

WHAT IS CLAIMED IS

1. A method comprising:
generating, by a first computer device, a public key and a corresponding private key, the public key for transmitting a message from a sender to a recipient, the first computer device associated with the sender;
encrypting, by the first computer device, the message using the public key and a cryptographic key of the recipient to generate a first data package, the cryptographic key of the recipient indicating an identity of the recipient;
signing, by the first computer device, a second data package using a cryptographic key of the sender to generate a third data package, the cryptographic key of the sender indicating an identity of the sender, the second data package comprising the identity of the sender, the identity of the recipient, the public key, and a hash function of the first data package;
transmitting, by the first computer device, the first data package and the third data package to a second computer device associated with the recipient;
receiving, by the first computer device, a signed version of the third data package from the second computer device, the signed version of the third data package signed using the cryptographic key of the recipient;
determining, by the first computer device, that the signed version of the third data package has been posted to a blockchain; and
responsive to the determining that the signed version of the third data package has been posted to the blockchain, posting, by the first computer device, the private key to the blockchain for decrypting the message by the recipient.
2. The method of claim 1, wherein the second data package indicates a deadline for the first computer device to receive the signed version of the third data package from the second computer device.
3. The method of claim 1, wherein the second data package indicates a deadline for the second computer device to post the signed version of the third data package to the blockchain,

and wherein the first computer device posts the private key to the blockchain responsive to determining that the signed version of the third data package is posted to the blockchain at a time earlier the deadline.

4. The method of claim 1, wherein the hash function is a collision-resistant hash function, and wherein a first size of the first data package is larger than a second size of the third data package.

5. The method of claim 1, wherein the third data package indicates a deadline for the first computer device to post the private key to the blockchain after the signed version of the third data package is posted to the blockchain by the second computer device.

6. The method of claim 1, wherein the first data package further comprises the cryptographic key of the recipient and the cryptographic key of the sender.

7. A method comprising:

receiving, by a first computer device associated with a recipient of a message, a first data package and a third data package from a second computer device associated with a sender of the message, the first data package excluding a private key for decrypting the message, the third data package generated by signing a second data package using a cryptographic key of the sender that indicates an identity of the sender, the second data package comprising the identity of the sender, an identity of the recipient, a public key for transmitting the message, and a hash function of the first data package;

transmitting, by the first computer device, a signed version of the third data package to the second computer device, the third data package signed using a cryptographic key of the recipient indicating the identity of the recipient;

determining, by the first computer device, a failure of the first computer device to receive the private key from the second computer device; and

responsive to the determining of the failure to receive the private key, posting, by the first computer device, the signed version of the third data package to a blockchain, the

posting of the signed version of the third data package indicating, to the second computer device, the failure of the first computer device to receive the private key from the second computer device.

8. The method of claim 7, wherein the first data package is generated by encrypting the message using the public key and the cryptographic key of the recipient.

9. The method of claim 7, wherein the hash function of the first data package is a collision-resistant hash function, and wherein a first size of the first data package is larger than a second size of the third data package.

10. The method of claim 7, further comprising:
determining, by the first computer device, that the private key is posted to the blockchain by the second computer device; and
decrypting, by the first computer device, the first data package using the private key to obtain the message.

11. A method comprising:
generating, by a first computer device, a public key and a private key, the public key for transmitting a message from a sender to a recipient;
encrypting, by the first computer device, the message using the public key and a cryptographic key of the recipient to generate a first data package;
signing, by the first computer device, a second data package comprising a hash function of the first data package, using a cryptographic key of the sender to generate a third data package;
transmitting, by the first computer device, the first data package and the third data package to a second computer device;
receiving, by the first computer device, a signed version of the third data package signed using the cryptographic key of the recipient from the second computer device;
determining, by the first computer device, that the signed version of the third data package has been posted to a blockchain; and

posting, by the first computer device, the private key to the blockchain.

12. The method of claim 11, wherein the second data package indicates a deadline for the first computer device to receive the signed version of the third data package.

13. The method of claim 11, wherein the second data package indicates a deadline for the second computer device to post the signed version of the third data package to the blockchain.

14. The method of claim 11, wherein the hash function is a collision-resistant hash function, and wherein a first size of the first data package is larger than a second size of the third data package.

15. The method of claim 11, wherein the third data package indicates a deadline for the first computer device to post the private key to the blockchain after the signed version of the third data package is posted to the blockchain by the second computer device.

16. A method comprising:

receiving, by a first computer device, a first data package and a third data package from a second computer device, the first data package comprising a message from a sender to a recipient and excluding a private key for decrypting the message;

transmitting, by the first computer device, a signed version of the third data package to the second computer device, the third data package signed using a cryptographic key of the recipient indicating an identity of the recipient;

determining, by the first computer device, a failure to receive the private key from the second computer device; and

responsive to the determining of the failure to receive the private key, posting, by the first computer device, the signed version of the third data package to a blockchain.

17. The method of claim 16, wherein the first data package is generated by encrypting the message using a public key generated by the second computer device and the cryptographic key of the recipient.

18. The method of claim 16, wherein the third data package is generated by signing a second data package using a cryptographic key of the sender indicating an identity of the sender, the second data package comprising the identity of the sender, the identity of the recipient, the public key, and a hash function of the first data package.

19. The method of claim 16, wherein the hash function of the first data package is a collision-resistant hash function, and wherein a first size of the first data package is larger than a second size of the third data package.

20. The method of claim 16, further comprising:
determining, by the first computer device, that the private key is posted to the blockchain;
and
decrypting, by the first computer device, the first data package using the private key to obtain the message.

21. A method comprising:
generating, by a first computer device, a public key and a private key, the public key for transmitting a message from a sender to a recipient;
encrypting, by the first computer device, the message using the public key and a cryptographic key of the recipient to generate a first data package;
signing, by the first computer device, a hash function of the first data package using a cryptographic key of the sender to generate a second data package;
transmitting, by the first computer device, the first data package and the second data package to a second computer device; and
receiving, by the first computer device, a signed version of the second data package signed using the cryptographic key of the recipient from the second computer device.

22. The method of claim 21, further comprising:
determining, by the first computer device, that the signed version of the second data
package has been posted to a blockchain; and
posting, by the first computer device, the private key to the blockchain.