

WHAT IS CLAIMED IS:

1 1. A blockchain system comprising:
2 an issuer network node configured to:
3 receive a request to issue a credential for a communication device,
4 the request including a communication device public key;
5 determine the credential to issue to the communication device;
6 provision the credential to the communication device;
7 generate a payload derived from hashing the credential and the
8 communication device public key;
9 store the payload in a record of a blockchain; and
10 synchronize the record to other network nodes on the blockchain;
11 and
12 a verification network node configured to:
13 receive the credential, the communication device public key, and a
14 communication device signature generated by the communication device to
15 request access to a resource, wherein the communication device signature is
16 generated by encrypting a numeric value using a communication device private
17 key corresponding to the communication device public key, wherein the numeric
18 value is a block identifier identifying which block in the blockchain contains the
19 record;
20 verify the communication device signature using the communication
21 device public key;
22 in response to verifying the communication device signature,
23 generate a hash value based on the credential and the communication device
24 public key;
25 determine that the hash value is stored in the blockchain; and
26 in response to determining that the hash value is stored in the
27 blockchain, authenticate the communication device for access to the requested
28 resource.

1 2. The blockchain system of claim 1, wherein the record includes a
2 record signature that is generated with a signature key.

1 3. The blockchain system of claim 2, wherein the signature key is an
2 issuer key associated with the issuer network node, or a certificate authority key
3 associate with a certificate authority.

1 4. The blockchain system of claim 2, wherein the verification network
2 node is further configured to verify the record signature of the record to authenticate the
3 communication device.

1 5. The blockchain system of claim 1, wherein the payload is further
2 derived from a hash of a previous block of one or more records in the blockchain.

1 6. The blockchain system of claim 5, wherein the issuer network node
2 is further configured to provide to the communication device the block identifier
3 identifying which block in the blockchain contains the record.

1 7. The blockchain system of claim 1, wherein the block identifier is a
2 hash of a previous block of the block in the blockchain containing the record.

1 8. A computer-implemented method comprising:
2 receiving, by a credential issuer computer, a request to issue a credential
3 for a communication device, the request including a communication device public key
4 associated with the communication device;
5 determining, by the credential issuer computer, the credential to issue to
6 the communication device;
7 provisioning, by the credential issuer computer, the credential to the
8 communication device, wherein provisioning the credential to the communication device
9 includes providing to the communication device a block identifier identifying a block in a
10 blockchain;
11 generating, by the credential issuer computer, a payload derived from
12 hashing the credential and the communication device public key;

13 storing, by the credential issuer computer, the payload in a record in the
14 block of the blockchain; and
15 synchronizing, by the credential issuer computer, the record to other
16 network nodes on the blockchain.

1 9. The computer-implemented method of claim 8, wherein the record
2 includes a signature generated with a signature key.

1 10. The computer-implemented method of claim 9, wherein the
2 signature key is an issuer key associated with the credential issuer computer.

1 11. The computer-implemented method of claim 9, wherein the
2 signature key is a certificate authority key associated with a certificate authority.

1 12. The computer-implemented method of claim 8, wherein the record
2 includes a first signature generated with an issuer key associated with the credential
3 issuer computer; and a second signature generated with a certificate authority key
4 associated with a certificate authority.

1 13. The computer-implemented method of claim 8, wherein the payload
2 is further derived from a hash of a previous block of the blockchain.

1 14. The computer-implemented method of claim 8, wherein the
2 credential is an account identifier, or a token that is a substitute for the account
3 identifier.

1 15. A computer-implemented method comprising:
2 receiving, by a network node associated with a blockchain, a credential, a
3 communication device public key associated with a communication device, and a
4 communication device signature to request access to a resource, wherein the
5 communication device signature is generated by encrypting a numeric value using a
6 communication device private key corresponding to the communication device public
7 key, wherein the numeric value is a block identifier identifying which block in the
8 blockchain contains a record;

9 verifying, by the network node, the communication device signature using
10 the communication device public key;
11 in response to verifying the communication device signature, generating,
12 by the network node, a hash value based on the credential and the communication
13 device public key;
14 determining, by the network node, that the hash value is stored in the
15 record of the blockchain;
16 verifying, by the network node, a record signature associated with the
17 record of the blockchain; and
18 in response to determining that the hash value is stored in the blockchain
19 and verifying the record signature of the record, authenticating the communication
20 device for access to the requested resource.