

CLAIMS

1. A non-transitory computer readable medium, wherein a software architecture is encoded on the non-transitory computer readable medium, the software architecture comprising:

a first protocol, wherein the first protocol is configured to form a plurality of groups, wherein each group of the plurality of groups comprises a set of randomly selected nodes from a network;

a second protocol, wherein the second protocol is configured to randomly select a first group from the plurality of groups formed by the first protocol;

a third protocol, wherein the third protocol is configured to designate the first group to sign a first message by generating a first group signature;

a hash function, wherein the hash function is configured to generate a hash value from the first group signature, wherein the hash value is configured to select a plurality of block makers; and

a twelfth protocol, wherein the twelfth protocol is configured to prioritize each block maker of the plurality of block makers based on a ranking system,

wherein the ranking system comprises:

an eighth protocol, wherein the eighth protocol is configured to derive a rank for the each block maker of the plurality of block makers, wherein the rank is derived from the first group signature;

a ninth protocol, wherein the ninth protocol is configured to assign a plurality of first weights, to each block associated with a respective block maker of the plurality of block makers, wherein each first weight of the plurality of first weights of the each block is based on the rank of the respective block maker of the plurality of block makers; and

a tenth protocol, wherein the tenth protocol is configured to assign a second weight to at least one chain of blocks, wherein the second weight of the at least one chain of blocks is based on the each first weight of the each block in the at least one chain of blocks, wherein a block of the at least one chain of blocks references another block of the at least one chain of blocks.

2. The software architecture of claim 1, wherein the hash value is configured to select a second group, wherein the second group comprises a node from the network.
3. The software architecture of claim 1, wherein a size of the each group of the plurality of groups is a system parameter.
4. The software architecture of claim 1, wherein the first group signature is configured to be generated by a threshold set of the first group, wherein a size of the threshold set is smaller than or equal to a size of the first group.
5. The software architecture of claim 1, wherein the first message comprises a value derived from a preceding group signature.
6. The software architecture of claim 1, wherein the first message is a system parameter.
7. The software architecture of claim 1, further comprising a universal network, wherein each node of the universal network is configured to interact with each other via a communication channel.
8. The software architecture of claim 7, wherein the communication channel comprises at least one of a peer-to-peer network, a broadcast network, or a gossip network.
9. The software architecture of claim 1, wherein the second protocol is configured to select the first group from the plurality of groups based on a seed.
10. The software architecture of claim 9, wherein the seed is derived from a preceding group signature produced by the third protocol.
11. The software architecture of claim 10, wherein the derivation of the seed from the preceding signature is by the hash function.
12. The software architecture of claim 1, further comprising a setup protocol, wherein the setup protocol is configured to establish a group public key for the first group of the plurality of groups formed by the first protocol, wherein the first group signature is configured to be validated by the group public key.
13. The software architecture of claim 12, wherein the first group signature is configured to be unique to the group public key and the first message.

14. The software architecture of claim 13, wherein the first group signature is based on at least one of bilinear pairings, bilinear pairings on elliptic curves, Gap Diffie-Hellman groups (GDH) or Boneh-Lynn-Shacham (BLS) signature scheme.
15. The software architecture of claim 12, wherein the setup protocol is configured to establish an individual private key share for each node of the each group of the plurality of groups formed by the first protocol.
16. The software architecture of claim 15, wherein the individual private key shares of each of the nodes of a threshold set of the first group are configured to be used for generating the first group signature, wherein a size of the threshold set is smaller than or equal to a size of the first group.
17. The software architecture of claim 1, further comprising a sixth protocol, wherein the sixth protocol is configured to nominate a plurality of nodes, wherein the set of randomly selected nodes are part of the plurality of nodes.
18. The software architecture of claim 17, wherein the sixth protocol is configured to adapt a methodology for nominating the plurality of nodes, wherein the methodology comprises at least one of a proof-of-work puzzle, an external third-party endorsement, or a validation of computational resources.
19. The software architecture of claim 17, wherein the sixth protocol is configured to assess a monetary value associated with each node of the plurality of nodes.
20. The software architecture of claim 17, further comprising a seventh protocol, wherein the seventh protocol is configured to detect misbehavior of a select node of the set of randomly selected nodes.
21. The software architecture of claim 20, wherein the seventh protocol is configured to penalize the select node.
22. The software architecture of claim 20, wherein the seventh protocol is configured to revoke a nomination of the select node.
23. The software architecture of claim 1, further comprising a thirteenth protocol, wherein the thirteenth protocol is configured to prioritize each block among a plurality of blocks available for timestamping; and

a fourth protocol, wherein the fourth protocol is configured to designate the first group to timestamp a prioritized block of the plurality of blocks.

24. The software architecture of claim 1, further comprising a fourth protocol, wherein the fourth protocol is configured to designate the first group to timestamp a first block of a plurality of blocks.

25. The software architecture of claim 24, wherein the timestamp is configured to be generated by a threshold set of the first group, wherein a size of the threshold set is smaller than or equal to a size of the first group.

26. The software architecture of claim 24, further comprising a fifth protocol, wherein the fifth protocol is configured to broadcast at least one of the timestamp or a timestamped first block to the network.

27. The software architecture of claim 1, further comprising a fourth protocol, and wherein the fourth protocol is configured to designate the first group to validate a first block of a plurality of blocks.

28. The software architecture of claim 27, further comprising a fifth protocol, wherein the fifth protocol is configured to broadcast a notarization or a notarized first block.

29. The software architecture of claim 1, wherein each block maker of the plurality of block makers is configured to create a plurality of blocks, wherein a block of the plurality of blocks references another block of the plurality of blocks.

30. The software architecture of claim 29, wherein the another block is at least one of timestamped or notarized.

31. The software architecture of claim 29, wherein the block comprises transactions collected by a block maker of the plurality of block makers.

32. The software architecture of claim 1, further comprising an eleventh protocol, wherein the eleventh protocol is configured to select a preceding block of a chain of blocks of the at least one chain of blocks based on a factor, wherein the factor comprises the first weight of the preceding block of the chain of blocks or the second weight of the chain of blocks.

33. A non-transitory computer readable medium, wherein a software architecture is encoded on the non-transitory computer readable medium, the software architecture comprising:

a first protocol, wherein the first protocol is configured to form a plurality of groups, wherein each group of the plurality of groups comprises a set of randomly selected nodes from a network;

a second protocol, wherein the second protocol is configured to randomly select a first group from the plurality of groups formed by the first protocol;

a third protocol, wherein the third protocol is configured to designate the first group to sign a first message by generating a first group signature;

a hash function, wherein the hash function is configured to generate a hash value from the first group signature, wherein the hash value is configured to select a plurality of block makers; and

a twelfth protocol, wherein the twelfth protocol is configured to prioritize each block maker of the plurality of block makers based on a ranking system,

wherein the ranking system comprises:

an eighth protocol, wherein the eighth protocol is configured to derive a rank for the each block maker of the plurality of block makers, wherein the rank is derived from the first group signature;

a ninth protocol, wherein the ninth protocol is configured to assign a plurality of first weights, to each block associated with a respective block maker of the plurality of block makers, wherein each first weight of the plurality of first weights of the each block is based on the rank of the respective block maker of the plurality of block makers;

a tenth protocol, wherein the tenth protocol is configured to assign a second weight to at least one chain of blocks, wherein the second weight of the at least one chain of blocks is based on the each first weight of the each block in the at least one chain of blocks, wherein a block of the at least one chain of blocks references another block of the at least one chain of blocks; and

an eleventh protocol, wherein the eleventh protocol is configured to select a preceding block of a chain of blocks of the at least one chain of blocks based on a factor, wherein the factor comprises the first weight of the preceding block of the chain of blocks or the second weight of the chain of blocks.

34. The software architecture of claim 33, further comprising a hash function, wherein the hash function is configured to generate a hash value from the first group signature.
35. The software architecture of claim 33, further comprising a sixth protocol, wherein the sixth protocol is configured to nominate a plurality of nodes, wherein the set of randomly selected nodes are part of the plurality of nodes.
36. The software architecture of claim 33, further comprising a setup protocol, wherein the setup protocol is configured to establish a group public key for the first group of the plurality of groups formed by the first protocol, wherein the first group signature is configured to be validated by the group public key.
37. The software architecture of claim 36, wherein the first group signature is configured to be unique to the group public key and the first message.