

CLAIMS

1. An access management process orchestration method, comprising:

receiving, by an access management governance orchestrator blockchain network, a request for accessing a first managed resource of a first information system, wherein the first managed resource is one of a plurality of managed resources locally managed by one of a plurality of information systems and wherein each of the plurality of information systems includes a local access control system that manages a local authorization policy for a respective plurality of local resources, wherein the local access control system is not part of the blockchain network;

querying, by the access management governance orchestrator blockchain network, an authorization for accessing the first managed resource from an access manager;

in response to the querying of the authorization, requesting, by the access management governance orchestrator blockchain network, an access control policy update to grant access to the first managed resource from an owner of the first information system;

receiving an approval of the request for the access control policy update from the owner of the first information system; and

in response to the approval of the request for the access control policy update, calling, by the access management governance orchestrator blockchain network, a respective one of the local access control systems to request a change to its respective local authorization policy with respect to the first managed resource;

wherein receiving the request for accessing the first managed resource, querying the authorization, receiving the approval, and requesting the access control policy update each comprises:

- generating a transaction record; and
- adding the transaction record to a distributed ledger, wherein the distributed ledger simultaneously maintains the transaction record at multiple nodes throughout the blockchain network, wherein requesting the access control policy update comprises executing a smart contract that processes transactions in the distributed ledger.

2. The method of claim 1, wherein the method further comprises exchanging the transaction record between the multiple nodes of the distributed ledger.

3. The method of any one of the preceding claims, wherein the multiple nodes are interconnected via cryptographically secured channels.
4. The method of any one of the preceding claims, wherein the transaction record comprises at least one administrative action selected from the group consisting of a request access action, an access approved action, an access denied action, an access granted action, a revoke access action, and an access revoked action.
5. The method of claim 4, wherein the administrative action associated with the access granted action changes an authorization policy to allow access of a user to the first information system.
6. The method of any one of claims 4 to 5, wherein the administrative action associated with the revoke access action changes an authorization policy to deny access of a user to the first information system.
7. The method of any one of claims 4 to 6, further comprising:
 - transmitting the transaction record to the first information system; and
 - automatically executing the administrative action on the first information system.
8. An access management governance orchestrator, comprising:
 - a peer node associated with a blockchain network, the blockchain network comprising a plurality of nodes associated with at least one of an asset owner function, an administrator function, and an auditor function, the peer node adapted to:
 - receive a request for accessing to a first managed resource of a first information system, wherein the first managed resource of the first information system is one of a plurality of managed resources locally managed by one of a plurality of information systems and wherein each of the plurality of information systems includes a local access control system that manages a local authorization policy for a respective plurality of local resources, wherein the local access control system is not part of the blockchain network;
 - record a request access record in a distributed ledger;

record an owner approval record from the asset owner function in the distributed ledger, the owner approval record responsive to the request access record;

execute a smart contract responsive to the request access record and the owner approval record granting access on the first information system, wherein the smart contract requests a change in the local authorization policy of the first information system to allow access of a user to the first information system outside of the blockchain network, wherein changing the authorization policy comprises calling the local access control system associated with the first information system to request the change to the local authorization policy; and

record an execution record of the smart contract in the distributed ledger.

9. The access management governance orchestrator of claim 8, wherein the peer node is further adapted to:

storing one or more of the request access record, the owner approval record, and the execution record in a transaction block;

selecting one of the plurality nodes as a signature node to sign the transaction block according to a consensus protocol; and

signing, by the selected signature node, the transaction block.

10. The access management governance orchestrator of any one of claims 8 to 9, wherein the peer node is further adapted to:

receive a new peer request to add a new node to the blockchain network; and

transmitting the new peer request to the plurality of nodes in the blockchain network for approval according to a consensus protocol.

11. The access management governance orchestrator of any one of claims 8 to 10, wherein the peer node is further adapted to review the distributed ledger for execution records that are not associated with owner approval records.

12. A computer program product comprising a non-transitory computer readable storage medium having a plurality of instructions stored thereon, which, when executed by a processor, cause the processor to:

receive, by an access management governance orchestrator blockchain network, a request for accessing a first managed resource of a first information system, wherein the first managed resource of the information system is one of a plurality of managed re-sources of a plurality of information systems and wherein each of the plurality of information systems includes a local access control system that manages a local authorization policy for a respective plurality of local resources, wherein the local access control system is not part of the blockchain network;

query, by the access management governance orchestrator blockchain network, an authorization for accessing the first managed resource from an access manager;

in response to the querying the authorization, request, by the access management governance orchestrator blockchain network, a change to the local access control policy of a respective one of the plurality of information systems to grant access to the first managed resource from an owner of the first information system;

receive an approval of the request for the access control policy update from the owner of the information system; and

in response to the approval of the request for the access control policy update, call, by the access management governance orchestrator blockchain network, a respective one of the local access control systems to request a change to its respective local authorization policy with respect to the first managed resource;

wherein receiving the request for accessing the first managed resource, querying the authorization, receiving the approval, and requesting the access control policy update each comprises:

generating a transaction record; and

adding the transaction record to a distributed ledger, wherein the distributed ledger simultaneously maintains the transaction record at multiple nodes throughout the blockchain network, wherein requesting the access control policy update

comprises executing a smart contract that processes transactions in the distributed ledger.

13. The computer program product of claim 12, wherein the transaction record includes at least one administrative action chosen from the group consisting of a request access record, an access approved record, an access denied record, an access granted record, a revoke access record, and an access revoked record.