

CLAIMS

1. A computer-implemented method for processing blockchain data under a trusted execution environment (TEE), the method comprising:

receiving, by a blockchain node, a request to execute a smart contract comprising one or more software instructions in a TEE executing on the blockchain node;

identifying, by a virtual machine in the TEE based on the request, data associated with one or more blockchain accounts related to the execution of the one or more software instructions of the smart contract;

in response to identifying the data associated with the one or more blockchain accounts, traversing, by the virtual machine, a global state of a blockchain stored in the TEE to locate the data associated with one or more blockchain accounts, wherein the global state of the blockchain stored in the TEE defines a relationship between a plurality of blockchain accounts of the blockchain and states of the plurality of blockchain accounts;

executing, by the virtual machine, the one or more software instructions of the smart contract based on the data, wherein the execution of the one or more software instructions of the smart contract comprises changes to at least one of plurality of blockchain accounts of the blockchain and the states of the plurality of blockchain accounts and wherein the global state of the blockchain stored in the TEE is updated during execution of the one or more software instructions to reflect the changes to the at least one of plurality of blockchain accounts of the blockchain and the states of the plurality of blockchain accounts and to produce an updated global state;

in response to executing the one or more software instructions, generating, by the blockchain node, an encrypted representation of the updated global state; and

storing, by the blockchain node, the encrypted representation of the updated global state in a storage location separate from the TEE.

2. The computer-implemented method of claim 1, wherein the request includes one or more input parameters and is made to an interface function of the TEE.

3. The computer-implemented method of any of the preceding claims, wherein the global state is stored in the TEE as a Merkle Patricia tree (MPT).

4. The computer-implemented method of claim 3, wherein the global state includes a mapping between addresses and states of a plurality of blockchain accounts of the blockchain, and the plurality of blockchain accounts include one or more of externally owned accounts or contract accounts, and wherein each of the contracts accounts includes a storage root.

5. The computer-implemented method of claim 4, wherein the storage root includes a hash of a root node of a Merkle Patricia tree (MPT), and wherein the MPT encodes a hash of storage content of a corresponding contract account.

6. The computer-implemented method of claim 5, wherein the updated global state is produced by updating the MPT that encodes the hash of the storage content of the corresponding contract account.

7. The computer-implemented method of any of the preceding claims, wherein the storage location separate from the TEE is associated with a cache or a database.

8. The computer-implemented method of any of the preceding claims, wherein the request is received through an application-programming interface associated with the TEE.

9. A system for processing blockchain data under a TEE, the system comprising: one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon which are executable by the one or more processors to perform the method of any of claims 1-8.

10. An apparatus for processing blockchain data under a TEE, the apparatus comprising a plurality of modules for performing the method of any one of claims 1-8.