BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

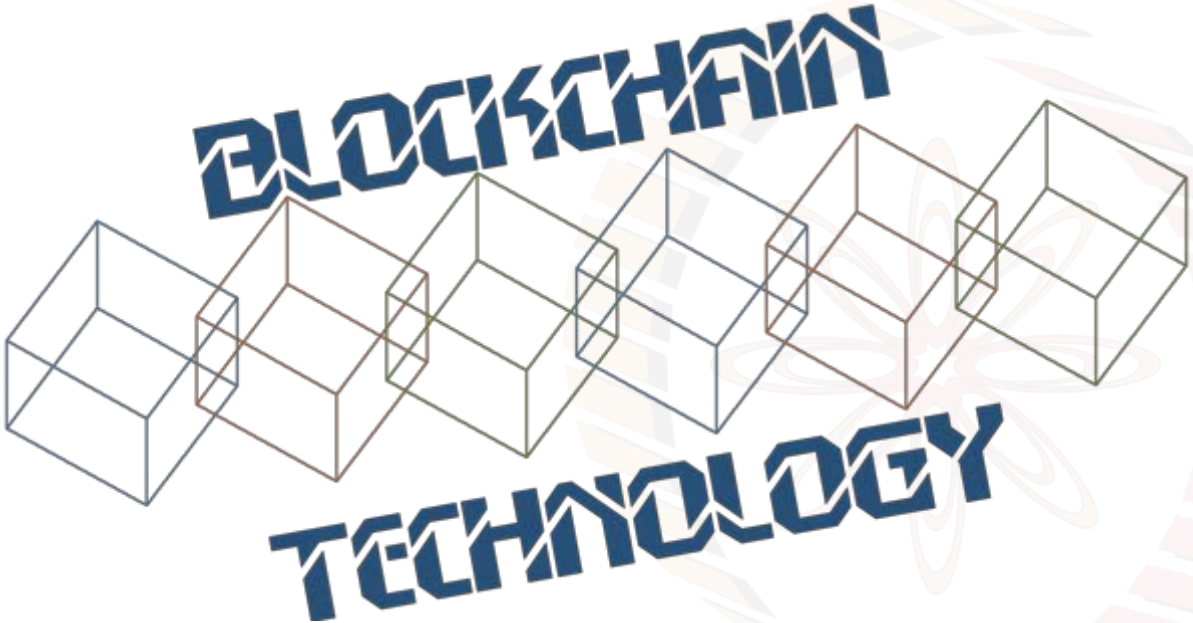


Image courtesy: http://beetfusion.com/

THE MINERS

The Life of a Miner

- Validate transactions and construct a block
- Use hash power to vote on consensus and commit transactions with a new block
- Store and broadcast the blockchain to the peers

Mining Bitcoins

- Join the network and listen for transactions – validate the proposed transactions
- Listen for new blocks – validate and re-broadcast a new block when it is proposed
- Collect transactions for a predefined time and construct a new block

Mining Bitcoins

- Find a nonce to make the new block valid
- Broadcast the new block – everybody accepts it if it is a part of the main chain
- Earn the reward for participating in the mining procedure

Mining Difficulty

- A measure of how difficult it is to fond a hash below a given target
  - Bitcoin network has a global block difficulty
  - Mining pools also have a pool-specific share difficulty

- The difficulty changes for every 2016 blocks
  - Desired rate – one block each 10 minutes
  - Two weeks to generate 2016 blocks
  - The change in difficulty is in proportion to the amount of time over or under two weeks the previous 2016 blocks took to find (en.bitcoin.it)

Setting the Difficulty

- Compute the following for every two weeks

```
current_difficulty = previous_difficulty *
      (2 weeks in milliseconds)/(milliseconds to
                                 mine last 2016 blocks)
```

Hash-rate versus Difficulty

- The hash is a random number between 0 and 2^{256}-1
  - To find a block, the hash must be less than a given target

- The offset for difficulty 1 is **`0xffff * 2^208`**

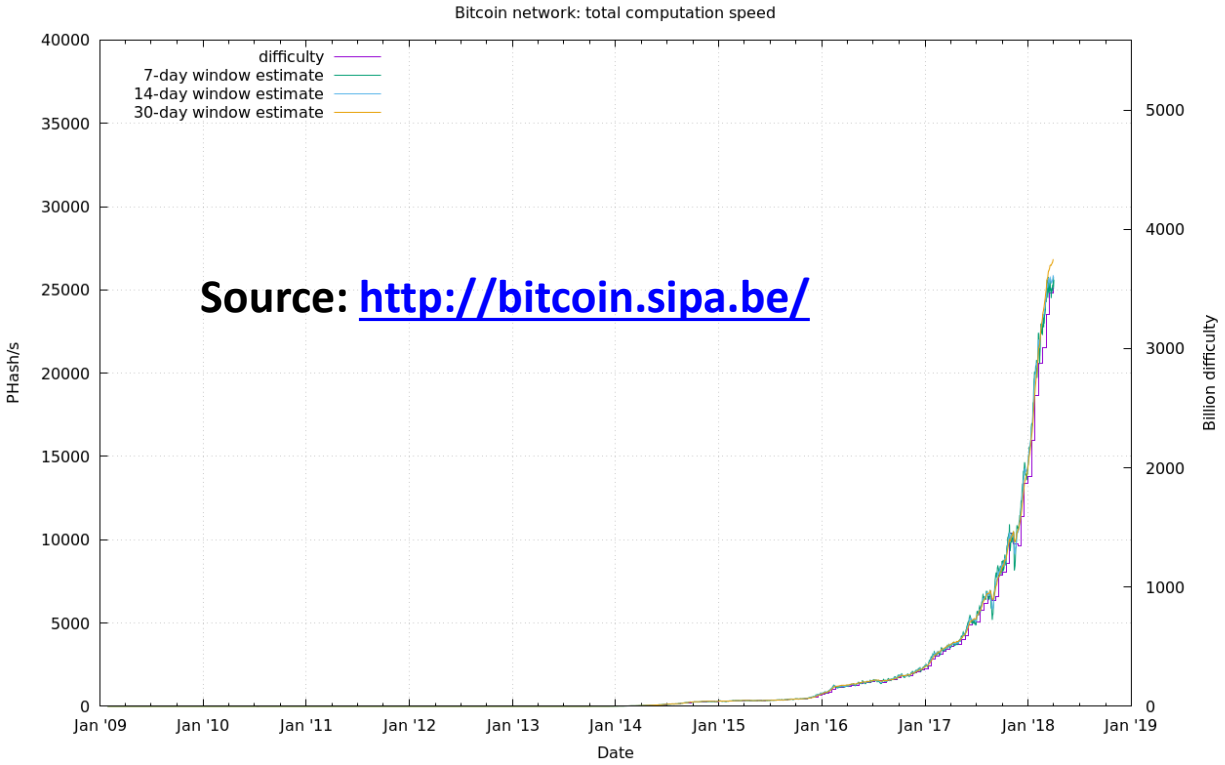
- The offset for difficulty D is **`0xffff * 2^208/D`**

- The expected number of hashes we need to calculate to find a block with difficulty D is **`(D * 2^256) / (0xffff * 2^208)`**

Mining Difficulty

- Current difficulty: 3511060552899.72 (as of 2nd April, 2018)
  - https://blockexplorer.com/api/status?q=getDifficulty

Mining Difficulty



Source: http://bitcoin.sipa.be/

Mining Hardware

- Specialized hardware
  - GPU
  - FPGA
- ASIC
  - Released in 2013
  - Fast computation of SHA256

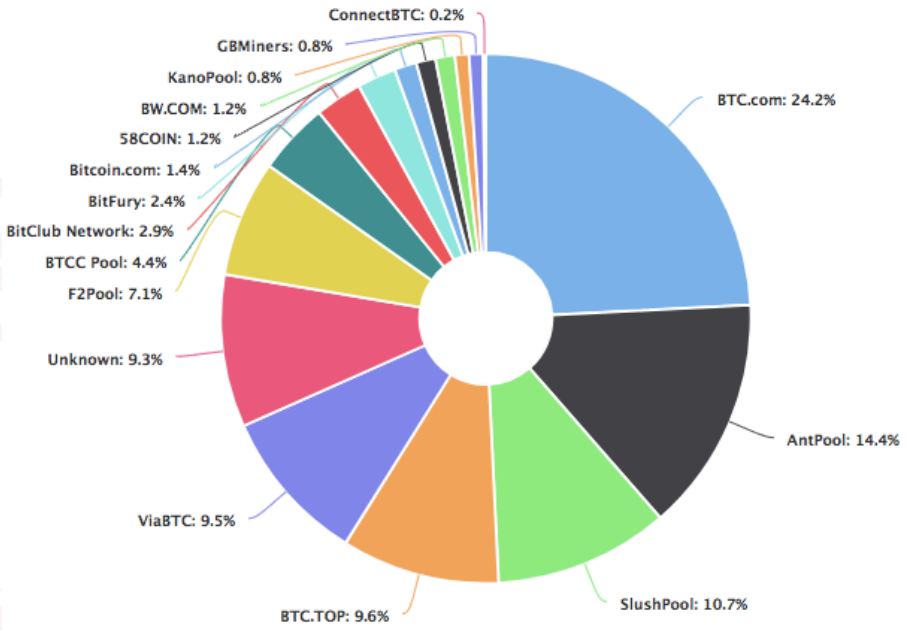
Image source:
https://steemkr.com/bitcoin/@pawank/bitcoin-mining

TerraMiner IV

- ASIC based bitcoin mining rig
- 2 Terahash per second
- Cost: USD 3500 approx

Mining Pool

- Pooling of resources by the miners
  - Share the processing power over a network to mine a new block
  - Split the reward proportionally to the amount of work they contributed



Hash-rate Distribution: blockchain.info

Mining Pool Methods

- Contains hundreds or thousands of miners through special protocols
- B: Block reward minus pool fee
- p: Probability of finding a block in a share attempt ($p = 1/D$), D is the block difficulty

Mining Pool Methods

- Pay per Share (PPS)
  - Instant guaranteed payout to a miner
  - Miners are paid from pool's existing balance, share of a miner is $R = B \times p$
  - Miners get almost equal payment, risk is at the pool operator

Mining Pool Methods

- Proportional
  - Miners earn share until the pool finds a block (end of mining round)
  - $R = B \times \frac{n}{N}$, where n is amount of his own share, and N is amount of all shares in the round
  - Payments are made once a pool finds out a block

Mining Pool Methods

- Pay per Last N Share (PPLNS)
  - Similar to proportional
  - Miner's reward is calculated on the basis of N last shares
  - Miners get more profit for a short round

Mining Pools – Pros and Cons

- Pros
  - Small miners can participate
  - Predictable mining
- Cons
  - Leads to centralization
  - Discourages miners for running complete mining procedure

Summary – Permissionless Blockchain and Bitcoin

- The permissionless or open model of blockchain – any user can join the network and participate in transactions
  - Bitcoin is developed on this principle

- The blockchain provides the backbone of the permissionless digital currency
  - Provides a decentralized architecture
  - Tamper-proof through hash-chain

- Miners ensures the consensus in the system

thank you!