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]

Imagine a globally accepted currency that works with lightning speed,[3] and costs virtually nothing.[4] Now imagine that this currency is open-source and decentralized.[5] Then add a recording feature that makes 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 manipulation by central banks or financial institutions.[7] This is the basic pitch for bitcoin[8] and the thousands of alt-coin cryptocurrencies that have followed in its wake. It is not hard to find true believers touting each of these supposed cryptocurreny traits as though they were gospel.

The term '*hodl*'[9] capture some of the evangelical fervor of bitcoin's proponents. It stands for long-term commitment to cryptocurrencies in the face of wild fluctuations. The thread *"why are all cryptos dropping in price'* on *Bitcointalk.com* is an example. Comment after comment

---

[1] Kirsten Grind, *Let Me Tell You Some More About Bitcoin, Hello? Hello?,* WALL S TREET JOURNAL (January 19, 2018) (quoting Doug Scribner, 50, of Edina, Minn).

[2] Fred Imbert, *JPMorgan CEO Jamie Diamon Says Bitcoin is a 'Fraud' that Will Eventually Blow Up*, CNBC.com (September 12, 2017) 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

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

[4] *See e.g.*, Jerry Brito and Andrea Castillo, Bitcoin: A Primer for Policymakers 15 (2016) (asserting that "because there are no third-party intermediaries, bitcoin transactions can be cheaper and quicker than traditional payment networks."); *see also What is Bitcoin,* COINDESK.COM https://www.coindesk.com/information/what-is-bitcoin/("The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.")

[5] *Bitcoin is an Innovative Payment Network and a New Kind of Money,* BITCOIN.ORG https://bitcoin.org/en/.

[6] *Bitcoin for Individuals,* BITCOIN.ORG https://bitcoin.org/en/bitcoin-for-individuals.

[7] Patrick Mansfield, *A Bitcoin Guide: A Brief History, How to Buy, and the Latest Quote,* USCF.com https://www.usconsumerfinance.com/bitcoin-information

[8] For a more expansive discussion of "the promise of bitcoin," *see* Lawrence Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox,* 20 RICHMOND J. L. & TECH. 1, 58-71 (2014).

[9] What's HODL? Reditt.com (July 20, 2014) https://www.reddit.com/r/Bitcoin/comments/2b8t78/whats_hodl/; *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. *I am Hodling,* BITCOIN FORUM (Dec. 23, 2013) *https://bitcointalk.org/index.php?topic=375643.0?red*

advised the original poster to relax and wait for the inevitable bounce as the market returns to 'normal.'[10]

True believers posit a world with virtually limitless applications for the block chain—the technology at the core of cryptocurrencies. They suggest that cryptocurrencies will replace fiat currencies, including 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,[11] and expensive,[12] because the core technology, called a blockchain,[13] scales poorly.[14] These technological issues, which may or may not be fixable, have repeatedly made headlines. However, the really interesting divergence between pitch and reality has to do with the purported consequences of decentralization[15]—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."[16] In the 2008

---

[10] *Why are all cryptos dropping in price?* BITCOINTALK.COM (Feb. 1, 2018)

[1111] In July 2017, average transaction time was 116 minutes. *See*, *Alex Lielacher, How Long Should My Bitcoin Transaction Take?* BITCOIN MARKET JOURNAL (July 6, 2017). In February 2017, transactions ranged from 20 minutes to 600 minutes, depending on the day. https://blockchain.info/charts/avg-confirmation-time?timespan=30days.

[12] Bitcoin is what one user described as a "pay to play protocol." Brianddk, *Average Confirmation Times* REDDIT R/BITCOIN (undated) 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. Fluffy 1337, *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.Com R/btc 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 (March 2, 2016) https://localbitcoins.com/forums/#!/general-discussion:i-have-issues-with-my-bitco.

[13] Blockchains are discussed in detail in part__ infra.

[14] Darryn Pollock, *SEgWit2x's Failure Confirms Bitcoin's Status as Digital Gold,* COINTELEGRAPH.COM (Nov. 14, 2017) (quoting Morgan Stanley analysts).

[15] *See*, *What is Bitcoin*, *supra* n. 4 ("bitcoin's most important characteristic, and the thing that makes it different to conventional money, is that it is *decentralized*. No single institution controls the bitcoin network. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.")

[16] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1, https://bitcoin.org/bitcoin.pdf. The protocol behind the blockchain was first described in 1998 by Wei Dai. Wei Dai, B-Money, http://www.weidai.com/bmoney.txt.

whitepaper that launched Bitcoin, Satoshi Nakamoto criticized existing electronic payment systems for requiring a trusted third-party.[17] Nakamoto wrote at the depths of the 2008 financial crisis, when trust in the ability of governments and banks to manage the economy was at its nadir.[18] A decade later, the so-called 'trustless' nature of cryptocurrency is still a big selling point. For example, cyptocurrency news site Coindesk offers a Bitcoin 101 which touts that: "You don't need to trust anyone else."[19] Coindesk goes 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."[20] With the blockchain, by contrast, cryptocurrency's boosters claim that trust, along with centralization, is no longer necessary.[21]

Depending on who you ask, Bitcoin, and cryptocurrencies more generally are "world-changing"[22] and "the wave of the future,[23]" or a mania,[24] 'more religion than asset,'[25] and a fraud.[26] 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

---

[17] Satoshi Nakamoto, *supra* n. 16 at 1.
[18] *See, Distrust, Discontent, Anger and Partisan Rancor*, PEW RESEACH CENTER http://www.people-press.org/2010/04/18/section-1-trust-in-government-1958-2010/ (noting that an October 2008 poll found that only 17% of respondents trusted the government to do what was right.)
[19] https://www.coindesk.com/information/why-use-bitcoin/
[20] https://www.coindesk.com/information/why-use-bitcoin/
[21] *See e.g.*, Bryan Chia, *What is Cryptocurrency? (Part 2: Trustless, Decentralized & Immutable)*, MEDIUM (Nov. 27, 2017)
[22] *See generally, The Rise and Rise of Bitcoin http://bitcoindoc.com/.*
[23] Mike Ayers, *'Shark Tank' Investor Robert Herjavec Has a Bold Prediction for the Future of Cryptocurrency,* MONEY (Feb. 8, 2018). 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." *Everyone is Getting Hilariously Rich and You're Not, https://www.nytimes.com/2018/01/13/style/bitcoin-millionaires.html* (quoting James Fickel).
[24] Felix Allen, '*Absolutely Bananas' Bitcoin Bubble Fears as Cryptocurrency Soars Toward Record $10,000 with Half a Million New Investors a Day*, THE SUN (Nov. 28, 2017).
[25] A.J. Dellinger, *Bitcoin, Cryptocurrency Predictions 2018: What Mark Cuban Thinks About the Future of the Currency*, INTERNATIONAL BUSINESS TIMES (January 21, 2018) http://www.ibtimes.com/bitcoin-cryptocurrency-predictions-2018-what-mark-cuban-thinks-about-future-coins-2643150 (quoting Marc Cuban). at
[26] *See* Imbert, *supra* n. 2. To be fair, Jamie Diamon has since said that he regrets calling bitcoin a fraud. *See* Tae Kim,*J.P. Morgan CEO Jaime Diamon Says He Regrets Calling Bitcoin a Fraud,* USA Today (January 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/

cryptocurrency. Indeed, the combination of rapidly rising cryptocurrency values, anonymity, and lack of regulation make cryptocurrency exchanges "natural targets" for theft.[27] As of late 2017, Reuters estimated that 980,000 coins, worth up to $15 billion had been stolen between 2011 and 2017.[28] And that was before the January 2008 $534 million hack of cryptocurrency exchange CoinCheck.[29]

This article interrogates the claim that trust can be replaced with blockchain technology. It begins with an overview of the current economics of cryptocurrency. Part II then gives a brief overview of the role that trust plays in a financial market, 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 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 users should understand that many legal protections they take for granted may not apply when purchasing cryptocurrency.

I. Overview

[27] 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.
[28] Jim Finkle and 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
[29] Guarav Sharma, *'Crypto Heist: Coincheck Hack Could Be the World's Biggest Every CryptoCurrency Theft*, FORBES (Jan. 27, 2018); *How to Steal $500 Million in Cryptocurrency*, FORTUNE (January 31, 2018) http://fortune.com/2018/01/31/coincheck-hack-how/

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 decentralized currency."[30] There are currently over 1500 different cryptocurrencies,[31] twenty-five of which currently have market capitalizations above $1 billion. [32] New coins are launched almost daily. That said, the three largest, Bitcoin, Etherium, and Ripple, account for approximately 2/3 of the overall cryptocurrency market,[33] with Bitcoin alone amounting to 35% of the market.[34]

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 with the embedded message "Chancellor on the brink of second bailout of banks."[35] Bitcoin began as an oddity—a small niche product among tech geeks, drug dealers,[36] and Hayek enthusiasts.[37] Since then, cryptocurrency has gone mainstream.

---

[30] Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* 1 (2016) (making the libertarian case for what the authors call 'permissionless innovation,' meaning no regulation of bitcoin.)

[31] 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.

[32] *Id*.

[33] Roughly $303 billion on February 27, 2018. Cryptocurrency Market Capitalization, https://coinmarketcap.com/all/views/all/.

[34] Valued at roughly $180 billion on February 27, 2018. *Id.* A year ago, bitcoin had about 85% market share of the cryptocurrency sector. *Bitcoin Transaction Volume is Puzzling Investors*, FORTUNE (March 2, 2018).

[35] Joshua Davis, *The Crypto-Currency*, NEW YORKER (Oct. 10, 2011). Indeed, the 2008 bitcoin White Paper, 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." Nakamoto, *supra* note 16 at 2.

[36] 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.COM (Jan. 11, 2018); Rebecca Camber and Chris Greenwood, *Drug Dealers Use Bitcoin Cashpoints to Launder Money*, DailyMail.com (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*, COINTELEGRAPH.COM (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*, COINTELEGRAPH.COM (Oct. 5, 2017); Andy Greenberg, *Monero, the Drug Dealer's Cryptocurrency of Choice, is on Fire*, Wired.com (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.com (Dec. 12, 2017)

[37] 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 (Oct. 2012). For a description of these views, *see* FREDERICK HAYEK,

The first known commercial use of bitcoin was the legendary 2011 purchase of two Papa John's pizzas for 10,000 bitcoins.[38] In January 2013, bitcoin was valued at $13 per coin,[39] making those pizzas worth $130,000. 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 $19,786.30 on December 17, 2017.[40] That gave bitcoin an overall market valuation of over $300 billion (for perspective, that figure is equivalent to Bank of America's market capitalization in December 2017).[41] The party was short-lived. Bitcoin ended 2017 at $14,290, down more than $5000 from its high of a few weeks earlier, but still a gain of 1400% over the course of the year.[42] That outsized gain did not even put bitcoin on Top 10 list for best cryptocurrency performers of 2017. [43] 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%.[44]

The market valuation for cryptocurrencies as a class peaked on January 10, 2018 at $728 billion[45]. 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

---

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*

[38] Julie Bort, *May 22 is Bitcoin Pizza Day Thanks to these Two Pizzas Worth $5 Million,* BUSINESS INSIDER (May 21, 2014). 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 a pizza. For a list of the companies that currently accept cryptocurrency, *see* *https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/*

[39] *Bitcoin, The Nationless Electronic Cash Beloved by Hackers, Bursts into Financial Mainstream,* FOXNEWS.COM (April 11, 2013) http://www.foxnews.com/tech/2013/04/11/bitcoin-electronic-cash-beloved-by-hackers.html

[40] 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/

[41] Bank of America Market Cap as of December 13, 2017, https://ycharts.com/companies/BAC/market_cap

[42] Adam Shell, *Bitcoin Price: Digital Currency Had Big Swings in 2017,* USA TODAY (Dec. 29, 2017)*; Bitcoin Futures Trade Near $20,000 in Debut on World's Biggest Exchange,* MARKETWATCH.COM (Dec. 18, 2017) https://www.marketwatch.com/story/bitcoin-futures-debut-on-worlds-biggest-exchange-at-20000-then-pull-back-2017-12-18?mg=prod/accounts-mw.

[43] Joon Ian Wong, *Here are the Top 10 CryptoAssets of 2017 (and Bitcoin's 1000% 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/.

[44] *Id.*

[45] For perspective that is roughly the GDP of the Netherlands. *See* ttps://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2016&start=2016&view=bar&year_high_desc=true

Greece."[46] He then went on to project that if cryptocurrencies reached his predicted target, they would become the 11th largest market.[47] Instead, just three weeks later, the combined market value of all cryptocurrencies had dropped by more than 50% to just under $360 billion.[48]

On February 6, 2018 bitcoin plummeted even further, to a low of $5920.[49] In the process, bitcoin's fall erased more than $55 billion in ascribed value[50]--roughly the market capitalization of Aetna.[51] Since then, bitcoin has bounced around between $7500 and $10,000.[52] 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 $23 billion in market cap—roughly the market capitalization of BestBuy.[53] In late June and early July of 2017, bitcoin's valuation had plunged 31%.[54] Indeed, one self-described bitcoin bull admits that the currency is "prone to 40% corrections."[55] Other cryptocurrencies are similarly volatile. For example, Ethereum, the largest alt- cryptocurrency, rose to $1302 in January 2018, before plummeting to $697.86 in early February.[56] 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."[57] Yet, even as Ethereum fell 31% in three days,[58] and

---

[46] *How to Approach CryptoCurrencies,* Bloomberg (Jan 24, 2018) https://www.youtube.com/watch?v=otf3-x0pKhQ (Tom Lee)
[47] *Id.*
[48] For perspective, this figure is slightly larger than the GDP of the United Arab Emirates. *Id.* By late February, the total market valuation of cryptocurrency had rebounding partially, to $456 billion. Cryptocurrency Market Capitalization, https://coinmarketcap.com/all/views/all/.
[49] 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.com (February 5, 2018).
[50] Arjun Kharpal, *Cryptocurrency Market Could Hit $1 Trillion This Year With Bitcoin Surging to $50,000 Experts Say,* CNBC.com (Feb. 7, 2018).
[51] https://ycharts.com/companies/AET/market_cap.
[52] Bitcoin price, https://charts.bitcoin.com/chart/price.
[53] *Bitcoin's Bear Market, https://www.youtube.com/watch?v=W6d9PiZ5ANs*
[54] Jeff John Roberts, *Five Big Bitcoin Crashes: What We Learned,* FORTUNE (Sept, 18, 2017)
[55] Adam Shell, *Bitcoin Price: Digital Currency Had Big Swings in 2017,* USA TODAY (Dec. 29, 2017) (quoting Tom Lee, co-founder of Fundstrat Global Advisors. For a tour of bitcoin's early wild swings in valuation, *see* Timonthy Lee, *An Illustrated History of Bitcoin Crashes,* FORBES (April 11, 2013) *https://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/#6c6062d44039*. For a similar description of the cryptocurrency's more recent swings, *see*
[56] Ether/USD Coinbase, https://www.cnbc.com/quotes/?symbol=ETH.CB%3D (last visited February 7, 2018).
[57] Vitalik Buterin, Tweet Feb. 17, 2017 https://twitter.com/VitalikButerin?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Ffortune.com%2F2018%2F02%2F19%2Fethereum-price-ether-vitalik-buterin%2F

bitcoin remained nearly 17% lower for February, and 39% lower for 2018 (so far),[59] its promoters project a new bull run that will see cryptocurrencies cross the $1 trillion mark.[60]

II. The Fiat Money System

The back of all United States currency carries the motto "In God We Trust." Yet, people using that money do so with 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" challenged the scope of barter systems, giving rise to the need for a more flexible unit of exchange. At first salt, metals (like gold or silver), or wampum filled this need—serving as a store of value and a unit of exchange. But the dangers and logistics associated with storage and transportation presented thorny problems that limited the utility of these items. Traders shifted to receipts that could be exchanged as representatives of the underlying commodities. ADD HERE ABOUT GOVERNMENTS.

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. 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.[61] The back of each dollar read "this note is legal tender for all debts, public and private, and is redeemable in lawful money at the United States Treasury or at any Federal Reserve Bank." On June 5, 1933, President Roosevelt signed House Joint Resolution 192, the so-called 'Gold Repeal Resolution' into law. [62] This Joint Resolution declared that obligations purporting to give the right to require payment in gold were against public policy.[63] The Resolution then went on to announce that any such debts would now be payable in "any coin or currency which

---

[58] David Zeiler, *Why the Ethereum Drop is Not as Bad as It Seems,* MONEYMORNING.COM (Sept. 5, 2017)
[59] *Id.*
[60] Kharpal, *supra,* n.50.
[61]
[62] House Joint Resolution 192, 48 Stat. 112 (June 5, 1933). http://www.educationcenter2000.com/HJR_192_73rdCongress.html
[63] *Id.* at (a).

at the time is legal tender for public and private debts."[64] By fiat, the United States changed the terms of by which currency issued by the United States was held.[65]

To be considered money, a currency must fulfill three roles: as a store for value, as a unit of account and 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[66] 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."[67] 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, only by its power to purchase goods or services in the economy.[68] 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 replaced by law and trust"[69] 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

---

[64] *Id.*

[65] Subsequently, Congress enacted a law which 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).

[66] I am indebted to N. Gregory Mankiw for this example. *See* N. Gregory Mankiw, *Brief Principles of MacroEconomics* 220 (2014)

[67] This language comes from the Coinage Act 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.")

[68] Though no gold, much to the dismay of

[69] Markus Iofcea, Kostas Viskanta and Kevin Kohler, *The Future of Currencies*, FORBES (Oct. 28, 2016) https://www.forbes.com/sites/ubs/2016/10/28/the-future-of-currencies/#551c41a623ef.

possible.[70] Without trust in the banking system, such transactions become extremely risky. Similarly, without trust in the legitimacy of a currency as a holder of value and a medium of exchange, the state's social institutions disintegrate. The Federal Reserve Banks are tasked with maintaining the stability of the money supply in order to cultivate this trust.

Indeed, collapse of trust in the monetary system is often a sign that a social system is under severe strain. This was the situation after Lehmen Brothers, Bear Stearns, AIG imploded, and other major "too big to fail" banks needed a federal bailout. During the depth of the resulting financial crisis, Nakamoro wrote: "The 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."[71]

There is no question that the 2008 financial crisis badly damaged trust in banks, and in the regulators who oversee them.[72] Things have gotten worse. Since the Trump administration began, the United States has experienced the steepest decline of trust ever measured.[73] 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.[74] Indeed, among the informed public, the United States has crashed from sixth place to dead last on the Edelman Trust Barometer, a global

[70] Some suggest that "law cannot produce trust" *see*, Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 556 (2001) while others insist that trust requires law. Tamar Frankel, *Trusting and Non-Trusting*, 81 B.U. L. REV. 457, 459 (2001).
[71] Satoshi Nakamoro, *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUNDATION (Feb. 11, 2009) http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source
[72] David Leonhardt, Lesson from a Crisis: When Trust Vanishes, Worry, N.Y TIMES, Oct. 1, 2008, at A1; Sarah Knapton, Financial Crisis: Home Safe Sales Soar as Trust in Banks Collapses, TELEGRAPH, Oct. 10, 2008, http://www.telegraph.co.uk/finance/ personalfinance/savings/3163645/Financial-crisis-Home-safe-sales-soar-as-trust-in-bankscollapses.html; Theresa Tedesco, Trust in Short Supply During Financial Crisis, FIN. POST, Sept. 17, 2008, http://www.financialpost.com/story.html?id=798071
[73] 2018 Edelman Trust Barometer, A World of Distrust: 6 General Public, 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).
[74] *Id.* at 7, Informed Public (reporting a 23% decline in trust in the United States).

trust index that ranks 28 countries.[75] 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.[76] While this recent decline in trust has been both steep and profound,[77] it is part of a larger trend. Indeed, 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.[78]

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.[79] Niklas Luhmann asserted that to trust is to organize one's world.[80] The growing lack of trust in the United States raising profound questions about the legitimacy of government decisions.[81] 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."[82] 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

---

[75] *Id.* at 11, Trust Crashes in the United States, (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.")
[76] *Id. at* 9, The Polarization of Trust (reporting an aggregate loss of trust at 37%).
[77] *Id.*
[78] The ANES Guide to Public Opinion and Electoral Behavior 1964-2012, http://www.electionstudies.org/nesguide/toptable/tab5a_2.htm, (tallying responses to the question: "Would you say 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?")
[79] SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 26–27 (1978)
[80] NIKLAS LUHMANN, TRUST AND POWER 4 (1979). Similarly, Russell Hardin calls trust "a way of dealing with the risks inherent in complexity." Russell Hardin, The Street-Level Epistemology of Trust, 23 POL. & SOC'Y 505, 516 (1993).
[81] 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, 580-582 (2009).
[82] Lisa Wade, *Money is a Social Construct,* THE SOCIETY PAGES (April 24, 2014) https://thesocietypages.org/socimages/2014/04/24/money-as-a-social-construction/

economy,[83] while technology is the most trusted sector.[84] 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. Indeed, cryptocurrency bull Tom Lee of Fundstrat Global Advisors explicitly ties falling trust in government to the growth of the technology.[85]

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,[86] but estimates that it is capable of handling 56,000 transactions per second.[87] Mastercard similarly claims to be able to handle 65,000 transactions per minute.[88] Both payment networks achieve these processing speeds while navigating more than 150 currencies in 210 countries and territories.[89] 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.[90] 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.

---

[83] 2018 Edelman Trust Barometer, *supra* note __ at 32, Sector and Home Country Provide Context for Business Leadership.
[84] *Id.*
[85] Fundstrat, UpFront Summit Presentation (January 31, 2018) http://www.fundstrat.com/.
[86] Visa Acceptance for Retailers, Visa.com https://usa.visa.com/run-your-business/small-business-tools/retail.html (citing 2010 testing). That works out to roughly 1667 transactions per second.
[87] Jan Vermulen, *VisaNet—Handling 100,000 Transactions Per Minute*, MYBROADBAND.COM (Dec. 17, 2016)
[88] 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
[89] MasterCard 2016 Annual Report 7, http://s2.q4cdn.com/242125233/files/doc_financials/supplemental/2016/Mastercard-2016-Annual-Report.pdf.
[90] The Nilson Report, Issue 1124 (Jan. 2018) https://www.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 2016 Annual Report 12, http://s2.q4cdn.com/242125233/files/doc_financials/supplemental/2016/Mastercard-2016-Annual-Report.pdf.

By virtue of their keystone position, these ledger keepers are privy to sensitive information, and control of various key points of the digital economy. A series of high profile hacks have soured the public on many formerly-trusted intermediaries.[91] Companies ranging from Linked In, to Target, to Experian have all reported massive data breaches that revealed private information from millions of people.[92] There is a growing perception that traditional data management practices have created an 'architecture of vulnerability' that does not sufficiently protect confidentiality.[93] 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.[94]

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,[95] and from untoward government meddling. For example, cryptocurrency supporters like to claim that one problem with regular fiat currency is that 'governments can print as much of it as they like, and they frequently do.[96] Unlike fiat currency, bitcoin is finite—the bitcoin protocol was designed so that only 21 million bitcoins could ever be created. Many cryptocurrency aficionados liken this fixed supply limitation to reinstating the gold standard.[97] Roughly 80% of the bitcoin that will ever exist have already been mined.[98] Current estimates are that the last bitcoin will be mined in

---

[91] *See e.g.,*Selena Larson, *The Hacks that Left Us Exposed in 2017,* CNN.COM (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)

[92]Rajeev Dhir, *13 Recent Data Breaches, Hacks You Should Know About,* NJ.COM (Feb. 24, 2017) http://www.nj.com/news/index.ssf/2017/02/emails_credit_cards_biggest_data_breaches_affect_nj_residents.html

[93] Daniel Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings Law Journal 1227 (2003).

[94] 2018 Edelman Trust Barometer, *supra* note __ at 33, Business Must Address Market Dynamics.

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

[96] *Why Use Bitcoin*, COINDESK https://www.coindesk.com/information/why-use-bitcoin/

[97] Fuathan, *Bitcoin as a Gold Standard,* BitcoinTalk Forum (Jan. 10, 2016) https://bitcointalk.org/index.php?topic=1322343.0. Wences Cesares, *Bitcoin the New Gold Standard,* YOUTUBE March 6, 2015) *https://www.youtube.com/watch?v=yPIvqJsCOSo*.

[98] *Bitcoin Mining Reward Halving Countdown,* http://www.bitcoinblockhalf.com/

2140.[99] What will happen at that date adds uncertainty to bitcoin.[100] Miners will still be needed to secure the integrity of the blockchain but will no longer obtain prizes for mining blocks. The system assumes that miners will continue to maintain the system to collect transaction fees.[101] Yet there is the possibility of a death spiral, if the economic incentive for mining is not adequate to keep a sufficiently dispersed mining pool in place.[102]

For supporters, cryptocurrency replaces law and trust with technology. Thus we see a slew of articles unironically asking questions like "*Why do People Trust Bitcoin*."[103] These articles generally wind up explaining why bitcoin, and cryptocurrency more generally, is indeed trustworthy. Indeed, one commenter summed it up by saying "bitcoin is trust."[104] For a purportedly trustless technology, this claim is rather staggering.

The key to understanding this claim is the virtual ledger called the blockchain. Every bitcoin transaction is encrypted and recorded in the blockchain.[105] The bitcoin blockchain is designed so that this virtual ledger adds a new page roughly every 10 minutes. This new page references all the prior transactions before adding the new transactions. The blockchain thus provides a system for participants to agree on a single history of transactions.[106] This allows users to verify that a transaction is legitimate (meaning that the party actually has the bitcoin s/he purports to be spending.) As a result, 'users purportedly need trust no one when using it.'[107] Indeed, cryptocurrency advocates seems to 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

---

99

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

101 For a detailed discussion of the possibilities and the vulnerabilities, *see How Much Will Transaction Fees Eventually Be*, BITCOIN STACK EXCHANGE *https://bitcoin.stackexchange.com/questions/876/how-much-will-transaction-fees-eventually-be/895#895*.

102 Joshua A. Kroll, Ian C. Davey & Edward W. Felton, *The Economics of Bitcoin Mining or Bitcoin in the Presence of Adversaries* 7, THE TWELFTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS 2013) http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf.

103 *Why Do People Trust Bitcoin*, *http://bitcoincasino.best/why-do-people-trust-bitcoin/*.

104 Tyler Willis, *Bitcoin is Trust* BigThink.com (http://bigthink.com/cue-the-future/bitcoin-is-trust

105 Jerry Brito & Andrea Castillo, Bitcoin: *A Primer for Policymakers* 3 (2013) *available at* http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf.

106 Nakomoto, *supra* n. __ at 2.

107 *https://www.coindesk.com/information/why-use-bitcoin/*

trust them" but "to find an agreement that is self-reinforcing."[108] 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."[109]

1. How does the Block Chain Work?

A key feature of cryptocurrency is the principle that when a bitcoin transaction is incorporated into the blockchain, there is no way to undo the transaction. This gives certainty and finality to the transaction. By comparison, a transaction conducted on credit card is subject to either return when a purchaser changes his/her mind, or challenge if a transaction is alleged to be fraudulent. These possibilities interject uncertainty for merchants, and correspondingly raise prices of transactions. However, the very permanence of bitcoin transactions adds a different kind of vulnerability—when bitcoins or other cryptocurrencies are transferred, there is very little prospect of getting them back, even in cases of fraud or other malfeasance.

Instead of using an identifiable third party like Visa to verify a transaction, bitcoin and other cryptocurrencies rely on a network of computers. These computers serve as a series interconnected "nodes" within the network. Nodes maintain and verify the blockchain consensus record of transactions. They do this by 'mining' transaction blocks. The owners of the computing equipment are called miners. In contrast with bitcoin 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."[110] 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, most of which are hidden from tax authorities. It is the activities of these nameless, faceless individuals that maintains the integrity of the blockchain.

---

[108] Geoffrey Hawthorne, *Three Ironies in Trust*, in TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 115 (Diego Gambetta ed., 1988).
[109] Ed Sohn, *alt.Legal: Amy Wan is Making the Blockchain a Safer Place for Contracts*, ABOVETHELAW.COM (Jan. 19, 2018).
[110] Nicholas T. Courtois and Lear Bahack, *On Subversive Miner Strategies and Block Withholding Attacks in Bitcoin Digital Currency*, 5 arXiv:1402.171 (2014) https://arxiv.org/pdf/1402.1718/.

To create a block, miners compete to complete solve a cryptographic puzzle, called a proof of work in order to collect a reward in Bitcoins. [111]The proof of work involves encrypting new transaction requests, 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.[112] The more mining power a miner applies, the greater its chances of completing the puzzle first and collecting the reward.[113] Once a miner generates a qualifying hash, it is shared across the network. Hashes are difficult to generate, but easy to retroactively verify. Once a hash has been verified, the Miner earns a set amount of bitcoin as a prize for completing the work. The block is then added to the blockchain.

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 work, which involves a significant expenditure of computing power. And, as new, later blocks are chained to it, anyone seeking to change a particular block, say to remove an included transaction, would also have to redo all the blocks after it. 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.[114] Because all full nodes in the network have a record of the complete blockchain, they all

[111] The reward for successfully generating a block is fixed by the system itself, divides in half after every 210,000 blocks. The reward is currently 12.6 coins per block. This reward will halve in approximately 144 days. *See Bitcoin Block Reward Halving Countdown*, http://www.bitcoinblockhalf.com/.
[112] A sample proof of work for the phrase "Hello World!", with an explanation of how such a hash is generated, can be found at https://en.bitcoin.it/wiki/Proof_of_work. An excellent explanation can be found at antonylewis2015, *A Gentle Introduction to the Immutability of Blockchains*, BITSONBLOCKS.NET (Feb. 29, 2016) https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/. A more detailed, technical analysis is available from Harvey, Campbell R., Cryptofinance (January 14, 2016). Available at SSRN: https://ssrn.com/abstract=2438299 or http://dx.doi.org/10.2139/ssrn.2438299.
[113] For a good explanation accessible to users, *see* Ittay 113 and Emin Gun Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, (Nov. 2013).
[114] *See generally*, Nakomoto, *supra* n. 16.

have access to a shared, single source of truth.[115] The nodes can work together but do not need to trust each other.

IV. Four 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.[116] 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 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."[117]

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.[118] As one blockchain expert stated: "when we transact with one another on the blockchain, we are anchoring our trust in the miners...."[119] Because the blockchain assumes the nodes act independently and do not trust each

---

[115] Quinlan & Associates, *From KYC To KYT* (Nov. 2016), available at: http://www.quinlanandassociates.com/wp-content/uploads/2016/12/QuinlanAssociates-From-KYC-to-KYT.pdf
[116] *See e.g.*, Nomad Wallet, *Blockchain—Believe in Cryptographic Proof Instead of Trust, https://digitalnomad.community/believe-in-cryptographic-proof-instead-of-trust/;* Cryptoclub, *In Cryptocurrency WE Trust, https://cryptobitclub.co/.*
[117] Preethi Kasireddy, *ELI5: What Do We Mean by "Blockchains are Trustless,"* MEDIUM (Feb. 2, 2018)
[118] *See* Nakamoto, *supra* note 16
[119] Preeti Kasireddy, ELI5" *What Do We Mean By 'Blockchains are Trustless'?* MEDIUM (undated) https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6

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."[120]

Despite the extravagant rhetoric about trustless interactions, multiple layers of trust are built into cryptocurrencies.[121] With regard to the blockchain itself, users are trusting developers to build secure software, [122] trusting miners not to collude or attack the blockchain,[123] and trusting the wider cryptocurrency community not to approve a hard-fork.[124] With regard to using the currency, users are trusting that markets are not being manipulated,[125] that wallets will generate secure keys,[126] and that exchanges are using best security practices.[127] That is an awful lot of trust for a trustless system. The biggest differences with more conventional markets is 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[128] and reliability of the blockchain. However, this

[120] Nakomoto, *supra* n. __ at 3. ("So long as a majority of the computing power in the system is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.")
[121] *See* Hashib Qureshi, *Why Bitcoin is Not Trustless*, HACKERNOON (Dec. 18, 2017) https://hackernoon.com/bitcoin-is-not-trustless-350ba0060fc9
[122] For a discussion of bugs that called off the SegWit2x rollout, *see* Jimmy Song, *SegWit2x Bugs Explained*, BitcoinTechTAlk.com (Nov. 20, 2017) *https://bitcointechtalk.com/segwit2x-bugs-explained-8e0c286124bc* (noting that the bugs could have allowed double-spending).
[123] https://blog.acolyer.org/2017/12/07/be-selfish-and-avoid-dilemmas-fork-after-withholding-attacks-on-bitcoin/
[124] See the discussion regarding the DAO, and Ethereum's hard fork in response to the theft.
[125] For a description of market manipulation, *see Who is Spoofy and How is He Manipulating Bitcoin's Price?* THE MERKLE.COM (Aug. 7, 2017) *https://themerkle.com/who-is-spoofy/*
[126] Alex Hern, *Bitcoin App Issues Critical Update After Rare Bug Leads to Total Crypto Breakdown*, THE GUARDIAN (June 1, 2015) https://www.theguardian.com/technology/2015/jun/01/bitcoin-app-critical-update-bug-crypto-breakdown.
[127] *Tokyo Based Cryptocurrency Exchange Hacked, Losing $530 Million*, REUTERS (Jan. 26, 2018) https://www.reuters.com/article/us-japan-cryptocurrency/tokyo-based-cryptocurrency-exchange-hacked-losing-530-million-nhk-idUSKBN1FF29C; *Bitcoin Worth $72 Million Was Stolen in Bitfinex Exchange Hack* 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 (March 3, 2014).
[128] *See e.g.*, Oscar Lage Serrano, *Is the Blockchain Really Immutable?,* Blockchain Revolution (July 5, 2017) https://www.bbva.com/en/blockchain-really-immutable/.

scenario also gives rise to a major limiting factor: the blockchain's current inability to scale.[129] 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.[130] 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 1,188 minutes (nearly 20 hours!).[131] As processing time shot up, fees increased as well. At the peak, average transaction fees topped $55 dollars per transaction.[132] 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."[133] 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.[134]

Because the system is decentralized, merely adding more servers, the go-to solution in a traditional, centralized database, will not shorten processing time. Moreover, electricity demands by the existing full nodes responsible for mining blocks and storing them on the blockchain has already reached unsustainable levels.[135] It seems clear that the blockchain will have to address

---

[129] Preethi Kasireddy, *Blockchains Don't Scale. Not Today, at Least. But There's Hope,* HACKERNOON (Aug. 23, 2017). The explanation in the rest of this paragraph is loosely based on Kasireddy's article.
[130] Alex Lielacher, *How Long Should My Bitcoin Transaction Take?*, BITCOIN MARKET JOURNAL (July 6 2017).
[131] Ryan Browne, *Big Transaction Fees are a Problem for Bitcoin—But There Could Be a Solution*, CNBC.com (December 19, 2017) https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html.
[132] *Bitcoin Avg. Transaction Fee Historical Chart*, BITINFOCHARTS https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#3m.Fees have fallen dramatically since then, but still average over $2.00 per transaction. *Id.* 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.
[133] Leilacher, *supra* note 130
[134] Rob Price, *A Major Bitcoin Conference is No Longer Accepting Bitcoin Payments Because the Fees and Lag Have Gotten So Bad*, Business Insider (Jan. 10, 2018) http://www.businessinsider.com/bitcoin-conference-stops-accepting-bitcoin-network-fees-congestion-2018-1.
[135] Moreover, bitcoin's energy footprint is already massive, far in excess of its value. Producing bitcoin currently consumes energy at the rate of 54.2 TWh per year, as much as the entire country of Bangladesh. *Bitcoin Energ Consumption Index*,https://digiconomist.net/bitcoin-energy-consumption; *see also* Timothy B. Lee, *Bitcoin's Insane Energy Consumption Explained*, ARSTECHNICA (January 2017) https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/. Each transaction produces 386 ktons of carbon, giving bitcoin an annual carbon footprint of 26,559 tons.

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.[136]

While the future of the blockchain will probably have to involve full nodes trusting each other in some fashion, the blockchain's present already explicitly incorporates trust in two very important respects. First, many cryptocurrency transactions use a simplified verification system, that involves trusting full nodes. Second, the blockchain needs honest nodes, and trusts to economic games to keep nodes honest.

1. Most Cryptocurrency Users Wind Up Trusting Individual Nodes Rather Than the Blockchain

Most cryptocurrency participants do not run a full node (there are only about 10,000 full nodes in existence).[137] Instead, many cryptocurrency hodlers rely on so-called light nodes and wallets, which use a simplified payment verification system (SVP). An SVP connects with one or more full nodes and ask that a cryptocurrency transaction be included in a block. The SVP then receives confirmation from the full node that the transaction was included in a block, and that the block is part of a chain.[138] SVP clients trust 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 built upon, SPV nodes will accept the transactions as valid without checking further. That means that a light wallet does not verify that the transaction was

[136] 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., Kasireddy*, *supra* note 129 for an explanation of some of the possible solutions.

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

[138] For a good description of the difference between light nodes and full nodes, *see*, adminfrog, *What are Full Nodes and Light Nodes of the Bitcoin Blockchain,* COINFROG (Jan. 14, 2018) https://coinfrog.io/full-nodes-light-nodes/

included in the correct chain—the one that is the single, agreed-upon history of all transactions.[139] Instead, the light wallet (and hence its user) trust one or more full nodes to verify transactions for them.[140]

SPV wallets are thus potentially at the mercy of rogue nodes, or even a sloppy ones. Indeed, in July 2015, after a blockchain system upgrade, this vulnerability resulted in a crisis.[141] Despite a consensus to upgrade to a new process, roughly half the network was mining without fully vetting blocks.[142] 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 confirmations that were not real. There were at least three forks, one of which added 6 blocks before the valid chain reasserted itself.[143]

In this kind of a situation, one set of nodes may accept transactions considered invalid by the other set of nodes. If the first group of nodes are numerically inferior, their validated blocks will not be incorporated into the main blockchain. This results in stranded blocks, and transactions that essentially disappear from the blockchain. The reverse could happen as well—one set of nodes rejects blocks or transactions that have already been incorporated into the main block chain. There would be two blockchains at that point, and one of the blockchains would not be providing accurate information. It should not take long for it to become clear which blockchain fork was growing longer, and therefore was the more valid chain. Yet, in the interim, a person trusting in a block later revealed to be a mere fork could be fooled. That person' transaction might be marooned in a stale block, excluded from the blockchain as invalid if the longer chain contained a contradictory transaction. Trust in the blockchain as a replacement for trusted

---

[139] Forks in the blockhain are discussed *infra*. For an explanation of how a chain can be forked into two branches and then pruned, *see* Ittay Eyal and EMin Gun Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, (Nov. 2013) (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.

[140] pwuille, *Full Node Question*, REDDIT.COM (July 27, 2015) 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 the 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!").

[141] Alert: *Some Miners Generating Invalid Blocks*, BITCOIN.ORG (July 4, 2015) https://bitcoin.org/en/alert/2015-07-04-spv-mining#list-of-forks.

[142] The new rule was called BIP66. It was intended to remove Open SSL from the consensus code for signature verification.*see* bitcoin/bps, GITHUB.COM https://github.com/bitcoin/bips/blob/master/bip-0066.mediawiki

[143] *Miners Generating Invalid Blocks*, *supra* n. 141.

intermediaries could expose such a person to significant losses because the fork creates a possibility of double-spending.

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."[144] It advises SPV clients[145] to connect to several full nodes and ensure they are all 'on the same chain with the same block height,[146] plus or minus several blocks to account for transmission delays and stale blocks.'[147] 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 are built into the transactions—that nodes are validly processing transactions, that SPV wallets are properly verifying transactions.

This vulnerability of light wallets is not a surprise. Satoshi Nakamoto himself noted that SVP verification "is reliable as long as honest nodes control the network, but is more vulnerable by an attacker . . . .[t]hey simplified method can be fooled by an attacker's fabricated transactions. . .. "[148] 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."[149] In Todd's own terms, using a light wallet is "just outsource[ing] your trust to others."[150] 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 Nodes

---

[144] Bitcoin Developers Guide, https://bitcoin.org/en/developer-guide#detecting-forks.
[145] SPV stands for "simplified payment verification." It is a method for verifying transactions without downloading the entire blockchain.
[146] 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. *What is a Soft Fork?* BITCOIN.COM (Oct. 4, 2014) https://bitcoin.org/en/alert/2015-07-04-spv-mining. At an average pace of 10 minutes per block, that would be a wait of 5 hours. The more usual wait was for six blocks, or an hour wait. Alex Lielacher, *How Long Should My Bitcoin Transaction Take?* Bitcoin Market Journal (July 6, 2017).
[147] *Id.*
[148] Nakamoto, *supra* note 16 at 5.
[149] From r/bitcoin thread *Bitnodes Recently Updated their Node Counter Crawling Algorithm—Apparently the Old One Was Off By an Order of Magnitude,* Peter Todd comment. The Bitcoin wiki makes this point as well. *See Lightweight Node,* Bitcoin Wiki, https://en.bitcoin.it/wiki/Lightweight_node. https://www.reddit.com/r/Bitcoin/comments/20hsql/bitnodes_recently_updated_their_node_counter/cg3d1qy/?context=3
[150] *Id.*

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 Satoshi Nakamoto onward, it has been clear that the blockchain is secure only so long as honest nodes control more computational power than a group of cooperating attackers.[151] 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.[152] 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."[153]

There has already been at least one 51% attack against smaller Ethereum chains.[154] To intentionally attack the larger Bitcoin blockchain in this fashion would require significant hashing power in order to control a majority of nodes. However, Bitcoin has come close. In 2014, one mining pool, Ghash.io controlled 50% of mining on the bitcoin blockchain.[155] 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."[156] 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.[157] BTC.com, which alone controls ¼ of the network,[158] and Antpool, which controls 16% are both projects of the same China-based company, Bitman.[159] Bitman's founder Jihan Wu has also invested in Via.BTC.[160] The

---

[151] Nakamoto, *supra* note 16 at 3.
[152] 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. CITE HERE
[153] *See e.g.* Eyal and Gun Sirer, *supra* note.
[154] *51% Crew Extorts and Hijacks Blockchains for Randsom,* CRYPTO HUSTLE (Sept. 3, 2016) https://cryptohustle.com/51-attack-crew-extorts-and-hijacks-blockchains-for-ransom
[155] 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/
[156] *Id.* (quoting CEX.IO CIO Jeffrey Smith,).
[157] *Hashrate Distribution*, BLOCKCHAIN https://blockchain.info/pools?timespan=4days.
[158] *Id.*
[159] 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).
[160] Darryn Pollock, *Bitmans Mining Monopoly Compromises Bitcoin's Decentralized Nature,* COINTELEGRAPH (Aug 30, 2017).

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.[161] For a system that depends on decentralization for validity, that seems remarkably centralized.[162]

However, even putting aside the prospect of a 51% attack, there are multiple, profitable ways for miners to game the verification system undermining the validity of the chain. A few of the best known techniques, Sybil attacks,[163] Block Withholding attacks,[164] Selfish Mining,[165] and Fork After Withholding attacks,[166] are maneuvers miners can use to increase their share of the mining rewards at the expense of other miners.[167] These are not merely hypothetical. At least one Block Withholding attack has been documented,[168] and scholars assert that the *only* defense against this attack is for mining pool managers to be work with miners they know personally and trust.[169] Fork after Withholding attacks have been described by scholars as 'always profitable,' and 'difficult to guard against.'[170] Selfish mining had traditionally been considered impractical because it was assumed that it required control of a majority of the network nodes. However,

---

[161] 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 Chrackdown on Bitcoin Mining,* INVESTOPIA (Jan. 11, 2018) https://www.investopedia.com/news/china-intensifies-crackdown-bitcoin-mining/?

[162] 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)

[163] Moshe Babaioff, et al., On Bitcoin and Red Balloons, 10 ACM SIGECOM EXCHANGES 5 (2011) http://www.sigecom.org/exchanges/volume_10/3/BABAIOFF.pdf (describing Sybil attacks. Lightwallets are particularly vulnerable to Sybil attacks.)

[164] Nicholas T. Courtois and Lear Bahack, *On Subversive Miner Strategies and Block Withholding Attacks in Bitcoin Digital Currency*, 5 arXiv:1402.171 (2014) https://arxiv.org/pdf/1402.1718/. *See also* Deepak K. Tosh, et al., *Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack,* (2016)

[165] *See* Ittay Eyal and Emin Gun Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable,* (Nov. 2013) (describing a selfish mining attack).

[166] Yujin Kwon, et al., *Be Selfish and Avoid Dilemmas: Fork After Withholding FAW) Attacks on Bitcoin,* arXiv:1708.09790 (2017)

[167] *See e.g.*, Yujin Kwon, et al., *Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin,* (Aug. 31, 2017) https://arxiv.org/pdf/1708.09790.pdf (describing attacks and asserting that the "Fork After Withholding' attack is always profitable for the miner).

[168] At least one Block Withholding Attack has already occurred. *See* Wizkid057, *Eligius: 0% Fee BTC, 105% PPS NMC, No registration, CPPSRB*, post #2348, BITCOINTALK.ORG (2014). https://bitcointalk.org/?topic=441465.msg7282674. One response to the attack was to assure mining pool participants that any changes required the signatures of both Eligius founders, plus a disinterested third party. This announcement sought to leverage trust in Wizkid057, Luke-Jr. and the unnamed 3rd party into trust in the validity of the mining pool payment algorithm.

[169] Courtois and Bahack, *supra* note 164 at IX(a).

[170] Kwon, *supra* n. __. Although this paper modeled the Fork after Withholding attack in bitcoin, the authors assert that other cryptocurrencies including Ethereum and Litecoin are also vulnerable.

recent research shows how such an attack could be successful, even without controlling 51% of the network.[171]

The lesson from this should be that rhetoric about the trustless blockchain may have been overblown. Indeed, from the earliest inception of cryptocurrency, it has been clear that the validity of the blockchain depends on there being sufficient minors to validate each block. The entire system runs on trust in that process. Most cryptocurrency participants do not realize they are trusting miners in this fashion. Instead, they probably accept the oft-repeated assertions that the blockchain cannot be hacked[172] as a proxy for a system that aligns miner interests with those of participants.

However, their trust is on much shakier ground than they realize. If enough miners cease or reduce their operations, the chain becomes vulnerable. Moreover should one actor or consortium obtain control of a majority of the nodes in the blockchain, they would be in a position to attack the integrity of the blockchain. Participants place a great deal of trust in nameless, faceless miners, and trust the bitcoin incentive system to align miner interests with those engaged in bitcoin transactions. Yet, there are identified strategies by which rogue miners can promote their self- interest at the expense of the integrity of immutable, trustless blockchain.

B. Trusting the Collective Decision-making Process

At the same time that transactions require trust in the blockchain itself and the 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.[173] Yet, what happens when the consensus protocol is changed? For example, the blockchain network needs occasional upgrades and repairs. In those moments, the wider community needs to trust that the

[171] Kevin Liao and Jonathan Katz, *Incentivizing Double-Spend Collusion in Bitcoin*, https://www.cs.umd.edu/~gasarch/reupapers/katzbitcoin16.pdf (describing a so-called 'whale' attack that could feasibly permit double-spending on the blockchain.)
[172] *See e.g.* BittBurger, *Can the Blockchain Be Hacked* BITCOIN FORUM (Dec. 5, 2013) https://bitcointalk.org/index.php?topic=358039.0.
[173] KPMG, *Consensus: Immutable Agreement on the Blockchain* 3-5 (2016) https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

network and all its constituents can appropriately handle the changes. The way that miners and other users interact with blockchain must change as well, potentially creating a fork in the blockchain.[174]

Sometimes, the protocol change will be backwards compatible, meaning that older protocol iterations will continue be compatible with the new protocol as the blockchain advances. In that case, it can be implemented with what has become known as a "soft fork," that results in a temporary divergence in the blockchain that resolves back into a single blockchain.[175] Miners need to upgrade to avoid being marooned on the losing chain, but merchants and users can continue to use the older protocol.[176] Sometimes, however, a protocol change is not backwards compatible, requiring all users to "upgrade [to the new protocol] or be left behind."[177] If the changes are popular, the entire community adopts them. The old chain still exists, but all the users—miners, merchants and users—have migrated in unison to the new chain.[178] 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 chain is not unanimously accepted. If the community does not agree on the hard fork update path, it can get "very, very bad."[179] 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 thus one of the forks. This kind of hard fork, called a

---

[174] Not to be confused with a software fork which involves taking the original code and modifying it to create a new product. This is more akin to a spin-off than to a hard or soft fork of the blockchain. *The Difference Between Hard and Soft Forks*, WEUSECOINS.COM https://www.weusecoins.com/hard-fork-soft-fork-differences/. For example, Litecoin is the result of a software fork from bitcoin.

[175] Softforks restrict block acceptance rules, but do so in a fashion that continues to allow a subset of the previously valid blocks. Under this circumstance, all blocks considered valid by the new protocol will also be also considered valid by the old protocol. *See,* Murch, answer to *What is a Soft Fork?* BITCOIN STACK EXCHANGE (OCT 4, 2014), *https://bitcoin.stackexchange.com/questions/30817/what-is-a-soft-fork*. If a majority of nodes adopt the new rules, the new blockchain will overtake any chain using the older protocol because blocks validated under the new rules will be accepted by all nodes, while blocks validated under the older rules will only be accepted by nodes employing the old rules.

[176] Charlie Lee, *What is a Soft Fork? supra* n. 175, answer provided (Aug. 18. 2015).

[177] Gavin Andreson, *Blockchain Rule Update Process,* (undated) https://gist.github.com/gavinandresen/2355445.

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

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

'contentious hard fork' splits the path of the blockchain—creating two separate chains running parallel to each other. Some nodes follow the old protocol 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. Users cannot send funds from one chain to the other, resulting in different versions of the same coin.[180] 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.'

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. As one commenter noted, the conflict that led to the hard fork "erode[d] trust within the community," [181] and unironically cautioned participants in the supposedly trustless system that "[p] arties that don't trust each other have a difficult time compromising and meeting possible future challenges."[182] This concern played out in the contentious hard fork that created Bitcoin Cash in August of 2017, 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.

The bitcoin protocol has a built-in limit of 1 MB per block. As usage ramped up, that size limit, combined with the decentralized network led to major delays in processing transactions. The disagreement that led to the hard fork was over how to respond to congestion on the bitcoin network: specifically whether to increase the size of the blocks in the chain or make other operational changes to increase speed of processing.[183] A group of miners led by Bitman founder Jihan Wu[184] (remember Bitman--the force behind two of the major mining pools) pushed

[180] https://www.weusecoins.com/hard-fork-soft-fork-differences/
[181] David Dinkens, *Collapse of Bitcoin's New York Agreement Would Have Long Term Consequences* COINTELEGRAPH.COM (Sept. 16, 2017).
[182] *Id.*
[183] 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.
[184] Prableen Bajpai, *Who is Jihan Wo and Does He Basically Control Bitcoin?* INVESTOPEDIA (May 1, 2017).

aggressively for an alternative solution – increase the size of each block added to the blockchain from 1 MB to 2 MB.[185] Wu is a controversial figure because of repeated allegations that he manipulated the cryptocurrency for his own gain.[186] Others advocated a more permanent solution in the form of a code called Segregated Witness (SegWit). [187] 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 raged on for years until finally a group of over 50 high profile companies met to resolve the situation, producing a compromise known as the New York Agreement.[188] 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.[189] The companies signing the agreement represented 83.25% of the computing power on the bitcoin blockchain.[190]

It should have been simple. As designed by Nakamoro, the miners decide which code changes to accept. However, an entire economic ecosystem has grown up over the blockchain, and that ecosystem was not happy. They argued that the change should not proceed without support from an 'economic majority' of the wallets and exchanges.[191] They offered an alternative proposal called BIP148—a user activated soft fork to achieve 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. [192] But, what was really happening was a power struggle over who gets to make choices for the blockchain—the miners or the users. For

---

[185] 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

[186] Jeff John Roberts, *Does Bitcoin Have a Mining Monopoly?* FORTUNE (Aug. 25, 2017) http://fortune.com/2017/08/25/bitcoin-mining/

[187] 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 Blockchains Don't Scale. Not Today at Least. But There's Hope*, HASH HACK (Dec. 15, 2017) https://www.hashhack.it/posts/blockchains-dont-scale-not-today-at-least-but-theres-hope .

[188] New York Agreement, MEDIUM (May 23, 2017) https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77

[189] *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.

[190] New York Agremeent, *supra* note 188.

[191] UASF Working Group, *BIP148 and UASF FAQ, http://www.uasf.co/*

[192] *Id.*

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.[193] Their position was that the economic majority should signal support for the change, and the miners should follow along.[194] The threat was that if miners did not follow along with the user proposal, users would not recognize their coins as 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.[195]
This twin threats posed the possibility of a split between a majority of the miners and an "economic majority" of the wallets and exchanges, raising the question of whose consensus mattered for blockchain governance.

The first part of the plan went off as planned, and SegWit was adopted. However, Bitcoin's core development team still opposed doubling the block size.[196] Signatories to the New York Agreement began reneging on their support for the increased block size.[197] In November 2017, the block size increase (known as SegWit2x) was suspended for lack of support.[198] Outraged commenters lamented that "[w]ithdrawing one's support from important agreements erodes trust within the community. Parties that don't trust each other have a difficult time compromising and meeting possible future challenges."[199]

1. Lessons from Smart Contracts

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

[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] David Dinkens, *Bitcoin Core 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
[197] Alyssa Hertig, *F2Pool Renegesl Bitcoin Pool Pulls SegWit2x Support Over Hard Fork,* COINDESK (Aug. 31, 2071) *https://www.coindesk.com/f2pool-reneges-mining-pool-pulls-segwit2x-support-hard-fork/*
[198] Email from Michael Belshe, *SegWit2x Final Stops,* Nov. 8, 2017) *https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html*
[199] Dinkens, *supra* n.__.

was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what." [200] For Nakamoto, cryptocurrency meant that "without the need to trust a third party middleman money can be secure and transactions effortless." [201] However the halo of security extends well beyond the blockchain itself, inducing participants to trust a host of third-parties who do act as middlemen. Participants in cryptocurrency find themselves trusting exchanges, wallets, and smart contracts, all under the halo of the blockchain's immutability.

Smart Contracts offer a good example of how participants confuse their decision to trust the blockchain with trusting operations that use the blockchain. Indeed, experience on the Ethereum blockchain shows how smart contracts can undermine the integrity of the blockchain itself. In 2016, an Ethereum startup called Slock.it created a so-called smart contract called the Distributed Autonomous Organization (The DAO).[202] 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."[203] 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.[204]

In early June, commenters began pointing out serious vulnerabilities in The DAO's code.[205] In response, on June 12, 2016, Slock.it founder Stephan Tual took to social media to announce that no DAO funds were at risk,[206] essentially saying "trust us." Five days later, hackers diverted

---

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

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

[202] The DAO was a smart contract on Ethereum that was supposed to act as a distributed venture capital firm. It was intended to pool contributors money and distribute it to projects the contributors voted to fund*;* For a detailed explanation of the programming flaw that allowed the hack, Other DAOs exist. For example, Digix Global, a company that tokenizes gold on the Ethereum network, runs a DAO called DigixDAO that issues DGD tokens. https://digix.global/ Similarly, the cryptocurrency Dash is a DAO.

[203] The DAO, http://web.archive.org/web/20160622212302/https://daohub.org/

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

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

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

Ether worth nearly $60 million out of The DAO into a new account.[207] Observers watched the unknown hackers drain off funds, but because of The DAO's 'unstoppable code' they could not do anything to stop it. 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.[208] Subsequent forensic investigations found that a majority of Ethereum smart contracts ignore best-practices for preventing hacks.[209]

In an extremely contentious move, the Ethereum community decided to create a hard fork to reverse the transfers out of The DAO. Anti-Hard Fork opponents argued vociferously against the decision on the ground that it would violate the immutability of the blockchain, and undermine the perception that blockchain contracts were permanent.[210] 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?
> 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.[211]

Hard Fork opponents pointed out that altering the blockchain is a slippery slope[212] and once the blockchain is modified in this fashion, there will inevitably be further calls for other

---

[207] *See I Think the Dao is Getting Drained Right Now,* Reddit.com (*https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/*; Vitalik Buterin, *Critical Update Re: DAO Vulnerability,* Ethereum.org (June 17, 216) https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

[208] Antonio Madera, *The DAO, the Hack, the Soft Fork and the Hard Fork* CRYPTOCOMPARE (Feb. 28, 2018) https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

[209] Zikai Alex Wen and Andrew Miller, *Scanning Live Ethereum Contracts for the 'Unchecked Send' Bug,* HackingDistributed.com (June 16, 2016) http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/ (calling Ethereum smart contracts "notoriously error-prone.").

[210] Madera, *supra* note 208.

[211] Derrend, *Code is Law* https://www.reddit.com/r/ethereum/comments/51bca4/code_is_law/#bottom-comments.

modifications.[213] More fundamentally, they argued that a hard fork to reverse this hack would violate the basic principle that "code is law."[214] Proponents of the hard fork retorted that "code is law" is un-nuanced and ignores the dynamic nature of law.[215] Instead, they offered a vision of decision-making in which human beings get to think and make choices that amount to a social consensus.[216]

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.[217] 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.[218] However, a sizeable minority of users rejected the new chain, giving rise to two Ethereum chains—Ethereum and Ethereum Classic which created a host of logistical issues.

Note the ironic role that trust plays in this drama—the immutable blockchain was altered in the name of reinstating trust in the block chain after a cryptocurrency exchange 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.[219] The DAO incident 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, could happen again, including for far less savory reasons.

---

[212] As the Bitcoin Wiki entry on Weaknesses indicates: "If it becomes possible for coins to be blacklisted in this way, then it is a slippery slope toward blacklisting of other "suspicious" coins." Bitcoin Wiki, Weaknesses https://en.bitcoin.it/wiki/Weaknesses

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

[214] Laurence Lessig, *Code is Law*, HARV. MAG. (March-April 2015) http://socialmachines.media.mit.edu/wp-content/uploads/sites/27/2015/03/Code-is-Law-Harvard-Magazine-Jan-Feb-2000.pdf.

[215] Madera, *supra* note 208.

[216] *Id*.

[217] Madera, *supra* note 208.

[218] Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (Jul. 20, 2016).

[219] *Bitcoin: In Crypto We Trust*, Errata Security (Dec. 19, 2017) (claiming that "the manifesto behind Bitcoin is that a transaction cannot be reversed -- and thus, can always be trusted")

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 is seeking a hard fork to undo the hack. The hacker took control of 587 wallets holding 513,774.16 Ether (worth roughly $300 million at the time.)[220] The user then destroyed the wallets, effectively freezing those coins.[221] Parity developers have requested another Ethereum hard fork to recover at least some of these coins.[222] It turns out that stuck, non-recoverable ether is a relatively common problem.[223] User error in the command line, as well as software bugs,[224] in addition to intentional hacks like Parity have all created millions of dollars worth of "stuck" ether, inaccessible to its owners.[225] 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.[226]

The current craze over cryptokitties highlights the mistake of conflating the blockchain with smart contracts that use the blockchain. Cryptokitties are cartoon-like digital cats.[227] Users pay to purchase and breed 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.[228] At least one purchaser paid $110,000 for a kitten, though most sell for far less.[229] The value proposition for these kittens as collectables rests on the immutable nature of the Ethereum

---

[220] *A Post-Morten on the Parity Multi-Sig Library Self-Destruct,* PARITYTECH.IO (Nov. 15, 2017) https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/.
[221] *Parity Technologies Muli-Sig Wallet Issue Update,* PARITYTECH.IO (Nov. 13, 2017) http://paritytech.io/parity-technologies-multi-sig-wallet-issue-update/.
[222] *Parity Post-Mortem*, *supra* note. 220. They concede however, that much of the coins cannot ever be recovered, and that "there is no timeline for when such an improvement proposal could be implemented." *Id*.
[223] *On Classes of Stuck Ether and Potential Solutions,* ParityTech.co (Dec. 11, 2017) https://paritytech.io/on-classes-of-stuck-ether-and-potential-solutions/.
[224] Peter Vessenes, *Ethereum Contracts are Going to Be Candy for Hackers,*(May 18, 2016) http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/
[225] *Id.* For more detail, *see* Peter Vessenes, *Ethereum Griefing Wallets: Send with Throw is Dangerous,* Vessenes.com (June 4, 2016) *http://vessenes.com/ethereum-griefing-wallets-send-w-throw-considered-harmful/*
[226] Robert DeVoe, *Parity to Ethereum Foundation: One Hard Fork Please,* COINBUREAU (Dec. 14, 2017).
[227] https://www.cryptokitties.co/
[228] Olga Kharif, *Cryptokitties Mania Overwhelming Ethereum Network Processing* BLOOMBERG (Dec. 4, 2017) https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app
[229] Joseph Young, *Ethereum-based Cryptokitten Sells for $117,712,* COINJOURNAL (Dec. 5, 2017)

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."[230]

The hype around these digital cats is another 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 Blockchain contract.[231] 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 that." [232] 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 pause the contract—sending all cryptokitties into permanent hibernation.[233] Moreover, the CEO of cryptokitties retains total discretion to change the breeding algorithm, with the possibility of making previously rare (and expensive) kitten traits commonplace.[234] 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,[235] 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 Exchanges

---

[230] *Getting Started with Cryptokitties*, http://cryptokittyworld.com/.
[231] Vicnaum post on reddit thread *Where Exactly is my Kitty on the Blockchain*, https://www.reddit.com/r/CryptoKitties/comments/7rio31/where_exactly_is_my_kitty_on_the_blockchain/
[232] Luke Zhang, *Your Cryptokitty isn't Forever,* Medium (Dec. 3, 2017)
[233] In the Parity hack described above, this is what a malicious user did to the wallets.
[234] *Id.*
[235] *See e.g.*, Kryptofan post on reddit thread *Where Exactly is my Kitty on the Blockchain*, https://www.reddit.com/r/CryptoKitties/comments/7rio31/where_exactly_is_my_kitty_on_the_blockchain/

Most individuals do not interact directly on the blockchain. They instead interact through exchanges 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"[236] 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, un-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.[237] Despite the purported immutable security of the blockchain, there are plenty of ways for thieves to steal cryptocurrency. Indeed, rapidly rising prices, anonymity, and lack of regulation make cryptocurrency exchanges "natural targets" for theft[238] and scams. Hacks and thefts are common occurrences. And because of the decentralized, unregulated nature of the coins, victims find themselves largely without recourse.

1. Hacks and Thefts

In late 2017, Reuters estimates that 980,000 coins, worth up to $15 billion had been stolen in the prior 6 years.[239] Here is a list of just a sampling of the most recent cryptocurrency hacks.[240]

---

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

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

[238] 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.

[239] Jim Finkle and 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

[240] Yugi Nakamura, *The Wretched, Endless Cycle of Bitcoin Hacks,* Bloomberg.com (Aug. 17 2016).

- February 2018-- CISCO confirmed that a Ukrainian hacker group called Coinhorder stole $50M from Blockchain.info wallets.[241]
- January 2018—Coincheck was hacked for $530 million—making it the largest cryptocurrency hack ever,[242] outstripping the 2014 Mt. Gox hack in which $400 million was stolen.[243]
- January 2018: Blackwallet announces it has been hacked and advises customers not to log in to their accounts. 700,000 lumens are 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.[244]
- December 2017—YouBit (S. Korea) thieves stole 3/5 of clients holdings. Worth 35 million at the time. Company files for bankruptcy[245]
- December 7, 2017: NiceHash—4700 bitcoin worth more than $75 million at the time. [246] NiceHash self-described as "the largest marketplace for mining digital currencies." It appears that the hacker entered the system with credentials for one of NiceHash's engineers.
- November 2017—Bitfinex, which had previously lost millions of dollars of customer money in multiple hackings, was hacked again, this time losing $30 of Tether from online wallets.[247]

Unfortunately, the list could go on and on. These hacks illustrate how trust in third parties that surround the blockchain might be misplaced.

Moreover, users have been unpleasantly surprised at how easily exchanges can unilaterally make choices that limit user access to their funds. The instances that follow describe a few of the most high-profile instances.

i. Access to Bitcoin Cash

[241] Jen Weiczner, *Hackers Stole $50 Million Using Poison Google Ads*, Fortune (Feb. 14, 2018).This one was a theft rather than a hack. Coinhorder 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.
[242] Daniel Shane, $530 Million Cryptocurrency Hack May Be Largest Ever, CNN (Jan. 29, 2018).
[243] Jose Pagliery, *How Mt. Gox Went Down*, CNN (Feb. 26, 2014)
[244] 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*
[245] Daniel Shane, Bitcoin Company Goes Bust After Hack, CNN.com (Dec.. 20, 2017
[246]Rishi Iyengar, *More than $70 Million Stolen in Bitcoin Hack,* CNN.COM (Dec. 8, 2017) http://money.cnn.com/2017/12/07/technology/nicehash-bitcoin-theft-hacking/index.html
[247] The company lost 1,500 Bitcoin, worth around $400,000, to a hacker in 2015. In August 2016, Bitfinex was hacked again, losing almost 120,000 Bitcoin, worth around $75 million at the time.Stan Higgens, *The Bitfinex Bitcoin Hack: What We Know and What We Don't Know,* COINDESK (Aug. 3, 2016). One of the more significant consequences of the 2016 Bitfinex hack is described in part 2 infra.

In August 2017, at the same time that the SegWit drama was unfolding, a small group of miners decided opt out of the debate and increase the size of bitcoin blocks on their own.[248] They created a hard fork, creating Bitcoin Cash from the older core Bitcoin Some miners stuck with the old protocol, while others moved to the new chain, resulting in two blockchains going forward: core Bitcoin and Bitcoin Cash. Bitcoin Cash immediately raised its block size to 8MB, while Core Bitcoin retained the original 1 MB block size.[249] *Hodlers* receives one Bitcoin Cash for each Bitcoin they held on the day of the hard fork.

However, Coinbase and Blockchain.info, two of the largest currency exchanges, opted not to support the new currency at the time of the hard fork. [250] That meant that any customers with bitcoin on either exchange would not receive their Bitcoin Cash, and could not access, use or sell the coins. Indeed, Coinbase made it very clear that customer "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)."[251] Bitcoin *hodlers* suddenly found themselves at the mercy of the exchanges, perhaps having never before thought about the trust they had placed in these enterprises which unilaterally prevented their access to the new currency.

Worse, Coinbase advised clients wishing to receive Bitcoin Cash to withdraw their bitcoin from the exchange,[252] cautioning that during the hard fork, customers would not be able to withdraw any "version of any Bitcoin from Coinbase."[253] That meant that the exchange using 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." [254] With transactions taking up to 12 hours to process, customers complained that they were locked into Coinbase and its decision about Bitcoin Cash.[255] Customers were only credited with the new

---

[248] Sudhir Khatwani, *Bitcoin Cash (BCH)—a New Feather in Bitcoin's Fork Cap,* COINSUTRA (Dec. 11, 2017) https://coinsutra.com/bitcoin-cash-bch/
[249] https://www.bitcoincash.org/
[250] Berk v. Coinbase, para 32 (citing Coinbase July 17, 2017 FAQ).
[251] *Coinbase GDAX Reiterate Position on Bitcoin Cash: Njet!* TRUSTNODES.COM (July 28, 2017) https://www.trustnodes.com/2017/07/28/coinbase-gdax-reiterate-position-bitcoin-cash-njet
[252] Berk v. Coinbase, para 32*Id.*
[253] *Id.; see also* David Farmer, *Update for Customers With Bitcoin Stored on Coinbase,* COINBASE.COM (July 27, 2017) (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.")
[254] Berk v. Coinbase, para 35
[255] *Coinbase Faces Exodus as Bitcoiners Race to Withdraw, Delays up to 12 Hours,* TRUSTNODES.COM (July 30, 2017) https://www.trustnodes.com/2017/07/30/coinbase-faces-exodus-bitcoiners-race-withdraw-delays-12-hours

currency on December 19, 2017,[256] months after the hard fork occurred. Blockchain.info waited two months, until mid-October to credit Bitcoin accounts with Bitcoin Cash.[257] During the interim, customers lost the opportunity to sell their coins. More importantly, they lost their trust in the promise that cryptocurrency offered them interference free transactions.[258]

ii. Bitfinex Hack

Two months after The DAO fiasco, hackers attacked the cryptocurrency exchange Bitfinex. The hackers stole 119,756 bitcoins (worth more than $65 million at the time).[259] Bitfinex responded by halting trading, deposits and withdrawals, and canceling out all margin positions.[260] This move harkened back to Mt. Gox's 2014 decision to stop investors from pulling out their money when the exchange discovered it was under attack.[261] In the Mt. Gox situation, the exchange filed for bankruptcy and the users lost their money. [262]

A few days after the hack, Bitfinex unilaterally announced that it had "generalized the losses across all accounts,"[263] by reducing all customer holdings by 36%. The exchange unilaterally decided to dock customer accounts. Imagine if a bank, regulated under United States law tried to take such a course of action. But, exchanges are at best loosely regulated, and Bitfinex is based in Hong Kong, well beyond the jurisdiction of United States regulators. 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.[264] In October 2016, Bitfinex offered to

---

[256] Bitcoin Cash FAQ, COINBASE.COM (Dec. 22, 2017). https://support.coinbase.com/customer/portal/articles/2911542

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

[258] *See e.g.*, Sue Marquette Poremba, *What Is Bitcoin? Everything You Need to Know*, Toms Guide (Feb. 5, 2018) *https://www.tomsguide.com/us/what-is-bitcoin,review-5061.html* (describing bitcoin as "free from interference by government and financial institutions.")

[259] Jethro Mullen, *Hackers Steal Bitcoins Worth Millions in Attack on Exchange*, CNN.com (Aug. 3, 2016)

[260] *Announcement: Security Breach*, (Aug. 2, 2016) https://www.bitfinex.com/posts/123.

[261] In this hack, 744,408 bitcoin stolen, worth nearly $400 million at the time.

[262] 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.

[263] *Announcement: Security Breach--Update 3*, (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.

[264] *Id.*

pay a bounty if the hacker would agree to return the coins.[265] In April 2017, the Exchange purportedly redeemed the 'hack coins' and reimbursed all investors.[266]

Time and again, cryptocurrency users have discovered that they have unexpectedly trusted cryptocurrency exchanges with powers far beyond their initial contemplation. The rhetoric about "trustless transactions" obscured the multiple layers of trust actually implicated.

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 (could be dollars, Bitcoin or most commonly Ether) an investor sends to a company's wallet represents a "smart contract" for purchasing ICO coins from the business. These ICO coins 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 will rise, boosting the value of the coins held by the initial investors. Entrepeneurs sell virtual currencies to investors to raise money for software they are building. Roughly 890 such projects raised over $6 billion in 2017.[267]

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—trust that the company exists and is not merely a scam; trust that the promoters have not struck secret deals to promote or prop up their coins. All of 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

---

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

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

[267] The website Icodata.io tracks the activity of ICOs. https://www.icodata.io/ICO/active

transaction, SEC regulations would provide what I have elsewhere called 'regulatory trust'[268]—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."[269] 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." At the time of the ICO, the company was little more than an idea spelled out in a white 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. 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 blockhains and the frenzy of ICOs for outright fraud. For example, the blockchain based fruit company Prodeum that was going to "revolutionize the fruit and vegetable industry"[270] 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.[271] The technology has obvious applications for protecting the public during a food-related health scare, and might also reduce food waste.[272] Yet, Prodeum was a scam. Nine days after the ICO began,

[268] *Bratspies,* Regulatory Trust, *supra* note 81.
[269] Laura Shin, *The Emperor's New Coins: How Initial Coin Offerings Fueled a $100 Billion Crypto Bubble,* FORBES (July 27, 2017).
[270] 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/
[271] Sylvain Charlebois, *How Blockchain Could Revolutionize Food Industry,* GLOBE AND MAIL (Dec. 12, 2017)
[272] *Id.*

Prodeum disappeared with investor money, leaving only the word "penis" on its website.[273] 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.[274] 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.[275]

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."[276] 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."[277]

Some online groups openly try to manipulate the prices of cryptocurrencies through pump-and-dump schemes.[278] These actors create countdown clocks for their coordinated pumping action, designed to move the price of a cryptocurrency. [279] Members pay for access, and for information to allow them to participate in the profitmaking.[280] The website *PumpMyCoin* is fairly typical.[281] One twitter user going by the name @pumpanddumpking boast "I will tweet out which coin will

---

[273] Brian Feldman, *The Blockchain- for-Vegetables StartUp Website Was Replaced with the Word Penis and No One Has a Clear Explanation As to Why* NEW YORK MAGAZINE (Jan. 29, 2018).
[274] Mizrahi, *supra* note 270
[275] Mix, *SCAM,* THE NEXT WEB https://thenextweb.com/hardfork/2018/01/29/cryptocurrency-prodeum-scam-exit-penis/
[276] *See,* The Emperor's New Tokens, *supra* n. __.
[277] Statement of SEC Chairman Jay Clayton (Dec. 11, 2017) https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
[278] Akshay Makadiya, *A Breakdown of Cryptocurrency Pump and Dump,* BtManager (Jan. 24, 2018) https://btcmanager.com/breakdown-cryptocurrency-pump-dump/
[279] Akshay Makadiya, *A Breakdown of Cryptocurrency Pump and Dump,* BtManager (Jan. 24, 2018) https://btcmanager.com/breakdown-cryptocurrency-pump-dump/
[280] Bruno, *The Anatomy of a Pump and Dump Group,* BITFALLS (Jan. 12, 2018) https://bitfalls.com/2018/01/12/anatomy-pump-dump-group/
[281] https://pumpmycoin.com/ 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 "maintains its uptrend to make sure that our community members are satisfied with their gains"

be pumped on binance. Join my personal pump and dump group below !!!"[282] *Wallet Investor* keeps a Pump & Dump Cryptocurrency List indicating which currencies have moved more than 5% in 5 minutes.[283] 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.[284] 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 debase the currency[285] and not commit fraud."[286] Yet, Frauds that leverage the aura of cryptocurrency to scam would-be investors are common.[287] Wildly fluctuating values driven by speculation, and the possibility of dirty deals fly in the face of the rationale behind viewing 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

[282] PumpandDumpKing, https://twitter.com/pumpanddumpking
[283]Pump and Dump Cryptocurrency List, WALLET INVESTOR https://walletinvestor.com/pump-and-dump
[284] Ryan Mac, *Bitcoin Scammers Are Using this App to Fleece People,* BUZZFEED (Jan. 25 2018)(quoting CryptoCallz administrator Maxwell Anderson) Anderson added "it 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."

[285] 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?" *What is Cryptocurrency Part 2*, *supra* n.__. Yet, $100 today, $1000 tomorrow (and $10 the day after) is a pretty good description of the price fluctuations cryptocurrencies routinely experience.
[286] What is Cryptocurrency Part 2, *supra* n.__.
[287] *See* SEC Charges Texas Man With Running Bitcoin Denominated Ponzi Scheme (July 23, 2013) https://www.sec.gov/news/press-release/2013-132.

cryptocurrency. There are quite a few retailers, mostly small and online that accept bitcoin.[288] However, cryptocurrency's touted anonymity has a dark side—it has been used to evade taxes, launder money and trade illicit goods. 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.

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.[289] In January 2017, the operators of cryptocurrency exchange Coin.mx pled guilty to multiple felonies associated with bank fraud.[290] Six months later, FinCEN settled money laundering charges against filed cryptocurrency exchange BTC-e for $110 million.[291] Perhaps the best-known such 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.

---

[288] Jonas Chokun, *Who Accepts Bitcoin as Payment? List of Companies, Stores and Shops,* 99BITCOINS.COM (Jan. 14, 2018) https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/. Some big players like Virgin, Overstock.com and Bloomberg are on this list. However, bitcoin reportedly made up only 0.0002% of Overstock's revenues in 2016-17. Jamie Toplin, *Merchants Aren't Accepting Bitcoin,* BUSINESS INSIDER (July 14, 2017) 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, and Sara Silverstein, *I Spent A Day Trying to Pay for Things With Bitcoin and a Bar of Gold*, BUSINESS INSIDER (Oct. 24, 2017) http://www.businessinsider.com/trying-to-pay-for-things-with-bitcoin-price-gold-2017-10

[289] *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies,* FIN-2013-G001, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[290] *Operator Of Unlawful Bitcoin Exchange Pleads Guilty In Multimillion-Dollar Money Laundering And Fraud Scheme*, Department of Justice, U.S. Attorney's Office for the Southern District of New York, January 9, 2017, https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-pleads-guilty-multimillion-dollar-money-laundering

[291] In the Matter of BTC-e, aka Canton Business Corporation, and Alexander Vinnik, No. 2017-03 (July 27, 2017) https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf ; *FinCEN Fines BTC-e Virtual Currency Exchange $100 Million for Facilitating Ransomware, Dark Net Drug Sales,* (July 17, 2017) https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

The United States is not alone in reacting to the illicit uses of cryptocurrency. China,[292] South Korea, India, Bolivia, Ecuador, Kyrgystan, Morocco and Nepal have all taken steps to outlaw, or severely restrict the use of cryptocurrencies as a medium of exchange.[293] Japan, by contrast, is one of the few countries where cryptocurrency is legally recognized as currency. [294] However, even there, unstable valuations make it a rarely-used option.[295] After the Coincheck hack, Japan cracked down on cryptocurrency exchanges—suspending two and fining five others.[296] Merchants that accept bitcoin as payment still typically price their goods in fiat currency, and immediately convert any paid in bitcoin to fiat currency.

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."[297] This investor behavior finds echo in IRS and SEC regulations, which 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, [298] and requiring investors to report capital gains and losses any time they transfer cryptocurrency.[299] This IRS decisions 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

---

[292] Saheli Roy Choudhury, *China Bans Companies from Raising Money Through ICOs, Asking Local Regulators to Inspect 60 major Platforms*, CNBC.COM (Sept. 4, 2017) https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html .
[293] Amanda Ranzani, *Countries that Have Banned Cryptocurrencies For Now*, COIN CLARITY (Dec. 19, 2017) https://coinclarity.com/countries-that-have-banned-cryptocurrency-for-now/
[294] Quinlan Associates, *Fools Gold* 7
[295] *Id.*
[296] Rishi Iyengar, *Japan Cracks Down on Cryptocurrency Exchanges After Massive Hack*, CNN (March 8, 2018).
[297] Jemima Kelly and Anna Irrera, *Bitcoin Fever Exposes Cryptocurrency Market Frailty*, BUSINESS INSIDER (Dec.13, 2017) http://www.businessinsider.com/r-bitcoin-fever-exposes-crypto-market-frailties-2017-12 (quoting Garrick Hileman)
[298] IRS Virtual Currency Guidance, FAQ I.R.S. Notice 2014-21, (April 14, 2014) http://www.irs.gov/pub/irs-drop/n-14-21.pdf. "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."
[299] *Id.* at Q-1: "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."

on the day of exchange and on the day of acquisition.[300] The IRS treats this gain or loss as ordinary income rather than a capital gain.[301] 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.[302] 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 when Coinbase issued 1099-K forms to its users in January 2018.[303]

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.[304] The very next month, in January 2018, the CFTC brought three fraud cases for unlawful solicitation with regard to Bitcoin futures.[305] The CFTC has brought charges related to virtual currencies before. In 2016, the agency reached a $75,000 settlement with Bitfinex, an exchange it said offered leveraged trading without its approval. The SEC recently refused to approve bitcoin ETFs, citing concerns over valuation and verification. Previously the SEC sued

---

[300] IRS Virtual Currency Guidance, FAQ I.R.S. Notice 2014-21, (April 14, 2014) http://www.irs.gov/pub/irs-drop/n-14-21.pdf. "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."

[301] *Id.* at Q-7. 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.* at Q-8. Miners may potentially be subject to self-employment taxes. *Id* at Q-10.

[302] United States v. Coinbase, Order Re Petition to Enforce IRS Summons (N.D.Cal, 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.).

[303] *Coinbase Has Turned Us All Over to the IRS!!*, REDDIT.COM https://www.reddit.com/r/Bitcoin/comments/7ugdng/coinbase_has_turned_us_all_over_to_the_irs/

[304] The Cboe January 2018 futures contracts were settled on January 17, 2018 for $10,900, a price set by a that day's 4 pm Gemini Exchange bitcoin auction. *Press Release: Cboe Conducts First Settlement of Cboe Bitcoin Futures*, WALL STREET JOURNAL (January 17, 2018) https://www.wsj.com/articles/PR-CO-20180117-915669

[305] 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. 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 STREET JOURNAL (January 19, 2018) https://www.wsj.com/articles/cftc-alleges-fraud-in-three-virtual-currency-cases-1516338060?mod=searchresults&page=1&pos=3

a promoter over an ICO alleging fraud.[306] It is unclear where and how government interventions will be successful.

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.[307] British banks Lloyds Banking Group and Virgin have followed suit, as has Canada's TD Bank.[308] The banks cite concern over volatility as a major justification for this policy.[309] However, it is worth noting that many of these institutions also identify competition from cryptocurrency as a potential business risk.[310] Prior to the ban, 18% of cryptocurrency purchasers reported using credit cards for their purchases, and nearly a quarter reported that they had not paid off the balance.[311]

V. Conclusion

A significant degree of trust is simply inescapable.[312] As blockchain expert Preethi Kasireddy noted: "Blockchain governance is an incredibly tricky problem and finding a balance between centralized and distributed control will be essential to maintaining everyone's trust in the

---

[306] Paul Vigna, *SEC Targets Initial Coin Offering Scam*, Wall St. J. (Dec. 4, 2017).
[307] Evelyn Chang, *J.P. Morgan, Chase, Bank of America & Citi Bar People from Buying Bitcoin With a Credit Card*, CNBC.COM (Feb. 2, 2018) https://www.cnbc.com/2018/02/02/jpmorgan-chase-bank-of-america-bar-bitcoin-buys-with-a-credit-card.html.
[308] John Egan, *Buy Bitcoin With a Credit Card? Big Banks Say No!*, CreditCards.com (Feb. 6, 2018) https://www.creditcards.com/credit-card-news/bitcoin-credit-card-issuers-bar-purchases.php.
[309] *Id.*
[310] *See, e.g.*, Bank of America 10-K, at 15 (2017) https://www.sec.gov/Archives/edgar/data/70858/000007085818000009/bac-1231201710xk.htm#s56FE8F57D1F551E9AF8D375ECF1A891E (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.)
[311] Mike Brown, *Poll: Some Investors Use a Credit Card to Buy Bitcoin and then Carry Over the Balance*, LENDEDU (Dec. 19, 2017) https://lendedu.com/blog/bitcoin-and-credit-cards/.
[312] Joel Valenzula, *Trustlessness is Effectively a Myth*, DASHFORCENEWS.COM (Oct. 8, 2017) https://www.dashforcenews.com/trustlessness-effectively-myth/

system."[313] 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,"[314] 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 "Everything requires trust. Aside from tautologies, it's impossible for you to verify anything without putting your trust *somewhere*."[315] Cryptocurrencies 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 is all about 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, he cryptocurrency Dash claims to be a form of decentralized governance run by its master nodes. Its website contains advice for how to start a 'trustless master node.'[316] 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."[317] As crypto bull, Michael Novogratz stated "Bitcoin is based on an amazing technology. There is a limited supply of it, people are trusting it."[318]

---

[313] Kasireddy, *supra* n. __.
[314] *See*, Nathanial Popper, *As Bitcoin Bubble Deflates, Frauds and Flaws Rise to the Surface,* NEW YORK TIMES (Feb 3, 2018).
[315] Haseeb Qureshi, *Why Bitcoin is Not Trustless*, HACKERNOON.COM (Dec. 18, 2017) https://hackernoon.com/bitcoin-is-not-trustless-350ba0060fc9.
[316] Unknown, *Starting a Trustless Masternode*, DASHPAY (OCT. 21, 2017) https://dashpay.atlassian.net/wiki/spaces/DOC/pages/118129512/Starting+a+Trustless+Masternode
[317] Robert Wiecko, *Understanding the Budget and Governance System*, DASHPAY (Jan. 23, 2018). https://dashpay.atlassian.net/wiki/spaces/DOC/pages/8585240/Understanding+the+Governance+and+Budget+System
[318] Michael Novogratz: *Bitcoin is Digital Gold,* CNBC.COM (Nov. 21, 2017).

At the same time, the lack of trustworthiness in cryptocurrency has created something of a crisis. In a recent Reddit thread, cryptocurrency fans discussed 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,[319] to others sharing similar tales of woe,[320] tto those advising DO NOT TRUST ANYONE"[321] or advocating elaborate security measures[322] to those cynics doubting any theft had happened at all.[323] The OP asks "do you think the solution is a hardware wallet or is there another way? I don't know what to trust."[324]. Another user advises "I personally put my trust in hardware wallets."[325] On another thread, *ADustedeWok* noted "No matter what, at some point your money will be in the hands of a 3rd party. At which point it is vulnerable."[326] In response to the *NiceHash* hack, *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 beginning and now EVERYTHING is a hack? How do you trust them or trust someone?"[327] Users are on their own. As one reddit poster chastises "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[328] 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."[329]

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

[319] [DevilsAdvocate9x1, Reddit: my 387 bitcoins got hacked and stolen]
[320] [Nicecash, yogibreakdance, and Lowrey1017, same thread],
[321] [?? Right after DevilsAdvocate9x1]
[322] [ente, same reddit. "Protip: you risk your coins when retyping the privkey to an online computer. Which you will have to do to actually spend. So create 10, or 100 privkeys/paperwallets, so you only risk the amount you were to spend anyway."]
[323] [BitderbergGroup}.
[324] [deleted, same Reddit threat]
[325] [nibbl0r, same thread]
[326] [Bitcoin reddit: nice hash was hacked looks like 60M stolen]
[327] [Nice Hash 60M thread] [compare to Protherium theft]
[328] [reddit, NiceHash 60M]
[329] Mark FrauenFelder, *I Forgot My Pin: An Epic Tale of Losing $30,000 in Bitcoin,* WIRED (Oct. 29, 2017) https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/.

nameless, unaccountable people they have 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 Web commenter 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."[330]

[330] Mr. Money Moustache, *Why Bitcoin is Stupid*, (Jan. 2, 2018) *http://www.mrmoneymustache.com/2018/01/02/why-bitcoin-is-stupid/*.