

Claims

1. A method of transferring access to a digital asset, the method comprising:-

- 5 receiving a first blockchain transaction from a first participant by each of a plurality of second participants, wherein said first participant has a first private key of a first private-public key pair of a cryptography system, and each said participant has a respective share of a second
- 10 private key of a second private-public key pair of the cryptography system, wherein said first blockchain transaction is signed with said first private key; verifying, by a plurality of said second participants, that said first blockchain transaction has been signed with said
- 15 first private key; applying a respective said share of said second private key to said first blockchain transaction to generate a respective share of a first secret value, wherein said first secret value is a second blockchain transaction signed with said
- 20 second private key, wherein said first secret value is accessible to a first threshold number of said shares of said first secret value and is inaccessible to less than said first threshold number of shares of said first secret value; and
- 25 combining at least said first threshold number of said shares of said first secret value from said first participant and a plurality of said second participants to generate said first secret value.

- 30 2. A method according to claim 1, wherein each of a plurality of said second participants has a respective private key of the cryptography system.

3. A method according to claim 1 or 2, further comprising distributing shares of a said share of said second private key in possession of said first participant among said first participant and at least one said second participant.

5

4. A method according to any one of the preceding claims, further comprising transferring access to said digital asset to a third private key of said cryptography system in the event of a said second participant becoming unresponsive.

10

5. A method according to claim 4, wherein the digital asset remains under control of said third private key for a predetermined time.

15

6. A method according to any one of the preceding claims, further comprising distributing said shares of said second private key among a plurality of said participants.

20

7. A method of transferring access to a digital asset, the method comprising:

sending a first blockchain transaction from a first participant to a plurality of second participants, wherein said first participant has a first private key of a first private-public key pair of a cryptography system, and each said participant has a respective share of a second private key of a second private-public key pair of the cryptography system, wherein said first blockchain transaction is signed with said first private key;

25

30

receiving, from a plurality of said second participants, a respective share of a first secret value, wherein said first secret value is a second blockchain transaction signed with said second private key, wherein said first secret value

is accessible to a first threshold number of said shares of said first secret value and is inaccessible to less than said first threshold number of shares of said first secret value, wherein each said share of said second private key is applied
5 to said second blockchain transaction after verification, by the corresponding said second participants, that said first blockchain transaction has been signed with said first private key; and
combining at least said first threshold number of said shares
10 of said first secret value from said first participant and a plurality of said second participants to generate said first secret value.

8. A method according to claim 7, wherein each of a
15 plurality of said second participants has a respective private key of the cryptography system.

9. A method according to claim 7 or 8, further comprising distributing shares of a said share of said second private
20 key in possession of said first participant among said first participant and at least one said second participant.

10. A method according to any one of claims 7 to 9, further comprising transferring access to said digital asset
25 to a third private key of said cryptography system in the event of a said second participant becoming unresponsive.

11. A method according to claim 10, wherein the digital
asset
30 remains under control of said third private key for a predetermined time.

12. A method according to any one of claims 7 to 11,

further comprising distributing said shares of said second private key among a plurality of said participants.

13. A method of digitally signing a message, the
5 method comprising:-
distributing first shares of a first secret value among a plurality of participants, wherein the first secret value is a private key of a public-private key pair of a cryptography system, said private key is accessible by means of a first
10 threshold number of said first shares, and is inaccessible to less than said first threshold number of said first shares;
distributing second shares of a second secret value among said plurality of participants, wherein said second secret value is an ephemeral key for use in generating digital
15 signatures, wherein said ephemeral key is accessible by means of said first threshold number of said second shares and is inaccessible to less than said first threshold number of said second shares; and
distributing third shares of a third secret value among said
20 plurality of participants, wherein each said third share is adapted to be applied to a message to generate a respective fourth share of a fourth secret value, wherein said fourth secret value is the message signed with said private key and using said ephemeral key, and wherein said fourth secret
25 value is accessible by means of a second threshold number of said fourth shares, and is inaccessible to less than said second threshold number of said fourth shares.

14. A method according to claim 13, wherein the shares
30 distributed to each said participant are inaccessible to each other said participant.

15. A method according to claim 13 or 14, wherein the step
of
distributing said shares to each said participant comprises
providing a respective encrypted communication channel with
5 the or each said participant.

16. A method according to any one of claims 13 to 15,
wherein
the first and/or second shares are created by means of
10 respective Shamir secret sharing schemes.

17. A method according to any one of claims 13 to 16,
wherein a plurality of said first and/or second shares are
respective values of a first polynomial function, and
15 corresponding secret value may be determined by deriving the
polynomial function from said first threshold number of said
shares.

18. A method according to any one of claims 13 to 17,
20 wherein at least one said first and/or second secret value is
shared among a plurality of said participants by means of
joint random secret sharing (JRSS).

19. A method according to any one of claims 13 to 18,
25 wherein sharing at least one said third secret value includes
sharing masking shares generated by joint zero secret sharing
(JZSS).

20. A method according to any one of the preceding claims,
30 wherein the cryptography system is an elliptic curve
cryptography system, wherein said public key of each said
public-private key pair is related to the corresponding

private key by multiplication of an elliptic curve generator point by said private key.

21. A computer implemented system for carrying out a method
5 according to any one of the preceding claims.