Optimistic and Zero-Knowledge Rollups

Understanding blockchain

Angelo PICERNO

Eduardo TEIXEIRA DE SOUSA

Elena PEROTTI

Micaela MASRI

November 2025

Contents

1. Introduction

The emergence and widespread adoption of blockchain technology has revealed a fundamental structural limitation: scalability. This issue, along with the possible solutions to overcome it, is the main focus of this document.

Scalability is one of the three fundamental components of the so-called blockchain Trilemma, along with decentralization and security.

The Trilemma states that a blockchain system can only optimize two of these three properties at the same time, forcing designers to accept trade-offs in performance or trust assumptions.

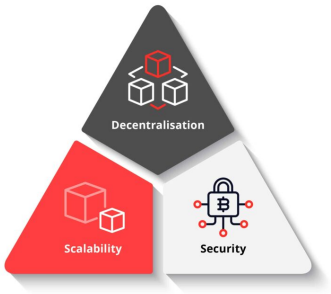

Figure 1: The blockchain trilemma

Interestingly, scalability challenges are not unique to blockchain systems. Traditional database architectures have long faced a comparable tension, often described as the CAP Theorem. Even though applied to different technologies, both frameworks highlight the same underlying idea: achieving perfect performance, resilience, and correctness at the same time is structurally difficult.

Thus, blockchain scalability can be understood not as an isolated limitation, but as the continuation of a broader historical challenge in distributed systems.

2. Technical Background

In this section, we will cover the core concepts required to frame the discussion on blockchain scalability.

2.1. Scalability and Layer 1

A Layer 1 blockchain is a foundational blockchain that processes and validates transactions independently within its own network, without relying on external systems. Examples of Layer 1 blockchains include Bitcoin, Ethereum, Solana, Aptos, and NEAR.

Several solutions have been proposed to increase the transaction processing capacity at the Layer 1 level. These include *sharding*, which enables parallel validation of transactions across different shards, and modifications to the consensus protocols to make them more efficient.

2.1.1 Sharding

Sharding consists of dividing a blockchain into smaller, more manageable segments, called shards, which can process transactions and execute smart contracts in parallel. By distributing the computational load across multiple shards, blockchain networks can significantly improve throughput while reducing latency and resource consumption.

Unlike traditional blockchain architectures where all nodes must process every single transaction, sharding allows subsets of nodes to validate only a portion of the total transactions, thus increasing scalability.

For example, if a network of 1,000 nodes is divided into 10 shards of 100 nodes each, the transaction processing speed can increase by approximately a factor of ten.

An example of a sharding implementation is the NEAR Protocol, a Layer 1 blockchain that uses Nightshade. Its network is capable of processing up to 160,000 transactions per second (TPS), outperforming many other blockchain platforms.

While sharding improves scalability, it also introduces potential security risks. If a shard contains too few nodes or if a single shard is targeted by malicious actors, it may become easier to compromise the consensus within that shard. Therefore, blockchain designers must carefully balance shard size, the total number of shards, and mechanisms for cross-shard communication to maintain the overall security of the network.

2.1.2 Consensus Protocols: PoW vs. PoS

Another approach to improving blockchain performance is the adoption of alternative consensus protocols, which affect transaction speed, security, and energy efficiency.

Proof of Work (PoW) is a transaction validation algorithm based on solving computational problems, requiring network participants (miners) to perform complex cryptographic operations. PoW-based networks have significant environmental costs due to the high energy consumption associated with mining. Additionally, the need for specialized, high-performance hardware further increases the economic burden of maintaining network security.

An alternative consensus protocol, **Proof of Stake (PoS)**, does not require high computational

power and significantly reduces transaction times, making it a more efficient solution compared to PoW. In PoS, instead of solving cryptographic puzzles to find the correct nonce, users must prove ownership of a certain amount of digital tokens to participate in block validation.

However, PoS introduces a potential risk of centralization: users holding a large number of tokens may exert disproportionate influence over the network, compromising decentralization.