BITCOIN OFF-CHAIN TRANSACTIONS: THEIR INVENTION AND USE

Michelle Mount*

CITE AS: 4 GEO. L. TECH. REV. 685 (2020)

TABLE OF CONTENTS

I. INTRODUCTION: WHAT IS AN OFF-CHAIN TRANSACTION, AND WHY IS IT IMPORTANT 685
II. A DIFFERENT BITCOIN MARKET THAN TEN YEARS AGO 686
III. TRADITIONAL BITCOIN TRANSACTIONS VERSUS OFF-CHAIN TRANSACTIONS 687
IV. MAIN METHODS OF OFF-CHAIN TRANSACTIONS 688
A. Payment Channels 689
B. The Omnibus Wallet System 689
V. MAIN BENEFITS OF OFF-CHAIN TRANSACTIONS 690
A. Safeguarding Privacy 690
B. Bolstering Security Protections 692
C. Reducing Lengthy Settlement Times 694
D. Circumventing Volatile Transaction Fees 695
VI. MIXED REGULATORY RESPONSES TO OFF-CHAIN TRANSACTIONS 697
VII. CONCLUSION 698

I. INTRODUCTION: WHAT IS AN OFF-CHAIN TRANSACTION, AND WHY IS IT IMPORTANT

Bitcoin off-chain transactions are transactions in bitcoin that are not recorded on the blockchain.[1] Today, most bitcoin transactions occur off-

* Georgetown University Law Center, J.D. Candidate 2020; Boston University, B.S. Business and Finance. A big thank you to the *GLTR* editors and to Professor Patrick McCarthy for his seminar class on Cryptocurrencies, Initial Coin Offerings and the Law.

[1] AM. BAR ASS'N, DIGITAL AND DIGITIZED ASSETS: FEDERAL AND STATE JURISDICTIONAL 34, (2019), https://www.americanbar.org/content/dam/aba/administrative/business_law/buslaw/committees/CL620000pub/digital_assets.pdf [https://perma.cc/W5WC-95FQ] [hereinafter ABA DIGITAL ASSET PAPER] (defining off-chain transactions in a bitcoin exchange context as

chain.[2] This dynamic runs counter to the quintessential principle espoused in the initial white paper conceptualizing bitcoin—that transactions would be immutably and reliably recorded on a public ledger.[3] As regulators voice concerns over bitcoin's divorce from its ledger technology, this explainer provides an understanding of this innovation's implications on privacy, security, settlement speed, and usability.

II. A DIFFERENT BITCOIN MARKET THAN TEN YEARS AGO

Bitcoin now operates much differently than was envisioned in the initial white paper released by Santoshi Nakamoto in the aftermath of the 2008 global financial crisis. Bitcoin was designed to operate as a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[4] Nakamoto proposed replacing financial intermediaries with blockchain technology,[5] which uses a network of independently-run computers and cryptographic proofs to authenticate currency transfers.[6] The system requires that bitcoin transactions be reported on the blockchain, which

"[a] trade between two parties transacting using a [centralized exchange] is not necessarily recorded on the blockchain"); Lewis Gudgeon et al., *SOK: Layer-Two Blockchain Protocols*, 2019 IACR CRYPTOLOGY EPRINT ARCHIVE 1–2 (defining off-chain transactions in a software protocol context as protocols that enable users to transact "through private and authenticated communication, rather than broadcasting every single transaction on the (parent) blockchain").

[2] *See* Matthew Hougan et al., Bitwise Asset Mgmt., Comment Letter on the Proposed Rule Change Relating to the Listing and Trading of Shares of the Bitwise Bitcoin ETF Trust Under NYSE Arca Rule 8.201-E (May 24, 2019), https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf [https://perma.cc/NKE6-MTY7]; *infra* note 10 and accompanying text.

[3] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1, 8 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/HH9T-EHAS] [hereinafter BITCOIN WHITE PAPER] (proposing a "peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change").

[4] *Id.* at 1.

[5] EUROPEAN SEC. & MKTS. AUTH., DISCUSSION PAPER: THE DISTRIBUTED LEDGER TECHNOLOGY APPLIED TO SECURITIES MARKETS 8 (2016), https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt_0.pdf [https://perma.cc/SM3A-CTSV] ("'Distributed ledgers' and 'Blockchain' are often used interchangeably when discussing the technology. However, the Blockchain is a particular type of distributed ledger originally designed and used for Bitcoins.").

[6] BITCOIN WHITE PAPER, *supra* note 3, at 1 ("What is needed is 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.").

functions as the public immutable accounting ledger for the peer-to-peer network.[7]

Today's bitcoin market departs from Nakamoto's visionary concept in two ways. One, bitcoin is now more popularly used as a speculative investment product, not as an online payment vehicle.[8] And two, most bitcoin transactions are facilitated by financial intermediaries.[9] The result is a bitcoin market where most transactions are not reported to the blockchain.[10]

III. TRADITIONAL BITCOIN TRANSACTIONS VERSUS OFF-CHAIN TRANSACTIONS

In a traditional bitcoin transaction, bitcoin is transferred from one digital wallet address to another. But there is no physical currency to transfer: bitcoin is a string of letters and number while a digital wallet is a public online address that can be accessed with a private key or passcode.[11] Legally, the bitcoin is considered to be transferred after the majority of the network has

---

[7] *Id.* at 8 (noting that the system prevents double spending through a "network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change"); *id.* at 3 (describing the six steps involved in reporting transactions to the blockchain); *see also* ABA DIGITAL ASSET PAPER, *supra* note 1, at 18–20 (giving a general description of blockchain technology).

[8] *See Mapping the Universe of Bitcoin's 460 Million Addresses*, CHAINALYSIS (Dec. 19, 2018), https://blog.chainalysis.com/reports/bitcoin-addresses [https://perma.cc/QD6K-X2MH] ("We estimate that on average only 20% of the bitcoin transaction value is economic, in that it is a final transfer between different people via economically relevant addresses.").

[9] *See* CHAINALYSIS, WHO'S WHO ON THE BLOCKCHAINS? THE CHAINALYSIS GUIDE TO CRYPTOCURRENCY TYPOLOGIES 14 (Feb. 2020), https://go.chainalysis.com/rs/503-FAP-074/images/Typologies-Report-final.pdf [https://perma.cc/J62B-FG8F] (finding that cryptocurrency exchanges account for 90% of all funds sent by services).

[10] *See* Hougan et al., *supra* note 2 (citing research finding that "95% of the [cryptocurrency trading] volume reported to popular data aggregators is either fake or wash trading" and is not reported on the blockchain); *Can On-chain Data Help Us Spot Fake Exchange Trading Volumes?* CHAINALYSIS BLOG (Nov. 15, 2019), https://blog.chainalysis.com/reports/fake-trade-volume-cryptocurrency-exchanges [https://perma.cc/7ZQK-QYTX] (finding the ratio of off-chain transactions to on-chain transactions is between 6:1 and (sometimes) 40,000:1); *see also* Kieran Smith, *TIE Report Names and Shames Fake Volume Exchanges*, BRAVE NEWCOIN (Mar. 26, 2019), https://bravenewcoin.com/insights/tie-report-names-and-shames-fake-volume-exchanges [https://perma.cc/4W87-3GKY].

[11] BITCOIN WHITE PAPER, *supra* note 3, at 2 (defining bitcoin as a "chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin."); *see* Noelle Acheson, *How to Store Your Bitcoin?* COINDESK (Jan. 26, 2018), https://www.coindesk.com/learn/bitcoin-101/what-is-bitcoin [https://perma.cc/7ZJ8-E2PX] (explaining the mechanics of digital wallets).

updated the blockchain ledger to reflect that the specified bitcoin is associated with the receiver's digital wallet.[12]

In an off-chain bitcoin transaction, legal ownership of the bitcoin changes, yet because the bitcoin stays associated with the same digital wallet, the blockchain ledger does not update.[13] To analogize to conventional currencies, a traditional transaction would be transferring money from one bank account to another, while an off-chain transaction would be putting money in a safe deposit box and giving someone the only key. In the second scenario, ownership of and access to the money changes, but the currency does not change locations, and the bank's ledger does not update to reflect the ownership change. Bitcoin intermediaries have developed numerous off-chain methods to transfer legal ownership of bitcoin to circumvent the blockchain.

IV. MAIN METHODS OF OFF-CHAIN TRANSACTIONS

Off-chain transactions regularly occur through a payment channel or an omnibus wallet system. Custodians also effectuate off-chain bitcoin transactions for funds and exchanges.[14] However, as the U.S. Securities & Exchange Commission (SEC) has noted, there are outstanding legal questions about the viability and industry standards of these services.[15]

---

[12] *See* David Mills, et al., *Distributed Ledger Technology In Payments, Clearing, and Settlement* 13–14 (Bd. of Governors of the Fed. Reserve Sys., Discussion Series 2016-095), https://doi.org/10.17016/FEDS.2016.095 (describing how DTL or Blockchain technology transfers ownership of an asset); *see also* BITCOIN WHITE PAPER, *supra* note 3, at 1 ("Digital signatures provide part of the solution . . . [and] [t]he network timestamps transactions by hashing them into an ongoing [block]chain[,] … forming a record that cannot be changed.").

[13] *See* ABA DIGITAL ASSET PAPER, *supra* note 1 and accompanying text.

[14] *See* PETER VAN VALKENBURG, COINCENTER, THE BANK SECRECY ACT, CRYPTOCURRENCIES, AND NEW TOKENS 11–15 (2017), https://coincenter.org/files/2017-05/report-bsa-crypto-token1.pdf [https://perma.cc/7XTX-2DPC] (outlining the differences between the legal definitions of custodial and non-custodial exchanges under the Bank Secrecy Act); *see generally* Chris Kentouris, *Custody: Unchartered Waters for Digital Assets*, FINOPS REPORT (2018), https://finopsinfo.com/investors/custody-unchartered-waters-for-digital-assets/ [https://perma.cc/8F9S-JN75] (describing the market dynamics of the cryptocurrency custodial industry).

[15] Joint Statement, Div. Trading & Mkts., U.S. Sec. & Exch. Comm'n & Fin. Indus. Regulatory Auth., Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities [https://perma.cc/7SU2-CMFJ] [hereinafter Joint Staff Statement] ("The Staffs acknowledge that market participants wishing to custody digital asset securities may find it challenging to comply with the broker-dealer financial responsibility rules…As the market, infrastructure, and law applicable to digital asset securities continue to develop, the Staffs will continue their constructive engagement with market participants and to gather additional information.").

A. Payment Channels

Payment channels are created through software programs that reference bitcoin's software[16] but avoid reporting every transaction immediately to the blockchain.[17] The most popular bitcoin payment channel software is the Lightning Network.[18] The Lightning Network, launched in beta form in March 2018, has grown exponentially, with its capacity increasing 62% between January 2019 and January 2020.[19] Currently, the Lightning Network has the ability to transfer approximately $7 million in bitcoin.[20] The Lightning Network allows parties to pre-allocate capital to a payment channel and keep accounts of transactions between themselves on their ledgers, with net amounts being transferred at a later time.[21] Once the net amount is transferred, the final transaction is reported on the blockchain.[22] Additionally, in December 2019, Bitfinex, one of the world's largest cryptocurrency exchanges, integrated the network into its platform for easier transfers.[23]

B. The Omnibus Wallet System

The omnibus wallet system is another off-chain mechanism used by cryptocurrency exchanges, which are currently responsible for 86% of the economically useful bitcoin wallet addresses.[24] The omnibus wallet system facilitates exchanges' private accounting ledgers.[25] When a customer opts to trade on an exchange, their bitcoin is transferred from their digital wallet to an

---

[16] Bitcoin's software, called "Bitcoin Core," runs on the network of computers that support the bitcoin blockchain; it maintains the rules for how cryptographic proofs are solved and how transactions are reported. *Bitcoin Core*, BITCOIN (Apr. 24, 2020), https://bitcoin.org/en/bitcoin-core/ [https://perma.cc/FC9S-DMVC].

[17] Gudgeon et al., *supra* note 1, at 1–2.

[18] *The Lightning Network Journal: An Overview*, BITFINEX BLOG (Jan. 31, 2010), https://blog.bitfinex.com/trading/the-lightning-network-journey-an-overview/ [https://perma.cc/5QU5-CC74].

[19] *Id.*

[20] *Real-Time Lightning Network Statistics*, 1ML, https://1ml.com/statistics [https://perma.cc/5E4F-NWGC].

[21] Joseph Poon & Thaddeus Dryja, Lightning Network, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments 3–6 (Jan. 14, 2016) (unpublished manuscript), https://lightning.network/lightning-network-paper.pdf [https://perma.cc/J42W-AMFN] (noting that the Bitcoin Lightning Network effectuates real "bitcoin transactions, only electing to defer the broadcast to the blockchain," creating payments that are "communicated and exchanged off-chain").

[22] *Id.*

[23] *The Lightning Network Journal: An Overview*, supra note 18.

[24] *Mapping the Universe of Bitcoin's 460 Million Addresses*, *supra* note 8.

[25] ABA DIGITAL ASSET PAPER, *supra* note 1, at 33–34.

omnibus wallet that the exchange controls.[26] When the customer purchases or sells bitcoins on the exchange, those coins stay in the omnibus wallet.[27] The corresponding amount is debited or credited on the exchange's internal ledger and reflected in the customer's statement of account.[28] Thus, these transfers are not reported on the blockchain.[29] The SEC cited research showing that 95% of the bitcoin transactions on cryptocurrency exchanges consist of these off-chain transactions.[30]

V. MAIN BENEFITS OF OFF-CHAIN TRANSACTIONS

As bitcoin became a global store of value, innovative bitcoin businesses provided services to reduce the costs and risks of trading bitcoin.[31] Bitcoin's transformation into a rapidly traded asset class brought new challenges. For example, bitcoin's public ledger of financial data created serious privacy concerns. Additionally, the lack of intermediaries meant that losses from theft or mistakes were almost irreversible. Further, bitcoin's blockchain settlement time was far too long. And the fees to use bitcoin's blockchain prohibited smaller transactions. Especially for intermediaries with additional financial and regulatory obligations, solving these problems was imperative.[32] Off-chain transacting offered a popular way to address privacy concerns, provide more robust security, reduce costs, and increase transaction speed.

A. Safeguarding Privacy

The transparent nature of bitcoin's public ledger creates privacy challenges.[33] Many people believe that blockchain technology is somewhat anonymous because a person does not need to provide their legal identity to

---

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *See* Matthew Hougan et al., *supra* note 2; *see also* Order Disapproving a Proposed Rule Change Relating to the Listing and Trading of Shares of the Bitwise Bitcoin ETF Fund Under NYSE Arca Rule 8.201-E, 84 Fed. Reg. 55,382, 55,393–94 (Oct. 9, 2019), https://www.sec.gov/rules/sro/nysearca/2019/34-87267.pdf [https://perma.cc/TH4U-ABJA].
[31] *See* Matthew Hougan et al, *supra* note 2, at 4–6 (discussing the rise of bitcoin exchanges).
[32] *See infra* notes 39–40 and accompanying text.
[33] *See* JERRY BRITO & ANDREA CASTILLO, MERCATUS CTR., BITCOIN: A PRIMER FOR POLICY MAKERS 10–12 (2013), https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf [https://perma.cc/J7WJ-D6YF].

transfer bitcoin.[34] But the details of that transaction are broadcast to the blockchain public ledger, resulting in a record of the amounts of bitcoin moving to different wallet addresses.[35] Nakamoto forewarned that, by reviewing the transaction data, the wallet address can be connected with the associated transactions and that when amounts from two wallets are combined and spent in one transaction, the transactions from both wallets may be traced to one wallet owner.[36]

As it turns out, gleaning real-world identities from merely looking at the blockchain is not terribly difficult.[37] Regulatory agencies and cryptocurrency exchanges have increasingly relied on companies that map the blockchain and connect suspicious or illicit transactions to various bitcoin addresses.[38] Chainalysis, one of the more popular providers of this service, claims to have already identified 147 million, or 86%, of the relevant bitcoin wallet addresses.[39] One identity mapping method is a "dust attack." In a "dust attack," identity thieves send small amounts of bitcoin to digital wallets in an attempt to analyze the wallet owner's spending patterns and uncover their identity.[40] The potential for identity mapping engenders serious security concerns. Once a bitcoin holder's identity is uncovered, the holder could be the target of phishing or physical attacks.

In contrast, off-chain transactions do not broadcast information on the public ledger.[41] This alternative practice provides additional privacy that is particularly helpful to bitcoin intermediaries who are "engaged as a business

---

[34] *See id.*; *see also* BITCOIN WHITE PAPER, *supra* note 3, at 6 ("The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.").

[35] BITCOIN WHITE PAPER, *supra* note 3, at 6.

[36] *Id*. (advising that "a new key pair [to a wallet address] should be used for each transaction to keep them from being linked to a common owner…Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner."). Because of bitcoin dust—small amounts of bitcoin left over from larger transactions—combining the amounts in two wallets is often necessary.

[37] BRITO & CASTILLO, *supra* note 33, at 11; *see* Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, 2012 IACR CRYPTOLOGY EPRINT ARCHIVE 596, 597 (2012), http://fc13.ifca.ai/proc/1-3.pdf [https://perma.cc/375L-VDPH] (finding that in a research study using behavior-based clustering techniques, researchers could identify 40% of the bitcoin users in their simulated experiment).

[38] *See* Jimmy Aki, *Chainalysis Raises $30 Million in Series B Funding from Accel Ventures*, BITCOIN MAG. (Feb. 14, 2019), https://bitcoinmagazine.com/articles/chainalysis-raises-30-million-series-b-funding-accel-ventures [https://perma.cc/CLQ3-AU7W].

[39] *Mapping the Universe of Bitcoin's 460 Million Addresses*, *supra* note 8.

[40] *See What Is a Dusting Attack?* BINANCE ACAD. (Sept. 12, 2019), https://www.binance.vision/security/what-is-a-dusting-attack [https://perma.cc/ZH9A-9NAM].

[41] *See supra* note 1 and accompanying text.

in the exchange of virtual currency."[42] These companies are required by the Bank Secrecy Act to collect their customers' identification information for reporting purposes.[43] As a result, these intermediaries carry additional privacy risk by holding customers' personal information along with customers' digital wallet information. In a cybersecurity breach, off-chain transactions can provide another layer of protection between their customers' identities, private keys, and financial data.[44]

B. Bolstering Security Protections

Bitcoin operates through a network of independently-run computers, so no governing third party can reverse fraudulent transactions.[45] If a hacker gains access to a server that holds a user's private key information, they can use the private key to gain control of the user's digital wallet and irreversibly transfer the bitcoin.[46] As Chainalysis advised in its 2019 report on crypto

---

[42] *See* VAN VALKENBURG, *supra* note 14, at 5–8 (discussing Financial Crimes Enforcement Network's guidance on applying the Bank Secrecy Act requirements to cryptocurrency businesses); *see also* Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151, 45151–74 (Aug. 4, 2014) (to be codified in 31 CFR Parts 1010, 1020, 1023, 1024, and 1026), https://www.fincen.gov/sites/default/files/shared/CDD-NPRM-Final.pdf [https://perma.cc/6UJK-NU9S].

[43] *See BSA Requirements for MSBs*, FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/bsa-requirements-msbs [https://perma.cc/2A7J-ZCT4] (listing requirements for MSBs including the issuance of Currency Transaction Reports, Suspicious Activity Reports, and establishment of an Anti-Money Laundering program); *see also* Public Statement, Heath Tarbert, Chairman, CFTC, Kenneth A. Blanco, Director, FinCEN, & Jay Clayton, Chairman, SEC, Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets, (Oct. 11, 2019), https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets [https://perma.cc/Y8PP-HV7X].

[44] *See* Elli Androulaki*, Private and Confidential Transactions with Hyperledger Fabric*, IBM INFRASTRUCTURE BLOG (Feb. 8, 2019), https://developer.ibm.com/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/ [https://perma.cc/7BH8-P67H] (discussing the cybersecurity risks of public blockchain's and advocating for private ledger for reporting systems that are built on top of the bitcoin blockchain); Jeff Eckard, *Storage for Blockchain and Modern Distributed Database Processing*, IBM INFRASTRUCTURE BLOG (May 11, 2018), https://www.ibm.com/blogs/systems/storage-for-blockchain-and-modern-distributed-database-processing/ [https://perma.cc/6HLM-U2KF] (detailing examples of off-chain reporting solutions).

[45] *See* BITCOIN WHITE PAPER, *supra* note 3, at 1 (noting that by removing financial intermediaries "[c]ompletely non-reversible transactions" would be possible).

[46] *See* ABA DIGITAL ASSET PAPER, *supra* note 1, at 20–21 (discussing the mechanisms of digital wallets); *see also generally* CHAINALYSIS, CRYPTO CRIME REPORT (2019), https://assets.website-files.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20Januar

crime, "Hacking is on the rise partly because it works. It is hard to defend against given the scale of the adversaries. So, the stakes are high for exchanges and the cryptocurrency ecosystem more generally."[47] In 2018 alone, cryptocurrency hackers stole $1 billion worth of digital assets.[48]

Additionally, bitcoin are susceptible to being lost and misplaced.[49] Without a third-party intermediary, lost bitcoin passwords, or private keys, are not recoverable and there is no controller to reverse the transaction if a user inadvertently sends bitcoin to the wrong digital wallet address.[50] A 2018 study estimated that more than 13.5% of all mined bitcoin had been lost.[51] At the time of the writing of this article, that amounts to $142.2 billion.[52]

In an off-chain transaction, bitcoin stays in the same digital wallet address, and a private key is not used.[53] Therefore, private keys may be held off-line or in a manner that is less accessible to hackers, reducing the risk of theft.[54] Additionally, when a cryptocurrency exchange initiates an off-chain transaction on its private accounting ledger, the exchange can reverse it. Especially for bitcoin businesses, reliance on off-chain transactions can mitigate the cost of mistakes in governance, operational structure, and network security.[55]

---

y%202019%20Crypto%20Crime%20Report.pdf [https://perma.cc/3FA2-KB5H] [hereinafter CRYPTO CRIME REPORT] (providing on overview on cryptocurrency hacking).

[47] CRYPTO CRIME REPORT, *supra* note 46, at 9.

[48] *Id.* at 4.

[49] *See Bitcoin's $30 Billion Sell-Off*, CHAINALYSIS INSIGHTS BLOG (June 8, 2018), https://blog.chainalysis.com/reports/money-supply [https://perma.cc/658X-DZEN] (calculating the amount of lost bitcoin from misdirected transactions or loss of private keys).

[50] *See generally* FIN. INDUS. REGULATORY AUTH., DISTRIBUTED LEDGER TECHNOLOGY (2017), https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf [https://perma.cc/AG3E-VUQZ] [hereinafter DISTRIBUTED LEDGER TECHNOLOGY] (discussing governance risks of operating the bitcoin network without a central governing body).

[51] *See Bitcoin's $30 Billion Sell-Off, supra* note 49 ("[O]f the 21 million Bitcoins that will ever exist, around 4 million are currently unmined, [and] at least 2.3 million are lost").

[52] *Id.*; *see Bitcoin Price,* COINDESK (Mar. 21, 2020, 1:20 PM), https://www.coindesk.com/price/bitcoin [https://perma.cc/WK6V-T3DS] (showing the current price of bitcoin at $6,184). Based on 2.3 million lost bitcoin multiplied by an exchange rate of $6,184 per bitcoin.

[53] *See* discussion *supra* Part III.

[54] *See* DISTRIBUTED LEDGER TECHNOLOGY, supra note 50, at 10–11 (raising questions illustrating the role of key management in cryptocurrency broker-dealer's network security and design).

[55] *Id.* at 7–11 (discussing the governance, operational, and network security risks to broker–dealers when effecting transactions that are reported on the bitcoin blockchain).

C. Reducing Lengthy Settlement Times

Bitcoin transactions can take hours to settle. This delay is partly due to an encoded limitation in bitcoin's software and partly due to market dynamics. Bitcoin's software is limited to processing up to seven transactions per second.[56] However, it takes around ten minutes for a group of transactions to be confirmed and reported in a block on the blockchain.[57] If there is a disputed transaction, it may take six blocks (around one hour) before the network reaches a satisfactory consensus on the transaction's validity.[58] The processing speed also depends on the cost of the transaction fee paid.[59] If a user opts to pay a cheaper transaction fee, they may only be guaranteed that the transaction is reported in one of the next six blocks.[60] As a result, the clearing times for blockchain transactions could be up to two hours.[61]

Off-chain transactions through exchanges and payment channels do not utilize the blockchain and, therefore, can be executed and settled immediately.[62] These benefits are critical for cryptocurrency exchanges,

---

[56] Ramil Khalil et al., *Revive: Rebalancing Off-Blockchain Payment Networks*, *in* CCS '17: PROCEEDINGS OF THE 2017 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS 439–53, (2017), https://acmccs.github.io/papers/p439-khalilA.pdf [https://perma.cc/A5GE-88RD].

[57] M. Szmigiera, *Average Confirmation Time of Bitcoin Transactions from September 2017 to September 2018,* STATISTA (Oct. 4, 2019), https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time [https://perma.cc/KQ8H-K7YE] (noting that in September 2019, "the average confirmation time for a bitcoin transaction was 10.08 minutes," lower than bitcoin's two-year peak of over fourteen minutes).

[58] *See* Joseph Bonneau, *How Long Does It Take for a Bitcoin Transaction to Be Confirmed,* COINCENTER (Nov. 3, 2015), https://coincenter.org/entry/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed [https://perma.cc/M8TC-MSRC]; BITCOIN WHITE PAPER, *supra* note 3, at 7–8 (stating "[w]e now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. [Calculating] the probability the attacker could still catch up . . . we can see the probability drop off exponentially with z," and finding that the probability is less than 0.1% after 5 blocks).

[59] David Easley et al., *From Mining to Markets: The Evolution of Bitcoin Transaction Fees*, 134 J. FIN. ECON. 91, 95 (2019) ("Users submit transactions . . . they want verified and posted on the blockchain. They play a game in which they can chose to pay a fee to move up in the queue and thus reduce their waiting time, or they cannot pay a fee and experience a longer waiting time.").

[60] *Bitcoin Transaction Fees*, BILLFODL (Mar. 21, 2020, 1:20 PM), https://billfodl.com/pages/bitcoinfees [https://perma.cc/JA9H-HDRL] (showing fees to have a transaction mined in the next block, within three blocks, and within six blocks).

[61] *See id.*

[62] Gertude Chavez-Dreyfuss, *Blockchain Launches Cryptocurrency Exchange with Trades at High Speed*, REUTERS (July 30, 2019), https://www.reuters.com/article/us-crypto-currency-

which can execute billions of bitcoin transactions a day.[63] Even in one large transaction between two parties, an off-chain transaction may be needed to reduce counterparty and clearing risk.[64] Unlike the central clearing systems in securities, commodities, and derivatives, bitcoin's decentralized system means that there is no central counterparty to guarantee the settlement before the transaction clears. Third parties can guarantee off-chain transactions and provide instantaneous execution to reduce parties' counterparty risk and currency risk during periods of price volatility.[65]

D. Circumventing Volatile Transaction Fees

Using bitcoin has costs.[66] The businesses running the computers behind the peer-to-peer nodes (often called miners) use considerable electricity and sophisticated computing equipment while expecting to earn a profit.[67] Initially, the system rewards the miners for their work with new bitcoin.[68] Yet, Nakamoto believed in a finite supply of bitcoin, and he programmed the bitcoin software to decrease the miners' compensation as the number of transactions rises, so eventually the miners' compensation would be zero.[69] Nakamoto hypothesized that as bitcoin became more popular, users would voluntarily pay fees to the miners to expedite their transactions, the size of which would be dictated by market demand.[70]

---

exchange/blockchain-launches-cryptocurrency-exchange-with-trades-at-high-speed-idUSKCN1UP18H [https://perma.cc/4CUF-V26Z] (discussing the competition between cryptocurrency exchanges that execute trades in microseconds, and those that execute in milliseconds); Poon & Dryja, *supra* note 21, at 1–4 (showing how the Lightning Network solves bitcoin's scalability problem by facilitating many more transactions per second).

[63] *Top 100 Cryptocurrency Exchanges by Trade Volume,* COINMARKETCAP, https://coinmarketcap.com/rankings/exchanges/ [https://perma.cc/F7X4-3RWB].

[64] *See* ABA DIGITAL ASSET PAPER, *supra* note 1, at 33 (noting that exchanges—which use off-chain transactions—mitigate counterparty risk).

[65] *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 50, at 5–6 (noting that real-time settlement or the functional equivalent—which takes place in off-chain transactions—can mitigate counterparty risk and decrease market inefficiencies).

[66] *See What is the Bitcoin Mining Block Reward?*, BITCOIN MINING, https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/ [https://perma.cc/Q2KT-5EVT].

[67] *Id.*

[68] *Id.*

[69] Easley et al., *supra* note 59, at 94 (estimating that the miners' programmed reward will reach zero around the year 2140).

[70] *See* BITCOIN WHITE PAPER, *supra* note 3, at 4 (envisioning transaction fees as an additional incentive for miners).

That hypothesis has come to pass. The fees paid to miners to expedite bitcoin transactions have increased rapidly and can vary wildly.[71] Before 2017, the average fee per transaction rarely reached $1.[72] Then in late 2017, the average transaction fee touched $55; it has since retreated.[73] The market dynamics behind transaction fees are complex and hard for companies to protect against through hedges or budgeting.[74] Bitcoin transaction fees are fixed per transaction, unlike credit card fees, which are calculated as a percentage of the dollar value of the transaction.[75] In periods of high transaction fees, smaller amounts of bitcoin may be worth less than the transaction fees.[76] Thus, these amounts become effectively unspendable—trapped as "bitcoin dust."[77] One study estimated that at the height of transaction prices in 2017, almost $50 million' worth of bitcoin became bitcoin dust.[78]

Off-chain transactions may be the only way to spend bitcoin dust and avoid its accumulation. Because transacting off-chain does not utilize the blockchain, there are no bitcoin transaction fees, and thus bitcoin is not trapped as dust. Circumventing transaction fees is critical for businesses that require high-volume trading, such as bitcoin exchanges and high-frequency bitcoin traders.[79] Also, payment channels can facilitate small transactions that would not have been possible on the blockchain due to transaction fees.[80] Overall, off-chain transactions can reduce users' exposure to transaction fees'

---

[71] Easley et al., *supra* note 59, at 93 (with table panel A, showing that from 2013 to 2015, total transaction fees stayed around $2.3 million, but in 2016 bitcoin users were opting to pay $13.5 million in fees for expedited processing time).

[72] *Bitcoin Avg. Transaction Fee Historical Chart*, BITINFOCHARTS, https://bitinfocharts.com/comparison/bitcoin-transactionfees.html [https://perma.cc/TBV8-HN5C].

[73] *Id.*

[74] *See Bitcoin Hash Rate, Miner Margins Shift Back into Growth* 3 DIAR, Mar. 4, 2019, at 2 https://diar.co/volume-3-issue-8/#2 [https://perma.cc/N769-RDL9] (discussing the complex interplay of miners' revenues, cash flow, overall gross margin, and the bitcoin hash rate, which put smaller miners out of the market); *see generally* Easley et al., *supra* note 59 (analyzing the market economics of bitcoin mining and its impact on miners' and bitcoin users' decisions).

[75] *Bitcoin Transaction Fees, supra* note 60; *but see* Dhruv Bansal, *Bitcoin Data Science Part 3: Dust & Thermodynamics*, UNCHAINEDCAPITAL (Dec. 18, 2018), https://www.unchained-capital.com/blog/dust-thermodynamics/ [https://perma.cc/6M6S-UYE9] (explaining how fees are more complicated to calculate when various containers of bitcoin are spent in a single transaction).

[76] *See* Bansal, *supra* note 75.

[77] *Id.*

[78] *Id*.

[79] Chavez-Dreyfuss, *supra* note 62.

[80] Poon & Dryja, *supra* note 21, at 1–4.

variability and to unexpected liquidity crunches resulting from bitcoin's dust dynamic.

VI. MIXED REGULATORY RESPONSES TO OFF-CHAIN TRANSACTIONS

Regulators are still navigating the implications of off-chain bitcoin innovations. While off-chain transactions have made the cryptocurrency significantly more usable, there are risks in bitcoin's widespread divorce from its blockchain accounting functionality. Thus far, the regulatory consensus is mixed. The SEC has raised a concern that because unregulated off-chain transactions now account for a significant portion of the total bitcoin market, bitcoin's price is susceptible to market manipulation.[81] The Commodity Futures Trading Commission (CFTC) cautioned that it may be hard to "adequately assess the inherent risk of virtual currency contracts."[82] The SEC and the Financial Industry Regulatory Authority have cautioned that there are still ongoing questions around broker-dealer custody digital assets.[83] While the SEC has thus far disapproved every attempt to launch a bitcoin-based ETP on national stock markets,[84] the CFTC has approved a variety of bitcoin derivative products to launch under a heightened regulatory review process.[85]

---

[81] *See* Order Disapproving a Proposed Rule Change, as Modified by Amendment No. 1, To Amend NYSE Arca Rule 8.201–E (Commodity-Based Trust Shares) and To List and Trade Shares of the United States Bitcoin and Treasury Investment Trust Under NYSE Arca Rule 8.201–E, 85 Fed. Reg. 12595, 12600–01 (Mar. 3, 2020) (discussing the types of possible fraud and manipulation from unregulated off-chain transactions and noting that this could affect the values that the ETF would be based on); *id.* at 12600 n.66 ("[S]tating that the sponsor of the proposed ETP presented an analysis of the bitcoin spot market that asserts that 95% of the spot market is dominated by fake and non-economic activity, such as washtrades."); *but see* Comm'r Hester M. Peirce, Sec. & Exchange Comm'n, Dissenting Statement, In Response to Release No. 34-88284; File No. SR-NYSEArca-2019-39 (Feb. 26, 2020), https://www.sec.gov/news/public-statement/peirce-dissenting-statement-34-88284 [https://perma.cc/6KAB-STD4].

[82] CFTC Staff Advisory No. 18-14 (May. 21, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/%40lrlettergeneral/documents/letter/2018-05/18-14_0.pdf [https://perma.cc/MT96-2V6Q].

[83] Joint Statement, *supra* note 15 ("Staffs have been engaged with industry participants regarding . . . custody solution[s] for digital asset securities. . . . The Staffs encourage and support innovation and look forward to continuing our dialogue . . . .").

[84] *See* sources cited *supra* note 81.

[85] Public Resource, U.S. Commodity Futures Trading Comm'n, CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets 2–3 (Jan. 4, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf [https://perma.cc/KKG4-USN7].

VII. CONCLUSION

Bitcoin innovation will likely continue. Other exchanges and custodial wallet services may follow Bitfinex's lead by integrating the Lightning Network into their systems, redistributing more bitcoin into payment channels.[86] If cryptocurrency exchanges move to facilitate high frequency trading, the number of possible off-chain transactions per second will increase.[87] More numerous and rapid transactions could make tracing fraudulent payments more difficult.[88] An influx of activity in cryptocurrency exchanges could also result in wallets holding more bitcoin dust, spurring the need for further innovation.[89] Bitcoin intermediaries, security experts, and regulators must stay vigilant as the marketplace continues to evolve.

[86] *See The Lightning Network Journal: An Overview*, *supra* note 18.
[87] Chavez-Dreyfuss, *supra* note 62.
[88] CRYPTO CRIME REPORT, *supra* note 46.
[89] Poon & Dryja, *supra* note 21, at 54.