

Claims

1. A computer system, comprising:

a network of externally owned presence (EOP) member nodes;

i) wherein each EOP member node is owned by a distinct entity;

ii) wherein the network of externally owned presence (EOP) nodes comprises:

1) at least one supervisory EOP member node and

2) a plurality of peer EOP member nodes;

iii) wherein the at least one supervisory EOP member node is configured to generate at least one personalized cryptographic private key for each peer EOP member node;

iv) wherein each personalized cryptographic private key is only known to a corresponding peer EOP member node which controls a secrecy of such personalized cryptographic private key;

at least one distributed database, storing a plurality of persistent data objects; and

a plurality of self-contained self-executing software containers (SESCs);

i) wherein each SESC comprises an independently executable software code which is at least configured to:

1) generate at least one state hash representative at least one current state of at least one persistent data object,

2) perform at least one data action with the at least one persistent data object; and

3) determine that a particular EOP member node has a permission to cause the SESC to perform the at least one data action with the at least one persistent data object based, at least in part on a particular personalized cryptographic private key of the particular EOP member node and at least one attribute associated with the particular EOP member node; and

4) determine that the at least one data action with the at least one persistent data object has been based, at least in part, on at least one explicit policy criteria check to which all EOP member nodes have agreed to follow.

2. The computer system of claim 1, wherein the plurality of SESC comprises:

a plurality of meeting SESC, wherein each meeting SESC is at least configured to:

obtain current data related to a particular corporate event of a publicly traded company from at least one electronic source associate with at least one EOP member node;

perform the at least one explicit policy criteria check associated with at least one of the at least one electronic source, the at least one EOP member node, and the current data;

generate at least one meeting state hash representative the current data of the particular corporate event;

store the at least one meeting state hash and the current data of the particular corporate event in at least one meeting persistent data object in the at least one distributed database;

keep the at least one meeting state hash within the meeting SESC;

and generate an output representative of a current state of the particular corporate event.

3. The computer system of claim 2, wherein the particular corporate event is an annual meeting.

4. The computer system of claim 3, wherein the current data related to the annual meeting comprises agenda data, ballot data, entitlement data, and voting data.

5. The computer system of claim 3, wherein the at least one explicit policy criteria check is at least one of:

- i) verifying that a particular investor can access only a vote entitlement related to the particular investor;
- ii) verifying that a particular custodian can access only the vote entitlement when the particular investor is a client of the particular custodian; and
- iii) verifying that a particular issuer can access only vote details without accessing related investor data.

6. The computer system of claim 2, wherein each meeting SESC is further configured to generate the at least one meeting state hash based on at least one of the following cryptographic hash functions: SHA-256, Dagger-Hashimoto Hashes, and SHA3.

7. The computer system of claim 1, wherein the plurality of SESCOs comprises:

a plurality of re-purchase contract SESCOs, wherein each re-purchase contract SESCO is at least configured to:

obtain current re-purchase contract data for a particular re-purchase contract from at least one electronic source associate with at least one EOP member node;

perform the at least one explicit policy criteria check associated with at least one of the at least one electronic source, the at least one EOP member node, and the current re-purchase contract data;

obtain electronic signatures from all parties to the particular re-purchase contract;

generate at least one re-purchase contract state hash representative the current re-purchase contract data;

store the at least one re-purchase contract state hash and the current re-purchase contract data of the particular re-purchase contract in at least one re-purchase contract persistent data object in the at least one distributed database;

keep the at least one re-purchase contract state hash within the re-purchase contract SESCO;

substitute at least one first collateral being used in the particular re-purchase contract for another collateral;

and generate an output representative of an updated current state of the particular re-purchase contract.

8. A computer-implemented method, comprising:

programming a network of externally owned presence (EOP) member nodes;

i) wherein each EOP member node is owned by a distinct entity;

ii) wherein the network of externally owned presence (EOP) nodes comprises: 1) at least one supervisory EOP member node and 2) a plurality of peer EOP member nodes;

iii) wherein the at least one supervisory EOP member node is configured to generate at least one personalized cryptographic private key for each peer EOP member node;

iv) wherein each personalized cryptographic private key is only known to a corresponding peer EOP member node which controls a secrecy of such personalized cryptographic private key;
programming at least one distributed database, storing a plurality of persistent data objects;

and programming a plurality of self-contained self-executing software containers (SESCs);

i) wherein each SESC comprises an independently executable software code which is at least configured to:

- 1) generate at least one state hash representative at least one current state of at least one persistent data object,
- 2) perform at least one data action with the at least one persistent data object; and
- 3) determine that a particular EOP member node has a permission to cause the SESC to perform the at least one data action with the at least one persistent data object based, at least in part on a particular personalized cryptographic private key of the particular EOP member node and at least one attribute associated with the particular EOP member node; and
- 4) determine that the at least one data action with the at least one persistent data object has been based, at least in part, on at least one explicit policy criteria check to which all EOP member nodes have agreed to follow.

9. The computer-implemented method of claim 8, wherein the plurality of SESC comprises:
a plurality of meeting SESC, wherein each meeting SESC is at least configured to:
obtain current data related to a particular corporate event of a publicly traded company from at least one electronic source associate with at least one EOP member node;
perform the at least one explicit policy criteria check associated with at least one of the at least one electronic source, the at least one EOP member node, and the current data; generate at least one meeting state hash representative the current data of the particular corporate event;
store the at least one meeting state hash and the current data of the particular corporate event in at least one meeting persistent data object in the at least one distributed database;
keep the at least one meeting state hash within the meeting SESC;
and generate an output representative of a current state of the particular corporate event.

10. The computer-implemented method of claim 9, wherein the particular corporate event is an annual meeting.

11. The computer-implemented method of claim 10, wherein the current data related to the annual meeting comprises agenda data, ballot data, entitlement data, and voting data.

12. The computer-implemented method of claim 10, wherein the at least one explicit policy criteria check is at least one of:

- i) verifying that a particular investor can access only a vote entitlement related to the particular investor;
- ii) verifying that a particular custodian can access only the vote entitlement when the particular investor is a client of the particular custodian; and
- iii) verifying that a particular issuer can access only vote details without accessing related investor data.

13. The computer-implemented method of claim 9, wherein each meeting SESC is further configured to generate the at least one meeting state hash based on at least one of the following cryptographic hash functions: SHA-256, Dagger-Hashimoto Hashes, and SHA3.

14. The computer-implemented method of claim 8, wherein the plurality of SESCOs comprises:
a plurality of re-purchase contract SESCOs, wherein each re-purchase contract SESCO is at least configured to:

obtain current re-purchase contract data for a particular re-purchase contract from at least one electronic source associate with at least one EOP member node;

perform the at least one explicit policy criteria check associated with at least one of the at least one electronic source, the at least one EOP member node, and the current re-purchase contract data;

obtain electronic signatures from all parties to the particular re-purchase contract;

generate at least one re-purchase contract state hash representative the current re-purchase contract data;

store the at least one re-purchase contract state hash and the current re-purchase contract data of the particular re-purchase contract in at least one re-purchase contract persistent data object in the at least one distributed database;

keep the at least one re-purchase contract state hash within the re-purchase contract SESCO;

substitute at least one first collateral being used in the particular re-purchase contract for another collateral;

and generate an output representative of an updated current state of the particular re-purchase contract.