

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;
 - dynamically modifying a number of shards in the group world state based on one or more criteria, including at least one of (i) partitioning one of the shards into two or more shards, (ii) merging two or more shards into one shard, (iii) adding one or more new shards to the group world state, or (iv) removing one or more shards from the group world state; 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 dynamically modifying a number of shards in the group world state based on one or more criteria comprises partitioning a first shard into a second shard and a third shard, the second shard includes a second subset of world states of the first shard, and the third shard includes a third subset of world states of the first shard.
3. The method of claim 1 in which dynamically modifying a number of shards in the group world state based on one or more criteria comprises merging a second shard and a third shard to generate a first shard, in which the first shard includes one or more world states of the second shard and one or more world states of the third shard.
4. The method of any one of claims 1 to 3 in which dynamically modifying a number of shards in the group world state based on one or more criteria comprises adding one or more new shards to the group world state, in which the one or more new shards include one or more world states that were previously not included in the group world state.
5. The method of any one of claims 1 to 4 in which dynamically modifying a number of shards in the group world state based on one or more criteria comprises removing one or

more shards from the group world state, including removing one or more world states in the one or more shards removed from the group world state.

6. The method of any one of claims 1 to 5, comprising at a system comprising one or more computers in one or more locations, evaluating the one or more criteria, and partitioning one of the shards into two or more shards upon determining that the one or more criteria are met.

7. The method of any one of claims 1 to 6, comprising at a system comprising one or more computers in one or more locations, evaluating the one or more criteria, and merging two or more shards into one shard upon determining that the one or more criteria are met.

8. The method of any one of claims 1 to 7, comprising dynamically modifying resources allocated to the group world state based on the number of shards in the group world state.

9. The method of claim 8, comprising allocating more resources to the group worlds state in response to an increase in the number of shards in the group world state.

10. The method of claim 8 or 9, comprising allocating fewer resources to the group world state in response to a decrease in the number of shards in the group world state.

11. The method of any one of claims 8 to 10 in which the resources comprise at least one of computation power, memory, data storage capacity, or data bandwidth.

12. The method of any one of claims 1 to 11 in which the one or more criteria comprise at least one of quality of service measure, computation power requirement, memory capacity requirement, data storage capacity requirement, or data bandwidth requirement.

13. The method of claim 12, comprising determining at least one of (i) the quality of service measure is below a threshold, (ii) the computation power requirement is not met, (iii) the memory capacity requirement is not met, (iv) the data storage capacity requirement is not met, or (v) the data bandwidth requirement is not met,

in response to the determination, partitioning one of the shards into two or more shards, and

allocating more resources to a combination of the two or more shards, as compared to the resources allocated to the one of the shards, in which the resources comprise at least one of computation power, memory capacity, data storage capacity, or data bandwidth.

14. The method of claim 12 or 13, comprising determining that at least one of (i) the quality of service measure is above a threshold, (ii) idle or excess computation power is above a threshold, (iii) available memory capacity is above a threshold, (iv) available data storage capacity is above a threshold, or (v) available data bandwidth is above a threshold,

in response to the determination, merging two or more shards into a single shard, and allocating fewer resources to the single shard after the merging, as compared to the resources allocated to the two or more shards before the merging, in which the resources comprise at least one of computation power, memory capacity, data storage capacity, or data bandwidth.

15. The method of any one of claims 1 to 14 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.

16. The method of any one of claims 1 to 15 in which partitioning one of the shards into two or more shards comprises partitioning a first shard into a second shard and a third shard, the first shard comprising a first world state database that comprises a first set of world states, the partitioning of the first shard into the second shard and the third shard comprising:

generating a first snapshot of the first shard, in which the first snapshot includes a snapshot of a 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 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 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.

17. The method of any one of claims 1 to 16 in which partitioning one of the shards into two or more shards comprises partitioning one of the shards into three or more shards.
18. The method of any one of claims 1 to 17 in which merging two or more shards into one shard comprises merging a second shard and a third shard into a first shard,
the second shard comprises a second world state database that comprises a second set of world states that stores state information associated with a second set of user accounts,
the third shard comprises a third world state database that comprises a third set of world states that stores state information associated with a third set of user accounts,
the first shard comprises a first world state database that comprises a first set of world states that includes the second set of world states and the third set of world states, the first set of world states stores state information associated with a first set of user accounts that includes the second set of user accounts and the third set of user accounts.
19. The method of any one of claims 1 to 18 in which partitioning one of the shards into two or more shards comprises partitioning a first shard into a second shard and a third shard, 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.
20. The method of any one of claims 1 to 19, 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.
21. The method of claim 20 in which the user accounts are associated with the world states based on characteristics of user account identifiers.
22. The method of claim 21 in which the user accounts are associated with the world states based on predetermined bytes or byte words of the user account identifiers.

23. The method of claim 22 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, $1 \leq m \leq 2^n$.
24. The method of claim 23 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, $1 \leq m \leq 65,536$.
25. The method of claim 20 in which the user accounts are associated with the world states based on priority levels of user accounts.
26. The method of any one of claims 1 to 24, comprising providing a first set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be increased.
27. The method of any one of claims 1 to 26, comprising providing a second set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be decreased.
28. A computer-implemented method of processing world state information associated with one or more blockchains, the method comprising:
- providing a first shard that is associated with a first set of user accounts, in which the first shard comprises a first blockchain database and a first world state database, the first blockchain database comprises a first blockchain managed by a first blockchain network in which blockchain data are stored on the first blockchain through consensus of blockchain nodes of the first blockchain network, the first world state database comprises a plurality of world states, each world state is associated with a plurality of user accounts, and each world state stores current states of the user accounts associated with the world state; and
 - partitioning the first shard into a second shard and a third shard, 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.

29. The method of claim 28, comprising allocating more resources to a combination of the second shard and the third shard as compared to the resources allocated to the first shard after the partitioning of the first shard into the second shard and the third shard.

30. The method of claim 28 or 29 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.

31. The method of any one of claims 28 to 30 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 second set of user accounts does not overlap the third set of user accounts.

32. The method of any one of claims 29 to 31 in which allocating more resources comprises allocating more of at least one of computation power, memory, data storage capacity, or data bandwidth.

33. The method of any one of claims 28 to 32 in which generating the snapshot of the first shard comprises using a virtual machine associated with the first shard to generate the snapshot of the first shard.

34. The method of any one of claims 28 to 33 in which 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 snapshot of the first shard comprises using the non-validating peer nodes to generate the snapshot.

35. The method of claim 34 in which the consensus blockchain network 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 snapshot of the first shard comprises increasing a number of validating peer nodes, and using the validating peer nodes to generate the snapshot.

36. The method of any one of claims 28 to 35 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.

37. The method of any one of claims 28 to 35 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.

38. The method of claim 36 or 37, 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.

39. The method of any one of claims 36 to 38, 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.

40. The method of any one of claims 28 to 39 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.

41. The method of claim 40, comprising allocating more resources to a combination of the fourth shard and the fifth shard as compared to the resources allocated to the third shard.

42. The method of any one of claims 28 to 41 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.

43. The method of claim 42, 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.

44. The method of claim 43, 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.

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

providing a first shard of a blockchain ledger in which the first shard comprises a first blockchain database and a first world state database, the first world state database comprises a plurality of world states, and each world state stores current states of user accounts associated with the world state;

generating a first copy of the first shard including a copy of the first blockchain database and a copy of the first world state database;

generating a second shard by removing one or more world states in the first world state database of the first shard, in which a second subset of one or more world states in the first shard remains in the second shard; and

generating a third shard by removing one or more world states in the first world state database in the first copy of the first shard, in which a third subset of one or more world states in the first shard remains in the third shard, and the third subset of one or more world states is different from the second subset of one or more world states.

46. The method of claim 45, comprising allocating more resources to a combination of the second shard and the third shard as compared to the resources allocated to the first shard.

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

partitioning a plurality of user accounts into at least a first set of user accounts and a second set of user accounts;

associating a first blockchain database and a first world state database with the first set of user accounts, in which the first blockchain database comprises a first blockchain managed by a first blockchain network in which blockchain data are stored on the first blockchain through consensus of blockchain nodes of the first blockchain network, the first world state database comprises a plurality of world states, each world state is associated with a subset of the first set of user accounts, and each world state stores current states of the user accounts associated with the world state;

associating a second blockchain database and a second world state database with the second set of user accounts, in which the second blockchain database comprises a second blockchain managed by a second blockchain network in which blockchain data are stored on the second blockchain through consensus of blockchain nodes of the second blockchain network, the second world state database comprises a plurality of world states, each world state is associated with a subset of the second set of user accounts, and each world state stores current states of the user accounts associated with the world state;

generating a first hash value representing a digital fingerprint of the world states of the first world state database, in which the first hash value is generated based on root hash values of each world state in the first world state database;

generating a second hash value representing a digital fingerprint of the world states of the second world state database, in which the second hash value is generated based on the root hash values of each world state in the second world state database;

at a block header of a first block of the first blockchain, storing the first hash value;

at a block header of a first block of the second blockchain, storing the second hash value; and

generating a group world state root hash value representing a digital fingerprint of the world states of the first and second world state databases, in which the group world state root hash value is generated based on the first hash value and the second hash value.

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

partitioning a plurality of user accounts into at least a first set of user accounts and a second set of user accounts;

associating the first set of user accounts with a first blockchain database and a first world state database, in which the first blockchain database stores a first blockchain that stores transaction data associated with the first set of user accounts, the first world state database comprises a plurality of world states, and each world state is associated with a subset of the first set of user accounts;

associating the second set of user accounts with a second blockchain database and a second world state database, in which the second blockchain database stores a second blockchain that stores transaction data associated with the second set of user accounts, the second world state database comprises a plurality of world states, and each world state is associated with a subset of the second set of user accounts;

at a block header of a first block of the first blockchain, storing a first hash value that represents a digital fingerprint of the world states in the first world state database;

at a block header of a first block of the second blockchain, storing a second hash value that represents a digital fingerprint of the world states in the second world state database; and

generating a group world state root hash value that represents a digital fingerprint of the world states in the first and second world state databases based on the first hash value and the second hash value.

49. 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 a world state database, the world state database comprises a plurality of world states, each world state stores information about states of user accounts associated with the world state, each shard is associated with a blockchain database that comprises a blockchain that comprises one or more blocks that store transaction data associated with the user accounts associated with the blockchain;

wherein a first shard of the plurality of shards comprises a first world state database that comprises a first set of world states that stores state information about a first set

of user accounts, a second shard of the plurality of shards comprises a second world state database that comprises a second set of world states that stores state information about a second set of user accounts; and

merging the first shard and the second shard to generate a third shard, including merging the first world state database and the second world state database to generate a third world state database that includes a third set of world states that includes the first set of world states and the second set of world states, in which the third set of world states stores state information about the first set of user accounts and the second set of user accounts.

50. The method of claim 49 in which each world state is maintained using a digital tree, the first set of world states is maintained using a first set of digital trees, the second set of world states is maintained using a second set of digital trees, and the third set of world states is maintained using a third set of digital trees that comprises the first set of digital trees and the second set of digital trees.

51. The method of claim 50 in which each digital tree comprises at least one of a Merkle tree, a Patricia tree, a Merkle Patricia tree, a modified Merkle Patricia tree, or a Bucket tree.

52. The method of any one of claims 49 to 51, comprising determining that the first shard was generated by a partition process that includes generating a snapshot of a fourth shard, trimming the fourth shard or the snapshot of the fourth shard to generate the first shard, and waiting for the trimming of the fourth shard or the snapshot of the fourth shard to be completed before merging the first shard and the second shard.

53. The method of any one of claims 49 to 52, comprising allocating fewer resources to the third shard as compared to the resources allocated to a combination of the first shard and the second shard.

54. The method of claim 53 in which the resources comprise at least one of computation power, memory, data storage capacity, or data bandwidth.

55. The method of any one of claims 49 to 54 in which the first shard is associated with a first blockchain database that comprises a first blockchain that stores transaction data associated with the first set of user accounts, the second shard is associated with a second

blockchain database that comprises a second blockchain that stores transaction data associated with the second set of user accounts, and the method comprises:

merging the first blockchain database and the second blockchain database to generate a third blockchain database that comprises a third blockchain that stores transaction data associated with the first set of user accounts and the second set of user accounts.

56. The method of claim 55 in which the third blockchain comprises a first block that stores information indicating that the third blockchain is generated by merging at least two blockchains.

57. The method of claim 55 or 56 in which the first blockchain database comprises a first data structure to facilitate searching of data in the first blockchain, the second blockchain database comprises a second data structure to facilitate searching of data in the second blockchain, and the third blockchain database comprises the first data structure and the second data structure to facilitate searching of data in the third blockchain database.

58. The method of any one of claims 55 to 57 in which the first blockchain database stores a first root hash value for the first set of world states, the second blockchain database stores a second root hash value for the second set of world states, and the third blockchain database stores a third root hash for the third set of world states.

59. 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 a world state database, the world state database comprises a plurality of 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 database that comprises a blockchain that comprises one or more blocks that store transaction data associated with the user accounts associated with the blockchain;

wherein a first shard of the plurality of shards of the group world state comprises a first world state database;

generating an intermediate shard by generating a snapshot of the first shard;

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

removing one or more world states in the intermediate shard to generate a third shard 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.

60. The method of claim 59, comprising allocating more resources to a combination of the second shard and the third shard as compared to the resources allocated to the first shard.

61. 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;

dynamically modifying a number of shards in the group world state based on a result of a comparison of consensus processing at a first consensus node and consensus processing at one or more other consensus nodes; and

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

62. The method of claim 61 in which dynamically modifying a number of shards in the group world state comprises at least one of (i) partitioning one of the shards into two or more shards, (ii) merging two or more shards into one shard, (iii) adding one or more new shards to the group world state, or (iv) removing one or more shards from the group world state.

63. The method of claim 61 in which dynamically modifying a number of shards in the group world state comprises increasing the number of shards in the group world state if the consensus processing at the first consensus node is slower than the consensus processing at one or more other consensus nodes by a first threshold.

64. The method of claim 61 in which dynamically modifying a number of shards in the group world state comprises decreasing the number of shards in the group world state if the

consensus processing at the first consensus node is faster than the consensus processing at one or more other consensus nodes by a second threshold.

65. The method of any of claims 61 to 63, comprising providing a first set of one or more rules that specify one or more conditions for which the number of shards in the group world state is to be increased.

66. The method of any one of claims 61, 62, or 64, comprising providing a second set of one or more rules that specify one or more conditions for which the number of shards in the group world state is to be decreased.

67. The method of any one of claims 61 to 66, comprising determining a first speed of consensus processing at the first consensus node,
determining a second speed of consensus processing at one or more other consensus nodes;
comparing the first speed of consensus processing at the first consensus node and the second speed of consensus processing at the one or more other consensus nodes; and
generating the result of the comparing of the consensus processing at the first consensus node and the consensus processing at the one or more other consensus nodes.

68. 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 67.

69. An apparatus comprising a plurality of modules for performing the method of any of claims 1 to 67.

70. A system for processing world state information associated with one or more blockchains, the system comprising:
a blockchain-based application module configured to provide a service to users associated with user accounts;

a blockchain ledger comprising at least one blockchain and a group world state that comprises a plurality of shards, in which each shard comprises a world state database, the world state database comprises a plurality of world states, each world state is configured to store information about states of user accounts associated with the world state, each shard is associated with a blockchain database that comprises a blockchain that comprises one or more blocks that store transaction data associated with the user accounts associated with the blockchain; and

a blockchain ledger modification module configured to dynamically modify a number of shards in the group world state based on one or more criteria, including at least one of (i) partition one of the shards into two or more shards, (ii) merge two or more shards into one shard, (iii) add one or more new shards to the group world state, or (iv) remove one or more shards from the group world state.

71. The system of claim 70, comprising a root hash generation module configured to generate a root hash value of the group world state based on root hash values of the world states in the group world state.

72. The system of claim 70 or 71, comprising a rule set database comprising a first set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be increased.

73. The system of any one of claims 70 to 72, comprising a rule set database comprising a second set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be decreased.

74. A system for processing world state information associated with one or more blockchains, the system comprising:

a blockchain-based application module configured to provide a service to users associated with user accounts;

a blockchain ledger comprising at least one blockchain and a group world state that comprises a plurality of shards, in which each shard comprises a world state database, the world state database comprises a plurality of world states, each world state is configured to store information about states of user accounts associated with the world state, each shard is associated with a blockchain database that comprises a blockchain that comprises one or

more blocks that store transaction data associated with the user accounts associated with the blockchain; and

a blockchain ledger modification module configured to dynamically modify a number of shards in the group world state based on a result of a comparison of consensus processing at the system and consensus processing at one or more other consensus nodes.

75. The system of claim 74 in which the blockchain ledger modification module is configured to dynamically modify a number of shards in the group world state, including at least one of (i) partitioning one of the shards into two or more shards, (ii) merging two or more shards into one shard, (iii) adding one or more new shards to the group world state, or (iv) removing one or more shards from the group world state.

76. The system of claim 74 or 75, comprising a rule set database comprising a first set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be increased.

77. The system of any one of claims 74 to 76, comprising a rule set database comprising a second set of one or more rules that specify one or more conditions for which a number of shards in the group world state is to be decreased.