

CLAIMS

1. A computer-implemented method of processing world state information associated with one or more blockchains, the method comprising:

providing a group world state that comprises a plurality of shards, in which each shard comprises one or more world states, each world state stores information about states of user accounts associated with the world state, and each shard is associated with a blockchain that comprises one or more blocks that store transaction data associated with the user accounts associated with the blockchain;

partitioning a first shard of the plurality of shards into a second shard and a third shard, wherein the first shard comprises a first blockchain database and a first world state database, the partitioning comprising:

generating a first snapshot of the first shard, in which the first snapshot includes a snapshot of the first blockchain database and a snapshot of the first world state database;

trimming the first shard to generate the second shard, including removing one or more world states in the first world state database of the first shard to generate a second world state database that includes a second subset of one or more world states in the first shard; and

trimming the first snapshot of the first shard to generate the third shard, including removing one or more world states in the first world state database in the first snapshot to generate a third world state database that includes a third subset of one or more world states in the first shard, in which the third subset of one or more world states is different from the second subset of one or more world states;

and

generating a root hash value of the group world state, in which the root hash value represents a digital fingerprint of states of the user accounts associated with the world states in the shards in the group world state.

2. The method of claim 1 in which each world state is maintained using at least one of a Merkle tree, a Patricia tree, a Merkle Patricia tree, a modified Merkle Patricia tree, or a Bucket tree.

3. The method of claim 1 in which the first shard is associated with a first set of user accounts, the second shard is associated with a second set of user accounts, the third shard is associated with a third set of user accounts, the second set of user accounts is a second subset of the first set of user accounts, the third set of user accounts is a third subset of the first set of user accounts, and the third subset of the first set of user accounts is different from the second subset of the first set of user accounts.
4. The method of any one of claims 1 to 3, comprising associating user accounts with the world states based on a characteristic of the user accounts, in which each user account is associated with only one of the world states.
5. The method of claim 4 in which the user accounts are associated with the world states based on characteristics of user account identifiers.
6. The method of claim 5 in which the user accounts are associated with the world states based on predetermined bytes or byte words of the user account identifiers.
7. The method of claim 6 in which the group world state supports a maximum of 2^n world states, and a user account whose user account identifier has the predetermined bytes or byte words equal to m is associated with an m -th world state, $1 \leq m \leq 2^n$.
8. The method of claim 7 in which the group world state supports a maximum of $2^{16} = 65,536$ world states, and a user account whose user account identifier has first two byte words equal to m is associated with the m -th world state, $1 \leq m \leq 65,536$.
9. The method of claim 4 in which the user accounts are associated with the world states based on priority levels of user accounts.
10. The method of claim 3 in which the first world state database is associated with the first set of user accounts, the second world state database is associated with a second set of user accounts, the third world state database is associated with a third set of user accounts, and the first set of user accounts comprises a sum of the second set of user accounts and the third set of user accounts.

11. The method of claim 10 in which the second set of user accounts does not overlap the third set of user accounts.
12. The method of any one of claims 1 to 11 in which generating the first snapshot of the first shard comprises using a virtual machine associated with the first shard to generate the first snapshot of the first shard.
13. The method of any one of claims 1 to 12 in which the first blockchain database comprises a first blockchain managed by a first blockchain network, and the first blockchain network comprises a consensus blockchain network that comprises validating peer nodes that participate in a consensus process for determining whether to write data on the first blockchain and non-validating peer nodes that do not participate in the consensus process, and
generating the first snapshot of the first shard comprises using the non-validating peer nodes to generate the first snapshot.
14. The method of claim 13
comprising increasing a number of the validating peer nodes, and using the validating peer nodes to generate the first snapshot of the first shard.
15. The method of any one of claims 1 to 14 in which each world state in the plurality of world states of the first world state database comprises a root node, the first blockchain of the first blockchain database comprises a first block, the first block comprises a block header and a block body, the block header stores a first hash value derived from a hash of hash values of the root nodes of the plurality of world states of the first world state database, and the first hash value represents a digital fingerprint of the current states of the user accounts associated with the plurality of world states of the first world state database.
16. The method of any one of claims 1 to 14 in which each world state in the plurality of world states of the first world state database comprises a root node, the first blockchain of the first blockchain database comprises a first block, the first block comprises a block header and a block body, and the block header stores hash values of the root nodes of the world states in the first world state database.

17. The method of claim 15 or 16, in which the second shard comprises a second blockchain database that comprises a second blockchain that stores transaction data associated with user accounts that are associated with the second shard, the second blockchain comprises a first block, the first block of the second blockchain comprises a block body that stores information about transactions, and trimming the first shard comprises removing information about transactions associated with user accounts that are not associated with the second subset of the one or more world states in the second world state database.

18. The method of any one of claims 15 to 17, in which the third shard comprises a third blockchain database that comprises a third blockchain that stores transaction data associated with user accounts that are associated with the third shard, the third blockchain comprises a first block, the first block of the third blockchain comprises a block body that stores information about transactions, and trimming the first snapshot of the first shard comprises removing information about transactions associated with user accounts that are not associated with the third subset of one or more world states in the third world state database.

19. The method of any one of claims 1 to 18 in which the third shard comprises a third blockchain database that comprises a third blockchain that stores transaction data associated with user accounts that are associated with the third shard,

the method comprises partitioning the third shard into a fourth shard and a fifth shard, comprising:

generating a second snapshot of the third shard, in which the second snapshot includes a snapshot of the third blockchain database and a snapshot of the third world state database;

trimming the third shard to generate the fourth shard, including removing one or more world states in the third world state database of the third shard to generate a fourth world state database that includes a fourth subset of one or more world states in the third shard; and

trimming the second snapshot of the third shard to generate the fifth shard, including removing one or more world states in the third world state database in the second snapshot to generate a fifth world state database that includes a fifth subset of one or more world states in the third shard, in which the fifth subset of the one or more world states is different from the fourth subset of the one or more world states.

20. The method of any one of claims 1 to 19 in which each world state is maintained using a digital tree comprising at least one of a Merkle tree, a Patricia tree, a Merkle Patricia tree, a modified Merkle Patricia tree, or a Bucket tree.

21. The method of claim 20, comprising generating a group world state hash value representing the world states of the first and second shards based on hash values of root nodes of the digital trees maintaining the world states of the first and second shards.

22. The method of claim 21, comprising generating a simplified payment verification proof of a transaction associated with a user account by generating a first proof based on a path from a root node of a group world state to a root node of a sharding world state, generating a second proof based on a path from the root node of the sharding world state to a root node of a world state associated with the user account, and generating a third proof based on a path from the root node of the world state to a node representing the user account.

23. A 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 that are executable by the one or more processors to perform the method of any of claims 1 to 22.

24. An apparatus comprising a plurality of modules for performing the method of any of claims 1 to 22.