WHAT IS CLAIMED IS:

1. A method performed by a browser server including conveying an indication of a payment instead of a payment instrument of a user to a merchant server during a transaction between a computing device of the user and the merchant server over a network, comprising:

~~communicating data from a browser to an electronic shopping cart during a transaction;~~receiving, by the browser server, the payment instrument of the user from the computing device;

performing, by the browser server, a secure handshake with an electronic shopping cart on the merchant server over the network;

receiving, by the browser server from a browser client application of the computing device, user-authenticating data ~~from a user interface of the browser~~;

retrieving, by the browser server from the computing device, encrypted secure user data;

decrypting by the browser server, the retrieved encrypted secure user data using the user-authenticating data~~secure user data stored on a computing device executing at least part of the browser~~;

authenticating, by the browser server, the~~a~~ user based on the user-authenticating data and the decrypted secure user data;

in response to authenticating the user, transmitting, by the browser server, the ~~an~~ indication of the~~a~~ payment ~~from the browser~~ to the electronic shopping cart;

processing, by the browser server, the transaction using the payment instrument of the user after transmitting the indication of the payment; and

recording, by the browser server, the transaction in a blockchain in the computing device including the payment instrument of the user~~stored on the computing device~~.

~~2. The method of claim 1, wherein communicating from the browser to the electronic shopping cart comprises:~~

~~initiating the transaction using a protocol-based handshake that identifies the browser and the electronic shopping cart.~~

2~~3~~. The method of claim 1, further comprising ~~storing~~, prior to the retrieving the encrypted secure user data:

encrypting, by the browser client application, ~~by the browser,~~ the secure user data; and storing, by the browser client application, the encrypted secure user data on the computing device~~on the computing device encrypted by the user-authenticating data~~.

34. The method of claim 23, further comprising: storing, by the browser server, the encrypted ~~wherein the~~ secure user data ~~is stored~~ in a block of the blockchain.

45. The method of claim 1, wherein recording the transaction in the blockchain comprises:

generating a block of the blockchain, including the payment instrument, an identification of the transaction and an identification of the electronic shopping cart; and

encrypting the block using a key associated with the browser server.

56. The method of claim 1, wherein receiving the user-authenticating data comprises:

receiving biometric data ~~and~~ or a personal identification number (PIN) from the browser client application of the computing device~~a human user via the user interface~~.

67. The method of claim 1, wherein processing the transaction comprises:

transmitting an identification of the transaction and at least a portion of the decrypted secure user data to a financial entity.

78. The method of claim 1, wherein transmitting the indication of the payment includes displaying, by the browser client application of the computing device of the user, ~~causing to be displayed on the computing device an interface to allow the user to select~~ a selectable payment option, the user interface ~~while~~ omitting entry of user account information into the electronic shopping cart.

89. The method of claim 1, wherein recording the transaction in the blockchain comprises:

recording the transaction in a side chain of the blockchain during the transaction; ~~and~~

determining that the transaction has been completed; and

adding the side chain to the blockchain in response to the determining that ~~a completion of~~ the transaction has been completed.

9. A system, comprising:

one or more hardware processors; and

a non-transitory memory storing instructions that, when executed by the one or more hardware processors, cause the one or more hardware processors to perform a method including conveying an indication of a payment instead of a payment instrument of a user to a merchant server during a transaction between a computing device of the user and the merchant server over a network, the method comprising:

receiving the payment instrument of the user from the computing device;

performing a secure handshake with an electronic shopping cart on the merchant server over the network;

receiving user-authenticating data from a browser client application of the computing device;

retrieving encrypted secure user data from the computing device;

decrypting the retrieved encrypted secure user data using user-authenticating data;

authenticating the user based on the user-authenticating data and the decrypted secure user data;

in response to authenticating the user, transmitting the indication of the payment to the electronic shopping cart;

processing the transaction using the payment instrument of the user after transmitting the indication of the payment; and

recording the transaction in a blockchain in the computing device including the payment instrument of the user.

10. The system of claim 9, wherein the instructions, when executed by the one or more hardware processors, further causes the one or more hardware processors to further perform the method of: storing the encrypted secure user data in a block of the blockchain.

11. The system of claim 9, wherein the recording the transaction in the blockchain comprises:

generating a block of the blockchain, including an identification of the transaction and an identification of the electronic shopping cart; and

encrypting the block using a key associated with the browser.

12. The system of claim 9, wherein the receiving the user-authenticating data further comprises:

receiving biometric data or a personal identification number (PIN) from the browser client application of the computing device.

13. The system of claim 9, wherein the processing the transaction further comprises:

transmitting an identification of the transaction and at least a portion of the decrypted encrypted secure user data to a financial entity.

14. The system of claim 9, wherein the recording the transaction in the blockchain further comprises:

recording the transaction in a side chain of the blockchain during the transaction;

determining that the transaction has been completed; and

adding the side chain to the blockchain in response to the determining that the transaction has been completed.

15. A non-transitory machine-readable medium having stored thereon machine-readable instructions that, when executed, cause one or more hardware processors to perform a method including conveying an indication of a payment instead of a payment instrument of a user to a merchant server during a transaction between a computing device of the user and the merchant server over a network, the method comprising:

receiving the payment instrument of the user from the computing device;

performing a secure handshake with an electronic shopping cart on the merchant server over the network;

receiving user-authenticating data from a browser client application of the computing device;

retrieving encrypted secure user data from the computing device;

decrypting the retrieved encrypted secure user data from the computing device;

authenticating the user based on the user-authenticating data and the decrypted secure user data;

in response to authenticating the user, transmitting the indication of the payment to the electronic shopping cart;

processing the transaction using the payment instrument of the user after transmitting the indication of the payment; and

recording the transaction in a blockchain in the computing device including the payment instrument of the user.

~~10. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:~~

~~identifying a browser is associated with an electronic shopping cart during a transaction;~~

~~receiving user-authenticating data from the browser; authenticating a user, including decrypting secure user data with the user-authenticating data;~~

~~in response to authenticating the user, transmitting an indication of payment from the browser to the electronic shopping cart; and~~

~~recording the transaction in a blockchain.~~

~~11. The non-transitory machine-readable medium of claim 10, wherein the operations further comprise:~~

~~processing the transaction after transmitting the indication of payment.~~

~~12. The non-transitory machine-readable medium of claim 10, wherein identifying the browser comprises:~~

~~initiating the transaction using a protocol-based handshake between the browser and the electronic shopping cart.~~

~~13. The non-transitory machine-readable medium of claim 10, wherein the operations further comprise:~~

~~storing the secure user data on the computing device and encrypted by the user-authenticating data.~~

~~14. The non-transitory machine-readable medium of claim 13, wherein the secure user data is stored in a block of the blockchain.~~

~~15. The non-transitory machine-readable medium of claim 10, wherein recording the transaction in the blockchain comprises the operations:~~

~~generating a block of the blockchain, including an identification of the transaction and~~

an identification of the electronic shopping cart; and

encrypting the block using a key associated with the browser.

16. The non-transitory machine-readable medium of claim 10, wherein receiving user-authenticating data comprises the operations:

receiving biometric data and a personal identification number (PIN) from a human user via the user interface.

17. A system, comprising:

a non-transitory memory; and

one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the system to perform operations comprising:

performing a handshake between a browser and an electronic shopping cart during an electronic transaction;

authenticating a user in response to decrypting secure user data with received user-authenticating data;

after authenticating the user, transmitting an indication of payment from the browser to the electronic shopping cart; and

recording the transaction in a blockchain stored on a computing device executing at least part of the browser.

18. The system of claim 17, wherein authenticating the user comprises the operations:

receiving biometric data and a personal identification number (PIN) from a human user via the user interface.

19. The system of claim 17, wherein recording the transaction in the blockchain comprises the operations:

generating a block of the blockchain, including an identification of the transaction and an identification of the electronic shopping cart; and

encrypting the block using a key associated with the browser.

20. The system of claim 17, wherein the secure user data is stored in a block of the blockchain.