Protocol

A user submits a Tx to a sequencer that

- part of the fields are known, e.g., sender

, gas price

, gas limit

, calldata

length

, nonce

are known, but to

address and the actual calldata

are unknown/hidden.

- the hidden fields are VDF-encoded - a sequencer can still decode the fields eventually, but it cannot decode it until computing the VDF for T_d

seconds.

- validity proof in ZK to prove that the Tx is valid such that 1. the signature is correct on the hash of the Tx including hidden ones; 2. the hidden ones can be decoded by the VDF.

When a sequencer receives such a Tx, it would

- (Validity check

) check the validity of the Tx via the ZK proof and make sure the sender

has sufficient ETH as gas

- (Sequence commitment

) if the Tx is valid (although some fields are still hidden at the time of submission), it will sign the Tx with an increasing sequence id, where the sequencer is committed to execute the Tx sequentially at the id.

- (Reveal hidden fields

) when a user receives the commitment from sequencer, it will reveal the hidden fields after T_r

seconds (or observed some numbers of other Txs are committed after the user's submission)

- (Liveness with VDF-Decoding

) if the sequencer does not receive the revealed fields from the user in T_r

seconds, it would try to decode the Tx via VDF.

Attacks

Malicious Sequencer

- If the sequencer does not execute the Tx in order (according to sequencer id), then the sequencer will be slashed by the protocol
- The sequencer may VDF decode the Txs to gain MEV before signing the Tx with the commitment. However, since the sequencer cannot tell the MEV values of a Tx, it means the sequencer has to decode all Txs and know the MEV after T_d

seconds, which could result in significant cost and low TPS.

Malicious Users

- After the sequencer signing and returning a sequence commitment of a Tx, a user may not reveal the hidden fields of

a Tx, trying to DDoS the sequencer. A way is to add a few incentive for the sequencer who decodes the hidden fields. Further, the sequencer may maintain a denylist for those users/addresses that frequently fail to reveal the hidden fields.