Title:

A Study of Threshold-Decrypted Mempools, MEV and Their Benefit to Users

Team:

Antoine Rondelet

Flashbots contact

: @Quintus

Created:

2023-03-24

Status:

Completed

Github:

https://github.com/flashbots/mev-research/blob/main/FRPs/active/FRP-31.md

A Study of Threshold-Decrypted Mempools, MEV and Their Benefit to Users

Background and Problem Statement

Encrypted mempools are a class of solutions to mitigate behaviours considered nefarious to users such as 'frontrunning' or 'sandwiching'.[^1] The basic approach consists in minimizing user data leakage by hiding sensitive transaction data until the blocks (in which the transaction is included) or the ordering is committed.

There are multiple ways to build an encrypted mempool. Designs based on threshold decryption schemes are favorite candidates of projects like Arbitrum, Osmosis, Anoma, and Penumbra. This is because:

- such designs are elegant as some of them can be overlaid on top of Byzantine Fault Tolerant consensus protocols (ie. by reusing the 2/3 majority assumption and appending threshold key shares to consensus votes).
- such designs mesh relatively well with first-come first-serve ordering protocols to create latency-minimized 'blind-order fairness'.
- the complexity of implementation is seemingly low, especially in the Cosmos ecosystem where this will soon be implementable out of the box using the Cosmos SDK once abci++ and vote extensions are implemented.
- many of these designs are implemented/ready to be implemented today (the additional overhead & latency works for many networks with a small number of validators, the technology actually works).

However, there are multiple known drawbacks to such solutions, acknowledged and discussed in several works already. Non-exhaustively, these include two broad categories:

- security:
- 2/3 honesty majority assumption, and how it overlays with consensus majority assumption made, especially if also combined with an ordering protocol
- non-attributability of misbehavior
- incentive compatibility for committee members
- liveness attacks on the system
- blind-order fairness gameability
- reorg incentives on chains without fast finality
- cap on size of the validator set: the overhead currently doesn't work for consensus protocols like ethereum if all validators were participating in the protocol
- 2/3 honesty majority assumption, and how it overlays with consensus majority assumption made, especially if also

combined with an ordering protocol

- non-attributability of misbehavior
- incentive compatibility for committee members
- liveness attacks on the system
- blind-order fairness gameability
- reorg incentives on chains without fast finality
- cap on size of the validator set: the overhead currently doesn't work for consensus protocols like ethereum if all validators were participating in the protocol
- economic welfare
- welfare loss from latency incurred from encryption/decryption, and additional bandwidth needed
- welfare loss from markets moving 'slower' than their counterparts and users swapping on stale prices
- welfare loss from sub-optimal blockspace allocation by not being able to see transactions and therefore order them, or backrun them efficiently. (ie. spam transactions from searchers)
- welfare loss from latency incurred from encryption/decryption, and additional bandwidth needed
- welfare loss from markets moving 'slower' than their counterparts and users swapping on stale prices
- welfare loss from sub-optimal blockspace allocation by not being able to see transactions and therefore order them, or backrun them efficiently. (ie. spam transactions from searchers)

This has prompted some to dismiss the family of solutions entirely, while others have forged ahead, claiming these issues are fixeable, partially charmed by the ease of implementation of such solutions. However, we haven't seen rigorous analysis of the drawbacks listed above yet. We fear this might end up being at the detriment of users of the systems that choose to adopt such solutions.

This leads us to our problem statement for this work: is using threshold-decrypted mempool a net improvement for users?

Plan and Deliverables

We plan to produce a paper or a blogpost with a summary of our findings.

A few steps we plan to take as part of our study include:

- thoroughly analyse the drawbacks and benefits of threshold-decrypted mempools (and the nuances that may exist in their different design & implementation)
- put ourselves in the shoes of an MEV searcher (i.e. a quant trader) and think through the ways a trading opportunity can be seized in a simplified system with a threshold-decrypted mempool

While we plan to share our findings of the study above. We would also like our work to survey the problem space and and open the discussion to the broader community by surfacing what we see as interesting research questions needing further work.

If need be, the study may then be refined to account for specificities of selected networks and projects (e.g. to account for specific markets, different MEV governance processes - how it is redistributed and captured within a specific network etc.). Our study will be limited by the lack of data about systems using threshold decrypted mempools, and may thus be revisited once a data trail exists on such systems.

Further Work

We hope the work above can pave the way for other work and interesting questions we already have in mind, those include:

- devise a unifying framework to think of tradeoffs between 'complete' privacy and full transparency wrt to mempool!
- More generally, we hope see this piece of research can be an invitation to further research the tradeoffs, and the spectrum, between complete mempool privacy and mempool 'transparency'. Better understanding the tradeoffs of privacy preserving techniques on blockchains will, we believe, help projects in the industry decide the approach that best aligns with their vision and requirements, and choose between transparency/"MEV-aware" block construction, and privacy/(threshold) encrypted mempools.

- More generally, we hope see this piece of research can be an invitation to further research the tradeoffs, and the spectrum, between complete mempool privacy and mempool ‘transparency’. Better understanding the tradeoffs of privacy preserving techniques on blockchains will, we believe, help projects in the industry decide the approach that best aligns with their vision and requirements, and choose between transparency/“MEV-aware” block construction, and privacy/(threshold) encrypted mempools.
- creating a testing framework to experiment with different mempool designs through simulations
- explore potentially deeper results that are not only specific to threshold crypto but can be generalized to all mechanisms that hides the mempool with no expressivity, also called ‘complete privacy mempools’.
- elucidate potential mitigations to problems found and different market structures that could increase the attractiveness of such solutions.

Some deeper threads we would hope our initial study or further work hit on include consensus protocol design, leaderless block construction and security analyses of out-of-protocol threshold-decryption solutions like EigenLayer & Shutter Network versus in-protocol solutions like abci++.

References

- FRP-18: Cryptographic Approaches to Complete Mempool Privacy by James Stearn
- Ferveo: Threshold Decryption for Mempool Privacy in BFT networksby Joseph Bebel (Anoma), Dev Ojha (Osmosis Labs)
- Performance of EdDSA and BLS Signatures in Committee-Based Consensus by Li, Sinnino, Jovanovic
- Cryptoeconomic Security for Data Availability Committees by Tas and Boneh
- Questions around mempool privacy using threshold encryption by @ra (Flashbots)
- MEV and Fair Ordering - Valeria Nikolaenko and Dan Boneh
- Penumbra docs on threshold encryption
- John Charbonneau’s Survey of Encrypted Mempools
- Justin Drake on Encrypted Mempools
- Threshold Decrypted Transactions: Thwarting Front-Running and Enabling Privacy at the Protocol Level by Sunny Aggarwal (Osmosis Labs)
- Shutterized Beacon Chain
- Shutterizing Gnosis Chain: Step 0

[1] - whether it is nefarious or not is the subject of a longer piece beyond the scope of this note.