

WHAT IS CLAIMED IS:

1. A method of updating received digital assets transactions in an isolated device, comprising:
using at least one processor of an isolated device having no network connectivity for:
 receiving at least one limited length string indicating a value of digital assets transferred in at least one transaction from at least one other device to an account associated with the isolated device, the at least one transaction is recorded in a blockchain maintained by a plurality of networked computing nodes with a respective identifier computed based on at least one input value of digital assets included in the at least one transaction which corresponds to a respective output value of at least one previous transaction stored in a predefined order in a depository allocated for the isolated device in the at least one other device, the isolated device is informed of each previous transaction stored in the depository;
 inferring the respective identifier of the at least one transaction according to the at least one output value of at least one previous transaction identified based on the transferred value according to the predefined order; and
 updating the isolated device with a balance of digital assets of the associated account according to the at least one transaction including the respective identifier.
2. The method of claim 1, wherein the digital assets comprise cryptocurrency and the isolated device is a cryptocurrency wallet.
3. The method of claim 1, further comprising the at least one other device allocates a plurality of depositories each for a respective one of a plurality of isolated devices.
4. The method of claim 1, wherein the at least one limited length string is received by the isolated device via at least one limited capacity interface of the isolated device configured to receive at least one limited length string.
5. The method of claim 1, wherein the at least one other device is networked and aware of each transaction of digital assets on the blockchain network, the at least one other device is a member of a group consisting of: a network connected device and at least one of the plurality of networked computing nodes.

6. The method of claim 1, wherein the at least one other device is implemented by a subset of the plurality of networked computing nodes using at least one Multi-Party Computation (MPC) protocol to maintain the depository and carry out the transaction.
7. The method of claim 1, wherein the respective identifier is a hash value computed using at least one hash function.
8. The method of claim 1, further comprising the value transferred to the at least one other device in each of the at least one previous transaction is indexed in the output of the respective at least one previous transaction with a predefined index used by the isolated device to infer the respective identifier of the at least one transaction.
9. The method of claim 1, further comprising assigning a respective predefined value for each additional parameter potentially affecting the respective identifier computed for the at least one transaction.
10. The method of claim 1, wherein the isolated device is informed of each previous transaction stored in the depository via at least one limited length string received by the isolated device thus the isolated device is informed of the at least one previous transaction stored in the depository.
11. The method of claim 1, wherein each previous transaction stored in the depository relates to a respective transaction previously transferred from the isolated device to the at least one other device thus the isolated device is informed of the at least one previous transaction stored in the depository.
12. The method of claim 1, wherein the predefined order is based on a time of transfer of each previous transaction.
13. The method of claim 12, wherein the isolated device infers the respective identifier of the at least one transaction based on the transferred value and the at least one input of at least one most recent previous transaction which was most recently transferred from the isolated device to the at least one other device such that a cumulative value of digital assets transferred in the at least one most recent previous transaction is at least equal to the transferred value.

14. The method of claim 13, wherein, in case the cumulative value exceeds the transferred value, the at least one other device transfers an excess transaction to itself which comprises the difference between the cumulative value and the transferred value, the excess transaction is stored in the depository as the transaction most recently transferred from the isolated device to the at least one other device.

15. The method of claim 13, further comprising the at least one other device transfers a second value of digital assets from an account associated with the isolated device to at least one third device, the at least one other device transfers the second value from at least one least recent previous transaction which was least recently transferred from the isolated device to the at least one other device, a second cumulative value of digital assets transferred in the at least one least recent transaction is at least equal to the second value.

16. The method of claim 15, further comprising the at least one other device transfers the second value to the at least one third device via another depository allocated in the at least one other device for at least one third device.

17. The method of claim 16, further comprising, in case the value of the at least one output of the at least one least recent previous transaction is significantly larger than the second value, the at least one other device creates at least one hierarchical split level for the at least one least recent previous transaction, each hierarchical split level comprises a predefined number of artificial sub-transactions each having the identifier of the at least one least recent previous transaction and associated with a predefined sub-value such that a sum of the sub-value of all sub-transactions of a certain split level equals the value of a next higher hierarchy transaction, the at least one other device transfers at least part of the second value from at least one of the sub-transactions.

18. The method of claim 1, further comprising, in case a commission is allocated to at least one of the plurality of computing nodes for recording the at least one transaction, the isolated device is informed of a commission value to enable the isolated device to correctly identify the at least one previous transaction having a cumulative sum exceeding the transferred sum after the value of the commission is deducted from the cumulative sum.

19. The method of claim 18, wherein the commission value is predefined thus the isolated device is informed of the value of the commission.

20. The method of claim 18, wherein the isolated device is informed of the commission value via at least one limited length string received by the isolated device.
21. The method of claim 18, wherein the commission value is adjusted in a predefined manner compared to a commission value of at least one previous transaction transferred from the at least one other device to the isolated device.
22. The method of claim 18, wherein the commission value is predefined for the at least one transaction which is recorded in the blockchain by at least one of the plurality of computing nodes which receives a second commission value for recording the at least one transaction.
23. The method of claim 22, further comprising the second commission value is allocated for at least one subsequent transaction succeeding the at least one transaction such that the commission and the second commission are transferred to the at least one computing node which records in the blockchain both the at least one transaction and the at least one subsequent transaction.
24. The method of claim 22, wherein the at least one other device delivers the second commission directly to the at least one computing nodes which records in the blockchain both the at least one transaction.
25. The method of claim 1, wherein, in case the respective identifier is further based on a signature generated by the at least one other device, the isolated device is further configured to derive the signature from a unique private key assigned to the at least one other device and available to the isolated device in order to infer the respective identifier according to the to the at least one output value of the at least one previous transaction identified based on the transferred value according to the predefined order and the signature generated by the at least one other device.
26. The method of claim 25, wherein the isolated device is further configured to infer the respective identifier based on the signature according to at least one malleability parameter of the signature indicated by the at least one limited length string received by the isolated device.
27. The method of claim 25, wherein, in case the respective identifier is further based on a random value selected by the at least one other device, the isolated device is further configured to derive the random value in order to infer the respective identifier based on based on the at least one output

value of the at least one previous transaction identified according to the transferred value with respect to predefined order, the signature and the random value.

28. The method of claim 27, wherein, the isolated device derives the random value from a plurality of random values securely transmitted previously by the isolated device via a unidirectional secured channel of the isolated device to the at least one other device.

29. The method of claim 27, wherein the isolated device derives the random value from a random seed transferred previously from the isolated device to the at least one other device via a unidirectional secured channel of the isolated device.

30. The method of claim 27, wherein the isolated device derives the random value from the at least one limited length string indicating a predefined random value used by the at least one other device to create the respective identifier.

31. The method of claim 25, further comprising, in case the at least one other device comprises a subset of computing nodes of the plurality of computing nodes, the isolated device infers the respective identifier according to the private key of the subset of computing nodes which participated in transferring the at least one transaction, the subset of computing nodes is indicated by the at least one limited length string.

32. The method of claim 25, wherein the isolated device is further configured to create in advance a plurality of valid transactions for a predefined number of hierarchical split levels using the private key of the at least one other device and transmit the plurality of valid transactions to the at least one other device which updates the depository accordingly.

33. The method of claim 32, further comprising, in case the at least one other device comprises multiple computing nodes of the plurality of computing nodes, the isolated device splits each of the plurality of valid transactions to a plurality of partial valid transactions using at least one secret sharing algorithm and transmits plurality of partial valid transactions to the multiple computing nodes.

34. The method of claim 32, wherein the at least one other device transfers a second value of digital assets from an account associated with the isolated device to at least one third device by

transferring at least one least recent valid transaction of the plurality of valid transactions selected according to the second value.

35. The method of claim 32, wherein the isolated device is further configured to receive the at least one transaction by creating in advance a valid transaction according to the transferred value indicated by the at least one limited length string and transmit the valid transaction to the at least one other device which updates the depository accordingly, the at least one other device transfers the transferred value to the isolated device in the at least one transaction which is based on the valid transaction, the isolated device infers the respective identifier of the at least one transaction based on the valid transaction.

36. The method of claim 35, wherein the isolated device is further configured to create a plurality of valid transactions for a predefined number of hierarchical split levels using the private key of the at least one other device for at least one excess transaction transferred from the at least one other device to itself comprising a difference between the transferred value and a cumulative value of digital assets of at least one output of at least one most recent transaction of the plurality of valid transactions stored in the depository.

37. The method of claim 32, wherein the isolated device is further configured to receive the at least one transaction by creating in advance a plurality of valid transactions for a plurality of predefined values of digital assets according to a predefined number of hierarchical split levels and transmit the plurality of valid transactions to the at least one other device which updates the depository accordingly, the at least one other device transfers the transferred value to the isolated device by transferring the at least one transaction selected from the plurality of valid transactions according to the transferred value.

38. The method of claim 32, wherein the isolated device is further configured to receive the at least one transaction by creating a plurality of valid transactions for a plurality of predefined values of digital assets according to a predefined number of hierarchical split levels and transmit the plurality of valid transactions to the at least one other device which updates a plurality of depositories allocated for the isolated device in the at least one other device such that each of the plurality of valid transactions is stored in a respective one of the plurality of depositories, the at least one other device transfers the transferred value to the isolated device by transferring the at

least one least transaction from at least one of the plurality of depositories selected according to the transferred value.

39. The method of claim 32, wherein the isolated device is further configured to receive the at least one transaction by creating in advance at least one valid predefined value transaction that comprises a plurality of output values each for a predefined limited value of digital assets and transmit the at least one valid predefined value transaction to the at least one other device which updates the depository accordingly, the at least one other device transfers the transferred value to the isolated device by transferring the at least one valid transaction selected from of the plurality of valid predefined value transactions according to the transferred value.

40. The method of claim 25, wherein the isolated device is further configured to receive a plurality of transactions each from a respective one of a plurality of accounts of the other device, each of the plurality of accounts is associated with a different unique private key of a plurality of private keys which is deterministically derivable from another one of the plurality of private keys of another account used to create a succeeding transaction of the plurality of transactions, the isolated device is informed of the value transferred in each of the plurality of transactions and the private key of the account used to transfer the latest transaction of the plurality of transactions, the isolated device deterministically derives the private key of each of the plurality of private keys based on the private key of the account used for the succeeding transaction, the isolated device infers the respective identifier of each of the plurality of transactions by deriving the private key of each account used for each transaction to derive the respective signature used to compute the respective identifier.

41. The method of claim 40, wherein each of the plurality of accounts used to create a respective transaction to the isolated device is emptied from all digital assets by creating a respective excess transaction to an account of the plurality of accounts used to create the succeeding transaction.

42. The method of claim 1, wherein the isolated device having a unidirectional secured channel is first synchronized with all previous transactions made between its associated account and any other account prior to transmitting at least one transaction via its unidirectional secured channel, the synchronization comprises receiving at least one limited length string indicative of all transactions related to the associated account which the isolated device was not informed of previously.

43. The method of claim 1, wherein the isolated device is further configured to receive the at least one transaction from another isolated device disconnected from the blockchain network and thus potentially unaware of at least one previous transaction transferred from the isolated device to the another isolate device, the at least one transaction is based on the at least one previous transaction stored in the predefined order in the depository allocated for the isolated device in the another isolated device, the at least one limited length string is indicative of each previous transaction transferred from the isolated device to the another isolated device that the another isolated device is aware of.

44. The method of claim 43, wherein the isolated device is further configured to transfer at least one transaction to each of a first and second other isolated devices based on a plurality of previous transactions received from the two other isolated devices and stored in a single depository allocated for the two other isolate devices in the isolated device, the isolated device is configured to transfer:

- at least one transaction to the first other isolated device based on at least one left-most recent transaction stored in the single depository, and
- at least one transaction to the second other isolated device based on at least one right-most recent transaction stored in the single depository.

45. The method of claim 43, wherein the isolated device is further configured to transfer to itself a transaction which comprises a plurality of outputs each for a predefined value of digital assets, the isolated device transfers a respective value of digital assets to each of a plurality of other devices by transferring to each respective other device a transaction which comprises at least one input derived from at least one output of the plurality of outputs according to the respective value.

46. The method of claim 45, wherein the isolated device is further configured to transfer to at least one of the plurality of other devices a plurality of transactions each comprising a respective one of a plurality of inputs derived from a subset of consecutive outputs of the plurality of outputs.

47. The method of claim 45, wherein the isolated device is further configured to create a plurality of recursive transactions each comprising a plurality of outputs of predefined value of digital assets cumulatively equal to an output of a respective output of a previous iteration, the isolated device transfers a respective value of digital assets to at least one of the plurality of other devices by transferring to the at least one other device a transaction which comprises at least one input derived from at least one output of the plurality of outputs according to the respective value such that the

at least one other device infers the recursion level according to the transferred value with respect to the predefined value of each output of each recursive transaction.

48. An isolated device for storing digital assets, comprising:

a limited capacity interface configured to receive at least one limited length string;

a storage medium string a code; and

at least one processor coupled to the limited capacity interface and to the storage medium,

the at least one processor executes the code, the code comprising:

code instructions to receive at least one limited length string indicating a value of digital assets transferred in at least one transaction from at least one other device to an account associated with the isolated device, the at least one transaction is recorded in a blockchain maintained by a plurality of networked computing nodes with a respective identifier computed based on at least one input value of digital assets included in the at least one transaction which corresponds to a respective output value of at least one previous transaction stored in a predefined order in a depository allocated for the isolated device in the at least one other device, the isolated device is informed of each previous transaction stored in the depository,

code instructions to inferring the respective identifier of the at least one transaction according to the at least one output value of at least one previous transaction identified based on the transferred value according to the predefined order, and

code instructions to update the isolated device with a balance of digital assets of the associated account according to the at least one transaction including the respective identifier.