

Claims

1. A computer-implemented method for generating verification keys of a public-key signature scheme in a distributed network, the distributed network comprising a plurality of nodes, the plurality of nodes being subdivided into two or more subnetworks, wherein each of the plurality of nodes is configured to run one or more computational units, wherein the computational units are configured to execute computations in a deterministic and replicated manner across the subnetworks of the plurality of nodes, thereby traversing a chain of execution states, the method comprising

performing, by a subset of the nodes of a first subnetwork of nodes, a first distributed key generation protocol, the first distributed key generation protocol being configured to generate jointly a verification key for the first subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the first subnetwork;

performing, for a second subnetwork, by a subset of the plurality of nodes of the first subnetwork, a second distributed key generation protocol, the second distributed key generation protocol being configured to generate jointly a verification key of the second subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the second subnetwork;

signing, by a subset of the nodes of the first subnetwork, the verification key of the second subnetwork

with a permissible subset of the secret key shares of the nodes of the first subnetwork, thereby generating a joint signature on the verification key of the second subnetwork; and

signing, by the second subnetwork, a state information package of the second subnetwork with a permissible subset of secret key shares corresponding to the verification key of the second subnetwork, thereby generating a joint signature on the state information package of the second subnetwork, the state information package comprising an execution state or a hash of an execution state of the second subnetwork.

2. A computer-implemented method according to claim 1, further comprising

signing, by the first subnetwork, a state information package of the first subnetwork with a permissible subset of secret key shares corresponding to the verification key of the first subnetwork, thereby generating a joint signature on the state information package of the first subnetwork, the state information package comprising an execution state or a hash of an execution state of the first subnetwork.

3. A computer-implemented method according to claim 2, wherein the distributed network comprises a plurality of second subnetworks, wherein the state information package of the first subnetwork comprises a list comprising

the node verification keys of the plurality of second subnetworks; and

the plurality of nodes of the plurality of second subnetworks.

4. A computer-implemented method according to claim 1, wherein the performing of the second distributed key generation protocol for the second subnetwork comprises generating, by the nodes of the first subnetwork, the second verification key and a first set of corresponding secret key shares for the nodes of the first subnetwork; wherein each node of the first subnetwork holds one secret key share of the first set of secret key shares;

redistributing, by a secret-redistribution protocol, the secret key shares of the first set of secret key shares to the nodes of the second subnetwork, thereby creating a second set of secret key shares corresponding to the second verification key of the second subnetwork.

5. A computer-implemented method according to claim 1, further comprising

publishing the verification key of the second subnetwork together with the joint signature of the first subnetwork, thereby providing a certificate of the verification key of the second subnetwork.

6. A computer-implemented method according to claim 5, further comprising

verifying, by a node, in particular by a catch-up node that wants to connect or reconnect to the second subnetwork of the distributed network, the state information package by

verifying the verification key of the second subnetwork corresponding to the joint signature of the state information package by verifying the certificate with the verification key of the first

subnetwork; and verifying the joint signature on the state information package with the verified verification key of the second subnetwork corresponding to the joint signature of the state information package.

7. A computer-implemented method according to any of the preceding claims, further comprising generating, by the distributed network, a blockchain of blocks; wherein the state information package comprises block verification information for verifying subsequent blocks of the blockchain, in particular the validity of subsequent blocks.

8. A computer-implemented method according to claim 7, wherein the block verification information comprises a set of verification keys which are required to verify the validity of blocks of the blockchain.

9. A computer-implemented method according to claim 6, wherein the state information package of the second subnetwork comprises the verification key of the second subnetwork and the certificate.

10. A computer-implemented method according to any of the preceding claims, wherein the state information package further comprises

key generation information of the distributed key generation protocol that was used to generate the verification key of the second subnetwork.

11. A computer-implemented method according to any of the preceding claims, wherein the state information package comprises a complete set of

information which allows to synchronize the execution state of a catch-up node that wants to connect or reconnect to the distributed network with a recent execution state.

12. A computer-implemented method according to any of the preceding claims 7-11, further comprising adding, at predefined intervals, the state information package to a block of the blockchain.

13. A computer-implemented method according to any of the preceding claims 1-12,

wherein the state information package provides the execution state as a Merkle-tree structure, in particular as the hash root of the Merkle-tree structure.

14. A computer-implemented method according to claim 13, further comprising

requesting, by a catch-up node that wants to connect or reconnect to the second subnetwork from an up-to-date node of the second subnetwork, leaf hashes of the Merkle-tree structure;

comparing, by the catch-up node, the leaf hashes of its own state with the leaf hashes of the up-to-date node; and

requesting, by the catch-up node from the up-to-date node, only the state information corresponding to leaves with different leaf hashes.

15. A computer-implemented method according to any of the preceding claims, wherein the distributed

key generation protocol is a distributed threshold key generation protocol.

16. A computer-implemented method according to claim 4,

wherein the secret-redistribution protocol is a threshold key redistribution protocol.

17. A computer-implemented method according to any of the preceding claims, wherein the joint signature is a multi-signature.

18. A computer-implemented method according to any of the preceding claims, wherein the distributed key generation protocol comprises

accepting, by a catch-up node, one or more connections from unknown nodes;

limit the communication exchange with the unknown nodes to the communication concerning the state information package and the certificate; and

stop the communication with the unknown nodes once the state information package and the certificate have been received.

19. A distributed network comprising a plurality of nodes, wherein each of the plurality of nodes is configured to run one or more computational units, wherein each of the plurality of nodes is configured to run one or more computational units, wherein the computational units are configured to execute computations in a deterministic and replicated manner across the subnetworks of the plurality of nodes, thereby

traversing a chain of execution states, wherein the distributed network is configured to

perform, by a subset of the nodes of a first subnetwork of nodes, a first distributed key generation protocol, the first distributed key generation protocol being configured to generate jointly a verification key for the first subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the first subnetwork;

perform, for a second subnetwork, by a subset of the plurality of nodes of the first subnetwork, a second distributed key generation protocol, the second distributed key generation protocol being configured to generate jointly a verification key of the second subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the second subnetwork;

sign, by a subset of the nodes of the first subnetwork, the verification key of the second subnetwork with a permissible subset of the secret key shares of the nodes of the first subnetwork, thereby generating a joint signature on the verification key of the second subnetwork; and

sign, by the second subnetwork, a state information package of the second subnetwork with a permissible subset of secret key shares corresponding to the verification key of the second subnetwork, thereby generating a joint signature on the state information package of the second subnetwork, the state information package comprising an execution state or a hash of an execution state of the second subnetwork.

20. A node for a distributed network according to claim 19, the node being configured to

participate in a first distributed key generation protocol, the first distributed key generation protocol being configured to generate jointly a verification key for the first subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the first subnetwork;

participate in a second distributed key generation protocol, the second distributed key generation protocol being configured to generate jointly a verification key of the second subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the second subnetwork; and

participate in a joint signature of the verification key of the second subnetwork comprising a permissible subset of the secret key shares of the nodes of the first subnetwork; and

participate in a joint signature on the state information package of the second subnetwork comprising a permissible subset of secret key shares corresponding to the verification key of the second subnetwork, the state information package comprising an execution state or a hash of an execution state of the second subnetwork.

21. A computer program product for operating a distributed network, the distributed network comprising a plurality of nodes, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by one or more of the plurality of nodes to cause the one or more of the plurality of nodes to perform a method comprising

executing computations in a deterministic and replicated manner across the subnetworks of the plurality of nodes, thereby traversing a chain of execution states;

performing, by a subset of the nodes of a first subnetwork of nodes, a first distributed key generation protocol, the first distributed key generation protocol being configured to generate jointly a verification key for the first subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the first subnetwork;

performing, for a second subnetwork, by a subset of the plurality of nodes of the first subnetwork, a second distributed key generation protocol, the second distributed key generation protocol being configured to generate jointly a verification key of the second subnetwork and a plurality of corresponding secret key shares for a subset of the nodes of the second subnetwork;

signing, by a subset of the nodes of the first subnetwork, the verification key of the second subnetwork with a permissible subset of the secret key shares of the nodes of the first subnetwork, thereby generating a joint signature on the verification key of the second subnetwork; and

signing, by the second subnetwork, a state information package of the second subnetwork with a permissible subset of secret key shares corresponding to the verification key of the second subnetwork, thereby generating a joint signature on the state information package of the second subnetwork, the state information package comprising an execution state or a hash of an execution state of the second subnetwork.