WHAT IS CLAIMED IS:

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

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

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

c) the node, further

i) generating a random string;

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

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

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

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

2. The method of claim 1, further comprising:

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

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

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

5. The method of claim 1, wherein the node is a first node, and the solution is a first solution, and the method further comprises:

receiving, by the first node, a second solution from a second node in the node committee;

verifying, by the first node, the second solution; and

electing, by the first node, the second node to the subcommittee if the second solution is acceptable.

6. The method of claim 1 further comprising:

determining, by the node, the leader committee based on the sampler graph, wherein the sampler graph indicates a number of nodes in the sampler graph, and wherein the number of nodes in the sampler graph is less than a predefined threshold.

7. The method of claim 1 further comprising:

partitioning, by the node in the leader committee, the plurality of nodes in the computer network to form sharding committees.

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

9. A node comprising:

a processor;

a memory device; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method performed by a node in a computer network including a plurality of nodes, each node having a node identifier, the method comprising:

a) receiving node identifiers from other nodes of the plurality of nodes in the computer network;

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

c) the node, further

i) generating a random string;

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

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

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

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

10. The node of claim 9, wherein the method further comprises:

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

11. The node of claim 9, wherein the sampler graph is a random bipartite graph with the plurality of nodes and the plurality of node committees.

12. The node of claim 9, wherein every node in a node committee performs steps i) through iv).

13. The node of claim 9, wherein the node is a first node, and the solution is a first solution, and wherein the method further comprises:

receiving a second solution from a second node in the node committee;

verifying the second solution; and

electing the second node to the subcommittee if the second solution is acceptable.

14. The node of claim 9, wherein the method further comprises:

determining the leader committee based on the sampler graph, wherein the sampler graph indicates a number of nodes in the sampler graph, and wherein the number of nodes in the sampler graph is less than a predefined threshold.

15. The node of claim 9, wherein the method further comprises:

partitioning the plurality of nodes in the computer network to form sharding committees.

16. The method of claim 9, wherein the node identifier is a public key.

17. A method comprising:

receiving, by a first node in a first committee in a computer network, a request including a node identifier to join a committee by a second node;

providing, by the first node of the first committee to the second node, a proof of work process to the second node;

receiving, by first node of the first committee, a solution to the proof of work process from the second node, wherein a plurality of nodes in the first committee verifies the solution;

generating, by the first node of the first committee a random string, which is used by the first node to determine a second committee for the second node;

introducing, by the first node to second committee, the second node, wherein the second committee displaces a node to allow the second node to join the second committee; and

communicating, by the first node, information regarding the second node being in the second committee to other nodes in the computer network.

18. The method of claim 17, wherein the second committee displaces a random number of nodes of the second committee based on a random value generated by a leader committee.

19. The method of claim 17, wherein displaced nodes are assigned to random inactive committees.

20. The method of claim 17, wherein the first node is a leader node of the first committee.

21. The method of claim 17, wherein the plurality of nodes in the first committee verify the solution if the solution solves the proof of work process, is less than a predetermined security value, and is received within a predetermined amount of time.

22. The method of claim 17, wherein the first node is a leader node of the first committee.

23. The method of claim 17, wherein at least two thirds of nodes in each committee in the computer network are non-malicious nodes.

24. A node comprising:

a processor;

a memory device; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

receiving, by a first node in a first committee in a computer network, a request including a node identifier to join a committee by a second node;

providing, by the first node of the first committee to the second node, a proof of work process to the second node;

receiving, by first node of the first committee, a solution to the proof of work process from the second node, wherein a plurality of nodes in the first committee verifies the solution;

generating, by the first node of the first committee a random string, which is used by the first node to determine a second committee for the second node;

introducing, by the first node to second committee, the second node, wherein the second committee displaces a node to allow the second node to join the second committee; and

communicating, by the first node, information regarding the second node being in the second committee to other nodes in the computer network.

25. The node of claim 24, wherein the second committee displaces a random number of nodes of the second committee based on a random value generated by a leader committee.

26. The node of claim 25, wherein displaced nodes are assigned to random inactive committees.

27. The node of claim 24, wherein the first node is a leader node of the first committee.

28. The node of claim 24, wherein the plurality of nodes in the first committee verify the solution if the solution solves the proof of work process, is less than a predetermined security value, and is received within a predetermined amount of time.

29. The node of claim 24, wherein the first node is a leader node of the first committee.

30. The node of claim 24, wherein at least two thirds of nodes in each committee in the computer network are non-malicious nodes.

31. A method comprising:

receiving, by a first node in a committee, an interaction request, the interaction request including interaction data from a client computer;

incorporating, by the first node, the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting, by the first node, the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the committee.

~~32. The method of claim 31, wherein the committee is a verification committee, and if the block parts of the interaction data or the other interaction data cannot be validated by the other nodes in the committee, the method further comprises:~~

~~contacting, by the first node, a source committee with nodes to validate the block parts.~~

~~33. The method of claim 32, wherein the source committee verifies the block parts and transmits a verification message to the verification committee.~~

~~34. The method of claim 32 further comprising:~~

~~determining, by the first node, the source committee based on the block parts.~~

~~35. The method of claim 31 further comprising:~~

~~receiving, by the first node, a plurality of blocks from the other nodes in the committee; and~~

~~merging, by the first node, the plurality of blocks with the block.~~

~~36. The method of claim 31 further comprising:~~

~~generating, by the first node, a list of all block parts to be verified.~~

~~37. The method of claim 31, wherein the committee includes more than 5 nodes.~~

~~38. A node comprising:~~

~~a processor;~~

~~a memory device; and~~

~~a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:~~

~~receiving, by a first node in a committee, an interaction request, the interaction request including interaction data from a client computer;~~

incorporating, by the first node, the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting, by the first node, the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the committee.

39. The node of claim 38, wherein the committee is a verification committee, and if the block parts of the interaction data or the other interaction data cannot be validated by the other nodes in the committee, the method further comprises:

contacting a source committee with nodes to validate the block parts.

40. The node of claim 39, wherein the source committee verifies the block parts and transmits a verification message to the verification committee.

41. The node of claim 39, wherein the method further comprises:

determining, by the first node, the source committee based on the block parts.

42. The method of claim 38, wherein the method further comprises:

receiving, by the first node, a plurality of blocks from the other nodes in the committee; and

merging, by the first node, the plurality of blocks with the block.

43. The method of claim 38, wherein the method further comprises:

generating, by the first node, a list of all block parts to be verified.

44. The method of claim 43, wherein the blockchain comprises data regarding payment transactions.

45. A method comprising:

determining, by a first node in a computer network, a leader committee comprising a plurality of elected nodes including the first node, the leader committee being a first committee;

receiving, by the first node, a request from a second node to join a committee of the computer network, the request including a node identifier;

determining, by the first node, that the second node can join a second committee based on a proof of work process computed by the second node;

introducing, by the first node to the second committee, the second node, wherein the second committee displaces a node to allow the second node to join the second committee, wherein information regarding the second node being in the second committee is communicated to other nodes in the computer network;

receiving, by the first node, an interaction request, the interaction request including interaction data from a client computer;

incorporating, by the first node, the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting, by the first node, the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the first committee.

46. A node comprising:

a processor;

a memory device; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

determining, by a first node in a computer network, a leader committee comprising a plurality of elected nodes including the first node, the leader committee being a first committee;

receiving a request from a second node to join a committee of the computer network, the request including a node identifier;

determining that the second node can join a second committee based on a proof of work process computed by the second node;

introducing the second node to the second committee, wherein the second committee displaces a node to allow the second node to join the second committee, wherein information regarding the second node being in the second committee is communicated to other nodes in the computer network;

receiving an interaction request, the interaction request including interaction data from a client computer;

incorporating the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the first committee.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a first node in a first committee in a computer network, a request including a node identifier to join a committee by a second node;

providing, by the first node of the first committee to the second node, a proof of work process to the second node;

receiving, by first node of the first committee, a solution to the proof of work process from the second node, wherein a plurality of nodes in the first committee verifies the solution;

generating, by the first node of the first committee a random string, which is used by the first node to determine a second committee for the second node;

introducing, by the first node to second committee, the second node, wherein the second committee displaces a node to allow the second node to join the second committee; and

communicating, by the first node, information regarding the second node being in the second committee to other nodes in the computer network.

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

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

4. The method of claim 1, wherein the first node is a leader node of the first committee.

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

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

7. A method comprising:

receiving, by a first node in a committee, an interaction request, the interaction request including interaction data from a client computer;

incorporating, by the first node, the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting, by the first node, the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the committee.

8. The method of claim 7, wherein the committee is a verification committee, and if the block parts of the interaction data or the other interaction data cannot be validated by the other nodes in the committee, the method further comprises:

contacting, by the first node, a source committee with nodes to validate the block parts.

9. The method of claim 8, wherein the source committee verifies the block parts and transmits a verification message to the verification committee.

10. The method of claim 8 further comprising:

determining, by the first node, the source committee based on the block parts.

11. The method of claim 7 further comprising:

receiving, by the first node, a plurality of blocks from the other nodes in the committee; and

merging, by the first node, the plurality of blocks with the block.

12. The method of claim 7 further comprising:

generating, by the first node, a list of all block parts to be verified.

13. The method of claim 7, wherein the committee includes more than 5 nodes.

14. A method comprising:

determining, by a first node in a computer network, a leader committee comprising a plurality of elected nodes including the first node, the leader committee being a first committee;

receiving, by the first node, a request from a second node to join a committee of the computer network, the request including a node identifier;

determining, by the first node, that the second node can join a second committee based on a proof of work process computed by the second node;

introducing, by the first node to the second committee, the second node, wherein the second committee displaces a node to allow the second node to join the second committee, wherein information regarding the second node being in the second committee is communicated to other nodes in the computer network;

receiving, by the first node, an interaction request, the interaction request including interaction data from a client computer;

incorporating, by the first node, the interaction data along with other interaction data associated with other client computers into a block comprising interaction data, wherein the block includes block parts;

broadcasting, by the first node, the block to other nodes in the committee, wherein the other nodes in the committee verify the block; and

incorporating the block into a shard of a blockchain managed by the first committee.

15. A node comprising:

a processor;

a memory device; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for performing the method according to any of the preceding claims.