter.com/AriDavidPaul/status/943489940352061440.

274. Jim Finkle & Jeremy Wagstaff, *Hackers Steal $64 Million from Cryptocurrency Firm NiceHash*, REUTERS (Dec. 6, 2017), https://www.reuters.com/article/us-cyber-nicehash/hackers-steal-64-million-from-cryptocurrency-firm-nicehash-idUSKBN1E10AQ.

275. Yugi Nakamura, *The Wretched, Endless Cycle of Bitcoin Hacks*, BLOOMBERG (Aug. 17, 2016), https://www.bloomberg.com/news/articles/2016-08-17/the-wretched-endless-cycle-of-bitcoin-hacks.

276. Jon Russell, *The Crypto World's Latest Hack Sees Bancor Lose $23.5M*, TECHCRUNCH, (July 11, 2018), https://techcrunch.com/2018/07/10/bancor-loses-23-5m/. In this hack, a Bancor wallet was hacked and used to steal money from associated smart contracts. Bancor (@Bancor), TWITTER (July 9, 2018, 4:35 PM), https://twitter.com/Bancor/status/1016420621666963457.

277. Nick Chong, *Breaking News: Bithumb Hacked for $30 Million in Cryptocurrencies, Market Drops*, NEWSBTC (June 20, 2018), https://www.newsbtc.com/2018/06/20/breaking-news-bithumb-hacked-for-30-million-in-cryptocurrencies-market-drops/.

278. Tim Culpan, *$2.3 Billion in Losses Highlights Crypto's Moral Hazard*, BLOOMBERG OPINION (June 11, 2018), https://www.bloomberg.com/opinion/articles/2018-06-11/-2-3-billion-in-losses-highlights-crypto-s-moral-hazard.

- February 2018—CISCO confirmed that a Ukrainian hacker group called Coinhorder stole $50 million from Blockchain.info wallets.[279]
- February 2018—Bitgrail informed users that 17 million Nano had been stolen, worth $170 million.[280]
- January 2018—Japanese platform Coincheck was hacked for $530 million—making it the largest cryptocurrency hack ever,[281] outstripping the 2014 Mt. Gox hack in which $400 million was stolen.[282]
- January 2018—Blackwallet announces it has been hacked advises customers not to log in to their accounts. 700,000 lumens stolen (value $400,000).
- January 2018—Users on the Bitcoin cash Reddit (commonly known as /r/BTC) reported their Tippr accounts had been hacked and emptied out of their funds.[283]
- December 2017—YouBit (S. Korea) thieves stole cryptocurrency worth $35 million dollars, or 3/5 of clients' holdings on the platform. Company filed for bankruptcy[284]
- December 7, 2017—NiceHash thieves stole 4700 bitcoin—worth more than $75 million at the time.[285] NiceHash described itself as "the largest marketplace for mining digital currencies." It appears that the hacker entered the system with credentials for one of NiceHash's engineers.

---

279. Jen Wieczner, *Hackers Stole $50 Million Using 'Poison' Google Ads*, FORTUNE (Feb. 14, 2018), http://fortune.com/2018/02/14/bitcoin-cryptocurrency-blockchain-wallet-hack/. This was a theft rather than a hack. Coinhoarder created fake google ads for fraudulent sites. People googling common cryptocurrency terms like blockchain or Bitcoin wallet were directed to malicious sites posing as the real thing. It was this sort of scheme that prompted Facebook to ban all cryptocurrency advertising in early 2018.

280. Adam Reese, *Class Action Suit Against Nano Core Devs Calls for Hard Fork*, ETHNEWS (April 9, 2018), https://www.ethnews.com/class-action-suit-against-nano-core-devs-calls-for-hard-fork.

281. Daniel Shane, *$530 Million Cryptocurrency Hack May Be Largest Ever*, CNN BUS. (Jan. 29, 2018), https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html.

282. Jose Pagliery, *How Mt. Gox Went Down*, CNN BUS. (Feb. 26, 2014), https://money.cnn.com/2014/02/25/technology/security/bitcoin-mtgox/index.html.

283. Bryan Menegus, *How a Reddit Email Vulnerability Led to Thousands in Stolen Bitcoin Cash*, GIZMODO (Jan. 5, 2018), https://gizmodo.com/reddit-email-vulnerability-leads-to-thousands-of-dollar-1821808073.

284. Daniel Shane, *Bitcoin Exchange Goes Bust After Hack*, CNN BUS. (Dec. 20, 2017), https://money.cnn.com/2017/12/20/technology/south-korea-bitcoin-exchange-closes/index.html.

285. Rishi Iyengar, *More Than $70 Million Stolen in Bitcoin Hack*, CNN BUS. (Dec. 8, 2017), https://money.cnn.com/2017/12/07/technology/nicehash-bitcoin-theft-hacking/index.html.

- November 2017—Bitfinex, which had previously lost millions of dollars of customer money in multiple hackings, was hacked again, this time losing $30 million of Tether from online wallets.[286]

Unfortunately, the list could go on and on. These hacks illustrate how trust in third parties that surround the blockchain might be misplaced. As the Wall Street Journal reported, cryptocurrency platforms are getting hacked because lack of regulation makes it "easy."[287]

Thefts and hacks aside, many platform users have been unpleasantly surprised at how easily cryptocurrency trading platforms can unilaterally make choices that limit user access to their funds. The instances that follow describe a few of the most high-profile instances.

2. Access to Bitcoin Cash

The Bitcoin Cash hard fork highlighted the unanticipated trust that *hodlers* were placing in trading platforms that managed their trustless cryptocurrency. Akin to how shares are distributed after a corporate spin-off, each *hodler* was slated to receive one Bitcoin Cash for each Bitcoin they held on the day of the hard fork. Bitcoin Cash's promotional website specifically distinguishes Bitcoin Cash from bank accounts which it claims "are only as safe as political leaders describe. Even under the best of conditions, banks can make mistakes, hold funds, freeze accounts and otherwise prevent you from accessing your own money."[288] By contrast, Bitcoin Cash promised to give users "full, sovereign control over your funds, which you can access from anywhere in the world."[289]

Coinbase and Blockchain.info, two of the largest currency platforms, had other plans. These platforms opted not to support the new currency at the time of the hard fork.[290] That meant that any customers with bitcoin on

---

286. Stan Higgins, *Tether Claims $30 Million in US Dollar Token Stolen*, COINDESK (Nov. 21, 2017), https://www.coindesk.com/tether-claims-30-million-stable-token-stolen-attacker. Bitfinex lost 1,500 Bitcoin, worth around $330,000, to a hacker in 2015. Izabella Kaminska, BITCOIN BITFINEX EXCHANGE HACKED: THE UNANSWERED QUESTIONS, FIN. TIMES (Aug. 4, 2016), https://www.ft.com/content/1ea8baf8-5a11-11e6-8d05-4eaa66292c32. In August 2016, Bitfinex was hacked again, losing almost 120,000 Bitcoin, worth around $66 million at the time. Stan Higgens, *The Bitfinex Bitcoin Hack: What We Know (and Don't Know)*, COINDESK (Aug. 3, 2016), https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know. One of the more significant consequences of the 2016 Bitfinex hack is described *infra* pp. 44-46.

287. Steven Russolillo and Eun-Young Jeong, *Cryptocurrency Exchanges are Getting Hacked Because It's Easy*, WALL ST. J. (July 16, 2018).

288. *Frequently Asked Questions*, BITCOIN CASH, https://www.bitcoincash.org/#faq (last visited Nov. 23, 2018).

289. *Id.*

290. Class Action Complaint at 6, Berk v. Coinbase, Inc., No. 4:18-cv-01364-KAW (N.D. Cal. filed Mar. 1, 2018); William Suberg, *Blockchain.info Releases Full Bitcoin Cash*

either platform would not receive their Bitcoin Cash, and could not access, use or sell the coins. Indeed, Coinbase made it very clear that customers "will only have access to the current version of bitcoin we support (BTC). Customers will not have access to, or be able to withdraw, bitcoin cash (BCC)."[291] In other words, the platforms took it upon themselves to prevent their customers from receiving valuable property that, by all ordinary measures, those customers owned and were entitled to receive. Bitcoin *hodlers* discovered that their trustless, immutable cryptocurrency was actually held at the mercy of the platforms they had trusted perhaps without realizing it.

Worse, Coinbase advised clients wishing to receive their Bitcoin Cash to withdraw their bitcoin from the platform,[292] cautioning that during the hard fork, "customers would not be able to withdraw any version of any Bitcoin from Coinbase."[293] In other words, the platform used its power to shut down cryptocurrency owners' ability to buy or sell their coins. As customers raced to withdraw their bitcoin before the hard fork, Coinbase reported experiencing "a high backlog."[294] With transactions taking up to 12 hours to process, customers complained that they were locked into Coinbase and its decision about Bitcoin Cash.[295] Blockchain.info waited two months, until mid-October to credit Bitcoin accounts with Bitcoin Cash.[296] Coinbase waited even longer, finally crediting customers with their Bitcoin Cash on December 19, 2017,[297] months after the hard fork occurred. During the interim, customers lost the opportunity to sell their coins. More importantly, they

---

Support, Users Receive Coins, COINTELEGRAPH (Oct. 12, 2017), https://cointelegraph.com/news/blockchaininfo-releases-full-bitcoin-cash-support-users-receive-coins.

291. *Coinbase GDAX Reiterate Position on Bitcoin Cash: Njet!* TRUSTNODES (July 28, 2017), https://www.trustnodes.com/2017/07/28/coinbase-gdax-reiterate-position-bitcoin-cash-njet.

292. David Farmer, *Update for Customers With Bitcoin Stored on Coinbase*, COINBASE BLOG (July 27, 2017), https://blog.coinbase.com/update-for-customers-with-bitcoin-stored-on-coinbase-99e2d4790a53.

293. Class Action Complaint at 6, Berk v. Coinbase, Inc., No. 4:18-cv-01364-KAW (N.D. Cal. filed Mar. 1, 2018); *see also* Farmer *supra* note 292 (reiterating that "We plan to temporarily suspend bitcoin buy/sells, deposits and withdrawals on August 1, 2017 as the fork is likely to cause disruption to the bitcoin network. This means your funds will be safe but you will be unable to access your bitcoin (BTC) for a short period of time.").

294. Class Action Complaint at 6, Berk v. Coinbase, Inc., No. 4:18-cv-01364-KAW (N.D. Cal. filed Mar. 1, 2018).

295. *See Coinbase Faces Exodus as Bitcoiners Race to Withdraw, Delays up to 12 Hours*, TRUSTNODES (July 30, 2017), https://www.trustnodes.com/2017/07/30/coinbase-faces-exodus-bitcoiners-race-withdraw-delays-12-hours.

296. William Suberg, *Blockchain.info Releases Full Bitcoin Cash Support, Users Receive Coins*, COINTELEGRAPH (Oct. 12, 2017), https://cointelegraph.com/news/blockchaininfo-releases-full-bitcoin-cash-support-users-receive-coins.

297. *See Bitcoin Cash FAQ*, COINBASE, https://support.coinbase.com/customer/portal/articles/2911542 (last visited Nov. 23, 2018).

lost their trust in the promise that cryptocurrency offered them interference-free transactions.[298]

3. Bitfinex Hack

Two months after the DAO fiasco, hackers attacked the cryptocurrency platform Bitfinex. The hackers stole 119,756 Bitcoins (worth more than $65 million at the time).[299] Bitfinex responded by halting trading, deposits and withdrawals, and canceling out all margin positions.[300] This move harkened back to Mt. Gox's 2014 decision to stop investors from pulling out their money when the platform discovered it was under attack.[301] In the Mt. Gox situation, the exchange filed for bankruptcy and the users lost their money.[302]

A few days after the hack, Bitfinex unilaterally announced that it had "generalized the losses across all accounts,"[303] by reducing all customer holdings by 36%. The trading platform unilaterally decided to dock customer accounts. It would be unimaginable for a bank, regulated under United States law to take such a course of action in response to embezzlement or a bank robbery. But cryptocurrency trading platforms are at most loosely regulated, and Bitfinex is based in Hong Kong, well beyond the jurisdiction of United States regulators. Thus, the company was free to act as it chose. In exchange for the reduced holdings, Bitfinex issued BTX (so-called "hack coins") to users as a promise that it would return those funds at an unspecified future date.[304] In October 2016, Bitfinex offered to pay a bounty if the hacker would agree to return the coins.[305] It took Bitfinex six months to purportedly redeem the hacked coins and reimbursed investors.[306]

---

298. *See, e.g.*, Sue Marquette Poremba, *What Is Bitcoin? Everything You Need to Know,* TOM'S GUIDE (Feb. 5, 2018,) https://www.tomsguide.com/us/what-is-bitcoin,review-5061.html (describing the inspiration for bitcoin as being "free from interference by government and financial institutions.").

299. Jethro Mullen, *Hackers Steal Bitcoins Worth Millions in Attack on Exchange*, CNN (Aug. 3, 2016), https://money.cnn.com/2016/08/03/technology/bitcoin-exchange-bitfinex-hacked/index.html.

300. *See Announcements > Security Breach,* BITFINEX (Aug. 2, 2016), https://www.bitfinex.com/posts/123.

301. In this hack, 744,408 bitcoin were stolen, worth nearly $400 million at the time. David Goldman, *14 Biggest Tech Fails of 2014*, CNN (Dec. 16, 2014), https://money.cnn.com/gallery/technology/2014/12/16/tech-fails-2014/11.html.

302. Jemima Kelly and Anna Irrera, *Bitcoin Fever Exposes Crypto-Market Frailties*, REUTERS (Dec. 13, 2017), https://www.reuters.com/article/uk-markets-bitcoin-risks-insight/bitcoin-fever-exposes-crypto-market-frailties-idUSKBN1E724X.

303. *Announcements: Security Breach - Update 3*, BITFINEX (Aug. 6, 2016), https://www.bitfinex.com/posts/129. The company explains that it distributed the loss to mimic what would have happened in a liquidation.

304. *Id.*

305. *Announcements: Message to the Individual Responsible for the Bitfinex Security Incident of August 2, 2016*, BITFINEX (Oct. 21, 2016), https://www.bitfinex.com/posts/159.

Bitfinex was not the only trading platform to commandeer investor assets in a liquidity crunch. On July 31, 2018, OKEx, a Chinese-run trading platform,[307] invoked its 'societal loss risk management mechanism'[308] to cover losses associated with an enormous Bitcoin gamble gone wrong. [309] A trader had made a heavily-leveraged bet (worth $416 million) that Bitcoin would rise against the US dollar.[310] The trader was unable or unwilling to meet a margin call when Bitcoin's value plunged. As per its forced liquidation policy,[311] OKEx liquidated the account. Unfortunately, the losses extended well beyond the assets available to cover them. The platform had an insurance fund for such situations, but since the insurance fund had only 10 Bitcoin, it was rapidly depleted.[312] OKEx reportedly contributed an additional 2500 bitcoin (worth $18.5 million at the time) to the insurance fund, but that was not enough to cover the total margin call losses generated by the situation. To cover this shortfall, OKEx clawed back 1200 bitcoins (worth $8.8 million at the time) from other traders on the platform. That worked out to roughly 18% of profits from these other traders. Moreover, it is worth noting that the OKEx platform was no stranger to controversy, having been accused a few months earlier of manipulating market prices in order to liquidate margin positions,[313] and fielding allegations that its trading

---

The post suggested that the hacker contact Bitfinex on Tor to preserve his/her anonymity, assuring that "our interest is not to accuse, blame, or make demands, but rather to discuss an arrangement that we think you will find interesting." *Id.*

306. *Announcements: 100% Redemption of Outstanding BFX Tokens*, BITFINEX (Apr. 3, 2017), https://www.bitfinex.com/posts/198. *See also* Garrett Keirns, *Bitcoin Exchange Bitfinex Buys Back All Remaining 'Hack Credit' Tokens*, COINDESK (April 2, 2017), https://www.coindesk.com/bitfinex-pledges-buy-back-remaining-hack-credit-tokens/.

307. OKEx is based in Hong Kong, and is Chinese run. *See* Avi Misrahi, *Okex Fights Market Manipulation Rumors Following Painful Future Contracts Rollback*, BITCOIN.COM (April 4, 2018), https://news.bitcoin.com/okex-fights-market-manipulation-rumors-following-painful-futures-contracts-rollback/. However, the company is actually a corporation registered in Belize. *See* Clarification of Recent Events, OKEX SUPPORT (April 3, 2018), https://support.okex.com/hc/en-us/articles/360002350972.

308. *Regarding the Forced Liquidation Incident on Jul 31, 2018*, OKEX SUPPORT, https://support.okex.com/hc/en-us/articles/360011941512-Regarding-the-Forced-Liquidation-Incident-on-Jul-31-2018 (last visited Nov. 26, 2018).

309. Lucinda Shen, *One Faulty $416 Million Trade On Bitcoin Puts Several OKEx Traders on the Hook*, FORTUNE (Aug. 3, 2018), http://fortune.com/2018/08/03/okex-losses-among-counter-parties/.

310. *Id.*

311. *See Forced Liquidation*, OKEX SUPPORT (Jan. 18, 2018), https://support.okex.com/hc/en-us/articles/360000139652-Forced-Liquidation.

312. *See* Austerity Sucks, *The $415 Million Elephant in the Room (OKEx Futures Unfilled BTCUSD Liquidation)*, MEDIUM (July 31, 2018), https://medium.com/@Austerity_Sucks/the-415-million-elephant-in-the-room-okex-futures-unfilled-btcusd-liquidation-aa601b188007.

313. *See Clarification of Recent Events*, OKEX SUPPORT (April 3, 2018), https://support.okex.com/hc/en-us/articles/360002350972.

volume was dramatically overstated.[314] Even assuming that allegations about OKEx's nefarious conduct are false, it seems clear that neither traders subject to the societal loss risk management mechanism, nor the platform itself were prepared for the magnitude of their exposure.

Imagine if a big bank took 18% of client funds to cover a big loan that went bad, or if E-Trade docked all customers 36% to cover thefts from other accounts. Time and time again, cryptocurrency users have discovered that they have unexpectedly trusted cryptocurrency platforms with powers far beyond their initial contemplation. The rhetoric about "trustless transactions" obscured the multiple layers of trust actually implicated in trading on a cryptocurrency platform. The SEC has expressed concern that "many online trading platforms appear to investors as SEC-registered and regulated marketplaces when they are not. Many platforms refer to themselves as 'exchanges,' which can give investors the mis-impression that they are regulated or meet the regulatory standards of a national securities exchange."[315] In short, platforms not only cloak themselves in the halo of the blockchain's immutability, these unregulated entities also benefit from the halo of the regulatory trust generated through rigorous regulation of national securities exchanges.[316]

D. *Trusting an ICO*

Many of the new cryptocurrencies rely on a novel form of crowdfunding called an "initial coin offering" or ICO. In an ICO, every unit of currency—usually Ether, dollars, or Bitcoin—an investor sends to a company's wallet represents a "smart contract" for purchasing ICO coins from the business. These ICO tokens purport to give investors special access to whatever the underlying business does, as well as giving the investor equity in the network. Theoretically, as the company's product becomes popular, demand for its coins or tokens will rise, boosting the value of those held by the initial investors. Entrepreneurs sell virtual currencies to investors to raise money for software they are building. Roughly 875 such projects raised over $6 billion in 2017.[317]

Even bracketing the judgments that go into assessing whether such an investment is likely to be lucrative, there are multiple levels of trust embedded in these ICO interactions: first, trust that the company exists and is not merely a scam; and second, trust that the promoters have not struck secret

314. Sylvain Ribes, *Chasing Fake Volume: A Crypto-Plague*, MEDIUM (Mar. 10, 2018), https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e (alleging that over 90% of the platform's volume was fabricated).

315. SEC, *supra* note 29.

316. *See, e.g.*, 17 C.F.R. pts. 201, 240, 242, 249 (2017).

317. The website Icodata.io tracks the activity of ICOs. *Funds Raised in 2017*, ICODATA.IO, https://www.icodata.io/stats/2017 (last visited Nov. 26, 2018).

deals to promote or prop up their coins. These layers of trust are necessary for an ICO, but none of them can be protected by the blockchain's touted immutability. In a more conventional transaction, SEC regulations would provide what I have elsewhere called "regulatory trust"[318]—regulatory assurances that provide confidence to the public.

Yet, in the new "trustless" world of the blockchain, regulatory trust does not apply, and instead these ancillary levels of trust get swept into the blockchain's halo of reliability. As a result, "every new coin offering presents another chance to translate a flaky business into an absurd valuation."[319] Take the April 2017 Gnosis ICO as an example. The company self-described as "a user-driven prediction market" based on a coming "Cambrian explosion of machine intelligence."[320] At the time of the ICO, the company was little more than an idea spelled out on paper and some open-source code. The company held a Dutch auction, hoping to raise $12.5 million dollars by selling up to 10 million of its coins. The auction lasted 11 minutes, closing when the sale raised the targeted sum.[321] Turns out, the company met its goal by selling only a fraction (about 42,000) of the 10 million coins allocated to the auction. Gnosis suddenly had a market-ascribed valuation of $300 million. Within two months, that valuation had mushroomed to $3 billion (more than Revlon or Time Inc.) with each coin selling for hundreds of dollars.

Some have leveraged the buzz surrounding blockchains and the frenzy of ICOs to commit outright fraud. For example, the blockchain based fruit company Prodeum that was going to "revolutionize the fruit and vegetable industry"[322] by "keep[ing] track of produce on the Ethereum blockchain" launched an ICO on January 20th. The concept itself was not as far-fetched as it might sound. Walmart has been experimenting with blockchain pilot projects to track its produce.[323] The technology has obvious applications for protecting the public during a food-related health scare, and might also reduce food waste.[324] Yet, Prodeum was a scam. Nine days after the ICO began, Prodeum disappeared with investor money, leaving only the word "pe-

318. Bratspies, *supra* note 64 (discussing public trust in the government).

319. Laura Shin, *The Emperor's New Coins: How Initial Coin Offerings Fueled a $100 Billion Crypto Bubble*, FORBES, July 27, 2017, at 62, 65.

320. *Id.; Gnosis Whitepaper*, at 9 (Apr. 5, 2017), https://gnosis.pm/assets/pdf/gnosis-whitepaper.pdf.

321. Shin, *supra* note 319.

322. Avi Mizrahi, *Vegetables on Blockchain ICO Exit Scams After Paying People to Write on Their Bodies*, BITCOIN.COM (Jan. 30 2018), https://news.bitcoin.com/vegetables-on-a-blockchain-ico-exit-scams-after-paying-people-to-write-on-their-bodies/.

323. Sylvain Charlebois, Opinion, *How Blockchain Could Revolutionize Food Industry*, GLOBE & MAIL (Dec. 12, 2017), https://www.theglobeandmail.com/report-on-business/rob-commentary/how-blockchain-could-revolutionize-the-food-industry/article37305425/.

324. *Id.*

nis" on its website.[325] After the company disappeared, it turned out that they had used fraudulent images in a viral social media campaign—with "fans" who showed support for the concept by writing #prodeum on their bodies turning out to be freelancers hired from a task website.[326] At least one of the people identified on the now-defunct Prodeum website as a company founder claimed that he had no association with the company and was instead a victim of identity theft.[327] According to a recent report from the ICO advisory firm Satis Group, 78% of the ICOs in 2017 were scams, and another 7% had failed or otherwise gone dead.[328]

According to an account in Forbes magazine, one ICO creator offered one crypto asset hedge fund manager the following deal: "If you agree to buy tokens at the ICO and support the price, then 30 days later, we'll secretly sell you any leftover tokens at a lower, pre-agreed price."[329] In the stock market, such an offer would amount to felony insider trading. Yet, ICO organizers manage to sidestep securities regulations by claiming that they are not actually offering a share in the company. The SEC is poised to crack down on this practice, issuing a statement indicating that "by and large, the structures of initial coin offerings . . . involve the offer and sale of securities and directly implicate the securities regulations."[330] Acting on this statement, the SEC has brought fraud charges against at least one unlicensed platform and its founder.[331] In May of 2018, regulators in the United States and Canada conducted "cryptosweep," a coordinated enforcement action cracking down on fraudulent ICOs. The effort resulted in scores of cease and desist letters against fraudulent or deceptive practices.[332] Many more such investi-

325. Brian Feldman, *The Blockchain- for-Vegetables StartUp Website Was Replaced with the Word Penis and No One Has a Clear Explanation As to Why*, N.Y. MAG.: INTELLIGENCER (Jan. 29, 2018), http://nymag.com/intelligencer/2018/01/prodeum-scam-cryptocurrency-for-produce-disappears.html.

326. *See* Mizrahi, *supra* note 322.

327. Mix, *Cryptocurrency Startup Prodeum Pulls an Exit Scam, Leaves a Penis Behind*, NEXT WEB (Jan. 29, 2018), https://thenextweb.com/hardfork/2018/01/29/cryptocurrency-prodeum-scam-exit-penis/.

328. Sherwin Dowlat, *Cryptoasset Market Coverage Initiation: Network Creation*, SATIS GRP. 24 (July 11, 2018), https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

329. Shin, *supra* note 319, at 69.

330. CHAIRMAN JAY CLAYTON, SEC, STATEMENT ON CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

331. SEC, SEC CHARGES FORMER BITCOIN-DENOMINATED EXCHANGE AND OPERATOR WITH FRAUD, (2018), https://www.sec.gov/news/press-release/2018-23.

332. *State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown*, N. AM. SEC. ADM'R ASS'N (May 21, 2018), http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/.

gations are ongoing, and regulators warn that these enforcement actions "are just the tip of the iceberg."[333]

ICO issuers are not the only group engaging in fraudulent practices. Some online groups openly try to manipulate the prices of cryptocurrencies through pump-and-dump schemes.[334] These actors create countdown clocks for their coordinated pumping action, designed to move the price of a cryptocurrency. [335] Members pay for access, and for information to allow them to participate in the profitmaking.[336] The website *PumpMyCoin* is fairly typical.[337] One twitter user going by the name @pumpanddumpking boast "I will tweet out which coin will be pumped on binance. Join my personal pump and dump group below !!!"[338] *Wallet Investor* keeps a Pump & Dump Cryptocurrency List indicating which currencies have moved more than 5% in 5 minutes.[339] Similar schemes involving stocks are illegal, but so far cryptocurrencies are a grey area. Indeed, the spokesperson for one pump and dump has stated the belief that the fraud rules against pump and dump for securities do not apply to cryptocurrency.[340] Caveat emptor rules the day.

E. *Government to the Rescue?*

One of the touted trustless aspects of cryptocurrency is that it is free from governmental control. And, indeed, cryptocurrencies have operated largely outside of existing regulatory systems—giving rise to a Wild West mentality. The technology's boosters claim that "[c]ryptocurrency removes this need to trust someone by incentivizing every actor in the network to not

---

333. *Id.*

334. Akshay Makadiya, *A Breakdown of Cryptocurrency 'Pump and Dump'*, BTCMANAGER.COM (Jan. 24, 2018 0:30) https://btcmanager.com/breakdown-cryptocurrency-pump-dump/.

335. *Id.*

336. *See* Bruno, *The Anatomy of a Pump & Dump Group*, BITFALLS (12/01/2018), https://bitfalls.com/2018/01/12/anatomy-pump-dump-group/.

337. *See Pump But Never Dump*, PUMPMYCOIN, https://pumpmycoin.com/ (last visited Oct. 26, 2018). Pumpmycoin self-describes as "a cryptocurrency voting community that will choose the next coin to pump." Where Pumpmycoin claims to differ from "other pump and dump scam/groups" is that this group "maintain[s] its uptrend to make sure that our community members are satisfied with their gains." *Id.*

338. *@PumpandDumpKing Bio*, TWITTER, https://twitter.com/pumpanddumpking (last visited Oct. 26, 2017) ("I will tweet out which coin will be pumped on binance. Join my personal pump and dump group below !!!").

339. *Pump and Dump Cryptocurrency List*, WALLET INVESTOR, https://walletinvestor.com/pump-and-dump (last visited Oct. 26, 2018).

340. Ryan Mac, *Bitcoin Scammers Are Using this App to Fleece People*, BUZZFEED (Jan. 25 2018), https://www.buzzfeednews.com/article/ryanmac/cryptocurrency-scammers-are-running-wild-on-telegram ("[CryptoCallz administrator Maxwell Anderson] acknowledged that '[i]t is an unfortunate situation for anyone left holding the bags,' but noted that as long as his group members saw consistent profits they weren't particularly worried about others getting hurt.").

debase the currency[341] and not commit fraud."[342] Yet, frauds that leverage the aura of cryptocurrency to scam would-be investors are common.[343] Wildly fluctuating values driven by speculation, along with the possibility of dirty deals, undermine the idea that one can view cryptocurrency as "trustless."

Governments are increasingly exerting control over various aspects of cryptocurrencies, sometimes with serious ramifications for the expectations of users. Bitcoin originated as a cryptocurrency. There are quite a few retailers, mostly small and online that accept bitcoin.[344] However, cryptocurrency's touted anonymity has a dark side—it has been used to evade taxes, launder money and trade illicit goods.[345] For that reason, cryptocurrencies have drawn the scrutiny of regulators around the world who are concerned that cryptocurrencies facilitate illegal activities ranging from drug peddling to terrorism to child pornography on the so-called Dark Web.[346]

In the United States, the Department of Justice and the Treasury Department's Financial Crimes Enforcement Network (FinCEN) have used anti-money-laundering provisions of the Bank Secrecy Act to go after cryptocurrency exchanges engaged in illegal activities.[347] In January 2017, the

---

341. The author of this particular claim uses the following parable as an example: "The buyer or seller of goods and services in the transaction must make the same assumptions you do; if 1 cow is worth 100 dollars today and 1000 dollars tomorrow, why would you sell 1 cow today?" Chia, *supra* note 22. Yet, $100 today, $1000 tomorrow (and $10 the day after) is a pretty good description of the price fluctuations cryptocurrencies routinely experience.

342. *Id.*

343. *See SEC Charges Texas Man With Running Bitcoin Denominated Ponzi Scheme*, SEC (July 23, 2013), https://www.sec.gov/news/press-release/2013-132.

344. Some big players like Virgin, Overstock.com and Bloomberg are on this list. Jonas Chokun, *Who Accepts Bitcoin as Payment? List of Companies, Stores and Shops*, 99BITCOINS, https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ (last updated September 13, 2018). However, bitcoin reportedly made up only 0.0002% of Overstock's revenues in 2016-17. Jamie Toplin, *Merchants Aren't Accepting Bitcoin*, BUS. INSIDER (Jul. 14, 2017 12:12PM), http://www.businessinsider.com/merchants-arent-accepting-bitcoin-2017-7. Subway is also on this list, but after a video of a reporter trying, and failing, to pay with bitcoin went viral, Subway issued a statement that "Each local Subway is independently owned and operated and it is the individual franchisee's decision to accept this form of payment. We are not aware of any restaurants currently accepting this payment." Emmanuel Ocbazghi, Graham Flanagan & Sara Silverstein, *I Spent A Day Trying to Pay for Things With Bitcoin and a Bar of Gold*, BUS. INSIDER (Oct. 24, 2017 11:15AM), http://www.businessinsider.com/trying-to-pay-for-things-with-bitcoin-price-gold-2017-10.

345. *See* Tristan Greene, *Study: 44% of Bitcoin transactions are for illegal activities*, TNW (Feb. 7, 2018), https://thenextweb.com/cryptocurrency/2018/02/07/study-44-of-bitcoin-transactions-are-for-illegal-activities/.

346. Aatif Sulleyman, *Bitcoin Price is so High Because Criminals are Using it For Illegal Trades, Research Suggests*, INDEPENDENT (Wednesday 24 January 2018 11:39), https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html.

347. *See Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies*, FINANCIAL CRIMES ENFORCEMENT NETWORK (March 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

operators of cryptocurrency exchange Coin.mx pled guilty to multiple felonies associated with bank fraud.[348] Six months later, FinCEN settled money laundering charges against filed cryptocurrency exchange BTC-e for $110 million.[349] Perhaps the best-known case involved the criminal prosecution involving the Silk Road, an infamous Dark Web site. In 2015, its creator Ross Ulbrecht was sentenced to life in prison for multiple felony convictions stemming from his operation of the website. However, such actions barely scratch the surface. Despite the massive investigation and prosecution, Silk Road was up and running again in short order.

The United States is not alone in reacting to the illicit uses of cryptocurrency. China,[350] South Korea, India, Bolivia, Ecuador, Kyrgyzstan, Morocco and Nepal have all taken steps to outlaw, or severely restrict, the use of cryptocurrencies as a medium of exchange.[351] Japan, by contrast, is one of the few countries where cryptocurrency is legally recognized as currency.[352] After the Coincheck hack, Japan cracked down on cryptocurrency exchanges, suspending two exchanges and fining five others.[353] Merchants that accept cryptocurrency as payment still typically price their goods in fiat currency, and immediately convert any paid in cryptocurrency to fiat currency.[354]

---

348. DEPARTMENT OF JUSTICE, OPERATORS OF UNLAWFUL BITCOIN EXCHANGE PLEADS GUILTY IN MULTIMILLION-DOLLAR MONEY LAUNDERING AND FRAUD SCHEME (Jan. 9, 2017), https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-pleads-guilty-multimillion-dollar-money-laundering.

349. Assessment of Civil Money Penalty at 9, *In re* BTC-E, No. 2017-03 (Dep't of Treas., Fin. Crimes Enforcement Network, July 26, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf.

350. Saheli Roy Choudhury, *China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms*, CNBC (2:51 AM Mon., 4 Sept. 2017), https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html.

351. Amanda Razani, *Countries that Have Banned Cryptocurrency for Now*, COIN CLARITY (Dec. 19, 2017), https://coinclarity.com/countries-that-have-banned-cryptocurrency-for-now/#; Kate Rooney, *Your guide to cryptocurrency regulations around the world and where they are headed*, CNBC (March 27, 2018), https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html; *India bans cryptocurrency trades*, BBC (April 6, 2018), https://www.bbc.com/news/world-asia-india-43669730.

352. Kate Rooney, *Your guide to cryptocurrency regulations around the world and where they are headed*, CNBC (March 27, 2018), https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html.

353. Rishi Iyengar, *Japan Cracks Down on Cryptocurrency Exchanges After Massive Hack*, CNN (Mar. 8, 2018, 3:48 AM), https://money.cnn.com/2018/03/08/investing/japan-cryptocurrency-exchanges-crackdown/index.html.

354. C. Edward Kelso, *80,000 New Merchants in Europe Gain Option to Accept Crypto*, BITCOIN.COM (Mar. 27, 2018), https://news.bitcoin.com/80000-new-merchants-in-europe-gains-option-to-accept-crypto/; Utrust, *The vast_majority of merchants are still afraid to ac-*

As cryptocurrencies have entered the mainstream, supporters have attempted to shed its criminal reputation. Most new buyers do not treat their bitcoin as a means of exchange and payment. Rather, purchasers are *hodlers*—buying cryptocurrency "as a speculative investment, attracted by massive price gains."[355] Perhaps because they recognize this investor behavior, both the IRS and the SEC treat cryptocurrency as property rather than as a currency. The IRS has issued guidance specifically clarifying that it does not consider bitcoin as a currency, [356] and requiring investors to report capital gains and losses any time they transfer cryptocurrency.[357] This IRS decision has an important ramification. Any exchange of cryptocurrency for goods, services, or a fiat currency may generate a taxable gain or loss, depending on the relationship between the fair market value on the day of exchange and on the day of acquisition.[358] The IRS treats this gain or loss as ordinary income rather than a capital gain.[359] To enforce this rule, the IRS recently won a lawsuit against the cryptocurrency exchange Coinbase, requiring the company to turn over account information for 14,000 users suspected of tax avoidance.[360] The relevance of the actual legal system to cryptocurrency transactions seems to have come as a surprise to some users. Outraged customers took to social media to vent their outrage and sense of betrayal when Coinbase issued 1099-K forms to its users in January 2018.[361]

---

cept crypotcurrencies, MEDIUM (Jan. 24, 2018), https://medium.com/@UTRUST/why-the-vast-majority-of-merchants-are-afraid-to-accept-cryptocurrency-618cebaa82b8.

355. Jemima Kelly and Anna Irrera, *Bitcoin Fever Exposes Crypto-Market Frailties*, BUS. INSIDER (Dec. 13, 2017, 10:45 AM), https://www.businessinsider.com/r-bitcoin-fever-exposes-crypto-market-frailties-2017-12.

356. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (April 14, 2014) ("Q-2: Is virtual currency treated as currency for purposes of determining whether a transaction results in foreign currency gain or loss under U.S. federal tax laws? A-2: No. Under currently applicable law, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes.")

357. *Id.* ("How is virtual currency treated for federal tax purposes? A-1: For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.").

358. *Id.* ("Q-6: Does a taxpayer have gain or loss upon an exchange of virtual currency for other property? A-6: Yes. If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency.").

359. *Id.* Similarly, the IRS considers mining cryptocurrency to be a taxable event, with the virtual currency considered ordinary income and valued at the fair market value on the day of acquisition. *Id.* Miners may potentially be subject to self-employment taxes. *Id.*

360. Order Re Petition to Enforce IRS Summons at 25-26, United States v. Coinbase, Inc., No. 17-cv-01431-JSC (N.D. Cal. filed Nov. 28, 2017) (requiring Coinbase to produce names, social security numbers and other identifying information for its roughly 14,000 customers who had at least one $20,000 or greater transaction between 2013 and 2015).

361. *See* Coin_Junkie, *Coinbase has turned us all over to the IRS!!!!*, REDDIT (Feb. 1, 2018, 12:32 AM), https://www.reddit.com/r/Bitcoin/comments/7ugdng/coinbase_has_turned_us_all_over_to_the_irs/.

The Commodities Futures Trading Commission, CFTC, allowed futures trading for Bitcoin in September 2017. In December 2017, CME Group and Cboe Global Markets Inc. both launched bitcoin futures.[362] The very next month, in January 2018, the CFTC brought three fraud cases for unlawful solicitation with regard to Bitcoin futures.[363] The CFTC has brought charges related to virtual currencies before. In 2016, the agency reached a $75,000 settlement with Bitfinex for engaging in what the agency found to be "illegal, off-exchange commodity transactions" and for failure to register as a futures commission merchant.[364]

The SEC has also gotten into the cryptocurrency enforcement game. The agency recently refused to approve three cryptocurrency exchange traded fund (ETF) proposals, citing concerns over valuation and verification.[365] Previously the SEC classified the now-defunct DAO smart contract as a security,[366] and took its first action to halt an ICO it deemed to be a scam.[367] The SEC also issued a cease and desist order to at least one other company,

362. The Cboe January 2018 futures contracts were settled on January 17, 2018 for $10,900, a price set by a that day's 4:00 PM Gemini Exchange bitcoin auction. CBOE GLOBAL MARKETS, CBOE CONDUCTS FIRST SETTLEMENT OF CBOE BITCOIN FUTURES (Jan. 17, 2018), http://ir.cboe.com/~/media/Files/C/CBOE-IR-V2/press-release/2018/cboe-xbt-settlement.pdf.

363. In the first case, the CFTC charged Patrick K. McDonnell of Staten Island, N.Y., and his company CabbageTech with soliciting customer funds for virtual-currency trading advice and other trading services but transferring the funds into personal bank accounts without providing the promised services. On August 23, 2018, the CFTC obtained a verdict permanently enjoining the defendants from trading digital assets and fining them over $1.1 million for "egregious intentional violations" of federal law. Mark Emem, *'Vicious' Crypto Fraudster Fined $1.1 Million, Slapped with Lifetime Trading Ban*, CCN (Aug. 25, 2018, 12:57 AM), https://www.ccn.com/vicious-crypto-fraudster-fined-1-1-million-slapped-with-lifetime-trading-ban/. In the second case, the CFTC alleged that Colorado resident Dillon Michael Dean and his company Entrepreneurs Headquarters Ltd. engaged in a "Ponzi-style" scheme to solicit $1.1 million in bitcoin from more than 600 customers by telling them that their money would be pooled and invested. The details of the third case remained under seal as of Thursday night. Gabriel T. Rubin, *CFTC Alleges Fraud in Three Virtual-Currency Cases*, WALL ST. J. (Jan. 19, 2018, 11:49 AM), https://www.wsj.com/articles/cftc-alleges-fraud-in-three-virtual-currency-cases-1516338060.

364. *In re* BFNXA d/b/a Bitfinex, CFTC No. 16-19, 2016 WL 3137612 (June 2, 2016).

365. Order Disapproving a Proposed Rule Change to ProShares Bitcoin ETF and the ProShares Short Boitcoin ETF, Exchange Act Release No. 34-83904 (Aug. 22, 2018); Order Disapproving a Proposed Rule Change to GraniteShares Bitcoin ETF and the Granite Shares Short Bitcoin ETF, Exchange Act Release No. 34-83913 (Aug. 22, 2018); Order Disapproving a Proposed Rule Change to Direxion Daily Bitcoin Bear IX Shares, Exchange Act Release No. 34-83912 (Aug. 22, 2018). Just one month earlier, the SEC had rejected a similar petition from the Winklevoss Bitcoin Trust. Order Setting Aside Action, Exchange Act Release No. 34-83723, 83 Fed. Reg. 37579 (Aug. 1, 2018).

366. Report of Investigation, Exchange Act Release No. 81207 at 11 (July 25, 2017).

367. Paul Vigna, *SEC Targets Initial Coin Offering Scam*, WALL ST. J. (Dec. 4, 2017, 11:51 AM), https://www.wsj.com/articles/secs-cyber-unit-charges-canadian-firm-with-coin-offering-fraud-1512400168.

halting its ICO as an unregistered security.[368] The SEC also created a fake ICO with a website spoofing a scam ICO in order to warn investors about the risks associated with ICOs.[369] However, regulatory actions are few and far between. It is unclear where and how government will decide to intervene in cryptocurrency markets, and even less clear whether those interventions will be successful in protecting the public.

Private actors are also beginning to exert influence over cryptocurrencies. Facebook recently banned cryptocurrency ads. Major credit card issuers Capital One, Discover, J.P. Morgan Chase, Bank of America and Citigroup have all banned cryptocurrency purchases by their credit card customers.[370] British banks Lloyds Banking Group and Virgin have followed suit, as has Canada's TD Bank.[371] The banks cite concern over volatility as a major justification for this policy.[372] However, it is worth noting that many of these institutions also identify competition from cryptocurrency as a potential business risk.[373] Prior to the ban, 18% of cryptocurrency purchasers reported using credit cards for their purchases, with nearly a quarter of those purchasers reporting that they had not paid off the balance.[374]

V. CONCLUSION

A significant degree of trust is simply inescapable.[375] As blockchain expert Preethi Kasireddy noted, "Blockchain governance is an incredibly tricky

368. SEC, COMPANY HALTS ICO AFTER SEC RAISES REGISTRATION CONCERNS (Dec. 11, 2017), https://www.sec.gov/news/press-release/2017-227.

369. HOWEYCOINS, https://www.howeycoins.com/index.html (last visited Nov. 26, 2018). *See also* SEC, THE SEC HAS AN OPPORTUNITY YOU WON'T WANT TO MISS: ACT NOW! (May 16, 2018), https://www.sec.gov/news/press-release/2018-88.

370. Evelyn Chang, *J.P. Morgan Chase, Bank of America & Citi Bar People from Buying Bitcoin with a Credit Card*, CNBC (Feb. 3, 2018, 7:47 AM), https://www.cnbc.com/2018/02/02/jpmorgan-chase-bank-of-america-bar-bitcoin-buys-with-a-credit-card.html.

371. John Egan, *Buy Bitcoin With Credit Cards? Big Banks Say 'No'*, CREDITCARDS.COM (Feb. 6, 2018), https://www.creditcards.com/credit-card-news/bitcoin-credit-card-issuers-bar-purchases.php.

372. *See id.*

373. *See, e.g.*, Bank of America Corp., Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (10-K) at 15 (Feb. 22, 2018) (noting that "clients may choose to conduct business with other market participants who engage in business or offer products in areas we deem speculative or risky, such as cryptocurrencies" and that increased competition from cryptocurrency "may negatively affect our earnings by creating pressure to lower prices or credit standards on our products and services requiring additional investment to improve the quality and delivery of our technology and/or reducing our market share, or affecting the willingness of our clients to do business with us.").

374. Mike Brown, *Poll: Some Investors Use a Credit Card to Buy Bitcoin and then Carry Over the Balance*, LENDEDU (Aug. 18, 2018), https://lendedu.com/blog/bitcoin-and-credit-cards/.

375. Joel Valenzula, *Trustlessness is Effectively a Myth*, DASH FORCE NEWS (Oct. 8, 2017), https://www.dashforcenews.com/trustlessness-effectively-myth/.

problem and finding a balance between centralized and distributed control will be essential to maintaining everyone's trust in the system."[376] The notion that one can trust in the immutability of the blockchain spreads a halo of trust over the universe of cryptocurrencies. Combined with the lack of government oversight, this trust halo makes cryptocurrencies "almost a perfect vehicle for scams."[377] The blockchain rhetoric of a trustless system obscures the many places at which a market participant must trust another, sometimes dubious, actor. As one commenter noted, "[e]verything requires trust. Aside from tautologies, it's impossible for you to verify anything without putting your trust somewhere."[378] Cryptocurrencies currently relocate that trust from regulators and the commercial actors they oversee, to nameless, faceless actors accountable to no one. Moreover, those cryptocurrency interactions are typically not mediated by the conventional regulatory signifiers of trust in financial transactions.

Ironically, the success of "trustless" cryptocurrency depends largely on trust. Indeed, blockchain, the limited supply of coins, the lack of centralized control—the very things that purportedly make it a system that does not require trust—are all touted as reasons to trust this technology. For example, the cryptocurrency Dash claims to be a form of decentralized governance run by its masternodes. Its website contains advice for how to start a "hosted masternode."[379] Yet Dash's explanation of its governance system also proclaims that "[e]very masternode operator establishes a bond of trust and a social contract with the network in which she is bound to contribute to the development and maintenance of the ecosystem she benefits from."[380] As crypto bull, Michael Novogratz stated that, "Bitcoin is based on an amazing technology. There's a limited supply of it, people are trusting it."[381]

At the same time, the lack of trustworthiness in cryptocurrency has created something of a crisis. As *ADustedEwok* noted, "No matter what, at some point your money will be in the hands of a 3rd party. At which point

376. Kasireddy, *supra* note 128.

377. *See* Nathanial Popper, *As Bitcoin Bubble Loses Air, Frauds and Flaws Rise to Surface*, N.Y. TIMES (Feb. 5, 2018), https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html.

378. Haseeb Qureshi, *Why Bitcoin is Not Trustless*, HACKER NOON (Dec. 18, 2017), https://hackernoon.com/bitcoin-is-not-trustless-350ba0060fc9.

379. *Hosting Services*, DASH https://docs.dash.org/en/latest/masternodes/hosting.html#starting-a-hosted-masternode (last visited Oct. 27, 2018).

380. *Understanding Dash Governance*, DASH, https://docs.dash.org/en/latest/governance/understanding.html (last visited Oct. 27, 2018).

381. Jeff Cox, *Novogratz: Bitcoin is 'Digital Gold' and Will End the Year at $10,000*, CNBC (Nov. 21, 2017, 11:27 AM), https://www.cnbc.com/2017/11/21/novogratz-bitcoin-is-digital-gold-and-will-end-the-year-at-10000.html.

it's vulnerable."[382] This vulnerability has created insecurities like those found in a recent Reddit thread, discussing an announced theft of roughly $2 million in bitcoin from an individual's wallet. The conversation ranged from worried owners who had "always trusted" the service in question,[383] to others advising "DO NOT TRUST ANYONE" [384] to cynics doubting any theft had happened at all.[385] The original poster bemoaned "I don't know what to trust,"[386] prompting a user to advise, "I personally put my trust in hardware wallets."[387]

In response to the *NiceHash* hack, a poster called *Showthatflop* expressed what is a fairly common sentiment when s/he posted "How do we know that they were hacked for real and it wasn't a planned scam since the begging [sic] and now EVERYTHING is a hack? How do you trust them or trust someone?"[388] The message is clear—users are on their own. As one reddit poster chastised those sharing their losses: "It's your job to secure your funds. It can be done easily. It was your decision to trust people who didn't deserve your trust, either because they weren't competent enough to secure their bitcoins or because they ran with your money[389] Or as another commenter noted, "This decentralized nature of the bitcoin network is not without consequences—the main one being that if you screw up, it's your own damn problem."[390]

---

382. ADustedEwok, Comment to *NiceHash was hacked. Looks like ~$60M stolen.*, REDDIT (Dec. 6, 2017, 6:11 PM), https://www.reddit.com/r/Bitcoin/comments/7i0u82/nicehash_was_hacked_looks_like_60m_stolen/.

383. DevilsAdvocate9x1, Comment to *My 387 Bitcoins got hacked and stolen!*, REDDIT (Oct. 30, 2017, 10:09 AM), https://www.reddit.com/r/Bitcoin/comments/79nbei/my_387_bitcoins_got_hacked_and_stolen/.

384. KIND_REDDITOR, Comment to *My 387 Bitcoins got hacked and stolen!*, REDDIT (Oct. 30, 2017, 10:20 AM), https://www.reddit.com/r/Bitcoin/comments/79nbei/my_387_bitcoins_got_hacked_and_stolen/.

385. BitderbergGroup, Comment to *My 387 Bitcoins got hacked and stolen!*, REDDIT (Oct. 30, 2017, 10:34 AM), https://www.reddit.com/r/Bitcoin/comments/79nbei/my_387_bitcoins_got_hacked_and_stolen/.

386. [deleted], Comment to *My 387 Bitcoins got hacked and stolen!*, REDDIT (Oct. 30, 2017, 6:18 PM), https://www.reddit.com/r/Bitcoin/comments/79nbei/my_387_bitcoins_got_hacked_and_stolen/.

387. nibbl0r, Comment to *My 387 Bitcoins got hacked and stolen!*, REDDIT (Oct. 31, 2017, 4:17 AM),https://www.reddit.com/r/Bitcoin/comments/79nbei/my_387_bitcoins_got_hacked_and_stolen/.

388. Showthatflop, Comment to *NiceHash was hacked. Looks like ~$60M stolen.*, REDDIT (Dec. 6, 2017, 4:55 PM), https://www.reddit.com/r/Bitcoin/comments/7i0u82/nicehash_was_hacked_looks_like_60m_stolen/.

389. Exotemporal, Comment to *NiceHash was hacked. Looks like ~$60M stolen.*, REDDIT (Dec. 6, 2017, 9:47 PM), https://www.reddit.com/r/Bitcoin/comments/7i0u82/nicehash_was_hacked_looks_like_60m_stolen/.

390. Mark Frauenfelder, *'I Forgot My Pin': An Epic Tale of Losing $30,000 in Bitcoin*, WIRED (Oct. 29, 2017, 5:00 PM), https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/.

The subtext to these discussion threads is that everyone is always vulnerable; predators are everywhere, and the slightest mistake is enough to create catastrophe. And there is no recourse. It is only after catastrophe has occurred that many cryptocurrency users realize just how many nameless, unaccountable people they had blithely trusted during their interactions with the much-touted trustless blockchain system. Their new world order resembles *Lord of the Flies* far more than *Utopia*. A finance blogger who goes by the name Mr. Money Moustache summed it up nicely when he wrote, "Government-issued currencies have value because they represent human trust and cooperation. There is no wealth and no trade without these two things . . . There are no financial instruments that will protect you from a world where we no longer trust each other."[391]

391. *Why Bitcoin is Stupid*, MR. MONEY MUSTACHE (Jan. 2, 2018), http://www.mrmoneymustache.com/2018/01/02/why-bitcoin-is-stupid/.