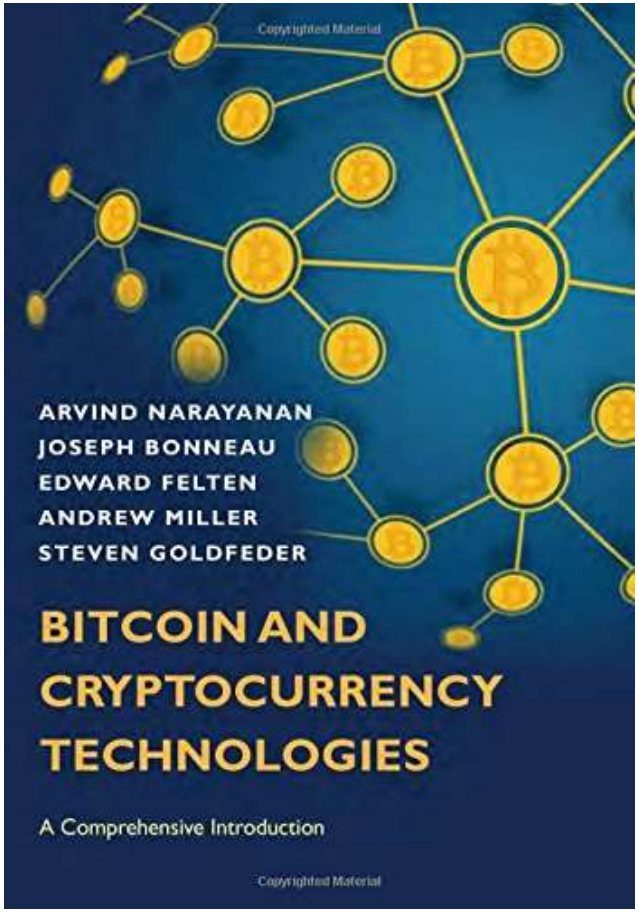
Blockchain
&
Business Application

Lecture :
Proof of Work
Mining

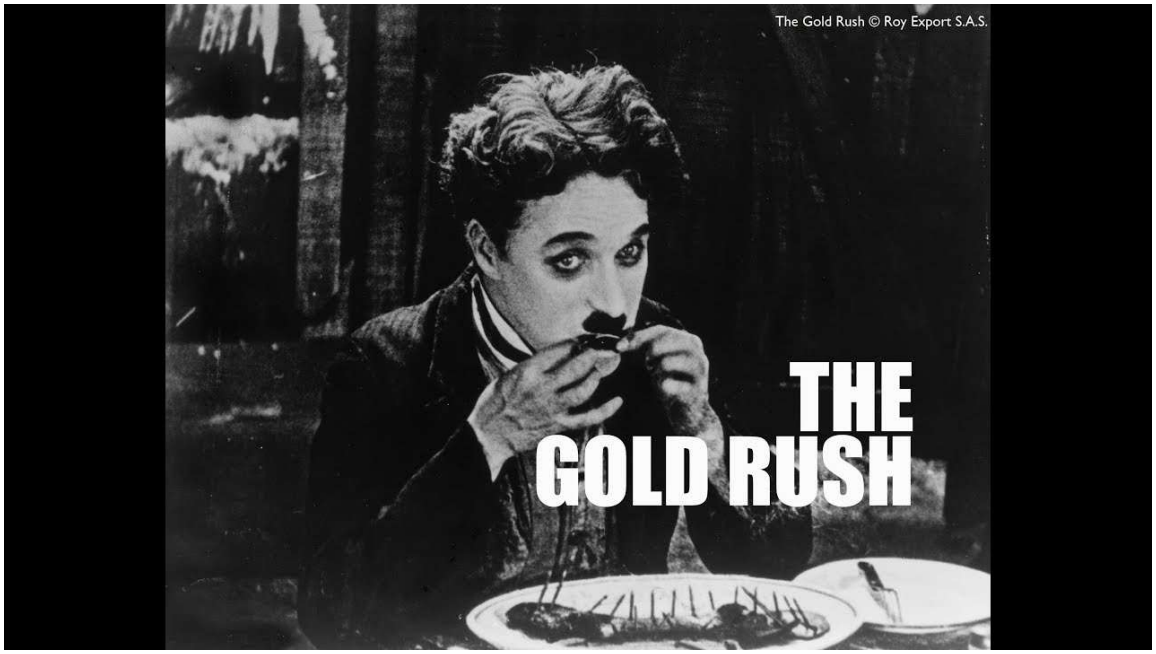
Chapter 5.1-5.4:Bitcoin Mining



Miners?

- They
  - validate transactions
  - build & store blocks
  - reach consensus on blocks,
  - and.. rewarded $ BTC $
- But
  - Who are they?
  - How they get into; how they operate
  - Business model?
  - Impact on the environment?

Please watch this movie before this chapter



Once connected to network, 6 tasks

1. Listen for transactions
2. Maintain blockchain & listen for new blocks
3. Assemble a candidate block
4. Find a nonce that makes your block valid
5. Hope your block is accepted
6. Profit $$$$ BTC $$$$ ☺

Once connected to network, 6 tasks

1. Listen for transactions
   - Listen on the network
   - Validate them
     - Check signatures
     - Outputs not spent before
2. Maintain blockchain & listen for new blocks
   - Ask other nodes all the historical blocks
   - Listen for new ones
   - Validate each block you receive

3. Assemble a candidate block
   - Validate each transaction
   - Group transactions to construct a block
4. Find a nonce that makes your block valid
   - Most work
   - Real difficulty for miners
5. Hope your block is accepted
6. Profit: Block reward:

   (2015) 25 BTC = 6.000$ + tr. Fee

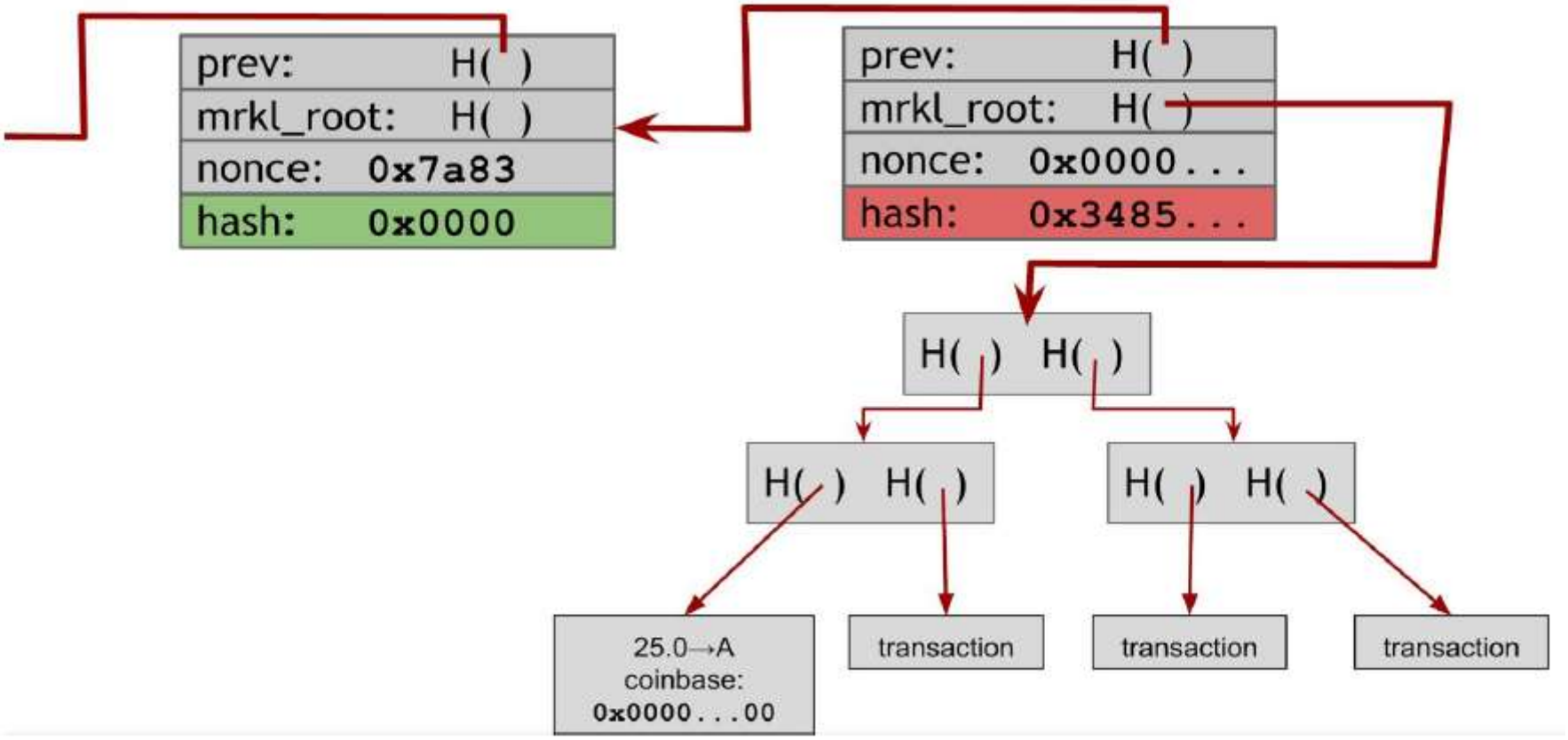
   (2019) 12,5 BTC x 9.300$ per coin = 120K $!!!

   (2021) 12,5 BTC x 50.000$ per coin = 625K $!!!

   The amount of the reward halves every 210,000 blocks = 4 years The amount is expected to hit zero around 2140.

Finding a valid nonce

- 32 bit nonce: block's hash to be under target



- Is everyone solving the same puzzle?
  - Faster miner always wins?
- No: Propagation, different transactions

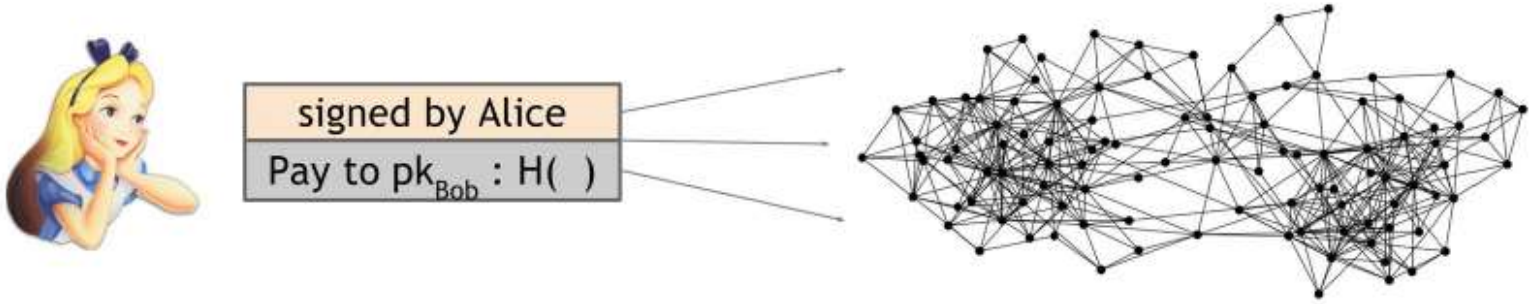


Figure 2.1 Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network.

Difficulty of finding a valid block

- March 2015, difficulty was:

  00000000000000172EC0000000000000000000000000000000000000 (hexadecimal)

  – Any valid hash: below this value

  – 1 on 2^{67}, huge number!

- Difficulty changes in every 2016 blocks

  – 1 block in 10 mins; 2016 blocks: 2 weeks!

  next_difficulty = (previous_difficulty * 2016 * 10 minutes) / (time to mine last 2016 blocks)

2014: ~150K TH/s

- Network grows, hardware faster, but difficulty increases → Next block always in 10 mins

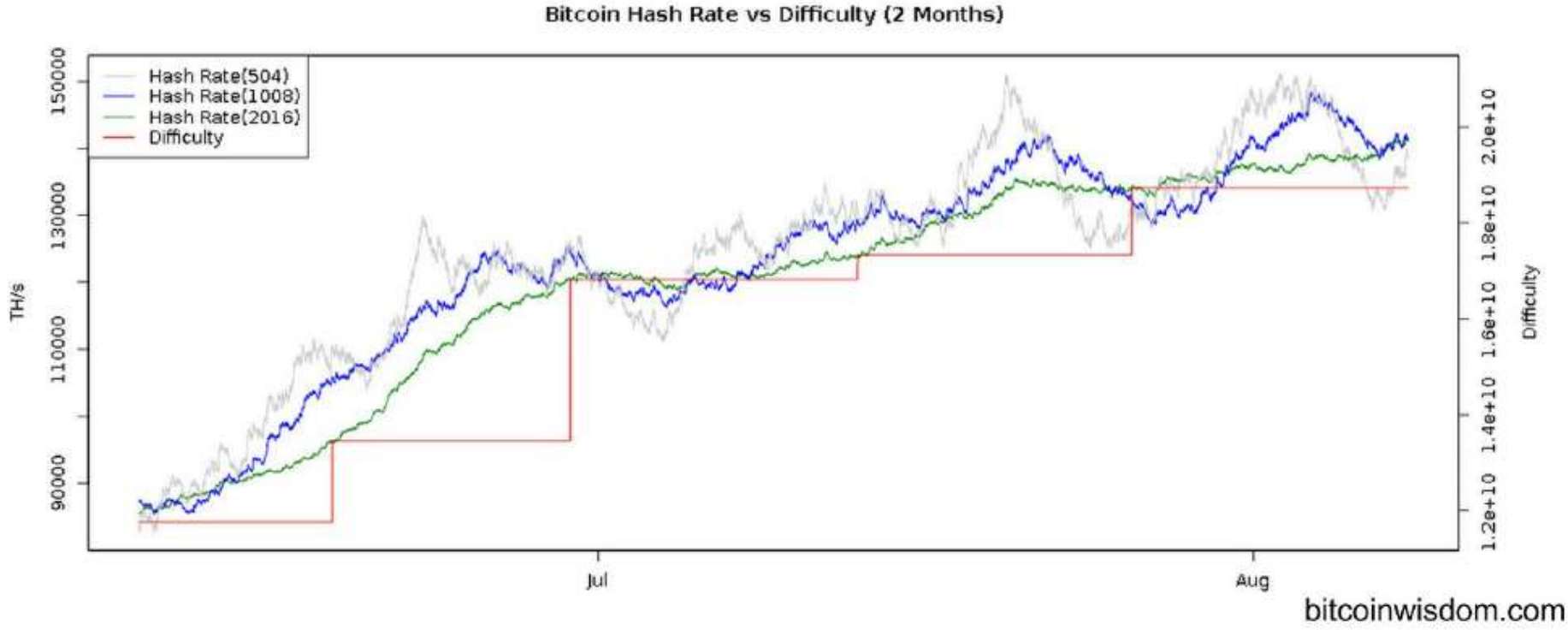
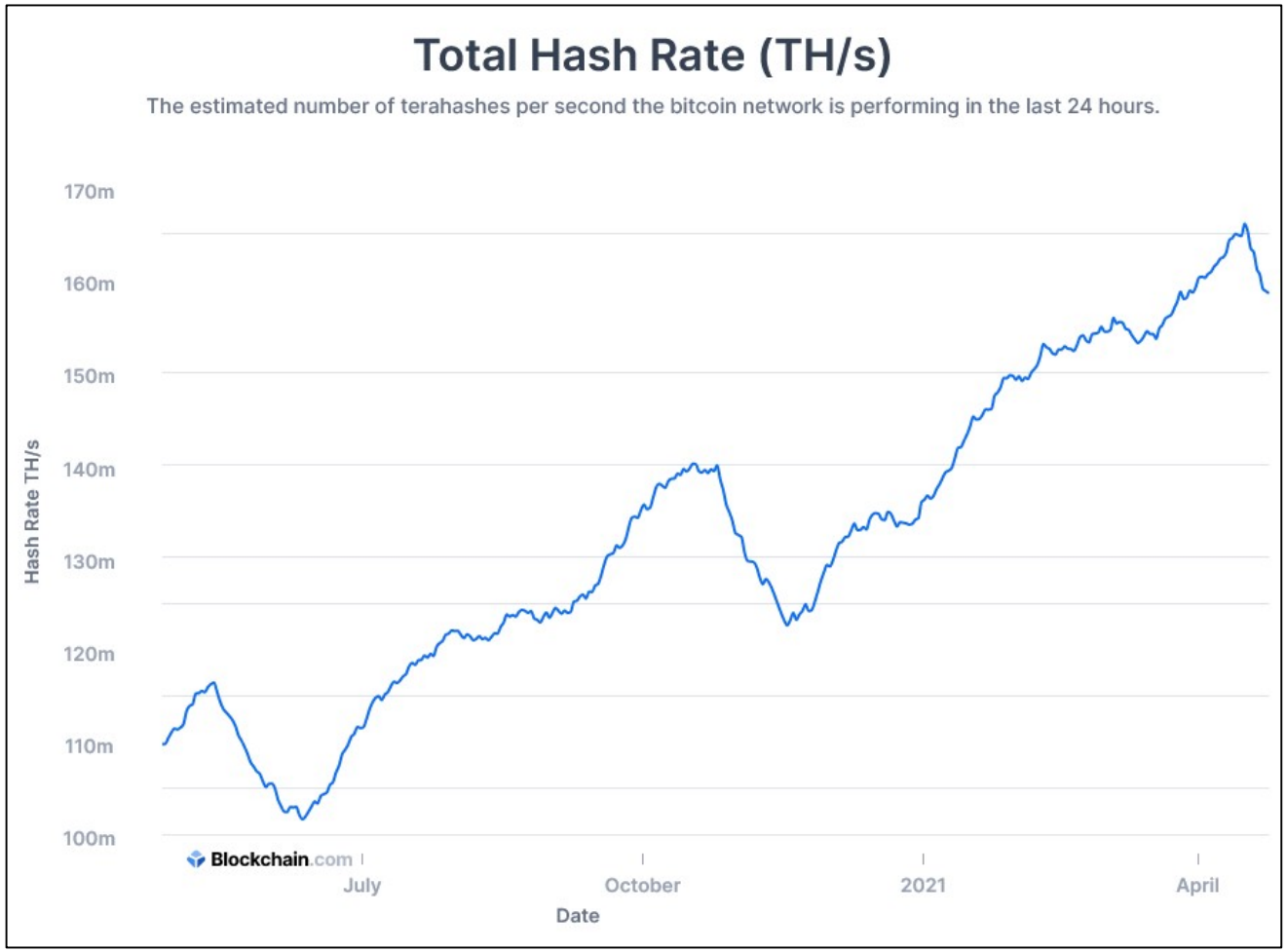


Figure 5.3: Mining difficulty over time (mid-2014). Note that the y-axis begins at 80,000 TH/s.

2021: ~150M TH/s



Mining Hardware

- Difficulty arises from SHA-256
  - SHA-256 comes from US National Security Agency
  - Will eventually become weak
    - Processors becoming faster
    - Quantum computers!
  - Yet still strong enough
- Why difficult → Technical detail

- Hardware for Mining:
  - CPU
  - GPU
  - FGPA
  - ASIC

CPU Mining

- First generation; general purpose computers
  - Search nonces linearly;
  - compute SHA-256;
  - Check if block valid

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

Figure 5.6 : CPU mining pseudocode.

CPU Mining, profitable?

- High-end PC 20 million hashes per sec (MH/s).
- Current difficulty level →

  Several hundred thousand years!!!

- Profitable?

GPU Mining

- Performance graphics processing
- 2010, OpenCL introduced for other tasks
- Bitcoin Mining easily parallelized:
  - Compute multiple hashes
  - Different nonces
- For amateurs, easily
  - Available
  - Set up
  - Overclocked!

GPU Mining

- Overclocking GPU
  - Run faster
  - Risk: Malfunction, overheat
  - For BTC Mining, profitable

  - Overclock for 50% faster → 1.5 times
  - Errors: 30% → 0.7 times correct
  - Product: 1.5 x 0.7 = 1.05; means 5% gain!

GPU Mining

- One PC with multiple GPU; Still early days

Figure 5.7: A home-built rack of GPUs used for Bitcoin mining. You can also see the fans that they used to build a primitive cooling system. Source: LeonardH, cryptocurrenciestalk.com.

GPU Mining

- Disadvantages
  - Floating points in videos, not needed in SHA256
  - Not designed for cooling several of them
- Gamers turned to miners
- Electricity & initial cost
- One good GPU: 200 MH/s
- Hundreds → 300 years for a block (625K$)
- Dead for Bitcoin, still alive for early altcoins

FPGA Mining

- “Field Programmable Gate Array”

Figure 5.8: A home-built rack of FPGAs. Although you don't see the cooling setup pictured here, a rack like this would need a cooling system.

FPGA Mining

- Field Programmable Gate Array
- Advantages
  - Customize for SHA-256
  - Easier systematic cool down
- One good FPGA: 1 GH/s (billion hashes / sec)
- Hundreds of FPGA → 50 years for a block ☹

ASIC Mining

- “Application-Specific Integrated Circuits”
- Designed & Optimized specifically for mining
- Requires expertise & time
- Early times < 2015, race condition (shipping)

- You can start mining and earning
- Yet not profitable (price, electricity, cooling)

Today: Professional Mining

- Obtain new ASIC not available to public

Figure 5.9: BitFury mining center, a professional mining center in the republic of Georgia.

Setting up a mining center

- 3 biggest considerations:
  - Climate
  - Cost of electricity
  - network speed

- Georgia & Iceland are popular

Similarities & Evolution

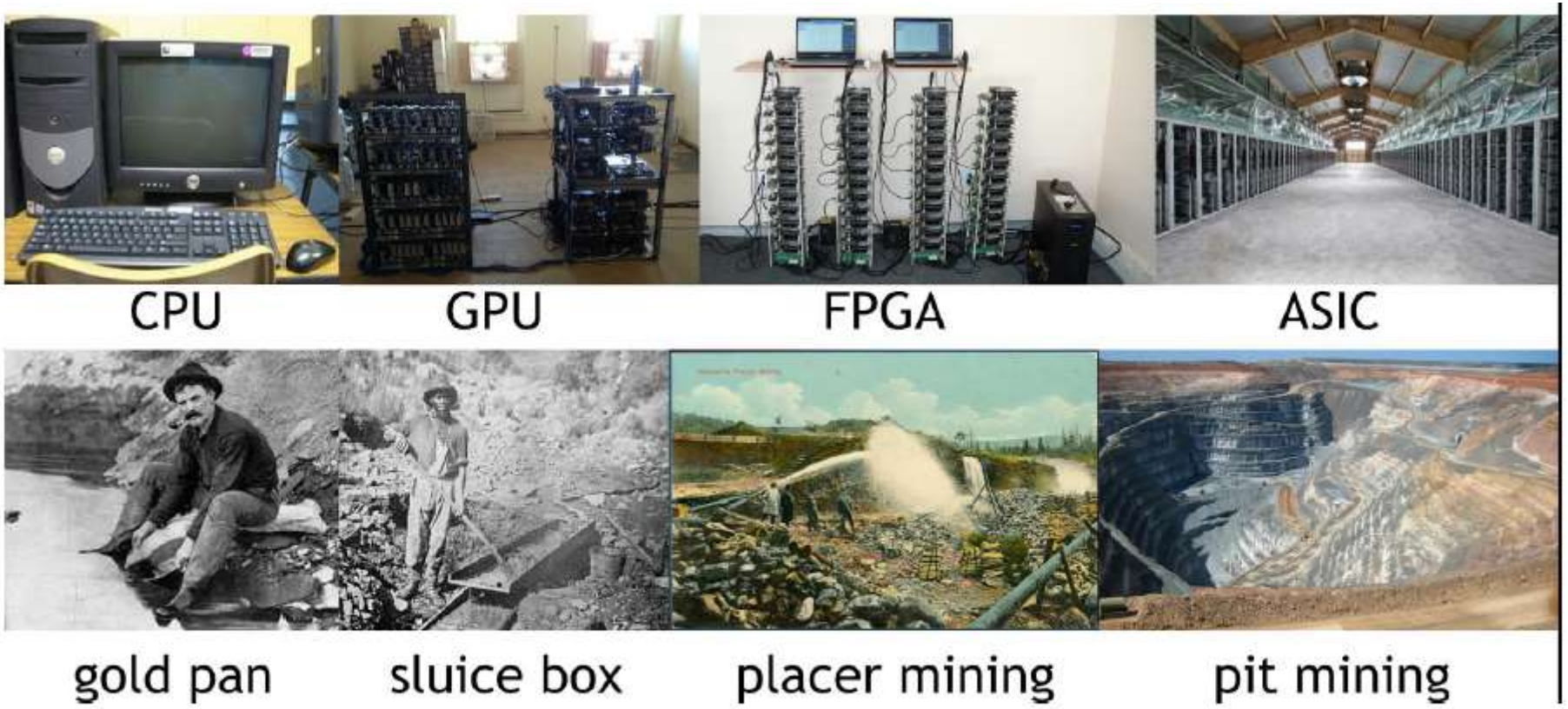


Figure 5.10: Evolution of mining. We can see a clear parallel between the evolution of Bitcoin mining and the evolution of gold mining. Both were initially friendly to individuals and over time became massive operations controlled by large companies.

Future?

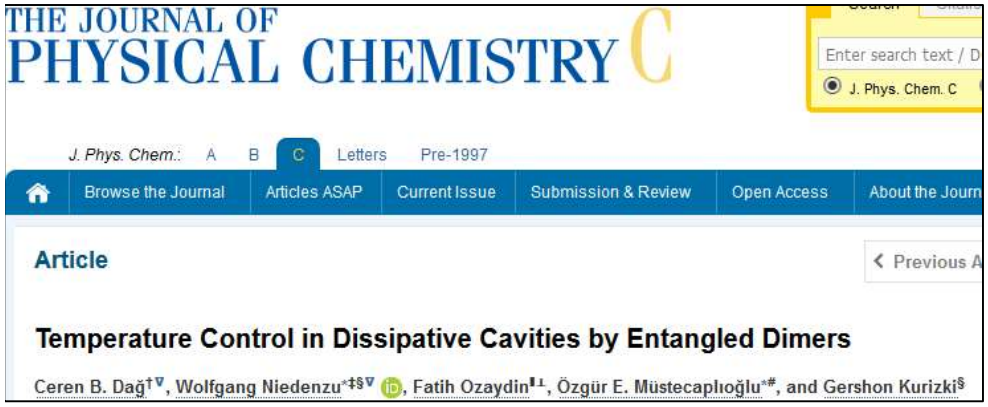
- Only ASICS & Professional miners?
- What about individuals
  - How to incorporate them?
- Violating decentralization?
- A method for only individuals?

- Altcoins?

One of my current projects:
Quantum Fuels for Space Applications

cost
EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

CA COST Action CA15220
Quantum Technologies in Space


THE JOURNAL OF PHYSICAL CHEMISTRY C

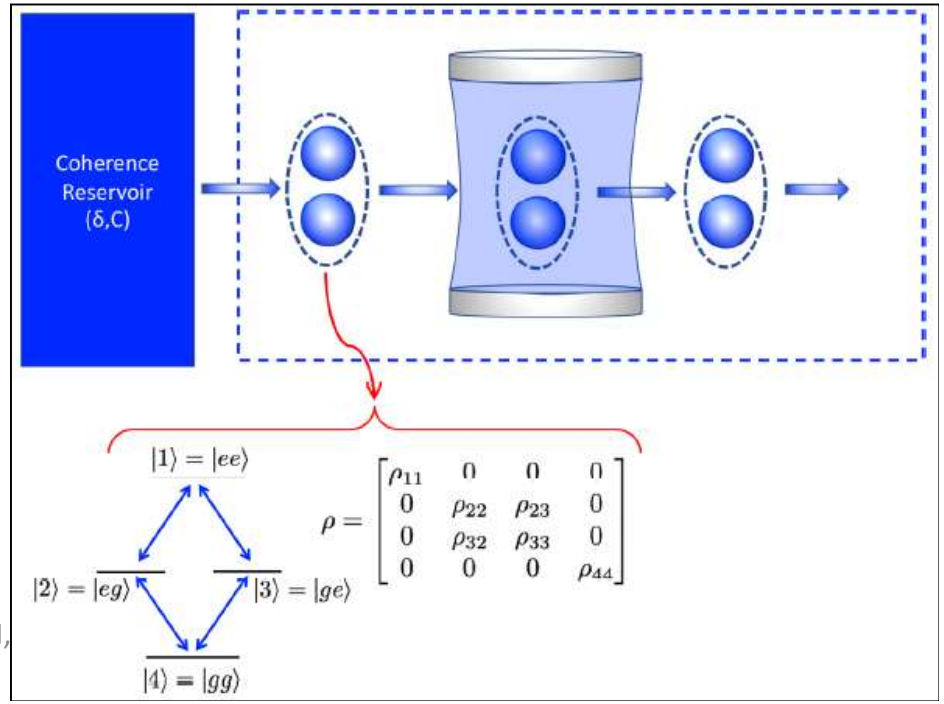
J. Phys. Chem.: A B C Letters Pre-1997

Browse the Journal | Articles ASAP | Current Issue | Submission & Review | Open Access | About the Journ

Article

Temperature Control in Dissipative Cavities by Entangled Dimers

Ceren B. Dağ, Wolfgang Niedenzu, Fatih Ozaydin, Özgür E. Müstecaplıoğlu, and Gershon Kurizki



Energy consumption and ecology

- “Information is physical”
- Thermodynamics limit
- *Landauer’s principle* (1960s)
  - *“any non-reversible computation must use a minimum amount of energy”*
  - Not that optimized yet but a hard lower limit
  - Erasing information.. Logical operations?
  - SHA-256 is irreversible
  - *Reversible computation?*

How does Bitcoin mining use energy?

- Embodied energy
  - Manufacturing: Raw materials → ASIC; Shipping?
  - May go down in future
- Electricity
  - Circuits: Going down (optimization, efficiency)
  - Landauer's principle, forever there!
- Cooling
  - Gets worse by scale

How to estimate energy consumption

- Small dams: 10 MW
- Typical Dam: 1000 MW
- Typical Nuclear PP: 4000 MW
- Largest Nuclear PP: 7000 MW (Japan)
- Largest dam 10.000 MW (China)

How to estimate energy consumption

- Top-down approach
  - Each block found: 25 BTC = 6,500 $
  - 10 dollars / second
  - If all spent on electricity (upper bound)
  - 350 MW, in 2014

  - Block rate almost constant but difficulty increases

How to estimate energy consumption

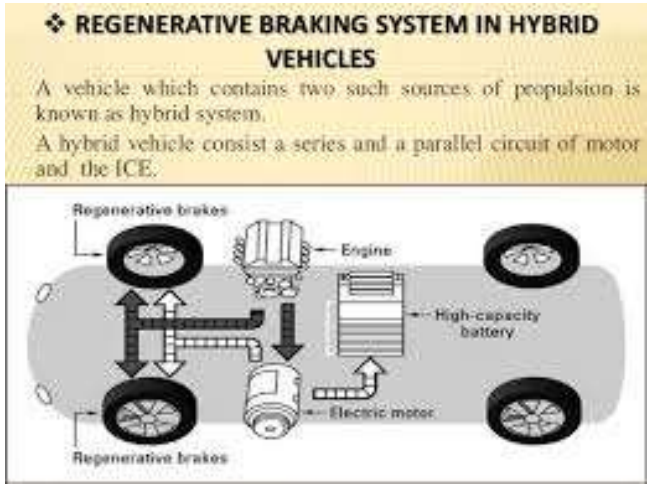
- Bottom-up approach
  - Most efficient ASIC: 3 GHashes / Watt
  - Total Hash Rate 350 Million Giga Hashes / sec
  - (3 GH/W)x(350 M G H/s) = 120 MW
  - Just computation;
  - Add Manufacturing & Cooling

Bitcoin: Waste of Energy?

- Computing SHA-256, only for Bitcoin
- Unauthorized cost
- Energy Harvesting?
  - Bitcoin Prius ☺

- Opportunity Cost
  - Any method for “currency/payment” consumes
  - ATMs, Banks..

Repurposing energy?



- Data Furnace:
  - Instead of buying a heater, buy a Mining Kit
  - Efficiency similar
  - Complexity similar

Drawbacks of Repurposing

- Electric Heaters not efficient (as gas heaters)
- During summer?
- Ownership not clear
  - Who takes coin rewards?
  - Digital Rights Management (DRM) Battles?

Turning electricity in cash

- Providing free or low-cost electricity is open to new forms of abuse
- Governments subsidize industrial electricity
- Free electricity outlets everywhere!

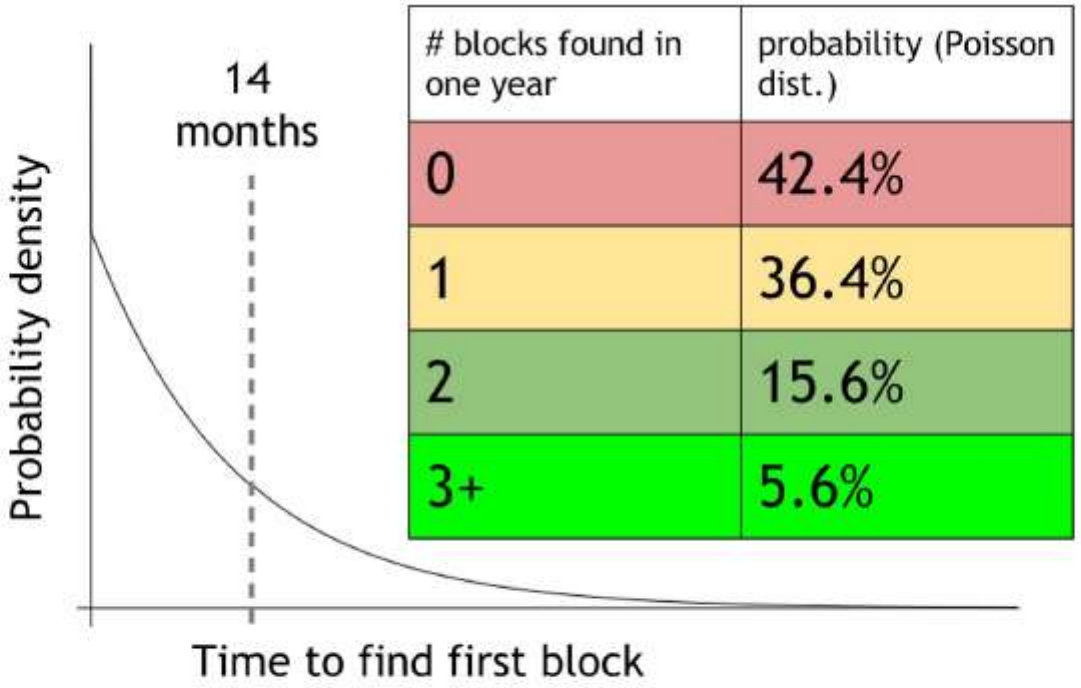
Mining Pools

- Consider the economics
  - Individual attempts
  - Initial Cost vs. Reward in every 14 months?
  - Add electricity & cooling costs;
  - Prefer a check every month?

  - Mining is random

- Blocks found in the first year:
  - Variance: High
  - Expected number: Low
  - Poisson Distribution

  - If expectance: 1 Block in 14 months
  - → 40% chance you won't find another same year
  - Actual chance: 36% in the first year: Too bad



# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

Figure 5.11: Illustration of uncertainty in mining. Assuming that the global hash rate is constant and the mean time to find a block is 14 months, the variance for a small miner is quite high.

- Mutual Insurance companies to lower the risk
  - e.g. Farmers
- Mining Pools
  - Individuals get together in a pool
  - Pool manager receives all rewards to share among
  - How to share just? Who worked harder?

Mining Shares

- Elegant solution: Miners can prove probabilistically how much they worked
- By **outputting** shares , or near-valid blocks.
  - e.g. target number beginning with 67 zeros.
  - Miners find hashes with less zeros (but they find)

Figure 5.12: Mining Shares. Miners continually try to find blocks with a hash below the target.

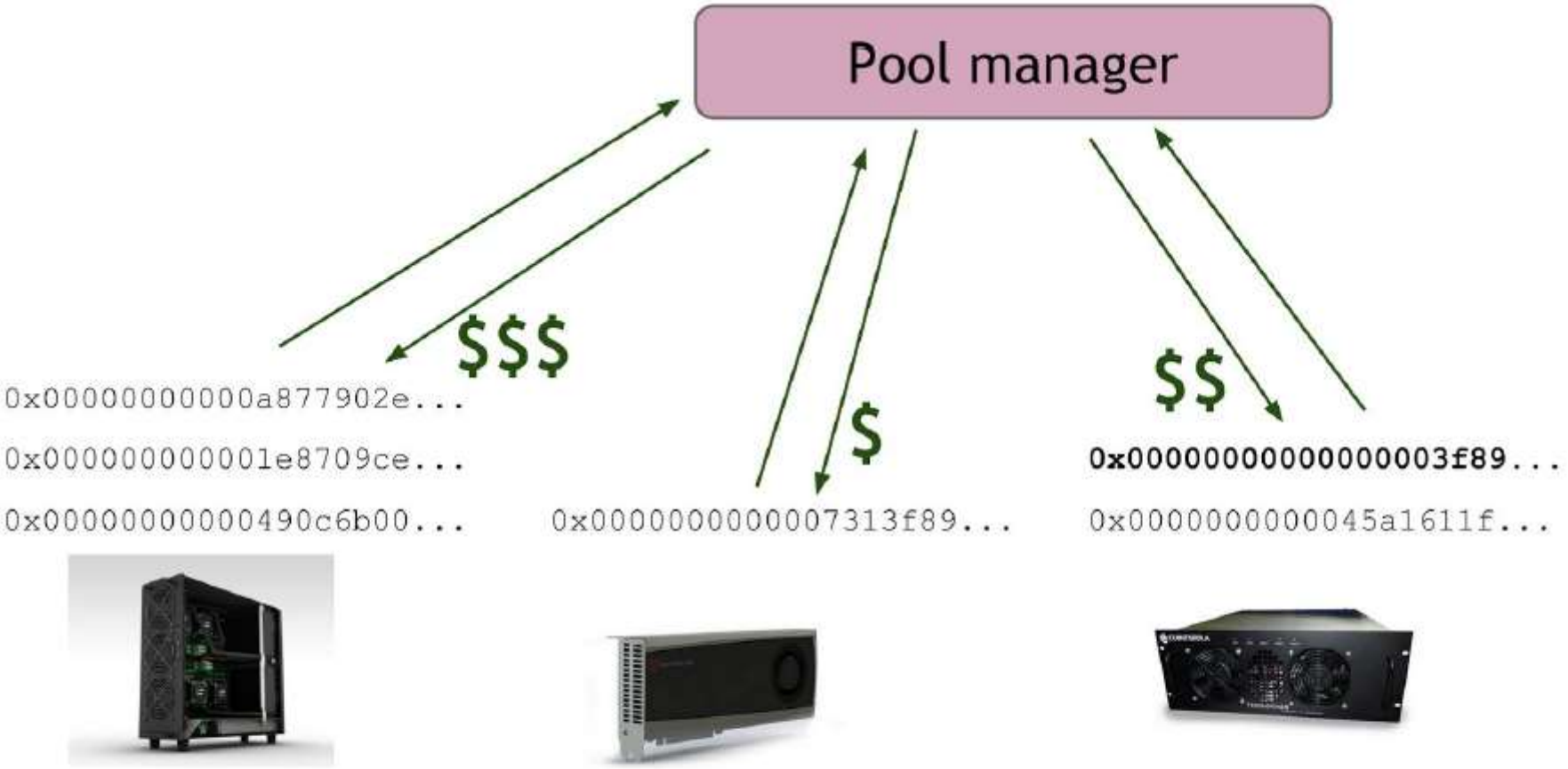


Figure 5.13: Mining rewards. Three participants pictured here are all working on the same block. They are awarded commensurate with the amount of work done. Even though the miner on the right was the one to find the valid block, the miner on the left is paid more since this miner did more work. There is (typically) no bonus paid to the miner who actually finds the block.

Pay per Share

- Manager pays to each miner when they share
  - Does not wait for a valid block
  - Manager absorbs the risk → Takes more
  - May look the best
- Problems
  - Miners may not share valid blocks → Big loss to all
  - What if manager is malicious? Can attack the pool

Proportional

- Whenever a valid block is found
- Reward is shared proportionally wrt work
- To measure each miner’s work
  - Advanced techniques
  - More work

Pool Hopping

- Miners may wish to switch betweens pools
  - From purely proportional in the early cycles
  - To Pay-per-share in the later cycles
- An open problem
- 51% Concern !

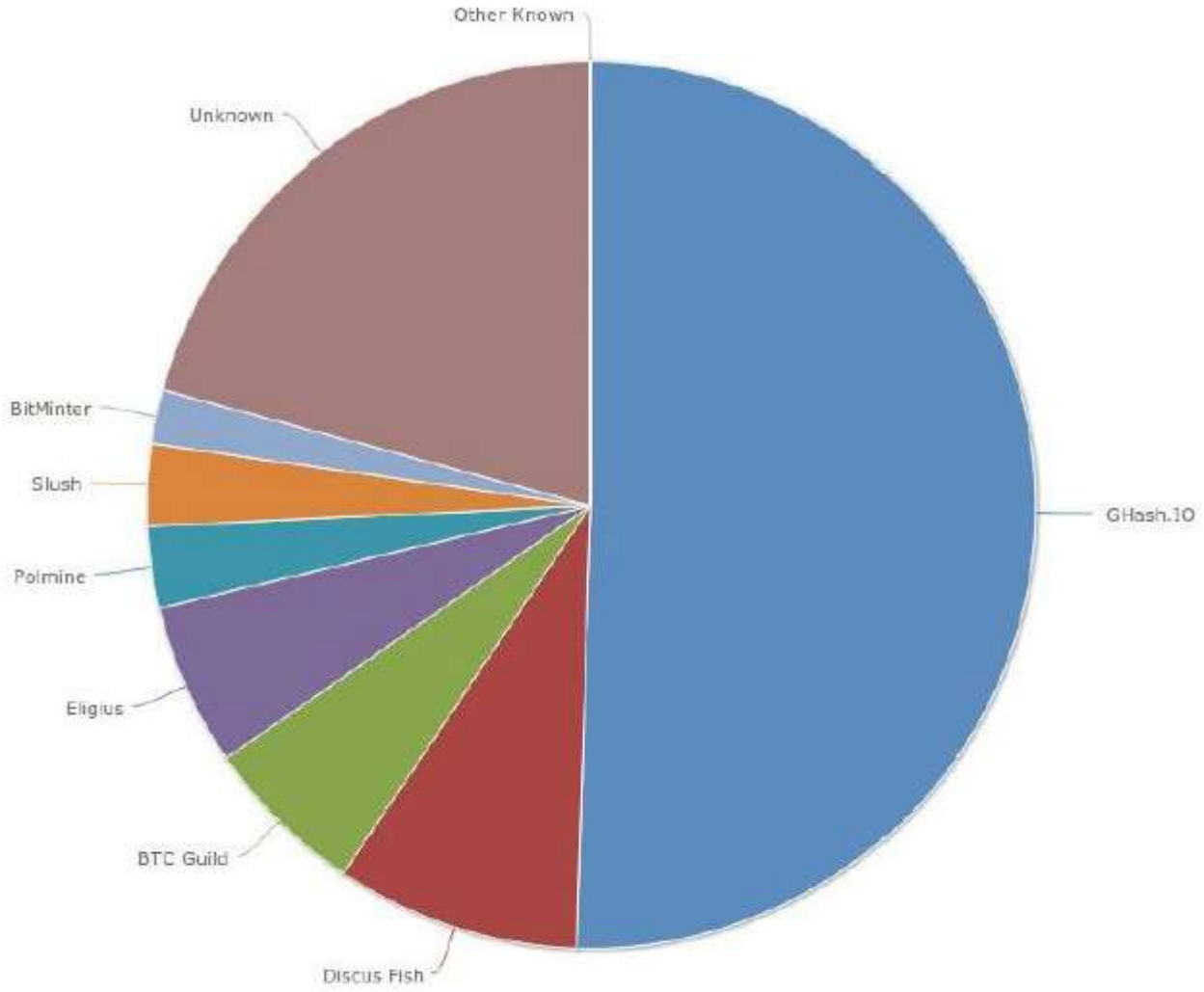


Figure 5.14 (a) Hash power by mining pool, via blockchain.info (June 2014)

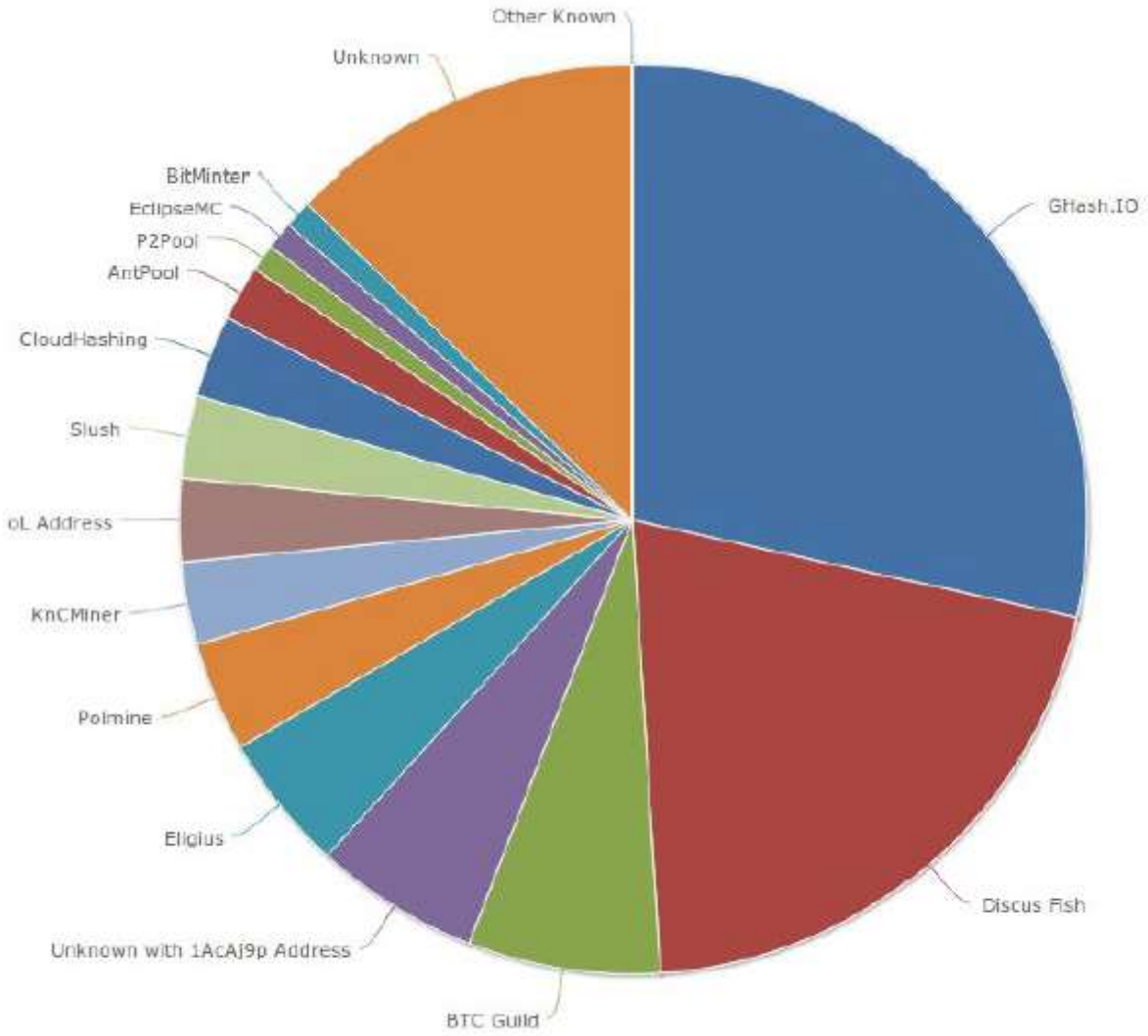


Figure 5.14 (b) Hash power by mining pool, via blockchain.info (August 2014)

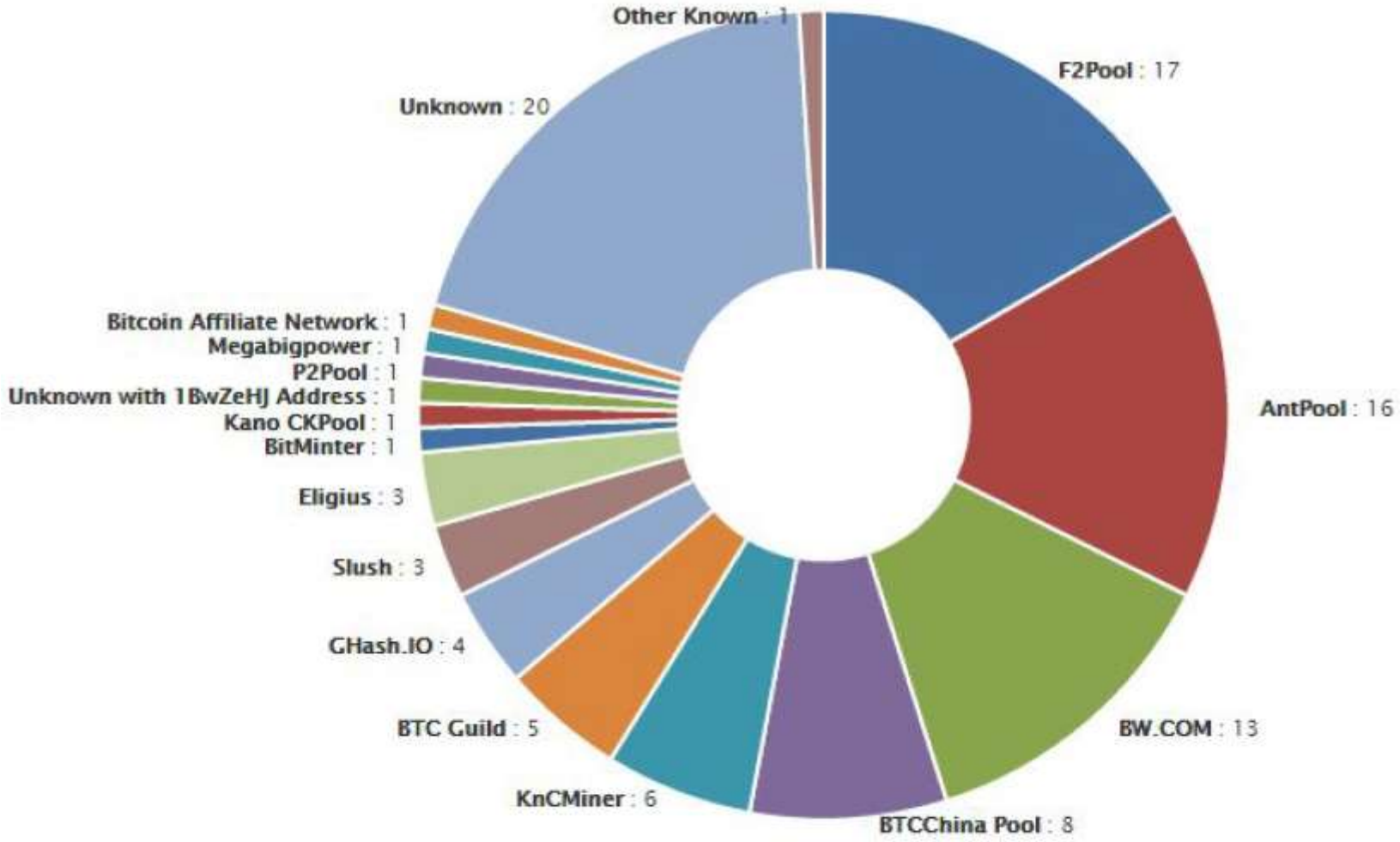


Figure 5.14 (c) Hash power by mining pool, via blockchain.info (April 2015)

Are Mining Pools a Good Thing?

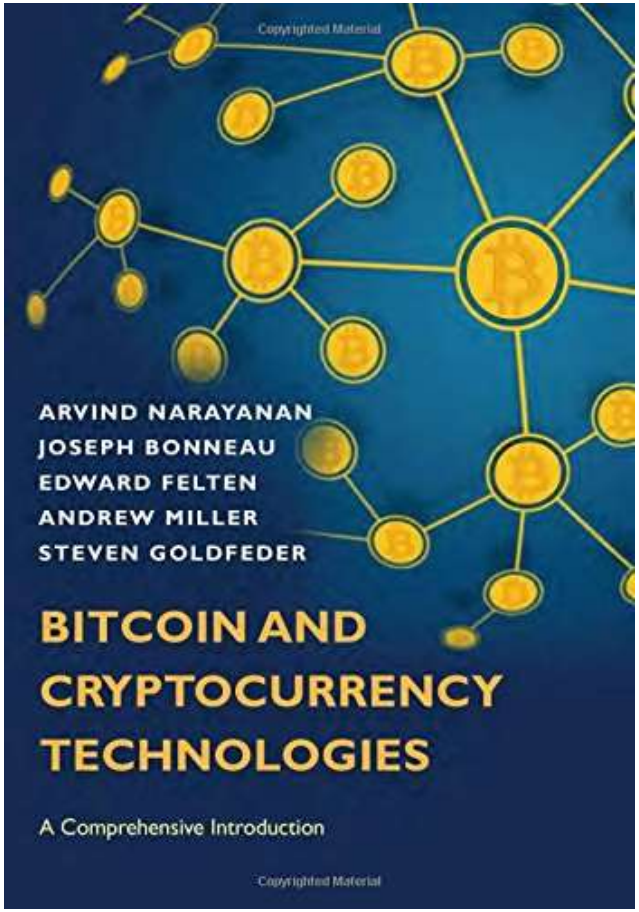
- Advantages
  - Lower variance, higher profit predictability
  - Required for small miners
  - One central manager assembling the blocks
  - Easier system upgrade

Are Mining Pools a Good Thing?

- Disadvantages
  - Centralization!
  - Leaving the pool?
    - In theory OK, in practice?
  - Lowers number of miners running full validation

- Redesigning the Pool Mechanism?

Chapter 5.5: Bitcoin Incentives & Strageties, Mining Attacks



MIT Technology Review

Blockchain / Smart Contracts

Once hailed as unhackable, blockchains are now getting hacked

More and more security holes are appearing in cryptocurrency and smart contract platforms, and some are fundamental to the way they were built.

by **Mike Orcutt** Feb 19, 2019

Early last month, the security team at Coinbase noticed something strange going on in Ethereum Classic, one of the cryptocurrencies people can buy and sell using Coinbase's popular exchange platform. Its blockchain, the history of all its transactions, was under attack.

Blockchain Mar 26

Nearly all Bitcoin trades are fake, apparently

There have been suspicions for a while that the markets are overinflated. In fact, fears of market manipulation have held up regulatory approval for a number of proposed Bitcoin exchange-traded funds (ETFs), frustrating many enthusiasts who believe that the eventual approval of ETFs will spur broader adoption of the technology by investors.

Incentives & Strategies

- So far:
  - Mechanisms,
  - Electricity,
  - Pools, etc

- What about strategies?
  - Which blocks to work on?

Strategies for each miner

- Which transactions to include.
  - The default strategy is to include any transaction which includes a transaction fee higher than some minimum.
- Which block to mine on.
  - The default behavior: extend the longest known valid chain.

- Choosing between blocks at the same height
  - If two different blocks are mined and announced at around the same time, it results in a 1-block fork.
  - The default behavior is to build on top of the block that they heard about first.
- When to announce new blocks.
  - When they find a block, miners have to decide when to announce this to the Bitcoin network.
  - The default behavior is to announce it immediately, but they can choose to wait some time before announcing it.

Forking Attack

Assumption: A non-default miner with mining power: α

- The miner sends some money to a victim, Bob, in payment for some good or service.
- Bob waits and sees that the transaction paying him has indeed been included in the block chain.
- Perhaps he follows the common heuristic and even waits for six confirmations to be sure.
- Convinced that he has been paid, Bob ships the good or performs the service.

Forking Attack

- The miner now goes ahead and begins working on an earlier block
  - Before block that contains the transaction to Bob.
- In this forked chain, the miner inserts an alternate transaction — or a double spend
  - which sends the coins paid to Bob on the main chain back to one of the miner's own addresses.

Forking Attack

- For the attack to succeed, the forked chain must overtake the current longest chain.
- Once this occurs, the transaction paying Bob no longer exists on the consensus block chain.
- This will surely happen eventually if the attacking miner has a majority of the hash power: $\alpha > 0.5$
- Since the miner's coins have already been spent (on the new consensus chain), the transaction paying Bob can no longer make its way onto the blockchain

Forking Attack

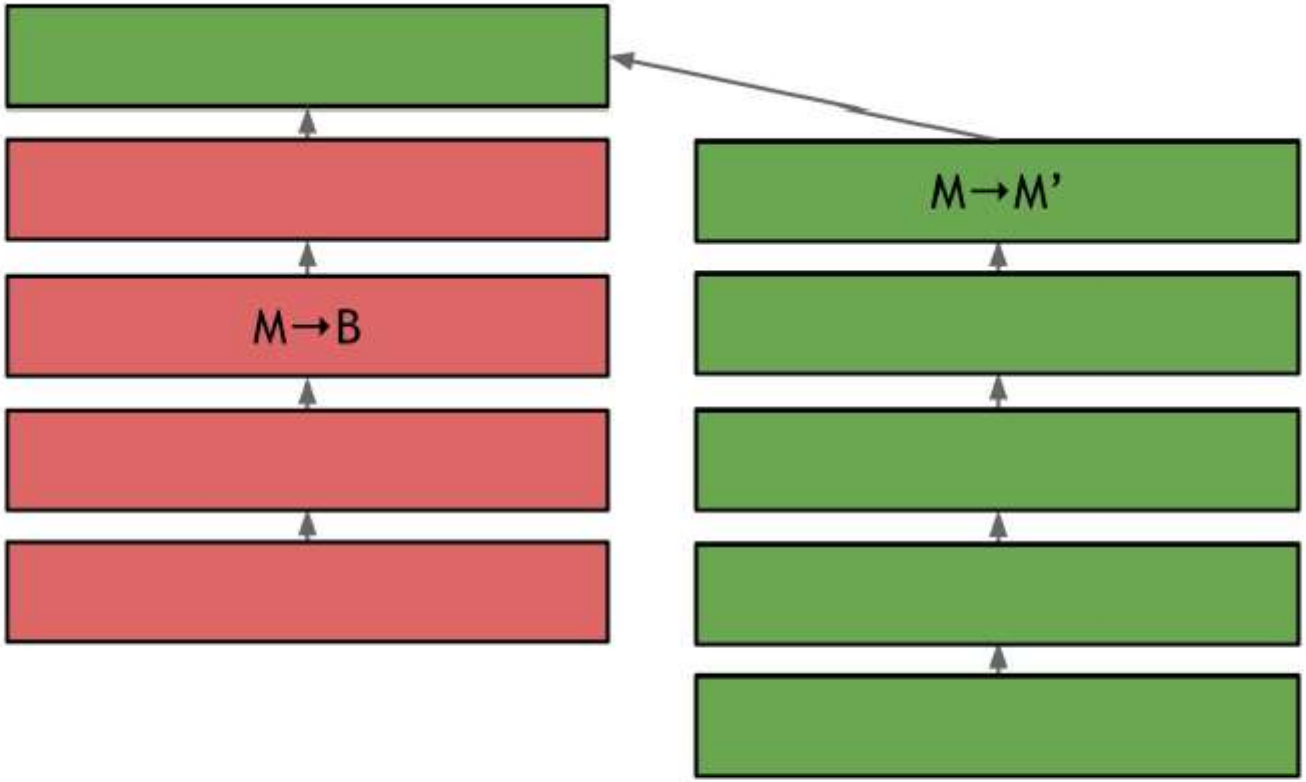


Figure 5.15 Forking attack. A malicious miner sends a transaction to Bob and receives some good or service in exchange for it. The miner then forks the block chain to create a longer branch containing a conflicting transaction. The payment to Bob will be invalid in this new consensus chain.

Is 51% necessary?

- Forking attack is certainly possible if $\alpha > 0.5$
  - Even less power works: Network delays overheads
- Exceeding 50% percent makes it faster
- Historically called 51% attackers

- **Practical countermeasures:** It's not clear whether a forking attack would actually work:
  - The attack is detectable,
  - community would decide to block the attack
  - by refusing to accept the alternate chain even though it is longer

- **Attacks and the exchange rate.**
  - More importantly, it's likely that such an attack would completely crash the Bitcoin exchange rate

- Attacker gains small in short term
- But destroys the system
  - *"Goldfinger Attack"*

Reading Assignments

- Bitcoin and the age of bespoke Silicon
- Analysis of Large-Scale Bitcoin Mining Operations
- Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
- Analysis of bitcoin pooled mining reward systems
- Majority is not enough: Bitcoin mining is vulnerable
- The economics of Bitcoin mining, or Bitcoin in the presence of adversaries
- The Miner's Dilemma