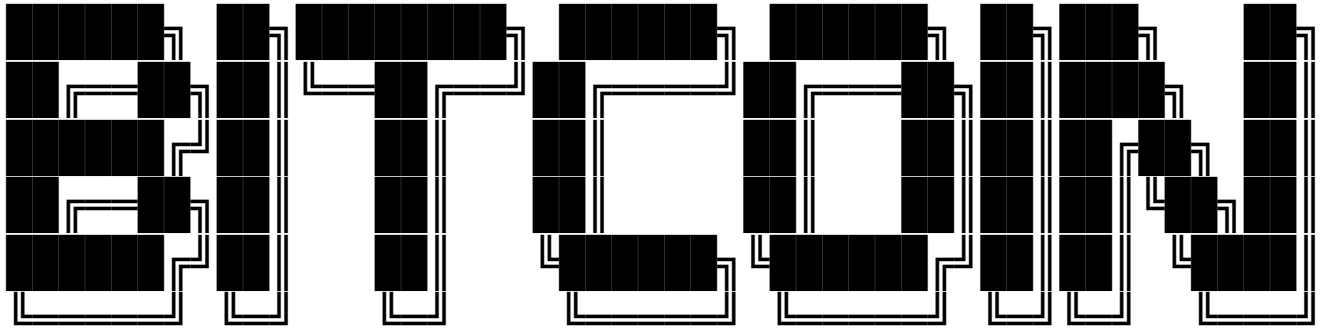

BITCOIN

Brief History

- An online p2p payment system invented by Satoshi Nakamoto
- Invented in 2008 – research paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Open source implementation was published in 2009
- The first decentralized crypto-currency based on the blockchain

Overview

- Peers can send money to each other without an intermediary
- Transactions are verified by the “network”
- All transactions are publically stored in a ledger called the “blockchain”
- Bitcoins are distributed by the network (created) as a reward for donating processing power to verify and record payment history
- A finite number of bitcoins will ever exist (21 million) to be fully distributed by roughly 2110 – 2140 CE

Bitcoin was the first **blockchain application**

The Bitcoin Blockchain

- A public ledger that records bitcoin transactions
- The Bitcoin blockchain is kept on nodes in the network running the bitcoin software (i.e. people's computers and servers)
  - Currently 34Gb in size
- When transactions are broadcast to the network and verified each node's blockchain is updated (but not all nodes get these messages)
- Every 10 minutes (roughly) a block of accepted transactions created and added to the Bitcoin blockchain
- Each block contains a hash of the previous block so as time passes it becomes harder for the chain to be modified because each block after the modified block would need to be created and valid

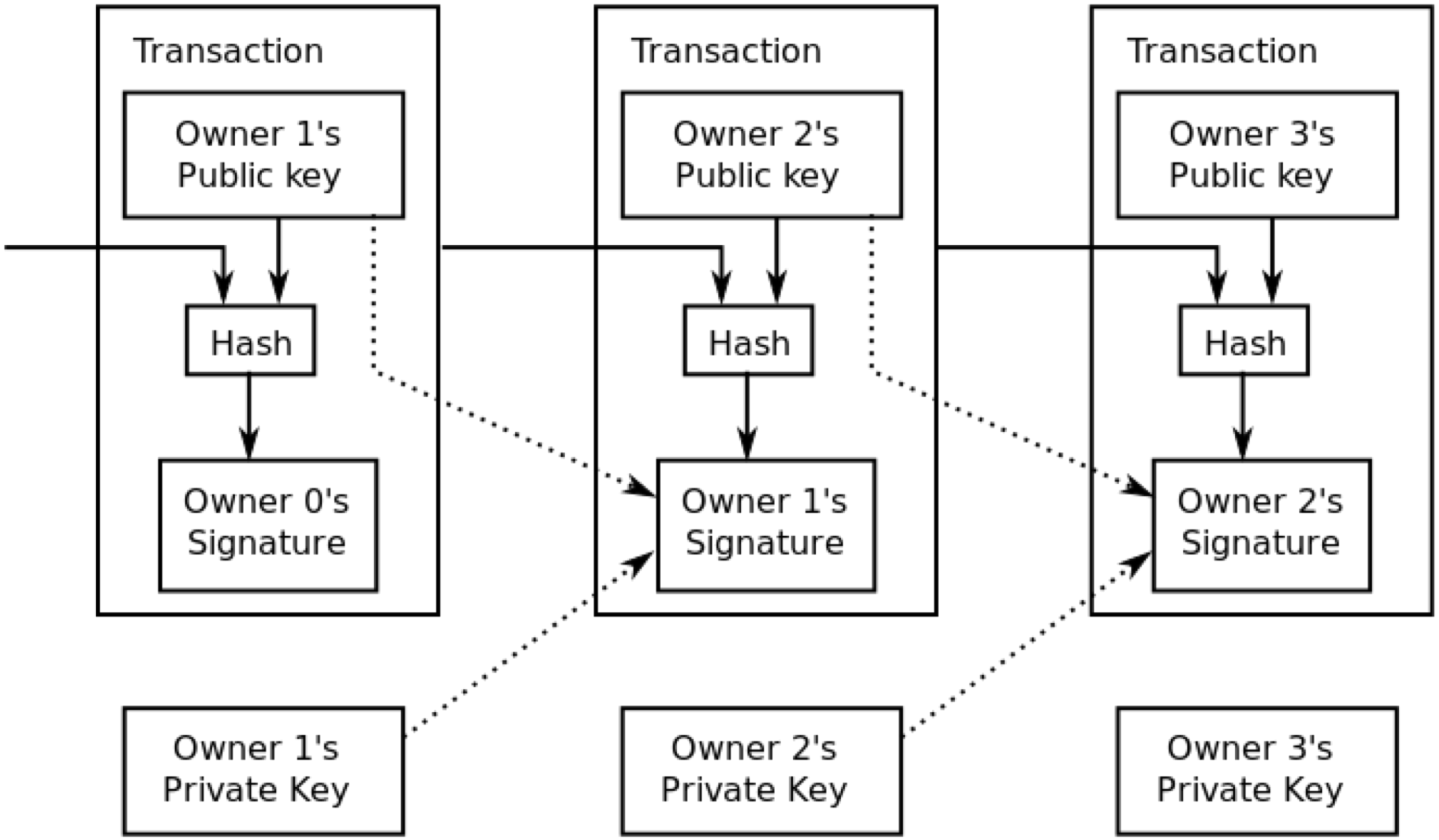
Transactions

- Each transaction must be sourced from the unspent output of a previous transaction
- Every input to the transaction must be digitally signed
- Only the owner of the Bitcoins is able to digitally sign the transaction
- Therefore only the owner may “spend” a bitcoin

Ownership

- Ownership means the ability to spend
- Coins don’t exist in a physical realm, they can’t be possessed in a traditional sense
- In order to send bitcoin to someone (spend it) the transaction must be signed with the corresponding private key
- The network verifies the transaction with the public key
- If the private key for some coins are lost then they are un-spendable and effectively gone

Ownership


Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

Wallets

- Wallets don’t “store” Bitcoin
- Bitcoin doesn’t exist outside of the block chain
- The wallet is simply a collection of the two keys needed to send and receive Bitcoin
  - Public key (so people transfer bitcoin to you)
  - Private key (so you can authorize transactions and transfer bitcoin to other addresses)

Wallet Addresses

- 25 to 34 alphanumeric characters
  - Except O, L, l, 0
- Begins with a 1 or 3
  - 1 is a traditional address
  - 3 is a multi-signature address
- Represents the destination of a Bitcoin transaction
- New addresses can be generated freely and per transaction if the user wants

Mining

- Miners verify and collect transactions broadcast to the network into a block
- Each block contains the SHA-256 hash of the previous block
- For a block to be “accepted” by the network a miner must find a random number (nonce) that when hashed with the block of transactions results in a number that is smaller than the network’s difficulty target

Mining

- The proof of work is easy to verify (single hashing operation) but expensive to generate – brute force
- Every 2016 blocks (about 2 weeks) the difficulty target is adjusted so the average time for finding the proof-of-work is about 10 minutes
- As the network computing power goes up the proof-of-work becomes harder

http://www.vnbitcoin.org/bitcoincalculator.php

Video

https://www.youtube.com/watch?v=l9jOJk30eQs

More Detailed Video

https://www.youtube.com/watch?v=Lx9zgZCMqXE

Uses

- Money can be sent to anyone, by anyone
- All transactions are public and in the clear
- A push based transfer scheme instead of pull based
- A giant decentralized cryptographically secure leger provides a way of:
  - Recording information
  - Voting
  - Publishing
  - Signing contracts

Anonymity

- Bitcoin is not anonymous, all transactions are public
- Someone can separate themselves from their bitcoin transactions, but there is no built in anonymity
- Once bitcoin addresses and transactions touch external markets anonymity is lost
- Any anonymity relies on operational security

Sources

- https://en.wikipedia.org/wiki/Bitcoin
- https://en.bitcoin.it/wiki/Address
- https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses
- http://www.vnbitcoin.org/bitcoincalculator.php