

WHAT IS CLAIMED IS:

1. A method comprising:

initiating, by a mobile application stored on a mobile device operated by a first user, communication with an access device operated by a second user in a transaction between the first user and the second user;

transmitting, by the mobile application, a request for transaction data to the access device;

receiving, by the mobile application, the transaction data comprising a transaction amount and a second cryptocurrency address from the access device;

receiving, by the mobile application from a token provider computer, an access token and a private cryptographic key, wherein the access token comprises a payment token associated with a first cryptocurrency address;

signing, by the mobile application using the private cryptographic key, the first cryptocurrency address, the second cryptocurrency address, and the amount to create a signed cryptocurrency transaction;

transmitting, by the mobile application, the signed cryptocurrency transaction to a node of a blockchain network;

receiving, by the mobile application, a cryptocurrency transaction identifier from the node;

generating, by the mobile application, a cryptogram using at least the access token on the mobile application and at least some of the transaction data; and

transmitting, by the mobile application, at least the cryptogram, the access token, and the cryptocurrency transaction identifier to the access device, wherein the access device generates an authorization request message requesting authorization for the transaction;

wherein the token provider computer validates the cryptogram, maps the access token to the first cryptocurrency address, extracts the cryptocurrency transaction identifier from the authorization request message, and queries the node in the blockchain network with the first cryptocurrency address and the cryptocurrency transaction identifier to verify that the mobile application previously transmitted the signed cryptocurrency transaction to the node of the blockchain network, thereby

causing the transaction amount to be transferred from the first cryptocurrency address to the second cryptocurrency address based on the verification.

2. The method of claim 1, wherein the token provider computer transmits an authorization response message approving of the transaction to the access device after the token provider computer queries the node.

3. The method of claim 1, wherein the second cryptocurrency address is associated with the second user.

4. The method of claim 1, wherein the second cryptocurrency address is associated with a third party service provider that is not the second user.

5. The method of claim 1, wherein the node of the blockchain network verifies the signed cryptocurrency transaction with a public key associated with the mobile application, before sending the cryptocurrency transaction identifier to the mobile application.

6. The method of claim 1, wherein the mobile device is a mobile phone.

7. The method of claim 1, wherein the first cryptocurrency address and the second cryptocurrency address are public keys.

8. The method of claim 1, wherein the request for transaction data is included within a processing options data object list (PDOL) message between the mobile device and the access device.

9. The method of claim 1, wherein the mobile device is a mobile phone with NFC capability.

10. A mobile device comprising:
a processor; and
a computer readable medium, the computer readable medium comprising code, executable by the processor to implement a method comprising:

initiating, by a mobile application stored on the mobile device operated by a first user, communication with an access device operated by a second user in a transaction between the first user and the second user;

transmitting, by the mobile application, a request for transaction data to the access device;

receiving, by the mobile application, the transaction data comprising a transaction amount and a second cryptocurrency address associated with the second user from the access device;

receiving, by the mobile application from a token provider computer, an access token and a private cryptographic key, wherein the access token comprises a payment token associated with a first cryptocurrency address;

signing, by the mobile application using the private cryptographic key, the first cryptocurrency address, the second cryptocurrency address, and the amount to create a signed cryptocurrency transaction;

transmitting, by the mobile application, the signed cryptocurrency transaction to a node of a blockchain network;

receiving, by the mobile application, a cryptocurrency transaction identifier from the node;

generating, by the mobile application, a cryptogram using at least the access token on the mobile application and at least some of the transaction data; and

transmitting, by the mobile application, at least the cryptogram, the access token, and the cryptocurrency transaction identifier to the access device, wherein the access device generates an authorization request message requesting authorization for the transaction;

wherein the token provider computer validates the cryptogram, maps the access token to the first cryptocurrency address, extracts the cryptocurrency transaction identifier from the authorization request message, and queries the node in the blockchain network with the first cryptocurrency address and the cryptocurrency transaction identifier to verify that the mobile application previously transmitted the signed cryptocurrency transaction to the node of the blockchain network, thereby

causing the transaction amount to be transferred from the first cryptocurrency address to the second cryptocurrency address.

11. The mobile device of claim 10, further comprising a memory storing a limited use key, wherein the limited-use key is used to generate the cryptogram.

12. The mobile device of claim 10, in the method, responsive to receiving the transaction data, the mobile application performs an authentication process of the first user.

13. A method comprising:

transmitting, by a token provider computer to a mobile device, an access token and a private cryptographic key, wherein the access token comprises a payment token associated with a first cryptocurrency address;

receiving, by the token provider computer, an authorization request message comprising a cryptogram, the access token, and a cryptocurrency transaction identifier from an access device;

validating, by the token provider computer, the cryptogram;

mapping, the access token to the first cryptocurrency address;

extracting the cryptocurrency transaction identifier from the authorization request message; and

querying a node in a blockchain network with the first cryptocurrency address and the cryptocurrency transaction identifier to verify that a mobile application on the mobile device that interacted with the access device previously transmitted a signed cryptocurrency transaction to the node of the blockchain network, thereby causing a transaction amount to be transferred from the first cryptocurrency address to a second cryptocurrency address.

14. The method of claim 13, wherein the method further comprises after querying the node of the blockchain network with the first cryptocurrency address and the cryptocurrency transaction identifier to verify that the mobile application transmitted the signed cryptocurrency transaction to the node,

generating an authorization response message and transmits the authorization response message to the access device.

15. The method of claim 13, wherein the mobile device is a wearable device.

16. The method of claim 13, wherein mapping, the access token to the first cryptocurrency address further comprises:

accessing, by the token provider computer, a token mapping table;

matching, by the token provider computer, the access token to an access token stored in the token mapping table; and

retrieving, by the token provider computer, the first cryptocurrency address associated with the matched access token.

17. The method of claim 13, wherein the access token is generated by the token provider computer during a token provisioning process.

18. The method of claim 13, wherein the node of the block chain network verifies the cryptocurrency transaction by validating the received cryptocurrency transaction identifier.