Offchain Computing in Blockchains

Nikhil Kottoli — 231CS236

Abstract

Blockchain technology faces fundamental scalability challenges due to the computational and storage limitations inherent in onchain execution. Every transaction must be validated by numerous nodes in the network, creating bottlenecks in throughput, latency, and cost. Offchain computing has emerged as a critical solution paradigm that enables complex computations to occur outside the main blockchain while preserving security guarantees through cryptographic verification mechanisms.

1 Offchain Computing Architectures

This section examines the landscape of offchain computing architectures, including state channels, sidechains, rollups, and trusted execution environments. We analyze the security models underlying these approaches, particularly examining trust assumptions, liveness requirements, and data availability guarantees.

Zero-knowledge proofs enable succinct verification of arbitrary computations without revealing underlying data, while optimistic approaches rely on fraud-proof mechanisms and challenge periods, trading immediate finality for reduced computational overhead.

These approaches aim to improve scalability by shifting computational workloads off the main blockchain while maintaining verifiability and decentralization.

2 Case Study: Agora

Agora is a novel Polkadot parachain implementing verifiable offchain computation through a cryptoeconomic commit-reveal protocol and Cross-Consensus Message Format (XCM). Agora establishes a decentralized marketplace where parachains outsource computationally intensive or I/O-bound tasks to a network of staked workers.

Unlike trusted execution environment approaches that rely on hardware security modules, Agora achieves Byzantine fault tolerance through a two-phase commit-reveal game with hash verification, eliminating dependencies on specialized hardware like Intel SGX.

The system employs a hybrid execution model where offchain workers handle resource-intensive operations including API requests, cryptographic computations, and data processing, while only cryptographic commitments and reveals are recorded onchain. Workers submit commitments in the form of hashed results concatenated with random salts, preventing post-commitment manipulation.

During the reveal phase, the protocol verifies submitted results against committed hashes and establishes consensus through majority voting among worker submissions. Honest workers collaboratively providing the majority result share the job bounty, while dishonest participants face dual penalties through economic slashing and persistent reputation decay.

Agora leverages Polkadot's native XCM infrastructure to enable cross-parachain job submission and asynchronous result delivery through HRMP channels. Sovereign accounts facilitate atomic multi-asset bounty payments without bridge trust assumptions.

The architecture demonstrates how specialized computation parachains can provide verifiable offchain services to the broader ecosystem while inheriting security from relay chain validators, eliminating the need for independent validator bootstrapping and reducing operational costs for computation marketplace participants.