

ABSTRACT

METHOD FOR IMPLEMENTING LAYER 2 NETWORK ROLLUP, LAYER 2 NETWORK, AND PROVER

A method for implementing rollup of a layer 2 network is provided, where an executor and a prover in the layer 2 network are implemented by using trusted execution environments, and the method includes: pulling, by a sequencer of the layer 2 network, transactions from a transaction pool, sorting and batching the pulled transactions, reading an SPV proof of initial states/read sets obtained before batched transactions are executed to the prover, and sending the initial states/the read sets and the batched transactions to the executor; executing, by the executor, the batched transactions based on all the initial states/the read sets, generating a first signature for a generated write set by using a secret key of the executor, and sending the write set and the first signature to the prover; constructing, by the prover, a Merkle tree according to the SPV of the initial states/the read sets after verifying that the first signature succeeds, using a tree root as a pre-state root, updating the write set to a leaf node of the Merkle tree, updating a Merkle root, and using the updated Merkle root as a post-state root; and generating, by the prover, a second signature for the pre-state root and the post-state root by using a secret key of the prover, using the second signature as a proof, and sending, together with the pre-state root and the post-state root, the proof to a rollup contract on a mainnet through a second mainnet transaction.

Fig. 10