

Intro

Decentralized relays will play a critical role in the credible neutrality and future of the Ethereum network. Zero-Knowledge Proofs (ZKP) will enable that future through bolstering security and privacy.

Zero-Knowledge Proofs allow one party to prove the validity of a statement without revealing any information about the statement itself. In decentralized relays, ZKPs can be used to validate transactions or state transitions without disclosing sensitive data.

Novel architecture and actors are needed to create functioning decentralized relay. A novel decentralized relay has been created, The Proof of Neutrality Relay (PoN), and is currently live on testnet.

Encrypted Blocks with Payment Proofs

The decentralized relay can employ encrypted blocks with payment proofs to ensure that validators

receive their rewards without divulging the contents of the block. This approach not only safeguards transaction privacy but also guarantees that validators are properly compensated for their work.

Encrypted Mempool

An encrypted mempool allows for secure storage and transmission of transactions within the relay network.

Introduction of “Reporters”

To maintain the smooth functioning of a decentralized relay, a system of reporters can be implemented to monitor the actions of builders and proposers. These reporters help detect any malicious behavior or violations within the network, submitting reports and earning rewards for upholding the protocol’s integrity. Both builders and proposers will be required to provide collateral, and proposers can be penalized as well.

Proposer-Builder Separation

Proposer-builder separation is a solution designed to mitigate the centralization risks associated with miner extractable value (MEV) in consensus networks. MEV incentivizes economies of scale, which disproportionately benefit large pools and compromise the network’s decentralization. The PoN relay was specifically developed with proposer-builder separation in mind to address these concerns.

Decentralized Pooling

MEV complicates decentralized pooling because a sole entity, usually centralized, is responsible for packaging and proposing the block can secretly extract MEV without sharing revenue with the pool. A protocol operated entirely through smart contracts can enable decentralized payout pool for validators. In the PoN relay this is called the PBS Smoothing Pool and disburses payments to validators on a weekly basis.

Conclusion

Incorporating cryptographic techniques to enable proposer-builder separation and build out the architecture of a decentralized relay will be an important addition to Ethereum. The in-depth [documentation](#) that I created and the [website](#) is now live. Looking forward to any thoughts and opinions on this matter.