

What is claimed is:

1. A computer-implemented method of validating a certificate associated with a first node, the method comprising:
 - receiving a transaction template from the first node, the transaction template containing a first input that references a certification transaction output and is signed by a certification transaction key;
 - obtaining a copy of a certification transaction and determining that the certification transaction includes the certificate associated with the first node and that the certification transaction is signed by a certification authority key; and
 - propagating the transaction template on a blockchain network, wherein the transaction template propagated includes a second input transferring resources to an output address,
 - and whereby the transaction template is to be validated by nodes on the blockchain network if the certification transaction output is contained within an unspent transaction output set.
2. The method of claim 1, wherein the transaction template includes an input from a first public key associated with the first node, and wherein the certificate includes the first public key.
3. The method of claim 2, wherein propagating includes adding, to the transaction template prior to propagation, an output to a second public key associated with a second node.
4. The method of claim 1, wherein the transaction template includes an output to a first public key associated with the first node, and wherein the certificate includes the first public key.

5. The method of claim 4, wherein propagating includes adding, to the transaction template prior to propagation, an input from a second public key associated with a second node.
6. The method of any one of claims 1 to 5, wherein the certification transaction output includes a pay-to-public-key output in the certification transaction.
7. The method of claim 6, wherein the certification transaction output is one of a plurality of pay-to-public-key outputs in the certification transaction, and wherein each of the pay-to-public-key outputs in the certification transaction involves a different respective public key.
8. The method of any one of claims 1 to 5, wherein obtaining includes identifying a last transaction in a series of linked transactions based on the last transaction containing the certification transaction output, and tracing through the series of linked transactions to identify the certification transaction.
9. The method of claim 8, wherein obtaining further includes verifying that the certification transaction output is a multi-signature output for which a permitted signatory includes the certification authority key.
10. The method of any one of claims 1 to 9, wherein the unspent transaction output set includes all transaction outputs not yet utilized as an input to a further transaction, and wherein the unspent transaction output set is maintained by the blockchain network.
11. The method of any one of claims 1 to 10, wherein the certification transaction output is in a transaction having a transaction identifier, and wherein first input in the transaction template references the transaction identifier and wherein the certification transaction key is a private key associated with the transaction identifier and an index.

12. The method in any one of claims 1 to 11, wherein obtaining includes transmitting a request for the certification transaction to a node in the blockchain network and receiving a response containing the certification transaction.
13. The method in any one of claims 1 to 11, wherein obtaining includes receiving, from the first node, the copy of the certification transaction and a Merkle path associated with the certification transaction, and wherein the method further includes verifying that the certification transaction existing in a blockchain based on the copy of the certification transaction, the Merkle path, and a set of block headers for the blockchain.
14. A computing device to validate a certificate associated with a first node, 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 13.
15. A computer-readable medium storing processor-executable instructions for validating a certificate associated with a first node, 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 13.