WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

establishing, with at least one processor, a secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a second user device associated with a second user, wherein at least one server computer does not have access to the secret key;

receiving, with the at least one server computer, from the first user device, a split-payment request message comprising encrypted data including a first value and a second value, wherein the encrypted data included in the split-payment request message is encrypted based on the secret key;

generating, with the at least one server computer, an encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message; and

transmitting, with the at least one server computer, to the second user device, a split-payment confirmation message including the encrypted balance for the requesting user and/or the second user.

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

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encryption data including an indication that the first value and/or the second value is approved;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

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

receiving, with the at least one server computer, from the second user device, a split-payment message comprising a null value associated with a transaction that does not modify the first value and the second value;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on data of the split-payment confirmation message, wherein the updated encrypted balance does not modify the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

4. The computer-implemented method of claim 2, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the second user device.

5. The computer-implemented method of claim 1, wherein generating the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message comprises:

generating, with the at least one server computer, the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

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

generating, with the at least one server computer, at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, the at least one checksum value to the first user device and/or the second user device.

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

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the first value and/or the second value is not approved;

in response to receiving the indication, generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

8. A system, comprising:

at least one processor programmed or configured to:

receive, from a first user device associated with a requesting user, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on at least one secret key, wherein the at least one secret key is established for communication between a plurality of user devices, and wherein at least one server computer does not have access to the at least one secret key;

generate an encrypted balance for at least one responding user of a plurality of responding users based on the encrypted data of the split-payment request message; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

9. The system of claim 8, wherein the at least one processor is further programmed or configured to:

receive, from at least one second user device of the plurality of second user devices, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

10. The system of claim 9, wherein the at least one processor is further programmed or configured to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

11. The system of claim 9, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point

in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

12. The system of claim 8, wherein, when generating the encrypted balance for the at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message, the at least one processor is programmed or configured to:

generate the encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

13. The system of claim 8, wherein the at least one processor is further programmed or configured to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum to one or more user devices of the plurality of user devices.

14. The system of claim 8, wherein the at least one processor is further programmed or configured to:

receive, from the at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

15. A computer-program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

establish at least one secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a plurality of second user devices associated with a plurality of responding users, wherein at least one server computer does not have access to the at least one secret key;

receive, from the first user device, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on the secret key;

generate an encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

16. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

receive, from the at least one second user device of the at least one responding user associated with the encrypted balance, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the

split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

17. The computer-program product of claim 16, wherein the one or more instructions further cause the at least one processor to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

18. The computer-program product of claim 16, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

19. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum to one or more user devices of the plurality of user devices.

20. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

receive, from the at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

21. A computer-implemented method, comprising:

establishing, with at least one processor, a secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a second user device associated with a second user, wherein at least one server computer does not have access to the secret key;

receiving, with the at least one server computer, from the first user device, a split-payment request message comprising encrypted data including a first value and a second value, wherein the encrypted data included in the split-payment request message is encrypted based on the secret key;

generating, with the at least one server computer, an encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message; and

transmitting, with the at least one server computer, to the second user device, a split-payment confirmation message including the encrypted balance for the requesting user and/or the second user.

22. The computer-implemented method of claim 21, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encryption data including an indication that the first value and/or the second value is approved;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

23. The computer-implemented method of claims 21 or 22, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment message comprising a null value associated with a transaction that does not modify the first value and the second value;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on data of the split-payment confirmation message, wherein the updated encrypted balance does not modify the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

24. The computer-implemented method of any of claims 21–23, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the second user device.

25. The computer-implemented method of any of claims 21–24, wherein generating the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message comprises:

generating, with the at least one server computer, the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

26. The computer-implemented method of any of claims 21–25, further comprising:

generating, with the at least one server computer, at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, the at least one checksum value to the first user device and/or the second user device.

27. The computer-implemented method of any of claims 21–26, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the first value and/or the second value is not approved;

in response to receiving the indication, generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

28. A system, comprising:

at least one processor programmed or configured to:

receive, from a first user device associated with a requesting user, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on at least one secret key, wherein the at least one secret key is established for communication between a plurality of user devices, and wherein at least one server computer does not have access to the at least one secret key;

generate an encrypted balance for at least one responding user of a plurality of responding users based on the encrypted data of the split-payment request message; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

29. The system of claim 28, wherein the at least one processor is further programmed or configured to:

receive, from at least one second user device of the plurality of second user devices, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

30. The system of claims 28 or 29, wherein the at least one processor is further programmed or configured to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from

another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

31. The system of any of claims 28–30, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

32. The system of any of claims 28–31, wherein, when generating the encrypted balance for the at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message, the at least one processor is programmed or configured to:

generate the encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

33. The system of any of claims 28–32, wherein the at least one processor is further programmed or configured to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum to one or more user devices of the plurality of user devices.

34. The system of any of claims 28–33, wherein the at least one processor is further programmed or configured to:

receive, from the at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

35. A computer-program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

establish at least one secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a plurality of second user devices associated with a plurality of responding users, wherein at least one server computer does not have access to the at least one secret key;

receive, from the first user device, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on the secret key;

generate an encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message

~~including the encrypted balance for the requesting user and/or the at least one responding user.~~

~~36. The computer-program product of claim 35, wherein the one or more instructions further cause the at least one processor to:~~

~~receive, from the at least one second user device of the at least one responding user associated with the encrypted balance, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;~~

~~generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and~~

~~transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.~~

~~37. The computer-program product of claims 35 or 36, wherein the one or more instructions further cause the at least one processor to:~~

~~in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,~~

~~wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and~~

~~wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.~~

38. The computer-program product of any of claims 35–37, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

39. The computer-program product of any of claims 35–38, wherein the one or more instructions further cause the at least one processor to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum to one or more user devices of the plurality of user devices.

40. The computer-program product of any of claims 35–39, wherein the one or more instructions further cause the at least one processor to:

receive, from the at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

41. A computer-implemented method, comprising:

establishing, with at least one processor, a secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a second user device associated with a

second user, wherein at least one server computer does not have access to the secret key;

receiving, with the at least one server computer, from the first user device, a split-payment request message comprising encrypted data including a first value and a second value, wherein the encrypted data included in the split-payment request message is encrypted based on the secret key;

generating, with the at least one server computer, an encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message; and

transmitting, with the at least one server computer, to the second user device, a split-payment confirmation message including the encrypted balance for the requesting user and/or the second user.

42. The computer-implemented method of claim 41, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encryption data including an indication that the first value and/or the second value is approved;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

43. The computer-implemented method of claims 41 or 42, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment message comprising a null value associated with a transaction that does not modify the first value and the second value;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on data of the split-

payment confirmation message, wherein the updated encrypted balance does not modify the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

44. The computer-implemented method of any of claims 41–43, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the second user device.

45. The computer-implemented method of any of claims 41–44, wherein generating the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message comprises:

generating, with the at least one server computer, the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

46. The computer-implemented method of any of claims 41–45, further comprising:

generating, with the at least one server computer, at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, the at least one checksum value to the first user device and/or the second user device.

47. The computer-implemented method of any of claims 41–46, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the first value and/or the second value is not approved;

in response to receiving the indication, generating, with the at least one server computer, an updated encrypted balance for the requesting user and the

second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

48. A system, comprising:

at least one processor programmed or configured to:

receive, from a first user device associated with a requesting user, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on at least one secret key, wherein the at least one secret key is established for communication between a plurality of user devices, and wherein at least one server computer does not have access to the at least one secret key;

generate an encrypted balance for at least one responding user of a plurality of responding users based on the encrypted data of the split-payment request message; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

49. The system of claim 48, wherein the at least one processor is further programmed or configured to:

receive, from at least one second user device of the plurality of second user devices, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the

split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

50. The system of claims 48 or 49, wherein the at least one processor is further programmed or configured to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

51. The system of any of claims 48-50, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

52. The system of any of claims 48-51, wherein, when generating the encrypted balance for the at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message, the at least one processor is programmed or configured to:

generate the encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

53. The system of any of claims 48–52, wherein the at least one processor is further programmed or configured to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum to one or more user devices of the plurality of user devices.

54. The system of any of claims 48–53, wherein the at least one processor is further programmed or configured to:

receive, from the at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

55. A computer-program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

establish at least one secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a plurality of second user devices associated with a plurality of responding users, wherein at least one server computer does not have access to the at least one secret key;

~~receive, from the first user device, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on the secret key;~~

~~generate an encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm; and~~

~~transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user~~.

1. A computer-implemented method, comprising:

establishing, with at least one processor, a secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a second user device associated with a second user, wherein at least one server computer does not have access to the secret key;

receiving, with the at least one server computer, from the first user device, a split-payment request message comprising encrypted data including a first value and a second value, wherein the encrypted data included in the split-payment request message is encrypted based on the secret key;

generating, with the at least one server computer, an encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message; and

transmitting, with the at least one server computer, to the second user device, a split-payment confirmation message including the encrypted balance for the requesting user and/or the second user.

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

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted

data, the second encrypted data including an indication that the first value and/or the second value is approved;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

3. The computer-implemented method of claim 2, further comprising:

receiving, with the at least one server computer, from the second user device, a split-payment message comprising a null value associated with a transaction that does not modify the first value and the second value;

generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on data of the split-payment confirmation message, wherein the updated encrypted balance does not modify the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

4. The computer-implemented method of claim 2, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the second user device.

5. The computer-implemented method of claim 1, wherein generating the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message comprises:

generating, with the at least one server computer, the encrypted balance for the requesting user and the second user based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

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

generating, with the at least one server computer, at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the second user; and

transmitting, with the at least one server computer, the at least one checksum value to the first user device and/or the second user device.

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

receiving, with the at least one server computer, from the second user device, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the first value and/or the second value is not approved;

in response to receiving the indication, generating, with the at least one server computer, an updated encrypted balance for the requesting user and the second user based on the encrypted balance for the requesting user and the second user and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmitting, with the at least one server computer, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the second user.

8. A system, comprising:

at least one processor programmed or configured to:

receive, from a first user device associated with a requesting user, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on at least one secret key, wherein the at least one secret key is established for communication between a plurality of user devices, and wherein at least one server computer does not have access to the at least one secret key;

generate an encrypted balance for at least one responding user of a plurality of responding users based on the encrypted data of the split-payment request message; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

9. The system of claim 8, wherein the at least one processor is further programmed or configured to:

receive, from at least one second user device of a plurality of second user devices, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

10. The system of claim 9, wherein the at least one processor is further programmed or configured to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

11. The system of claim 9, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

12. The system of claim 8, wherein, when generating the encrypted balance for the at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message, the at least one processor is programmed or configured to:

generate the encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm.

13. The system of claim 8, wherein the at least one processor is further programmed or configured to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum value to one or more user devices of the plurality of user devices.

14. The system of claim 8, wherein the at least one processor is further programmed or configured to:

receive, from at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.

15. A computer-program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

establish at least one secret key for communication between a plurality of user devices, the plurality of user devices comprising a first user device associated with a requesting user and a plurality of second user devices associated with a plurality of responding users, wherein at least one server computer does not have access to the at least one secret key;

receive, from the first user device, a split-payment request message comprising encrypted data associated with a value for a split-payment transaction, the encrypted data included in the split-payment request message encrypted based at least in part on the secret key;

generate an encrypted balance for at least one responding user of the plurality of responding users based on the encrypted data of the split-payment request message and an additive homomorphic cryptographic algorithm; and

transmit at least one split-payment confirmation message to at least one user device of the plurality of user devices, the split-payment confirmation message including the encrypted balance for the requesting user and/or the at least one responding user.

16. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

receive, from at least one second user device of the at least one responding user associated with the encrypted balance, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is approved by the at least one responding user associated with the encrypted balance;

generate an updated encrypted balance for the requesting user and the at least one responding user associated with the encrypted balance that approved the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and/or the at least one responding user that approved the split-payment transaction.

17. The computer-program product of claim 16, wherein the one or more instructions further cause the at least one processor to:

in response to transmitting the at least one split-payment confirmation message to the at least one user device of the plurality of user devices, receive, from another second user device of the plurality of second user devices, a split-payment message comprising a null value associated with a transaction that does not modify the value for the split-payment transaction,

wherein generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction is based on data of the split-payment confirmation message, and

wherein, when generating the updated encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction, the data of the split-payment confirmation message does not cause the at least one processor to modify the encrypted balance for the requesting user and the at least one responding user that accepted the split-payment transaction.

18. The computer-program product of claim 16, wherein the split-payment confirmation response message is received after a random interval of time has elapsed from a point in time when the split-payment confirmation message was transmitted to the at least one user device of the plurality of user devices.

19. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

generate at least one checksum value based on the data of the split-payment confirmation message and/or the encrypted balance for the requesting user and the at least one responding user that approved the split-payment transaction; and

transmit the at least one checksum value to one or more user devices of the plurality of user devices.

20. The computer-program product of claim 15, wherein the one or more instructions further cause the at least one processor to:

receive, from at least one second user device associated with the at least one responding user, a split-payment confirmation response message comprising second encrypted data, the second encrypted data including an indication that the split-payment transaction is not approved;

in response to receiving the indication, generate an updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction based on the encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction and the second encrypted data of the split-payment confirmation response message, wherein the updated encrypted balance corresponds to an initial encrypted balance established prior to the generation of the encrypted balance; and

transmit, to the first user device, a split-payment response message comprising the updated encrypted balance for the requesting user and the at least one responding user that did not approve the split-payment transaction.