Bitcoin **201**

BITCOIN'S HISTORY, DESIGN, AND DEVELOPMENT

NYDIG

TABLE OF CONTENTS

Introduction

This document is intended for investors who are new to Bitcoin (uppercase “B” Bitcoin is the technology or network, and lowercase “b” bitcoin is the asset native to the network). Interest in Bitcoin continues to grow, and with that, a desire to understand more. The concept of Bitcoin, its technology, and its terminology can be overwhelming at first. This document is intended to describe Bitcoin’s history, design, and development in terms that can be understood by all.

This document is organized into topics with important questions and answers on each topic. Some questions have more in-depth answers, designated as “bitcoin deep insight sections,” for readers who wish to know more.

01

Overview

What is Bitcoin?

Bitcoin is an open source monetary system - that is, a system for storing and transmitting an asset of value whose underlying code is fully open to the public. This system allows bitcoin (lowercase “b”), the native digital asset of the Bitcoin network, to be sent securely between users over the internet without the need of an intermediary. Transactions are verified and recorded in a public ledger called a blockchain through a process called mining.

Trustless

Bitcoin enables financial transactions on a peer-to-peer basis without the need of a financial intermediary, like a bank.

Permissionless

Bitcoin software is free to download and can be installed by anyone anywhere in the world.

Censorship Resistant

Bitcoin is a decentralized network not controlled by a single person, organization, or government, rendering it nearly impossible to suppress access or deny transactions.

Digital Scarcity

The supply of bitcoins is finite and capped at 21 million. The issuance of new bitcoins declines to zero over time.

02

Origin

Who Created Bitcoin?

Satoshi Nakamoto, a pseudonym for an unknown individual or group, created Bitcoin. A whitepaper describing Bitcoin was first published to The Cryptography Mailing List on October 31, 2008, and Bitcoin officially launched when the first block was created on January 3, 2009. In this first block, also called the genesis block, Nakamoto encoded a message "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." It is important to note that Bitcoin was not only a technical innovation, but an economic statement.

Nakamoto's identity has been the source of much media speculation over the years, but his, her, or their identity has never been confirmed. Nakamoto stepped away from active development of Bitcoin in 2010, and today, Bitcoin is an open-source project. Its code is available for anyone to download, inspect, suggest changes, and run.

DEEP INSIGHT

Bitcoin's Creator

The last public message from Satoshi Nakamoto was on the Bitcointalk forum on December 12, 2010. Nakamoto's last confirmed private communication was on April 26, 2011 to Gavin Andresen, who was entrusted as Bitcoin Core Maintainer of the project by Nakamoto. Over the years, there have many attempts to uncover the identity of Nakamoto, who revealed little personal information in his communications. Several people have been linked to his identity, including Nick Szabo, creator of bit gold, Dorian Nakamoto, a Japanese American man living in California, and Hal Finney, the first person to use the Bitcoin network.

03

Evolution

How is Bitcoin Developed?

Bitcoin has been under active development since its inception. Hundreds of developers from around the world have contributed and continue to contribute to the building of Bitcoin and its ecosystem. Bitcoin is an open-source software project, which grants developers the right to use, modify, and distribute its codebase. Bitcoin is developed in a collaborative manner with discussions on GitHub, mailing lists, and chat channels.

DEEP INSIGHT

Bitcoin's On-Going Development

Over 300 developers from around the world actively contribute to the building of Bitcoin and the surrounding ecosystem of software applications monthly. Dutch developer Wladimir J. van der Laan currently serves as Bitcoin Core Maintainer, its lead developer, a position he has held since April 2014. Van der Laan was entrusted with this responsibility by American computer scientist Gavin Andresen, who served as Bitcoin Core Maintainer from 2010 to 2014 after he was handed the reins from Satoshi Nakamoto.

Bitcoin has a process by which new features are implemented, called the Bitcoin Improvement Proposal (BIP). BIPs start as new ideas championed by a developer whose job it is write the BIP design document in a specific format, shepherd discussions about the idea through various discussion forums, and build developer consensus. Draft BIPs are submitted to the bitcoin-dev mailing list with the BIP's author collecting feedback and changes. BIPs that are accepted move into the reference implementation or coding phase. Once the reference implementation is complete and accepted by the community, the process will be complete. BIPs and other updates are aggregated and released in new software versions. The current version of Bitcoin Core is v0.21.

04

Technology

How Does One Use Bitcoin?

Most individuals interact with Bitcoin through a piece of software called a wallet, which allows users to receive, hold, and send bitcoin. Wallets safeguard private keys, passwords that are secret to the wallet's owner, that allow bitcoin to be spent. A wallet can run on a personal computer, cell phone, secure hardware device, or it can be hosted by a third party on the web.

Bitcoin Core is the official software implementation, or reference client, of Bitcoin. It contains both a wallet and a full copy of Bitcoin's blockchain, a historical log of all transactions that have occurred on the network. Bitcoin Core is the backbone of the Bitcoin network and guarantees the security and consistency of the data stored on the blockchain. It is important to note that although Bitcoin Core is the reference client, there are many other Bitcoin clients written in different programming languages or developed for different operating systems.

DEEP INSIGHT

Bitcoin Software

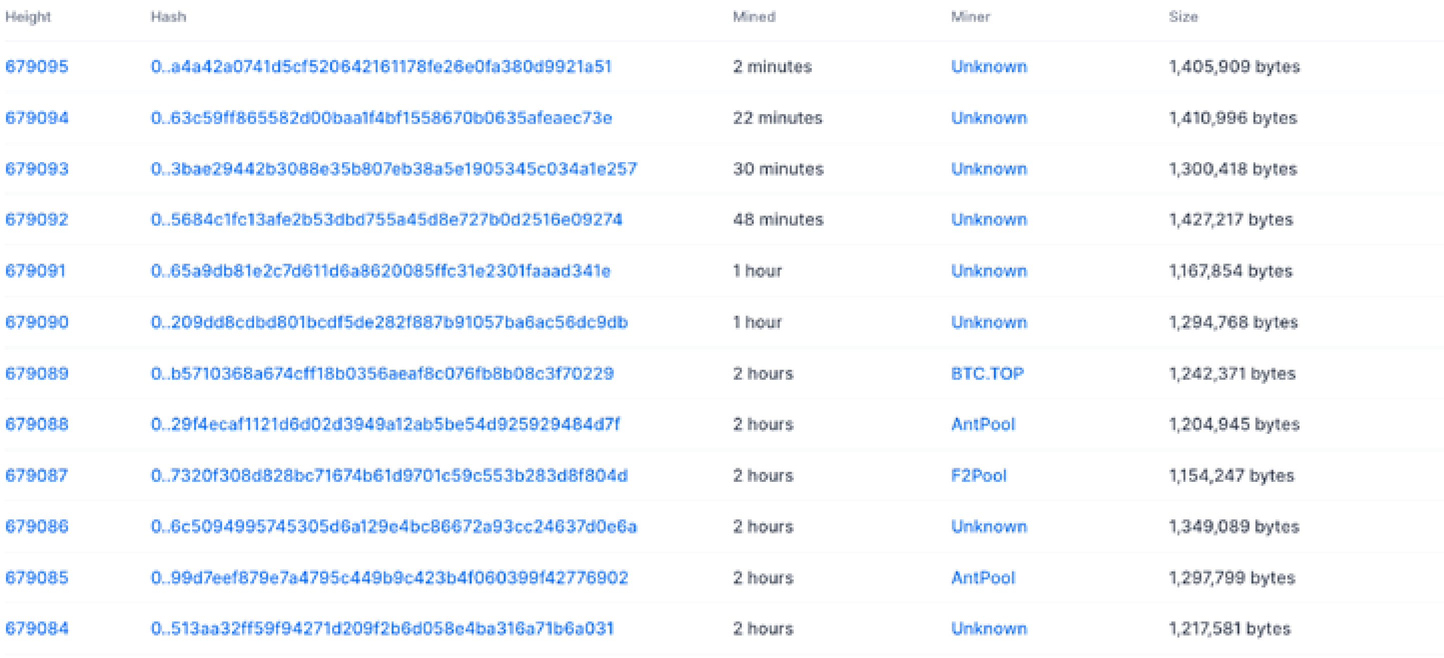
Bitcoin clients are the software that facilitate private key generation, secure private keys, send bitcoin, and provide information about the network. The Bitcoin protocol is specified by the behavior of the reference client, Bitcoin Core. Bitcoin Core is the third Bitcoin reference client, following Bitcoinind and wxBitcoin.

Bitcoin Core is written in the C++ programming language, but because Bitcoin is an open-source project, there are other clients written in different programming languages or are written for other various operating systems. Currently, there are approximately 80,000 instances of various Bitcoin clients, also called nodes, currently running. The overwhelming majority of clients currently running are a version of Bitcoin Core.

Clients come in both full node versions and light node versions. Full nodes are the backbone of the Bitcoin network and guarantee the security and consistency of the data stored on the blockchain. They store copies of every transaction that has occurred on the network, verify the validity of all transactions, and enforce consensus rules, or how the network agrees to its current state. Running a full node requires one to download a copy of the Bitcoin blockchain, a history of all past transactions, currently about 340 GB. Light nodes, designed to reduce the computational strain of running a full node, only contain a portion of each block, called the header, which allows them to verify blocks and interact with the network. Mining, covered below, utilizes special mining software, such as CGMiner.

What is the Blockchain?

The blockchain is an ever-growing ledger of all the transactions that have occurred on the Bitcoin network. This ledger is public and available for anyone to inspect and verify. Transactions between participants are batched together in blocks, processed simultaneously, and linked chronologically by cryptography.



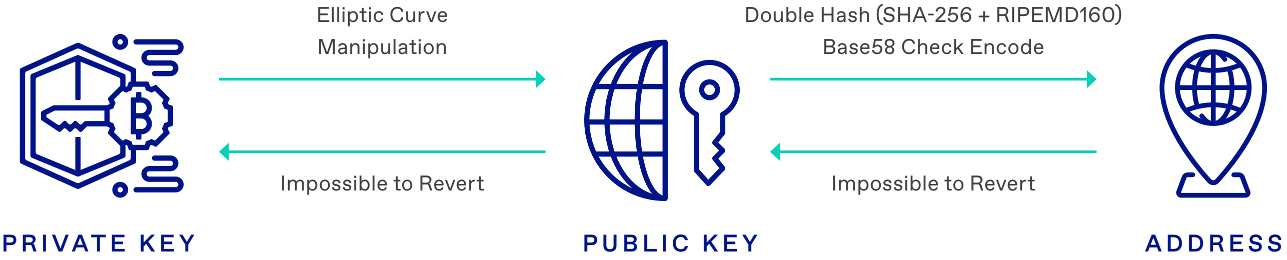
Height	Hash	Mined	Miner	Size
679095	0..a4a42a0741d5cf520642161178fe26e0fa380d9921a51	2 minutes	Unknown	1,405,909 bytes
679094	0..63c59ff865582d00baa1f4bf1558670b0635afeaec73e	22 minutes	Unknown	1,410,996 bytes
679093	0..3bae29442b3088e35b807eb38a5e1905345c034a1e257	30 minutes	Unknown	1,300,418 bytes
679092	0..5684c1fc13afe2b53dbd755a45d8e727b0d2516e09274	48 minutes	Unknown	1,427,217 bytes
679091	0..65a9db81e2c7d611d6a8620085ffc31e2301faaad341e	1 hour	Unknown	1,167,854 bytes
679090	0..209dd8cdbd801bcdf5de282f887b91057ba6ac56dc9db	1 hour	Unknown	1,294,768 bytes
679089	0..b5710368a674cff18b0356aeaf8c076fb8b08c3f70229	2 hours	BTC.TOP	1,242,371 bytes
679088	0..29f4ecaf1121d6d02d3949a12ab5be54d925929484d7f	2 hours	AntPool	1,204,945 bytes
679087	0..7320f308d828bc71674b61d9701c59c553b283d8f804d	2 hours	F2Pool	1,154,247 bytes
679086	0..6c5094995745305d6a129e4bc86672a93cc24637d0e6a	2 hours	Unknown	1,349,089 bytes
679085	0..99d7eef879e7a4795c449b9c423b4f060399f42776902	2 hours	AntPool	1,297,799 bytes
679084	0..513aa32ff59f94271d209f2b6d058e4ba316a71b6a031	2 hours	Unknown	1,217,581 bytes

05

Transactions

How are Transactions Kept Secure?

Bitcoin uses public-key cryptography to make and verify transactions. Three important elements are linked together that are used in transactions: private keys, public keys, and addresses. Private keys are used to create signatures, transferring bitcoin ownership to someone else, while public keys are used to check signatures.



Private Keys

A private key is the password that allows bitcoins to be spent and thus transition ownership. Private keys must be kept secret and safe or else someone could access and take your bitcoin. The following is an example of a private key:

cxprv9xg3pXGrrmSQNqRCZRFmphUZpkzt8s43ESotbcPXk5fLXt6NT3
fh2tTPyQ7tW2SWAS9uWjhDJzzex9m8qmAHsJvTN1hctsgiYFK9Moo9Nx1

Because the preceding number can be cumbersome to record or retain and the error in even a single character will result in the entire loss of funds, private keys are rarely handled directly by users. Instead, mnemonic keys are typically used. The preceding private key can be completely expressed by a 12-word mnemonic, making saving, storing, and transporting private keys much easier. The following is an example of a mnemonic key:

faith joke visa range turkey expose they bacon gentle hill cushion recipe

Public Keys

A public key is mathematically derived from a private key, but unlike a private key, it does not necessarily need to be kept secret. Public keys are used to determine if a signature of a transaction is genuine without divulging the private key. The following is an example of a public key:

xpub6E9pP9ny45P14SNMCzCBFCPwr2QHgWQqZggJg6sMjnGgPo8
Hf9tzPwtzHYeKXn6GdACpoKRcvkb2w6pvcAj6kwdw5mKLyDErWXKX8Bhozed

Addresses

Addresses are derived from public keys using mathematical operations called hash functions and encoded to make them into human readable strings. Addresses are shared between transaction parties to receive bitcoins. The following is an example of a public address:

1LGpghBaX7AGbxA5dvpVwR7vMy53R8HcXX

How are Transactions Sent?

A Bitcoin transaction is a signed message that transfers ownership from one address to another. Each transaction includes the sender's address, the receiver's public key, and a signature created using the sender's private key. Once a transaction has been signed, it goes through multiple steps to be appended to the blockchain through a process called mining:

- New transactions are broadcast to the entire Bitcoin network.
- Miners aggregate new transactions together into a block.
- Miners work to find a *proof of work* for their block.
- When a proof of work is found, the miner broadcasts the block throughout the network.
- Network participants validate the transactions in the block.
- Miners acknowledge the block as valid by moving to work on the next block.

06

Creation & Mining

How are Bitcoins Created?

Bitcoins are created by the software itself as a reward for a process called mining, the essential process of creating new blocks and appending transactions in Bitcoin's blockchain. This mining process also protects the security of the Bitcoin network by providing proof of work, which we discuss below.

The miner of a block is paid two fees: newly created bitcoins issued by the Bitcoin software itself (called the block reward), and transaction fees, which are paid by the senders of bitcoin. Bitcoin's block reward was initially set at 50 bitcoins per block but over time has been reduced to 6.25 bitcoins per block. Every 210,000 blocks, roughly every 4 years, Bitcoin reduces the block reward it pays to miners by 50% until it is eventually exhausted in the year 2140. At that point, all 21 million bitcoins will have been created, and no more new ones will ever be minted.

What is Proof of Work?

Mining, a function that provides vital security of the Bitcoin network, is designed to be computationally resource intensive so that it is impractical for any one entity to modify or control the blockchain. To be considered valid, blocks must contain a "proof of work", a piece of data that is difficult to produce but easy to verify. Producing a proof of work is a random computational process and therefore requires repeated trial and error.

How is Block Production Regulated?

Bitcoin is designed to produce blocks at 10-minute intervals on average. Every 2,016 blocks, Bitcoin measures the amount of time it took to produce those blocks and compares it to the expected production time, exactly 14 days. If those blocks took a shorter amount of time to produce, Bitcoin increases the difficulty of creating new blocks. If those blocks took longer to produce than 10 minutes on average, Bitcoin decreases the difficulty of creating new blocks. The purpose of this reflexive difficulty adjustment is to keep block production at 10-minute intervals as computational resources are added or removed from the network. It also enables Bitcoin's mining ecosystem to grow organically and fairly.

DEEP INSIGHT

Mining and Hash Functions

Producing a proof of work involves combining text from the previous block with an integer, called a nonce, in a cryptographic hash function, called SHA-256, to produce an output called a hash. If the value of this hash is lower than a number specified by the protocol, called a target, the new block is considered valid. If not, the nonce is changed until a hash is produced that is lower than the target. Because the text from the previous block also includes a hash of the previous block, this proof of work is chained together from block-to-block making it exceedingly difficult to revert or redo.

Cryptographic hash functions like SHA-256 are one-way mathematical algorithms that map data of arbitrary size into an array of fixed size. They are not encryption, meaning the hash cannot be decrypted back to its original text, and changing even one-character results in vastly different outputs. SHA-256 is a patented cryptographic hash function created by the National Security Agency that outputs a value that is 256 bits long. Some examples of SHA-256 hashes are:

Example:
Adding an "!" completely changes the hash.

Message: NYDIG
SHA-256 Hash: f08562886ddce54745bd29b1d
bf5e4b1ae54c34718938265a6b36b22917e8445

Message: NYDIG!
SHA-256 Hash: 45dc5108edee25df658f1300b0
a45c358243751e7bc3c1571aabb58fb4f36e80

Example:
Significantly adding text to a message does not change the length of the hash.

Message: It
SHA-256 Hash: 555c7b8b3856c5f4e5d6cd2 ec93
e4fc54678c49fd0d972d02608fab3ee7b37b3

Message: It was a bright cold day in April, and the clocks were striking thirteen.
SHA-256 Hash: 8ea71671a6edd987ad9e90974
28fc3f169decba3ac8f10da7b24e0ca16803bf0

DISCLOSURES

This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument or to adopt any investment strategy. Charts and graphs provided herein are for illustrative purposes only. This report does not represent valuation judgments with respect to any financial instrument, issuer, security or sector that may be described or referenced herein and does not represent a formal or official view of New York Digital Investment Group or its affiliates (collectively, "NYDIG").

It should not be assumed that NYDIG will make investment recommendations in the future that are consistent with the views expressed herein, or use any or all of the techniques or methods of analysis described herein in managing client accounts. NYDIG may have positions (long or short) or engage in securities transactions that are not consistent with the information and views expressed in this report.

There can be no assurance that any investment strategy or technique will be successful. Historic market trends are not reliable indicators of actual future market behavior or future performance of any particular investment, which may differ materially, and should not be relied upon as such. Target or recommended allocations contained herein are subject to change. There is no assurance that such allocations will produce the desired results. The investment strategies, techniques or philosophies discussed herein may be unsuitable for investors depending on their specific investment objectives and financial situation.

The information provided herein is valid only for the purpose stated herein and as of the date hereof (or such other date as may be indicated herein) and no undertaking has been made to update the information, which may be superseded by subsequent market events or for other reasons.

Information furnished by others, upon which all or portions of this report are based, are from sources believed to be reliable. However, NYDIG makes no representation as to the accuracy, adequacy or completeness of such information and has accepted the information without further verification. No warranty is given as to the accuracy, adequacy or completeness of such information. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions that occur subsequent to the date hereof.

Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. Legal advice can only be provided by legal counsel. Before deciding to proceed with any investment, investors should review all relevant investment considerations and consult with their own advisors. Any decision to invest should be made solely in reliance upon the definitive offering documents for the investment. NYDIG shall have no liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the information set forth herein. By accepting this report in its entirety, the recipient acknowledges its understanding and acceptance of the foregoing terms.

NYDIG

Find More Resources by Visiting

NYDIG.COM/RESEARCH