

Claims

~~1.~~

1. A method of transferring access to a digital asset, the method comprising:-
 receiving a first blockchain transaction from a first participant (8) by each of a plurality of second participants, (6, 10, 12), wherein said first participant has a first private key of a first private-public key pair of a cryptography system, and each said participant (6, 8, 10, 12) 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;
 verifying, by a plurality of said second participants, (6, 10, 12), that said first blockchain transaction has been signed with said 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 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
 combining at least said first threshold number of said shares of said first secret value from said first participant (8) and a plurality of said second participants (6, 10, 12) to generate said first secret value.

~~2.~~

2. A method according to claim 1, wherein each of a plurality of said second participants (6, 10, 12) has a respective private key of the cryptography system.

~~3.~~

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 (8) among said first participant and at least one said second participant (6, 10, 12).

4.

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 (6, 10, 12) becoming unresponsive.

5.

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

6.

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 (6, 8, 10, 12).

7.

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

sending a first blockchain transaction from a first participant (8) to a plurality of second participants (6, 10, 12), wherein said first participant (8) has a first private key of a first private-public key pair of a cryptography system, and each said participant (6, 8, 10, 12) 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;
receiving, from a plurality of said second participants (6, 10, 12),

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 to said second blockchain transaction after verification, by the corresponding said second participants, (6, 10, 12), that said first blockchain transaction has been signed with said first private key; and combining at least said first threshold number of said shares of said first secret value from said first participant (8) and a plurality of said second participants (6, 10, 12) to generate said first secret value.

~~8.~~

8. A method according to claim 7, wherein the method further comprises at least one of:

wherein each of a

plurality of said second participants (6, 10, 12) has a respective private key of the cryptography system; or

~~9. A method according to claim 7 or 8, further comprising~~

distributing shares of a said share of said second private key in possession of said first participant (8) among said first participant (8) and at least one said second participant: (10).

~~10.~~

9. A method according to any one of claims 7 to ~~9~~, 8, 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 (10) becoming unresponsive.

~~11.~~

10. A method according to claim ~~10~~9, wherein the digital asset

remains under control of said third private key for a predetermined time.

~~12.~~

11. A method according to any one of claims 7 to ~~11~~10,

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

~~13.~~

12. A method of digitally signing a message, the method comprising:-
 distributing first shares of a first secret value among a plurality of participants, (6, 8, 10, 12), 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 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, (6, 8, 10, 12), wherein said second secret value is an ephemeral key for use in generating digital 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 plurality of participants, (6, 8, 10, 12), 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 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.~~

13. A method according to claim ~~13~~12, wherein the method further comprises at least one of: the shares distributed to each said participant are inaccessible to each other said participant; or

~~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 the or each said participant;; or

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

~~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 corresponding secret value may be~~
~~determined by deriving the polynomial function from said first~~
~~threshold number of said shares;~~ ; or

~~18. A method according to any one of claims 13 to 17, 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) ~~;~~ ; or

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

~~20.~~

14. A method according to any one of the preceding
 claims,

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.~~ 15.

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