data. However, the group of four people may be unable to identify which person is to receive the single key, or such an identification may be time consuming or otherwise inconvenient for the party.

Thus, there is a need for a technical solution for the transfer of data for accessibility by a plurality of entities via the use of a single access key. Furthermore, there is a need for a technical solution whereby the transferring party can provide data to each of the plurality of entities for negotiation of ownership by the entities without participation by the transferring party. In such an instance, the data may be transferred securely with a minimal likelihood of being compromised, and with access only being available to a single entity, which may be selected among the plurality of entities without requiring additional participation by the transferring party.

SUMMARY

The present disclosure provides a description of systems and methods for distributing multiple cryptographic keys to be used in the accessing of data.

In an aspect, the present disclosure refers to a method for accessing data through the distribution of multiple cryptographic keys, comprising: transmitting, by a transmitting device of a computing device, a shared public key to a processing server; receiving, by a receiving device of the computing device, a first private key of a first cryptographic key pair from the processing server, wherein the received first private key is encrypted with a shared secret generated from the transmitted shared public key and a transfer private key possessed by the processing server; receiving, by the receiving device of the computing device, a shared private key from each of one or more additional computing devices, wherein each shared private key is different from the first private key; applying, by the computing device, a key derivation algorithm to the first private key and each shared private key to derive an access private key; accessing, by the computing device, a restricted data set, where the restricted data set is encrypted; and decrypting, by the computing device, the restricted data set using the derived access private key, wherein the restricted data set is accessed from a publicly accessible data source, and wherein the publicly accessible data source is a blockchain.

In another aspect, the present disclosure refers to a system for accessing data through the distribution of multiple cryptographic keys, comprising: a computing device comprising a processor, a memory, a transmitting device, a receiving device, a derivation module, a communication module and a decryption module, wherein the transmitting device of a computing device configured to transmit a shared public key to a processing server; the receiving device of the computing device configured to receive a first private key of a first cryptographic key pair from the processing server, wherein the received first private key is encrypted with a shared secret generated from the transmitted shared public key and a transfer private key possessed by the processing server, and receive a shared private key from each of one or more additional computing devices, wherein each shared private key is different from the first private key; the derivation module of the computing device configured to apply a key derivation algorithm to the first private key and each shared private key to derive an access private key; the communication module of the computing device configured to access a restricted data set, where the restricted data set is encrypted; and a decryption module of the computing device configured to decrypt the restricted data set using the derived access private key, wherein the restricted data set is accessed from a publicly accessible data source, and wherein the publicly accessible data source is a blockchain.

In an example, ~~A~~ a method for distributing multiple cryptographic keys used to access data includes: receiving, by a receiving device of a processing server, a data signal superimposed with an access key request, wherein the access key request includes at least a number, n, greater than 1, of requested keys; generating, by a generation module of the processing server, n key pairs using a key pair generation algorithm, wherein each key pair includes a private key and a public key; deriving, by a derivation module of the processing server, an access private key by applying the private key included in each of the n key pairs to a key derivation algorithm; generating, by the generation module of 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.

In an example, ~~A~~ a system for distributing multiple cryptographic keys used to access data includes: 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, of requested keys; a generation module of the processing server configured to generate n key pairs using a key pair generation algorithm, wherein each key pair includes a private key

WHAT IS CLAIMED IS:

1. A method for ~~distributing~~ accessing data through the distribution of multiple cryptographic keys ~~used to access data~~, comprising:

~~receiving, by a receiving device of a processing server, a data signal superimposed with an access key request, wherein the access key request includes at least a number, *n*, greater than 1, of requested keys;~~

~~generating, by a generation module of the processing server, *n* key pairs using a key pair generation algorithm, wherein each key pair includes a private key and a public key;~~

~~deriving, by a derivation module of the processing server, an access private key by applying the private key included in each of the *n* key pairs to a key derivation algorithm;~~

~~generating, by the generation module of 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.~~a computing device, a shared public key to a processing server;

~~2. The method of claim 1, further comprising:~~

~~storing, in~~receiving, by a ~~memory~~receiving device of the computing device, a first private key of a first cryptographic key pair from the processing server, ~~a transfer key pair including a transfer~~wherein the received first private key is encrypted with a shared secret generated from the transmitted shared public key and a transfer private key possessed by the processing server;

receiving, by the receiving device of the ~~processing server~~computing device, a ~~data signal superimposed with a~~ shared ~~public~~private key from each of ~~*n*~~one or more additional computing devices, wherein each shared private key is different from the first private key;

~~generating, by the generation module of the processing server, *n* shared secrets, wherein each shared secret is generated using a shared public key of the *n*~~

~~shared public keys and the transfer~~applying, by the computing device, a key derivation algorithm to the first private key and ~~the key pair generation algorithm; and~~

~~encrypting, by an encryption module of the processing server, the~~ each shared private key ~~included in each of the *n* key pairs with one of the *n* shared secrets using an encryption algorithm, wherein~~

~~the~~ to derive an access private key ~~included superimposed in the electronically transmitted data signal is the respective encrypted private key.~~;

accessing~~3. The method of claim 2, further comprising:~~

~~electronically transmitting~~, by the ~~transmitting~~computing device ~~of the processing server~~, a restricted data ~~signal superimposed with~~set, where the restricted data set is encrypted; and

decrypting, by the ~~transfer public key to~~computing device, the ~~*n* computing devices.~~restricted data set using the derived access private key,

wherein the restricted data set is accessed from a publicly accessible data source, and

wherein the publicly accessible data source is a blockchain.

2. The method of claim 1,

~~4. The method of claim 3,~~ wherein the key derivation algorithm includes use of an XOR logical operation.

3. The method of claim ~~data signal superimposed with the transfer public key is electronically transmitted to the *n* computing devices prior to~~ 1, further comprising:

receiving, by the ~~data signal superimposed with~~receiving device of the computing device, a second shared public key~~.~~ from the processing server, the received second shared public key being different from the first shared public key;

generating, by the computing device, a second shared secret using the second shared public key and a second private key of a second cryptographic key pair, the second cryptographic key pair including the second private key and the transmitted shared public key; and

decrypting, by the computing device, the first private key using the generated second shared secret prior to deriving the access private key.

4.

~~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.~~

~~7.~~ the second shared public key and the first private key are received in a single transmission from the processing server, and

the second private key is stored in a memory of the computing device.

5. The method of claim 1, wherein the ~~key pair generation algorithm is an~~ first private key and each shared private key are generated using an elliptic curve key agreement scheme.

~~8~~6. The method of claim ~~7~~5, wherein the elliptic curve key agreement scheme is the elliptic curve Diffie-Hellman key agreement protocol.

~~9~~7. The method of claim 1, wherein receiving the shared private key from each of the one or more additional computing devices comprises receiving a decrypted shared private key from each of the one or more additional computing device,

wherein each received decrypted shared private key is based on the one or more additional computing devices receiving a respective encrypted shared private key from the processing server and decrypting the respective encrypted shared private key using a respective shared secret associated with each of the one or more additional computing devices.

8. The method of claim 7, wherein each respective shared secret associated with each of the one or more additional computing devices is based on (i)

the transfer private key possessed by the processing server and (ii) a respective shared public key associated with each of the one or more additional computing devices.

9. A system for accessing data through the distribution of multiple cryptographic keys, comprising:

a computing device comprising a processor, a memory, a transmitting device, a receiving device, a derivation module, a communication module and a decryption module, wherein

the transmitting device of a computing device configured to transmit a shared public key to a processing server;

the receiving device of the computing device configured to

receive a first private key of a first cryptographic key pair from the processing server, wherein the received first private key is encrypted with a shared secret generated from the transmitted shared public key and a transfer private key possessed by the processing server, and

receive a shared private key from each of one or more additional computing devices, wherein each shared private key is different from the first private key;

the derivation module of the computing device configured to apply a key derivation algorithm to the first private key and each shared private key to derive an access private key;

the communication module of the computing device configured to access a restricted data set, where the restricted data set is encrypted; and

a decryption module of the computing device configured to decrypt the restricted data set using the derived access private key,

wherein the restricted data set is accessed from a publicly accessible data source, and

wherein the publicly accessible data source is a blockchain.

10. The system of claim 9, wherein the key derivation algorithm includes use of an XOR logical operation.

~~10.~~

11. The ~~method~~system of claim ~~1~~9, 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.~~

~~11. 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*, of requested keys;~~

a generation module 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~~computing device, wherein

the receiving device of the computing device is further configured to receive a ~~derivation module of~~second shared public key from the processing server ~~configured to derivce an access private key by applying the private~~, the received second shared public key ~~included in each of the *n*~~being different from the first shared public key ~~pairs to a key derivation algorithm, wherein~~,

the generation module of the ~~processing server~~computing device is ~~further~~ configured to generate ~~an access public key corresponding to the derived access~~a second shared secret using the second shared public key and a second private key of a second cryptographic key pair, the second cryptographic key pair including the second private key and the transmitted shared public key, and

the decryption module of the computing device is further configured to decrypt the first private key using the ~~key pair generation algorithm, and~~generated second shared secret prior to deriving the access private key.

~~the transmitting device of the 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.~~

12. The system of claim 11, ~~further comprising:~~wherein

~~an encryption module of~~ the second shared public key and the first private key are received in a single transmission from the processing server~~;~~, and

the second private key is stored in a memory of the ~~processing server configured to 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 generation module of the processing server is further configured to generate *n* shared secrets, 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,~~

~~the encryption module of the processing server is configured to 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~~device.

13. ~~The system of claim 12, wherein the transmitting device of the processing server is further configured to electronically transmit a data signal superimposed with the transfer public key to the *n* computing devices.~~

~~14. The system of claim 13, 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.~~

~~15.~~ The system of claim ~~13, 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~~9~~.~~

~~16. The system of claim~~ 12, 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.~~

~~17. The system of claim 11~~, wherein the ~~key pair generation algorithm is an~~ first private key and each shared private key are generated using an elliptic curve key agreement scheme.

~~18~~14. The system of claim ~~17~~13, wherein the elliptic curve key agreement scheme is the elliptic curve Diffie-Hellman key agreement protocol.

~~19~~15. The system of claim ~~11~~9, wherein the ~~key derivation algorithm includes use of an XOR logical operation.~~

~~20. The system of claim 11, wherein the transmitting~~receiving device of the ~~processing server~~ computing device is further configured to ~~electronically transmit a data signal superimposed with a transaction request to a node in a blockchain network, wherein~~ receive the shared private key from each of the ~~transaction request includes at least a destination address signed using the derived access~~one or more additional computing devices by receiving a decrypted shared private key from each of the one or more additional computing device,

wherein each received decrypted shared private key is based on the one or more additional computing devices receiving a respective encrypted shared private key from the processing server and decrypting the respective encrypted shared private key using a respective shared secret associated with each of the one or more additional computing devices.

16. The system of claim ~~-~~15, wherein each respective shared secret associated with each of the one or more additional computing devices is based on (i) the transfer private key possessed by the processing server and (ii) a respective shared public key associated with each of the one or more additional computing devices.