CLAIMS

1. A computer-implemented method of sharing blockchain transactions, wherein the method is performed by a first party and comprises:

receiving, from a second party over a QUIC connection, a payment destination, wherein the payment destination comprises a public key and/or a public-key-based address; and

sending a transaction to the second party over the QUIC connection, wherein the transaction comprises an output locked to the payment destination.

2. The method of claim 1, wherein receiving the payment destination over the QUIC connection comprises:

receiving an incoming QUIC handshake message from the second party, wherein the incoming QUIC handshake message comprises the payment destination.

3. The method of claim 2, wherein the incoming QUIC handshake message comprises a payload field, and wherein the payload field comprises the payment destination.

4. The method of claim 3, wherein the payload field comprises a transaction template, and wherein the transaction is generated based on the transaction template.

5. The method of claim 4, wherein the transaction template comprises the payment destination.

6. The method of any preceding claim, comprising sending a payment destination request for the payment destination to the second party over the QUIC connection.

7. The method of claim 6, wherein sending the payment destination request comprises:

sending an outgoing QUIC handshake message to the second party, wherein the outgoing QUIC handshake message comprises the payment destination request.

8. The method of claim 7, wherein the outgoing QUIC handshake message comprises a source connection ID field, and wherein the source connection ID field comprises the payment request.

9. The method of any of claims 7 to 8, wherein the outgoing QUIC handshake message comprises a source connection ID field, and wherein the source connection ID field comprises an identifier linked to the first party.

10. The method of claim 2 or any claim dependent thereon, wherein the incoming QUIC handshake message comprises a source connection ID field, and wherein sending the transaction to the second party over the QUIC connection comprises sending an outgoing QUIC message to the second party, wherein the outgoing QUIC message comprises i) a destination connection ID field corresponding to the source connection ID field of the incoming QUIC handshake message, and ii) a payload field comprising the transaction.

11. The method of claim 2, wherein sending the transaction over the QUIC connection comprises:

sending an outgoing handshake message to the second party, wherein the outgoing handshake message comprises the transaction.

12. The method of claim 11, wherein the outgoing QUIC handshake message comprises a source connection ID field, and wherein the source connection ID field comprises the transaction.

13. The method of claim 11, wherein the outgoing QUIC handshake message comprises a payload field, and wherein the payload field comprises the transaction.

14. The method of any of claims 11 to 13, wherein the incoming QUIC handshake message comprises a source connection ID field, and wherein the source connection ID field comprises the payment destination.

15. The method of any preceding claim, wherein the transaction is an initial transaction for a payment channel, and wherein the method comprises:

sending one or more updated versions of the initial transaction to the second party over the QUIC connection, wherein each updated version of the initial transaction is sent using a respective QUIC message.

16. The method of claim 15, comprising receiving one or more payment update requests from the second party, wherein each payment update request is sent to the first party using a respective QUIC message, and wherein each updated version of the initial transaction is sent to the second party in response to receiving a respective payment update request.

17. The method of claim 15 or claim 16, comprising:

in response to the QUIC connection being terminated, sending a latest one of the one or more updated versions of the initial transaction to one or more blockchain nodes of a blockchain network.

18. A computer-implemented method of sharing blockchain transactions, wherein the method is performed by a second party and comprises:

receiving a transaction from a first party over a QUIC connection, wherein the transaction comprises a payment destination, wherein the payment destination comprises a public key and/or a public-key-based address; and

sending the transaction to one or more blockchain nodes of a blockchain network.

19. Computer equipment comprising:

memory comprising one or more memory units; and

processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 1 to 18.

20. A computer program embodied on computer-readable storage and configured so as, when run on one or more processors, to perform the method of any of claims 1 to 18.