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 one or more software instructions in a TEE executing on the blockchain node;

determining, by a virtual machine in the TEE, data associated with one or more blockchain accounts to execute the one or more software instructions based on the request, wherein the data associated with the one or more blockchain accounts are one or more key-value pairs (KVPs), and an internal cache hash table stores a plurality of KVPs associated with frequently accessed storage contents of a plurality of accounts of a blockchain;

traversing, by the virtual machine, the internal cache hash table stored in the TEE to determine whether the data are included in the internal cache hash table;

traversing, by the blockchain node, an external cache hash table through direct memory access to determine a first portion of KVPs that are included in the external cache hash table and a second portion of KVPs that are not included in the internal cache hash table;

in response to determining that the data is included in the internal cache hash table, executing, by the virtual machine, the one or more software instructions by retrieving the data from the internal cache hash table and by retrieving the second portion of KVPs from the external cache hash table, if the second portion of KVPs are included in the external cache hash table;

updating, by the virtual machine, the internal cache hash table in response to executing the one or more software instructions;

updating, by the blockchain node, the external cache hash table in response to executing the one or more software instructions; and

synchronizing, by the blockchain node, the external cache hash table with a global state of a blockchain stored in a database separate from the TEE and the internal cache hash table with the external cache hash table that comprises data associated with the one or more blockchain accounts, wherein the external cache hash table is stored in a cache memory separate from the TEE.

2. The computer-implemented method of claim 1, wherein the external cache hash table stores a plurality of KVPs associated with states and storage content of frequently accessed accounts of the blockchain.

3. The computer-implemented method of any of the preceding claims, further comprising:

executing, by the virtual machine, the one or more software instructions by retrieving the at least a portion of the one or more KVPs from the global state, if the second portion of KVPs are not included in the internal cache hash table or the external cache hash table; and

updating, by the blockchain node, the global state in response to executing the one or more software instructions.

4. The computer-implemented method of any of the preceding claims, wherein the global state is stored in the database outside of an enclave as a Merkle Patricia tree (MPT).

5. The computer-implemented method of any of the preceding claims, 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.

6. The computer-implemented method of claim 5, wherein the storage root includes a hash of a root node of an MPT, and wherein the MPT encodes hash of storage contents of the corresponding contract account.

7. A system for processing blockchain data under a TEE, 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 1-6.

11. 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 1-6.