Bitcoin

Lars Erik Wik

February 1, 2022

Summary

Bitcoin is a decentralized currency based on a cryptographic ledger of transactions called a blockchain. A blockchain consists of blocks connected through hash references, each pointing to the previous block. Each block additionally contains a Merkle tree of transactions, which lets us efficiently verify the integrity of a subset of the information within the ledger (e.g. a transaction). [1–4]

The blockchain is maintained by "miners", who validates transactions by building new blocks, and by reaching a consensus on which block is the next to be appended onto the ledger. For each block successfully appended, the proposer is rewarded in bitcoin, which incentivises the miner to keep maintaining the ledger. [4]

The consensus algorithm is based on a concept called proof-of-work, in which all participants try to solve a cryptographic puzzle. Only when you solve the puzzle, will you be able to propose a new valid block to be appended onto the blockchain. The block is accepted if other miners start working on appending new blocks on top of the proposed one. [3–5]

There are quite a few challenges with the bitcoin mining puzzle. One challenge is that bitcoin incentivises miners to work in mining pools, and to use custom-built hardware, both of which causes decentralization. Another challenge is that the mining puzzle is quite energy deficient. Altcoins and other research proposes alternative consensus concepts to tackle these challenges. E.g. proof-of-useful-work, proof-of-storage and proof-of-stake, just to mention a few. But they all seem to have their own quirks and drawbacks, leading us to think that the perfect mining puzzle is yet to be discovered. [4, 5]

References

[1] Alex Chumbley, Karleigh Moore, and Jimin Khim. "Merkle Tree". In: *Brilliant* (). URL: https://brilliant.org/wiki/merkle-tree/ (visited on 01/24/2022).

[2] Brian Curran. "What is a Merkle Tree? Beginner's Guide to this Blockchain Component". In: *Blockonomy* (Apr. 2020). URL: https://blockonomi.com/merkle-tree/ (visited on 01/24/2022).

[3] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tech. rep. bitcoin.org.

[4] Arvind Narayanan et al. *Bitcoin and Cryptocurrency Technologies*. Draft. Princeton University Press, 2016. Chap. 5, 8.

[5] Florian Tschorsch and Björn Scheuermann. *Bitcoin and Beyond. A Technical Survey on Decentralized Digital Currencies*. Tech. rep. Humboldt University of Berlin.