CLAIMS

1. A system that implements an interbank information network architecture that provides a secure and decentralized network, the system comprising:

a first bank node of a distributed ledger network, wherein the first bank node is communicatively coupled to a first in-bank system, the first bank node comprising:

a client internal system that communicates with application business logic via an application programing interface (API); and

a blockchain node that supports a permissioned shared ledger and a private database that contains transactional, customer and personally identifiable information (PIT);

a second bank node of the distributed ledger network, wherein the second bank node is communicatively coupled to a second in-bank system; and

an interbank information network that is layered on top of the distributed ledger network and supports a plurality of hosting models that include an on-premise hosting model, a third-party hosting model, a public cloud hosting model, and a private cloud hosting model, wherein the interbank information network establishes a direct communication channel between the first node and the second node, wherein the interbank information network encrypts each communication sent between the first node and the second node,

wherein the first bank node (310) is configured to:

secure a connection to the distributed ledger network via an application programming interface (API), wherein the secure connection to the distributed ledger network applies a two-way Secure Sockets Layer (SSL) for a web-interface and the API;

receive inquiry activity;

check, through a blockchain node for the first bank node, permissions;

validate, through the blockchain node for the first bank node, permissions against a known fraudster list that is shared across the interbank information network in real-time;

obtain consensus on the distributed ledger network associated with the interbank information network;

record and publish, through the blockchain node for the first bank node, a hash that represents the inquiry activity, onto a public ledger for the distributed ledger network associated with the interbank information network;

send one or more private inquiry details comprising an inquiry message directly to the second bank node over the distributed ledger network;

receive a response to the inquiry message over the distributed ledger network, wherein the second bank node receives the request message, processes one or more transaction details and generates a response;

separately receiving at least one decryption key for information that is stored in an encrypted format; and

process a payment responsive to the response to the inquiry message,

wherein the inquiry message comprises a message that requests the second bank node to share client data and the client data comprises an account open date and name matching conditions.

2. The system of claim 1, wherein the message relates to one of: fraud, validation, sanctions, tracking, clearing, settlement and advising.

3. The system of claim 1, further comprising an administrator node that maintains a list of nodes that are authorized to participate in the interbank information network.

4. The system of claim 1, wherein each bank node in the interbank information network is responsible for in-bank user access to node functions.

5. The system of claim 1, wherein the message is encrypted.

6. The system of claim 1, wherein the message comprises a request to validate an account associated with the second bank node.

7. The system of claim 1, wherein the first in-bank system comprises a payment information application, a client information application, a sanctions application and the known fraudster list.

8. The system of claim 1, wherein a user associated with the first bank node access the API via a web-based interface from a client device.

9. A method that implements an interbank information network architecture that provides a secure and decentralized network, the method comprising:

provisioning a first bank node of a distributed ledger network, wherein the first bank node is communicatively coupled to a first in-bank system, the first bank node comprising:

a client internal system that communicates with application business logic via an application programing interface (API); and

a blockchain node that supports a permissioned shared ledger and a private database that contains transactional, customer and personally identifiable information (PIT);

provisioning a second bank node of the distributed ledger network, wherein the second bank node is communicatively coupled to a second in-bank system; and

layering an interbank information network on top of the distributed ledger network, wherein the interbank information network establishes a direct communication channel between the first node and the second node, wherein the interbank information network encrypts each communication sent between the first node and the second node,

wherein the first bank node (310) is configured to:

secure a connection to the distributed ledger network via an application programming interface (API), wherein the secure connection to the distributed ledger network applies a two-way Secure Sockets Layer (SSL) for a web-interface and the API;

receive inquiry activity;

check, through a blockchain node for the first bank node, permissions;

validate, through the blockchain node for the first bank node, permissions against a known fraudster list that is shared across the interbank information network in real-time;

obtain consensus on the distributed ledger network associated with the interbank information network;

record and publish, through the blockchain node for the first bank node, a hash that represents the inquiry activity, onto a public ledger for the distributed ledger network associated with the interbank information network;

send one or more private inquiry details comprising an inquiry message directly to the second bank node over the distributed ledger network;

receive a response to the inquiry message over the distributed ledger network, wherein the second bank node receives the request message, processes one or more transaction details and generates a response;

separately receiving at least one decryption key for information that is stored in an encrypted format; and

process a payment responsive to the response to the inquiry message,

wherein the inquiry message comprises a message that requests the second bank node to share client data and the client data comprises an account open date and name matching conditions.

10. The method of claim 9, wherein the message relates to one of: fraud, validation, sanctions, tracking, clearing, settlement and advising.

11. The method of claim 9, further comprising an administrator node that maintains a list of nodes that are authorized to participate in the interbank information network.

12. The method of claim 9, wherein each bank node in the interbank information network is responsible for in-bank user access to node functions.

13. The method of claim 9, wherein the message is encrypted.

14. The method of claim 9, wherein the message comprises a request to validate an account associated with the second bank node.

15. The method of claim 9, wherein the first in-bank system comprises a payment information application, a client information application, a sanctions application and the known fraudster list.

16. The method of claim 9, wherein a user associated with the first bank node access the API via a web-based interface from a client device.