

WHAT IS CLAIMED IS:

1. A method for distributing multiple cryptographic keys used to access data, comprising:
receiving, by a receiving device of a processing server, a data signal superimposed with an
5 access key request, wherein the access key request includes at least a number, n , greater than 2,
of requested keys; generating, by the processing server, n key pairs using a key pair generation
algorithm, wherein each key pair includes a private key and a public key and the key pair
generation algorithm is an elliptic curve key agreement scheme; deriving, by the processing
server, an access private key by applying the private key included in each of the n key pairs to a
10 key derivation algorithm, wherein the key derivation algorithm is at least one XOR logical
operation; generating, by the processing server, an access public key corresponding to the
derived access private key using the key pair generation algorithm; and electronically
transmitting, by a transmitting device of the processing server, a data signal superimposed with a
private key included in one of the n key pairs for each of the n key pairs.

15 2. The method of claim 1, further comprising: storing, in a memory of the processing server, a
transfer key pair including a transfer public key and a transfer private key; receiving, by the
receiving device of the processing server, a data signal superimposed with a shared public key
from each of n computing devices; generating, by the processing server, n shared secrets,
20 wherein each shared secret is generated using a shared public key of the n shared public keys and
the transfer private key and the key pair generation algorithm; and encrypting, by the processing
server, the private key included in each of the n key pairs with one of the n shared secrets using
an encryption algorithm, wherein the private key included superimposed in the electronically
transmitted data signal is the respective encrypted private key.

25 3. The method of claim 2, further comprising: electronically transmitting, by the transmitting
device of the processing server, a data signal superimposed with the transfer public key to the n
computing devices.

4. The method of claim 3, wherein the data signal superimposed with the transfer public key is electronically transmitted to the n computing devices prior to receiving the data signal superimposed with the shared public key.
- 5 5. The method of claim 3, wherein each data signal superimposed with the transfer public key is a same data signal as each data signal superimposed with an encrypted private key.
6. The method of claim 2, wherein the transmitted data signal is electronically transmitted to a node in a blockchain network and where the encrypted private key is included in a transaction request that further includes a destination address corresponding to the respective shared public key.
- 10 7. The method of claim 1, wherein the elliptic curve key agreement scheme is the elliptic curve Diffie-Hellman key agreement protocol.
- 15 8. The method of claim 1, further comprising: electronically transmitting, by the transmitting device of the processing server, a data signal superimposed with a transaction request to a node in a blockchain network, wherein the transaction request includes at least a destination address signed using the derived access private key.
- 20 9. A system for distributing multiple cryptographic keys used to access data, comprising: a transmitting device of a processing server; a receiving device of the processing server configured to receive a data signal superimposed with an access key request, wherein the access key request includes at least a number, n, greater than 2, of requested keys; and a processor of the processing server configured to generate n key pairs using a key pair generation algorithm, wherein each key pair includes a private key and a public key and the key pair generation algorithm is an elliptic curve key agreement scheme, derive an access private key by applying the private key included in each of the n key pairs to a key derivation algorithm, wherein the key derivation algorithm is at least one XOR logical operation, and the generation module of the processing server is further configured to generate an access public key corresponding to the derived access private key using the key pair generation algorithm, wherein the transmitting device of the
- 25 30

processing server is configured to electronically transmit a data signal superimposed with a private key included in one of the n key pairs for each of the n key pairs.

10. The system of claim 9, further comprising: a memory of the processing server configured to
5 store a transfer key pair including a transfer public key and a transfer private key, wherein the receiving device of the processing server is further configured to receive a data signal superimposed with a shared public key from each of n computing devices, the processor of the processing server is further configured to generate n shared secrets, wherein each shared secret is
10 generated using a shared public key of the n shared public keys and the transfer private key and the key pair generation algorithm, and encrypt the private key included in each of the n key pairs with one of the n shared secrets using an encryption algorithm, and the private key included superimposed in the electronically transmitted data signal is the respective encrypted private key.

11. The system of claim 10, wherein the transmitting device of the processing server is further
15 configured to electronically transmit a data signal superimposed with the transfer public key to the n computing devices.

12. The system of claim 11, wherein the data signal superimposed with the transfer public key is
20 electronically transmitted to the n computing devices prior to receiving the data signal superimposed with the shared public key.

13. The system of claim 11, wherein each data signal superimposed with the transfer public key is a same data signal as each data signal superimposed with an encrypted private key.

25 14. The system of claim 10, wherein the transmitted data signal is electronically transmitted to a node in a blockchain network and where the encrypted private key is included in a transaction request that further includes a destination address corresponding to the respective shared public key.

30 15. The system of claim 1, wherein the elliptic curve key agreement scheme is the elliptic curve Diffie-Hellman key agreement protocol.

16. The system of claim 9, wherein the transmitting device of the processing server is further configured to electronically transmit a data signal superimposed with a transaction request to a node in a blockchain network, wherein the transaction request includes at least a destination
5 address signed using the derived access private key.