CentraleSupélec | université PARIS-SACLAY

Optimistic and Zero-Knowledge Rollups

Understanding blockchain

Angelo PICERNO

Eduardo TEIXEIRA DE SOUSA

Elena PEROTTI

Micaela MASRI

November 2025

Contents

1. Introduction **2**

2. Technical Background **3**

2.1. Scalability and Layer 1 3

2.1.1. Sharding 3

2.1.2. Consensus Protocols: PoW vs. PoS 4

2.2. Scalability and Layer 2 4

2.2.1. Optimistic Rollups 5

2.2.2. Zero Knowledge Rollups (ZK Rollups) 5

1. Introduction

The emergence and widespread adoption of blockchain technology has revealed a fundamental structural limitation: scalability. Along with decentralization and security, scalability is one of the three fundamental components of the blockchain trilemma. 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.

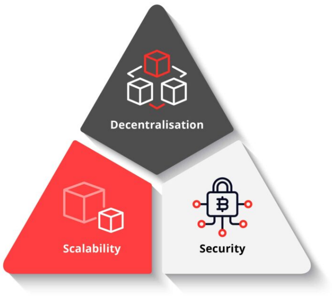

Figure 1: The blockchain trilemma

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, and often impossible.

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

There are two main strategies to improve blockchain scalability. The first one is to modify the underlying blockchain architecture (Layer1, or L1). The second is to implement a second layer (L2) consisting of auxiliary technologies built on top of L1.

Among L2 solutions, Rollups (and in particular Optimistic Rollups and Zero-Knowledge Rollups) have gained central importance because they shift most computational load off-chain, while preserving the security guaranteed by Layer 1.

This document examines the technical and functional characteristics of both approaches and discusses their differences, advantages and limitations, as well as potential adoption scenarios. The goal is to assess how these mechanisms contribute to addressing the scalability challenge and to evaluate the extent to which they can offer a viable path toward more efficient and widely deployable blockchain 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.

2.2. Scalability and Layer 2

To improve transaction throughput and overall scalability, several Layer 2 solutions have been developed. These solutions operate as external integrations built on top of the base layer and help overcome performance limitations while preserving the security guarantees of the underlying blockchain.

Although different approaches exist, including State Channels and Sidechains, this document focuses exclusively on Rollups, a Layer 2 scalability solution designed to increase blockchain throughput and reduce transaction costs while preserving the security of Layer 1. Rollups have become the most widely adopted Layer 2 strategy, particularly for public blockchains, most notably Ethereum.

A Rollup works by executing transactions outside the main blockchain, while still relying on it for data availability and final verification. Instead of having every node on Layer 1 process every transaction, the Rollup aggregates a large number of transactions into a single batch, computes the resulting new state, and submits only the essential data back to the Layer 1 chain. This drastically reduces the amount of computation and storage required on the base layer, which in turn increases throughput and lowers fees. Even though execution happens off chain, Layer 1 blockchain is responsible for verifying correctness through proofs or dispute mechanisms, ensuring that all state transitions produced by the Rollup are valid.

Overall, Rollups represent an effective compromise between scalability, transaction costs and security, and they are rapidly becoming one of the key technologies for improving blockchain performance.

2.2.1 Optimistic Rollups

Optimistic Rollups work on the principle that all off-chain transactions are valid by default, allowing high throughput and reduced latency compared to immediate verification on Layer 1. Transactions are grouped into batches and processed off-chain by operators, who then submit a proposed new state to Layer 1. After submission, there is a defined *challenge period* during which any participant can contest a transaction in the batch using a *fraud proof.*

The fraud proof process follows a game-theoretic protocol: the disputing participant and the operator who proposed the state interact to isolate the dispute down to a single computational step, which is then executed on Layer 1. If the execution result differs from the proposed state, the fraud proof is successful, the batch is reverted, and the operator responsible is penalized, often by forfeiting a staked deposit.

If no disputes are raised during the challenge period, the proposed state is accepted as final, and the batch of transactions is confirmed on Layer 1. This mechanism allows most computation to occur off-chain while relying on Layer 1 to enforce correctness and ensure security.

2.2.2 Zero Knowledge Rollups (ZK Rollups)

Zero Knowledge Rollups (ZK Rollups) generate a cryptographic proof known as a validity proof for each batch of transactions. This proof, published on Layer 1, guarantees that all transactions were executed correctly, which removes the need for dispute periods. ZK Rollups offer faster confirmation times than Optimistic Rollups, but generating the proofs can require substantial computational resources.