

Claims

1. A computer implemented method including the step of processing at least one blockchain transaction (Tx) comprising a transaction ID (TxID) and:
 - 5 at least one discretionary transaction ID (DTxID);
 - a protocol flag;
 - at least one discretionary public key (DPK); and
 - a plurality of inputs, each input comprising:
 - 10 i) a parent public key (PPK) and
 - ii) a signature (S) generated using the parent public key (PPK).
2. A method according to claim 1 wherein the transaction (Tx) further comprises:
a portion of data, or a reference to a portion of data.
- 15 3. A method according to claim 1 or 2 wherein the portion of data or reference to the portion of data, the protocol flag, the at least one discretionary public key (DPK) and/or the at least one discretionary transaction ID (DTxID) are provided within an output (UTXO) of the blockchain transaction (Tx);
preferably within a locking script associated with the output (UTXO).
- 20 4. A method according to any preceding claim wherein:
each parent public key (PPK) in the plurality of inputs is associated with a respective logical parent transaction (LPTx) that is identified by a respective discretionary transaction ID (DTxID) provided in an output (UTXO) of the transaction (Tx).
- 25 5. A method according to claim 4 wherein the blockchain transaction (Tx) is arranged such that:
 - i) at least two of the parent public keys (PPKs) of the plurality of inputs are required to sign the output (UTXO) of the transaction (Tx); or
 - 30 ii) all of the parent public keys (PPKs) of the plurality of inputs are required to sign the output (UTXO) of the transaction (Tx).
6. A method according to any preceding claim wherein:
the portion of data, reference to the portion of data, the protocol flag, the at least one
35 discretionary public key (DPK) and/or the at least one discretionary transaction ID

(DTxID) are provided within the blockchain transaction (Tx) at a location following a marker or code for marking an output as invalid for subsequent use as an input to a subsequent transaction.

- 5 7. A method according to any preceding claim, and further comprising the step of:
 using the discretionary public key (DPK) and the transaction ID (TxID) to search for
 and/or identify the transaction (Tx) or the logical parent transaction within a
 blockchain.
- 10 8. A method according to any preceding claim and further comprising the step of:
 using the blockchain transaction (Tx) to represent a data node in a hierarchy, tree or
 graph of data nodes.
9. A method according to any preceding claim wherein the protocol flag is associated with
15 and/or indicative of a blockchain-based protocol for searching for, storing in and/or
 retrieving data in one or more blockchain transactions.
- 10 A method according to any preceding claim and comprising the step of processing at
 least one further blockchain transaction (Tx2) comprising a further transaction ID
20 (TxID2) and:
 at least one further discretionary transaction ID (DTxID);
 a protocol flag;
 at least one further discretionary public key (DPK); and
 a plurality of inputs, each input comprising:
25 i) a parent public key (PPK) and
 ii) a signature (S) generated using the parent public key (PPK).
11. A method according to claim 10 wherein the at least one transaction (Tx) and the at
 least one further transaction (Tx2) are arranged to form a hierarchy of blockchain
30 transactions, and such that a portion of data provided in or referenced in the at least
 one further transaction (Tx2) in a lower level of the hierarchy can be accessed or
 identified by comparison with a cryptographic key used to sign the at least one
 transaction in a higher level of the hierarchy.
- 35 12 A computer-implemented method comprising the step of:

providing or using a plurality of blockchain transactions in a hierarchy such that a portion of data provided or referenced in at least one further transaction in a lower level of the hierarchy can be accessed or identified by comparison with a cryptographic key used to sign a first transaction in a higher level of the hierarchy; wherein:

5 the first transaction and/or the at least one further transaction comprises:

a transaction ID (TxID); a protocol flag; a discretionary public key (DPK); a discretionary transaction ID (DTxID) and a plurality of inputs, each input comprising:

- i) a parent public key (PPK) and
- 10 ii) a signature (S) generated using the parent public key (PPK).

13. A computer-implemented method comprising the step:

using a first blockchain transaction to allow or prohibit access to a portion of data provided or referenced in at least one further transaction in a lower level in a

15 hierarchy of blockchain transactions based on a cryptographic key used to sign the first blockchain transaction; wherein:

the first and/or a further transaction comprises:

a transaction ID (TxID); a protocol flag; a discretionary public key (DPK); a discretionary transaction ID (DTxID); and a plurality of inputs, each input

20 comprising:

- i) a parent public key (PPK) and
- ii) a signature (S) generated using the parent public key (PPK).

14. A computer-implemented system arranged to enable a user to search for, access,

25 view, write and/or retrieve a portion of data provided in at least one blockchain transaction (Tx), wherein:

the system is arranged to identify the at least one transaction (Tx) based on a transaction index (TX_{index}) comprising a transaction ID and a public key associated with the transaction (Tx); and the at least one transaction comprises:

30 at least one output (UTXO) comprising

at least one discretionary transaction ID (DTxID);

a protocol flag; and

at least one discretionary public key (DPK);

and

35 a plurality of inputs, each comprising:

- i) a parent public key (PPK) and
- ii) a signature (S) generated using the parent public key (PPK).

15. A blockchain-implemented network or system comprising a plurality of computing
5 nodes, wherein each computing node in the blockchain-implemented network or system
comprises:

a processor; and
memory including executable instructions that, as a result of execution by
the processor, causes the system or network to perform the computer-implemented
10 method of any preceding claim.

16. A network or system according to claim 15 and further comprising:
at least one wallet function, preferably wherein the wallet is arranged to store, generate
and/or process hierarchical deterministic keys.

15 17. A non-transitory computer-readable storage medium having stored thereon executable
instructions that, as a result of being executed by a processor of a computer system, cause
the computer system to perform the computer-implemented method of any one of claims 1
to 13.

20