Blockchain structure

Tereza Burianová

June 2023

This article describes main blockchain components and the way they cooperate to achieve a successful implementation. On a large scale, there are several layers working together. These manipulate various data structures that carry out asset transfers and store important data, like the accounts and their balances or the transaction history, in a secure manner [4].

1 Stacked model

Similarly to the OSI model, a networking system description, blockchain can also be divided into several layers, each having its own significant role in the whole functionality, as seen in Figure 1.

Data Layer handles data representation. It describes the block formation from a batch of transactions. The blocks are then connected together, forming a ledger. The whole process uses various cryptography methods to protect data, making the chain tamper-proof.

Network Layer secures the communication with peers in the peer-to-peer networking. Although not directly related to the blockchain network, the lower OSI layers are also needed for a successful implementation. That includes functionality like routing, domain name resolution (DNS) or addressing.

Consensus Layer describes the exact rules for mutual agreement, allowing to maintain consistency across the network. Topics like transaction order, security or incentive mechanisms are included in the consensus layer. Some of the consensus mechanisms are described in detail in section 5.

Replicated State Machine Layer defines the way transactions are processed. The goal of this process is to add the new transactions, represented as a block, into the ledger. There are high-level programming languages allowing developers to implement smart contracts, if possible for the particular blockchain implementation. The codes need to be compiled and later executed, generating new transactions that need to be processed.

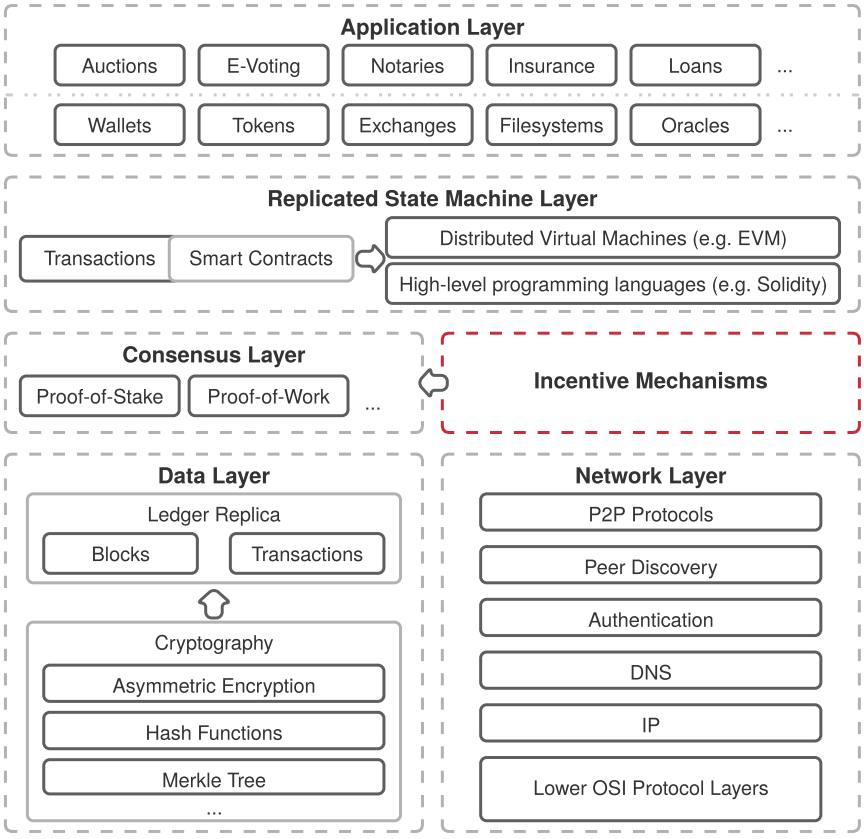

Figure 1: A model of the blockchain network implementation [4, 8].

Application Layer includes the end-user services, both basic functionalities and high-level applications. These interfaces can be used by users to communicate with the blockchain network, separating the user from the lower layers.

2 Blocks

Blockchain is a list of blocks chained together, where each of these contains a batch of **transactions** (section 3) and a **header** with other important information. Blocks are identified by a cryptographic hash containing the block header encoded using a secure hashing algorithm, for example, SHA256 or other. The identifying hash does not have to be stored in the block header, as it can be computed by every node individually. Another form of identification is the block height, meaning the position of the block in the blockchain (where the position

of the first block, which is usually called the genesis block, is 0). The chained structure is created by referencing the previous (parent) block in each block's header [2].

3 Transactions

In a bank, a transaction is a process of **transferring assets** from one account to another account, changing both accounts' balances. In the blockchain, the meaning remains, but technically, a transaction is a cryptographically signed set of information needed to execute the transfer of currencies and tokens between accounts.

The object needs to be signed using the sender's private key to confirm his identity before being included in the transaction pool as a transaction request. This is achieved using cryptography. After the transaction is created, a request is added to a list and later gets placed into a block and processed based on the used consensus protocol (section 5). Sending a transaction is a paid service and the speed of transaction processing is usually affected by the fee, making the processing faster when the fee is higher [2, 1].

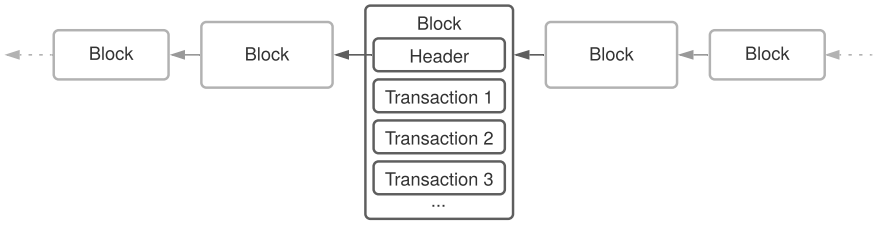

Figure 2: Structure of blockchain, showing blocks and transactions.

4 Nodes

Nodes are computers in the network, which communicate with each other and share information, being the peers in the **peer-to-peer** network. The aim is to connect a large number of independent nodes, allowing the network to function securely and reliably, without the danger of a security attack or censorship.

Nodes also hold information regarding pending transactions. When a node receives an incoming transaction, it gets stored in the **mempool**. The transaction is then sent to other nodes in the network and stays in the mempool until it gets processed and included in a block.

There are two main types of nodes: a full node and a light node. The **full node** contains a copy of the whole blockchain, including all the blocks and the corresponding transactions. It can validate all processed transactions, and query

blockchain data, but the hardware requirements are significant. The solution to this problem is the **light node**, which only holds the headers of blocks, without the included transactions. They can validate the block headers and also determine the effect of the included transactions on the network, making the nodes capable of validating them [1].

5 Consensus mechanisms

A consensus mechanism is a technology that allows peers to securely work together. It affects the way blocks are processed, the system of rewards and the safety measures against fraud [3].

The following two consensus mechanisms, used by many publicly well-known blockchains like Bitcoin, Ethereum, Cardano or Solana, work differently in the sense of block processing and also require the blockchain to be in different parts of the life cycle.

5.1 Proof-of-work (PoW)

In the proof-of-work consensus, the blocks are created and chained together by special nodes in the network called **miners**, who use their hardware to solve computationally difficult puzzles. First, the miner gathers a batch of transactions to be put into the new block and checks their validity. The puzzle required to connect the block to the chain is based on finding a pseudo-random value, the block's **nonce**, by random chance. To do that, the miner needs to transform the found value using a cryptographic hash function and see if the final value matches the conditions given by the difficulty, which is periodically recalculated based on the previous blocks' solution search time. In case of higher difficulty, the number of nonces that meet the conditions is lower, therefore it takes longer to find a solution. Once a solution is found, it gets broadcast to other nodes, who verify its validity, accept the new state of the blockchain if valid and remove the processed transaction requests from the list. The successful miner is rewarded according to the incentive mechanism.

Mining requires **computation power** and time. Increased computational power means a bigger chance of finding the solution because more nonces can be generated and checked in a shorter amount of time. The needed hardware and energy costs are too high for individuals to succeed in this competition and miners need to collaborate. The collaborating groups are called mining pools. Participants make use of their united computation power and divide the reward. That makes the individual rewards lower, but the income is steady.

A situation called soft fork may arise when several miners find the solution at once. That results in inconsistencies among the nodes. This state must be resolved, as only one child block (the new block created by the miner) can be chained to the parent block (already existing in the blockchain). To solve this issue, all nodes select the chain with the greatest total amount of executed work to achieve consistency [7, 2].

Figure 3: Proof-of-work consensus mechanism.

5.2 Proof-of-stake (PoS)

To become a validator and start validating blocks in the proof-of-stake consensus, a fixed amount of assets must be locked as a **stake**. Therefore, the main requirement is to have enough assets in the account. **Validators** with higher stakes have a better chance to be chosen to forge (process) the new block. To make the process fair and more randomized, other conditions are usually added to the validator selection process. In the "randomized block selection" mechanism, the size of the stake is combined with the lowest hash value as an additional condition. The "coin-age based selection" method adds the number of days the stake has been held. After forging a block, the counter resets and sets a limit when the validator cannot be chosen again. The set of rules is set individually by every cryptocurrency using proof-of-stake.

The chosen validator must check the validity of all transactions in the block. If the validated transactions were fraudulent, part of the stake and the right to further participate as a validator would be taken away. To disrupt the blockchain security without consequences, a node would have to own 51% of the assets. This phenomenon is called the "51% attack". The risk of this attack is higher for smaller networks, where the investment would be levelled out by the profitability.

After the transactions are validated and the block is created, the validator adds it to the blockchain and is rewarded with the transaction fees.

Proof-of-stake is currently the chosen consensus mechanism for the Ethereum protocol, after the change from the proof-of-work mechanism in 2022, also called "The Merge" [6, 5].

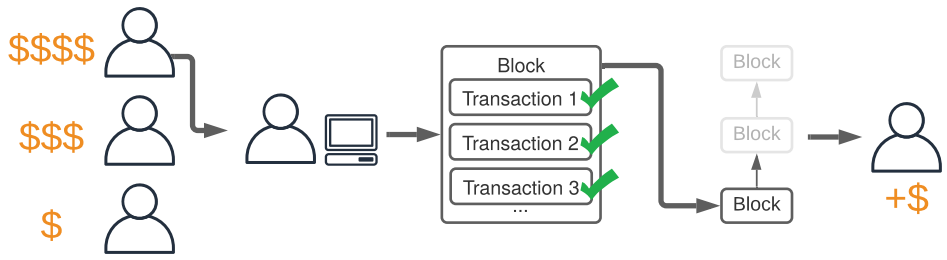

Figure 4: Proof-of-stake consensus mechanism.

References

[1] Andreas M. Antonopoulos, G. W. *Mastering Ethereum.* 2nd ed. O'Reilly Media, Inc., 2019. ISBN 978-1-491-97194-9.

[2] Antonopoulos, A. M. *Mastering bitcoin: programming the open blockchain.* Second editionth ed. Beijing: O'Reilly, 2017. ISBN 978-1-491-95438-6.

[3] *Consensus Mechanisms.* October 2021 [cit. 2021-11-07]. Available at: `https://ethereum.org/en/developers/docs/consensus-mechanisms/`.

[4] Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R. et al. *The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses.* October 2019.

[5] *Proof-of-stake (PoS).* January 2022 [cit. 2022-01-17]. Available at: `https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/`.

[6] *ProofOfStake.com.* 2018. Available at: `https://proofofstake.com/`.

[7] *Proof-of-work (PoW).* October 2021 [cit. 2021-11-07]. Available at: `https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/`.

[8] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D. et al. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access.* 2019, vol. 7, p. 22328–22370. DOI: 10.1109/ACCESS.2019.2896108. ISSN 2169-3536. Available at: `https://ieeexplore.ieee.org/document/8629877/`.