

CLAIMS

WE CLAIM:

1. A system for providing a distributed platform for enabling the private and secure exchange of data and for ensuring the authenticity of such data, the system comprising:
 - a plurality of nodes communicatively coupled to each other via a network, each node in the plurality of nodes having logic for receiving messages exchanged in a common subspace;
 - a subset of nodes within the plurality of nodes, the subset of nodes corresponding to a domain and having permission to access messages exchanged within a private subspace within the domain;
 - a set of validating nodes within the subset of nodes, each validating node having logic for generating a state root based on messages exchanged within the private subspace; and
 - the nodes within the subset of nodes having further logic for generating a global state root value based on the state root.
2. The system of claim 1 wherein the state root is a hash value that is the result of a hash function performed on data in the private subspace, and wherein the global state root is a hash value that is the result of a hash function performed on a set of data comprising the state root.
3. The system of claim 1 wherein each node in the set of validating nodes has logic for validating messages exchanged within the private subspace based on a consensus voting process involving other nodes in the set of validating nodes.
4. The system of claim 1 wherein permission information for each node is maintained in the common subspaces, and wherein changes to permission information are managed through the plurality of nodes exchanging and validating messages in the common subspace.
5. The system of claim 4 wherein each node in the plurality of nodes has logic for forwarding received messages to other nodes permissioned to receive such messages based on the permission information.

6. The system of claim 1 wherein each node in plurality of nodes is communicatively coupled to a database, and each node in the plurality of nodes stores within the database messages and blocks that have been validated.
7. The system of claim 6 wherein each node further comprises logic for deleting messages and blocks according to one or more sets of criteria, wherein deleting messages preserves the subspace hash value and global hash value.
8. A network node in a distributed platform for enabling the private and secure exchange of data and for ensuring the authenticity of such data, the system comprising:
 - logic for receiving messages exchanged in common subspace, where all nodes in the network have permission to access messages in the common subspace, and for receiving messages exchanged in a private subspace for which the node is permissioned;
 - logic for generating a subspace hash value based on messages exchanged within the private subspace; and
 - logic for generating a global hash value based on the subspace hash value.
9. The network node of claim 8 further comprising logic for validating messages exchanged within the private subspace based on a consensus voting process involving other nodes in the distributed platform.
10. The network node of claim 8 wherein permission information for each node in the distributed platform is maintained in the common subspaces, and wherein changes to permission information are managed through the network node exchanging and validating messages in the common subspace.
11. The network node of claim 10 further comprising logic for forwarding received messages to other nodes permissioned to received such messages based on the permission information.
12. The network node of claim 8 wherein the network node is communicatively coupled to a database, and wherein the network node stores within the database messages and blocks that

have been validated.

13. The network node of claim 12 further comprising logic for deleting messages and blocks according to one or more sets of criteria, wherein deleting messages preserves the subspace hash value and global hash value.

14. A distributed data structure, implemented in a computer memory, for securely exchanging private data among a plurality of nodes in a distributed network and ensuring the authenticity of such data, the data structure comprising:

one or more private subspaces having contents accessible only by nodes in the plurality of nodes that have sufficient access credentials, each subspace comprising a state root;

a common subspace, accessible to all nodes in the plurality of nodes, the common subspace identifying validating nodes for each private subspace; and

a header comprising: a global state root based on the state root of the one or more subspaces.

15. The distributed data structure of claim 14 wherein the state root of each private subspace is a hash value that is the result of a hash function performed on data in that private subspace.

16. The distributed data structure of claim 14 wherein the global state root is a hash value that is the result of a hash function performed on a set of data comprising the state roots of the one or more private subspaces.

17. The distributed data structure of claim 14 wherein the common subspace includes a script for managing permissions of each node in the plurality of nodes.

18. The distributed data structure of claim 14 wherein each private subspace contains policies for deleting blocks and messages within the private subspace through a deletion process that preserves the hash value of the subspace.

19. The distributed data structure of claim 14 wherein the header further comprises one or

more cryptographic signatures which are used to validate the distributed data structure.

20. The distributed data structure of claim 14 wherein the header further comprises a message root whose value is a function of all messages contained within the distributed data structure.