CENTER FOR DEMOCRACY & TECHNOLOGY

Crypto-asse

t

Blockchain

Crypt

o

e-money

Crypto-currency

Crypto-Ledgers 101

Benjamin C. Dean

Center for Democracy and Technology

bdean@cdt.org

18 October 2017

Agenda

- A short history of money
- Use case: Bitcoin
  - Digital signatures
  - Blockchain
  - Mining and consensus
- A breather
- Emergent phenomena
- Future developments
- Policy implications

A short history of money

Barter

Shells

Commodities

Fiat currency

Representative money

Digital

Crypto-ledgers

INCREASING ABSTRACTION

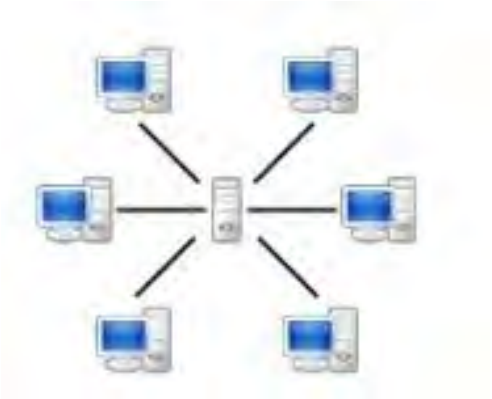
Bitcoin: A Peer-to-Peer Electronic Cash System

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.

The double-spend problem

- How can we ‘exchange’ digital 1s and 0s with no central administrator?



Centralized model:
A central administrator (e.g. bank) maintains a ledger that keeps track of who has what. Requires trust in the central administrator.

Decentralized model:
In the absence of no central administrator, how do we agree on who has what when exchange occurs between people who do not trust one another?

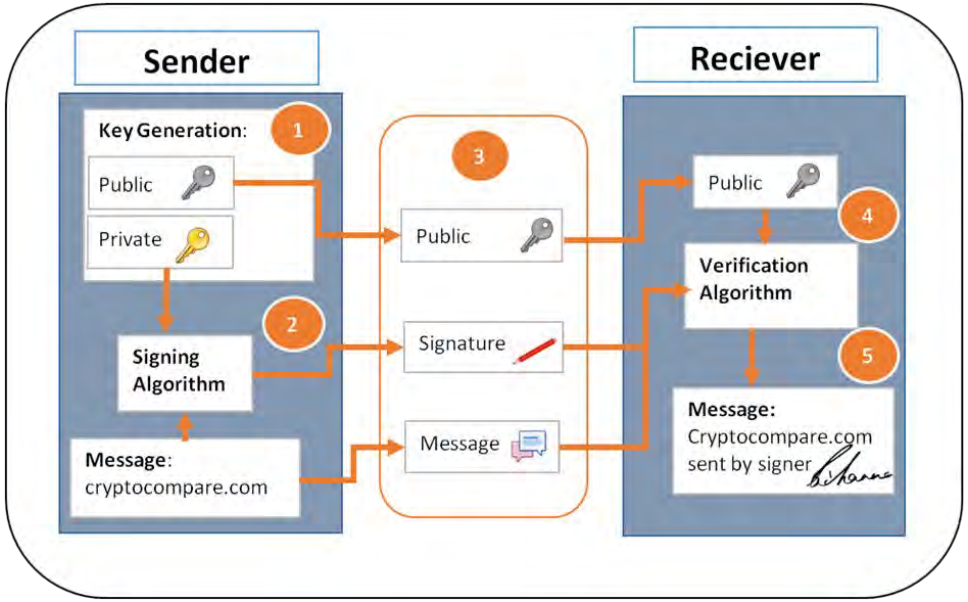
‘Trustless’ double-entry book-keeping at scale

1. Are the transactions valid?

2. How to ensure ledger is accurate?

Digital signatures and transactions

[If need be, go back and revise your public-key crypto]

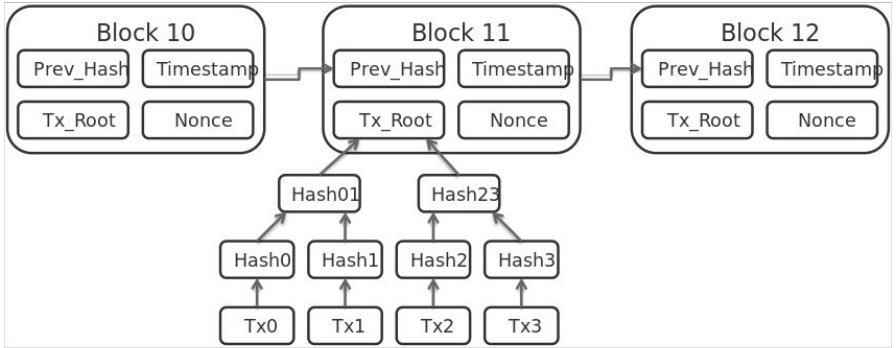


Source:
CryptoCompare

Transactions grouped in blocks… then chained together

- A shared ledger
- Transactions are appended every ~10min
- 1MB blocks
  - Timestamp: tells us *when* the transaction took place
  - Nonce: arbitrary value
  - Merkle tree and hashing to condense transaction data
  - Hash of previous block

What goes into a Bitcoin block?



Source: Matthäus Wander via Wikipedia

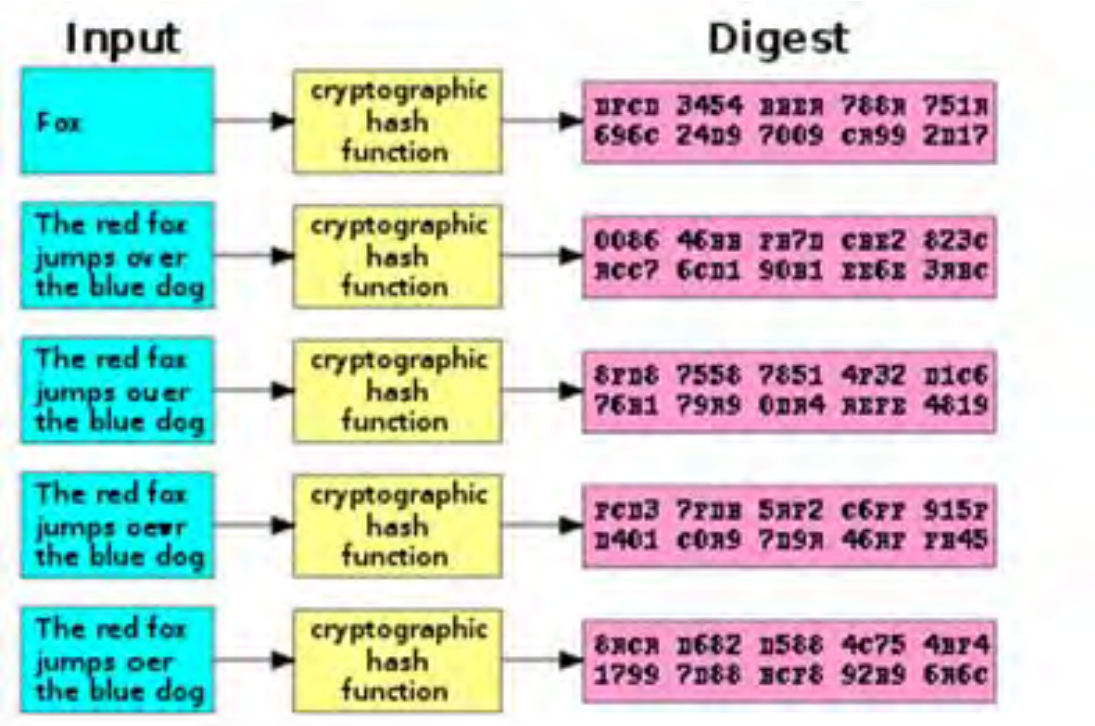
How to be sure the ledger is accurate? Where do Bitcoins come from?

- Solving difficult math problems using computing power (‘mining’)
- Bitcoins are a reward for taking part in the consensus mechanism (’proof of work’)
- Block reward added to account (12.5 Bitcoin at time of writing)
- Difficulty increases over time
- Reward decreases over time

Bitcoin mining in an undisclosed location in China

Source: The Coins Man, 2014

Hashing - easy to verify but hard to compute



Source: GuadaTech

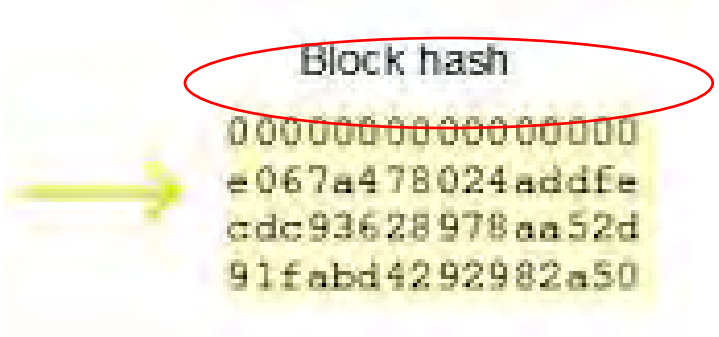
Nonces and their effect on hashes

nonce	hash
0	5c56c2883435b38aeba0e69fb2e0e3db3b22448d3e17b903d774dd5650796f76
1	28902a23a194dee94141d1b70102accd85fc2c1ead0901ba0e41ade90d38a08e
2	729577af82250aaf9e44f70a72814cf56c16d430a878bf52fdaceeb7b4bd37f4
3	8491452381016cf80562ff489e492e00331de3553178c73c5169574000f1ed1c
39	03fd5ff1048668cd3cde4f3fb5bde1ff306d26a4630f420c78df1e504e24f3c7
990	0001e3a4583f4c6d81251e8d9901dbe0df74d7144300d7c03cab15eca04bd4bb
52117	0000642411733cd63264d3bedc046a5364ff3c77d2b37ca298ad8f1b5a9f05ba
1813152	00000c94a85b5c06c9b06ace1ba7c7f759e795715f399c9c1b1b7f5d387a319f
19745650	000000cdccf49f13f5c3f14a2c12a56ae60e900c5e65bfe1cc24f038f0668a6c
243989801	0000000ce99e2a00633ca958a16e17f30085a54f04667a5492db49bcae15d190
856192328	0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50

Source: [Kenn Shirriff]

Mining: Guessing the nonce that leads to 0s

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	



Source: Kenn Shirriff

CENTER FOR DEMOCRACY & TECHNOLOGY

Let's stop for a breather…

1. Crypto-ledgers allow decentralized digital transactions
2. Bitcoin solves the double-spend problem
3. Digital signatures use PKI to ensure validity of transactions
4. Blockchain is a public ledger
5. Mining process ensures integrity of public ledger + creates new bitcoins + rewards miners for taking part in consensus process
6. Mining involves solving difficult math problems

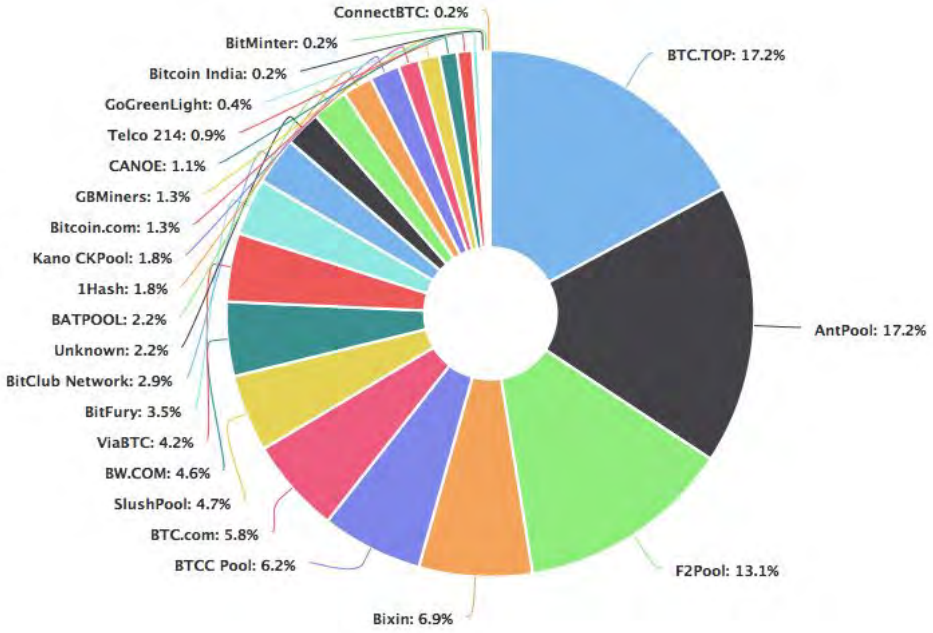
What's the value of a Bitcoin?

- What determines value?
  - The **cost of the work** you put into something (like 'proof of work')
  - The **supply** of the thing
  - The **demand** for the thing
    - Means of exchange
    - Store of value
    - Unit of account
- All of these have some partial bearing on the value of Bitcoins
- But which ones (over time)?

The Bitcoin experiment

- Immutability, decentralisation, transparency, freedom and trustlessness
  - What could go wrong?
- Mining concentration
- Intermediaries e.g. Coinbase, Mt. Gox
- Block size: Classic vs XT
- Transaction fees
- Non-reversible transactions
  - Ransomware
  - ‘Can Bitcoin send me my money back?’

Distribution of Bitcoin mining pools, July 2017



Source: blockchain.info/pools

Beyond Bitcoin

- Building bigger blocks (‘scaling up’)
- What other intermediaries could we do away with? e.g. Ethereum and ‘smart’ contracts
- Anonymity instead of pseudonymity e.g. Zcash
- How else to reach consensus? e.g. proof of stake
- Private/permissioned blockchains

Policy and legal issues in the US

- Pseudonymous/anonymous transactions
  - Terrorist financing and anti-money Laundering
  - Ransomware
- Initial Coin Offerings
- Crypto-currency, -security, -asset, -commodity?
  - SEC, IRS, CFTC
- Ethereum ‘smart contracts’ – not smart, not contracts

Further reading

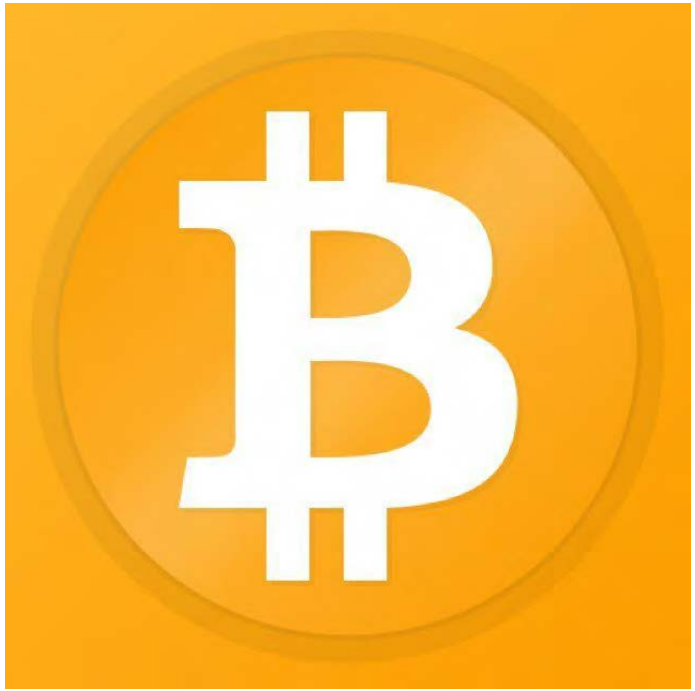
- Bitcoin Wiki
- 3Blue1Brown, "Ever wonder how Bitcoin (and other cryptocurrencies) actually work?" (video)
- Computerphile, "SHA: Secure Hashing Algorithm" or "Hashing algorithms and security" (videos)
- David Birch, "Explaining Bitcoin to the man on the street"
- Steve Wilson, "Bitcoin plain and simple"
- Wikipedia, "Bitcoin" and "Blockchain"
- Kenn Sherriff, "Mining bitcoin with pencil and paper", (more technical – but truly excellent blog)

CENTER FOR DEMOCRACY & TECHNOLOGY

Appendix

Bitcoin: a peer-to-peer payments network

- Peer-to-peer payment network operating on a cryptographic protocol
- Blockchain: a huge, distributed database (e.g. ledger) for which everyone can have a copy
- Unchangeable record of the *order* of all transactions tracing back to the first transaction
  - Bitcoin blockchain size 7/1/17: 144.35 GB (source)
- Uses a cryptographic protocol for transactions



Odds of solving the math problem

Kenn Sherriff:

- “finding a successful hash is harder than finding a particular grain of sand out of all the grains of sand on Earth.”

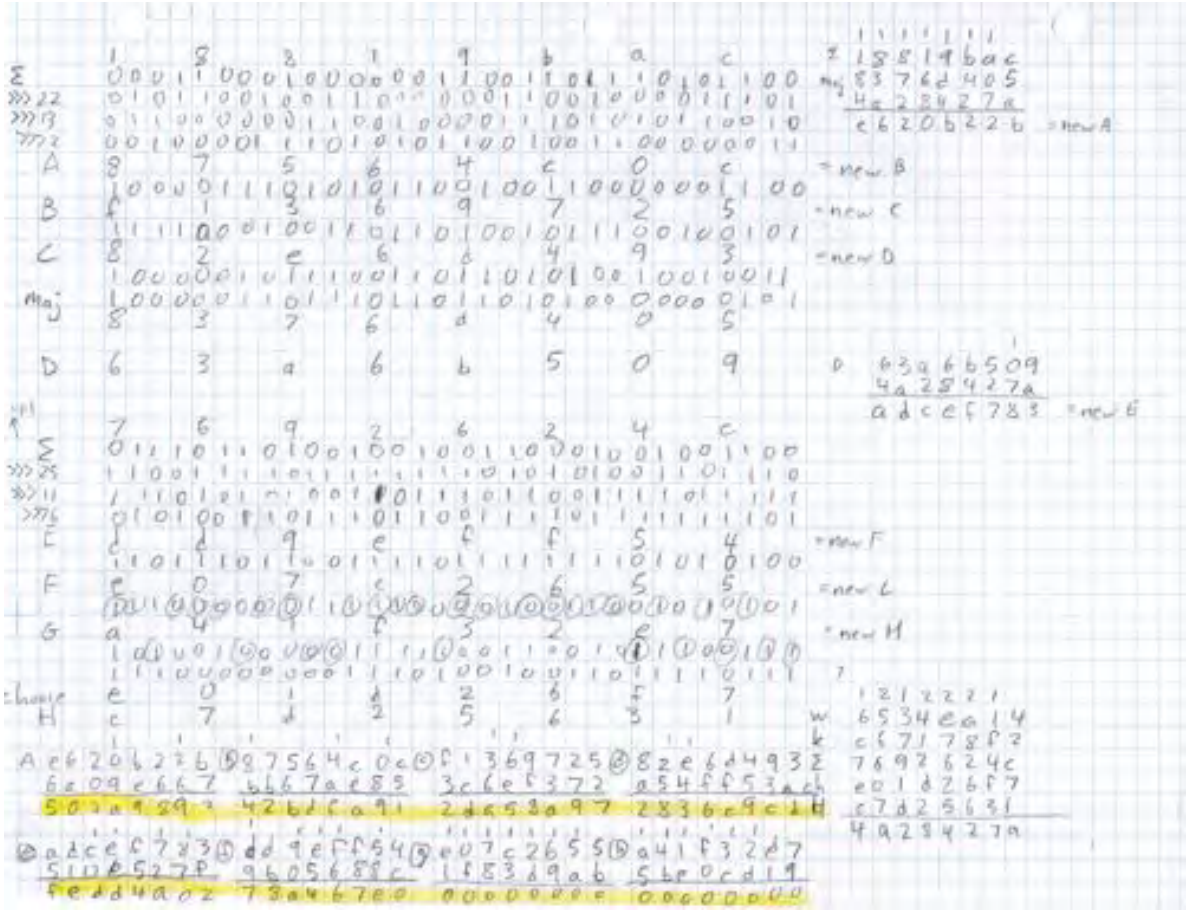
Source: CNN

Addresses, accounts and wallets

- Accounts (hold many wallets)
  - Each Bitcoin user is like a bank
  - Multiple accounts in a bank
  - Each Bitcoin you send goes from a different account
- Addresses (used for transactions)
  - Accept Bitcoins (don’t send)
  - Most addresses are 34 characters (some are shorter)
  - One per transaction
  - Created using a public and private key

- Wallets (hold keys and addresses)
  - Keypairs for each of your addresses
  - Transactions done from/to your addresses
  - User preferences
  - Default key
  - Reserve keys
  - Accounts
  - A version number

Try it yourself!

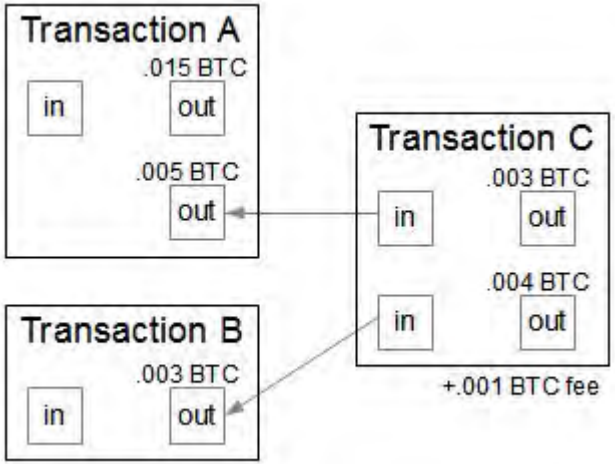


Benjamin Dean | 18 October 2017 | @benjamindean

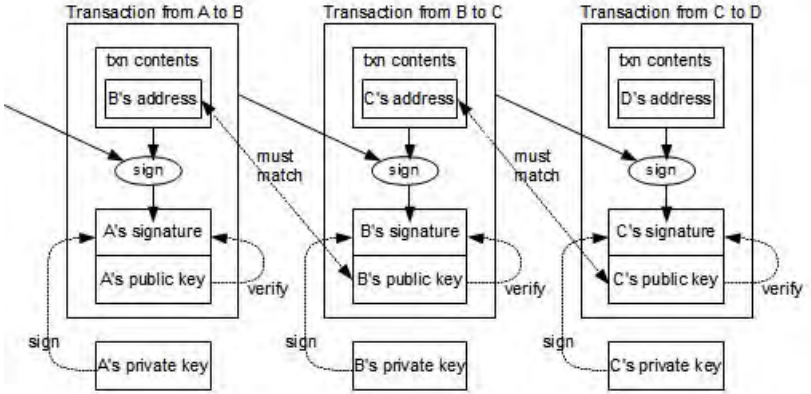
Source: Kenn Sherriff

The ins-and-outs of transactions

How transactions work

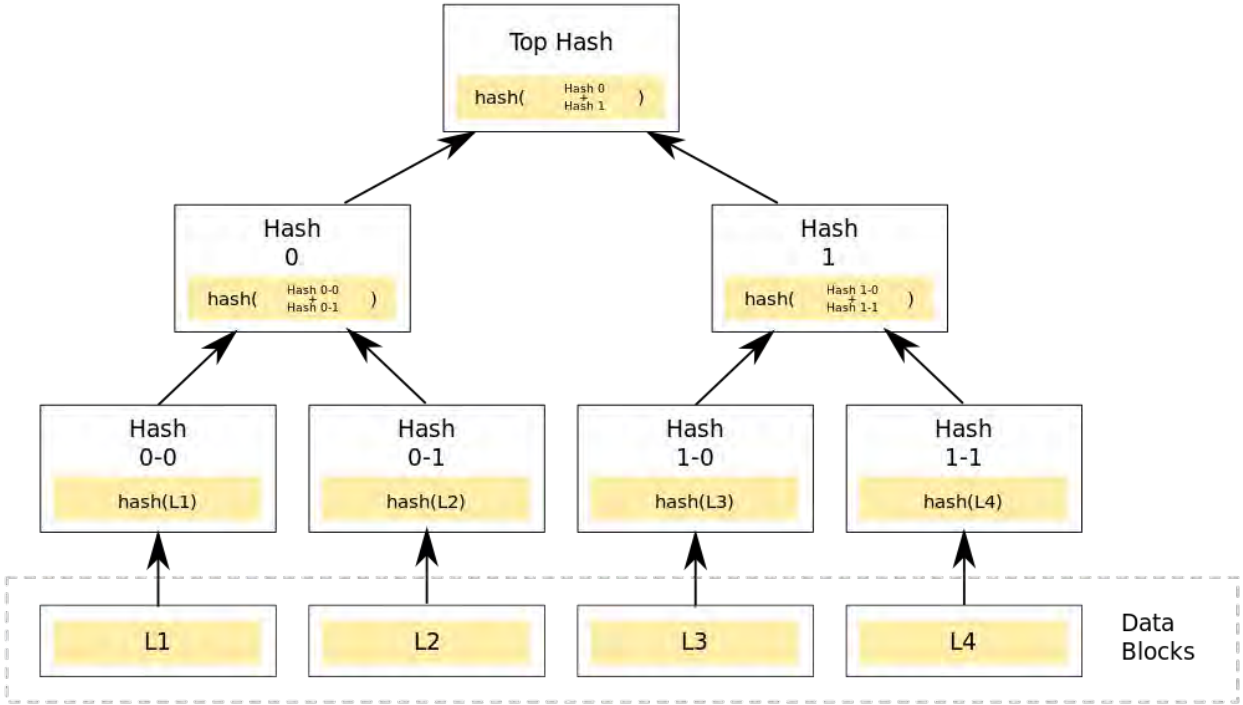


Chaining blocks together



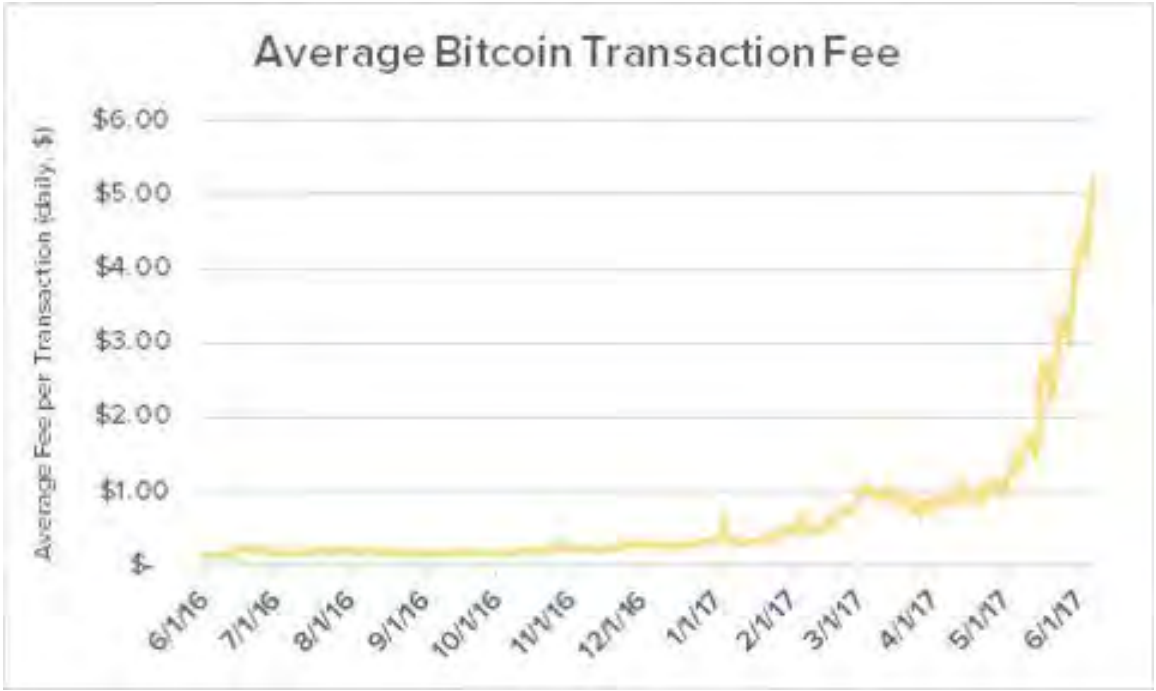
Source:
Kenn Sherriff

Merkle trees



Source: Azaghal

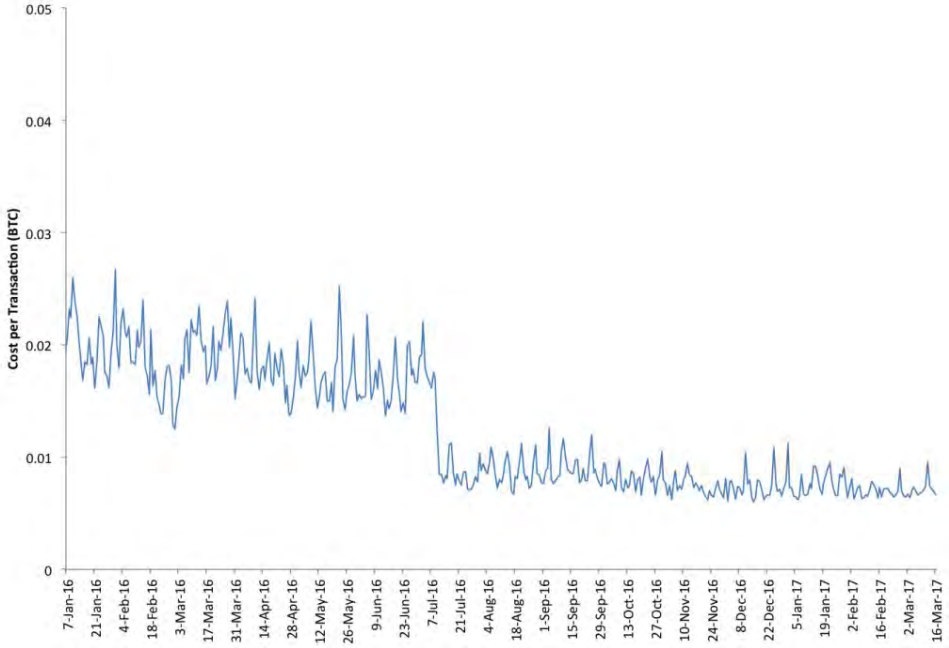
Transaction fees



Source: [Alex Sunnarborg]

Transaction fees (another perspective)

Average cost per transaction (block reward plus transaction fees, divided by number of transactions)



Source: Elaine