CLAIMS

The invention claimed is:

1. A computer-implemented method of controlling access to a resource, the method comprising:

splitting a verification element into a plurality of shares;

determining a common secret at two or more nodes in a network; and

using the common secret to transmit at least one share of the verification element between the two or more nodes, wherein:

the common secret is determined by first (C) and second (S) nodes in the network, wherein the first node (C) is associated with a first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}), and the second node (S) is associated with a second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}); and wherein

the method further comprises:

determining a first node second private key (V_{2C}) based on at least the first node master private key (V_{1C}) and a Generator Value (GV);

determining a second node second public key (P_{2S}) based on at least the second node master public key (P_{1S}) and the Generator Value (GV); and

determining the common secret (CS) based on the first node second private key (V_{2C}) and the second node second public key (P_{2S}),

wherein the second node (S) has the same common secret (S) based on a first node second public key (P_{2C}) and a second node second private key (V_{2S}), wherein:

the first node second public key (P_{2C}) is based on at least the first node master public key (P_{1C}) and the Generator Value (GV); and

the second node second private key (V_{2S}) is based on at least the second node master private key (V_{1S}) and the Generator Value (GV).

2. A method according to claim 1 wherein the verification element is a cryptographic key, a representation of a cryptographic key, or some element which may be used to access, calculate or retrieve the cryptographic key.

3. A method according to claim 1 and further comprising the step of using the common secret to generate an encryption key, wherein the encryption key is used to encrypt the at least one share of the verification element or a message comprising or relating to said at least one share.

4. A method according to claim 1 and further comprising the step of:

storing at least three shares of the verification element at different locations relative to each other; and

wherein at least one of the at least three shares is stored in or on a back-up or safe-storage facility which is separate, independent and/or distinct from at least two other locations of the different locations.

5. A method according to claim 1, wherein the resource is a digital wallet or other resource relating to some form of currency.

6. A method according to claim 1, wherein the verification element is split into a plurality of shares such that the verification element can be restored or regenerated from two or more of the shares; and wherein the verification element is split into a plurality of shares using Shamir's Secret Sharing Scheme.

7. A method according to claim 1, wherein the common secret is:

i) determined at the two or more nodes independently of each other, such that the common secret does not require transmission over a communications channel between the nodes; and/or

ii) shared only by the two or more nodes.

8. A method according to claim 1 comprising the step of setting up, creating or registering a digital wallet, wherein the verification element is associated with the digital wallet.

9. A method according to claim 1, wherein the Generator Value (GV) is based on a message (M).

10. A method according to claim 9 and further comprising the steps of:

generating a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}); and

sending, over a communications network, the first signed message (SM1) to the second node (S),

wherein the first signed message (SM1) can be validated with a first node second public key (P_{2C}) to authenticate the first node (C).

11. A method according to claim 9 and further comprising:

receiving, over a communications network, a second signed message (SM2) from the second node (S);

validating the second signed message (SM2) with the second node second public key (P2S); and

authenticating the second node (S) based on a result of validating the second signed message (SM2), wherein the second signed message (SM2) was generated based on the message (M), or a second message (M2), and the second node second private key (V_{2S}).

12. A method according to claim 9 further comprising: receiving the message (M), over a communications network, from the second node (S).

13. A method according to claim 9 further comprising: receiving the message (M), over a communications network, from another node.

14. A method according to claim 1 and further comprising: generating a message (M); and sending, over a communications network, the message (M) to the second node (S).

15. A method according to claim 1, wherein the first node master public key (P_{1C}), second node master public key (P_{1S}) are based on elliptic curve point multiplication of respective first node master private key (V_{1C}) and second node master private key (V_{1S}) and a base point (G).

16. A method according to claim 1 further comprising the steps of:

receiving, over a communications network, the second node master public key (P_{1S}); and

storing, at a data store associated with the first node (C), the second node master public key (P_{1S}).

17. A method according to claim 1 further comprising the steps of:

generating, at a first node (C), the first node master private key (V_{1C}) and the first node master public key (P_{1C});

sending, over a communications network, the first node master public key (P_{1C}) to the second node (S) and/or another node; and

storing, in a first data store associated with the first node (C), the first node master private key (V_{1C}).

18. A method according to claim 1, wherein the Generator Value (GV) is based on determining a hash of a previous Generator Value (GV).

19. A method according to claim 1, wherein the first asymmetric cryptography pair and the second asymmetric cryptography pair are based on a function of respective previous first asymmetric cryptography pair and previous second asymmetric cryptography pair.

20. A computer-based system arranged to perform the steps of claim 1.

21. A system according to claim 20, wherein:

the resource is a digital wallet or other resource relating to some form of currency.

22. A system according to claim 20, wherein the system comprises software arranged to enable the setup, creation or registration of a digital wallet, wherein the verification element is associated with the digital wallet.