

CLAIMS:

1. A blockchain-implemented security method involving a requestor and a group of nodes, the method comprising:

- 5 generating a cryptographic key of the requestor based on i) a password chosen by the requestor and ii) a plurality of first quantities sent by the group of nodes, wherein the plurality of first quantities is based on private key shares of the group of nodes and a generator function of a digital signature scheme employing a bilinear mapping on an elliptic curve;
- 10 generating a cryptographic signature for a blockchain transaction of the requestor, the cryptographic signature corresponding to the cryptographic key of the requestor based on the bilinear mapping on an elliptic curve of the digital signature scheme, wherein the cryptographic signature is based on i) the password chosen by the requestor and ii) a plurality of second quantities sent by the group of nodes, wherein the plurality of second
- 15 quantities is based on the private key shares of the group of nodes; and
- verifying the cryptographic signature of the blockchain transaction using the cryptographic key of the requestor.

2. A blockchain-implemented security method according to claim 1, further comprising:

- 20 establishing a group of nodes operably coupled to one another via at least one communication network, wherein each node of the group transfers a digital asset to the group; and/or
- receiving (preferably by at least one node belonging to the group of nodes) a funding transaction from a requestor, wherein the funding transaction specifies one or
- 25 more digital assets of the requestor where all or some of such digital assets may be transferred using a password chosen by the requestor; and/or
- receiving (preferably by at least one node belonging to the group of nodes) a spending transaction that transfers some portion of the one or more digital assets of the requestor as specified in the funding transaction, wherein the spending transaction includes
- 30 the cryptographic signature corresponding to the cryptographic key of the requestor; and/or

verifying (preferably by at least one node belonging to the group of nodes) the cryptographic signature included in the spending transaction using the cryptographic key of the requestor.

- 5 3. A blockchain-implemented security method according to claim 2, further comprising:
receiving (preferably by at least one node belonging to the group of nodes) an
initialisation transaction from the requestor, wherein the initialisation transaction indicates
a desire to set a password associated with the requestor; and/or
generating (preferably by at least one node belonging to the group of nodes) a first
10 quantity in response to the initialisation transaction; and/or
sending (preferably by at least one node belonging to the group of nodes) a first
message to the requestor, wherein the first message includes the first quantity.
- 15 4. A blockchain-implemented security method according to claim 2, further comprising:
receiving (preferably by at least one node belonging to the group of nodes) a pre-
spending transaction from the requestor, wherein the pre-spending transaction transfers a
transaction deposit and includes the hash of at least part of the spending transaction,
wherein the hash of at least part of the spending transaction is based on a hash function of
the digital signature scheme; and/or
20 generating (preferably by at least one node belonging to the group of nodes) a
second quantity in response to the pre-spending transaction; and/or
sending (preferably by at least one node belonging to the group of nodes) a second
message to the requestor, wherein the second message includes the second quantity.
- 25 5. A blockchain-implemented security method according to claim 1, further comprising:
broadcasting a funding transaction from the requestor for communication to the
group of nodes, wherein the funding transaction specifies one or more digital assets of the
requestor where all or some of such digital assets may be transferred using a password
chosen by the requestor; and/or
30 broadcasting a spending transaction from the requestor for communication to the
group of nodes, wherein the spending transaction transfers some portion of the one or more

digital assets of the requestor as specified in the funding transaction, and wherein the spending transaction includes the cryptographic signature.

6. A blockchain-implemented security method according to claim 5, further comprising:
- 5 broadcasting an initialisation transaction from the requestor for communication to the group of nodes, wherein the initialisation transaction indicates a desire to set a password associated with the requestor, wherein the plurality of first quantities are generated and sent by the group of nodes in response to the initialisation transaction; and/or
- 10 generating the cryptographic key based at least in part on the password chosen by the requestor and the plurality of first quantities sent by the group of nodes in response to the initialisation transaction.
7. A blockchain-implemented security method according to claim 5, further comprising:
- 15 broadcasting a pre-spending transaction from the requestor for communication to the group of nodes, wherein the pre-spending transaction transfers a transaction deposit and includes the hash of at least part of the spending transaction, wherein the hash of at least part of the spending transaction is based on a hash function of the digital signature scheme, wherein the plurality of second quantities are generated and sent by the group of
- 20 nodes in response to the pre-spending transaction.
8. A blockchain-implemented security method according to claim 5, further comprising:
- establishing the group of nodes operably coupled to one another via at least one communication network, wherein each node of the group transfers a digital asset to the
- 25 group, and wherein each node of the group stores a corresponding private key share; and/or
- broadcasting, by a requestor system, an initialisation transaction from the requestor for communication to the group, wherein the initialisation transaction indicates a desire to set a password associated with the requestor;
- generating, by the nodes of the group, a plurality of first quantities in response to
- 30 the initialisation transaction, wherein the first quantity generated by a given node is based at least in part on the private key share of the node and a generator function of the digital signature scheme;

-47-

sending, by the nodes of the group, respective first messages to the requestor, wherein the first messages include the plurality of first quantities;

generating, by the requestor system, the cryptographic key based on the password chosen by the requestor and the plurality of first quantities;

5 broadcasting, by the requestor system, a funding transaction from the requestor for communication to the group, wherein the funding transaction specifies one or more digital assets of the requestor where all or some of such digital assets may be transferred using the password chosen by the requestor;

10 broadcasting, by the requestor system, a pre-spending transaction from the requestor for communication to the group, wherein the pre-spending transaction transfers a transaction deposit and includes a hash of an unsigned spending transaction that transfers some portion of the certain funds of the requestor using a hash function of the digital signature scheme;

15 generating, by the nodes of the group, a plurality of second quantities in response to the pre-spending transaction, wherein the second quantity generated by a given node is based at least in part on the hash of the unsigned spending transaction as included in the pre-spending transaction and the private key share of the node;

sending, by the nodes of the group, second messages to the requestor, wherein the second messages include the plurality of second quantities;

20 generating, by the requestor system, the cryptographic signature based on the password chosen by the requestor and the plurality of second quantities; and

25 broadcasting, by the requestor system, a spending transaction from the requestor for communication to the group, wherein the spending transaction transfers some portion of the certain funds of the requestor, and wherein the spending transaction is based on the unsigned spending transaction and includes the cryptographic signature; and

verifying, by at least the nodes of the group, the cryptographic signature of the spending transaction using the cryptographic key of the requestor.

9. A blockchain-implemented security method according to any of claims 3, 6 or 8, wherein:

the initialisation transaction includes an initialisation fee that is paid by the requestor to the group; and/or

-48-

the initialisation fee is preferably paid to a public group address associated with the group; and/or

the initialization fee is preferably returned to the requestor in the event that at least one node of the group sends an inconsistent first quantity to the requestor; and/or

5 inconsistency of the first quantity is preferably determined using a verifiable secret sharing scheme.

10. A blockchain-implemented security method according to any of claims 4, 7 or 8, wherein:

10 the pre-spending transaction further defines a spending fee; and/or

the transaction deposit is locked under the public group address associated with the group; and/or

the group selectively transfers the transaction deposit less the spending fee back to the requestor in the event that the verifying is successful; and/or

15 the group selectively confiscates the transaction deposit in the event that the verifying fails; and/or

the transaction deposit is preferably returned to the requestor in the event that at least one node of the group of nodes sends an inconsistent second quantity to the requestor; and/or

20 inconsistency of the second quantity is preferably determined using a verifiable secret sharing scheme; and/or

the spending fee is preferably paid to a public group address associated with the group; and/or

25 the nodes of the group verify that the spending fee is sufficient, wherein sufficiency of the spending fee is preferably based on computation resources required to process the third transaction and the spending transaction; and/or

the nodes of the group selectively bypass further processing of the pre-spending transaction in the event of failed verification of sufficiency of the spending fee; and/or

30 the group selectively distributes the spending fee to the group in the event of successful verification of the signature of the spending transaction.

11. A blockchain-implemented security method according to any of claims 2-10, wherein:

the funding transaction specifies that the one or more digital assets of the requestor are locked by the cryptographic key and thus can be spent by the cryptographic signature; and

the verifying of the signature of the spending transaction is performed by the group
5 and optionally by other nodes that do not belong to the group.

12. A blockchain-implemented security method according to any of claims 2-10, wherein:

the funding transaction specifies that the one or more digital assets of the requestor are locked by a public key of the group and thus can be spent by a signature based on a
10 threshold number of private key shares of the group;

the verifying of the signature of the spending transaction is performed only by the group; and

upon successful verification of the signature of the spending transaction, the group cooperates to generate a signature based on a threshold number of private key shares of the
15 group and to construct a secondary spending transaction that includes such signature.

13. A blockchain-implemented security method according to any of claims 2-12, wherein:

the plurality of first quantities are included in private messages sent from the nodes of the group to the requestor and/or are encrypted with a public key of the requestor; and/or

20 the nodes of the group each have a trusted execution environment that stores the private key share of the node; and/or

the trusted execution environment of the node generates the first quantity based at least in part on the private key share of the node and the generator function of the digital signature scheme; and/or

25 the plurality of second quantities are included in private messages sent from the nodes of the group to the requestor and/or are encrypted with a public key of the requestor; and/or

the trusted execution environment of the node generates the second quantity based at least in part on the hash of the unsigned spending transaction as included in the pre-
30 spending transaction and the private key share of the node; and/or

-50-

the private message sent from a node of the group to the requestor is associated with the public key of the trusted execution environment of the node and is signed with the corresponding private key of the trusted execution environment of the node; and/or

5 one or more nodes mine the funding transaction and the spending transaction for storage in a proof-of-work blockchain.

14. A computer readable storage medium comprising computer-executable instructions which, when executed, configure a processor to perform any part of the method of any one of claims 1 to 13.

10

15. An electronic device comprising:

an interface device;

a processor coupled to the interface device;

a memory coupled to the processor, the memory having stored thereon computer

15 executable instructions which, when executed, configure the processor to perform any part of the method of any one of claims 1 to 13.