Purpose

Create a global payment and monetary system that does not rely on central third parties, paired with an internet-native asset that cannot be confiscated or inflated away.

The System

- Settles transactions
- No single points of failure
- Open to anyone
- Secured by cryptographic proofs

The Asset

- Transferrable
- Borderless
- Divisible
- Verifiable
- Disinflationary

Network Participants

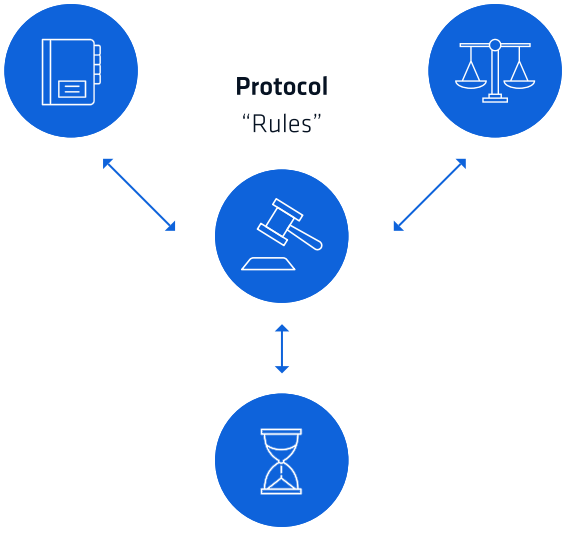
Miners
"Block Producers"

Full Nodes
"Verifiers"

Components

Blockchain
"Transaction Record"

UTXO Set
"Account Balances"



Protocol
"Rules"

Mempool
"Outstanding Transactions"

General Info

Creator	Satoshi Nakamoto
Launch	Jan 2009
Consensus	Proof-of Work
Asset	BTC
Max Supply	21 million
Smallest Unit	.00000001
Pre-mine	0
Core Contributors	774

Quick Stats

Market Capitalisation	1.07t
Current Supply	18.66m
1 Year Active Supply	8.19m
Annual Inflation	1.91%
Transfer Value (USD/day)	18.11b
Miner Revenue (USD/day)	59.59m
Unique Addresses	36.96m
Active Addresses	1.11m
Chain Settlement Protection (GW)	16.79

Quick Stats

2011	1,474.4%
2012	155.8%
2013	+5,372.4%
2014	-57.3%
2015	+36.5%
2016	+122.9%
2017	+1,295.9%
2018	-72.6%
2019	+88.21%
2020	+304.7%

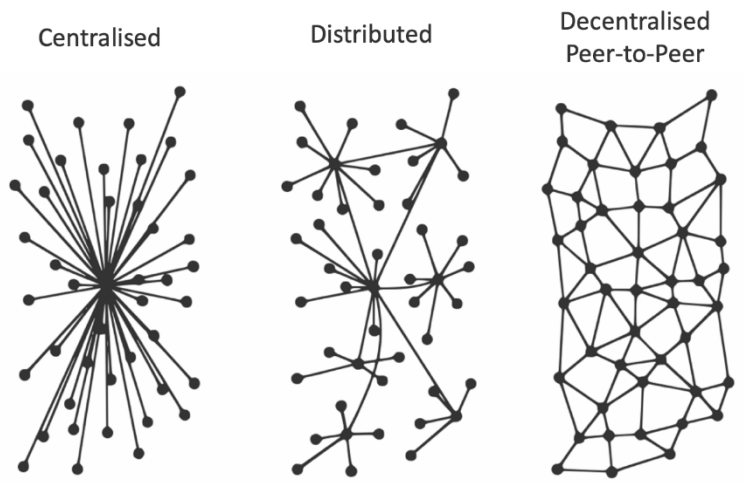
Data as of 21st March 2021 All statistics by Coinmetrics except:

Core Contributors: https://github.com/bitcoin/bitcoin/graphs/contributors | Chain Settlement Protection: https://cbeci.org/

Purpose

Bitcoin has its origin in the desire to create a global payment and monetary system that does not rely on central third parties, itself hosting an internet-native asset that cannot be confiscated or inflated away.

This is reflected in the abstract of the Bitcoin Whitepaper where the pseudonymous author states that "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."



From the extensive archive of Satoshi Nakamoto's correspondence with early Bitcoin users and developers we can discern that there was a whole laundry list of grievances that led down the path of creating a fully peer-to-peer global monetary system. Among these we find:

- The power imbalance between governments and its citizens created by a centralised monetary and banking systems where the end users have no sovereignty or control over their finances;
- The systemic risk introduced by single points of failure in critical societal infrastructure;
- The risk of theft and fraud inherent to untransparent monetary systems, especially to citizens of authoritarian or kleptocratic regimes;
- The costs of inflation on society, disproportionately harming citizens with low levels of asset ownership;
- The desire for an internet native money capable of small casual transactions between peers.

Bitcoin delivers on these goals by incorporating a set of properties meant to ensure that they are perpetually upheld:

- Sovereign ownership of bitcoin units is ensured through the use of public key cryptography – the modern standard of cryptographic tools underpinning important societal functions such as military communication, banking and system critical infrastructure
- Third parties are eliminated through the use of a decentralised peer-to-peer networking structure, enabled by the ability of anyone, anywhere to participate in the Bitcoin network at a permission level that is equal to everyone else
- Inflation risks are eliminated by the implementation of a fixed and predetermined monetary policy, and dilution costs on bitcoin holders are exponentially decreased by cutting new supply in half approximately every four years

While most of the original goals are indeed met by Bitcoin in its current form, the desire for microtransactions on the base-layer has since been found to be incompatible with the desire for decentralisation.

Effectively, casual retail transactions settled directly on the blockchain is not possible while at the same time retaining the ability of large numbers of users running full Bitcoin nodes on consumer-grade hardware.

To still accommodate microtransactions using bitcoins as the monetary unit, additional protocol layers have been introduced. These layers have effectively unlimited transaction volume capacity and use the Bitcoin blockchain as an industrial settlement chain for more economically dense transactions.

People

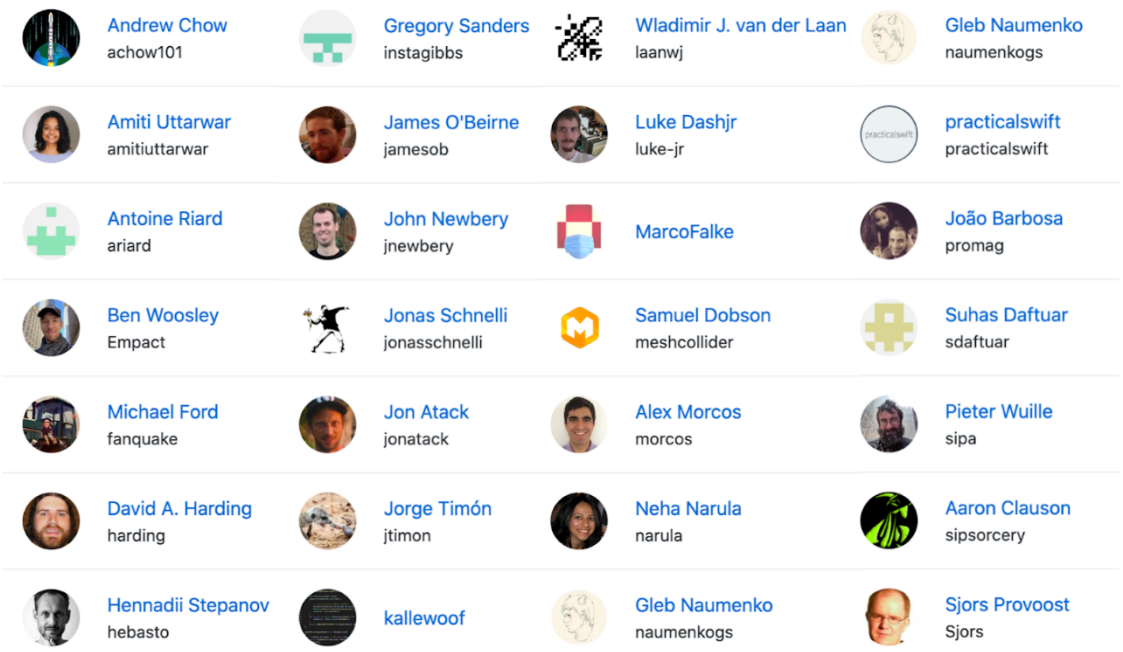
The idea behind Bitcoin was initially introduced on an obscure mailing list for cryptographers and computer scientists. At the time, it received very limited attention. Several decades of failed attempts at peer-to-peer cash systems had convinced most people that such a system was impossible. Further fuelling these doubts, the author, Satoshi Nakamoto, was unknown and had no credentials or goodwill in the community.

Among the people who immediately took a liking for the idea, however, we find venerable cryptographers and computer scientists such as Hal Finney, Nick Szabo and Wei Dai. Hal Finney, since deceased, was in fact the first recipient of a Bitcoin transaction, receiving 10 bitcoins from Nakamoto on 12 January 2009, only three days after the software was first released.

To this day, not much is known about Satoshi Nakamoto. It is not even known if the pseudonym represents a single person or a group of people. The whitepaper uses the pronoun 'we' whereas in correspondence, Nakamoto almost always uses 'I'. In public profiles, Nakamoto claimed to be a Japanese male born on 5 April 1975 – the same date that Franklin D. Roosevelt signed the executive order forbidding private ownership of gold in 1933. Nakamoto often used British spelling and the time windows of activity suggests a location in Europe or the US.

The developer pool working on Bitcoin has seen significant turnover since the initial launch. Early on, most actual coding work was done by Nakamoto, with the remaining community members mainly helping with testing and finding bugs. Eventually, other developers began contributing to the codebase and duties became increasingly distributed. When Nakamoto disappeared in 2011, Gavin Andreesen briefly took over as lead programmer before the job passed to Wladimir van der Laan (aka Orionwl) who holds the position to this day.

Currently, several hundred people actively contribute to the development of the Bitcoin software, and the development model is similar to that of other free open source software systems such as Linux. Many of the developers who came to the project in the first few years remain steady contributors while some have moved on. Every year however there is a steady stream of new developers coming in, and several companies in the Bitcoin sphere provide full-time funding grants for developers.



Development

All we know of the earliest development of Bitcoin is that Nakamoto claimed to have been working on the project for some time leading up to its release. Unlike many standards and open source projects, there has never existed a formal specification for Bitcoin, the software itself acts as the reference guide. So when the first version came out, the major rules were effectively set in stone forever.

It is also important to remember that Bitcoin did not appear out of nowhere, it leans heavily on more than half a century of breakthroughs in computer science and cryptography. Among the most important innovations are hashing algorithms and elliptic curve cryptography.

> The reason why peer-to-peer money was thought to be infeasible was the perceived impossibility of uncoordinated participants (or 'nodes') in a computer network to agree on what time it is. If nobody can agree what time it is, no one can know which transactions came before or after others. If that is the case, there is the potential for bad actors to spend the same money twice.
>
> Bitcoin elegantly solves this by using proof-of-work – a revolutionary computer science technique based on the properties of hashing algorithms – as a decentralised global clock. This was the fundamental breakthrough that enabled an uncoordinated set of geographically distributed nodes to finally be able to agree on a canonical transaction ordering, thereby enabling distributed ledgers.

Interestingly, the original codebase came with an online poker client. While this never took off in popularity it offers an interesting peek into the ideas Nakamoto might have had for Bitcoin's usage.

As the system got increasingly popular and developed exchange prices with large international currencies such as the Dollar, bitcoins saw their first budding use as a medium of exchange. Initially used as the sole currency of the infamous Silk Road online marketplace, bitcoin began to gain notoriety amongst the tech-savvy community.

Bitcoin quickly got more widely noticed for its ability to protect privacy and resist censorship. These unique attributes pushed Bitcoin right into the international limelight during the Wikileaks debacle in mid 2011. Having had all their funding channels blocked by the US government, Wikileaks successfully avoided an anemic death from lack of funding by using bitcoin as its primary inbound funding channel. The system clearly worked, but the perceived incoming scrutiny also caused Nakamoto to disappear from the public, never to be heard from again.

Development then passed to its current distributed voluntaryist form and work continued more or less unabated. Between 2009 and 2017, most changes to the codebase were incremental performance improvements, bug fixes as well as the addition of a non-command line user interface. Among the more spectacular bugs found along the way was the 2010 inflation bug whereby a user was able to award himself more than 80bn btc due to an integer overflow error. This remains Bitcoin's only 'intentional' hardfork.

In 2017 however, a significant change to the Bitcoin protocol called Segregated Witness was introduced, enabling a whole new range of different transaction types whilst increasing transaction capacity. Not long thereafter, and enabled by its activation, the Lightning Network started forming. Utilizing new transaction formats introduced by SegWit, Lightning sits as a layer on top of Bitcoin, acting much in the same way as a bar tab, and only using the Bitcoin base layer (the actual blockchain) for settlement. Lightning enables virtually unlimited transaction volumes and the possibility of sending instant payments of arbitrarily small sizes in a highly private fashion.

Network Participants

Outside of the people directly involved in development there are also tens of thousands of full node operators. A full node is simply a computer running the Bitcoin protocol. It is a peer in the peer-to-peer network that broadcasts, relays and validates transactions. Nodes serve as recipients and transmitters of transactional messages, and all full nodes independently validate the Bitcoin blockchain from the first block in order to verify that the rules of the Bitcoin protocol are never violated.

From the blockchain, all nodes also independently calculate the current state of Bitcoin ownership, called the UTXO (Unspent TransaXion Output) Database. This database is then queried when nodes are assessing whether transactions they receive as messages have sufficient funds to cover their transactional amounts. If an incoming transaction is found to be invalid in any way, the node will refuse to propagate it to its peers, and if the sender is a repeat-offender, the node may choose to refuse any further messages.

Running a full node can be done on cheap consumer-grade hardware and most node operators are Bitcoin users who want the added trust benefits of self-verifying their bitcoin ownership. While it is impossible to say with certainty exactly how many Bitcoin nodes there are, best estimates tend to range between 50,000 to 100,000 spread throughout the world. Fully destroying Bitcoin would require wiping the software off of every single one of those nodes.

Some full nodes also choose to act as block producers, called miners. Miners do not have any special permissions or privileges, rather, they are service providers producing blocks so that new transactions can be added to the blockchain ledger and the payment system can progress through time. This service provision entails the provable expenditure of cost, for which they are rewarded by the network via transaction fees and newly minted bitcoins.

At the time of writing, the Bitcoin mining network draws approximately 11 GW of electricity on an ongoing basis, for which the miners receive approximately 100 btc of fees, and 900 new bitcoins – worth approximately US$20m – daily. The cost of adding blocks to the ledger incentivises miners to act honestly, adds incremental economic settlement finality to transactions with each added block, and proves (on average) that the required amount of time has passed since the last block.

In order to participate in block creation, miners use specialised hardware whose single purpose is to prove expended cost, or work. The proof of work consists of finding the solution to a mathematical problem which can only be found through repeated guessing. The correct blockchain is by definition the one with the most accumulated cost, or work. This is Bitcoin's main consensus rule and ensures that the transaction record is always the result of a cooperative effort by at least 50% of miners.

The mining ecosystem is a multi-billion dollar industry with major hardware production footprints in Taiwan, South Korea, China and Malaysia. Major mining operations tend to be located in global regions of cheap electricity, with concentrations in the US, Canada, Scandinavia, the Caucasus, Iran, Kazakhstan, Russia and China.

Market Participants

Over the course of the last twelve years, a global network of interconnected services has emerged to serve participants in Bitcoin markets. Bitcoin users can now access dozens of large international exchanges offering markets for bitcoin against almost every existing fiat currency. Adding to that, more sophisticated traders can access a wide range of financial products referencing bitcoin, including futures, options, swaps, and even interest-bearing deposit accounts.

Outside of the retail sphere, larger-scale users such as high net worth individuals, hedge funds, asset managers and institutional investors can now also choose between a wide range of Bitcoin-related services including professional custody, prime brokerage, over-the-counter trading, and fully regulated derivatives.

Its now extant network of market participants has recently evolved bitcoin from its roots as a pure cash-like internet money into a fully fledged new asset class supporting a full complement of referenced financial products.

Questions?

Get in touch at research@coinshares.com

IMPORTANT DISCLOSURE

The information contained in this document is for general information only. Nothing in this document should be interpreted as constituting an offer of (or any solicitation in connection with) any investment products or services by any member of the CoinShares Group where it may be illegal to do so. Access to any investment products or services of the CoinShares Group is in all cases subject to the applicable laws and regulations relating thereto.

This document is directed at professional and institutional investors. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance.

Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of CoinShares, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, CoinShares does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Third party data providers make no warranties or representation of any kind in relation to the use of any of their data in this document. CoinShares does not accept any liability whatsoever for any direct, indirect or consequential loss arising from any use of this document or its contents.

Any forward-looking statements speak only as of the date they are made, and CoinShares assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time. Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

CoinShares Capital Markets (UK) Limited is an appointed representative of Strata Global Ltd. which is authorised and regulated by the Financial Conduct Authority (FRN 563834). The address of CoinShares Capital Markets (UK) Limited is Octagon Point, 5 Cheapside, St. Paul's, London, EC2V 6AA.