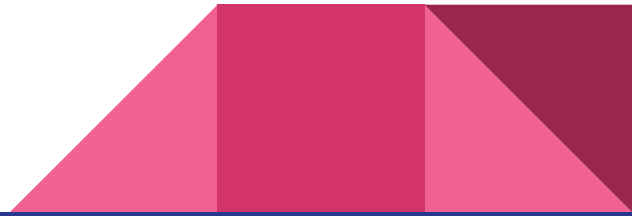
Bitcoin Mining

A high-level technical introduction

Konstantinos Karasavvas

Outline

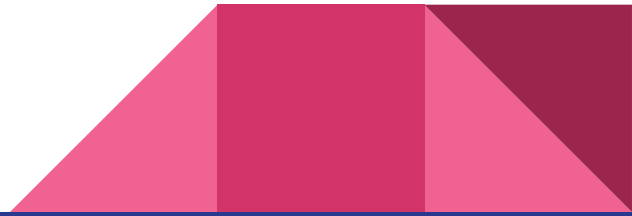
- PoW / Hashcash
- Transaction propagation
- Block mining
- Block propagation
- Mining Profitability



Proof of Work

From wikipedia:

> A **proof-of-work** (**POW**) **system** (or **protocol**, or **function**) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.



Hashcash

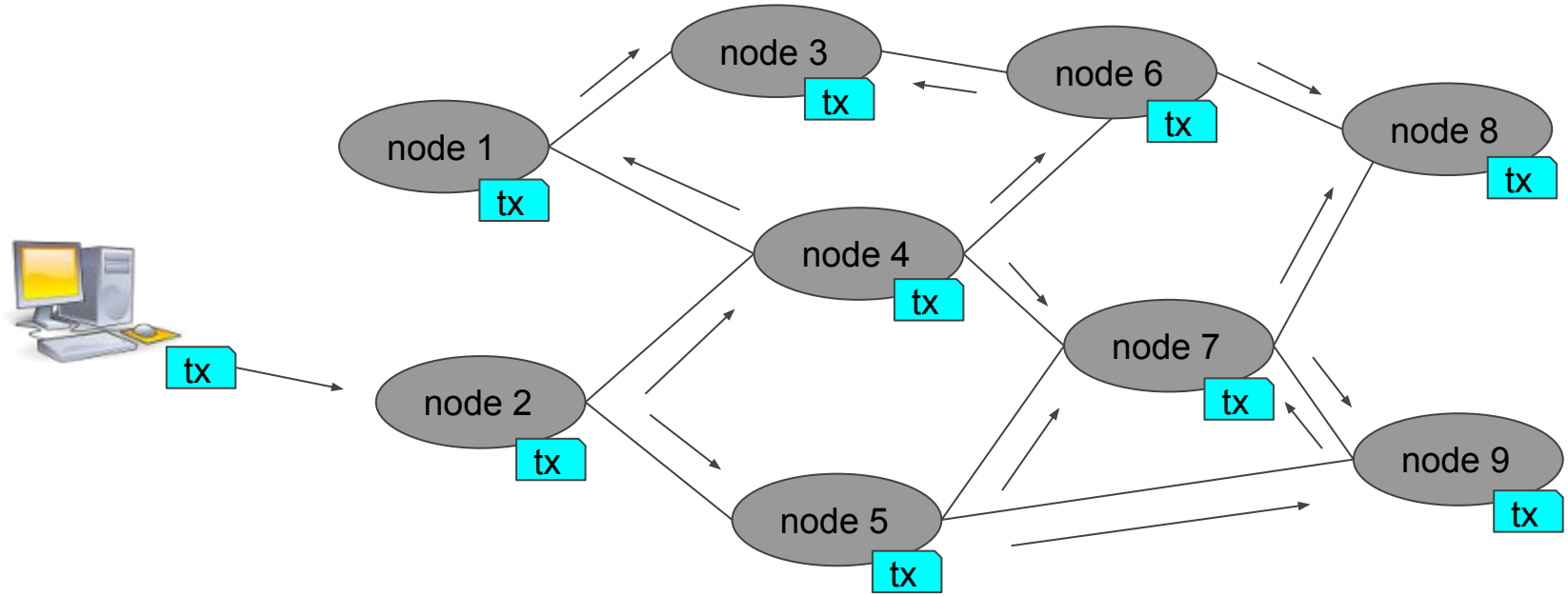
- Proof-of-work system
- hashing
  - arbitrary size to fixed size
  - one-way function

SHA256(“Bitcoin meetup!”) =>
d7d8992096b2261cd5fb01306149e1ab14a1cefa07e67
41feade682ecb307e89c

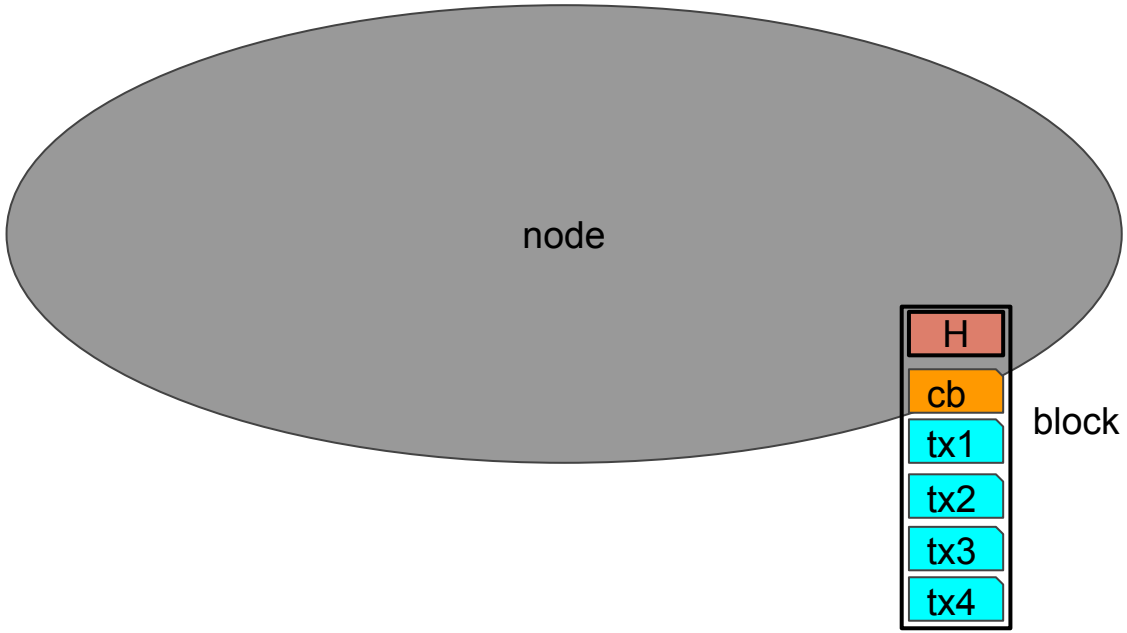
SHA256(“Bitcoin meetup.”) =>
a0236682605c9b25eddf5a82fc9cbe326ae7bffe69807
47ba39f5d4cd7cc2d17

- Example: dealing with email spam
  - hashcash stamp is required in the email
  - email and random number are hased
  - first 20 bits need to be zero
  - validation requires finding only one hash
  - proposed by Adam Back in 1997
- Example: dealing with Bitcoin transaction spam

Transaction Network Propagation



Miner Nodes - Blocks

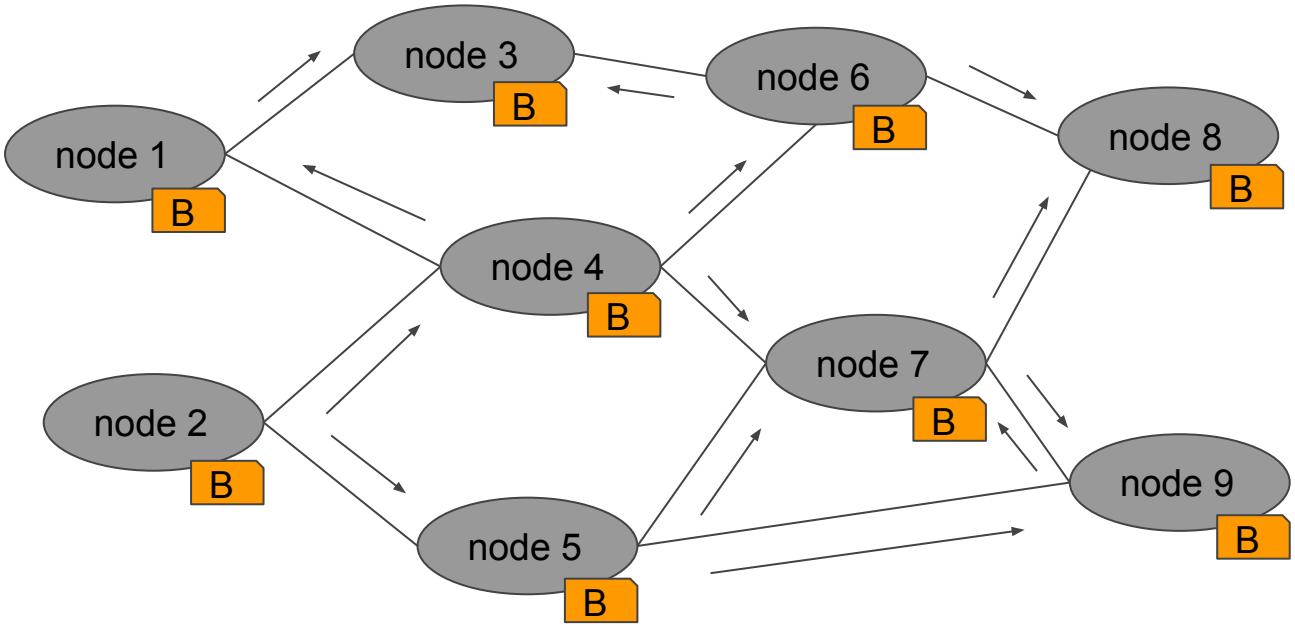


Bitcoin Mining

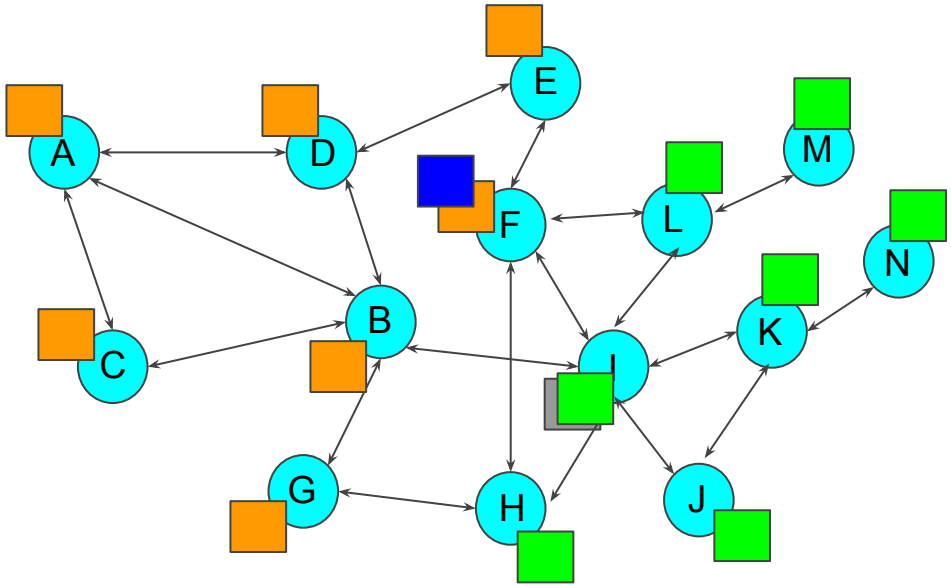
- block is decided
- mining process begins
  - block header is hashed
  - until hash is below target
  - nonce is increased
  - repeat
- nonce space limited (~4.2B)
  - timestamp
  - coinbase transaction

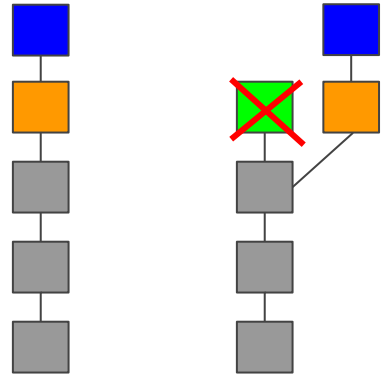
Block Header
Version
hashPrevBlock
hashMerkleRoot
timestamp
target / difficulty
nonce

Block Network Propagation



Regular forks (frequent)





Block Propagation and Validation

- Blocks need to propagate to all known peers
  - of each node
- Each node will validate the new block
  - and add it to their blockchain
  - forever (!) - immutable ledger
- Miner with first valid new block gets the reward
  - After 100 confirmations!

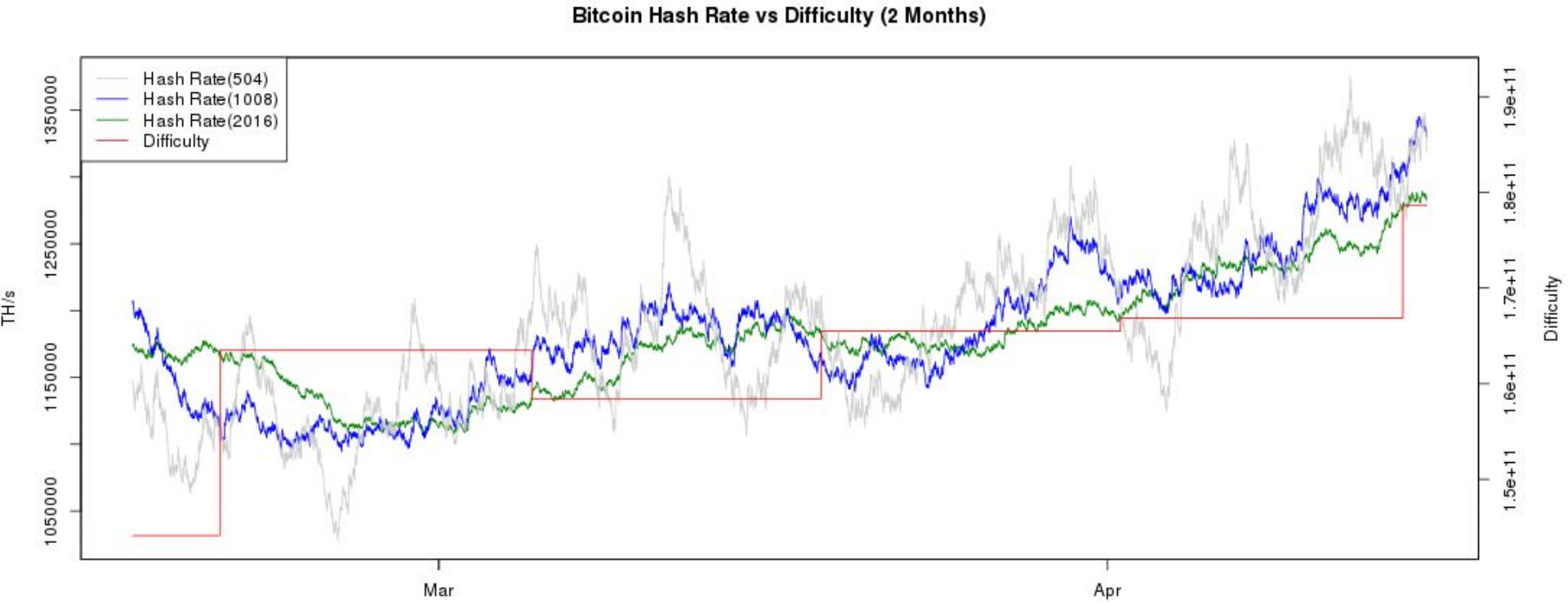
- How do we ensure that miners will not spam the network?
- How do we ensure consistent coin generation?

Mining predictability (15/04/2016)

- current network hashrate: 1,279,029 Th/s (1.27 Eh/s)
  - new block / ~10 minutes
- current difficulty: 178,678,307,672
  - many leading zeros
- but hashrate is fluctuating
  - 2016 blocks (~14 days)

```
Difficulty    = hashrate / (2^256 / max_target / intended_time_per_block)
              = hashrate / (2^256 / (2^208*65535) / 600)
              = hashrate / (2^48 / 65535 / 600)
              = hashrate / 7158388.055
```

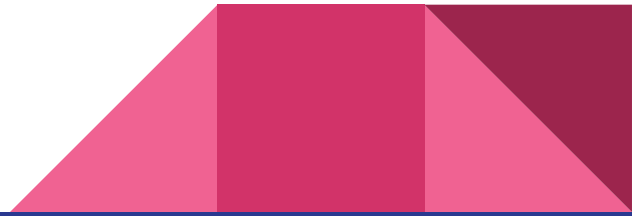
Bitcoin Hash Rate vs Difficulty



Next: Different ways to mine

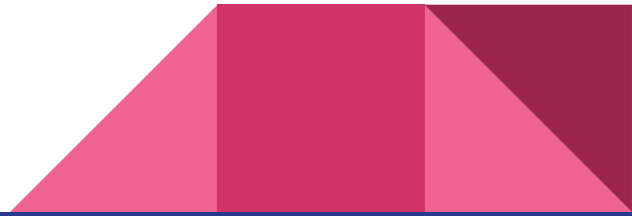
Different ways to mine

- Solo mining
  - **mining hardware**
  - **electricity costs**
  - bitcoin node
  - maintenance
- Pool mining
  - **mining hardware**
  - **electricity costs**
  - mining pool fee
- Cloud mining
  - buy mining contract and/or subscription



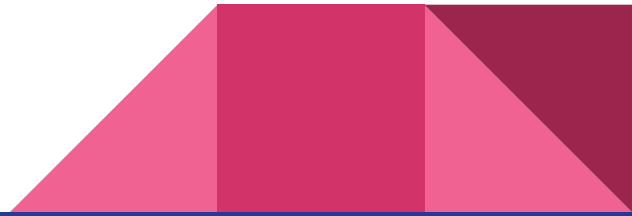
Mining hardware required to mine?

- Hardware capable of producing hashes
- In the past
  - CPU (~2011)
  - GPU (~2012
  - FPGA (~2012)
- Now
  - ASIC (mining farms)
- Examples
  - AntMiner S7 (4.73 Th/s, 0.25 W/Gh, ~$650)
  - Avalon6 (3.5 Th/s, 0.29 W/Gh, ~$870)
  - SP20 Jackson (~1.5 Th/s, 0.65 W/Gh, ~$149)
- Solo vs Pool mining?



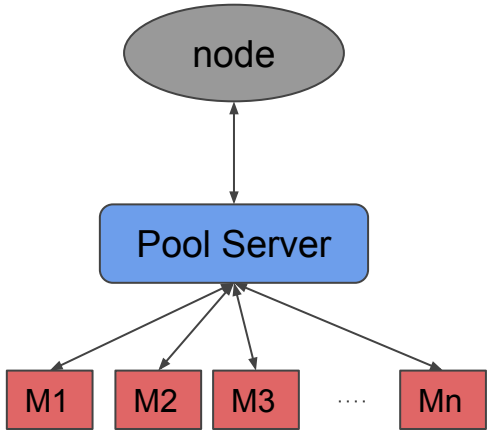
Mining Pools (18/04/2016)

- AntPool (28%)
- F2Pool (24.3%)
- BTCC Pool (13.4%)
- BitFury (9.8%)
- BW.COM (8.2%)
- Slush (5.2%)
- BitClub Network (4.3%)
- KnCMiner (4.3%)



Pool Mining

- Asking for work
  - JSON-RPC
    - `getwork` method/protocol (<v0.10.0)
      - 4Gh/s limit (nonce is 32bits = 4.2B iterations)
      - `rollntime` extension
    - `getblocktemplate` method/protocol (>v0.7.0)
      - flexible coinbase / extra nonce
      - easier to extend
  - Stratum protocol
    - uses `getblocktemplate`
    - uses TCP
    - easier to implement / debug



Pool Mining, cont.

- Pool rewards
  - based on shares
- Examples
  - Proportional
  - Pay Per Last N Shares (PPLNS)
  - Pay Per Share (PPS)
  - Shared Maximum Pay Per Share (SMPPS)
  - ESMPPS, RSMPPS, PPLNSG, POT, DMG, CPPSRB, Score
- Minus the pool fee

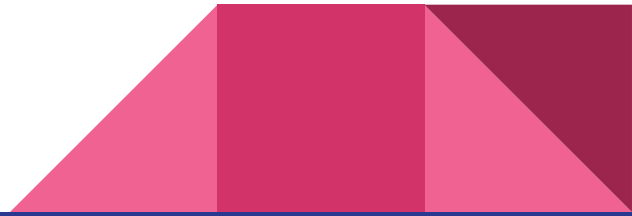
Profitability / ROI

- Several online calculators
  - https://bitcoinwisdom.com/bitcoin/calculator
- Example (18/04/2016)
  - Hashrate: 1.27 Eh/s --- Hashrate increase: 20%
  - Difficulty: 178,678,307,672
  - Electricity rate: 0.12 (Euro/kWh)
  - Pool fee: 0%
  - Hardware: 1 AntMiner S7 (~€650) -- 0.25W / 1Gh = 1225W
  - BTC Price: ~€390

Date	Difficulty	Revenue	Profit	Return
2016				-1.529
4-20 – 4-26 (7 days)	178 G	0.02149	0.02149	-1.508
4-27 – 5-9 (19 days)	214 G	0.01026	0.01026	-1.498
5-10 – 5-21 (32 days)	257 G	-0.01326	-0.01326	-1.511

Professional Mining

- Successful mining farms
  - Very large investments
  - Deals with hardware manufacturers
- Cheap cooling
  - Cold climates
  - …
- Cheap electricity



Questions?

Linkedin: https://www.linkedin.com/in/kkarasavvas
Twitter: @kkarasavvas
Email: kkarasavvas@gmail.com
Bitrated: https://www.bitrated.com/kostas