

CLAIMS

1. A method of storing certified data on a blockchain, the method comprising:-
generating a first blockchain transaction, wherein a first output of said first blockchain
5 transaction contains first data based on a first public key of a first private/public key pair,
comprising a first private key and a first public key, of a cryptography system, the first
blockchain transaction contains a first digital signature signed by means of a second
private key of a second private/public key pair, comprising a second private key and a
second public key, of a cryptography system, and the first digital signature has an input
10 containing second data related to said first public key; and
broadcasting the first blockchain transaction to the blockchain.
2. A method according to claim 1, further comprising generating at least one second
blockchain transaction, wherein a first output of said second blockchain transaction
15 contains third data based on a third public key of a third private/public key pair, comprising
a third private key and a third public key, of a cryptography system, the second blockchain
transaction contains a second digital signature signed by means of a fourth private key of
a fourth private/public key pair, comprising a fourth private key and a fourth public key, of
a cryptography system, and the second digital signature has an input containing fourth
20 data related to said third public key; and
broadcasting the second blockchain transaction to the blockchain.
3. A method according to claim 2, wherein the first output of the second blockchain
transaction contains the third data, the fourth data and the second digital signature, and
25 the second digital signature has an input containing the third data.
4. A method according to claim 2 or 3, wherein an input of the second blockchain
transaction corresponds to an output of the first blockchain transaction.
- 30 5. A method according to claim 4, wherein said input of said second blockchain
transaction contains a digital signature signed by means of the second private key.
6. A method according to any one of claims 2 to 5, wherein the fourth data is derived by
applying a one-way function to data included in the first output of the second blockchain
35 transaction and related to the third public key.

7. A method according to any one of claims 2 to 6, wherein a second output of said second blockchain transaction is spendable by means of a private key corresponding to a predetermined public key, wherein said predetermined public key is different from said
5 fourth public key.

8. A method according to any one of claims 2 to 7, further comprising generating at least one further public/private key pair from the third public/private key pair and a deterministic private/public key pair.
10

9. A method according to any one of claims 2 to 8, wherein a third output of the second blockchain transaction is spendable by means of a private key corresponding to a predetermined public key.

15 10. A method according to claim 9, wherein the third output of the second blockchain transaction is time-locked.

11. A method according to any one of claims 2 to 10, wherein the first public key and the fourth public key are a same public key.
20

12. A method according to any one of claims 2 to 10, wherein the second public key and the fourth public key are a same public key.

13. A method according to any one of claims 2 to 12, wherein said third data is
25 derived by applying a one-way function to data including said third public key.

14. A method according to any one of the preceding claims, wherein said first data is derived by applying a one-way function to data including said first public key.

30 15. A method according to any one of the preceding claims, further comprising generating an updated first blockchain transaction, wherein a first output of the updated first blockchain transaction contains updated first data based on an updated first public key, the updated first blockchain transaction contains an updated first digital signature signed by means of said second private key, and the updated first digital signature has an input
35 containing updated second data related to said updated first public key; and

broadcasting said updated first blockchain transaction to the blockchain.

16. A method according to claim 15, wherein the first output of the updated first blockchain transaction contains the updated first data, the updated second data and the updated first digital signature, and the updated first digital signature has an input containing the updated second data.

17. A method according to any one of the preceding claims, wherein the first output of the first blockchain transaction contains the first data, the second data and the first digital signature, and the first digital signature has an input containing said second data.

18. A method according to any one of the preceding claims, wherein the second data is derived by applying a one-way function to data included in the first output of the first blockchain transaction and related to the first public key.

19. A method according to any one of the preceding claims, wherein a second output of said first blockchain transaction is spendable by means of a private key corresponding to a predetermined public key, wherein said predetermined public key is different from said second public key.

20. A method according to any one of the preceding claims, wherein at least one said first output is an unspendable output.

21. A method according to any one of the preceding claims, wherein a first input of the first blockchain transaction contains a digital signature signed by means of the second private key.

22. A method according to any one of the preceding claims, wherein a second output of said first blockchain transaction is spendable by means of a private key corresponding to a predetermined public key.

23. A method according to claim 22, wherein the second output of the first blockchain transaction is time-locked.

24. A method according to any one of the preceding claims, wherein a third output of said first blockchain transaction is spendable by means of a private key corresponding to a predetermined public key, wherein said predetermined public key is different from said second public key.

5

25. A method according to any one of the preceding claims, further comprising generating at least one further public/private key pair from the first public/private key pair and a deterministic private/public key pair.

10 26. A method according to claim 8 or 25, further comprising providing digital signatures signed by means of at least one said further private key and by means of the corresponding deterministic private key.

15 27. A method according to claim 8 or 25, further comprising providing a digital signature signed by means of at least one said further private key and providing data related to the corresponding deterministic private key.

20 28. A method according to claim 27, wherein the corresponding deterministic private key is derived by applying a one-way function to the data related to the corresponding deterministic private key.

25 29. A method according to claim 8 or any one of claims 25 to 28, further comprising providing proof of knowledge of a said deterministic private key to a verifier, based on an encrypted version of the deterministic key, and on a value selected by the verifier.

25

30. A method according to any one of the preceding claims, further comprising sharing a secret value between first and second parties based on a private key of the first party and a public key of the second party, wherein the secret can also be determined from the public key of the first party and the private key of the second party.

30

31. A method according to any one of the preceding claims, further comprising generating a plurality of deterministic keys by means of repeated application of a one-way function to data.

32. A method according to claim 31, wherein a private key to be updated is based on application of a one-way function to the updated key.

33. A method according to any one of the preceding claims, wherein the first output of the
5 first blockchain transaction includes location data for indicating location of data off-chain.

34. A method of verifying certified data stored in a blockchain transaction, the method comprising:

10 identifying (i) first data based on a first public key of a first private/public key pair, comprising a first private key and a first public key, of a cryptography system and (ii) a first digital signature, stored in a blockchain transaction, wherein a first output of said blockchain transaction contains said first data, said first digital signature is signed by means of a second private key of a second private/public key pair, comprising a second
15 private key and a second public key, of a cryptography system, and the first digital signature has an input containing second data related to said first public key; and verifying said first digital signature by means of said second public key.

35. A method according to claim 34, wherein the first output of the blockchain transaction
20 contains the first data, the second data and the first digital signature, and the first digital signature has an input containing said first data.

36. A method according to claim 34 or 35, wherein at least one said first output is an unspendable output and the method further comprises identifying said first digital
25 signature and said first public key from said unspendable output.

37. A method according to any one of claims 34 to 36, wherein the second data is derived by applying a one-way function to data included in the first output of the blockchain transaction and related to the first public key, and the method further comprises identifying
30 said second data and said data included in the first output, and applying said one-way function to said data included in the first output and verifying that the resulting data corresponds to said first data.

38. A method according to any one of claims 34 to 37, further comprising identifying said blockchain transaction by means of identification data on the blockchain corresponding to said transaction.

5 39. A method according to any one of claims 34 to 38, wherein said first data is derived by applying a one-way function to data based on said first public key.

40. A method according to any one of claims 34 to 39, further comprising determining whether the blockchain transaction is unspent.

10

41. A method according to any one of claims 34 to 40, wherein said first digital signature is verified by means of said second public key subsequently to submission of the blockchain transaction to a blockchain.

15 42. A method of sharing a public key of a cryptography system between a first participant and a second participant, wherein the first participant has a first private key of a first private/public key pair comprising the first private key and a first public key of a cryptography system having a homomorphic property, the second participant has a
20 second private key of a second private/public key pair comprising the second private key and a second public key of the cryptography system, a first digital signature is signed by means of a third private key, the first digital signature has an input containing first data related to said first public key, a second digital signature is signed by means of the third private key, and the second digital signature has an input containing second data related to said second public key, the method comprising:

25 determining, by said first participant, a common secret by means of said first private key and said second public key, wherein said common secret can also be determined by means of said second private key and said first public key; and
determining, by said first participant, at least one further public key of the cryptography system based on the first public key and the common secret.

30

43. A method according to claim 42, wherein the cryptography system is an elliptic curve cryptography system or a cryptography system based on a digital signature algorithm.

44. A method according to claim 42 or 43, wherein at least one said further public key is determined based on the first public key and a deterministic key determined by means of application of a deterministic function to data based on the common secret.

5 45. A method according to claim 44, wherein the deterministic function is a one-way function.

46. A method according to claim 44 or 45, further comprising determining a plurality of said further public keys from said first public key and a plurality of deterministic keys
10 determined by means of repeated application of the deterministic function to data based on the common secret.

47. A method according to any one of claims 44 to 46, further comprising proving ownership of the first private key by providing a digital signature signed by means of a
15 private key corresponding to at least one said further public key and providing data related to at least one corresponding said deterministic key.

48. A method according to claim 47, wherein a private key corresponding to at least one said deterministic key is derived by applying a one-way function to the data related to the
20 corresponding said deterministic key.

49. A method according to any one of claims 42 to 48, further comprising proving ownership of said first private key by means of a zero knowledge proof.

25 50. A method according to any one of claims 42 to 49, further comprising proving ownership of said first private key by providing a pair of digital signatures based on respective private keys of a cryptography system having a homomorphic property, wherein said respective private keys are related to each other by said first private key.

30 51. A method according to any one of claims 42 to 50, wherein a first said digital signature is contained in a first blockchain transaction.

52. A method according to any one of claims 42 to 51, wherein a second said digital signature is contained in a second blockchain transaction.

35

53. A method of generating at least one private key of a cryptography system, wherein a first digital signature is signed by means of a second private key, and the first digital signature has an input containing first data related to a first public key of a first private/public key pair comprising a first private key and said first public key of a
- 5 cryptography system having a homomorphic property, the method comprising generating at least one third private key of the cryptography system based on the first private key and a deterministic private key.
54. A method according to claim 53, wherein the cryptography system is an elliptic curve
- 10 cryptography system or a cryptography system based on a digital signature algorithm.
55. A method according to claim 53 or 54, wherein at least one said deterministic private key is determined by means of application of a deterministic function to data.
- 15 56. A method according to claim 55, wherein the deterministic function is a one-way function.
57. A method according to claim 55 or 56, further comprising determining a plurality of said deterministic keys determined by means of repeated application of the deterministic
- 20 function to data.
58. A method according to any one of claims 53 to 57, further comprising proving ownership of said first private key by providing a digital signature signed by means of at least one said third private key and providing data related to at least one corresponding
- 25 said deterministic private key.
59. A method according to any one of claims 53 to 58, further comprising proving ownership of said first private key by means of a zero knowledge proof.
60. A method according to any one of claims 53 to 59, further comprising proving
- 30 ownership of said first private key by providing a pair of digital signatures based on respective private keys of a cryptography system having a homomorphic property, wherein said respective private keys are related to each other by said first private key.
61. A method according to claim 60, wherein a first said digital signature is contained
- 35 in a first blockchain transaction.

62. A method according to claim 60 or 61, wherein a second said digital signature is contained in a second blockchain transaction.

63. A computer implemented system comprising;

5 a processor; and

memory including executable instructions that, as a result of execution by the processor, causes the system to perform any embodiment of the computer implemented method as claimed in any one of claims 1 to 62.

10 64. A non-transitory computer readable storage medium having stored thereon executable instructions that, as a result of being executed via processor of a computer system, cause the computer system to at least perform an embodiment of the method as claimed in any one of claims 1 to 62.