Resilient Shared Sequencers

Introduction

Current shared sequencer solutions like Espresso use a pipelined BFT algorithm(HotShot) for achieving consensus among the several sequencer nodes.

There are significant challenges in MEV (Maximal Extractable Value) extraction in blockchain systems using pipelined BFT algorithms to achieve consensus. This detailed analysis explores the nuances of these challenges and proposes innovative solutions to ensure liveness of the network.

Problem Statement

Understanding Pipelined BFT Consensus Algorithms

- Mechanism of Pipelined BFT

: In pipelined BFT consensus algorithms, each block(nth

block) contains a Quorum Certificate (QC) or a Timeout Certificate (TC) for the previous block((n-1)th

block). The QC represents a majority of yes votes, while the TC indicates a majority of no or timeout votes. Alongside this, the block includes a list of transactions proposed by the current leader, Alice, for the nth

time slot.

- Roles in Block Propagation

: The (n+1)th

block proposer, Bob, is responsible for gathering the QC/TC for the transactions proposed by Alice. This sequential responsibility is crucial for maintaining the integrity and order of transactions.

Identifying the Attack Vector

- Scenario Analysis

: An attack vector emerges when Alice, the block proposer, discovers an MEV opportunity and proposes a specific transaction order. If Bob, the proposer of the next block, times out without proposing any block, the opportunity for MEV theft arises.- Collusion and MEV Theft

: In this scenario, Charlie, the proposer of the (n+2)th

block, gains access to Alice’s transaction order. If Bob and Charlie are Byzantine nodes, they can collude, allowing Charlie to steal the MEV. With BFT assumptions of 1/3rd

faulty nodes, we expect two consecutive faulty actors every 2.25 blocks.

The Magnified Problem in PBS Model

- Transaction Flow in PBS

: In a Proposer-Builder Separation (PBS) model, this problem is exacerbated. The builder sends the block content to the proposer Alice along with the fee for including the transaction. If the proposer of the next block(Bob) times out, the block content remains in the network, vulnerable to exploitation by Charlie(the proposer of the (n+2)th

block).

- Losses to Builders

: The builder not only loses the MEV opportunity but also incurs financial loss, having paid some amount to Alice for the initially including the transaction. This disincentivises the builders to capture MEV.

[

76b6383a-64f4-4b6e-8d13-82a420914904

2096×1302 155 KB

](https://ethresear.ch/uploads/default/original/2X/5/5b67cffdb6f7e969763e9ccb057d05ae2daeb7a8.png)

The DoS Vector

- Issues with Sequencers

: With MEV disincentivised, sequencers lack an up-to-date view of the state. This raises the risk of them including transactions from accounts that have depleted their gas, creating a Denial-of-Service (DoS) attack vector.

Proposed Solutions

Introducing FIFO Ordering

- Implementation of FIFO

: To counter these issues, we propose a verifiable FIFO (First In, First Out) ordering at the protocol level. In this system, non-faulty nodes will only sign blocks that adhere to FIFO ordering. This strategy effectively removes incentives for sequencers to engage in MEV theft.

- Benefits of FIFO in MEV Extraction

: FIFO ordering ensures that transactions are processed in the order they are received, promoting fairness and reducing the likelihood of MEV-related manipulations and decreasing throughput.

Security Deposit Mechanism

- Concept of Security Deposit

: To address the DoS issue, a security deposit mechanism is introduced. This involves a one-time payment to prevent spam and misuse of network resources.

- Operational Mechanics

: A part of the security deposit is charged when a transaction is included in a block and deducted again at execution time. After the new state commitment, the amount is refunded. This allows the sequncers to include valid transaction while maintaining a single state(state of the security deposit), which can be only updated either directly by the user or requires a QC from the sequencers.

Compatibility with L2 Protocols

- Integration with Existing Protocols

: Importantly, the introduction of security costs does not alter the underlying Layer 2 (L2) at the protocol level. It’s an additional layer, implemented through a smart contract, enhancing the system’s robustness without disrupting existing operations.

I would love to get in touch with and chat with interested folks.

You can get in touch with me on mytwitter or drop a comment bellow. My TG is @trojan0x

.