

## CLAIMS:

1. A blockchain-implemented control method, the method comprising:

~~generating or deriving a one or both public-key-private-key keys in a cryptographic~~

5 pair for an item or portion of data; ~~by determining, at a first node (C), a common~~  
~~secret (CS) that is common with the first node (C) and a second node (S), wherein the~~  
~~first node (C) is associated with a first asymmetric cryptography pair having a first~~  
~~node master private key ( $V_{1C}$ ) and a first node master public key ( $P_{1C}$ ), and the second~~  
~~node (S) is associated with a second asymmetric cryptography pair having a second~~  
10 ~~node master private key ( $V_{1S}$ ) and a second node master public key ( $P_{1S}$ ), wherein the~~  
~~generating or deriving comprises:~~

~~- determining a first node second private key ( $V_{2C}$ ) based on at least the first node~~  
~~master private key ( $V_{1C}$ ) and a deterministic key (DK);~~

~~- determining a second node second public key ( $P_{2S}$ ) based on at least the second~~  
15 ~~node master public key ( $P_{1S}$ ) and the deterministic key (DK); and~~

~~- determining the common secret (CS) based on the first node second private key~~  
~~( $V_{2C}$ ) and the second node second public key ( $P_{2S}$ ),~~

~~wherein the second node (S) has the same common secret (S) based on a first~~  
~~node second public key ( $P_{2C}$ ) and a second node second private key ( $V_{2S}$ ), wherein:~~

20 ~~- the first node second public key ( $P_{2C}$ ) is based on at least the first node~~  
~~master public key ( $P_{1C}$ ) and the deterministic key (DK); and~~

~~- the second node second private key ( $V_{2S}$ ) is based on at least the second~~  
~~node master private key ( $V_{1S}$ ) and the deterministic key (DK);~~

~~deriving a signature for the data using the public-key-private-key cryptographic pair;~~  
25 ~~and~~

codifying the data to generate codified metadata for the data.

2. A method according to claim 1 and comprising the step of deriving one or both of the  
keys in the ~~public-key-private-key~~ cryptographic ~~keypair~~ from an existing cryptographic  
30 key pair, by:

determining a first entity second private key based on at least a first entity master  
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, the second entity second private key corresponding to a second entity second public key;

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

wherein:

10 the first entity second public key and the second entity second public key are respectively based on at least the first/second entity master key and the generator value.

3.- A method according to Claim 1 or 2, the method further comprising:  
transmitting the codified metadata to the blockchain.

15

4.- A method according to any preceding claim, the method further comprising:  
receiving a signature and a script from at least one user to enable access to the ~~embedded~~ data.

20 5.- A method according to Claim 4 wherein the script comprises a public key of a signatory.

6.- A method according to any preceding claim wherein the metadata comprises a hash of the data.

25

7.- A method according to any preceding claim wherein the metadata comprises a pointer to the data.

30 8.- A method according to Claim 4 wherein the hash is used as a primary key in a lookup table where the data is stored.

9. A method according to any preceding claim ~~and comprising the step of generating or deriving one or both keys in a cryptographic key pair by determining~~ wherein the deterministic key (DK) is based on a message (M).

5 ~~10. A blockchain-implemented control system operative to:~~

~~determine~~, at a first node (C), a common secret (CS) that is common with the first node (C) and a second node (S), wherein the first node (C) is associated with a first asymmetric cryptography pair having a first node master private key ( $\forall i \in V_{1C}$ ) and a first node master public key ( $P_{1C}$ ), and the second node (S) is associated with a

10 second asymmetric cryptography pair having a second node master private key ( $\forall i \in V_{1S}$ ) and a second node master public key ( $P_{1S}$ ), by:

~~wherein the step comprises:~~

\_\_\_ - determining a first node second private key ( $\forall 2 \in V_{2C}$ ) based on at least the first node master private key ( $\forall i \in V_{1C}$ ) and a deterministic key (DK);

15 \_\_\_ - determining a second node second public key ( $P_{2S}$ ) based on at least the second node master public key ( $P_{1S}$ ) and the deterministic key (DK); and

\_\_\_ - determining the common secret (CS) based on the first node second private key ( $\forall 2 \in V_{2C}$ ) and the second node second public key ( $P_{2S}$ ),

20 \_\_\_ wherein the second node (S) has the same common secret (S) based on a first node second public key ( $P_{2C}$ ) and a second node second private key ( $\forall 2 \in V_{2S}$ ), wherein:

\_\_\_ - the first node second public key ( $P_{2C}$ ) is based on at least the first node master public key ( $P_{1C}$ ) and the deterministic key (DK); and

\_\_\_ - the second node second private key ( $\forall 2 \in V_{2S}$ ) is based on at least the second node master private key ( $\forall i \in V_{1S}$ ) and the deterministic key (DK);

25 ~~10. A method according to claim 9 wherein the deterministic key (DK) is based on a message (M)~~

~~11. A blockchain-implemented control system operative to:~~

derive a public-key-private-key cryptographic key pair for an item or portion of data;

derive a signature for the data using the public-key-private-key cryptographic pair;

30 ~~and~~

codify the data to generate codified metadata for the data.

~~11.12.~~ A system according to Claim 10, the system further operative to:  
transmit the codified metadata to the blockchain.

~~13.~~

5 ~~12.~~ A system according to Claim ~~11~~10 or Claim ~~12~~11, the system further operative to:  
receive a signature and a script from at least one user to enable access to the  
~~embedded~~ metadata.

~~14.~~

10 ~~13.~~ A system according to Claim ~~13~~12, wherein the script comprises a public key of a  
signatory.

~~15.~~

~~14.~~ A system according to any of Claims ~~11~~10 to ~~14~~13, the system further operative  
to  
generate a hash of the data and to store that hash as part of the metadata.

15 ~~16.~~

~~15.~~ A system according to any of Claims ~~11~~10 to ~~15~~14, the system further operative  
to  
generate a pointer to the data.

20 ~~16.~~ ~~17.~~ A system according to Claim ~~15~~14, wherein the system is further operative to store  
the hash as a primary key in a lookup table where the data is stored.

25 ~~17.~~ ~~18.~~ A system according to any one of claims ~~11~~10 to ~~17~~, the system is arranged to  
determine, at a first node (C), a common secret (CS) that is common with the first node (C)  
and a second node (S), wherein the first node (C) is associated with a first asymmetric  
cryptography pair having a first node master private key (V<sub>ic</sub>) and a first node master  
public key (P<sub>ic</sub>), and the second node (S) is associated with a second asymmetric  
cryptography pair having a second node master private key (V<sub>is</sub>) and a second node master  
public key (P<sub>is</sub>), by:

30

—determining a first node second private key (V<sub>2c</sub>) based on at least the first node master  
private key (V<sub>ic</sub>) and a deterministic key (DK);

~~—determining a second node second public key ( $P_{2s}$ ) based on at least the second node master public key ( $P_{1s}$ ) and the deterministic key (DK); and~~

~~—determining the common secret (CS) based on the first node second private key ( $V_{2c}$ ) and the second node second public key ( $P_{2s}$ );~~

5 wherein the second node (S) has the same common secret (S) based on a first node second public key ( $P_{2c}$ ) and a second node second private key ( $V_{2s}$ ), wherein:

~~—the first node second public key ( $P_{2c}$ ) is based on at least the first node master public key ( $P_{1c}$ ) and the deterministic key (DK); and~~

10 ~~—the second node second private key ( $V_{2s}$ ) is based on at least the second node master private key ( $V_{1s}$ ) and the deterministic key (DK).~~

~~19. A system according to claim 18~~16, wherein the deterministic key (DK) is based on a message (M)).

~~20.~~

15 18. A system according to any of claims ~~11~~10 to ~~19~~17, wherein the system is arranged to derive one or both of the keys in the cryptographic key pair from an existing cryptographic key pair, by:

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

20 determining a second entity second private key based on at least a second entity master private key and the generator value, the second entity second private key corresponding to a second entity second public key;

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

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 key and the generator value.

30