

CLAIMS

1. A software architecture encoded on a 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 creation protocol, wherein the creation protocol is configured to create a plurality of dealing messages, wherein each dealing message of the plurality of dealing messages comprises information from each dealer node in a selected group of the plurality of groups;

a hash function, wherein the hash function is configured to generate a hash value from the each dealing message of the plurality of dealing messages;

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

a fifth protocol, wherein the fifth protocol is configured to broadcast a plurality of blocks to a network, wherein each block of the plurality of blocks comprises a dealing message of the plurality of dealing messages;

a fourth protocol, wherein the fourth protocol is configured to notarize the each block of the plurality of blocks, wherein the notary group is configured to use the fourth protocol; and

a reading protocol, wherein the reading protocol is configured to read the dealing message to a receiver node of the selected group, wherein the receiver node is different from a dealer node whose information is contained in the corresponding dealing message; and

a verification protocol, wherein the verification protocol is configured to verify veracity of the corresponding dealing message, wherein the verification protocol is configured to be run by the receiver node;

~~a complaint protocol, wherein the complaint protocol is configured to generate a complaint message, wherein the complaint message is signed by the receiver node, and wherein the complaint protocol is configured to be run by the receiver node;~~

~~a justification protocol, wherein the justification protocol is configured to create a justification message, wherein the justification message comprises justifications to the complaint message, wherein the dealer node is configured to run the justification protocol to create the justification message; and~~

~~a registration protocol, wherein the registration protocol is configured to consolidate confirmation of a plurality of justified public keys, wherein each justified public key of the plurality of justified public keys corresponds to the each dealing message, wherein the verification protocol has accepted veracity of each justified public key of the plurality of justified public keys.~~

2. The software architecture of claim 1, wherein the creation protocol is configured to be run by each dealer node of the selected group.

3. The software architecture of claim 1, wherein the reading protocol is configured to be run by each receiver node of the selected group.

4. ~~The software architecture of claim 1, further comprising:~~

~~— a second protocol, wherein the second protocol is configured to select a first group from the plurality of groups formed by the first protocol.~~

~~45.~~ The software architecture of claim ~~14~~, wherein the first group comprises the selected group.

~~56.~~ The software architecture of claim 1, wherein the verification protocol is configured to verify an encrypted key share from the dealer node relative to a verification vector, wherein the information in the corresponding dealing message comprises the encrypted key share from the dealer node and the verification vector.

~~67.~~ The software architecture of claim ~~56~~, wherein the verification protocol run by the receiver node is configured to verify the encrypted key share from the dealer node relative to the verification vector of the dealer node.

78. The software architecture of claim 6, further comprising a complaint protocol, wherein the complaint protocol is configured to generate a complaint message, wherein the complaint message is signed by the receiver node, and wherein the complaint protocol is configured to be run by the receiver node~~message comprises data regarding a lack of verification of the encrypted key share relative to the verification vector.~~

89. The software architecture of claim 74, wherein the complaint message comprises data regarding a lack of verification~~of the encrypted key share relative to the verification vector~~protocol is configured to verify veracity of the justification message relative to the verification vector, wherein the verification protocol is configured to be run by a verifying node.

940. The software architecture of claim 79, wherein the fifth~~verification protocol is configured to broadcast the complaint message to the network~~rejects veracity of the justification message.

104. The software architecture of claim 9, further comprising a justification protocol, wherein the justification protocol is configured to create a justification message, wherein the verification protocol accepts veracity of the justification message~~comprises justifications to the complaint message, wherein the dealer node is configured to run the justification protocol to create the justification message.~~

112. The software architecture of claim 10, wherein the fifth~~registration protocol is configured to broadcast the justification message to the network~~run by the verifying node.

123. The software architecture of claim 11, further comprising a second protocol, wherein the second protocol is configured to randomly select a notary group from the plurality of groups, wherein the verification protocol is configured to verify veracity of the justification message relative to the verification vector, wherein the verification protocol is configured to be run by a verifying node~~notary group is configured to use the fourth protocol.~~

134. The software architecture of claim 12, wherein the verification protocol rejects veracity of the justification message~~further comprising a fifth protocol, wherein the fifth protocol is configured to broadcast a plurality of blocks to a network, wherein each block~~

~~of the plurality of blocks comprises a dealing message of the plurality of dealing messages.~~

145. The software architecture of claim 134, further comprising ~~thea creation~~^{fourth} protocol, wherein the ~~creation~~^{fourth} protocol is configured to ~~create a plurality of second dealing messages, wherein each second dealing message of the plurality of second dealing messages comprises information about each dealer node in a second selected group of the plurality of groups~~^{notarize the each block of the plurality of blocks.}

15. The software architecture of claim 12, wherein the verification protocol accepts veracity of the justification message.

16. The software architecture of claim 15, further comprising a registration protocol, wherein the registration protocol is configured to consolidate confirmation of a plurality of justified public keys, wherein each justified public key of the plurality of justified public keys corresponds to the each dealing message, wherein the verification protocol has accepted veracity of each justified public key of the plurality of justified public keys.

17. The software architecture of claim 16, wherein the registration protocol is run by the verifying node.

18. The software architecture of claim 16, wherein the fifth protocol is configured to broadcast a consolidated confirmation to the network.

19. The software architecture of claim 1, further comprising a registration protocol, wherein the registration protocol is configured to consolidate a plurality of dealing messages of the selected group, wherein the registration protocol is run by the each receiver node.

20. The software architecture of claim 1, further comprising a second protocol, wherein the second protocol is configured to randomly select a notary group from the plurality of groups, wherein the notary group is configured to use the fourth protocol.

21. A software architecture encoded on a 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 creation protocol, wherein the creation protocol is configured to create a plurality of dealing messages, wherein each dealing message of the plurality of dealing messages comprises information from each dealer node in a selected group of the plurality of groups;

a fifth protocol, wherein the fifth protocol is configured to broadcast a plurality of blocks to a network, wherein each block of the plurality of blocks comprises a dealing message of the plurality of dealing messages;

a reading protocol, wherein the reading protocol is configured to read the dealing message to a receiver node of the selected group, wherein the receiver node is different from a dealer node whose information is contained in the corresponding dealing message

a verification protocol, wherein the verification protocol is configured to verify veracity of the corresponding dealing message, wherein the verification protocol is configured to be run by the receiver node;

a complaint protocol, wherein the complaint protocol is configured to generate a complaint message, wherein the complaint message is signed by the receiver node, and wherein the complaint protocol is configured to be run by the receiver node;

a justification protocol, wherein the justification protocol is configured to create a justification message, wherein the justification message comprises justifications to the complaint message, wherein the dealer node is configured to run the justification protocol to create the justification message; and

a registration protocol, wherein the registration protocol is configured to consolidate confirmation of a plurality of justified public keys, wherein each justified public key of the plurality of justified public keys corresponds to the each dealing message, wherein the verification protocol has accepted veracity of each justified public key of the plurality of justified public keys;

wherein the verification protocol is configured to verify veracity of the justification message relative to the verification vector, wherein the verification protocol is configured to be run by a verifying node and the verification protocol accepts or rejects veracity of the justification message.

22. The software architecture of claim 21, wherein the creation protocol is configured to be run by each dealer node of the selected group.

23. The software architecture of claim 21, wherein the reading protocol is configured to be run by each receiver node of the selected group.

24. The software architecture of claim 21, further comprising:

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

25. The software architecture of claim 24, wherein the first group comprises the selected group.

26. The software architecture of claim 21, wherein the verification protocol is configured to verify an encrypted key share from the dealer node relative to a verification vector, wherein the information in the corresponding dealing message comprises the encrypted key share from the dealer node and the verification vector.

27. The software architecture of claim 26, wherein the verification protocol run by the receiver node is configured to verify the encrypted key share from the dealer node relative to the verification vector of the dealer node.

28. The software architecture of claim 26, wherein the complaint message comprises data regarding a lack of verification of the encrypted key share relative to the verification vector.