

What is claimed is:

1. A computer-implemented method of managing public key infrastructure using a blockchain network, comprising:
 - at a certification authority, generating a digital certificate for a first entity, the first entity having a first public key, by:
 - creating a certification transaction, wherein the certification transaction includes a digital signature from a certificate authority, a first output to an address based on a second public key, and a second output having an information field that contains the first public key;
 - determining a certification transaction identifier from a hash of the certification transaction; and
 - propagating the certification transaction on the blockchain network, wherein the digital certificate includes the first public key and the certification transaction identifier; and
 - at a computing device, verifying the digital certificate by:
 - obtaining a copy of the certification transaction from a blockchain based on the certification transaction identifier in the digital certificate;
 - determining that the first output is an unspent transaction output; and
 - determining that the first public key contained in the second output in the certification transaction matches a public key in the digital certificate.
2. The method of claim 1, wherein the second output includes an OP_RETURN field that contains at least the first public key.
3. The method of claim 1 or claim 2, wherein the first output includes a pay-to-public-key-hash (P2PKH) operation referencing an address obtained as a hash of the second public key.

4. The method of any one of claims 1 to 3, wherein the certificate authority holds a second private key corresponding to the second public key.
5. The method of claim 1, wherein determining that the first output is an unspent transaction output includes determining that the first output is present in an unspent transaction output pool of the blockchain network.
6. The method of any one of claims 1 to 5, wherein an input to the certification transaction further includes a certificate authority public key, and wherein verifying the digital certificate further includes determining that the certification transaction is signed by the certificate authority based on the certificate authority public key.
7. The method of any one of claims 1 to 6, further comprising revoking the digital certificate by generating a revocation transaction that includes, as an input, the first output of the certification transaction, and propagating the revocation transaction on the blockchain network.
8. The method of any one of claims 1 to 6, further comprising replacing the digital certificate with a new digital certificate for a new public key by:
 - creating a new certification transaction, wherein the new certification transaction includes as an input the first output of the certification transaction, a first new output to a new address based on a third public key, and a second new output having the information field, wherein the information field contains the new public key;
 - determining a new certification transaction identifier from hashing the new certification transaction; and
 - propagating the new certification transaction on the blockchain network, wherein the new digital certificate includes the new public key and the new certification transaction identifier.
9. The method claimed in any one of claims 1 to 8, wherein the information field is an

OP_RETURN output.

10. The method claimed in any one of claims 1 to 9, wherein the certification transaction includes an input referencing an unspent transaction outputpoint address obtained from a hash of a certificate authority public key, and wherein the certification transaction includes an unlocking script for the unspent transaction outputpoint address that includes the certificate authority public and the digital signature, and wherein the digital signature is generated based on a private key corresponding to the certificate authority public key.
11. The method claimed in any one of claims 1 to 10, wherein the first output includes a multi-sig locking script enabling any one of two or more private keys to utilize the first output.
12. A computing device to manage a public key infrastructure using a blockchain network, the computing device including:
 - one or more processors;
 - memory;
 - computer-executable instructions stored in the memory that, when executed by the one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 11.
13. A computer-readable medium storing processor-executable instructions for managing a public key infrastructure using a blockchain network, the processor-executable instructions including instructions that, when executed by one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 11.
14. A computer-implemented method of verifying a digital certificate using a blockchain network, the digital certificate including a first public key and a certification transaction identifier, the method comprising:
 - receiving the digital certificate from a first entity;
 - obtaining a copy of the certification transaction from a blockchain based on the certification transaction identifier in the digital certificate, wherein the

certification transaction includes a digital signature from a certificate authority, a first output to an address based on a second public key, and a second output having an information field;
determining that the information field contains a public key that matches the first public key in the digital certificate;
querying an unspent transaction output pool to determine that the first output in the certification transaction has not been used in any subsequent transaction;
and,
based on those determinations, verifying that the first public key is certified valid.

15. A computer-implemented method, comprising:

at a computing device,

receiving a digital certificate for a first entity, the digital certificate including a first public key for the first entity and a certification transaction identifier generated from a hash of a certification transaction, where the certification transaction includes a digital signature from a certificate authority, a first output to an address based on a second public key, and a second output having an information field that contains the first public key;
obtaining a copy of the certification transaction from a blockchain based on the certification transaction identifier in the digital certificate;
determining that the first output is an unspent transaction output; and
determining that the first public key contained in the second output in the certification transaction matches a public key in the digital certificate.

16. The method of claim 15, wherein the second output includes an OP_RETURN field that contains at least the first public key.

17. The method of claim 15 or claim 16, wherein the first output includes a pay-to-public-key-hash (P2PKH) operation referencing an address obtained as a hash of the second public key.

18. The method of any one of claims 15 to 17, wherein the certificate authority holds a second private key corresponding to the second public key.
19. The method of claim 15, wherein determining that the first output is an unspent transaction output includes determining that the first output is present in an unspent transaction output pool of the blockchain network.
20. The method of any one of claims 15 to 19, wherein an input to the certification transaction further includes a certificate authority public key, and wherein verifying the digital certificate further includes determining that the certification transaction is signed by the certificate authority based on the certificate authority public key.
21. The method claimed in any one of claims 15 to 20, wherein the information field is an OP_RETURN output.
22. The method claimed in any one of claims 15 to 21, wherein the certification transaction includes an input referencing an unspent transaction outpoint address obtained from a hash of a certificate authority public key, and wherein the certification transaction includes an unlocking script for the unspent transaction outpoint address that includes the certificate authority public and the digital signature, and wherein the digital signature is generated based on a private key corresponding to the certificate authority public key.
23. The method claimed in any one of claims 15 to 22, wherein the first output includes a multi-sig locking script enabling any one of two or more private keys to utilize the first output.
24. A computing device, the computing device including:
 - one or more processors;
 - memory;
 - computer-executable instructions stored in the memory that, when executed by the one or more processors, cause the processors to carry out the method claimed in any one of claims 15 to 23.

25. A computer-readable medium storing processor-executable instructions, the processor-executable instructions including instructions that, when executed by one or more processors, cause the processors to carry out the method claimed in any one of claims 15 to 23.