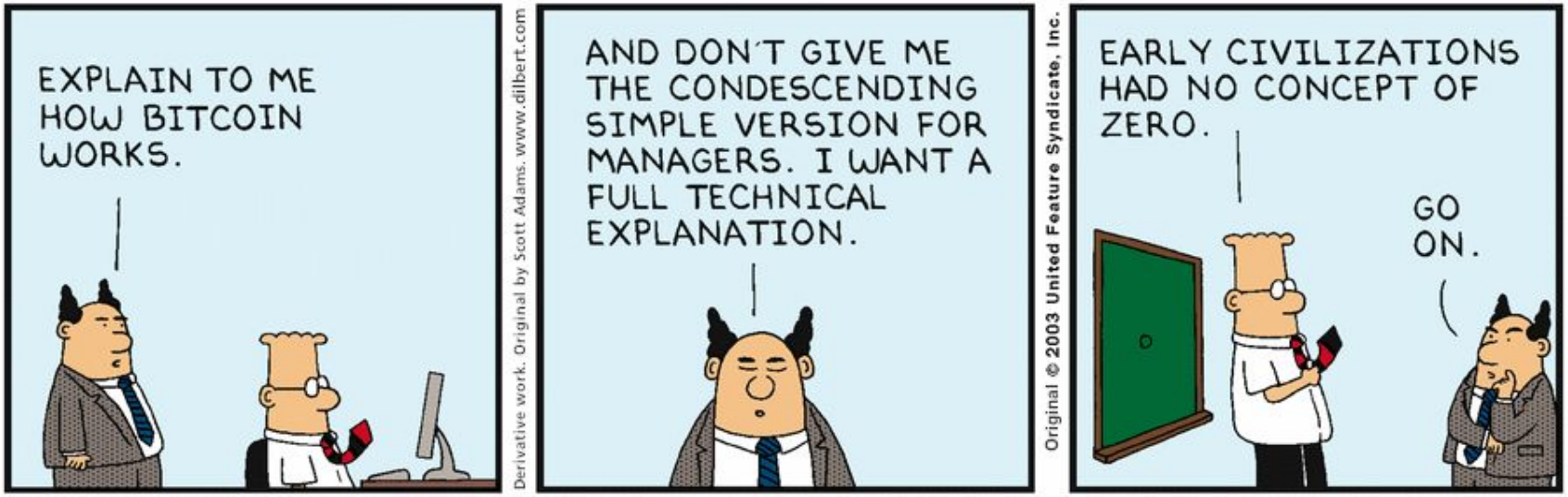
Introduction to Bitcoin

History, Problem, Solution, Implementation

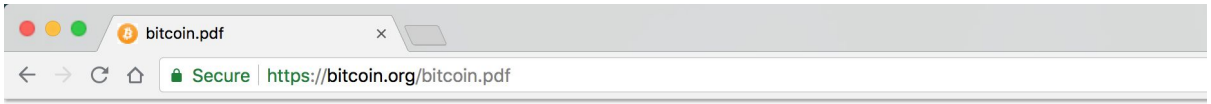
Kaspar Etter, October 2018

Let's start with some laughter:

But for real: How does Bitcoin work?



Well, almost ten years ago:



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Ingredients of the Magic Money

- Hash Function
- Proof-of-Work
- Hash Chain
- Digital Signature

What's **not** needed:

- Encryption

Hash Function

Deterministic: arbitrary data –> fixed-sized output

One-way function:

- Easy: input –> output
- Hard: output –> input

Collision: hash($input_1$) = hash($input_2$)

Cryptographic hash function: collision-resistant

Try it: https://anders.com/blockchain/hash.html

Proof-of-Work

Goal: Prove that you performed a certain amount of computation without requiring others to do so with a problem costly to solve but easy to verify.

Example: Find a nonce (number used only once) so that hash(input + nonce) < specified difficulty.

Proposed in 1992 to deter spam by making the sender waste processing power for a “stamp”.

https://anders.com/blockchain/block.html

Hash Chain

Chain hashes by using the output of the previous hash as an additional input to next hash function:

$\text{hash}(\text{input}_1) = \text{output}_1$

$\text{hash}(\text{hash}(\text{input}_1) + \text{input}_2) = \text{output}_2$

$\text{hash}(\text{hash}(\text{hash}(\text{input}_1) + \text{input}_2) + \text{input}_3) = \text{output}_3$

Altering **any** input alters **all** subsequent outputs.

https://anders.com/blockchain/blockchain.html

Digital Signature (Three Algorithms)

- **KeyGeneration**(entropy) –> private k, public K (called key because you can unlock things like coins; k –> K typically easy, K –> k always hard)
- **Signing**(message, k) –> signature (can only be produced by the person who knows the key k)
- **Verifying**(message, K, signature) –> true/false (anyone who knows the public key K can verify)

10^{77} possible private keys for Bitcoin
10^{80} atoms in the observable universe

Ledger: Coins Stay, Owner Changes

Digital data can be copied for free & without loss.
How to prevent an infinite amount of coin copies?

First insight: Instead of transferring coins, transfer their ownership; wallets consist of keys, not coins.

If you copy a wallet, you just have the keys twice.

Think of Bitcoin as parcels of land. Transacting is merging or splitting and assigning a new owner.

Prevention of Double-Spending

How to prevent one coin from being spent twice?

Easy with a trusted third party that can determine the order of transactions. How to do it without?

Second insight: Vote on the transaction history to establish an order of valid transactions.

Agreeing on the history of transactions means agreeing on the current state of the blockchain!

Problem: Who can vote (without central registry)?

Make Voting Costly & Compensate

Third insight: Vote by sacrificing a costly resource and be compensated for it with a digital currency.

This is inefficiency by design to avoid Sybil attack.

Most common: computing power (proof-of-work)

Alternatives:

- tied-up capital (proof-of-stake)
- computer memory (proof-of-space)

Bitcoin Address

Public keys are the identities of Bitcoin.

Only pseudonymous, not anonymous.

Use a different key for each transaction.

Address is encoding of public key (simplified).

Transactions and Blocks

Transaction: Unlock coins, then lock them again.

Example: 5 BTC from A –> B,

- which has to be signed with private key a;
- only B knows private key b to spend them then.

Block: 1 MB of transactions w. header containing among other things the hash of the previous block.

The hash of the block has to be smaller than the current mining difficulty (number of leading zeros).

Peer-to-Peer Network of Full Nodes

No central server, communication **among peers**
Connect to arbitrary peers, exchange information

Broadcast signed transaction to all your peers.

Miners keep track of **unconfirmed transactions**, which are not yet included in a block / the chain.

Miners try to find a new valid block with them, which they broadcast as soon as they found one.

Longest/Heaviest Chain Rule

Different miners might announce different blocks simultaneously, thus the **chain can diverge**.

All other miners append their next block to one of them. Since they can only include the hash of one block, they can only vote for one of the blocks.

All participants **take the longest/heaviest chain**.

Note: Voting = Appending, Appending = Voting

You can only double-spend with >50% of power.

Mining Difficulty

Difficulty: number of leading zeros of block hash

Depending on the difficulty, it takes more or less time to find a new block with its hash < difficulty.

Finding a new block should take on average 10 minutes. The difficulty is automatically adjusted accordingly every two weeks (in case of Bitcoin).

Block Rewards

Distribute coins over time and not from the start.

Whoever finds a block which makes it into the longest chain gets new Bitcoins out of nothing.

Since other nodes reject invalid blocks, miners are **incentivized** to adhere to the **agreed-upon rules**.

Current mining reward: 12.5 new BTC per block

Block reward **halves** every four years, leading to a fixed supply of around 21 million Bitcoins.

Transaction Fees

Miners are free to include whichever transactions they want into their blocks (given they are valid).

Transactions compete for being included in block.

Fee goes to miner that includes your transaction.

The higher the fee (per byte), the likelier a miner considers your transaction (you pay for fast lane).

Rules Upgrades and Chain Forks

The blockchain forks if some nodes accept transactions/blocks as valid that others don't.

Two kinds of forks:

- **Soft forks** restrict block acceptance rules, i.e. old nodes accept new blocks if a majority of miners upgraded their software to new rules.
- **Hard forks** widen block acceptance rules, i.e. old nodes reject new blocks and are left behind if a majority of miners and users upgraded.

Summary (from Bitcoin Whitepaper)

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. (https://bitcoin.org/bitcoin.pdf)

Always set up the wallet yourself!