

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 ~~comprises performing a modulo operation based on to~~ the parent cryptographic key, ~~and~~
 ~~wherein the N child cryptographic keys are collectively configured to enable reconstruction 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 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~~
20 ~~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~~
~~cryptographic key and the N-1 random numbers;~~
 ~~determining a number of the received plurality of cryptographic keys is equal to~~
25 ~~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~~
30 ~~auxiliary data.~~

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 any one of claims 1 to 2, wherein~~
5 ~~applying the predetermined algorithm to the parent cryptographic key comprises:~~
 ~~generating N-1 random numbers R_i , wherein i is an integer between 1 and N-1 and R_i~~
 ~~is a non-negative integer (S200);~~
 ~~determining a prime number P greater than the random numbers R_i , the prime number~~
 ~~P being greater than at least one of a value S of the parent cryptographic key or the random~~
10 ~~numbers R_i , and greater than the random numbers R_i (S202); and~~
 ~~determining N child cryptographic keys C_x , wherein the child cryptographic keys C_x~~
 ~~are calculated according to the following equation:~~

$$C_x = S + P \bmod \sum_{m=1}^{N-1} R_m X^m \text{ (S204).}$$

15 ~~34. The computer-implemented method according to any one of claims 1 to 3, wherein~~
 ~~applying the predetermined algorithm to the parent cryptographic key comprises:~~
 ~~modifying the parent cryptographic key based on a randomly generated character string~~
 ~~(S2).~~

20 ~~5. _____ The computer implemented method according to any one of claims 1 to 4, further~~
 ~~comprising:~~
 ~~receiving a plurality of cryptographic keys (S80);~~
 ~~determining that a number of received plurality of cryptographic keys is equal to the~~
 ~~number of parties sharing control over the blockchain object (S82); and~~
25 ~~in response to determining that a number of received plurality of cryptographic keys is~~
 ~~equal to the number of parties sharing control over the blockchain object, reconstructing the~~
 ~~parent cryptographic key by applying a reconstruction algorithm to the received plurality of~~
 ~~cryptographic keys (S82).~~

30 ~~6. _____ The computer implemented method according to any one of claims 1 to 5, wherein the~~
 ~~original key is generated by a local server or is received from a remote server.~~

~~7. The computer implemented method according to any one of claims 1 to 6, wherein the blockchain comprises a plurality of blocks configured to store blockchain data.~~

~~48.~~ A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations 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 ~~comprises performing a modulo operation based
onto~~ the parent cryptographic key, ~~and~~

~~wherein the N child cryptographic keys are collectively configured to enable
reconstruction~~ 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 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~~
20 ~~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
cryptographic key and the N-1 random numbers;~~

25 ~~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~~
30 ~~auxiliary data.~~

~~59.~~ The non-transitory, computer-readable medium according to claim ~~48~~, wherein the operations further comprise:

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

5

~~10. The non-transitory, computer-readable medium according to any one of claims 8 to 9, wherein applying the predetermined algorithm to the parent cryptographic key comprises:~~

~~generating N-1 random numbers Ri, wherein i is an integer between 1 and N-1 and Ri is a non-negative integer (S200);~~

10 ~~determining a prime number P greater than the random numbers Ri, the prime number P being greater than at least one of a value S of the parent cryptographic key or the random numbers Ri, and greater than the random numbers Ri (S202); and~~

~~determining N child cryptographic keys CX, wherein the child cryptographic keys CX are calculated according to the following equation:~~

15 ~~$$-C_x = S + P \bmod \sum_{m=1}^{N-1} R_m X^m \text{ (S204).}$$~~

~~611.~~ The non-transitory, computer-readable medium according to ~~any one of~~ claims ~~58 to 10~~, wherein applying the predetermined algorithm to the parent cryptographic key comprises:

20 ~~modifying the parent cryptographic key based on a randomly generated character string (S2).~~

~~12. The non-transitory, computer-readable medium according to any one of claims 8 to 11, wherein the operations further comprise:~~

~~receiving a plurality of cryptographic keys (S80);~~

25 ~~determining that a number of received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object (S82); and~~

~~in response to determining that a number of received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object, reconstructing the parent cryptographic key by applying a reconstruction algorithm to the received plurality of~~
30 ~~cryptographic keys (S82).~~

~~13. The non-transitory, computer-readable medium according to any one of claims 8 to 12, wherein the original key is generated by a local server or is received from a remote server.~~

~~14. The non-transitory, computer-readable medium according to any one of claims 8 to 13, wherein the blockchain comprises a plurality of blocks configured to store blockchain data.~~

~~15. A computer-implemented system, comprising:~~

~~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 greater than or equal to 2,~~

~~wherein applying the predetermined algorithm comprises performing a modulo operation based on to the parent cryptographic key, and~~

~~wherein the N child cryptographic keys are collectively configured to enable reconstruction 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 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 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~~

~~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.

~~816.~~ The computer-implemented system according to claim ~~715~~, wherein the operations further comprise:

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

~~17.—The computer implemented system according to any one of claims 15 to 16, wherein applying the predetermined algorithm to the parent cryptographic key comprises:~~

- 10 ~~generating N-1 random numbers Ri, wherein i is an integer between 1 and N-1 and Ri is a non-negative integer (S200);~~

~~determining a prime number P greater than the random numbers Ri, the prime number P being greater than at least one of a value S of the parent cryptographic key or the random numbers Ri, and greater than the random numbers Ri (S202); and~~

- 15 ~~determining N child cryptographic keys CX, wherein the child cryptographic keys CX are calculated according to the following equation:~~

$$\text{—}C_x = S + P \bmod \sum_{m=1}^{N-1} R_m X^m \text{ (S204).}$$

- ~~918.~~ The computer-implemented system according to ~~any one of~~ claims ~~715 to 17~~, wherein
20 applying the predetermined algorithm to the parent cryptographic key comprises:

~~modifying the parent cryptographic key based on a randomly generated character string (S2).~~

- ~~19.—The computer implemented system according to any one of claims 15 to 18, wherein the operations further comprise:~~

- 25 ~~receiving a plurality of cryptographic keys (S80);~~
 ~~determining that a number of received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object (S82); and~~

- 30 ~~in response to determining that a number of received plurality of cryptographic keys is equal to the number of parties sharing control over the blockchain object, reconstructing the parent cryptographic key by applying a reconstruction algorithm to the received plurality of cryptographic keys (S82).~~

~~20. The computer implemented system according to any one of claims 15 to 19, wherein the original key is generated by a local server or is received from a remote server.~~