

CLAIMS:

1. A computer-implemented transfer method comprising the steps of:
generating a blockchain transaction (Tx) having an output (TxO) related to a digital asset and a hash of a redeem script which comprises:
 metadata comprising a token which is a representation of, or a reference to, a tokenised entity;
 and
 at least one public cryptographic key.
2. The method of claim 1 wherein the digital asset is a quantity of cryptocurrency.
3. The method of claims 1 or 2 wherein the metadata is provided in the redeem script at a location which is designated in a blockchain protocol as a location for a cryptographic key.
4. The method of any preceding claim and further include the step of submitting the transaction Tx to a blockchain network.
5. A computer-implemented method of creating a first token (T1) by an issuer (I), wherein the first token (T1) is associated with a first quantity of an encrypted, electronically transferrable digital asset (B1), the method comprising:
 - receiving, over a communications network, a request from a first user (A) for a first token (T1);
 - determining a first user public key (P1A), wherein the first user public key (P1A) forms a cryptographic pair with a first user private key (V1A);
 - allocating a first quantity of an encrypted, electronically transferrable digital asset (B1) for association with the first token (T1);

- determining a first hash (H1) of a first redeem script (RS1), wherein the first redeem script (RS1) is based on:
 - at least a first metadata (MD1) that includes information associated with the first token (T1);
 - the first user public key (P1A); and
 - a first issuer public key (P1I) associated with the issuer (I), wherein the first issuer public key (P1I) forms a cryptographic pair with a first issuer private key (V1I);
 - sending, over the communications network, a first data output (O1) to a peer-to-peer distributed ledger comprising:
 - an indication of a transaction of the first quantity of said digital asset (B1) to the first user (A); and
 - the first hash (H1), wherein the first hash (H1) is associated with the first quantity of said digital asset (B1), to provide the first token (T1) that is associated with the first user (A) and issuer (I).
6. A method according to claim 5 wherein the first data output (O1) facilitates recording of a pay to script hash transaction.
7. A method according to claim 5 or 6 wherein the step of receiving a request from a first user (A) for a token (T) comprises:
- receiving an offer or an acceptance of a contract.
8. A method according to claim 7 wherein the step of receiving a request from a first user (A) for a token (T) comprises:
- receiving at least one or more terms and conditions of a contract.
9. A method according to any one of the preceding claims further comprising:

- sending at least one or more terms and conditions of a contract to the first user (A).

10. A method according to any one of claims 7 to 9 wherein the information in the first metadata (MD1) comprises a hash of at least one or more terms and conditions of a contract.

11. A method according to any one of claims 7 to 9 wherein the information in the first metadata (MD1) comprises information on one or more of:

- a type of contract;
- one or more terms and conditions of a contract;
- a pointer to terms and conditions of a contract; and
- information on how to process the transaction.

12. A method according to any one of claims 5 to 11 and further comprising:

- storing the first redeem script (RS1) in a data store.

13. A method according to any one of claims 5 to 12 wherein the first redeem script (RS1) is in the format:

<NumSigs MD1 ... P1A P1I ... NumKeys OP_CHECKMULTISIG>

wherein

NumSigs is the number of signatures required to redeem the first token (T1);

NumKeys is the total of public key slots in the script, including the metadata and public keys;

OP_CHECKMULTISIG is an operation comparing signatures with the public key slots in sequential order.

14. A method according to any one of the claims 5 to 13 and further comprising:

- determining whether the first user (A) has an account (ACA) with the issuer (I) to facilitate transactions associated with the first token (T1), wherein if the first user (A) does not have an account, the method further comprises:

sending, over a communications network, a request to open an account (ACA) for the first user (A), wherein the account (ACA) is associated with the cryptographic pair including the first user private key (V1A) and the first user public key (P1A) for the first user (A).

15. A method according to any one of claims 5 to 14, wherein the step of allocating a first quantity of said digital asset (B1) for association with the first token (T1) comprises:

- determining a first token value (TV1) of the first token (T1);
- determining a pegging rate (PR1) for the first token (T1); and
- determining the first quantity of said digital asset (B1) based on the pegging rate (PR1) and the first token value (TV1).

16. A method according to any one of claims 5 to 14, wherein the step of allocating a first quantity of said digital asset (B1) for association with the first token (T1) comprises:

- determining a minimum threshold of said digital asset (MT1) of the first token (T1); and
- determining a first quantity of said digital asset (B1) that is at or above the minimum threshold of said digital asset (MT1).

17. A computer-implemented method of redeeming a first token (T1) associated with a first quantity of an encrypted, electronically transferrable digital asset (B1) according to any one of the preceding claims, the method comprising the issuer:

- receiving, over the communications network, a request from the first user (A) to redeem the first token (T1);
- determining the first redeem script (RS1) associated with the first token (T1);

- receiving the first user private key (V1A);

- signing, with the first user private key (V1A) and the first issuer private key (V1I), the first redeem script (RS1) to unlock the first quantity of said digital asset (B1) associated with the first token (T1); and

- sending, over the communications network, a second data output (O2) to the peer-to-peer distributed ledger comprising an indication of a transaction of the first quantity of said digital asset (B1) to the issuer (I).

18. A method according to claim 17 wherein the first token (T1) has a token value of a first portion (R1) and a second portion (R2), and wherein the request from the first user (A) to redeem the first token (T1) comprises a request to redeem a value of the first portion (R1), the method further comprising:

- determining the first user public key (P1A);

- allocating a second quantity of said digital asset (B2) for association with a second token (T2), wherein the second token has a second token value (TV2) based on the second portion (R2);

- determining a second hash (H2) of a second redeem script (RS2), wherein the second redeem script (RS2) is based on:

- at least a second metadata (MD2) that is based, at least in part, on the first metadata (MD1) associated with the first token (T1);

- the first user public key (P1A); and

- the first issuer public key (P1I) associated with the issuer (I);

wherein the second data output (O2) to the public ledger further comprises:

- an indication of a transaction of at least the second quantity of said digital asset (B2) to the first user (A); and

- the second hash (H2), wherein the second hash (H2) is associated with the second quantity of said digital asset (B2), to provide the second token (T2) that is associated with the first user (A) and the issuer (I).

19. A computer-implemented method of creating a third token (T3) by an issuer (I), wherein the third token is associated with a transfer of value from a first token (T1), according to any one of claims 1 to 12, the method comprising:

- receiving, over the communications network, a request from the first user (A), and/or a second user (B), to create the third token (T3);
- determining the first redeem script (RS1) associated with the first token (T1);
- receiving the first user private key (V1A);
- signing, with the first user private key (V1A) and the first issuer private key (V1I), the first redeem script (RS1) to unlock the first quantity of said digital asset (B1) associated with the first token (T1);
- determining a second user public key (P1B), wherein the second user public key (P1B) forms a cryptographic pair with a second user private key (V1B);
- allocating a third quantity of said digital asset (B3) for association with the third token (T3);
- determining a third hash (H3) of a third redeem script (RS3), wherein the third redeem script (RS3) is based on:
 - at least a third metadata (MD3) that is based, at least in part, on the first metadata (MD1) associated with first the token (T1);
 - the second user public key (P1B); and
 - the first issuer public key (P1I);

- sending, over the communications network, a third data output (O3) to the peer-to-peer distributed ledger comprising:

- an indication of a transaction of at least the third quantity of said digital asset (B3) to the second user (B); and

- the third hash (H3), wherein the third hash (H3) is associated with the third quantity of said digital asset (B3) to provide the third token (T3) that is associated with the second user (B) and the issuer (I).

20. A method according to claim 19 wherein the first token (T1) has a token value of a first portion (R1) and a second portion (R2), and wherein the request to create the third token (T3) comprises a request to create the third token (T3) with a third token value (TV3) based on the first portion (R1), the method further comprising:

- determining the first user public key (P1A);

- allocating a second quantity of said digital asset (B2) for association with a second token (T2), wherein the second token has a second token value (TV2) based on the second portion (R2);

- determining a second hash (H2) of a second redeem script (RS2), wherein the second redeem script (RS2) is based on;

- at least a second metadata (MD2) that is based, at least in part, on the first metadata (MD1) associated with the first token (T1);

- the first user public key (P1A);

- the first issuer public key (P1I) associated with the issuer (I);

wherein the third data output (O3) to the peer-to-peer distributed ledger further comprises:

- an indication of a transaction of at least the second quantity of said digital asset (B2) to the first user (A); and

- the second hash (H2), wherein the second hash (H1) is associated with the second quantity of said digital asset (B2), to provide the second token (T2) that is associated with the first user (A) and the issuer (I).

21. A method according to 18 or 20 wherein the step of allocating a second quantity of said digital asset (B2) comprises:

- determining a pegging rate (PR2) for the second token (T2); and
- determining the second quantity of said digital asset (B2) based on the pegging rate (PR2) and the second token value (TV2).

22. A method according to claim 18 or 20 wherein the step of allocating a second quantity of said digital asset (B2) comprises:

- determining a minimum threshold of said digital asset (MT2) of the second token (T2); and
- determining the second quantity of said digital asset (B2) that is at or above the minimum threshold of said digital asset (MT2) of the second token (T2).

23. A method according to any one of claims 14 to 17, wherein the second quantity of said digital asset (B2) and/or the third quantity of said digital asset (B3) includes, at least part, the first quantity of said digital asset (B1).

24. A method according to any one of the preceding claims further comprising:

determining a fourth quantity of said digital asset (B4) as a transaction fee,

wherein the first data output (O1), second data output (O2) and third data output (O3) to the peer-to-peer distributed ledger further comprises:

- an indication of a transaction of the fourth quantity of said digital asset (B4) as a transaction fee.

25. A method according to any one of the preceding claims wherein the peer-to-peer distributed ledger comprises the bitcoin block chain.

26. A computer-implemented method of redeeming a first token (T1) associated with a first quantity of an encrypted, electronically transferrable digital asset (B1) according to any one of the preceding claims, the method comprising the issuer:

- receiving, over the communications network, a request from the first user (A) to redeem the first token (T1);
- determining the first redeem script (RS1) associated with the first token (T1);
- sending, over the communications network, the first redeem script (RS1) for signing by the first user (A);
- receiving, over the communications network, a first redeem script signed by the first user (RS1A) with the first user private key (V1A);
- signing, with the first issuer private key (V1I), the first redeem script signed by the first user (RS1A) to unlock the first quantity of said digital asset (B1) associated with the first token (T1);
- sending, over the communications network, a second data output (O2) to the peer-to-peer distributed ledger comprising an indication of a transaction of the first quantity of said digital asset (B1) to the issuer (I).

27. A computer-implemented method of creating a third token (T3) by an issuer (I), wherein the third token is associated with a transfer of value from a first token (T1), according to any one of claims 5 to 16, the method comprising:

- receiving, over the communications network, a request from the first user (A), and/or a second user (B), to create the third token (T3);
- determining the first redeem script (RS1) associated with the first token (T1);

- sending, over the communications network, the first redeem script (RS1) for signing by the first user (A);
- receiving, over the communications network, a first redeem script signed by the first user (RS1A) with the first user private key (V1A);
- signing, with the first issuer private key (V1I), the first redeem script signed by the first user (RS1A) to unlock the first quantity of said digital asset (B1) associated with the first token (T1);
- determining a second user public key (P1B), wherein the second user public key (P1B) forms a cryptographic pair with a second user private key (V1B);
- allocating a third quantity of said digital asset (B3) for association with the third token (T3);
- determining a third hash (H3) of a third redeem script (RS3), wherein the third redeem script (RS3) is based on:
 - at least a third metadata (MD3) that is based, at least in part, on the first metadata (MD1) associated with first the token (T1);
 - the second user public key (P1B); and
 - the first issuer public key (P1I);
- sending, over the communications network, a third data output (O3) to the peer-to-peer distributed ledger comprising:
 - an indication of a transaction of at least the third quantity of said digital asset (B3) to the second user (B); and
 - the third hash (H3), wherein the third hash (H3) is associated with the third quantity of said digital asset (B3) to provide the third token (T3) that is associated with the second user (B) and the issuer (I).

28. A computer program comprising machine-readable instructions to cause a processing device to implement the method according to any one of the preceding claims.
29. A device including a processing device to perform the method according to any preceding claim.