

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
5 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
10 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.

15 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
20 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
25 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
30 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 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 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

5 private key

WHAT IS CLAIMED IS:

1. 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
5 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;
 - 10 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;
 - 15 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
20 source, and
 - wherein the publicly accessible data source is a blockchain.
2. The method of claim 1, wherein the key derivation algorithm includes
use of an XOR logical operation.
25
3. The method of claim 1, further comprising:
 - receiving, by the 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;
 - 30 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.

5

4. The method of claim 3, wherein
the second shared public key and the first private key are received in a single
transmission from the processing server, and
10 the second private key is stored in a memory of the computing device.

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

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

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
20 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
25 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)
30 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
5 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
10 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
15 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
20 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.

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

11. The system of claim 9, further comprising:

a generation module of the computing device, wherein

30 the receiving device of the computing device is further configured to receive a
second shared public key from the processing server, the received second shared
public key being different from the first shared public key,

the generation module of the computing device is configured to generate 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 generated second shared secret prior to deriving
5 the access private key.

12. The system of claim 11, wherein
the second shared public key and the first private key are received in a single
transmission from the processing server, and
10 the second private key is stored in a memory of the computing device.

13. The system of claim 9, wherein the first private key and each shared private key are generated using an elliptic curve key agreement scheme.

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

15. The system of claim 9, wherein the receiving device of the computing device is further configured to receive the shared private key from each of the one or
20 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
25 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)
30 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.