Threshold Encrypted Mempools: Limitations and Considerations

This work was done between April and July 2023 under FRP31 originally named “A Study of Threshold-Decrypted Mempools, MEV and Their Benefit to Users”

Authors: Antoine Rondelet, Quintus Kilbourn

Abstract

Encrypted mempools are a class of solutions aimed at preventing or reducing negative externalities of MEV extraction using cryptographic privacy. Mempool encryption aims to hide information related to pending transactions until a block including the transactions is committed, targeting the prevention of frontrunning and similar behaviour. Among the various methods of encryption, threshold schemes are particularly interesting for the design of MEV mitigation mechanisms, as their distributed nature and minimal hardware requirements harmonize with a broader goal of decentralization.

This work looks beyond the formal and technical cryptographic aspects of threshold encryption schemes to focus on the market and incentive implications of implementing encrypted mempools as MEV mitigation techniques. In particular, this paper argues that the deployment of such protocols without proper consideration and understanding of market impact invites several undesired outcomes, with the ultimate goal of stimulating further analysis of this class of solutions outside of pure cryptograhic considerations. Included in the paper is an overview of a series of problems, various candidate solutions in the form of mempool encryption techniques with a focus on threshold encryption, potential drawbacks to these solutions, and Osmosis as a case study. The paper targets a broad audience and remains agnostic to blockchain design where possible while drawing from mostly financial examples.

Paper

arXiv.org

Threshold Encrypted Mempools: Limitations and Considerations

Encrypted mempools are a class of solutions aimed at preventing or reducing negative externalities of MEV extraction using cryptographic privacy. Mempool encryption aims to hide information related to pending transactions until a block including the...

Summary

This paper dives into the motivations, drawbacks and unintended consequences of using threshold encryption for mempool privacy in blockchains.

We start with a survey of issues like frontrunning and consensus-destabilizing incentives and explain how threshold encrypted mempools may be used to change these dynamics. In doing so, the paper touches on some of the decisions characterizing the design space of encrypted mempools such as user-optionality and what information to leave unencrypted.

The focus of the paper, however, is illuminating the various potential downsides and limitations of threshold encrypted mempools - critiques which often apply to similar designs.

These include:

- Decryptors inherently gain early access to data before others, creating information asymmetry and an incentive to delay decryption. This advantage merits thoughtful protocol design.
- Increased risk of inconspicuous collusion among decryptors, which is far harder to detect than consensus faults. This is especially concerning for PoS chains delegating significant duties to a small set of validators, and looking to use weighted decryption shares to align assumptions with those of Tendermint.
- Validators retain influence over transaction ordering despite encryption. This is a potential limitation not a drawback of encrypted mempool.
- Using threshold encryption may lead to adverse consequences in terms of transaction patterns, overhead costs, and can provide incentives for strategic users to spam the network.
- While it is harder to apply targeted censorship, censorship remains possible especially when not all transaction data is encrypted (e.g. plaintext user accounts to prevent DoS attacks). Less information, but unchanged censorship motivation may also lead to broader censorship, possibly empty blocks.

- Threshold encryption adds constraints on the size of the validator set due to additional technical overhead.
- Encrypted transactions can preclude economically efficient outcomes such as orderings which prevent reversions or timely liquidations.

In the final section, the paper looks at Osmosis' MEV mitigation agenda as a case study. This includes Osmosis' categorization of MEV, their plans to implement threshold encryption and their reliance on governance and ProtoRev to handle "benign" MEV.

Overall, by surfacing economic, incentive, and systems challenges and tradeoffs, this paper seeks to make a compelling case for more nuanced evaluation of encrypted mempool proposals beyond their cryptographic security.