

Claims

1. A method of attesting to an order of a sequence of data items, the method comprising, at an attesting node of a network:
 - receiving the sequence of data items from one or more client nodes of the network;
 - determining an order of the sequence of data items, whereby each successive data item in said sequence succeeds a preceding one of the data items in the sequence; and
 - based on said determination, attesting to the order by: including an indication of a respective set of one or more of the data items in each of a series of blockchain transactions, each successive transaction in said series succeeding a respective preceding transaction in the series, wherein the set indicated in each successive transaction succeeds the set indicated in the respective preceding transaction according to said order;
 - wherein each successive transaction comprises a respective input pointing to an output of the respective preceding transaction, wherein the output of the respective preceding transaction comprises a locking script, and the input of the respective successive transaction includes an unlocking script comprising a respective signature based on a respective key in a series of keys, the inclusion of the respective signature being a condition for unlocking the unlocking script of the respective preceding transaction;
 - wherein the respective signature in each successive transaction signs a portion of the respective successive transaction including at least the indication of the respective set of data items; and
 - wherein the step of attesting to the order further comprises sending the transactions to be recorded on a blockchain.
2. The method of claim 1, wherein said order is an order of receipt of the data items at the attesting node.
3. The method of claim 1 or 2, wherein the step of attesting to the order further comprises:
 - timestamping each of the transactions with timestamp information specifying at least one time of receipt of the respective set of data items, the time of receipt being the time of receipt at the attesting node.

4. The method of any preceding claim, wherein each of said sets comprises a respective plurality of the data items, wherein the indication included in each transaction comprises an indication of each individual one of the data items in the respective set, and wherein said step of attesting to the order comprises:

- in each of said series of transactions, including information specifying the order of the data items within the respective set, from a first data item in the set through one or more successive data items in the set.

5. The method of claim 4, wherein said information comprises an index mapped to the indication of each individual data item in the respective set, and/or an ordered list of the individual data items in the set.

6. The method of claim 4 or 5, wherein the plurality of data items of each respective set are selected on the basis of being received at the attesting node within a respective instance of a predetermined repeating time interval.

7. The method of claim 4, 5 or 6, as dependent on claim 3, wherein within each transaction:

the timestamp information comprises an individual timestamp corresponding to each individual one of the data items in the respective set, specifying the time of receipt at the attesting node of the individual data item.

8. The method of any of claims 4 to 7, wherein within each transaction:

the indication of each individual data item comprises at least a hash; the indication of the first data item comprising a hash of a first preimage, wherein the first preimage comprises at least the first data item; and the indication of each successive data item succeeding the first data item comprising a hash of a respective successive preimage, wherein each successive preimage comprises at least the preceding hash in the sequence.

9. The method of claim 8 as dependent on claim 7, wherein each of the first and successive preimages further comprises the corresponding timestamp.

10. The method of any of claims 4 to 9, wherein for each transaction, the individual data items are modelled as leaves of a Merkle tree, and the indication comprises one or both of:
 - a Merkle root of the Merkle tree, and/or
 - a merkle proof for each individual data item.
11. The method of any of claims 4 to 10, wherein within each transaction:
 - the indication of each individual data item comprises at least a corresponding public key, the indication of the first data item comprising a first public key generated based on the first data item, and the indication of each successive data item in the set comprising a successive public key generated based on that successive data item and the preceding public key in the sequence.
12. The method of claim 11, wherein said signing comprises including a separate signature using each of the public keys, each signing a message comprising the corresponding data item or hash thereof.
13. The method of any of claims 4 to 12, wherein within each transaction, the indication of each individual data item comprises an r-puzzle for the individual data item.
14. The method of any of claims 4 to 13, wherein the indication of each data item comprises the respective data item in-the-clear.
15. The method of any of claims 1 to 13, wherein each transaction does not include any of the data items in-the-clear.
16. The method of any preceding claim, wherein said network comprises a layered including a core layer of core nodes, one or more intermediate layers each comprising a plurality of intermediate layer nodes, and one or more outer layers each comprising a plurality of outer layer nodes; wherein the core nodes comprise one or more nodes of a blockchain network.

17. The method of claim 16, wherein the attesting node is one of the intermediate layer nodes.
18. The method of claim 16 or 17, wherein the transmitting node, or at least one of the transmitting nodes, is one of the outer layer nodes.
19. The method of claim 16, 17 or 18, wherein said sending comprises sending the transactions toward the core layer.
20. The method of claim 19, wherein said sending comprises sending at least some of the transactions directly to at least one of the core nodes over a connection between the attestation node and the core node.
21. The method of claim 19, wherein said sending comprises sending at least some of the transactions to one or more of the core nodes via a further one of the intermediate layer nodes.
22. The method of claim 21, wherein the further intermediate layer node is configured to add its own signature to each of the transactions received from the attesting node, wherein each unlocking script in the series of transactions is conditional on the signature of more than one of the intermediate layer nodes to unlock.
23. The method of any preceding claim, wherein the indication of each data item is included in an unspendable output of the respective transaction.
24. The method of any preceding claim, wherein the transactions and/or the attesting nodes are certified by a certificate authority.
25. Computer equipment comprising:
 - memory comprising one or more memory units,
 - processing apparatus comprising one or more processing units, and
 - a network interface comprising one or more network interface units;

wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when run on the processing apparatus to operate the computer equipment as the attesting node by performing the method of any preceding claim, including receiving the data items and sending the transactions via the network interface.

26. A computer program embodied on computer readable storage and configured so as when run on one or more processors to perform the method of any of claims 1 to 24.

27. A method of determining whether a recorded order of a sequence of data items matches an expected order, the method comprising, at a client node of a network:

determining the recorded order by reading an indication of a respective set of one or more of the data items from each of a series of transactions recorded on a blockchain, each successive transaction in said series succeeding a respective preceding transaction in the series; and

for each successive transaction, checking that the one or more data items of the respective set indicated in the successive transaction succeed the one or more data items of the respective set indicated in the respective preceding transaction according to said expected order;

wherein each successive transaction comprises a respective input pointing to an output of the respective preceding transaction, wherein the output of the respective preceding transaction comprises a locking script, and the input of the respective successive transaction includes an unlocking script comprising a respective signature based on a respective key in a series of keys, the inclusion of the respective signature being a condition for unlocking the unlocking script of the respective preceding transaction; and

the method comprises verifying the signature in each successive transaction.

28. The method of claim 27, wherein the client node previously transmitted at least one of the data items to an attesting node of the network, in order for the attesting node to attest to the recorded order by creating said series of transactions and sending them for recordal on the blockchain.

29. The method of claim 27 or 28, wherein at least part of said network comprises a layered network including a core layer of core nodes, one or more intermediate layers each comprising a plurality of intermediate layer nodes, and one or more outer layers each comprising a plurality of outer layer nodes; wherein the core nodes comprise one or more nodes of a blockchain network, the client node is one of the outer layer nodes, and the attesting node is one of the intermediate later nodes.

30. The method of claim 29, wherein the client node sends the at least one data item to the attesting node via a connection between the client node and one of the intermediate layers, but performs the reading via a direct connection between the client node and the core layer, where at least some of the nodes of the core layer maintain a copy of the blockchain.

31. Computer equipment comprising:
memory comprising one or more memory units,
processing apparatus comprising one or more processing units, and
a network interface comprising one or more network interface units;
wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when run on the processing apparatus to operate the computer equipment as the querying node by performing the method of any of claims 27 to 30, including reading said indications via the network interface.

32. A computer program embodied on computer readable storage and configured so as when run on one or more processors to perform the method of any of claims 27 to 30.