

WHAT IS CLAIMED IS:

1 1. A method, performed by a node in a computer network including a
2 plurality of nodes, each node having a node identifier, the method comprising:

3 a) receiving, by the node, node identifiers from other nodes of the plurality
4 of nodes in the computer network;

5 b) determining, by the node, a plurality of node committees in a sampler
6 graph comprising a plurality of nodes, wherein the node is present in a node committee
7 in the plurality of node committees;

8 c) the node, further

9 i) generating a random string;

10 ii) performing a proof of work process using the random string and
11 a hash function;

12 iii) if the proof of work process yields a solution that is acceptable,
13 then broadcasting the solution to all other nodes in the plurality of nodes, wherein the
14 other nodes verify the solution; and

15 iv) if the other nodes verify the solution, the node is elected to a
16 subcommittee for the node committee, wherein the subcommittee updates the sampler
17 graph; and

18 d) repeating steps b) and c) until a leader committee is determined.

1 2. The method of claim 1, further comprising:

2 determining, by the node, the sampler graph based upon the node
3 identifiers and a predefined seed, the sampler graph comprising the plurality of nodes,
4 wherein every node determines the sampler graph locally.

1 3. The method of claim 2, wherein the sampler graph is a random
2 bipartite graph with the plurality of nodes and the plurality of node committees.

1 4. The method of claim 1, wherein every node in a node committee
2 performs steps i) through iv).

1 5. The method of claim 1, wherein the node is a first node, and the
2 solution is a first solution, and the method further comprises:
3 receiving, by the first node, a second solution from a second node in the
4 node committee;
5 verifying, by the first node, the second solution; and
6 electing, by the first node, the second node to the subcommittee if the
7 second solution is acceptable.

1 6. The method of claim 1 further comprising:
2 determining, by the node, the leader committee based on the sampler
3 graph, wherein the sampler graph indicates a number of nodes in the sampler graph,
4 and wherein the number of nodes in the sampler graph is less than a predefined
5 threshold.

1 7. The method of claim 1 further comprising:
2 partitioning, by the node in the leader committee, the plurality of nodes in
3 the computer network to form sharding committees.

1 8. The method of claim 1, wherein the node identifier is a public key.

1 9. A method comprising:
2 receiving, by a first node in a first committee in a computer network, a
3 request including a node identifier to join a committee by a second node;
4 providing, by the first node of the first committee to the second node, a
5 proof of work process to the second node;
6 receiving, by first node of the first committee, a solution to the proof of
7 work process from the second node, wherein a plurality of nodes in the first committee
8 verifies the solution;
9 generating, by the first node of the first committee a random string, which
10 is used by the first node to determine a second committee for the second node;

11 introducing, by the first node to second committee, the second node,
12 wherein the second committee displaces a node to allow the second node to join the
13 second committee; and
14 communicating, by the first node, information regarding the second node
15 being in the second committee to other nodes in the computer network.

1 10. The method of claim 9, wherein the second committee displaces a
2 random number of nodes of the second committee based on a random value generated
3 by a leader committee.

1 11. The method of claim 9, wherein displaced nodes are assigned to
2 random inactive committees.

1 12. The method of claim 9, wherein the first node is a leader node of
2 the first committee.

1 13. The method of claim 9, wherein the plurality of nodes in the first
2 committee verify the solution if the solution solves the proof of work process, is less
3 than a predetermined security value, and is received within a predetermined amount of
4 time.

1 14. The method of claim 9, wherein at least two thirds of nodes in each
2 committee in the computer network are non-malicious nodes.

1 15. A method comprising:
2 receiving, by a first node in a committee, an interaction request, the
3 interaction request including interaction data from a client computer;
4 incorporating, by the first node, the interaction data along with other
5 interaction data associated with other client computers into a block comprising
6 interaction data, wherein the block includes block parts;
7 broadcasting, by the first node, the block to other nodes in the committee,
8 wherein the other nodes in the committee verify the block; and
9 incorporating the block into a shard of a blockchain managed by the
10 committee.

1 16. The method of claim 15, wherein the committee is a verification
2 committee, and if the block parts of the interaction data or the other interaction data
3 cannot be validated by the other nodes in the committee, the method further comprises:
4 contacting, by the first node, a source committee with nodes to validate
5 the block parts.

1 17. The method of claim 16, wherein the source committee verifies the
2 block parts and transmits a verification message to the verification committee.

1 18. The method of claim 16 further comprising:
2 determining, by the first node, the source committee based on the block
3 parts.

1 19. The method of claim 15 further comprising:
2 receiving, by the first node, a plurality of blocks from the other nodes in the
3 committee; and
4 merging, by the first node, the plurality of blocks with the block.

1 20. The method of claim 15 further comprising:
2 generating, by the first node, a list of all block parts to be verified.

1 21. The method of claim 15, wherein the committee includes more than
2 5 nodes.

1 22. A method comprising:
2 determining, by a first node in a computer network, a leader committee
3 comprising a plurality of elected nodes including the first node, the leader committee
4 being a first committee;
5 receiving, by the first node, a request from a second node to join a
6 committee of the computer network, the request including a node identifier;
7 determining, by the first node, that the second node can join a second
8 committee based on a proof of work process computed by the second node;

9 introducing, by the first node to the second committee, the second node,
10 wherein the second committee displaces a node to allow the second node to join the
11 second committee, wherein information regarding the second node being in the second
12 committee is communicated to other nodes in the computer network;
13 receiving, by the first node, an interaction request, the interaction request
14 including interaction data from a client computer;
15 incorporating, by the first node, the interaction data along with other
16 interaction data associated with other client computers into a block comprising
17 interaction data, wherein the block includes block parts;
18 broadcasting, by the first node, the block to other nodes in the committee,
19 wherein the other nodes in the committee verify the block; and
20 incorporating the block into a shard of a blockchain managed by the first
21 committee.

1 23. A node comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for performing the
6 method according to any of the preceding claims.

1