

CLAIMS:

1. ~~A computer-implemented system arranged to control a transfer made~~ actions related to an asset via a blockchain, the computer-implemented system comprising:

5 ~~an asset~~ a subordinate computing agent, comprising:

one or more processors; and

memory storing computer-executable instructions that, as a plurality result of private cryptographic keys, each private key being associated with execution by the one or more processors, cause the subordinate computing agent to:

10 receive an owner authorisation from a master computing agent to perform one or more actions in response to a triggering of the asset; one or more rules in a smart contract comprising at least one rule relating to automated generation of one or more blockchain transactions to enable the at least one or more actions in respect of the asset; and

15 perform the one or more actions authorised by the master computing agent; a distributed hash table storing the smart contract, wherein a hash of the smart contract is provided within metadata of a first blockchain transaction; and a registry comprising a plurality of public cryptographic keys, wherein:

ownership of the asset is split between multiple owners into shares of the asset, each owner associated with a respective private key of a plurality of private keys wherein, each public key corresponds to a private key in the asset's corresponding to a respective public key of the plurality of private public keys, and

each public key is associated with a redeem script hash of a redeem script that can be identified within an unspent blockchain transaction; a smart contract comprising at least one rule relating to the automated generation of one or more blockchain transactions to enable a transfer indicating a share of the asset associated with that public key to be made in respect redeemed according to an action of the asset; one or more actions, and

25 a computing agent arranged to evaluate and/or execute _____ in response to the triggering, to perform the one or more actions, the computer-executable instructions comprise further instructions, that, as a result of execution by the one or more processors, further cause the authorised subordinate computing agent to:

30

look up, using the hash of the smart contract, the smart contract in the distributed hash table;

perform the action of the one or more actions according to the at least one rule of the smart contract; based on using, from the registry, the public key associated with the redeem script hash for accessing the unspent blockchain transaction associated with the share of the asset; and

provide a result of the action, the result comprising generating a new blockchain transaction to redeem an output of the action on the share of the asset according to the redeem script.

2. A The computer-implemented system according to claim 1, wherein at least one of the plurality of private keys is generated as a sub-key of an existing cryptographic key pair, comprising the steps further wherein:

determining a first entity second private key is based on at least a first entity master private key and a generator value;

determining a second entity second private key is based on at least a second entity master private key and the generator value;

determining a common secret (CS) at ~~the~~ first entity is based on the first entity second private key and ~~the~~ second entity second public key, and determining the common secret (CS) at ~~the~~ second entity is based on the second entity second private key and first entity second public key; and, further wherein:

wherein:

the first entity second public key and the second entity second public key are

respectively based on at least the first/second entity master private key and the generator value; and

either the first entity or the second entity is the asset and the other of the first entity and the second entity is a controller or other entity associated with the asset.

3. A The computer-implemented system according to claim 1 or 2 wherein the transferaction is a transfer of currency to be made in respect of the asset, and wherein the transferaction relates to income or costs associated with the asset.

~~4. A~~

~~4. The computer-implemented system according to claim ~~wherein~~ 3 wherein the currency is Bitcoin, or any digital currency, or a tokenised value.~~

~~5. A~~

5 ~~5. The computer-implemented system according to any preceding claim wherein the at least one rule provided in the smart contract defines a payment schedule associated with the asset.~~

6. A ~~The computer-implemented system according to any preceding claim, further~~

10 ~~comprising one or more additional computing agents, each comprising one or more additional processors and additional memory storing additional executable instructions, wherein the master computing agent is arranged to communicate~~
~~communicates with further the one or more additional computing agents, each of said further computing agents arranged to perform the one or more additional~~
 15 ~~computing agents, as a result of execution of the additional executable instructions by the one or more additional processors, performing a task associated with the asset.~~

7. A ~~The computer-implemented system according to claim 6 wherein the each of the one or more additional computing agents are authorized by the master computing agent is~~
 20 ~~arranged to coordinate and/or authorise perform, as the activities of each of task, a discrete function, the further discrete function different from a function performed by another of the one or more additional computing agents.~~

8. A ~~The computer-implemented system according to any preceding claim and further comprising:~~

25 ~~i) at least one further, wherein the computer-executable instructions, as a result of execution by the one or more processors, further cause the subordinate computing agent arranged to generate to perform at least one of:~~

30 ~~i) generating, as the new blockchain transaction, a blockchain payment transaction relating to income associated with the asset to provide an individual payment to the share of the asset based on one or more payment rules of the smart contract;~~
~~ii) at least one further computing agent arranged to generate generating, as the new blockchain transaction, a blockchain payment transaction relating to a cost associated~~

with the asset to provide an individual payment from the share of the asset based on the one or more payment rules of the smart contract;

iii) ~~at least one further computing agent arranged to process the~~processing a netting off of income against payments associated with the asset; to consolidate multiple blockchain payment transactions from or to a single address into a single net transaction; and

iv) ~~at least one further computing agent arranged to generate~~generating and/or ~~transmit~~transmitting an alert to an owner of the asset, the alert providing a notification about an event relating to the asset.

9. ~~A~~ The computer-implemented system according to any preceding claim wherein the subordinate computing agent is arranged to generategenerates a blockchain transaction upon detection of an event or trigger specified in the smart contract.

~~10. A system according to any preceding claim wherein the smart contract is stored in a Distributed Hash Table, and a hash of the contract is provided within metadata associated with a blockchain transaction.~~

11. A computer-implemented method of controlling a transfer madeactions related to an asset via a blockchain, the computer-implemented method comprising the steps:
 defining an asset ~~comprising a~~whose ownership is split between multiple owners, the ownership associated with a plurality of private ~~cryptographic~~ keys, each private key ~~being associated with a~~respective owner of the asset;
generating a registry comprising a plurality of public~~cryptographic~~ keys wherein each public key:

corresponds to a private key in the ~~asset's~~ plurality of private keys, and is associated with a redeem script hash that can be identified within an unspent blockchain transaction, the unspent blockchain transaction indicating a number of shares of the asset owned by each public key;

generating a smart contract comprising at least one rule relating to ~~the~~ automated generation of one or more blockchain transactions to enable ~~a transfer to be made~~an action in respect of the shares of the asset;

and

using hashing the smart contract and storing a hash of the smart contract with the smart contract in a distributed hash table, wherein the hash of the smart contract is identified within metadata of a first blockchain transaction and is used to look up the smart contract in the distributed hash table;

5

and

evaluating and/or executing, by a computing agent to evaluate and/or execute, the at least one rule of the smart contract, further comprising:

performing the action according to the at least one rule of the smart contract based on using, from the registry, a first public key associated with a first redeem script hash for accessing the unspent blockchain transaction associated with the shares of the asset;

10

and

providing a result of the action, the result comprising generating a new blockchain transaction to redeem an output of the action on the shares of the asset according to a first redeem script associated with the first redeem script hash.

15

12. A The computer-implemented method according to claim 11 wherein at least one of the plurality of private keys is generated as a sub-key of an existing cryptographic key pair, comprising the steps by at least:

determining a first entity second private key based on at least a first entity master

20

private key and a generator value;

determining a second entity second private key based on at least a second entity master private key and the generator value; and

determining a common secret (CS) at ~~the~~ a first entity based on the first entity second private key and ~~the~~ a second entity second public key, and determining the common secret (CS) at ~~the~~ a second entity based on the second entity second private key and first entity second public key; ~~and~~

25

wherein:

the first entity second public key and the second entity second public key are

respectively based on at least the first/second entity master private key and the

30

generator value; and

either the first or second entity is the asset and the other of the first entity and the second entity is a controller or other entity associated with the asset.

13. A The computer-implemented method according to claim 12 wherein the ~~transferaction~~ is a transfer of currency to be made in respect of the asset, and wherein the ~~transferaction~~ relates to income or costs associated with the asset. ~~preferably,~~ wherein the currency is Bitcoin, or any digital currency, or a tokenised value.

5

14. A The computer-implemented method according to claim 12 or 13 wherein the at least one rule provided in the smart contract defines a payment schedule associated with the asset.

10 15. A The computer-implemented method according to claims 12 to 14 and further comprising ~~the step of~~ arranging the master computing agent to communicate with further computing agents, and arranging each of ~~said~~the further computing agents to perform a task associated with the asset.

15 16. A The computer-implemented method according to claim 15 wherein the master computing agent ~~is arranged to~~ coordinate~~coordinates~~ and/or ~~authorise the~~authorises activities of each of the further computing agents.

20 17. A The computer-implemented method according to claims 12 to 16 ~~and,~~ further comprising the step of providing:

i) at least one further computing agent ~~arranged to generate~~generating a blockchain transaction relating to income associated with the asset;

25 ii) at least one further computing agent ~~arranged to generate~~generating a blockchain transaction relating to a cost associated with the asset;

iii) at least one further computing agent ~~arranged to process the~~processing a netting off of income against payments associated with the asset; and

30 iv) at least one further computing agent ~~arranged to generate~~generating and/or ~~transmit~~transmitting an alert to an owner of the asset, the alert providing a notification about an event relating to the asset.

18. ~~A~~ The computer-implemented method according to claims 12 to 17 wherein the
master computing agent ~~is arranged to generate~~ generates the new blockchain
transaction upon detection of an event or trigger specified in the smart contract.

5 ~~19. A method according to claims 12 to 18 wherein the smart contract is stored in a Distributed
Hash Table, and a hash of the contract is provided within metadata associated with a
blockchain transaction.~~