

WHAT IS CLAIMED IS:

1. ~~— A computer implemented method for management of service keys for consortium blockchain networks within a blockchain as a service (BaaS) platform, the method comprising:~~

~~— receiving a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;~~

~~— determining that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;~~

~~— providing a key package comprising an encrypted private key of the service key, and a public key of the service key; and~~

~~— sending the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.~~

2. ~~— The method of claim 1, further comprising, prior to receiving the request for the service key from the participant, receiving an identity certificate from the participant.~~

3. ~~— The method of claim 2, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.~~

4. ~~— The method of claim 1, further comprising encrypting the private key of the service key using a public key associated with the participant.~~

5. ~~— The method of claim 1, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.~~

6. ~~— The method of claim 1, wherein the service key is absent from the BaaS platform after sending the key package to the participant.~~

7. ~~— The method of claim 1, wherein the participant uses the private key of the service key to encrypt transactions with one or more other participants within the consortium blockchain network.~~

5

8. ~~— One or more computer-readable storage media encoded with instructions that, when executed by one or more computers, cause the one or more computers to perform operations for management of service keys for consortium blockchain networks within a blockchain-as-a-service (BaaS) platform, the operations comprising:~~

10 ~~receiving a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;~~

~~— determining that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;~~

15 ~~— providing a key package comprising an encrypted private key of the service key, and a public key of the service key; and~~

~~— sending the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.~~

20 9. ~~— The computer-readable storage media of claim 8, wherein operations further comprise, prior to receiving the request for the service key from the participant, receiving an identity certificate from the participant.~~

25 10. ~~— The computer-readable storage media of claim 9, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.~~

30 11. ~~— The computer-readable storage media of claim 8, wherein operations further comprise encrypting the private key of the service key using a public key associated with the participant.~~

12. — ~~The computer readable storage media of claim 8, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.~~

13. — ~~The computer readable storage media of claim 8, wherein the service key is absent from the BaaS platform after sending the key package to the participant.~~

14. — ~~The computer readable storage media of claim 8, wherein the participant uses the private key of the service key to encrypt transactions with one or more other participants within the consortium blockchain network.~~

15. — ~~A system, comprising:~~

~~one or more computers; and~~

~~one or more computer readable memories coupled to the one or more computers and configured with instructions executable by the one or more computers to:~~

~~receive a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;~~

~~determine that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;~~

~~provide a key package comprising an encrypted private key of the service key, and a public key of the service key; and~~

~~send the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.~~

16. — ~~The system of claim 15, wherein the one or more computer readable memories are configured with further instructions executable by the one or more computers to, prior to receiving the request for the service key from the participant, receive an identity certificate from the participant.~~

~~17. The system of claim 16, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.~~

5 ~~18. The system of claim 15, wherein the one or more computer-readable memories are configured with further instructions executable by the one or more computers to encrypt the private key of the service key using a public key associated with the participant.~~

10 ~~19. The system of claim 15, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.~~

~~20. The system of claim 15, wherein the service key is absent from the BaaS platform~~
15 ~~after sending the key package to the participant.~~

~~21. The system of claim 15, wherein the participant uses the private key of the service key to encrypt transactions with one or more other participants within the consortium blockchain network.~~

CLAIMS

1. A computer-implemented method for management of service keys for consortium blockchain networks within a blockchain-as-a-service (BaaS) platform, the method comprising:
receiving a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;
determining that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;
providing a key package comprising an encrypted private key of the service key, and a public key of the service key; and
sending the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.
2. The method of claim 1, further comprising, prior to receiving the request for the service key from the participant, receiving an identity certificate from the participant.
3. The method of claim 2, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.
4. The method of claim 1, further comprising encrypting the private key of the service key using a public key associated with the participant.
5. The method of claim 1, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.
6. The method of claim 1, wherein the service key is absent from the BaaS platform after sending the key package to the participant.

7. The method of claim 1, wherein the participant uses the private key of the service key to encrypt transactions with one or more other participants within the consortium blockchain network.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations for management of service keys for consortium blockchain networks within a blockchain-as-a-service (BaaS) platform, the operations comprising:

receiving a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;

determining that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;

providing a key package comprising an encrypted private key of the service key, and a public key of the service key; and

sending the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.

9. The non-transitory, computer-readable storage medium of claim 8, wherein operations further comprise, prior to receiving the request for the service key from the participant, receiving an identity certificate from the participant.

10. The non-transitory, computer-readable storage medium of claim 9, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.

11. The non-transitory, computer-readable storage medium of claim 8, wherein operations further comprise encrypting the private key of the service key using a public key associated with the participant.

12. The non-transitory, computer-readable storage medium of claim 8, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.

13. The non-transitory, computer-readable storage medium of claim 8, wherein the service key is absent from the BaaS platform after sending the key package to the participant.

14. The non-transitory, computer-readable storage medium of claim 8, wherein the participant uses the private key of the service key to encrypt transactions with one or more other participants within the consortium blockchain network.

15. A system for management of service keys for consortium blockchain networks within a blockchain-as-a-service (BaaS) platform, comprising:

one or more computers; and

one or more computer-readable memories coupled to the one or more computers and having instructions stored thereon which are executable by the one or more computers to:

receive a request for a service key from a participant in a consortium blockchain network provisioned within the BaaS platform;

determine that the participant is authorized for the service key based on a service authorization table that records participant privileges within the consortium blockchain network;

provide a key package comprising an encrypted private key of the service key, and a public key of the service key; and

send the key package to the participant, the participant decrypting the private key of the service key using a public key associated with the participant.

16. The system of claim 15, wherein the one or more computer-readable memories are configured with further instructions executable by the one or more computers to, prior to receiving the request for the service key from the participant, receive an identity certificate from the participant.

17. The system of claim 16, wherein the identity certificate is received as an encrypted identity certificate, and the BaaS platform decrypts the identity certificate using a public key of the participant.

18. The system of claim 15, wherein the one or more computer-readable memories are configured with further instructions executable by the one or more computers to encrypt the private key of the service key using a public key associated with the participant.

19. The system of claim 15, wherein the service key is generated using a key derivation function (KDF) key tree in response to determining that the participant is authorized for the service key.

20. The system of claim 15, wherein the service key is absent from the BaaS platform after sending the key package to the participant.