kraken INTELLIGENCE

ORDO AB CRYPTO

BITCOIN

Vires in Numeris

BITCOIN (BTC)

Vires in Numeris

+ An asset primer detailing the history and core design of bitcoin
+ A discussion of scaling trends and challenges
+ An overview of observed adoption across the bitcoin network

PRICE	TX/DAY	MARKET CAP	TOTAL BTC SUPPLY
$9,673	302K	$174B	21M

Data as of 31 May 2020 • Source: blockchain.com

EXECUTIVE SUMMARY

Learning about bitcoin is hard. It may often entail wading through specialized courses targeting software developers, pages and pages of forums and tweets, or endless blog posts to find the answer to a single question. Even more challenging is knowing which questions to ask and where to start. This primer serves as a holistic guide to understanding the core design of bitcoin and as a starting point for more advanced reading.

Over the last decade bitcoin has proven to be an effective store of value, albeit with volatility, and has the potential to become a non-sovereign, accessible, and global payment mechanism. In this report, we begin with a brief background on the cypherpunk movement predating bitcoin, showing how many of the ideas contributing towards bitcoin's design were conceived decades in the past. We will describe the core components of the protocol and their roles. We then delve into a high-level timeline of key events to provide you with context for follow-up reading. Lastly, we cover key challenges with respect to scalability, discussing the transaction throughput of bitcoin's design, and dive into network scalability and adoption. We hope this primer represents a foundation for your crypto journey.

Table of Contents

Disclosures

This document is for information purposes only and must not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy with respect to any financial instrument or the issuers thereof. This report must be read with the Disclosure Appendix.

I.

ORIGINS

Bitcoin is the first globally-accepted, digital, and fully decentralized money.

Despite the novelty of bitcoin, the key ingredients underpinning its launch in 2009 came many years earlier. Perhaps the most important pillar of the bitcoin protocol - and cryptocurrency in general - is public-key cryptography. This asymmetric encryption method obfuscates communication such that it can be readable by anyone, but only be deciphered by the intended audience. This encryption method dates back to 1977, when Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA encryption algorithm, which proved foundational to the security of the internet and, by extension, the bitcoin network.[1] In 2001, the National Security Agency (NSA) developed a set of cryptographic hashing functions called Secure Hashing Algorithms, SHA-1 and SHA-2, which rely on RSA encryption methods. Today, the bitcoin network utilizes one of these SHA functions in its cryptographic design: the SHA-256 hashing algorithm.[2]

The public release of RSA sparked a 'cypherpunk' movement of independent cryptographers, each looking to build applications for the public domain. Cypherpunk roots can be traced back to David Chaum's 1982 paper "Blind Signatures for Untraceable Payments."[3] Though the intentions of the cypherpunk movement spanned a range of cryptographic applications, many of these activists devoted their efforts towards software-based payments systems that promote privacy and censorship resistance. Cypherpunks communicated and collaborated with each other from the 1990s through the 2000s via an email listserv. Among them are several, now-famous experts of the cryptosphere: Hal Finney, Adam Back, Nick Szabo, and Satoshi Nakamoto.[4] In some respects, bitcoin is the culmination of various cypherpunk projects, including

1 "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" R.L. Rivest, A. Shamir, and L. Adleman (https://people.csail.mit.edu/rivest/Rsapaper.pdf)

2 "Part 5: Hashing with SHA-256" Cédric Bellet (https://medium.com/biffures/part-5-hashing-with-sha-256-4c2afc191c40)

3 "Blind Signatures for Untraceable Payments" David Chaum (https://www.chaum.com/publications/Chaum-blind-signatures.pdf)

4 "The untold history of Bitcoin: Enter the Cypherpunks" PetriB (https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1)

David Chaum's eCash/Digicash,[5,6] Wei Dai's B-money,[7,8] Adam Back's Hashcash,[9,10] Nick Szabo's Bit Gold,[11,12] and Hal Finney's RPOW[13] (see figure 1). Satoshi Nakamoto, the pseudonymous author of the bitcoin whitepaper and the creator of the first version of the bitcoin protocol, referenced several of these cypherpunk projects in the whitepaper.[14] In 2010, Satoshi even stated that bitcoin was in fact a combination of B-money and Bit Gold,[15] proving bitcoin to be a refined version of prior attempts at a peer-to-peer cryptocurrency.

Though most of the building blocks for the bitcoin protocol came well before its inception, Satoshi Nakamoto is credited for designing a working protocol that allows unrelated participants to transact using bitcoin in a trustless manner.

Figure 1

Cypherpunk projects relating to payments and precursors to bitcoin

PROJECT	CREATOR	YEAR PUBLISHED	FEATURES	DESCRIPTION
eCash/ Digicash	David Chaum	1983	• Blind signatures	Semi-decentralized electronic money ideal for micropayments
B-money	Wei Dai	1998	• Distributed ledgers • Public/private keys • Proof-of-Stake • Smart Contracts	Two proposals for a fully decentralized digital money system, one similar to bitcoin and another similar to ethereum
Hashcash	Adam Back	1997	• Proof-of-Work	A Proof-of-Work mechanism to eliminate email spam. This was not a full-fledged currency system, but a tool to be used to create digital scarcity through computing power limitations.
Reusable Proofs of Work (RPOW)	Hal Finney	2004	• Proof-of-Work Tokens	A proposed decentralized money system using Proof-of-Work to create a reusable, scare token backed by a centralized server running cryptographically verifiable software
Bit Gold	Nick Szabo	2005	• Proof-ofWork • Chain of Hashes	A proposed decentralized money system using Proof-of-Work from Hashcash and a chain of hashes to create a digital ownership registry, both similar to bitcoin

Source: Kraken Intelligence

5 "DigiCash" David Chaum (https://www.chaum.com/ecash/)

6 "The Genesis Files: How David Chaum's ECash Spawned A Cypherpunk Dream" Bitcoin Magazine (https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream/)

7 Official Website of B-money (http://www.weidai.com/bmoney.txt)

8 "The Genesis Files: If Bitcoin Had A First Draft, Wei Dai's B-Money Was It" Bitcoin Magazine (https://bitcoinmagazine.com/articles/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it/)

9 Official Website of Hashcash (http://www.hashcash.org/)

10 "The Genesis Files: Hashcash Or How Adam Back Designed Bitcoin's Motor Block" Bitcoin Magazine (https://bitcoinmagazine.com/articles/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block/)

11 "Bit Gold" Nick Szabo (https://nakamotoinstitute.org/bit-gold/)

12 "The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin" Bitcoin Magazine (https://bitcoinmagazine.com/articles/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin/)

13 "Reusable Proofs of Work" Hal Finney (https://nakamotoinstitute.org/finney/rpow/index.html)

14 "Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf)

15 Bitcoin Talk Forum (https://bitcointalk.org/ndex.php?topic=342.msg4508#msg4508)

II.

THE PROTOCOL

The bitcoin protocol can be broken down into four components: the blockchain, network nodes, miners, and proof-of-work consensus.

- The **blockchain**, also known as the **distributed ledger**, is a database of transactions that is replicated and shared over a network of nodes (computers). This shared database has a complete record of all transactions, organized in linked containers called **blocks**. Blocks form a chain-like structure where each block contains metadata[16] of the preceding block, which allows the network to detect and reject attempts to alter historical records. Even the slightest alteration of historical data is easily detected by using the SHA-256 hashing algorithm.[17]
- **Nodes** store replica copies of the blockchain and are responsible for verifying incoming transactions. Nodes validate transactions in the memory pool (mempool), or a queue of unconfirmed transactions, and propagate successfully mined blocks.
- **Miners** run specialized hardware and compete to package and propose new blocks to the network, confirming transactions from the mempool in the process. Miners are rewarded with newly minted bitcoin and transaction fees if their block is accepted by the network. The process of mining involves an expenditure of computing power to create valid proof-of-work, the basis for bitcoin consensus.[18] The block reward and expenditure of computing power incentivizes honest mining and ultimately guards the security of the network.

Figure 2

Example of hashing via SHA-256

INPUT	OUTPUT (SHA-256 HASH)
bitcoin	6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
Bitcoin	b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

Source: Kraken Intelligence

Note: the change in input word - 'bitcoin' to capitalized 'Bitcoin' yields a completely new output

16 Metadata is a set of data describing other data.

17 SHA-256 Hash Generator (https://emn178.github.io/online-tools/sha256.html)

18 Cryptocurrency Mining - A Primer, Kraken Intelligence (https://blog.kraken.com/wp-content/uploads/2019/04/Cryptocurrency-Mining-A-Primer-April-2019.pdf)

- **Proof-of-work (PoW) consensus** is a set of network rules that take part in determining the order of blocks and transactions. The proof-of-work is the mathematical result that signals a miner exhausted a minimum expected amount of computational effort, consuming electricity in the process. The bitcoin network acknowledges the transaction history with the most accumulated proof-of-work as the "main chain," or the "true" transaction history. This is also referred to as the **Nakamoto consensus.**

The bitcoin protocol creatively solves the Byzantine Generals' Problem of peer-to-peer networks through the interplay of these components.[19] It decentralizes the transaction validation process to nodes dispersed across peers, enabling users to reliably access a trustless network without relying on a centralized third party. This underpins the network's censorship resistance and allows users to transact cheaply and securely. If one or more nodes fail or drop out of the network, there is enough redundancy to allow the network to continue functioning.

For a closer look at the mining process and proof-of-work consensus, we recommend our Cryptocurrency Mining Primer.[20]

19 The Byzantine Generals' Problem is a problem faced on distributed and trustless peer-to-peer networks, where all parties must reach consensus despite potential malicious actors.This is relevant to the bitcoin blockchain as participating nodes must agree on one main blockchain as the single source of truth, despite potential malicious nodes and miners. (https://medium.com/all-things-ledger/the-byzantine-generals-problem-168553f31480)

20 Cryptocurrency Mining - A Primer, Kraken Intelligence (https://blog.kraken.com/wp-content/uploads/2019/04/Cryptocurrency-Mining-A-Primer-April-2019.pdf)

III. KEY EVENTS

2008 — **bitcoin whitepaper published**

2009 — **launch of bitcoin (v0.1)**

2010 — **launch of BitcoinMarket.com, the first bitcoin exchange**: bitcoin made its way mainstream as cryptocurrency exchanges began to emerge. Despite the numerous cryptocurrency exchanges that saturate the industry today, exchanges or markets didn't appear until March 2010.[21]

bitcoin pizza: the first broadly discussed use of bitcoin as a payment method was on May 22, 2010, when a programmer named Laszlo Hanyecz used an online chat forum to purchase two large pizzas for 10,000 BTC,[22] worth around $30 at the time.[23] Bitcoin was just over a year old and not yet recognized as a viable form of payment. Today, this purchase would be worth ~$79M.

launch of the first bitcoin faucet: in its nascency, the acquisition and distribution of bitcoin was a challenge for everyday users. In June 2010 software developer Gavin Andresen created the first bitcoin "faucet." Faucets were a popular way to give away free bitcoin.[24] Faucets were important as bitcoin was largely only attainable through mining or direct purchases between two parties at the time.[25]

launch of Mt. Gox: Mt. Gox launched in July 2010, becoming the world's leading bitcoin exchange by 2013 and handling over 70% of the world's bitcoin trading volume at its peak.[26,27,28]

2011 — **emergence of cryptocurrencies**: following in the footsteps of bitcoin, rival cryptocurrencies emerged. Most notably, Namecoin (NMC), Swiftcoin (SWIFT), and Litecoin (LTC) were the first three initial alternative assets created as a code fork off of bitcoin.

2012 — **first bitcoin halving**: bitcoin's first halving took place at block 210,000, reducing the block reward from 50 bitcoins to 25 bitcoins. At 144 blocks are mined per day, the first halving caused daily rewards to decline from 7,200 to 3,600 bitcoins.[29]

2013 — **bitcoin banned in China**: China bans its banks from handling bitcoin-related transactions.

BerkeleyDB bug in release of bitcoin version 0.8: the implementation of bitcoin version 0.8 came with an accidental removal of a BerkeleyDB database lock limit, which increased the block size for those upgrading to this new version. This caused an unplanned hard fork as half the network that had migrated onto version 0.8 was incompatible with the other half still on version 0.7. This chainsplit was eventually resolved by forcing the bitcoin community and miners back to version 0.7.[30]

first U.S. congressional hearing: the Senate Committee on Homeland Security and Governmental Affairs held its first congressional hearing on bitcoin and the implications on the growing popularity of cryptocurrencies. The hearing was largely inconclusive yet positive.

2014 — **fall of Mt. Gox:** during 2011-2014, Mt. Gox experienced a series of exchange hacks where over 850,000 bitcoins were stolen, eventually leading to its messy demise.[31]

21 History of Bitcoin (historyofbitcoin.org)

22 Bitcoin Pizza Transaction ID: a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d (https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d)

23 Discussion about the Bitcoin Pizza on Bitcoin Talk Forum (https://bitcointalk.org/index.php?topic=137.0)

24 The promotion of cryptocurrency tokens through a free distribution to network community members' wallet addresses.

25 "Bitcoin History Part 3: Turning on the Faucet " Bitcoin.com (https://news.bitcoin.com/bitcoin-history-part-3-turning-on-the-faucet/)

26 History of Mt. Gox (https://www.investopedia.com/terms/m/mt-gox.asp)

27 "Bitcoin History Part 2: The Bitcoin Symbol" Bitcoin.com (https://news.bitcoin.com/bitcoin-history-part-2-the-bitcoin-symbol/)

28 "Hack Flasback: The Mt.Gox Hack – The Most Iconic Exchange Hack" Ledger (https://www.ledger.com/hack-flasback-the-mt-gox-hack-the-most-iconic-exchange-hack/)

29 The Halving: Trends and Implications of Bitcoin's Inflation Mechanism, Kraken Intelligence (https://blog.kraken.com/wp-content/uploads/2020/02/Bitcoin_Halving_F_v09.pdf)

30 Discussion about BDB Bug in Version 0.8 Upgrade on Bitcoin Talk Forum (https://bitcointalk.org/index.php?topic=152030.0)

31 "Hack Flasback: The Mt.Gox Hack – The Most Iconic Exchange Hack" Ledger (https://www.ledger.com/hack-flasback-the-mt-gox-hack-the-most-iconic-exchange-hack/)

2016

Lightning Network whitepaper published: the Lightning Network is a second layer protocol that emerged initially as a concept through Satoshi Nakamoto's idea of instant payment channels, but more successfully through the publication of a white paper in early-2016.[32] The Lightning Network is a network of nodes that can transfer value between each other nearly instantaneously, reducing traffic and fees on the main chain.[33]

second bitcoin halving: bitcoin's second halving took place at block 420,000, reducing the block reward from 25 bitcoins to 12.5 bitcoins. At 144 blocks mined per day, daily rewards declined from 3,600 bitcoins to 1,800 bitcoins.[34]

2017

the Bitcoin Scaling Agreement (New York Agreement): the NYA was a closed-door scaling announcement made at Consensus 2017 intending to move bitcoin's scaling debate forward with the SegWit2x proposal, which would increase block capacity.[35] The upgrade called for a user-activated soft fork for SegWit and miner activation at an 80% threshold, followed by a hard fork to increase block size to 2MB.

bitcoin cash hard fork: following disagreements on aggressively increasing block size to address scaling limitations, a competing implementation of the bitcoin protocol carried on with a hard fork called "bitcoin cash" on August 1, 2017. With the growth in network usage resulting from bitcoin's improvements, network traffic and transaction fees saw a subsequent uptick in 2017. Prior to this, some in the community believed that transaction costs were becoming too high for the hypothesized merchant payments use case, and there was strong disagreement on how to solve the problem. In 2017, this disagreement finally led to the bitcoin cash fork.[36]

2x hard fork suspension: 2x, a dangerous software update pushed by the NYA proponents that would trigger a block size increase at block 494,784 and increase transaction capacity, was called off due to strong developer and community opposition.[37]

Lightning Network protocol publicly released on Github: the protocol specifications for Lightning Network were released. There were 3 initial implementations - Eclair, c-lightning, and LN Daemon.[38]

CME Group launches futures trading: the CME Group launches its cash-settled bitcoin futures contract.[39]

2018

80% of total bitcoin supply mined: by January of 2018, over 16M bitcoins of total 21M bitcoins mined.

bitcoin is not a security: the U.S. SEC Chairman declares that bitcoin is not a security.

2019

launch of Bakkt: the Intercontinental Exchange (ICE) launched its crypto venture Bakkt, which released the first physically-settled bitcoin futures trading contract.

the UK Financial Conduct Authority (FCA) declares it won't regulate bitcoin: the UK's financial regulator, the FCA, issued a finalized policy on cryptocurrencies declaring that bitcoin doesn't fall under the regulatory scope of the FCA and described it as an 'exchange token.' [40]

2020

third bitcoin halving: bitcoin set to undergo its third halving in May at block 630,000, which reduces the block reward from the current 12.5 bitcoins to 6.25 bitcoins.[41]

32 "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" Joseph Poon and Thaddeus Dryja (https://lightning.network/lightning-network-paper.pdf)

33 "The Bitcoin Lightning Network" (https://lightning.network/lightning-network-summary.pdf)

34 The Halving: Trends and Implications of Bitcoin's Inflation Mechanism, Kraken Intelligence (https://blog.kraken.com/wp-content/uploads/2020/02/Bitcoin_Halving_F_v09.pdf)

35 New York Agreement on Bitcoin Magazine (https://bitcoinmagazine.com/tags/new-york-agreement)

36 A fork is a copy of the protocol and blockchain history for an existing network, like bitcoin, with changes implemented, resulting in a different network altogether. A fork retains all of the prior history of the original network, but diverges from the original network at the time of the fork, therefore owners of the original asset receive two distinct assets, but miners and nodes must decide which network to support going forward. This is different than a strict copy where the protocol is copied, but the blockchain history is not used.

37 "2x Called Off: Bitcoin Hard Fork Suspended for Lack of Consensus" Coindesk (https://www.coindesk.com/2x-called-off-bitcoin-hard-fork-suspended-lack-consensus)

38 "Lightning Network" Keerthi Nelaturu (https://medium.com/coinmonks/lightning-network-7fcdf3e7b735)

39 "CME Group Self-Certifies Bitcoin Futures to Launch Dec. 18" CME Group (https://www.cmegroup.com/media-room/press-releases/2017/12/01/cme_group_self-certifiesbitcoinfuturestolaunchdec18.html)

40 "UK Financial Regulator FCA Won't Regulate Bitcoin and Ether" Cointelegraph (https://cointelegraph.com/news/uk-financial-regulator-fca-wont-regulate-bitcoin-and-ether)

41 The Halving: Trends and Implications of Bitcoin's Inflation Mechanism, Kraken Intelligence (https://blog.kraken.com/wp-content/uploads/2020/02/Bitcoin_Halving_F_v09.pdf)

IV.

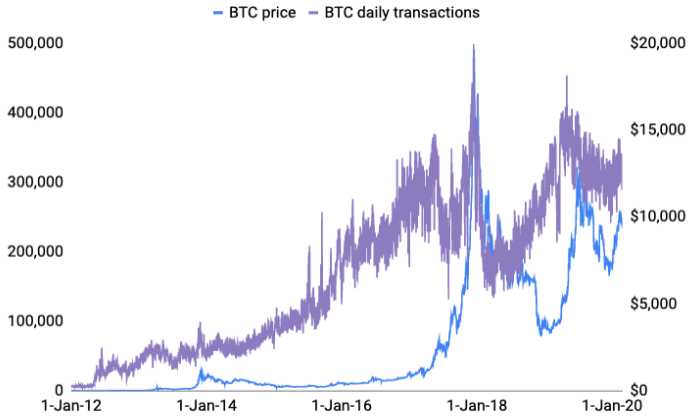
SCALABILITY

Scalability is often-cited as one of the greatest impediments to bitcoin's longer-term adoption as a day-to-day payment system, though it is worth noting that layer 1 scalability as part of bitcoin's intended purpose is still a contended issue. However, the scalability of the bitcoin network - as well as blockchain technology more generally - became a cornerstone debate after an explosion of global interest in 2017 led to increased demand for bitcoin block space and higher average transaction fees. Looking to figure 3, we can clearly observe bitcoin transaction volume reaching technical limitations as daily on-chain transactions grew from 30k in early-2013 to 409k at its peak in 2017.[42] Furthermore, median transaction fees grew to $32 per transaction in December 23, 2017 and the mempool backlog[43] grew to 137MB by January 10, 2018.[44]

Scalability also represents bitcoin's greatest technical challenge to this day, diverging into two paths for longer-term network scaling:

Figure 3

Bitcoin price and daily transactions



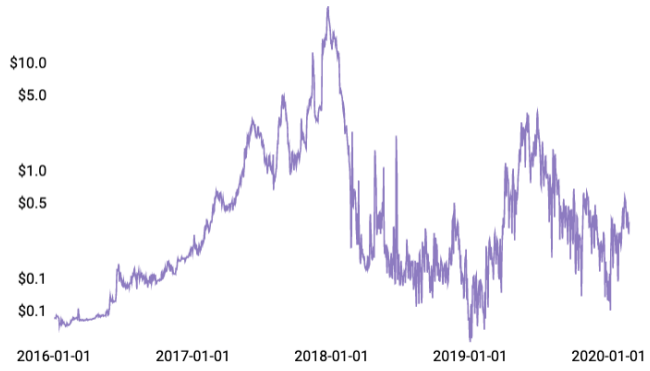
Source: blockchain.com

42 Bitinfocharts.com On-Chain Transactions (https://bitinfocharts.com/comparison/bitcoin-transactions.html)

43 A pool of unconfirmed transactions, waiting to be confirmed by miners

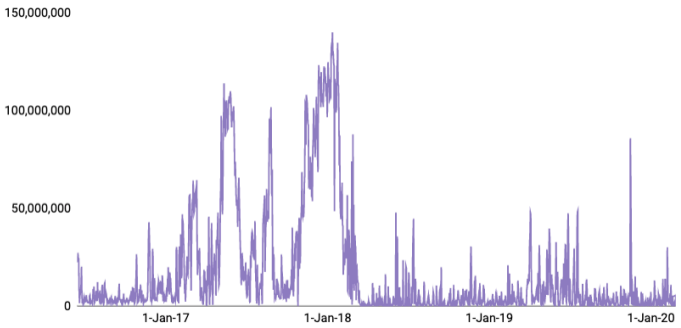
44 Bitcoin Mempool Size (https://www.blockchain.com/charts/mempool-size?timespan=all)

Figure 4
Bitcoin median transaction fees



Source: coinmetrics.io

Figure 5
Mempool size



Source: blockchain.com. Unit: bytes

On-chain (layer 1) scaling – Changes to the protocol that allow miners to include more transactions over a given time period. This has happened twice, once in 2013 and once in 2017. These past on-chain capacity increases did not require a hard fork. Future capacity increases may come in the form of efficiency upgrades or hard forks increasing the block size limit.

Off-chain (layer 2) scaling – Solutions that allow users to transact more quickly and seamlessly on distributed ledgers that are anchored by the bitcoin blockchain.

Currently, bitcoin's open source contributors are pursuing a combination of on-chain and off-chain scaling solutions. The Segregated Witness (SegWit) soft fork was activated in 2017, which increases on-chain capacity two-fold[45] and laid the foundation for off-chain solutions like the Lightning Network. To date, SegWit transactions represent less than 50% of transactions process on the bitcoin network, which implies significant room for increased throughput on the existing protocol.[46]

45 SegWit transactions strip the "witness data" from a transaction to save space. Jimmy Song (https://medium.com/@jimmysong/understanding-segwit-block-size-fd901b87c9d4)

46 Bitcoin SegWit Adoption (http://charts.woobull.com/bitcoin-segwit-adoption/)

Proponents of a more aggressive on-chain scaling roadmap, led by the BitcoinABC implementation, decided to splinter off and forked the bitcoin protocol with bitcoin cash. Much of the bitcoin cash network believes their implementation is better aligned with what they believe was the original intent of bitcoin: a peer-to-peer payment system with low-cost, on-chain transaction confirmation. As a result, the bitcoin cash network pursued an immediate increase to the block size allowance to 8MBs, which later grew to 32MBs in May 2018.[47] Though the proponents of this switch had hoped to see better on-chain scaling without the use of off-chain scaling solutions, activity on the network has yet to see enough throughput to make use of this increase, which raised further questions about the advantages of bitcoin cash.

Blockchain networks inherently have scalability limitations. Different solutions are highly experimental and usually accompany a tradeoff of decentralization. On-chain scaling solutions introduce risk of centralization due to the increased cost and difficulty of managing a full node. For example, if both the bitcoin and bitcoin cash networks were fully utilized for a year, a bitcoin node would record 210GBs[48] of additional transaction data, whereas the bitcoin cash node would record 1.7TBs[49] of additional transaction data. Based on Amazon Web Service (AWS) pricing, 210GBs of additional storage costs over $57 per year and 1.7TBs of additional storage costs $469 per year.[50] This difference grows over time, making it increasingly costly to operate a full node. In addition to this, currently, the difference in Initial Block Download (IBD)[51] time of cable and DSL versus fiber connection as well as differences in network latency further crowds out individuals and business node operators. If the bitcoin network cannot attract a healthy number of dispersed nodes to maintain the network, there is a risk of slipping into centralized decision making and inflationary changes to the monetary policy. As high speed fiber-optic internet spreads around the world, consensus may form around significantly increasing bitcoin's block size limit.

Off-chain networks like the Lightning Network can also see centralized "hubs" as a few, large and interconnected nodes facilitate the majority of transactions on this off-chain network. In particular, the largest 20 Lightning nodes have 8,901 channels, representing 25% of the Lightning Network, and maintain around 478 bitcoin, or 56% of all bitcoin held off-chain.[52] Centralization on Lightning is not a risk as it is not a global broadcast network like Bitcoin, so Lightning nodes can set their own local policies with regards to peering, channel management, and routing. Service degradation from centralization self-repairs as Lightning node operators are incentivized to disconnect from the troublesome centralized peer.

47 "Bitcoin Cash Milestones: Delivered Code, Upgrades and Platform Development" Bitcoin.com (https://news.bitcoin.com/bitcoin-cash-milestones-delivered-code-upgrades-and-platform-development/)

48 Bitcoin: 4MB/block*144 blocks/day*365 days/year = 210,240MB annually. (4MB due to SegWit)

49 Bitcoin Cash: 32MB/block*144 blocks/day*365 days/year = 1,681,920MB annually.

50 AWS Storage Pricing, based on US East storage pricing (https://aws.amazon.com/s3/pricing/)

51 Initial Block Download is the process of downloading all the existing blocks of a blockchain when new nodes join a network

52 Lightning Network Statistics (1ml.com)

Currently, the bitcoin blockchain itself handles around 2-7 transactions per second (TPS), close to the 7-8 TPS of funds transfer system Fedwire,[53] whereas a centralized payment network like Visa can reportedly process up to 65,000 TPS.[54] Looking to the broader roadmap for scalability, a number of proposals exist that look to increase bitcoin's competitiveness as a value transfer network. The Lightning Network (LN) has generated the most interest in the open source bitcoin community and can theoretically exceed Visa's throughput, though it is currently limited by the number of participating nodes and node capacity.

Figure 6 summarizes a number of additional scaling improvements, including: Schnorr Signatures,[55] MAST, MimbleWimble, Bulletproofs, and Drivechain.[56]

Figure 6

Scaling solutions

NAME	LAUNCH DATE	THROUGHPUT	IMPROVEMENT FEATURES
Current State	Jan 2009	2-7 tps	Current implementation of bitcoin
SegWit	Aug 2017	14 tps	Enables Lightning and other layer 2 scaling solutions
Lightning Network	Jan 2018	Unlimited	Allows for direct peer-to-peer transactions separate from the main bitcoin network
Liquid	Oct 2018	Unlimited	Allows for quicker transactions via a federated sidechain anchored to the bitcoin mainchain
Schnorr Signatures	Unknown BIP released Feb 2018	18 tps	Provides enhanced multisignature and privacy features
MAST (*Merkleized Abstract Syntax Trees)*	Unknown BIP released Nov 2016	Unclear	Allows for smaller complex transactions by creating a Merkle tree for the transaction itself. Useful for large, complex multi-signature transactions and transactions with many conditional execution parameters
MimbleWimble	Unknown Whitepaper released Oct 2016	Unclear	Allows for a dramatically reduced blockchain size (>99%) (100GBs to a few MBs), which improves verification times and storage requirements
Bulletproofs	Unknown Whitepaper released Oct 2017	Unclear	Provides an improved method for determining validity (proofs) of a transaction, which improves verification times and storage requirements, and lowers transaction sizes (potentially by >80%)
Drivechain	Unknown BIPs released Dec 2017	>20,000 tps	Provides for the flexible creation of an infinite number of sidechains each with their own separate features. A leading sidechain, RSK, promises to deliver 20,000 tps.

Source: Reddit, blockchain.com, SDWouters, blockstream.com, Github, MimbleWimble, Stanford
Note: higher/unlimited throughput does not guarantee scalability and are seen to bring complications in the security of a network.

53 Based on Fedwire's average daily volume in 2019: 667,929/(86400 seconds/day) = 7.7TPS (https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm)

54 Visa Factsheet (https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf)

55 Schnorr Signatures are a different type of transaction signature that aggregates and compresses transaction inputs, thus submitting only one signature to the blockchain per transaction vs. one signature per input to a transaction. This both reduces the amount of data per transaction and increases the privacy of transactions.

56 "Roadmap to Bitcoin Developments" Ian Edwards (https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122)

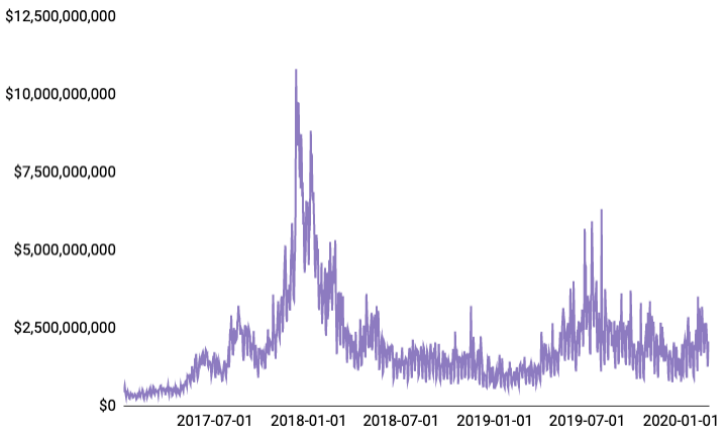
V.

ADOPTION

Bitcoin's on-chain transaction volumes, or the value of all transactions minus change transactions, shows a trend in bitcoin adoption and usage that corresponds with market fluctuations. Daily on-chain volume hit an all-time high in December 2017 at $10.5B transactions, and trended downwards until March 2019. Since then, the network has recorded growth of 205.4% in daily on-chain volume from March 2019 to end-February 2020, following several price rallies.[57]

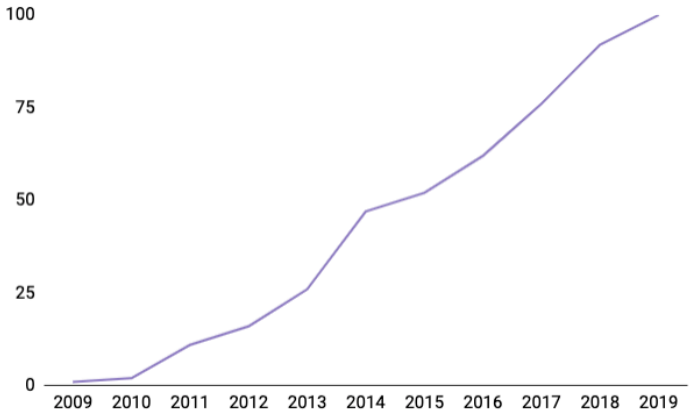
Development is an important barometer of adoption of the bitcoin network, as ongoing improvements lead to better security and usability. Bitcoin core has logged over 20K code changes by more than 600 distinct individuals and decentralization in the bitcoin developer

Figure 7
Daily on-chain volume



Source: coinmetrics.io

Figure 8
Bitcoin core contributors (excl. merge commits)



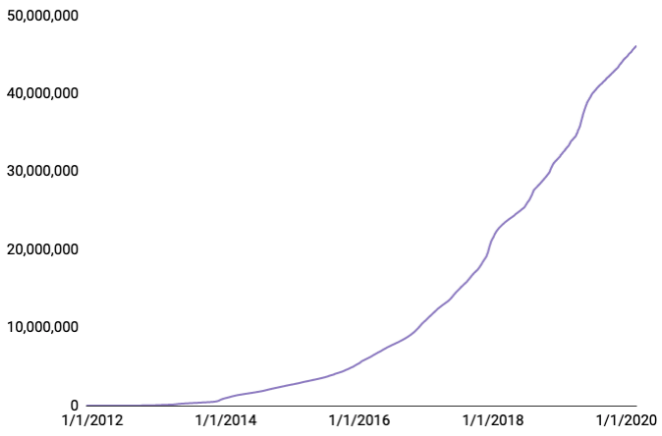
Source: Github

57 Bitcoin Daily On-Chain Volume (https://coinmetrics.io/charts/#assets=btc_log=false_roll=7_left=TxTfrValAdjUSD_zoom=1546300800000,1566777600000_sameAxisComparison=true)

community has been growing. Between 2009 and 2013, there were only 24 contributors, and the top 3 contributors represented 60% of the commits. Currently, of the 679 contributors, 47 have more than 25 commits.[58]

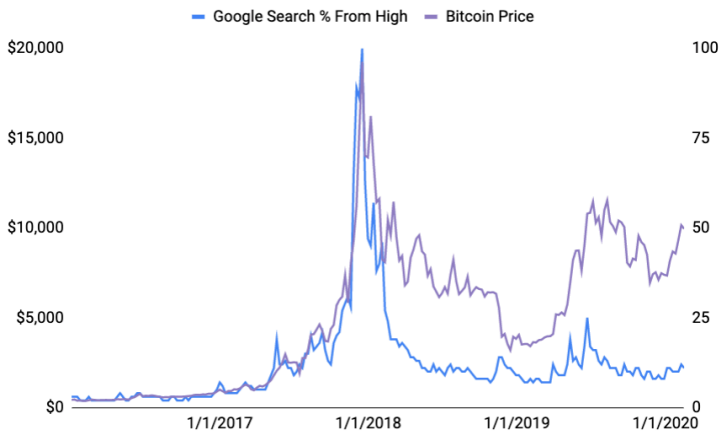
Redundancy and validation is another important indicator of adoption and network health. The number of full nodes has grown substantially and continues to make gains, with around 9,268 public nodes running on the bitcoin network.[59] As this only includes full nodes that are actively broadcasting themselves as such, the actual number of full nodes is estimated to be a magnitude larger than this, at over 57K.[60,61,62] The growth of full nodes on the network promotes the security and decentralization of the network. This is because the bitcoin network is vulnerable

Figure 9
Bitcoin wallet growth



Source: blockchain.com

Figure 10
Bitcoin Google search interest and price



Source: Google Trends

58 A commit is an update to a codebase contributed by one developer, and is the basic building block of software or protocol versions. Github (https://github.com/bitcoin/bitcoin/graphs/contributors)

59 Bitcoin Core Nodes Summary on Coin Dance (https://coin.dance/nodes/core)

60 Bitcoin Node Software (https://luke.dashjr.org/programs/bitcoin/files/charts/software.html)

61 "Bitcoin Network Surpasses 100,000 Nodes, New Data Shows" Bitcoinist (https://bitcoinist.com/bitcoin-network-surpasses-100000-nodes-new-data-shows/)

62 Full nodes are computers that have downloaded the entire bitcoin blockchain and provide verification of new transactions by insuring that 'double-spends' do not occur

to Sybil[63] and Eclipse[64] attacks if control of the network nodes are centralized in a few hands.[65] However, as each full node is required to validate the chain for themselves, an increase in this sovereign decision-making results in an increase in the security of the bitcoin network. Another popular metric for studying trends in adoption is the growth in bitcoin wallets, shown in figure 9. Blockchain.com reported to have surpassed 40M in wallet count by 2Q19, a 414% growth since 7M in 2Q16.[66,67] Though not a measure for the total number of unique individuals on the bitcoin network, this trajectory may represent a proxy for the number and pace of new entrants into the crypto space. In addition to wallet creation, daily active addresses recorded on the blockchain is a good substitute for daily active users. By mid-2019, daily active addresses reached 1 million, levels last seen in the second half of 2017, and it currently sits at around 810K.[68]

Adoption is also often analyzed in the context of mining hash power, which has grown significantly in recent years. In 2013, the hash rate for the entire network was 22.8TH/s (22,800,000,000,000 hashes per second) before growing to 15 EH/s (15,050,000,000,000,000,000 hashes per second) by end-2017 and currently recording around 119.8EH/s.[69] In dollar terms, the cost to replicate the hash power of the network is roughly $3B, based on the hash power (73TH/s) and cost ($2,019) of the Antminer S17+, one of the latest ASIC mining rigs.[70]

Interest from the general public, as measured through Google Trends, demonstrates a pattern that closely tracks the price of bitcoin. Looking to figure 10 Google search for “bitcoin” has declined 89% since December of 2017, falling to levels seen in May of 2017.[71] This closely follows the general ‘Hype Cycle’[72] of most new technologies, a cycle that bitcoin has experienced multiple times. We anticipate that general public interest in bitcoin may continue to follow a speculative trend.

63 A Sybil attack is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. An example of this in bitcoin would be if someone created thousands of fake nodes and then began propagating an altered version of the bitcoin network to create double-spends.

64 An eclipse attack involves the adversary targeting a specific node (as opposed to the network as a whole) so as to cut off all of their inbound/outbound communications with other peers

65 "Bitcoin's Attack Vectors: Sybil & Eclipse Attacks" Chainrift Research (https://medium.com/chainrift-research/bitcoins-attack-vectors-sybil-eclipse-attacks-d1b6679963e5)

66 Blockchain Wallet Users (https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/)

67 Blockchain Wallet Users (https://www.blockchain.com/en/charts/my-wallet-n-users)

68 Bitcoin Daily Active Addresses (https://coinmetrics.io/charts/#assets=btc_left=AdrActCnt_zoom=1549411200000,1580947200000)

69 Bitcoin Hash Rate, Blockchain.com (https://www.blockchain.com/charts/hash-rate)

70 An ASIC, or Application Specific Integrated Circuit, mining rig is a computer specially designed for mining bitcoin as efficiently and quickly as possible

71 Google Trends for 'bitcoin' (https://trends.google.com/trends/explore?date=all&q=bitcoin)

72 Gartner Hype Cycle (https://www.gartner.com/en/research/methodologies/gartner-hype-cycle)

VI.

CONCLUSION

Bitcoin is a revolutionary technology with promising qualities as a challenger monetary system and means to transfer and store value. Despite the ups and downs over the past decade, it is well on its way to becoming a global phenomenon. Bitcoin is currently in the midst of two major technological challenges that will set the stage for mass adoption - scalability and usability. It has historically been rather difficult for the average person to use and interact with bitcoin, partially because of its technical attributes and partially because it requires people to understand the global monetary system. Both are quite challenging, but new and improved consumer-facing applications and resources are beginning to provide more access and education into these areas. We anticipate these two key trends to underpin the next major adoption cycle and will likely be focal points of this technological and financial revolution, as both have been critical to bitcoin's mass adoption thus far.

We anticipate bitcoin to lead the greatest wealth transfer in history as it promises unprecedented economic freedom. This revolution still has significant development to be realized for us to fully see mass-adoption of the network, as we are in the early days of bitcoin and have only experienced a tiny fraction of the transformational potential of the technology. Learning about bitcoin is hard, but once you do, it can change paradigms. We hope this asset note provided a strong foundation to get you started.

Feedback

We appreciate your feedback! Please visit https://surveys.kraken.com/jfe/form/SV_eh6TQBohPZLKbvn to participate in a brief survey. For comments, suggestions, or questions related to this article or future topics you'd like to learn more about, you may also direct your communication to intel@kraken.com or to your account manager.

Kraken provides access to **33 cryptocurrencies** spanning over **150 markets** with **advanced trading features, industry-leading security, and on-demand client service.** With the acquisition of Crypto Facilities, Kraken now offers seamless access to **regulated derivatives** on **5 cryptocurrencies** with up to **50x leverage**. Sign up for a free account in minutes at www.kraken.com/sign-up. We look forward to welcoming you.

For **multi-exchange charting, trading, portfolio tracking, and high resolution historical data**, please visit https://cryptowat.ch. Create a free Cryptowatch account today at https://cryptowat.ch/account/create and enjoy a 14 day trial of premium service.

For **OTC-related execution services or inquiries**, please direct your communication to otc@kraken.com or to your account manager.

Disclosure appendix

The information in this report is provided by, and is the sole opinion of, Kraken's research desk. The information is provided as general market commentary and should not be the basis for making investment decisions or be construed as investment advice with respect to any digital asset or the issuers thereof. Trading digital assets involves significant risk. Any person considering trading digital assets should seek independent advice on the suitability of any particular digital asset. Kraken does not guarantee the accuracy or completeness of the information provided in this report, does not control, endorse or adopt any third party content, and accepts no liability of any kind arising from the use of any information contained in the report, including without limitation, any loss of profit. Kraken expressly disclaims all warranties of accuracy, completeness, merchantability or fitness for a particular purpose with respect to the information in this report. Kraken shall not be responsible for any risks associated with accessing third party websites, including the use of hyperlinks. All market prices, data and other information are based upon selected public market data, reflect prevailing conditions, and research's views as of this date, all of which are subject to change without notice. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research. Kraken and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction where such distribution or use would be contrary to applicable law or that would subject Kraken and/or its affiliates to any registration or licensing requirement. The digital assets described herein may or may not be eligible for sale in all jurisdictions.