

CLAIMS

What is claimed is:

1. A computer-implemented method for generating an encrypted digital identity record in a blockchain, the method comprising:

receiving, by a network node of a plurality of network nodes hosting a blockchain, a request to generate a digital identity record within the blockchain for an entity, wherein the request contains an entity type of the entity, and wherein the blockchain is a private party blockchain;

retrieving, by the network node, a digital identity record template associated with the entity type from a blockchain, wherein the digital identity record template comprises multiple data fields including mandatory and supplemental data fields;

receiving, by the network node, information for at least the mandatory data fields and a reference document from a client device associated with the entity;

generating, by the network node, a digital identity record for the entity by associating the received information to one or more data fields in the digital identity record template;

assigning, by the network, a status identifier to the one or more data fields based on the corresponding associated information;

associating, by the network node, a first data field of the one or more data fields with the reference document;

generating, by the network node, a one directional cryptographic hash of the reference document;

storing, by the network node, the reference document in a non-blockchain document repository;

storing, by the network node, the one directional cryptographic hash of the reference document in the digital identity record in association with the first data field;

setting, by the network node, permission controls for the digital identity record based on the entity type and the received information;

encrypting, by the network node, the digital identity record using one or more encryption keys retrieved from a non-blockchain key database;

generating, by the network node, a digital identity record block containing the encrypted digital identity record;

appending, by the network node, the digital identity record block to the blockchain;
receiving, by the network node, a request for a document from the client device associated with the entity;
retrieving, by the network node, a block address of the digital identity record block from the non-blockchain document repository;
accessing, by the network node, the digital identity block to retrieve a permissions executable coded script containing the permission controls of the entity;
executing, by the network node, the permissions executable coded script to determine if the request for the document is valid; and
in response to the network node determining that the request for the document is valid:
retrieving, by the network node, the document from the non-blockchain document repository; and
transmitting, by the network node, the retrieved document to the client device.

2. The method of claim 1, further comprising:

receiving, by the network node via a biometric web application, biometric information associated with the entity;
storing, by the network node, the received biometric information to a non-blockchain biometric repository;
generating, by the network node, a one directional cryptographic hash of the received biometric information; and
storing, by the network node, the one directional cryptographic hash of the received biometric information in the digital identity record.

3. The method of claim 1, wherein the multiple data fields comprise at least one of: entity name, registered address, jurisdiction, identity document hash, identity biometric hash, permission controls, relationship, and hierarchy.

4. The method of claim 1, wherein the status identifier comprises at least one of verified and unverified;

further comprising:

updating, by the network node, the status identifier from unverified to verified.

5. The method of claim 1, wherein encrypting the digital identity record comprises:
encrypting, by the network node, a first set of data fields using a first encryption key; and
encrypting, by the network node, a second set of data fields using a second encryption key.
6. The method of claim 1, further comprising:
associating, by the network node, a globally unique random digital identity reference with the entity; and
storing, by the network node, the globally unique random digital identity reference in the digital identity record.
7. The method of claim 1, further comprising:
associating, by the network node, the digital identity record with a smart contract in the blockchain.
8. The method of claim 1, wherein the permission controls delimit the entity's access to information within the blockchain and rights to initiate blockchain based events.
9. The method claim 1, further comprising:
generating, by the network node, a second digital identity record hierarchically below the digital identity record.
10. A system for generating an encrypted digital identity record in a blockchain, the system comprising:
a plurality of distributed network nodes, each including a non-transitory storage medium storing a respective local copy of the blockchain, wherein the blockchain is a private party blockchain;
at least one of the plurality of distributed network nodes having a processor configured to:
receive a request to generate a digital identity record within the blockchain for an entity, wherein the request contains an entity type of the entity;

retrieve a digital identity record template associated with the entity type from the blockchain, wherein the digital identity record template comprises multiple data fields including mandatory and supplemental data fields;

receive information for at least the mandatory data fields and a reference document from a client device associated with the entity;

generate a digital identity record for the entity by associating the received information to one or more data fields in the digital identity record template;

assign a status identifier to the one or more data fields based on the corresponding associated information;

associate a first data field of the one or more data fields with the reference document;

generate a one directional cryptographic hash of the reference document;

store the reference document in a non-blockchain document repository;

store the one directional cryptographic hash of the reference document in the digital identity record in association with the first data field;

set permission controls for the digital identity record based on the entity type and the received information;

encrypt the digital identity record using one or more encryption keys retrieved from a non-blockchain key database;

generate a digital identity record block containing the encrypted digital identity record;

append the digital identity record block to the blockchain;

receive a request for a document from the client device associated with the entity;

retrieve a block address of the digital identity record block from the non-blockchain document repository;

access the digital identify block to retrieve a permissions executable coded script containing the permission controls of the entity;

execute the permissions executable coded script to determine if the request for the document is valid; and

in response to the processor determining that the request for the document is valid:

retrieve the document from the non-blockchain document repository; and

transmit the retrieved document to the client device.

11. The system of claim 10, wherein the processor is further configured to:
receive, via a biometric web application, biometric information associated with the entity;
store the received biometric information to a non-blockchain biometric repository;
generate a one directional cryptographic hash of the received biometric information; and
store the one directional cryptographic hash of the received biometric information to the digital identity record.
12. The system of claim 10, wherein the multiple data fields comprise at least one of: entity name, registered address, jurisdiction, identity document hash, identity biometric hash, permission controls, relationship, and hierarchy.
13. The system of claim 10, wherein the status identifier comprises at least one of verified or unverified;

wherein the processor is further configured to:
update the status identifier from unverified to verified.
14. The system of claim 10, wherein the processor is further configured to encrypt the digital identity record by:
encrypt a first set of data fields using a first encryption key; and
encrypt a second set of data fields using a second encryption key.
15. The system of claim 10, wherein the processor is further configured to:
associate a globally unique random digital identity reference with the entity; and
store the globally unique random digital identity reference in the digital identity record.
16. The system of claim 10, wherein the processor is further configured to:
associate the digital identity record with a smart contract in the blockchain.
17. The system of claim 10, wherein the permission controls delimit the entity's access to information within the blockchain and rights to initiate blockchain based events.
18. The system claim 10, wherein the processor is further configured to:
generate a second digital identity record hierarchically below the digital identity record.