

Claims

1. A distributed network comprising a plurality of network nodes, wherein

the distributed network is configured to perform a method for reaching a consensus on a sequence of values, in particular by an asynchronous consensus protocol, the method comprising

performing consecutive notarization rounds, the notarization rounds comprising

creating, by one or more network nodes, value proposals to be added to the sequence, the value proposals comprising a link to a parent value proposal of a previous notarization round;

communicating the value proposals to a notarization subset of the plurality of nodes;

performing, by the notarization subset of the plurality of nodes, a validity check of received value proposals, the validity check comprising a check whether the received value proposals comply with a predefined validity rule set;

executing and communicating, by the notarization subset of the plurality of nodes, individual notarization signatures on a subset of the value proposals that are valid according to the validity check, thereby creating individually-notary signed value proposals;

notarizing, by the distributed network, a value proposal once a predefined notary rule set has been fulfilled, in particular once a predefined number of individual notarization signatures has been collected, thereby creating a fully notarized value proposal for the respective notarization round;

performing, by the nodes of the notarization subset, a consistency check of the value proposals of one or more notarization rounds with respect to its own individual notarization signatures executed in the current notarization round, the consistency check comprising a check whether the value proposals of one or more of the consecutive notarization rounds comply with a predefined consistency rule set;

executing and communicating, by the nodes of the notarization subset, a consistency signature on a subset of the value proposals which are consistent according to the consistency rule set, thereby creating consistency-signed value proposals;

wherein the method further comprises a finality procedure, the finality procedure comprising

finalizing, by the distributed network, a value proposal once a predefined finality rule set has been fulfilled for the value proposal, thereby creating a finalized value, wherein the finality rule set comprises a predefined minimum number of consistency signatures; and

adding the finalized value to the sequence of values.

2. A network according to claim 1, the method further comprising

performing the consistency check once a fully notarized value proposal of a current notarization round has been observed.

3. A network according to claim 1 or claim 2, wherein the value proposals comprise the current notarization round number.

4. A network according to any of the preceding claims, wherein the validity rule set specifies that a

value proposal is only valid if its corresponding parent value proposal has been fully notarized.

5. A network according to any of the preceding claims, wherein performing the validity check of a received value proposal comprises a check of one or more features of the received value proposal.

6. A network according to claim 5, wherein the one or more features are selected from the group consisting of:

the network node that has created the received value proposal;

the content of the received value proposal; and

the content of a previous value proposal that is linked by the received value proposal.

7. A network according to any of the preceding claims, wherein a value proposal is considered to be consistent according to the consistency rule set if a respective node of the notarization subset has, in the current notarization round, not executed any individual notarization signature which is in conflict with the value proposal.

8. A network according to any of the preceding claims, wherein a value proposal of a current notarization round is considered to be consistent according to the consistency rule set if a respective node of the notarization subset has not executed in the current notarization round an individual notarization signature on any value proposal different from the value proposal.

9. A network according to any of the preceding claims, wherein a value proposal of a previous notarization round is considered to be consistent according to the consistency rule set if all value proposals for which a respective node of the notarization subset has executed an

individual notarization signature in the current notarization round refer back to the value proposal of the previous notarization round.

10. A network according to any of the preceding claims, wherein the finality rule set is configured to be fulfilled for a value proposal once a predefined number of consistency signatures has been observed for the value proposal.

11. A network according to any of the preceding claims, wherein the finality rule set is configured to be fulfilled for a value proposal once

a predefined number of consistency signatures has been observed for the value proposal; and

the value proposal has been fully notarized.

12. A network according to any of the preceding claims, wherein the method further comprises moving to the next notarization round of the method once a fully notarized value proposal of a current notarization round has been observed.

13. A network according to any of the preceding claims, wherein the notarization rounds comprise a timeout period at the beginning of each notarization round, wherein the notarization subset of the plurality of nodes is configured to wait with the execution of the individual notarization signatures until the timeout period has expired.

14. A network according to claim 13, wherein the network is further configured to dynamically adjust the timeout period.

15. A network according to any of the preceding claims, the method further comprising

broadcasting, by the distributed network, the individual notarization signatures to the nodes of the notarization subset.

16. A network according to any of the preceding claims, the method further comprising

broadcasting, by the distributed network, the consistency signatures within the distributed network.

17. A network according to any of the preceding claims, wherein communicating the value proposals to the notarization subset comprises broadcasting the value proposals.

18. A network according to any of the preceding claims claim 15-17, wherein the broadcasting is performed by means of a gossip-protocol.

19. A network according to any of the preceding claims, wherein the network is configured to

add a finality signature of the respective last finalized value to the value proposals of the current notarization round.

20. A network according to any of the preceding claims, wherein the network is configured to

use the same notarization subset for a predefined time period.

21. A network according to claim 20, wherein the network is configured to

select the nodes of the notarization subset in dependence on the stake of the nodes.

22. A network according to any of the preceding claims, wherein the network is configured to

regularly change the nodes of the notarization subset.

23. A network according to claim 22, wherein the network is configured to

select the nodes of the notarization subset in dependence on a randomness beacon.

24. A network according to any of the preceding claims, wherein the individual notarization signatures and/or the consistency signatures are based on a signature scheme selected from the group consisting of:

- a threshold signature scheme;
- a multi-signature scheme; and
- an aggregate signature scheme.

25. A network according to any of the preceding claims, wherein the consistency-signed value proposals comprise

- the notarization round number to be finalized;
- the current notarization round number; and
- the signing node.

26. A network according to any of the preceding claims, wherein the values are blocks to be written to a blockchain.

27. A network according to claim 26, wherein performing the validity check of received value proposals comprises performing a verification of block headers of block proposals.

28. A network according to claim 26 or 27, wherein performing the validity check of received block proposals comprises performing a verification of the payload of block proposals.

29. A network according to any of the preceding claims, wherein the distributed network is configured to assign a rank to a value proposal, in particular according to a node rank of the corresponding node.

30. A network according to claim 29, wherein performing the validity check comprises

- disregarding invalid value proposals; and

compiling a list of valid value proposals;
and wherein executing the individual notarization signatures comprises

executing a single individual notarization signature only on the valid value proposal with the highest rank of the list.

31. A network according to any of the preceding claims,

wherein the step of performing the consistency check is performed for a single notarization round to be finalized.

32. A network according to any of the preceding claims 1 -30,

wherein the network is configured to perform the consistency check for multiple notarization rounds to be finalized.

33. A network according to claim 31, wherein the step of performing the consistency check is performed only for the current notarization round.

34. A network according to claim 31, wherein the step of performing the consistency check is performed for the d-th last notarization round, wherein d is an integer.

35. A network according to claim 31, wherein the step of performing the consistency check is performed for the oldest notarization round that is $0 \bmod n$ and has not been finalized, wherein n is a predefined integer.

36. A network according to any of the preceding claims, wherein

the network is configured to select a number n of the nodes of the notarization subsets, a predefined number t1 of individual notarization signatures required to notarize a value proposal and to create a fully

notarized value proposal and a predefined number t_2 of consistency signatures required to fulfill the finality rule set and to finalize a value proposal according to the equation as follows:

$$t_1 + t_2 > n + f;$$

wherein the network is configured for the security assumption that in every notarization subset at most f nodes are Byzantine, while the rest is honest.

37. A network according to any of the preceding claims, wherein

the communicating of the value proposals to the notarization subset is performed during a first period of the notarization rounds; and

the execution of the individual notarization signatures and of the consistency signatures and the communicating, in particular a broadcasting, of the individual notarization signatures and the consistency signatures is performed during a second period of the notarization rounds.

38. A network according to claim 37, wherein the first period of the notarization rounds is at least as long as the second period of the notarization rounds, in particular at least twice as long as the second period.

39. A network according to claim 38 or claim 37, wherein

the value proposals have a size of at least 1 MByte; and

the individual notarization signatures and the consistency signatures have a size of less than 200 Byte.

40. A network according to any of the preceding claims, wherein

the distributed network is configured to use at least 60% of the time for communicating the value proposals.

41. A computer-implemented method for reaching a consensus on a sequence of values by an asynchronous consensus protocol to be performed in a distributed network, the method comprising

performing consecutive notarization rounds, the notarization rounds comprising

creating, by one or more network nodes of the distributed network, value proposals to be added to the sequence, the value proposals comprising a link to a parent value proposal of a previous notarization round;

communicating the value proposals to a notarization subset of the plurality of nodes;

performing, by the notarization subset of the plurality of nodes, a validity check of received value proposals, the validity check comprising a check whether the received value proposals comply with a predefined validity rule set;

executing and communicating, by the notarization subset of the plurality of nodes, individual notarization signatures on a subset of the value proposals that are valid according to the validity check, thereby creating individually-notary signed value proposals;

notarizing, by the distributed network, a value proposal once a predefined notary rule set has been fulfilled, in particular once a predefined number of individual notarization signatures has been collected, thereby creating a fully notarized value proposal for the respective notarization round;

performing a consistency check of the value proposals of one or more notarization rounds with respect

to its own individual notarization signatures executed in the current notarization round, the consistency check comprising a check whether the value proposals comply with a predefined consistency rule set;

executing and communicating, by the nodes of the notarization subset, a consistency signature on a subset of the value proposals which are consistent according to the consistency rule set;

performing a finality procedure comprising

finalizing, by the distributed network, a value proposal once a predefined finality rule set has been fulfilled for the value proposal, thereby creating a finalized value, wherein the finality rule set comprises a predefined minimum number of consistency signatures; and

adding the finalized value to the sequence of values.

42. A network node for a distributed network according to any of the preceding claims 1-40, wherein the network node is in particular configured to perform one or more steps of the method according to claim 41.

43. A computer program product for operating a distributed network according to any of the preceding claims 1-40, the distributed network comprising a plurality of network 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 one or more of the steps of the computer-implemented method according to claim 41.

44. A computer program product for operating a node of a distributed network according to any of the

preceding claims 1-40, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by the node to cause the node to perform one or more of the steps of the computer-implemented method according to claim 41.