

CLAIMS

What is claimed is:

1. A computer-implemented method for managing shared ownership in a block chain network, the method comprising:

5 obtaining a parent cryptographic key associated with a blockchain object (1302);
 obtaining a number (N) of parties to share control over the blockchain object (1304);
and
 generating N child cryptographic keys based on the parent cryptographic key by
applying a predetermined algorithm to the parent cryptographic key, wherein N is an integer
10 greater than or equal to 2,

 wherein applying the predetermined algorithm to the parent cryptographic key
comprises:

 generating N-1 random numbers having bit-lengths equal to a bit-length of the
parent cryptographic key (1306) and performing a series of bitwise exclusive OR (XOR)
15 operations between the parent cryptographic key and ~~a first random number~~one of the N-1
random numbers to generate a first output then sequentially performing XOR operations
between an output of a previous XOR operation and a random number not previously used to
generate an XOR child cryptographic key and obtain the N child cryptographic keys, wherein
the N child cryptographic keys include the XOR child cryptographic key and the N-1 random
20 numbers;

 receiving a plurality of cryptographic keys comprising the XOR child
cryptographic key and the N-1 random numbers;

 determining a number of the received plurality of cryptographic keys is equal to
the number of parties sharing control over the blockchain object; and

25 in response to determining that the number of the received plurality of
cryptographic keys is equal to the number of parties sharing control over the blockchain object,
reconstructing the parent cryptographic key by performing a series of bitwise XOR operations,
sequentially, on the received plurality of cryptographic keys ~~and referencing third party~~
~~auxiliary data.~~
30

2. The computer-implemented method according to claim 1, further comprising:

 transmitting the N child cryptographic keys to corresponding parties (S4); and

deleting the parent cryptographic key (S6).

3. The computer-implemented method according to claim 1, wherein applying the predetermined algorithm to the parent cryptographic key comprises:

5 modifying the parent cryptographic key based on a randomly generated character string.

4. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

obtaining a parent cryptographic key associated with a blockchain object (1302);

10 obtaining a number (N) of parties to share control over the blockchain object (1304);
and

generating N child cryptographic keys based on the parent cryptographic key by applying a predetermined algorithm to the parent cryptographic key, wherein N is an integer greater than or equal to 2, wherein applying the predetermined algorithm to the parent cryptographic key comprises:

15 generating N-1 random numbers having bit-lengths equal to a bit-length of the parent cryptographic key (1306) and performing a series of bitwise exclusive OR (XOR) operations between the parent cryptographic key and ~~a first random number one~~ of the N-1 random numbers to generate a first output then sequentially performing XOR operations
20 between an output of a previous XOR operation and a random number not previously used to generate an XOR child cryptographic key and obtain the N child cryptographic keys, wherein the N child cryptographic keys include the XOR child cryptographic key and the N-1 random numbers;

receiving a plurality of cryptographic keys comprising the XOR child
25 cryptographic key and the N-1 random numbers;

determining a number of the received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object; and

in response to determining that the number of the received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object,
30 reconstructing the parent cryptographic key by performing a series of bitwise XOR operations,

sequentially, on the received plurality of cryptographic keys ~~and referencing third party auxiliary data.~~

5. The non-transitory, computer-readable medium according to claim 4, wherein the
5 operations further comprise:

transmitting the N child cryptographic keys to corresponding parties (S4); and
deleting the parent cryptographic key (S6).

6. The non-transitory, computer-readable medium according to claim 5, wherein applying
10 the predetermined algorithm to the parent cryptographic key comprises:

modifying the parent cryptographic key based on a randomly generated character string.

7. A computer-implemented system, comprising:

obtaining a parent cryptographic key associated with a blockchain object (1302);
15 obtaining a number (N) of parties to share control over the blockchain object (1304);
and

generating N child cryptographic keys based on the parent cryptographic key by
applying a predetermined algorithm to the parent cryptographic key, wherein N is an integer
greater than or equal to 2, wherein applying the predetermined algorithm to the parent
20 cryptographic key comprises:

generating N-1 random numbers having bit-lengths equal to a bit-length of the
parent cryptographic key (1306) and performing a series of bitwise exclusive OR (XOR)
operations between the parent cryptographic key and ~~a first random number~~one of the N-1
random numbers to generate a first output then sequentially performing XOR operations
25 between an output of a previous XOR operation and a random number not previously used to
generate an XOR child cryptographic key and obtain the N child cryptographic keys, wherein
the N child cryptographic keys include the XOR child cryptographic key and the N-1 random
numbers;

receiving a plurality of cryptographic keys comprising the XOR child
30 cryptographic key and the N-1 random numbers;

determining a number of the received plurality of cryptographic keys is equal to
the number of parties sharing control over the blockchain object; and

in response to determining that the number of the received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object, reconstructing the parent cryptographic key by performing a series of bitwise XOR operations, sequentially, on the received plurality of cryptographic keys ~~and referencing third party~~
5 ~~auxiliary data.~~

8. The computer-implemented system according to claim 7, wherein the operations further comprise:

transmitting the N child cryptographic keys to corresponding parties (S4); and
10 deleting the parent cryptographic key (S6).

9. The computer-implemented system according to claim 7, wherein applying the predetermined algorithm to the parent cryptographic key comprises:

modifying the parent cryptographic key based on a randomly generated character string.
15