

aspects, the computer-implemented method further comprises generating, with at least one processor, a payment token based on the peer-to-peer payment data. In non-limiting embodiments, the payment token comprises the encrypted payment data. In non-limiting embodiments, the encrypted payment data comprises an encrypted value of a payment amount. In non-limiting embodiments, the payment token comprises a unique identifier, an identifier associated with the second user, and the encrypted payment data, wherein the encrypted payment data comprises an encrypted value of a payment amount. In non-limiting embodiments or aspects, the computer-implemented method further comprises: communicating, with 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. In non-limiting embodiments or aspects, at least one processor of a payment system is arranged remotely from the first device, the second device, and the first issuer system generates the asymmetric key pair, encrypts the at least a portion of the peer-to-peer payment data, and communicates the second key to the first device.

[0005] According to non-limiting embodiments or aspects, provided is a system for revocable peer-to-peer payments, comprising 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 a first user to a second account associated with a second user, the peer-to-peer payment data comprising a payment amount; generate an asymmetric key pair comprising a first key and a second key; encrypt at least a portion of the peer-to-peer payment data with the first key to generate encrypted payment data; store the encrypted payment data; communicate the second key to a first device associated with the first user; receive the second key from a second device associated with the second user; decrypt the encrypted payment data based on the second key received from the second device; and process the payment from the first account to the second account based on decrypting the encrypted payment data.

[0006] In non-limiting embodiments or aspects, 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. In non-limiting embodiments or aspects, 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. In non-limiting embodiments or aspects, the at least one processor is further programmed or