University of Basel
Center for Innovative Finance

Bitcoin, Blockchain and Cryptoassets

Proof of Work

Prof. Dr. Fabian Schär
University of Basel

```
Release Ver.:  (Local Release)
Version Hash:  (None)
Version Date:  (None)
```

Competition via Resource Allocation

Basic Idea: An activity that can be executed too quickly is combined with a probabilistic trial and error task. The activity can only be executed if the task is solved correctly.

$\Rightarrow$ Only a small fraction of tries will lead to the desired result.

Origins of Proof of Work

The concept of Proof of Work was proposed in 1993 [1] to help deter spam and denial of service attacks.

Other mechanisms have been popularized in the meantime, but Proof of Work remains the best known mechanism to deter sybil attacks and still sees widespread usage due to its simplicity.

In the Context of Bitcoin

Proof of Work in the context of Bitcoin solves the following problems:

- Blocks need to be created within certain time intervals
  - Not too fast (Propagation delay)
  - Not too slow (Transaction throughput)
- The chain must be protected from simple replication
- Malicious behavior when creating blocks should be discouraged

Implementation in the Bitcoin Protocol

In the Bitcoin protocol, Proof of Work is implemented in the context of block header hash values. The properties of the `dSHA256` hash function make it impossible to create a block header hash with a desired value.

Trial and Error:

- Require certain properties from valid block header hashes
- Specifically: Below a certain threshold value
- Each newly created block candidate has a random chance to satisfy the criteria

⇒ Create new block candidates until the block header hash value is sufficiently low

A Simple Example

Assume the current threshold value is 0x1000000000000000000000000000000000000000000000000000000000000000.

- To be lower than this value, a hash must contain a 0 in the first position
- When generating a hash from a given input, each digit has a 1 in 16 chance to be of a certain value

⇒ The network would need to generate an average of 16 candidate blocks before being able to extend the chain.

Mining Bitcoin

The iterative process of creating block candidates and checking their block header hash values against the threshold is called mining.

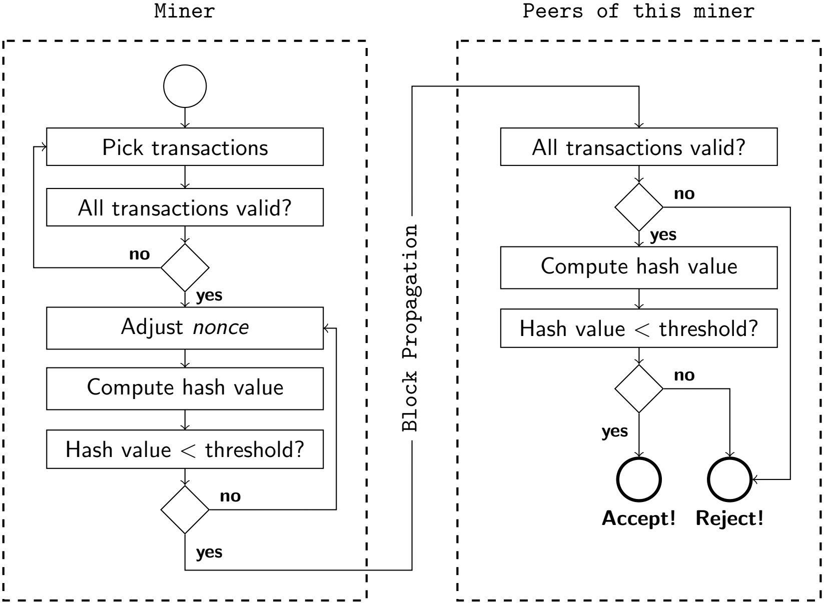
Block header hash value $\geq$ threshold

- Discard the candidate block
- Change the contents of the block header
- Recompute the new block header hash value

Block header hash value $<$ threshold

- The candidate block is relayed to the network
- The block can be appended to the chain

Mining Process Model



Dynamic Threshold

The threshold parameter δ is dynamically adjusted so that the network will produce a valid block on average every ten minutes.

- The adjustment happens every 2'016 valid blocks
- Assuming 10 minute blocks, this is every 14 days
- The new threshold value δ is calculated based on the expected value $E(t)$ and the actual duration t

$$\begin{aligned}\delta_{new} &= \delta_{old} \cdot \frac{t}{E(t)} \\ &= \delta_{old} \cdot \frac{t}{2016 \cdot 10}\end{aligned}$$

Dynamic Threshold

Blocks are generated faster than expected $t < E(t)$:

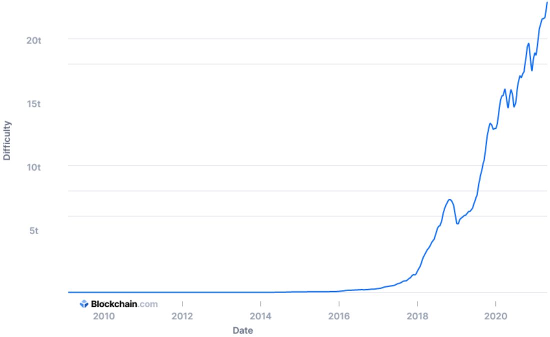
- $\frac{t}{E(t)}$ will be between 0 and 1 $\Rightarrow \delta_{new} < \delta_{old}$
- A lower threshold value will lead to fewer accepted block candidates in the following period

Blocks are generated slower than expected $t > E(t)$:

- $\frac{t}{E(t)}$ will be above 1 $\Rightarrow \delta_{new} > \delta_{old}$
- A higher threshold value will lead to more accepted block candidates in the following period

In both cases the average block creation time is moved closer to 10 minutes again.

Difficulty



Source: https://www.blockchain.com/charts/difficulty, April 2021

The Difficulty D shows the change of the threshold parameter over time. It is equal to the maximum threshold $\delta(B_0)$ divided by the current threshold $\delta(B_i)$.

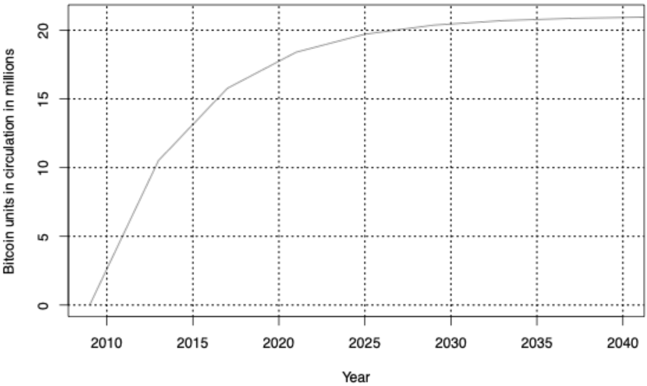
$$D_i := \frac{\delta(B_0)}{\delta(B_i)}$$

Incentives

Miners face costs. They must be incentivized:

1. Newly minted Bitcoin units (UTXO with no inputs)
2. Transaction fees (Difference between inputs and outputs of all trx in block)

Every 210,000 blocks (approx. 4 yrs), the reward rate is halved. Initially, it was at 50 Bitcoin per block.



References

[1] Cynthia Dwork and Moni Naor, *Pricing via Processing or Combatting Junk Mail*, Lecture Notes in Computer Science, 1993, pp. 139–147.