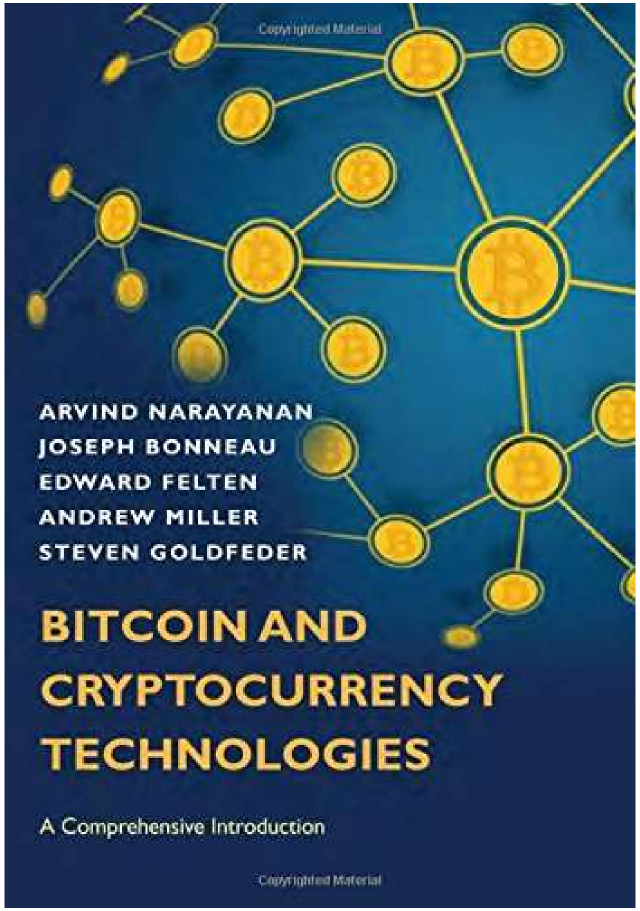
Blockchain
&
Business Application

Lecture:

Alternative Mining Puzzles

Chapter 8


Copyrighted Material
ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER
BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES
A Comprehensive Introduction
Copyrighted Material

- Mining Puzzles
- Control the Consensus Process
- Profit
  - Help solving, not only network maintenance

- Modifying/Designing puzzles!

Puzzle Requirements

- Secure?
- Difficult to solve, easy to verify
- Adjustable difficulty

(From Mining Chapter)

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

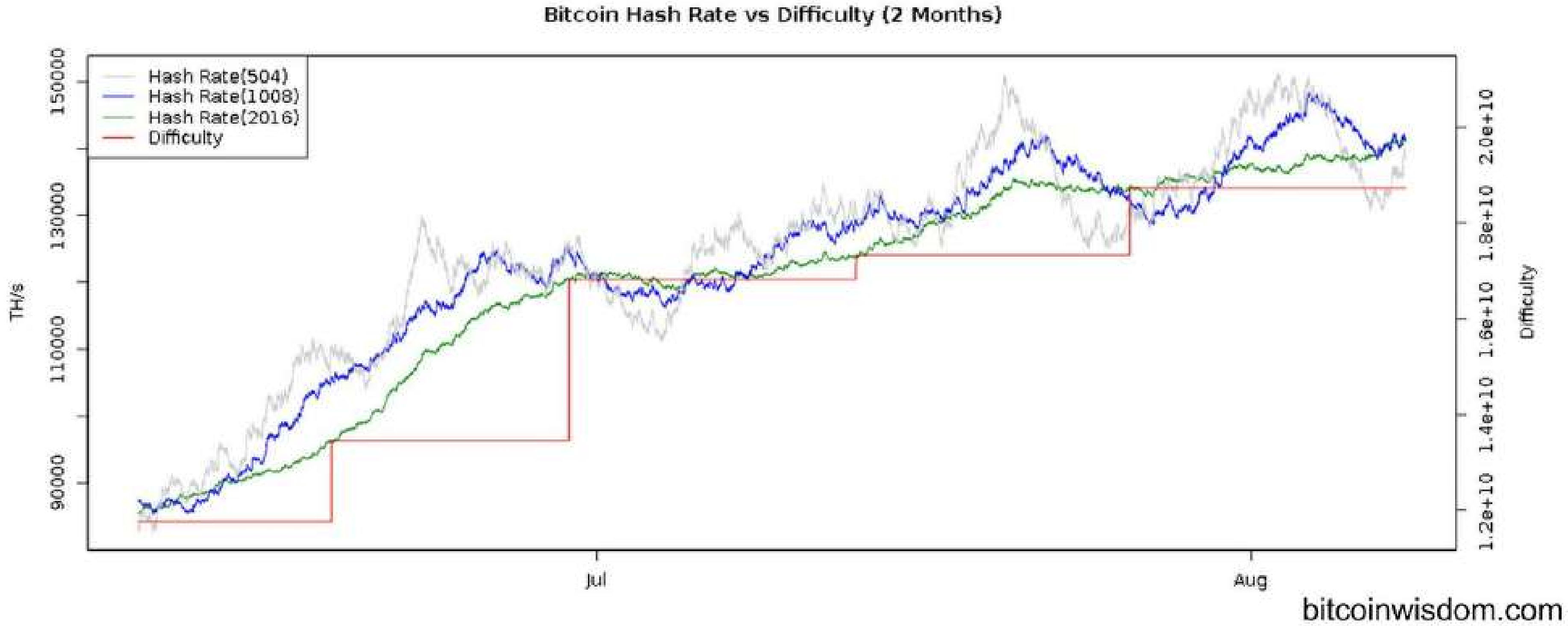


Figure 5.3: Mining difficulty over time (mid-2014). Note that the y-axis begins at 80,000 TH/s.

What is Bitcoin Puzzle?

- “Partial hash-preimage puzzle”
- Goal:
  – to find preimgs for partially specified hash output
  – namely, an output below a certain target value

- SHA-256 hash based puzzle satisfies both
  – Adjustable difficulty
  – Verification (checking solutions) trivial

Additional Requirement

- Progress-freeness:
  - Chance of winning: Only roughly proportional to hash-power
  - Small miners also should have some chance (r.p.)
  - Otherwise, no small/starters would join
  - Trial&Error
  - No reward for past efforts *(don't confuse pools)*
  - Mathematically: Memoryless

- SHA-256 hash based puzzle satisfies all three
  - Adjustable difficulty
  - Fast verification
  - Progress-free

- Transition
  - From “one-CPU-one-vote”
  - To powerful minority

ASIC Resistance

- Ideal Case
  - Each “computer” shall have equal power
  - Even recent CPU’s are optimized for cryptography
  - Can require to be a traditional computer? NO.

- Modest Case
  - Reduce the ASIC-CPU gap
  - Allow ASICs be more efficient only one order
  - Let everyone join the game

“But the Memory Remains”

- Processor technology
  - Improving fast
  - Costly
- Memory: slow progres, cheap

- Memory-bound
  - Memory access time dominates the total time
- Memory-hard
  - Require large memories
- We would require both memory-bound&hard

- SHA-256
  - Requires only 256 bits (fits to CPU registers)
- Scrypt
  - The most popular memory-hard puzzle
  - Used in Litecoin and some other altcoins
  - Already used for password-hashing; *why?*

Memory turns $O(N^2)$ to $O(N)$

Figure 8.1: Scrypt pseudocode

```
def scrypt(N, seed):
    V = [0] * N  // initialize memory buffer of length N

  // Fill up memory buffer with pseudorandom data
  V[0] = seed
  for i = 1 to N:
     V[i] = SHA-256(V[i-1])

  // Access memory buffer in a pseudorandom order
  X = SHA-256(V[N-1])
  for i = 1 to N:
     j = X % N  // Choose a random index based on X
     X = SHA-256(X ^ V[j]) // Update X based on this index

  return X
```

- Having a memory of N/k
- Compute (k+3) N/2

- Halving memory requirement:
  - k$\rightarrow$2k
  - Computations: 4N/2 $\rightarrow$ 5N/2

- Memory $\rightarrow$ Zero, if k$\rightarrow$N
  - Computations: 2N $\rightarrow$ (N+3) N/2 = $O(N^2)$

Additional Limitation of *Scrypt*

- Verification Cost
  - Requires as much memory to verify as to compute

- Drawback:
  - Verifiers require large memory
  - Takes long time to verify&propogate
  - Forking more likely

- Until recently no puzzle known to be
  - Solving: Memory hard/bound
  - Verifying: Memory easy
- Based on Cuckoo Hash Table (2001)
- A new puzzle Cuckoo Cycle proposed (2014)
  - No known way to compute without a large table
  - Easy to verify
- However no proof yet if solved without memory
- It takes time to be trusted & become common

Scrypt in Practice

- ASICs already appeared for efficient Scrypt
- Revealed that it is not ASIC-resistant (LiteCoin)
- No (A.R.) advantage over Bitcoin anymore

- Reason: Scrypt required only 128kB
- Exploit the tradeoff between memory & PU
- ASICs designed/optimized

Other Approaches for ASIC-R

- In addition to memory hard/bound?
- Design puzzle that makes hard to design ASIC
- X11. Used in DarkCoin (DASH)
  - Uses 11 different hash functions
  - So that it is inconvenient for ASIC designers
  - But once designed.. Oops!

11 Hashes?

- US National Inst. of Standards ran competition
- Design and submit
  - Design document
  - Source code
- Many candidates
- 24-winners
  - No known cryptographic attack

Another Approach

- “Moving Target” (not implemented yet)
- Not only the difficulty level but also
- Change the puzzle!
- e.g. ***Pick*** one among 24-winners
- How?
  - Centralized authority?
  - Periodically change with a schedule?

ASIC *Honeymoon*

- Despite potential market for X11
- No ASIC for X11 yet
- A new ASIC:
  - High cost & long time to design
  - Low cost to produce
- Eventually there will be ASICs for each C.C.
- A honeymoon for each ASIC

Arguments against ASIC-R

- It may be impossible
- It may be risky (already proven SHA256)
- Security vs. value
  - If attackers hack the CC, its value drops ☺
- ASIC-friendly puzzles
  - ASICs efficient only for mining

Proof-of-***Useful***-Work

- Current CCs terrible for the environment
- Any puzzle allows recycling, appreciated
- Use idle computers (spare-cycles) older idea
- Volunteering for society
- Design new such puzzles

Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new "largest prime number" twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants
Folding@home	2000	Atomic-level simulations of protein folding	Greatest computing capacity of any volunteer computing project. More than 118 scientific papers.

Table 8.3: Popular "Volunteer computing" projects

SETI@home, candidate?

- Huge computational power by people
- Statistical anomalies, difficult to find
- Drawbacks:
  - SETI has a fixed raw data (by radio telescopes)
  - Some segments may be more likely
    - Not “progress-free”
  - “Central” & “trusted” administration
- Prime numbers?

Great Internet Mersenne Prime Search

- Infinite numbers, primes, Mersenne numbers
  - Puzzle space is inexhaustable
- Drawbacks
  - Rare
  - Loong time to find
  - GIMPS found only 14 ***Mn*** in 18 years!

Primecoin

- Challenge: Find a Cunningham chain

- A sequence of k prime numbers $p_1, p_2 .. p_k$
- $p_i = 2p_{i-1} + 1$

- 2, … ?
  - Length: k=5
  - Next number: 95, not a prime, end of the chain
- Longest known: k=19, starts at
  - 79910197721667870187016101

- Not proven but believed that infinite chains
- Been used in Primecoin since 2014
- Most Cunningham chains found since then
- Variations emerged:

  $p_i = 2p_{i-1} - 1$
- Maybe used widely in future
- !! No known practical applications

Permacoin and proof-of-storage

- What if we could design a puzzle that required storing a large amount of data to compute?
- A large file F
  - Public
  - LHC's PB-large experimental data?
- Difficult to store F
  - Store H(F)
  - Or even store F as a Merkle tree & store root
- And some technical cryptographic details..

Public Good (PG)

Any proof-of-useful-work should be pure PG

- Non-excludable
  - Nobody can be prevented from using it
- Non-rivalrous
  - Good’s use by others does not affect its value
- Lighthouse ☺
- Is “protein folding” a pure PG?

Long Term Challenges & Economics

- Proof-of-useful-work
  - Natural goal
  - But challenging as different requirements

- Primecoin & Permacoin, candidates
  - Technical drawbacks (primes, rare)
  - Too minor public benefits (where is PG?)

Nonoutsourceable Puzzles

- Preventing the formation of mining pools
  - Most miners tend to join pools
  - Dangerous trend; threat to Bitcoin’s philosophy
- A large pool
  - Can attack the network (implementing strategies)
  - Pool operators may cheat
  - Target for hackers
  - Selling your vote?
- How to prevent the pools?

(Revisiting Mining Pools)

- A pool operator
- Members mine
- Send their partial solutions (proof)
- When one participant finds valid block
- Revenue distributed among members

Existence of Pools

- Two technical properties of Bitcoin
- Members can easily prove
  - their efforts
  - that the efforts are for the blocks of the pool

- Sabotage?
  - Member always send the shares, never valid block
  - Loss of the whole pool

- Sabotage, vandalism?
  - Loss to the pool, loss to himself/herself
  - Really?
- Surprisingly, it can be profitable!
  - Consider two pools, ***A*** & ***B***, each with 50% power
  - ***A*** dedicates its 25% power to ***B*** (discarding blocks)
  - ***A*** makes profit: 5/9
  - More than half: 4.5/9

- A new puzzle design
  - Members mine in pool but not submit valid blocks
  - Manager knows the secret key, and distributes
  - Puzzle requires/lets members know the secret key
- Change the puzzle from
  - “find a block with hash is below a certain target”
- To
  - “find a block for which the hash of *a signature on the block is* below a certain target.”

- Manager can

a) Distribute the key:
  - Members can steal coins!

b) Perform signature calc’s for members
  - Too much effort, better to mine solely

- This “non-outsourceable” prevent pools with untrusted members

- In current situation, this may cause opposite:
  - Individual miners don’t join pools, don’t mine
  - Only few & large pools can survive
  - Centralization!

- We do not know the solution yet ☹

Proof-of-Stake and Virtual Mining

Figure 8.5: The cycle of Bitcoin mining

- Why not simply allocate mining “power” directly to all currency holders in proportion to how much currency they actually hold?

Figure 8.6: The virtual mining cycle

Advantages

- Remove wasteful right half → Environment
- No ASIC, No AR → Centralization
- CC's value → Miners tend to behave good

Implementing Virtual Mining

- Not
  - researched scientifically
  - analyzed practically
  - (Bitcoin is too dominant)
- Peercoin (2012)
  - Hybrid: proof-of-work & proof-of-stake
  - Coin-age, coin-stake: solving & adjusting difficulty

Alternative forms of stake

- Proof-of-Stake
  - Similar to Peercoin but no coin-age
  - The richer, the easier to solve (become richer)
- Proof-of-deposit
  - When coins are used for a block, become frozen for some time
  - Reward miners who are willing to keep coins unmoved

Drawbacks of Virtual Mining

- Nothing-at-stake
  - Always attempt to fork
  - Low probability to gain
  - Nothing to lose
  - (no opt.cost as in traditional mining)
- Save-up to burst power
- Once 51%, keep it forever

Can V.M. work?

- Some believe real resources pay for security
  - Not proved ☺