Onther Inc. came up with how to use EVM in plasma chain. Please review the approach they took. If you want explained version, you can check here.

Abstract

Plasma EVM is a new version of Plasma that can execute EVM in plasma chain. We propose state-enforceable Plasma construction to guarantee only valid state submitted to root chain, providing a way to enter and exit account storage between two chains because each chain has identical architecture.

2 Types of Block

There are 2 types of block in Plasma EVM. requestBlock

applies enter(deposit ERC20 or account storage) and exit request that users make in the RootChain contract. nonRequestBlock

is typical block we know, to transfer ETH or to incur message-call.

Request Block

If users deposit ERC20 to participate plasma, operator have to include those requests in the very next block, requestBlock

, to apply it to plasma chain. It can be considered as root chain enforces how the state should change. Exit can be applied in a similar way as enter does. If operator submits invalid blocks with invalid request, the challenge on it reverts the block. This makes only valid state committed to root chain.

Non-request Block

it contains all transactions not related to the enter & exit requests.

Enter & Exit

Enter & Exit mean moving a account's single storage variable in one chain onto a corresponding contract in another chain. A contract is requestable

if it can accept storage change by enter and exit requests.

Fraud Proof

There are many types of challenges. But the most important one is a challenge on the computation of EVM. TrueBit-like verification game provides a way to resolve validity of the computation. The game uses solevm, by Andreas Olofsson and PARSEC labs ,to verify EVM computation.

Block Withholding Attack

We may use CAS to enforce operator to submit block that all transactions are confirmed, but this approach cannot completely resolve the attak.