

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 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; and
 - a hash function, wherein the hash function is configured to generate a hash value from the first group signature.
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.