

ABSTRACT

METHOD FOR IMPLEMENTING ROLLUP OF LAYER 2 NETWORK AND LAYER 2 NETWORK

This specification provides a method for implementing rollup of a layer 2 network, including: pulling, by a sequencer of the layer 2 network, transactions from a transaction pool, sorting and batching the pulled transactions, generating a first transaction root of the batched transactions, executing the batched transactions sequentially based on initial states obtained before the batched transactions are executed, and generating a first post-state root; sending, by the sequencer, to a prover of the layer 2 network, the batched transactions, the first transaction root, the initial states obtained before the batched transactions are executed, and a first pre-state root and the first post-state root that correspond to the initial states, where the prover is implemented by using a trusted execution environment; and verifying, by the prover, the first transaction root and the first pre-state root; and executing the batched transactions sequentially based on the initial states after the first transaction root and the first pre-state root are verified successfully, generating a second post-state root, signing information of the batched transactions by using a secret key in the trusted execution environment after verifying that the second post-state root is equal to the first post-state root, using the signature as a proof, and sending the proof to a blockchain ledger of a mainnet by using a second mainnet transaction.

Fig. 5