

Claims

1. A computer implemented method for transferring at least one asset between a first user and a second user by means of a blockchain, the method comprising:-

5

generating a first blockchain transaction comprising at least one first input representing a respective first asset transferrable from the second user to the first user, and at least one first output representing a respective second asset, the second asset redeemable by providing a cryptographic signature of the first user and a cryptographic signature of the second user;

10

generating a second blockchain transaction having at least one second input representing a respective said second asset, and at least one second output representing a respective third asset transferrable from the first user to the second user, wherein said third asset is exchanged for a respective said first asset, and wherein said third asset is redeemable by providing a cryptographic signature of the first user and a cryptographic signature of the second user; and

15

repeating generation of said second blockchain transaction to update the value of said third asset.

20

2. A method according to claim 1, wherein the second blockchain transaction has at least one third output representing a respective said first asset.

3. A method according to claim 1 or 2, wherein at least one said first input contains control data for generating a third blockchain transaction.

25

4. A method according to any one of the preceding claims, wherein at least one said second asset is redeemable as a result of non-redemption of a said third asset, by providing the cryptographic signature of the first user.

30

5. A method according to any one of the preceding claims, wherein at least one said second asset is redeemable, after expiry of a first locktime, by providing the cryptographic signature of the first user.

- 5 6. A computer implemented method for transferring at least one asset between a first user and a second user by means of a blockchain, the method comprising:-

generating a fourth blockchain transaction having at least one fourth output representing a respective first asset transferrable from the second user to the first user and
10 corresponding to a respective first input of a first blockchain transaction;

receiving a first blockchain transaction comprising at least one first input representing a respective said first asset, and at least one first output representing a respective second asset, the second asset being redeemable by providing a cryptographic
15 signature of the first user and a cryptographic signature of the second user;

submitting said first blockchain transaction to the blockchain;

receiving a plurality of second blockchain transactions, each said second
20 blockchain transaction comprising at least one respective second input representing a respective said second asset, and at least one respective second output representing a respective third asset transferrable from the first user to the second user, wherein said third asset is exchanged for a respective said first asset, wherein said third asset is redeemable by providing a cryptographic signature of the first user and a cryptographic signature of the
25 second user; and

submitting a said second blockchain transaction to the blockchain.

7. A method according to claim 6, further comprising submitting said fourth blockchain
30 transaction to the blockchain.

8. A method according to claim 6 or 7, wherein the first blockchain transaction comprises at least one fifth output representing a respective fourth asset redeemable by providing the cryptographic signature of the second user.

5 9. A method according to claim 8, wherein the fourth asset is redeemable as a result of non-redemption of a said third asset, by providing the cryptographic signature of the second user.

10 10. A method according to claim 8 or 9, wherein the fourth asset is redeemable after expiry of a second locktime, by providing the cryptographic signature of the second user.

11. A method according to any one of the preceding claims, wherein at least one said first and/or third asset comprises machine-executable code.

15 12. A computer-implemented method for performing an exchange or executing a contract via a blockchain, the method comprising the steps:

submitting a funding transaction to the blockchain network, wherein the funding transaction:

20 i) comprises a tokenised (smart) contract relating to an asset to be transferred from a second user to a first user; and
ii) is signed by the first user;

sending, from the first user to the second user, one or more subsequent transactions

wherein each said subsequent transaction spends an output of the funding transaction and is signed by the first user;

25 submitting one of the subsequent transactions to the blockchain network, the submitted transaction having been signed by the second user.

13. A method according to claim 12 wherein the method is a method of implementing and/or executing a micropayment channel on a blockchain.

30

14. A computer-implemented system arranged to perform a method according to any preceding claim, the system comprising:

A blockchain network; and

At least one computing-based resource arranged to generate a blockchain transaction and/or submit a blockchain transaction to a blockchain network.