NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

Bitcoin

Mining Alternatives and AltCoins

Dr Sourav SEN GUPTA

Lecturer, SCSE, NTU

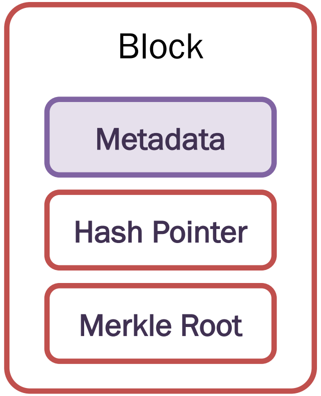
Bitcoin Mining

Properties of Proof-of-Work

Recall : Reusable Proof-of-Work (RPoW)

Mining Nodes need to solve the following puzzle to Mine.

- Choose random nonce in the Block Header (metadata).
- Hash the block and check if Hash(Block) < target value.
- If so, broadcast the block with that specific nonce value.
- If not, change the value of nonce in header to try again.



Successfully mining a block requires **multiple trials.**
However, verifying a correct Nonce is **constant time.**

Difficulty is re-adjusted every **2016 blocks**, so that the expected time to mine a block is **10 minutes.**

Bitcoin Mining Puzzle

Proof-of-Work mining in Bitcoin relies on finding a Partial Hash-Preimage

Given a *target*, find a *nonce* such that for a Block with some fixed *data*,

$$\text{SHA256}(\ \text{SHA256}(\ \mathit{data}\ |\ \mathit{nonce}\ )\ ) < \mathit{target}$$

Major properties required of this Mining Puzzle

○ **Adjustable Difficulty** : Easy to adjust using just a single parameter *target*

○ **Solution Verification** : Easy to verify *nonce* by computing a single **Hash( )**

Progress Freeness [1]

This is another subtle property ensured by the RPoW Mining Puzzle in Bitcoin.

Progress-Freeness

- Each trial with a different Nonce is independent
- Previous trials do not add up to your "progress"
- Probability of win depends only on hash power

Partial Hash-Preimage is a progress-free puzzle.

Analogy : Independent attempts on a dart-board.

[1] reading : Chapter 8 of the book "Bitcoin and Cryptocurrencies"

Mining Alternatives

ASIC-Resistant Mining Puzzles

ASIC-Resistance [1]

Goal : *Disincentivize* Miners to build and use **custom-built hardware** rigs.

Essential requirement is that the Mining Puzzle should be equally easy/hard on general-purpose computers and special-purpose custom-built computers.

- **Memory-hard Puzzles** : Requires larger memory over large compute power.
- **Multi-hashing Puzzles** : Requires multiple (chain) hash functions over one.

The idea of *ASIC-resistance* started with the boom in ASIC mining rigs (2011).

[1] reading : Chapter 8 of the book "Bitcoin and Cryptocurrencies"

Memory-hard Puzzle

scrypt (es-crypt) : Memory-hard Puzzle used in *Tenebrix*, *Litecoin*, etc.

Core idea for memory-hardness

1. Initialize a *large* memory buffer and fill up with *pseudorandom* data
2. Access (and update) the buffer in *reproducible* pseudorandom order
3. Output the values *read* from the buffer during pseudorandom access

At any step, the buffer must be either in the RAM, or computed on-the-fly.

Thus, it invokes a **time-memory trade-off**; using large RAM vs. computing.

Scrypt in Practice

Tenebrix : Launched in September 2011, the first one to use scrypt for PoW.

Claim : GPU, FPGA and ASIC resistant Cryptocurrency, meant for CPU mining.

Fate : Failed as cryptocurrency but paved the way for using scrypt in Litecoin.

Litecoin : Launched in October 2011, adopting scrypt for PoW, as in Tenebrix.

Offering : (CPU+RAM)-dominant mining and **lightweight currency parameters.**

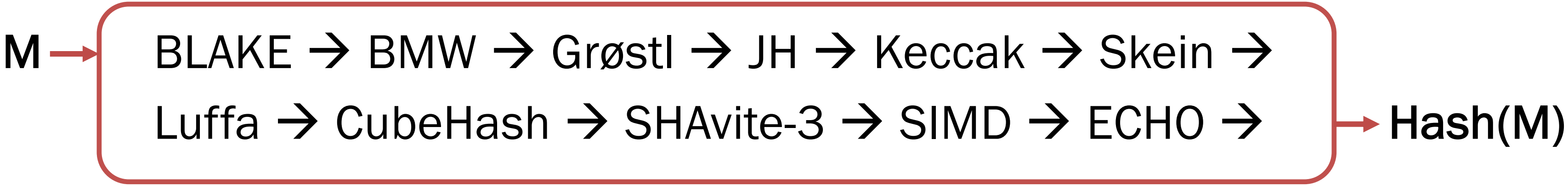
Currency Parameters : **2.5 minutes** per block and **84 million** coins by 2140.

Fate : Huge success as a cryptocurrency with several forks and followers.

ASICs manufactured for scrypt in Litecoin due to just 128 KB RAM.

Multi-hashing Puzzle

X11 : Combination of 11 different hash functions for the Mining Puzzle.



M → BLAKE → BMW → Grøstl → JH → Keccak → Skein → Luffa → CubeHash → SHAvite-3 → SIMD → ECHO → Hash(M)

Introduced by *Xcoin* in January 2014 and adopted by many other coins.
Xcoin rebranded to *Darkcoin*, and later renamed *DASH* in March 2015.

Fate : Not ASIC-resistant (may be deterrent). ASIC miners exist for Dash X11.

Mining Alternatives

Dual-Purpose Mining

Proof-of-Useful-Work

Bitcoin RPoW is based on a Partial Hash-Preimage search.

- Satisfies all nice properties of a Mining Puzzle for Bitcoin Consensus.
- Entirely “wasteful” process as the mining results are of no other use.

Quest for Proof-of-Useful-Work

- Should satisfy all desirable properties of a Mining Puzzle, for security.
- Should solve a specific problem “useful” to some real-world scenario.

Two main concerns : **Suitability** of the PoW and **Usefulness** of the Solution

PrimeCoin [2]

Announced in July 2013. Attempts at finding Cunningham Chain of Primes.

Cunningham Chain : $\{p_1, p_2, p_3, \ldots, p_k\}$ such that $p_i = 2p_{i-1} + 1$ for all $i > 1$

Conjecture : There exist Cunningham Chain of primes for any +ve integer k

Solving the Proof-of-Work produces new Chains with adjusting parameter k

Blockchain contains public record of discovered primes, useful in science.

Think about it : How do you convert this conjecture to a Reusable PoW?

[2] ref : https://primecoin.io/bin/primecoin-paper.pdf

PermaCoin [3]

Proposed in 2014 to use Proof-of-Storage or Proof-of-Retrievability for mining.

Proof-of-Storage or Retrievability

○ Suppose there is a large file F stored in parts across a distributed system.

○ Every miner stores a part of F and produces proof-of-retrievability for that.

○ End-users can check the proof through a challenge-response mechanism.

Overall, it can guarantee secure distributed storage of a large "important" file.

Think about it : How to satisfy the desirable properties of a standard RPoW?

[3] ref : http://elaineshi.com/docs/permacoin.pdf

NameCoin [4]

Decentralized **key-value pair** registration and transfer platform on blockchain.

Maintains a global Domain Name Registry for **.bit** accounts (alternative DNS).

Can also be used for other identities and namespaces, like email, certs, files.

- End-users pay a nominal Fee to the Miners to register Namespace
- Registration should be renewed every 36,000 blocks (~ 200 days)

Even though the PoW is identical to Bitcoin (SHA256 Partial Hash-Preimage), NameCoin offers some completely new applications as the **first Bitcoin fork.**

[4] ref : https://www.namecoin.org/

Consensus Alternatives

Proof-of-Stake and Variants

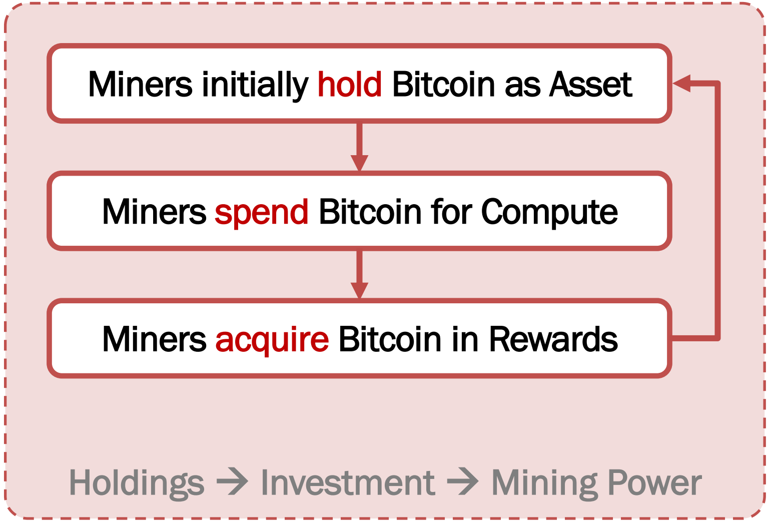
Virtual Mining

If you think about Bitcoin mining in its most abstract term, it embodies a **loop.**

How about removing the **spending** on computational power and equipment?

Mining :	Holdings → Investment → Mining Power
Virtual :	Holdings → Mining Power

Virtual Mining : Voting in the mining game is determined by how much coin one holds.



Miners initially hold Bitcoin as Asset
Miners spend Bitcoin for Compute
Miners acquire Bitcoin in Rewards
Holdings → Investment → Mining Power

Proof-of-Stake [1]

Proof-of-Stake is built on a set of simple observations

- Miners are stakeholders in the cryptocurrency ecosystem
- Prominent miners are the largest stakeholders in the coin
- Benefit to the system increases value of the coin they hold
- Miners have an incentive to benefit the system as a whole

Ensure that mining is done by stakeholders in the coin with strong incentive. Either ask the miners to prove their stake in the system or impose a penalty.

One may prove their stake through (1) Loyalty, (2) Holdings, or (3) Deposit.

[1] reading : Chapter 8 of the book "Bitcoin and Cryptocurrencies"

PeerCoin [5]

Hybrid between Proof-of-Work (as in Bitcoin) and Proof-of-Stake by “loyalty”.

Launched in August 2012; the first instance of a PoS-based cryptocurrency.

Loyalty measured by **CoinAge = Value of UTXO x Number of Blocks Unspent**

Miner includes a “coinstake” transaction within own block to reset “coinage”.

This staking of “coinage” reduces the SHA256 RPoW difficulty for that miner.

This poses a nice **PoS-PoW tradeoff** for miners in the hybrid mining routine.

[5] ref : https://www.peercoin.net/whitepapers/peercoin-paper.pdf

Stake vs. Deposit

Proof-of-Stake (pure version)

- Only the value of coin held (stake) is considered, and not the age (loyalty).
- Staking power always remain high for rich miners (no reset like “coinage”).

Proof-of-Deposit

- UTXOs (coins) staked by Miner in a block are “frozen” for a set time period.
- Mirrors “coin-age” in principle; incentivizes future “loyalty” instead of past.

Think about it : Can this consensus still result in forks by dominant Miners?