

THE INVENTION CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, with at least one processor of a payment system arranged remotely from a first device operated by a first user and a second device operated by a second user, a payment request from the first device, the payment request comprising peer-to-peer payment data for a payment to be made from a first account associated with the first user to a second account associated with the second user, the peer-to-peer payment data comprising a payment amount and a user identifier of the second user;

generating, with the at least one processor, an asymmetric key pair comprising a first key and a second key;

generating, with the at least one processor, a token based on the payment amount and an account of the first user;

encrypting, with the at least one processor, the token with the first key to generate an encrypted token;

storing the encrypted token;

communicating, with the at least one processor, the second key to the first device associated with the first user, wherein the at least one processor does not directly transmit the second key to the second device associated with the second user;

transmitting the second key from the first device to the second device;

receiving, with the at least one processor, a payment completion message comprising the second key from the second device associated with the second user;

decrypting, with the at least one processor, the encrypted token based on the second key received from the second device;

determining, with the at least one processor, that the second key is received from the second user within a predetermined time period; and

after determining that the second key is received within the predetermined time period, processing the payment from the first account to the second account based on decrypting the encrypted token.

2. The computer-implemented method of claim 1, further comprising: automatically transmitting the second key from the first device to the second device in response to input from the first user.

3. The computer-implemented method of claim 1, further comprising: automatically transmitting the second key from the first device to the second device in response to determining at least one rule has been satisfied.

4. The computer-implemented method of claim 1, further comprising generating, with the at least one processor, the token based on the peer-to-peer payment data.

5. The computer-implemented method of claim 4, wherein the payment token comprises the encrypted payment data.

6. The computer-implemented method of claim 1, wherein the encrypted token comprises an encrypted value of the payment amount.

7. The computer-implemented method of claim 1, wherein the token comprises a unique identifier, an identifier associated with the second user, and encrypted payment data, wherein the encrypted payment data comprises an encrypted value of the payment amount.

8. The computer-implemented method of claim 1, further comprising:

communicating, with the at least one processor, at least a portion of the peer-to-peer payment data to a first issuer system associated with the first account.

9. A system for revocable peer-to-peer payments, comprising at least one processor of a payment system arranged remotely from a first device

operated by a first user and a second device operated by a second user, the at least one processor programmed or configured to:

- receive peer-to-peer payment data for a payment to be made from a first account associated with the first user to a second account associated with the second user, a payment request from the first device, the payment request comprising the peer-to-peer payment data comprising a payment amount and a user identifier of the second user;

- generate an asymmetric key pair comprising a first key and a second key;

- generate a token based on the payment amount and an account of the first user;

- encrypt the token with the first key to generate an encrypted token;

- store the encrypted token;

- communicate the second key to the first device associated with the first user, wherein the at least one processor does not directly transmit the second key to the second device associated with the second user;

- transmit the second key from the first device to the second device;

- receive a payment completion message comprising the second key from the second device associated with the second user;

- decrypt the encrypted token based on the second key received from the second device;

- determine that the second key is received from the second user within a predetermined time period; and

- after determining that the second key is received within the predetermined time period, process the payment from the first account to the second account based on decrypting the encrypted token.

10. The system of claim 9, wherein the at least one processor is further programmed or configured to automatically transmit the second key from the first device to the second device in response to input from the first user.

11. The system of claim 9, wherein the at least one processor is further programmed or configured to automatically transmit the second key from the first device to the second device in response to determining at least one rule has been satisfied.

12. The system of claim 9, wherein the at least one processor is further programmed or configured to generate the token based on the peer-to-peer payment data.

13. The system of claim 12, wherein the token comprises encrypted payment data.

14. The system of claim 9, wherein the encrypted token comprises an encrypted value of the payment amount.

15. The system of claim 9, wherein the token comprises a unique identifier, an identifier associated with the second user, and encrypted payment data, wherein the encrypted payment data comprises an encrypted value of the payment amount.

16. The system of claim 9, wherein the at least one processor is further programmed or configured to communicate at least a portion of the peer-to-peer payment data to a first issuer system associated with the first account.

17. The system of claim 9, wherein the payment system comprises at least one of a transaction processing system or payment gateway.

18. A computer program product for revocable peer-to-peer payments, comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor of a

payment system arranged remotely from a first device operated by a first user and a second device operated by a second user, cause the at least one processor to:

- receive peer-to-peer payment data for a payment to be made from a first account associated with the first user to a second account associated with the second user, a payment request from the first device, the payment request comprising the peer-to-peer payment data comprising a payment amount and a user identifier of the second user;

- generate an asymmetric key pair comprising a first key and a second key;

- generate a token based on the payment amount and an account of the first user;

- encrypt the token with the first key to generate an encrypted token;

- store the encrypted token;

- communicate the second key to the first device associated with the first user, wherein the at least one processor does not transmit the second key to the second device associated with the second user;

- transmit the second key from the first device to the second device;

- receive a payment completion message comprising the second key from the second device associated with the second user;

- decrypt the encrypted token based on the second key received from the second device;

- determine that the second key is received from the second user within a predetermined time period; and

- after determining that the second key is received within the predetermined time period, process the payment from the first account to the second account based on decrypting the encrypted token.

19. The computer program product of claim 18, wherein the program instructions, when executed by the at least one processor, further cause the at least one processor to generate the token based on the peer-to-peer payment data.