

Claims

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

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;

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 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:

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 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 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.

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 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.

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

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.

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

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:
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

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:
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 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 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 the initialisation transaction, wherein at the first quantity generated by a first given node is based at least in part on a first the private key share of the first node and a generator function of the digital signature scheme employing a bilinear mapping on an elliptic curve; ;

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

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

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, further wherein ~~where~~ all or some of such digital assets are transferrable ~~may be transferred~~ using the password chosen by the requestor and include the cryptographic key; ;

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

a portion of funds of the one or more digital assets of the requestor using a hash function of the digital signature scheme;

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

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

generating, by the requestor system, ~~a~~the cryptographic signature based on the password chosen by the requestor and the plurality of second quantities, wherein the cryptographic signature corresponds to the cryptographic key of the requestor based on the bilinear mapping on the elliptic curve of the digital signature scheme; ; ~~and~~

broadcasting, by the requestor system, a spending transaction from the requestor for communication to the group, wherein the spending transaction transfers thesome portion of the ~~certain~~ funds of the one or more digital assets of the requestor, and wherein the spending

transaction is based on anthe unsigned spending transaction and is signed withincludes 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 in the funding transaction, wherein, based on the verification, the spending transaction is stored in the blockchain, confirming a transfer of the portion of funds of the requestor to a recipient of the spending transaction.

2. The9. A blockchain-implemented security method according to claim 1, further comprising:

receiving, by the nodes of the group, the funding transaction from the requestor; and receiving, by the nodes of the group, the spending transaction from the requestor.

any of claims 3. The blockchain-implemented security method according to claim 2, further comprising:

receiving, by the nodes of the group, the initialisation transaction from the requestor.

4. The blockchain-implemented security method according to claim 2, further comprising:
receiving, by the nodes of the group, the pre-spending transaction from the requestor.

5. The blockchain-implemented security method according to claim 1,
wherein the hash of the pre-spending transaction is a hash of at least part of the spending transaction .

~~6.~~ The blockchain-implemented security method according to claim 3 ~~or 8~~, wherein:
the initialisation transaction includes an initialisation fee that is at least one of: paid by the requestor to the group; ~~and/or~~

~~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

~~wherein inconsistency of the inconsistent first quantity is preferably determined using a~~
verifiable secret sharing scheme.

~~10-7. The~~ A blockchain-implemented security method

~~-according to claim~~any of claims 4, 7 or 8, wherein:

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

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

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~~

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

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

~~wherein inconsistency of the inconsistent 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

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 ~~a~~ 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

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

8. The

~~11. A~~ blockchain-implemented security method according to claim~~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 cryptographic signature of the spending transaction is performed by the group and optionally by other nodes that do not belong to the group.

~~12.~~ 9. The A blockchain-implemented security method according to claimany 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 threshold number of private key shares of the group;

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

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

~~13.~~ A10. The blockchain-implemented security method according to claimany 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

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

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

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 thea public key of the requestor; and/or

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

| a

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

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

~~14.~~ 11. A non-transitoryA computer readable storage medium comprising computer-executable instructions which, when executed, cause one or more processors of a requestor system and a group of nodes to:~~configure a processor to perform any part of the method of any one of claims 1 to 13.~~

establish 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 group, and wherein each node of the group stores a corresponding private key share;

broadcast, by the requestor system, an initialisation transaction from a requestor for communication to the group, wherein the initialisation transaction indicates a desire to set a password associated with the requestor;

generate, by the nodes of the group, a plurality of first quantities in response to the initialisation transaction, wherein a first quantity generated by a first node is based at least in part on a first private key share of the first node and a generator function of a digital signature scheme employing a bilinear mapping on an elliptic curve;

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

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

broadcast, 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, further wherein all or some of such digital assets are transferrable using the password chosen by the requestor and include the cryptographic key;

broadcast, by the requestor system, a pre-spending transaction from the requestor for communication to the group, wherein the pre-spending transaction is unsigned, transfers a

transaction deposit, and includes a hash of the pre-spending transaction that transfers a portion of funds of the one or more digital assets of the requestor using a hash function of the digital signature scheme;

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

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

generate, by the requestor system, a cryptographic signature based on the password chosen by the requestor and the plurality of second quantities, wherein the cryptographic signature corresponds to the cryptographic key of the requestor based on the bilinear mapping on the elliptic curve of the digital signature scheme;

broadcast, by the requestor system, a spending transaction from the requestor for communication to the group, wherein the spending transaction transfers the portion of funds of the one or more digital assets of the requestor, and wherein the spending transaction is based on an unsigned spending transaction and is signed with the cryptographic signature; and

verify, by at least the nodes of the group, the cryptographic signature of the spending transaction using the cryptographic key of the requestor in the funding transaction,

wherein, based on the verification, the spending transaction is stored in the blockchain, confirming a transfer of the portion of funds of the requestor to a recipient of the spending transaction.

15. 12. An electronic device comprising:

an interface device;

a processor coupled to the interface device; and

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

executable instructions which, when executed by, configure the processor, cause to perform any part of the electronic device of a requestor system or a group method of nodes to:

establish 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 group, and wherein each node of the group stores a corresponding private key share;

broadcast, by the requestor system, an initialisation transaction from a requestor for communication to the group, wherein the initialisation transaction indicates a desire to set a password associated with the requestor;

generate, by the nodes of the group, a plurality of first quantities in response to the initialisation transaction, wherein a first quantity generated by a first node is based at least in part on a first private key share of the first node and a generator function of a digital signature scheme employing a bilinear mapping on an elliptic curve;

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

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

broadcast, 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, further wherein all or some of such digital assets are transferrable using the password chosen by the requestor and include the cryptographic key;

broadcast, by the requestor system, a pre-spending transaction from the requestor for communication to the group, wherein the pre-spending transaction is unsigned, transfers a transaction deposit, and includes a hash of the pre-spending transaction that transfers a portion of funds of the one or more digital assets of the requestor using a hash function of the digital signature scheme;

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

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

generate, by the requestor system, a cryptographic signature based on the password chosen by the requestor and the plurality of second quantities, wherein the cryptographic signature corresponds to the cryptographic key of the requestor based on the bilinear mapping on the elliptic curve of the digital signature scheme;

broadcast, by the requestor system, a spending transaction from the requestor for communication to the group, wherein the spending transaction transfers the portion of funds of the one or more digital assets of the requestor, and wherein the spending transaction is based on an unsigned spending transaction and is signed with the cryptographic signature; and

verify, by at least the nodes of the group, the cryptographic signature of the spending transaction using the cryptographic key of the requestor in the funding transaction,

wherein, based on the verification, the spending transaction is stored in the blockchain, confirming a transfer of the portion of funds of the requestor to a recipient of the spending transaction.

13. The electronic device according to claim 12,

wherein

the computer-executable instructions, when executed by the processor, further cause the electronic device to:

receive, by the nodes of the group, the funding transaction from the requestor; and

receive, by the nodes of the group, the spending transaction from the requestor.

14. The electronic device according to claim 13,

wherein

the computer-executable instructions, when executed by the processor, further cause the electronic device to:

receive, by the nodes of the group, the initialisation transaction from the requestor.

15. The electronic device according to claim 13, wherein the computer-executable instructions, when executed by the processor, further cause the electronic device to:

receive, by the nodes of the group, the pre-spending transaction from the requestor.

16. The non-transitory computer readable storage

medium according to claim 11, wherein the computer-executable instructions

when executed, further cause the one or more processors to:

receive, by the nodes of the group, the funding transaction from the requestor;

and receive, by the nodes of the group, the spending transaction from the requestor.

17. The non-transitory computer readable storage medium according to claim 16, wherein the computer-executable instructions when executed, further cause the one or more processors to:

receive, by the nodes of the group, the initialisation transaction from the requestor.

18. The non-transitory computer readable storage medium according to claim 16, wherein the computer-executable instructions, when executed, further cause the one or more processors to:

receive, by the nodes of the group, the pre-spending transaction from the requestor.

19. The non-transitory computer readable storage medium according to claim 11, wherein the hash of the pre-spending transaction is a hash of at least part of the spending transaction.

20. The electronic device according to claim 12, wherein the hash of the pre-spending transaction is a hash of at least part of the spending transaction.

~~any one of claims 1 to 13.~~