

CLAIMS

What is claimed is:

1. A method of spending a digitally-represented economic value in a target distributed ledger where the digitally-represented economic value originates in a source distributed ledger and is owned by an entity, the method comprising:

determining an existing transaction in the source distributed ledger which has a transaction output that is unspent and owned by the entity;

constructing and submitting an initiating transaction for commission to the target distributed ledger, wherein the initiating transaction has a transaction output;

constructing and submitting a locking transaction for commission to the source distributed ledger, wherein the locking transaction spends and locks the transaction output of the existing transaction in the source distributed ledger and references the initiating transaction in the target distributed ledger; and

constructing and submitting a completing transaction for commission to the target distributed ledger, wherein the completing transaction spends the transaction output of the initiating transaction in the target distributed ledger and references the locking transaction in the source distributed ledger.

2. The method of claim 1, wherein the transaction output of the initiating transaction is only spendable by the completing transaction when the completing transaction references the locking transaction and when a value of the transaction output of the initiating transaction matches a value of the transaction output of the existing transaction.

3. The method of claim 2, wherein the locking transaction uses a Merkle tree reference to reference the initiating transaction.

4. The method of claim 3, wherein the completing transaction uses a Merkle tree reference to reference the locking transaction.

5. The method of claim 1, wherein the method is performed by a node-stack of the source distributed ledger.

6. The method of claim 5, wherein the initiating and completing transactions are submitted to a node-stack of the target distributed ledger, and the node-stack of the target distributed ledger further submits the initiating and completing transactions to the target distributed ledger.

7. The method of claim 1, wherein the method is performed by a node-stack of the target distributed ledger.

8. The method of claim 7, wherein the locking transaction is submitted to a node-stack of the source distributed ledger, and the node-stack of the source distributed ledger further submits the locking transaction to the source distributed ledger.

9. The method of claim 1, wherein the method is performed in a system that comprises:

a plurality of distributed ledger networks, each said distributed ledger network having a plurality of nodes and communicative connections therebetween; and

internetwork connections between the plurality of distributed ledger networks,

wherein a distributed ledger network that maintains a local distributed ledger includes a plurality of foreign payment verification nodes for other distributed ledgers in the system.

10. The method of claim 1, wherein the method is performed in a system that comprises:

a plurality of distributed ledger networks, each said distributed ledger network having a plurality of nodes and internetwork connections therebetween; and

a set of nodes that are shared by the plurality of distributed ledger networks, wherein nodes in the set provide, among other services, inter-ledger verification of transactions.

11. A non-transitory tangible computer-readable medium comprising instructions stored thereon, that when executed by a processor, perform the steps of:

determining an existing transaction in a source distributed ledger which has a transaction output that is unspent and owned by an entity;

constructing and submitting an initiating transaction for commission to a target distributed ledger, wherein the initiating transaction has a transaction output;

constructing and submitting a locking transaction for commission to the source distributed ledger, wherein the locking transaction spends and locks the transaction output of the existing transaction in the source distributed ledger and references the initiating transaction in the target distributed ledger; and

constructing and submitting a completing transaction for commission to the target distributed ledger, wherein the completing transaction spends the transaction output of the initiating transaction in the target distributed ledger and references the locking transaction in the source distributed ledger.

12. The computer-readable medium of claim 11, wherein the transaction output of the initiating transaction is only spendable by the completing transaction when the completing transaction references the locking transaction and when a value of the transaction output of the initiating transaction matches a value of the transaction output of the existing transaction.

13. The computer-readable medium of claim 12, wherein the locking transaction uses a Merkle tree reference to reference the initiating transaction.

14. The computer-readable medium of claim 13, wherein the completing transaction uses a Merkle tree reference to reference the locking transaction.

15. The computer-readable medium of claim 11, wherein the instructions are performed by a node-stack of the source distributed ledger.

16. The computer-readable medium of claim 11, wherein the instructions are performed by a node-stack of the target distributed ledger.

17. A method of transferring a digitally-represented amount of currency in an unspent transaction output of an existing transaction in a source blockchain to one or more transaction outputs which spend the digitally-represented amount of currency in a target blockchain, the method comprising:

constructing and submitting an initiating transaction for commission to the target blockchain, wherein the initiating transaction has the unspent transaction output which comprises the digitally-represented amount of currency;

constructing and submitting a locking transaction for commission to the source blockchain, wherein the locking transaction spends and locks the transaction output of the existing transaction in the source blockchain and references the initiating transaction in the target blockchain; and

constructing and submitting a completing transaction for commission to the target blockchain, wherein the completing transaction references the locking transaction in the source blockchain, and wherein the completing transaction comprises said one or more transaction outputs which spend the digitally-represented amount of currency in the target blockchain.

18. The method of claim 17, wherein the transaction output of the initiating transaction is only spendable by the completing transaction when the completing transaction references the locking transaction and when a value of the transaction output of the initiating transaction matches a value of the transaction output of the existing transaction

19. The method of claim 18, wherein the locking transaction uses a Merkle tree reference to reference the initiating transaction.

20. The method of claim 19, wherein the completing transaction uses a Merkle tree reference to reference the locking transaction.

21. The method of claim 1, wherein the distributed ledger comprises a blockchain.

22. The method of claim 1, wherein the distributed ledger utilizes a directed acyclic graph.

23. The computer-readable medium of claim 11, wherein the distributed ledger comprises a blockchain.

24. The computer-readable medium of claim 11, wherein the distributed ledger utilizes a directed acyclic graph.

25. A system with cross-ledger transfers between multiple distributed ledgers for highly-scalable transaction throughput, the system comprising:

a plurality of distributed ledger networks, each said distributed ledger network maintaining a local distributed ledger and comprising local nodes and communicative connections therebetween;

internetwork connections between the plurality of distributed ledger networks;
and

foreign payment verification nodes co-located with the local nodes of each said distributed ledger network, wherein the foreign payment verification nodes are used in a cross-ledger transfer for inter-ledger verification of transactions in other distributed ledger networks in the system.

26. The system of claim 25, further comprising, at each said foreign payment verification node:

a block header/signature chain that includes block headers and block signatures for a foreign distributed ledger.

27. The system of claim 25, further comprising, at each said payment verification node:

an index of block hashes to the block headers in the block header/signature chain.

28. The system of claim 25, wherein an existing transaction in a source distributed ledger contains a transaction output whose digitally-represented economic value is to be transferred to a target distributed ledger.

29. The system of claim 28, wherein inter-ledger verification comprises verifying existence of a locking transaction in the source distributed ledger, and wherein the locking transaction spends the transaction output of the existing transaction.

30. The system of claim 29, wherein verification of the existence of the locking transaction in the source distributed ledger is necessary for a completing transaction in

the target distributed ledger to spend a transaction output of an initiating transaction in the target distributed ledger.

31. The system of claim 25, wherein said co-location of the local node and the foreign payment verification nodes is implemented by a computer apparatus with one or more processors that includes a local node-stack of the local distributed ledger and foreign payment verification node-stacks of the other distributed ledgers in the system.

32. A system with cross-ledger transfers between a plurality of distributed ledgers for highly-scalable transaction throughput, the system comprising:

a plurality of distributed ledger networks, each said distributed ledger network maintaining a local distributed ledger and comprising local nodes and communicative connections therebetween; and

a set of shared nodes, wherein each said shared node comprises local nodes for at least two distributed ledger networks of the plurality of distributed ledger networks.

33. The system of claim 32, further comprising, at each said shared node:

an index of block hashes to block headers for each of the plurality of distributed ledgers.

34. The system of claim 32, wherein each said shared node comprises a computer apparatus which comprises local node-stacks of said at least two distributed ledger networks.

35. The system of claim 32, wherein each said shared node comprises local nodes for all of the plurality of distributed ledger networks.

36. The system of claim 35, wherein each said shared node comprises a computer apparatus which comprises local node-stacks of all of the plurality of distributed ledger networks.

37. The system of claim 32, wherein an existing transaction in a source distributed ledger contains a transaction output whose digitally-represented economic value is to be transferred to a target distributed ledger.

38. The system of claim 37, wherein a locking transaction spends the transaction output of the existing transaction, and wherein verification of the existence of the locking transaction in the source distributed ledger is necessary for a completing transaction in the target distributed ledger to spend a transaction output of an initiating transaction in the target distributed ledger.

39. A system with cross-ledger transfers between a plurality of distributed ledgers for highly-scalable transaction throughput, the system comprising:

a set of computer apparatus, each said computer apparatus comprising memory for holding computer-readable code and data and one or more processors for executing said computer-readable code so as to modify said data;

communicative connections between each said computer apparatus and a plurality of distributed ledger networks; and

computer-readable code for local node-stacks of the plurality of distributed ledger networks at each said computer apparatus.

40. The system of claim 39, further comprising, at each said computer apparatus:

an index of block hashes to block headers for each of the plurality of distributed ledgers.

41. The system of claim 39, wherein an existing transaction in a source distributed ledger contains a transaction output whose digitally-represented economic value is to be transferred to a target distributed ledger.

42. The system of claim 41, wherein a locking transaction spends the transaction output of the existing transaction, and wherein verification of the existence of the locking transaction in the source distributed ledger is necessary for a completing transaction in the target distributed ledger to spend a transaction output of an initiating transaction in the target distributed ledger.

43. The system of claim 39, wherein the distributed ledger comprises a blockchain.

44. The system of claim 39, wherein the distributed ledger utilizes a directed acyclic graph.

45. The system of claim 25, wherein the distributed ledger comprises a blockchain.
46. The system of claim 25, wherein the distributed ledger utilizes a directed acyclic graph.
47. The system of claim 32, wherein the distributed ledger comprises a blockchain.
48. The system of claim 32, wherein the distributed ledger utilizes a directed acyclic graph.
49. A computer apparatus for cross-ledger transfers between a plurality of distributed ledgers, the computer apparatus comprising:
- memory for holding computer-readable code and data;
 - one or more processors for executing said computer-readable code so as to modify said data;
 - computer-readable code for a local node-stack for a target distributed ledger of the plurality of distributed ledgers; and
 - computer-readable code for a foreign payment verification node-stack for a source distributed ledger of the plurality of distributed ledgers,
- wherein the local node-stack is configured to use the foreign payment verification node-stack to verify transactions in the source distributed ledger during a cross-ledger transfer of a digitally-represented economic value between the target and source distributed ledgers.
50. The computer apparatus of claim 49, further comprising, at the foreign payment verification node-stack:
- a block header/signature chain that includes block headers and block signatures for the source distributed ledger.
51. The computer apparatus of claim 50, further comprising, at the foreign payment verification node-stack:
- an index of block hashes to the block headers in the block header/signature chain.

52. The computer apparatus of claim 49, wherein an existing transaction in the source distributed ledger contains a transaction output which has the digitally-represented economic value for the cross-ledger transfer.

53. The computer apparatus of claim 52, wherein the local node-stack is configured to construct a locking transaction which spends and locks the digitally-represented economic value of the transaction output of the existing transaction such that the digitally-represented economic value cannot be further spent in the source distributed ledger.

54. The computer apparatus of claim 53, wherein the locking transaction comprises at least one intra-ledger transaction input, one cross-ledger reference transaction input, and zero or more transaction outputs.

55. The computer apparatus of claim 53, wherein the local node-stack is required, prior to constructing a completing transaction which spends a transaction output of an initiating transaction in the target distributed ledger, to verify existence of the locking transaction in the source distributed ledger and match a value of the transaction output of the initiating transaction against the value spent by the locking transaction.

56. The computer apparatus of claim 55, wherein the initiating transaction comprises no transaction inputs and one transaction output.

57. The computer apparatus of claim 55, wherein the completing transaction comprises one intra-ledger transaction input, one cross-ledger reference transaction input, and one or more transaction outputs.

58. A computer apparatus for cross-ledger transfers between a plurality of distributed ledgers, the computer apparatus comprising:

memory for holding computer-readable code and data;

one or more processors for executing said computer-readable code so as to modify said data; and

computer-readable code for node-stacks of the plurality of distributed ledgers,

wherein each said node-stack is configured to perform a cross-ledger transfer of a digitally-represented economic value from a source distributed ledger to a target distributed ledger.

59. The computer apparatus of claim 58, further comprising:

an index of block hashes to block headers for each of the plurality of distributed ledgers.

60. The computer apparatus of claim 58, wherein an existing transaction in the source distributed ledger contains a transaction output whose digitally-represented economic value is to be transferred to the target distributed ledger.

61. The computer apparatus of claim 60, wherein a locking transaction spends and locks the transaction output of the existing transaction.

62. The computer apparatus of claim 61, wherein the locking transaction comprises at least one intra-ledger transaction input, one cross-ledger reference transaction input, and zero or more transaction outputs.

63. The computer apparatus of claim 61, wherein verification of the existence of the locking transaction in the source distributed ledger is necessary for a completing transaction in the target distributed ledger to spend a transaction output of an initiating transaction in the target distributed ledger.

64. The computer apparatus of claim 63, wherein the initiating transaction comprises no transaction inputs and one transaction output.

65. The computer apparatus of claim 63, wherein the completing transaction comprises one intra-ledger transaction input, one cross-ledger reference transaction input, and one or more transaction outputs.

66. An apparatus for cross-ledger transfers between a plurality of distributed ledgers, the apparatus comprising:

means for determining an existing transaction in the source distributed ledger which has a transaction output that is unspent and owned by the entity;

means for constructing and submitting an initiating transaction for commission to the target distributed ledger, wherein the initiating transaction has a transaction output;

means for constructing and submitting a locking transaction for commission to the source distributed ledger, wherein the locking transaction spends and locks the transaction output of the existing transaction in the source distributed ledger and references the initiating transaction in the target distributed ledger; and

means for constructing and submitting a completing transaction for commission to the target distributed ledger, wherein the completing transaction spends the transaction output of the initiating transaction in the target distributed ledger and references the locking transaction in the source distributed ledger.

67. The apparatus of claim 66, wherein the transaction output of the initiating transaction is only spendable by the completing transaction when the completing transaction references the locking transaction and when a value of the transaction output of the initiating transaction matches a value of the transaction output of the existing transaction.

68. The apparatus of claim 66, wherein the distributed ledger comprises a blockchain.

69. The apparatus of claim 66, wherein the distributed ledger utilizes a directed acyclic graph.

70. The computer apparatus of claim 49, wherein the distributed ledger comprises a blockchain.

71. The computer apparatus of claim 49, wherein the distributed ledger utilizes a directed acyclic graph.

72. The computer apparatus of claim 58, wherein the distributed ledger comprises a blockchain.

73. The computer apparatus of claim 58, wherein the distributed ledger utilizes a directed acyclic graph.