Hi all,

I'm Tudor Malene, a member of a team of experienced engineers who have been working on decentralised systems for the past few years.

We propose a new Ethereum Layer 2 Rollup protocol designed to achieve data confidentiality and prevent MEV by leveraging hardware-based Trusted Execution Environments.

We call it Obscuro.

Below, you will find the Abstract of the paper.

The full draft whitepaper, including the pdf, can be found athttps://whitepaper.obscu.ro/.

The design of Obscuro ensures that hardware manufacturers do not have to be trusted for the safety of the ledger. If one manufacturer turns malicious or there is a breach in the TEE technology, the protocol falls back to the behavior of a public blockchain that preserves the ledger's integrity but makes the transactions public. This situation will lead to a partial liveness failure because the withdrawal function will be suspended.

The design also focuses on preserving privacy for the limited period when it matters most, which removes the need for a privacy technique that is robust against all adversaries in perpetuity.

Obscuro sits in what we believe is a sweet spot between the existing rollup-based L2 offerings: Optimistic and ZK Rollups. The use of confidential computing techniques coupled with economic incentives allows Obscuro to retain the performance and programming model simplicity of Optimistic rollups, and on top of that attain confidentiality, short withdrawal periods, and address MEV.

Other notable differentiators introduced by Obscuro:

- a new decentralised fair sequencing protocol called: "Proof of block inclusion" (POBI).
- a dependency mechanism between L2 rollup blocks and L1 blocks to achieve quick deposit periods.
- reasonable withdrawal delays, limited only by censorship resistance concerns.
- a transaction reveal mechanism configurable per smart-contract.
- support for the EVM.
- a novel incentive and fee mechanism.

We are very keen to get feedback from the Ethereum community.

I'd welcome any questions or discussion here.