DOI: https://doi.org/10.30837/csitic52021232174

The Overview of Decentralized Systems Scaling Methods

Oleksandr Marukhnenko[1],

Gennady Khalimov [2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.marukhnenko@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, hennadii.khalimov@nure.ua*

Abstract. *Decentralized systems and protocols are becoming more popular every year. The main limitations of public permissionless blockchains are low bandwidth and high fees. There are various ways to reduce the load on the network to address these drawbacks, the majority of them were developed for Ethereum but stay valid for many other chains. The paper considers the following options for scaling decentralized systems: consensus modification and sharding that are embedded in the core of a blockchain, second layer solutions and sidechains that can be built on top of a network.*

Keywords: *blockchain, scalability, rollup, sidechain, Ethereum,*

I. Introduction and Problem Statement

Decentralized technologies have developed rapidly in recent years, and their scope is constantly growing. States and international corporations implement blockchain solutions in their infrastructure. The main advantages of blockchain-based systems are transparency, observability and censorship resistance. Disadvantages include low bandwidth in comparison with centralized solutions and high cost of operations. These problems are due to the fact that all calculations are duplicated on a significant number of nodes, so reliability improvement causes efficiency to decrease.

The increased interest in decentralized solutions leads to an increase in the load on existing systems, which entails higher transaction prices. These problems are primarily relevant for public networks with unlimited access; private blockchain networks, which are a priori more centralized, are much less susceptible to them. This paper describes a number of approaches to solving these problems.

II. Consensus

The core of any decentralized system is the consensus protocol - the rules for coordinating the state transition of the system. The level of decentralization of the system and its throughput directly depends on it. The two most popular blockchain platforms - Bitcoin and Ethereum - were built on the basis of the Proof of Work (PoW) consensus. Its peculiarity lies in the fact that the functioning of the system requires continuous significant expenditures of energy, which causes high costs for miners and motivates them to take appropriate commissions.

Proof of Stake (PoS) consensus protocols do not require constant electricity waste; if a user wants to become a miner and validate blocks, it is enough to have a certain number of frozen tokens that guarantee the miner's honesty. This approach is more efficient and can reduce transaction costs. Ethereum is gradually updating to version 2.0 [1], which includes the transition to PoS consensus and the use of a new finality mechanism – Casper [2].

Delegated Proof of Stake (DPoS) is a special case of PoS, the main feature of which is that users can delegate their assets to validators and receive part of their reward. DPoS usually has a limited maximum number of validators. Various variations of this protocol are used in Polkadot, EOS, Cosmos, and other systems.

PoW consensus was especially relevant in the early days of blockchain and remains the most popular solution nowadays. However, its main drawbacks - low bandwidth and high fees - increase interest in other consensus algorithms, especially DPoS. The example of Ethereum shows that it is possible to switch to a different consensus algorithm to improve the platform's characteristics.

III. Sharding

The low throughput of the blockchain is related to the fact that all full nodes have to process all transactions on the network. Sharding is one of the possible solutions to this problem; this mechanism divides the network into interconnected subnets (shards), each of which is responsible for processing a certain part of transactions.

Sharding is one of the key features announced in Ethereum 2.0, in this model each chain (shard) uses the same protocol and provides equal capabilities for building DApps. Polkadot project proposes the concept of multiple interconnected chains (parachains) that share the security of main chain (Relay chain), this chain is also responsible for transferring cross-chain messages [3]. Relay chain was designed to provide only the most important functionality to avoid over-complication. For example, it doesn’t include smart contracts, but its upgradability mechanisms allow adding new features using governance system. At the same time, Polkadot doesn’t limit parachain builders, so they can add any necessary features, such as zero-knowledge proofs or smart contracts. That’s why each parachain may provide unique capabilities, the only requirement is the possibility to compile state transition function into Web assembler (WASM) so it can be verified by Relay chain validators.

One of the key challenges for sharding is cross-shard transactions, when several modules in different shards should simultaneously perform an atomic action. Such a situation is especially relevant for DeFi space where more complex protocols are often built on top of a simpler ones.

Sharding is not applicable for PoW-based blockchains because this leads to a dissipation of computing power and a decrease in the system's security. In the case of PoS, with a randomized assignment of validators for individual shards, the system's security is not reduced, so Ethereum plans to use this technology only after switching to PoS. Some other projects, in particular Polkadot and Near, put sharding functionality at the core of their architecture.

IV. Layer 2 Solutions

Changing consensus or implementing sharding requires modifying the core of the blockchain and usually a hard fork. Such deep changes require community approval, long development, and testing; therefore, such updates are rarely introduced. There is an alternative solution - the so-called second-layer solutions. They do not change the blockchain core but use only the platform's programmable logic, such as smart contracts. They allow performing calculations outside the main blockchain network (layer 1) and, accordingly, not pay a commission for these calculations, however, these protocols record the necessary information (the contents of transactions or proof of their correctness) in layer 1 to maintain the required level of security. The first second-layer solutions, in particular the Lightning Network, were created for Bitcoin. Later solutions were developed primarily for Ethereum; however, they can be adapted for almost any blockchain.

Plasma [4] is one of the first proposed methods to reduce the load on Ethereum. It is based on the concept of building a blockchain tree, where the results of the execution of child chains of blocks are recorded in the parent chains. This technology had a number of limitations associated with the need to verify a large number of transactions and a critical increase in the load on the main network when failures are detected in the secondary chain.

ZK-rollup. This approach was proposed as an alternative to Plasma. The idea of ZK-rollups is to replace the storage and verification of transactions with the storage and verification of some cryptographic proofs using zero-knowledge cryptographic protocols [5]. ZK cryptography allows proving the correctness of various statements without revealing the data itself; the statement should be transformed into a set of equations of a special form. In the case of ZK-rollups, the correctness of transactions and the state transition caused by them are proved. Layer 2 security is based on the fact that all evidence's correctness is checked on layer 1, which guarantees the same level of security as if the transactions are carried out in layer one itself.

ZK-rollups usually based on one of two classes of algorithms ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) or ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge). Each of the cryptographic protocols has advantages and disadvantages. The main limitations of ZK-rollup:

- High computational complexity of proof constructing.

- The proofs remain highly specialized and are suitable only for specific types of transactions; the provability of arbitrary program logic's execution is actively investigated.

ZK-rollup technique is used by StarkWare, ZKSwap, and Hermez projects.

Optimistic rollup [6]. When this approach is used, all transactions made on layer two and added to layer one are considered valid unless proven otherwise. Information about layer two transactions is included in layer one; however, the transactions themselves don't have to be performed, which allows for lower gas costs. For some time after the inclusion of a transaction in layer 1 (as a rule, about a week), any user can explicitly initiate this transaction's execution on layer one and pay a gas commission for this. If the transaction turns out to be incorrect, the participants who saved it are penalized, and the user who executed it is rewarded. This allows the detection of invalid transactions and provides the second level with the same security level as the first level. The most popular solutions based on optimistic rollup are Optimism and Arbitrum.

V. Sidechains

Layer 2 solutions are inextricably connected with the mainnet and based on its security. Sidechain is an independent blockchain with its own consensus and functionality; its main feature is the ability to receive liquidity from the mainchain and return it back. When transferred to the sidechain, coins are frozen and cannot be used in the mainchain until they are returned. The liquidity transfer mechanism can be designed in various ways, in particular, zero-knowledge algorithms can be used.

Sidechain applications include:

1) Sidechain can have more favorable terms of use: higher transaction speed or lower fees;

2) The sidechain may contain completely new functionality that is not available in the main chain;

3) Sidechain allows creating experimental systems in which tokens with real value are needed, for example, DeFi protocols or PoS consensus, and test them in real conditions.

There are various Ethereum sidechains, including Polygon (Matic), xDAI, Binance Smart Chain. The Horizen project positions itself as a platform for building sidechains, using a protocol based on zero knowledge – Zendoo [7] to transfer liquidity between chains.

VI. Conclusion

Decentralized blockchain platforms have a number of advantages and disadvantages. The main limitations relate to the system bandwidth. There are various ways to solve this problem, some require changes in the core of the blockchain (consensus, sharding), others are add-ons (Plasm, ZK-rollup, Optimistic rollup), and others allow value to be transferred to other systems (Sidechains). Active research and development of new solutions continues.

REFFERENCES

[1] V. Buterin et al. Ethereum 2.0 Specifications. [Online resource] https://github.com/ethereum/eth2.0-specs.

[2] V. Buterin, V. Griffith. Casper the friendly finality gadget. 2017.

[3] G. Wood. Polkadot: vision for a heterogeneous multi-chain framework. 2017

[4] J. Poon, V. Buterin. Plasma: Scalable Autonomous Smart Contracts. 2017.

[5] Alex Gluchowski. Zk rollup: scaling with zero-knowledge proofs. Matter Labs, 2019.

[6] Karl Floersch. Ethereum Smart Contracts in L2: Optimistic Rollup. 2019.

[7] A. Garoffolo, D. Kaidalov and R. Oliynykov, "Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains," *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, Singapore, Singapore, 2020, pp. 1257-1262, doi: 10.1109/ICDCS47774.2020.00161.