

Claims

1. A computer-implemented method of effecting a blockchain payment channel based on a series of spending transactions exchanged between parties, in which:

each transaction of the series of spending transactions has a future lock time, before which it cannot be committed to the blockchain, and comprises: (i) at least one transaction input containing a pointer a common spendable transaction output, and (ii) at least two spendable transaction outputs having respective digital asset values,

an initial transaction of the series of spending transactions has a lowest sequence number and each subsequent transaction of the series of spending transactions has a higher sequence number than the previous transaction and contains one or more function variables other than the respective digital asset values of its spendable transaction outputs;

wherein the method comprises, by one of the parties:

receiving, at computer equipment of the party, a previous transaction of the series of spending transactions;

applying a function to the one or more function variables contained in the previous transaction to do at least one of:

compute the digital asset values of the current transaction,

create a new data field for the current transaction, which does not correspond to any existing data field contained in the previous transaction, the current transaction containing the new data field, and

prevent an existing type of data field from being propagated from the previous transaction into the current transaction, such that the previous transaction contains a data field which does not correspond to any data field in the current transaction; and

cryptographically signing a portion of the current transaction, the signed portion comprising the at least two spendable transaction outputs, using a private key counterpart to the public key of the party, thereby computing a transaction signature for inclusion in the transaction input of the current transaction.

2. The method of claim 1, wherein the common spendable transaction output specifies m public keys of the parties and is locked to any $2 \leq n < m$ of the m public keys, the party

applying the function being a trusted oracle, whereby any other $n - 1$ of the parties may sign a portion of the current transaction for unlocking the common spendable transaction output.

3. The method of claim 2, wherein the trusted oracle signs the current transaction after receiving, from another of the parties, at least a transaction signature for the current transaction which is valid in respect of the public of the other party.

4. The method of claim 1 or 2, wherein said function is defined or otherwise evidenced in a funding transaction comprising the common spendable transaction output.

5. The method of claim 4 when dependent on claim 2, wherein the trusted oracle uses the funding transaction to determine or verify the function to be applied.

6. The method of claim 4 or 5, wherein the funding transaction contains or evidences a piece of code executable embodying the function, the function being applied by executing the piece of code on one or more computer processors of the computer equipment in dependence on the one or more previous input values.

7. The method of claim 6, wherein the piece of code is contained in:
the funding transaction, or
another transaction recorded in the blockchain, and in that event the funding transaction contains an identifier of the piece of code.

8. The method of claim 7 when dependent on claim 5, wherein the trusted oracle retrieves the piece of code from the blockchain for execution, and thereby determines the function to be applied.

9. The method of claim 6 or 7 when dependent on claim 5, wherein the trusted oracle receives the piece of code from an off-chain source and uses the funding transaction to verify the received piece of code.

10. The method of any preceding claim, wherein the one or more function variables in each transaction comprise one or more input values;

wherein the function is applied to at least the one or more input values of the previous transaction to additionally compute the one or more input values of the current transaction.

11. The method of any preceding claim, wherein the one or more function variables in each transaction comprise one or more external parameters which are not computed by applying the function;

wherein the function is applied to at least the one or more external parameters contained in the previous transaction in order to compute the digital asset values of the current transaction.

12. The method of claims 10 and 11, wherein the variables in each transaction comprise the one or more function variables and the one or more external parameters;

wherein the function is applied to the one or more input values and the one or more external parameters contained in the previous transaction in order to compute (a) and (b).

13. The method of claim 11 or 12, wherein the one or more external parameters of the current transaction are provided by another of the parties, other than the party applying the function.

14. The method of claim 13, wherein the one or more external parameters of the current transaction are contained in the signed portion of the current transaction, and the party signs the current transaction after the other party has provided the one or more external parameters.

15. The method of claim 10 or any claim dependent thereon, wherein the party also applies the same function to at least the one or more input values of the current transaction, in order to compute: (a') one or more input values of the next transaction, the

next transaction being the transaction after the current transaction in the series of spending transactions, and (b') the digital asset values of the next transaction.

16. The method of claim 11 or any claim dependent thereon, wherein the party applies the same function to at least the one or more external parameters of the current transaction in order to compute the digital asset values of the next transaction.

17. The method of claim 15, wherein the party creates the next transaction containing at least the digital asset values of the next transaction, cryptographically signs a portion of the next transaction, and sends the next transaction and the transaction signature to another of the parties.

18. The method of claim 12 or any claim dependent thereon, wherein:
the one or more input values in each transaction of the series of spending transactions represent a game state, and
the one or more external parameters in the previous transaction define a game move, the one or more external parameters in the previous transaction having been determined by a second of the parties,
wherein the function is applied to update the game state of the previous transaction to implement the game move of the previous transaction, the updated game state represented by the one or more input values of the current transaction, whereby the digital asset values of the current transaction are computed responsive to the game move.

19. The method of claim 18, wherein the current transaction is sent to a third of the parties for the third party to determine the one or more external parameters for the current transaction, representing the third party's game move responsive to the second party's game move.

20. The method of any preceding claim, wherein the one or more input values of the current transaction are contained in the signed portion of the current transaction.

21. The method of any preceding claim, wherein the party applies the function after the previous transaction has been signed by at least two of the parties.
22. The method of any preceding claim, wherein the function is applied to the one or more function variables and to the digital asset values of the previous transaction, in order to determine the digital asset values of the current transaction.
23. The method of any preceding claim dependent thereon, wherein the one or more external parameters of the previous transaction comprise a nonce value, wherein the function is applied to:
- add the nonce value to a partial data set, thereby determining a complete data set including the nonce value,
 - apply a hash function to the complete data set, thereby computing a hash value,
 - determine if the hash value meets a defined requirement, and
 - determine the digital asset values of the current transaction in dependence on whether the hash value meets the defined requirement.
24. The method of any preceding claim, wherein the final transaction in the series is used to compute a settlement transaction, by applying the same function to the one or more function variables of the final transaction to compute respective digital asset values of at least two spendable transaction outputs of the settlement transaction, wherein the settlement transaction comprises at least one transaction input containing a pointer to the common spendable transaction output, wherein the settlement transaction is committed to the blockchain.
25. The method of claim 24, wherein the settlement transaction has a maximum possible sequence number.
26. The method of any preceding claim, wherein the function is not applied to compute the digital asset values of the current transaction until the previous transaction has been finalized at least by the application of two or more required transaction signatures.

27. The method of any preceding claim, wherein the common spendable transaction output is part of a funding transaction, committed to a blockchain, and is locked to at least two public keys of the parties.

28. Computer equipment comprising one or more computer processors, the one or more computer processors being configured to implement the method of any preceding claims.

29. Computer program instructions stored on a transitory or non-transitory computer-readable medium or media, the computer program instructions for programming computer equipment to carry out the steps of any of claims 1 to 27.