Bitcoin

By Yi Zhang & Nikolaos Kokkinis-Ntrenis

Bitcoin

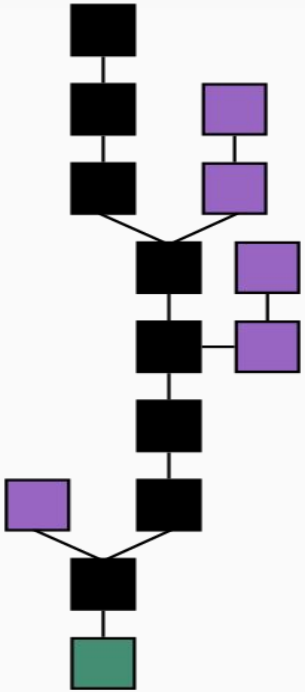
What is Bitcoin?

- It is a decentralized digital currency without any single Administrator
- Using peer-to-peer network
- Transactions recorded in a public distributed ledger called “blockchain”
- Invented in 2008, code released at 2009

Bitcoin

What is Blockchain?

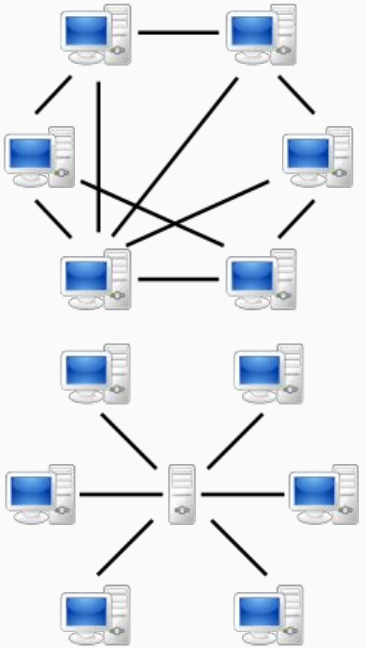
- List of records, called blocks
- Each block contains a cryptographic hash of the previous block, a timestamp and data
- Blockchain is resistant to modification of the data



Bitcoin

Peer to Peer Network

- Distributed application architecture that partitions tasks between peers
- Peers are equally privileged
- Peers are both suppliers and consumers of resources vs Client-Server where they only consumes

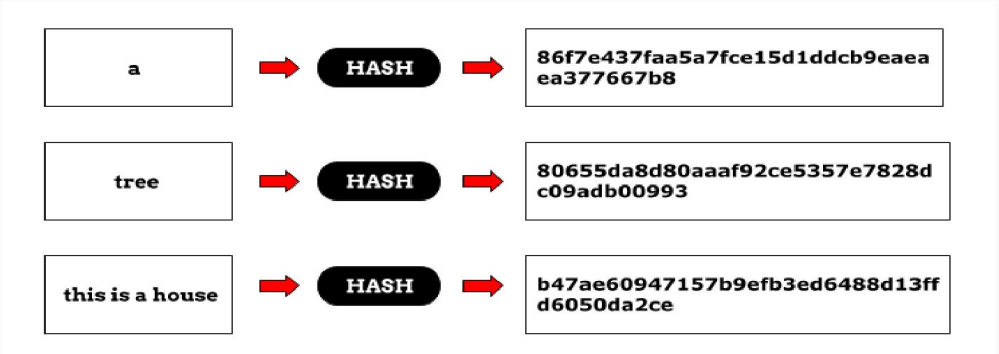


Bitcoin
Hash Function

Function that can be used to map data of arbitrary size to fixed-size values

Must satisfy two basic properties:

- should minimize duplication of output values (collisions)
- should be very fast to compute



How to get Bitcoin?

- First, sign up for a Bitcoin Wallet
- A Bitcoin Wallet is for your private key, not for storing Bitcoin, while your public key serves as the address published to the world
- Use regular money to buy Bitcoin

Where to use Bitcoin?

- Shop
- Donate **anonymously and privately**, charities who accept Bitcoin include: Wikipedia, Red Cross, Green Peace
- Invest
- Bitcoin ATMs

Mining

Block chain, a shared data structure, one form of distributed ledger design.

Bitcoin, reward for the agents in the Bitcoin network, who **contribute computational power** in order to **maintain, secure, and extend** Bitcoin's public ledger of past transactions, the block chain.

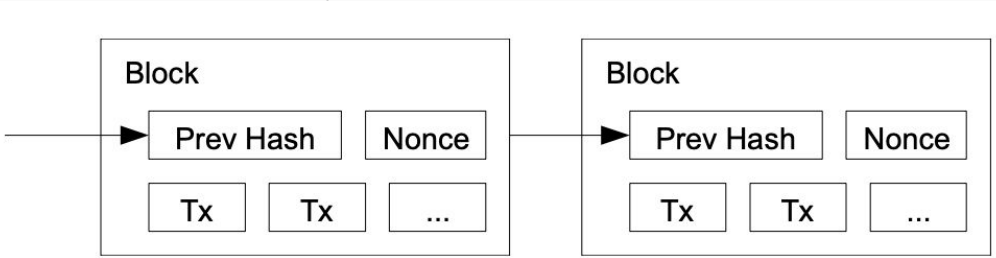
Miners, the network of participants, who **contribute computational power**.

Mining, the process to **maintain, secure, and extend** Bitcoin's public ledger.

Mining
Proof of work

Bitcoin uses the Hashcash proof-of-work function, such as with SHA-256, for block generation.

- Increment nonce in the block until a value is found that gives the hash of the block's header the required number of zero bits
- hash(b(nonce)) <= target, where the nonce is a 32-bit field, hash or the target is a 256-bit number
- Under the Bitcoin protocol, the longest chain is the only valid chainWhat if attacks happen, and transactions are changed?



Mining

Miners & Mining

Miner, who constantly attempts to solve cryptographic puzzles in the form of a hash computation until required hash is found

Mining, the process of validating a block in order to add it into the blockchain.

Mining

Mining Ecosystem - Hardware

CPU Mining, GPU Mining, FPGA Mining, ASIC Mining, Cloud Mining

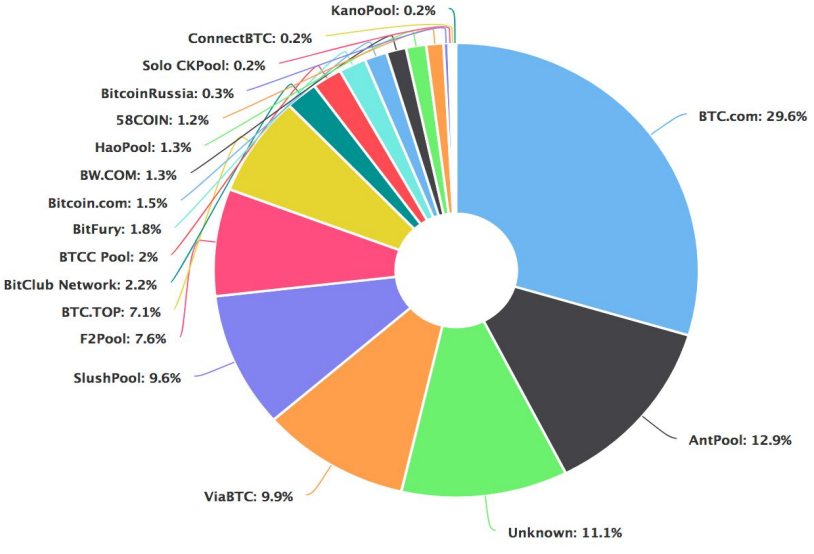
for the amount of power they consume, ASICs are vastly faster than all previous technologies

Mining

Mining Ecosystem - Pools

Mining pools are groups of cooperating miners who agree to share block rewards in proportion to their contributed mining hash power.

Game Theory



Mining
Difficulty

Difficulty, a measure of how difficult it is to find a hash below **a given target**. Each 10 min a new block is created, or every 2,016 blocks take two weeks, the target can be modified to match this. The lower the target, the more difficult it is to generate a block.

Hash rate, h/s, is an SI derived unit, representing the number of double SHA-256 computations performed in one second.

Currently the reward of mining is **12.5** bitcoins; this value will **halve** every 210,000 blocks. Additionally, the miner is awarded the bitcoins paid by users sending transactions.

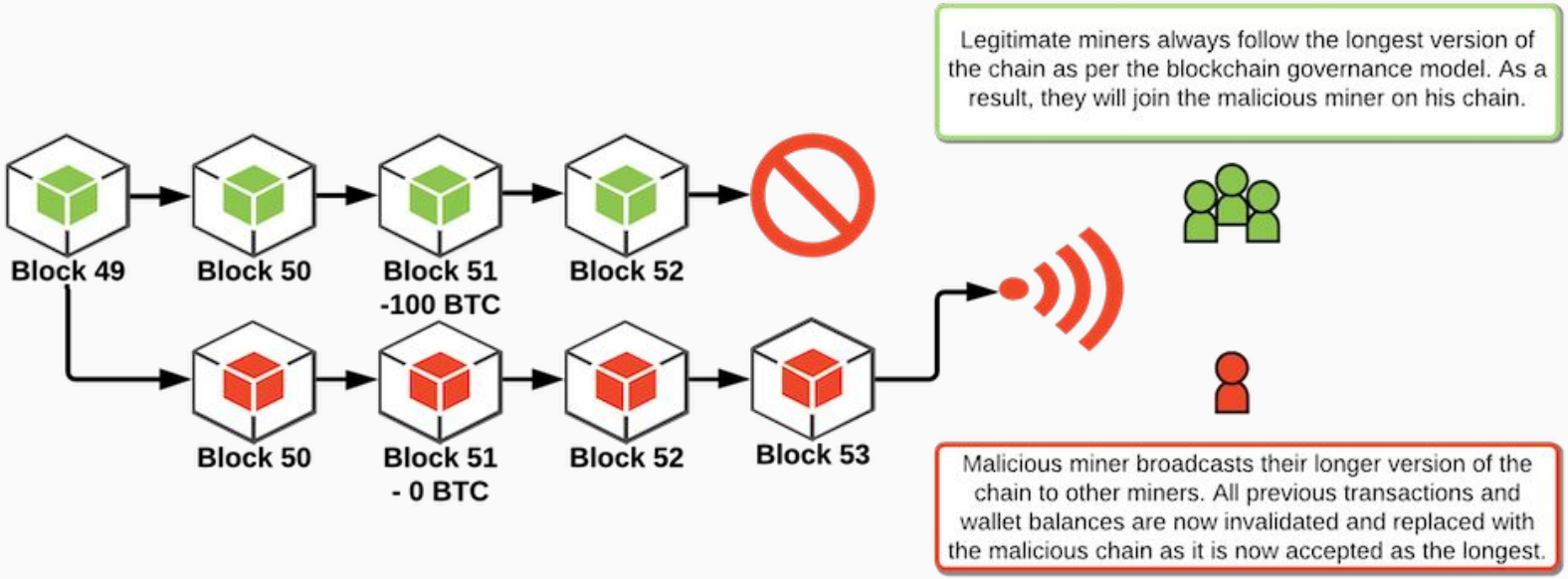
There are **21 million** bitcoins totally, around 18 million bitcoins in existence and 3 million bitcoins left to be mined.

Mining

Still worth mining?

https://www.blockchain.com/explorer

51% Attack


Block 49
Block 50
Block 51
-100 BTC
Block 52
Block 50
Block 51
- 0 BTC
Block 52
Block 53
Legitimate miners always follow the longest version of the chain as per the blockchain governance model. As a result, they will join the malicious miner on his chain.
Malicious miner broadcasts their longer version of the chain to other miners. All previous transactions and wallet balances are now invalidated and replaced with the malicious chain as it is now accepted as the longest.

Proof of work vs Proof of stake

Proof of work:

- Do expensive computational tasks (Mining)
- Miner get a reward
- Miner could create pools to increase efficiency
- Need lot of electricity

Proof of Stake:

- The creator of the block is chosen deterministic depending on his holding (Stake)
- No reward, receive transaction fees
- More decentralized system and significantly more cost effective
- Less power consuming

Questions?