Thanks @qizhou for discussing the idea

TL;DR

- We can use the zk state channel to provide a zk fraud proof to resolve the disputes swiftly in the optimistic systems, such as opRollup (optimistic rollup) and opML (optimistic machine learning)
- We can construct a zk state channel using zkVM
- When the challenger can open a ZK state channel with the defender (sequencer/submitter) for dispute resolution, followed by uploading ZK proof onto the chain

Background

Current interactive fraud-proof challenge protocols such as Optimism fruad proof system uses

- binary search method to pinpoint the specific step or instruction where a discrepancy arises between the defender (submitter/sequencer) and the challenger.
- when the specific step of disagreement is found, a one-step on-chain executor is used to adjudicate whether the defender or challenger is correct.

Considering about 40+B steps (instructions) per block transition, the protocol will take about 36 interactions,

which is costly in both time and gas.

To reduce the number of interactions, umerous researchers have explored the use of Zero-Knowledge (zk) fraud-proof approaches (RFP: OP Stack Zero Knowledge Proof · Issue #61 · ethereum-optimism/ecosystem-contributions · GitHub). Many have experimented with utilizing zkVM as the fraud-proof virtual machine to generate zk proofs for either full-step or multi-step executions. With zk proofs for multi-step executions, the number of interactions can be significantly reduced (Almost Instant Interactive Fraud Proof using Multi-Sect on DA BLOBs and multi-step ZK verifier). If a zk proof for the full-step execution can be provided, the fraud-proof system operates akin to a zk proof system, eliminating the need for any interaction to resolve disputes. However, the cost of generating zk proofs for multi-step executions in zkVM remains substantial. Besides, in instances where a zk proof for the full-step execution cannot be provided, on-chain interaction for locating the dispute step remains necessary.

Proposal

- We can first construct a Zero-Knowledge (zk) state channel utilizing zkVM, where the zkVM will host the dispute game program.
- Upon a validator (challenger) initiating a challenge, they can establish a zk state channel with the defender (sequencer/submitter).
- Within this channel, the challenger and defender engage with the dispute game program hosted in zkVM, simulating the on-chain interaction typical of smart contracts. They employ binary search techniques to pinpoint the disputed step and subsequently utilize one-step on-chain execution to determine the correct party.
- Once the dispute resolution concludes, they can generate a zk proof encapsulating the entire process within zkVM, subsequently submitting it on-chain for arbitration.

[

zkChannel

926×690 34.3 KB

](https://ethresear.ch/uploads/default/original/2X/5/5072fa67ff17eb01526b11051b76dbcafba92952.png)

Advantages

- The proposed zk fraud-proof mechanism integrated with zk state channels dramatically reduces on-chain interactions to just two: one for channel initiation and another for closure, including zk proof submission. All other interactions occur off-chain and are cryptographically guaranteed by zk proofs.
- As interactions between the defender and the challenger occur off-chain, the frequency of engagement can be heightened, allowing for a more dynamic interaction rate. The number of checkpoints can also be greatly increased (2048+ can be easily achieved), and the number of interactions can no longer be limited.

- This approach is more cost-effective compared to generating zk proofs for full-step or multi-step executions within zkVM.

Security Concern

One potential concern with this proposal is the possibility of non-cooperation between challengers and defenders. To address this issue:

- We still retain the original on-chain interactive dispute game, allowing both defenders and challengers to close the zk state channel at any time. In scenarios where the channel is closed, yet the dispute remains unresolved, parties can resort to the on-chain interactive dispute game contract for resolution.
- We can design an incentive mechanism to encourage challengers and defenders to participate in the zk state channel. For instance, participants could face reduced penalties for losing the dispute game and receive larger bonuses for winning.

Conclusion

This proposal works like an auxiliary plugin for expediting dispute resolution. It does not compromise the security of the existing fraud-proof system but instead offers a cost-effective and swift solution for dispute resolution.