WHAT IS CLAIMED IS:

1. A computer-implemented method for exchanging transaction data, the computer-implemented method comprising:

transmitting, with at least one processor, a first public encryption key via a near field communication (NFC) communication connection, the first public encryption key of a first computing device;

receiving, with at least one processor, transaction data associated with a transaction at the first computing device via the NFC communication connection, the transaction data associated with the transaction comprising:

a second public encryption key of a second computing device; and

a transaction identifier of the transaction,

generating, with at least one processor, a transaction message associated with the transaction based on the transaction data associated with the transaction and the first public encryption key;

encrypting, with at least one processor, at least a portion of the transaction message associated with the transaction with the second public encryption key;

determining, with at least one processor, that a network communication connection to a payment processing network different from the NFC communication connection can be established; and

transmitting, with at least one processor, the transaction message via the network communication connection based on determining the network communication connection to the payment processing network can be established.

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

determining the network communication connection to the payment processing network cannot be established.

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

signing at least a portion of the transaction message associated with the transaction by encrypting at least a portion of the transaction message with a first private encryption key of the first computing device.

4. The computer-implemented method according to claim 1, further comprising:

determining that the network communication connection to the payment processing network cannot be established after generating the transaction message associated with the transaction; and

storing the transaction message associated with the transaction and the first public encryption key in a memory of the first computing device based on determining the network communication connection to the payment processing network cannot be established.

5. The computer-implemented method according to claim 1, wherein transaction data associated with a transaction further comprises:

the second public encryption key of the second computing device.

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

transmitting the transaction message associated with the transaction to the second computing device.

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

transmitting a payment token associated with a payment account for a user associated with the first computing device to the second computing device,

wherein the first public encryption key and the payment token are stored in a first region of memory of the second computing device.

8. The computer-implemented method according to claim 1, wherein transmitting the first public encryption key from the first computing device comprises:

transmitting a payment token associated with a payment account for a user associated with the first computing device.

9. The computer-implemented method according to claim 1, wherein the transaction message associated with the transaction further comprises the second public encryption key.

10. The computer-implemented method according to claim 6, further comprising:

encrypting at least a portion of the transaction message using the second public encryption key prior to transmitting the transaction message to the second computing device via the NFC communication connection.

11. The computer-implemented method according to claim 6, wherein the second computing device is a NFC transponder device, and

wherein transmitting the transaction message associated with the transaction via the NFC communication connection causes an integrated circuit of the second computing device to append the transaction message to a first region in a memory of second computing device.

12. The computer-implemented method according to claim 11, further comprising: generating an electromagnetic field at the first computing device to power the second computing device,

wherein receiving the second public encryption key and the transaction data associated with the transaction from the second computing device via the NFC communication connection comprises:

receiving the second public encryption key and the transaction data associated with the transaction from the second computing device based on the second computing device being powered by the first computing device.

13. A system for exchanging transaction data, the system comprising:

at least one processor programmed or configured to:

transmit a first public encryption key via a near field communication (NFC) communication connection, the first public encryption key of a first computing device;

receive transaction data associated with a transaction at the first computing device via the NFC communication connection, the transaction data associated with the transaction comprising:

a second public encryption key of a second computing device; and

a transaction identifier of the transaction,

generate a transaction message associated with the transaction based on the transaction data associated with the transaction and the first public encryption key;

encrypt at least a portion of the transaction message associated with the transaction with the second public encryption key;

determine that a network communication connection to a payment processing network different from the NFC communication connection can be established; and

transmit the transaction message via the network communication connection based on determining the network communication connection to the payment processing network can be established.

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

determine the network communication connection to the payment processing network cannot be established.

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

sign at least a portion of the transaction message associated with the transaction by encrypting at least a portion of the transaction message with a first private encryption key of the first computing device.

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

determine that the network communication connection to the payment processing network cannot be established after generating the transaction message associated with the transaction; and

store the transaction message associated with the transaction and the first public encryption key in a memory of the first computing device based on determining the network communication connection to the payment processing network cannot be established.

17. The system according to claim 13, wherein transaction data associated with a transaction further comprises:

the second public encryption key of the second computing device.

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

transmit the transaction message associated with the transaction to the second computing device.

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

transmit a payment token associated with a payment account for a user associated with the first computing device to the second computing device,

wherein the first public encryption key and the payment token are stored in a first region of memory of the second computing device.

20. The system according to claim 13, wherein, when transmitting the first public encryption key from the first computing device, the at least one processor is further programmed or configured to:

transmit a payment token associated with a payment account for a user associated with the first computing device.

21. The system according to claim 13, wherein the transaction message associated with the transaction further comprises the second public encryption key.

22. The system according to claim 18, wherein the at least one processor is further programmed or configured to:

encrypt at least a portion of the transaction message using the second public encryption key prior to transmitting the transaction message to the second computing device via the NFC communication connection.

23. The system according to claim 18, wherein the second computing device is a NFC transponder device, and

wherein, when transmitting the transaction message associated with the transaction via the NFC communication connection, the at least one processor is further programmed or configured to cause an integrated circuit of the second computing device to append the transaction message to a first region in a memory of second computing device.

24. The system according to claim 23, wherein the at least one processor is further programmed or configured to:

generate an electromagnetic field at the first computing device to power the second computing device, and

wherein, when receiving the second public encryption key and the transaction data associated with the transaction from the second computing device via the NFC communication connection, the at least one processor is further programmed or configured to:

receive the second public encryption key and the transaction data associated with the transaction from the second computing device based on the second computing device being powered by the first computing device.

25. A computer program product for exchanging transaction data, 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:

transmit a first public encryption key via a near field communication (NFC) communication connection, the first public encryption key of a first computing device;

receive transaction data associated with a transaction at the first computing device via the NFC communication connection, the transaction data associated with the transaction comprising:

a second public encryption key of a second computing device; and

a transaction identifier of the transaction;

generate a transaction message associated with the transaction based on the transaction data associated with the transaction and the first public encryption key;

encrypt at least a portion of the transaction message associated with the transaction with the second public encryption key;

determine that a network communication connection to a payment processing network different from the NFC communication connection can be established; and

transmit the transaction message via the network communication connection based on determining the network communication connection to the payment processing network can be established.

26. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

determine the network communication connection to the payment processing network cannot be established.

27. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

sign at least a portion of the transaction message associated with the transaction by encrypting at least a portion of the transaction message with a first private encryption key of the first computing device.

28. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

determine that the network communication connection to the payment processing network cannot be established after generating the transaction message associated with the transaction; and

store the transaction message associated with the transaction and the first public encryption key in a memory of the first computing device based on determining the network communication connection to the payment processing network cannot be established.

29. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

the second public encryption key of the second computing device.

30. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

transmit the transaction message associated with the transaction to the second computing device.

31. The computer program product according to claim 25, wherein the one or more instructions further cause the at least one processor to:

transmit a payment token associated with a payment account for a user associated with the first computing device to the second computing device,

wherein the first public encryption key and the payment token are stored in a first region of memory of the second computing device.

32. The computer program product according to claim 25, wherein, the one or more instructions that cause the at least one processor to transmit the first public encryption key from the first computing device, further cause the at least one processor to:

transmit a payment token associated with a payment account for a user associated with the first computing device.

33. The computer program product according to claim 25, wherein the transaction message associated with the transaction further comprises the second public encryption key.

34. The computer program product according to claim 30, wherein the one or more instructions further cause the at least one processor to:

encrypt at least a portion of the transaction message using the second public encryption key prior to transmitting the transaction message to the second computing device via the NFC communication connection.

35. The computer program product according to claim 30, wherein the one or more instructions that cause the at least one processor to transmit the transaction message associated with the transaction via the NFC communication connection, further cause the at least one processor to: cause an integrated circuit of the second computing device to append the transaction message to a first region in a memory of second computing device.

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

generate an electromagnetic field at the first computing device to power the second computing device, and

wherein, when receiving the second public encryption key and the transaction data associated with the transaction from the second computing device via the NFC communication connection, the at least one processor is further programmed or configured to:

receive the second public encryption key and the transaction data associated with the transaction from the second computing device based on the second computing device being powered by the first computing device.

37. A method for receiving secure payment transactions while a connection to a payment processing network cannot be established, comprising:

transmitting, with at least one integrated circuit, a first public encryption key and transaction data associated with a transaction to a computing device via an NFC communication connection;

receiving, with at least one integrated circuit, a second public encryption key and a transaction message associated with the transaction via the NFC communication connection; and

appending, with at least one integrated circuit, the second public encryption key and the transaction message associated with the transaction to a database stored in a memory in communication with the at least one integrated circuit,

wherein the at least one integrated circuit is powered by an electromagnetic field generated by the computing device.

38. The method according to claim 37, wherein the memory in communication with the at least one integrated circuit has defined therein a first predefined region and a second predefined region.

39. The method according to claim 38, wherein the at least one integrated circuit is configured to limit communication of data to the first predefined region of the memory to computing devices associated with a merchant.

40. The method according to claim 38, wherein the at least one integrated circuit is configured to limit communication of data to the second predefined region of the memory to computing devices associated with users.

41. The method according to claim 38, wherein the at least one integrated circuit is configured to limit communication of data from the second predefined region of the memory to computing devices associated with a merchant.

42. A near-field communication (NFC) transponder device for receiving secure payment transactions while a connection to a payment processing network cannot be established, the NFC transponder device comprising:

at least one integrated circuit programmed or configured to:

transmit a first public encryption key and transaction data associated with a transaction to a computing device via an NFC communication connection;

receive a second public encryption key and a transaction message associated with the transaction via the NFC communication connection; and

append the second public encryption key and the transaction message associated with the transaction to a database stored in a memory in communication with the at least one integrated circuit,

wherein the at least one integrated circuit is powered by an electromagnetic field generated by a computing device.

43. The NFC transponder device according to claim 42, wherein the memory in communication with the at least one integrated circuit has defined therein a first predefined region and a second predefined region.

44. The NFC transponder device according to claim 43, wherein the at least one integrated circuit is further programmed or configured to:

limit communication of data to the first predefined region of the memory to computing devices associated with a merchant.

45. The NFC transponder device according to claim 43, wherein the at least one integrated circuit is further programmed or configured to:

limit communication of data to the second predefined region of the memory to computing devices associated with users.

46. The NFC transponder device according to claim 43, wherein the at least one integrated circuit is further programmed or configured to:

limit communication of data from the second predefined region of the memory to computing devices associated with a merchant.

47. A computer program product for receiving secure payment transactions while a connection to a payment processing network cannot be

established, comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one integrated circuit, cause the at least one integrated circuit to:

transmit a first public encryption key and transaction data associated with a transaction to a computing device via an NFC communication connection;

receive a second public encryption key and a transaction message associated with the transaction via the NFC communication connection; and

append the second public encryption key and the transaction message associated with the transaction to a database stored in a memory in communication with the at least one integrated circuit;

wherein the at least one integrated circuit is powered by an electromagnetic field generated by computing device.

48. The computer program product according to claim 47, wherein the one or more instructions further cause the at least one integrated circuit to subdivide the memory in communication with the at least one integrated circuit into a first predefined region and a second predefined region.

49. The computer program product according to claim 48, wherein the one or more instructions further cause the at least one integrated circuit to:

limit communication of data to the first predefined region of the memory to computing devices associated with a merchant.

50. The computer program product according to claim 48, wherein the one or more instructions further cause the at least one integrated circuit to:

limit communication of data to the second predefined region of the memory to computing devices associated with users.

51. The computer program product according to claim 48, wherein the one or more instructions further cause the at least one integrated circuit to:

limit communication of data from the second predefined region of the memory to computing devices associated with a merchant.