CLAIMS

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 first subset of nodes within the plurality of nodes, the first subset of nodes corresponding to a first domain and having permission to access messages exchanged within a first private subspace within the first domain;

a second subset of nodes within the plurality of nodes, the second subset of nodes corresponding to a second domain and having permission to access messages exchanged within a second private subspace within the second domain;

a first set of validating nodes within the first subset of nodes, each validating node in the first set having logic for generating a first state root based on messages exchanged within the first private subspace;

a second set of validating nodes within the second subset of nodes, each validating node in the second set having logic for generating a second state root based on messages exchanged within the second private subspace, wherein:

the first set of validating nodes do not have permission to access messages exchanged within the second private subspace within the second domain, and

the second set of validating nodes do not have permission to access messages exchanged within the first private subspace within the first domain; and

the validating nodes within the plurality of nodes having further logic for generating a global state root value based on the state roots of the subspaces, the global state root value being based on both the first state root and the second state root.

2. The system of claim 1 wherein the first state root is a first hash value that is the result of a hash function performed on data in the first private subspace, the second state root is a second hash value that is the result of the hash function performed on data in the second 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 first state root and the second state root.

3. The system of claim 1 wherein each node in the first set of validating nodes has logic for validating messages exchanged within the first private subspace based on a consensus voting process involving other nodes in the first 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 a subspace hash value and global hash value.

8. A method of using 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 method comprising:

receiving, by the network node, messages exchanged in common subspace, where the network node and other nodes in a plurality of nodes ~~all nodes~~ in ~~the~~ a network have permission to access messages in the common subspace, ~~and for~~

receiving, by the network node, messages exchanged in a first private subspace for which the node is permissioned, wherein:

the network node is in a first subset of nodes within the plurality of nodes in the network, and the first subset of nodes are permissioned to access messages exchanged within the first private subspace;

a second subset of nodes within the plurality of nodes in the network are permissioned to access messages exchanged within a second private subspace; and

~~for which at least one other node~~ the second subset of nodes in the network ~~does not have permission~~ are not permissioned to access messages exchanged within the first private subspace;

generating, by the network node, a first subspace hash value based on messages exchanged within the first private subspace, wherein another node in the second subset of nodes generates a second subspace hash value based on messages exchanged within the second private subspace; and

generating, by the network node, a global hash value based on the first subspace hash value and other subspace hash values corresponding to other subspaces, the other subspace hash values comprising at least the second subspace hash value corresponding to the second subspace.

9. The method of claim 8 further comprising validating, by the network node, messages exchanged within the first private subspace based on a consensus voting process involving other nodes in the first subset of nodes of the distributed platform having permission to access messages in the first private subspace.

10. The method of claim 8 wherein permission information for each node in the distributed platform is maintained in the common ~~subspaces~~ subspace, and wherein changes to permission information are managed through the ~~network~~ node exchanging and validating messages in the common subspace.

11. The method of claim 10 further comprising forwarding, by the network node, received messages to other nodes permissioned to receive such messages based on the permission information.

12. The method 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 method of claim 12 further comprising deleting messages and blocks according to one or more sets of criteria, wherein deleting messages preserves the first 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:

a plurality of private subspaces, ~~each~~ comprising at least a first private subspace and a second private subspace,

the first subspace having:

first contents accessible only by a first subset of nodes in the plurality of nodes that have sufficient access credentials, the first contents inaccessible by other nodes in the plurality of nodes that are not in the first subset, and

a first state root generated by a validating node in the first subset of nodes based on content within the first private subspace, and

the second subspace having:

contents accessible only by a second subset of nodes in the plurality of nodes that have sufficient access credentials, the contents inaccessible by other nodes in the plurality of nodes that are not in the second subset, and

a second state root generated by a validating node in the second subset of nodes based on content within the second private subspace;

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

a header comprising a global state root generated based on the state roots of the plurality of private 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 plurality of 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~~ 15 wherein each private subspace contains polices for deleting blocks and messages within the private subspace through a deletion process that preserves the hash value of the private subspace.

19. The distributed data structure of claim 14 wherein the header further comprises one or more cryptographic signatures by which the distributed data structure is validated.

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.