CLAIMS

What is claimed is:

1. A method for asset transfer, applied to a blockchain node, comprising the following:

receiving an asset transfer request sent by a first client device, wherein the asset transfer request is sent based on an asset transfer operation of a first user, and the asset transfer request comprises asset transfer information;

invoking a first smart contract in a blockchain, and locking a to-be-transferred asset based on the first smart contract and the asset transfer information, the locking the to-be-transferred asset resulting in a locked to-be-transferred asset;

sending asset information of the to-be-transferred asset to a designated trading platform, so that the trading platform determines, based on the asset information, a second user who trades with the first user; and

obtaining asset transfer confirmation information from the first client device, and performing transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information, so as to transfer the to-be-transferred asset to the second user, wherein the asset transfer confirmation information comprises information about the second user,

wherein the asset transfer information comprises first identification information of the to-be-transferred asset; and

the obtaining asset transfer confirmation information from the first client device comprises the following:

obtaining a first possessing code of the first user regarding the to-be-transferred asset and a first public key corresponding to the first possessing code from the blockchain based on the first identification information, wherein the first possessing code represents that the to-be-transferred asset belongs to the first user;

encrypting the first possessing code based on the first public key to obtain a ciphertext of the first possessing code;

sending the ciphertext of the first possessing code to the first client device, so that the first client device decrypts the ciphertext of the first possessing code based on a first private key corresponding to the first public key to obtain the first possessing code, and

generating the asset transfer confirmation information based on the first possessing code; and

receiving the asset transfer confirmation information sent by the first client device.

2. The method according to claim 1, wherein the performing transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information comprises the following:

invoking a second smart contract in the blockchain, and generating a second possessing code based on the second smart contract; and

receiving asset transfer verification information sent by a second client device, wherein the asset transfer verification information is generated based on the obtained first possessing code; and

if verification of the asset transfer verification information succeeds, sending the second possessing code to the second client device to represent that the to-be-transferred asset belongs to the second user.

3. The method according to claim 2, wherein the asset transfer confirmation information further comprises the following: the first identification information, and first signature data obtained by signing the first possessing code based on the first private key; and

the generating a second possessing code based on the second smart contract comprises the following:

obtaining the corresponding first public key from the blockchain based on the second smart contract and the first identification information; and

if verification of the first signature data based on the first public key succeeds, generating the second possessing code.

4. The method according to claim 2, wherein the asset transfer confirmation information further comprises a second public key of the second user; the asset transfer verification information comprises the following: the first identification information, and second signature data obtained by signing the first possessing code based on a second private key corresponding to the second public key;

after the generating a second possessing code based on the second smart contract, the method further comprises the following:

storing the second possessing code, the second public key, and the first identification information in association with the blockchain; and

the verification of the asset transfer verification information succeeds, comprising the following:

obtaining the second public key stored in association with the blockchain based on the first identification information in the asset transfer verification information; and

if verification of the second signature data based on the second public key succeeds, determining that the verification of the asset transfer verification information succeeds.

5. The method according to claim 1, wherein the asset transfer information comprises first identification information of the to-be-transferred asset; and

the locking a to-be-transferred asset based on the first smart contract and the asset transfer information comprises the following:

generating lock record information based on the first smart contract, the first identification information, and state information representing that the to-be-transferred asset is in a locked state; and

storing the lock record information in the blockchain.

6. The method according to any one of claims 1 to 5, after the performing transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information succeeds, comprising the following:

generating asset transfer success record information based on the asset transfer information; and

storing the asset transfer success record information in the blockchain.

7. A method for asset transfer, applied to a first client device, comprising the following:

sending an asset transfer request to a blockchain node in response to an asset transfer operation of a first user, so that the blockchain node locks a to-be-transferred asset based on asset transfer information comprised in the asset transfer request; and sending asset information of the to-be-transferred asset to a designated trading platform, so that the trading platform determines, based on the asset information, a second user who trades with the first user; and

sending asset transfer confirmation information to the blockchain node based on information about the second user, so that the blockchain node performs transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information, so as to transfer the to-be-transferred asset to the second user,

wherein the sending asset transfer confirmation information to the blockchain node based on information about the second user comprises the following:

receiving a ciphertext of a first possessing code sent by the blockchain node, wherein the ciphertext of the first possessing code is obtained by the blockchain node by encrypting the first possessing code based on a first public key of the first user; the first possessing code represents that the to-be-transferred asset belongs to the first user;

decrypting the ciphertext of the first possessing code based on a first private key corresponding to the first public key to obtain the first possessing code;

displaying the obtained first possessing code, so that the first user performs an asset transfer confirmation operation when verification of the first possessing code succeeds;

generating the asset transfer confirmation information based on the first possessing code and the information about the second user in response to the asset transfer confirmation operation of the first user; and

sending the asset transfer confirmation information to the blockchain node.

8. The method according to claim 7, wherein the generating the asset transfer confirmation information based on the first possessing code and the information about the second user comprises the following:

signing the first possessing code based on the first private key to obtain first signature data; and

generating the asset transfer confirmation information based on first identification information of the to-be-transferred asset, the first signature data, and obtained second public key of the second user.

9. An apparatus for asset transfer, applied to a blockchain node, comprising the following:

a receiving module, configured to receive an asset transfer request sent by a first client device, wherein the asset transfer request is sent based on an asset transfer operation of a first user, and the asset transfer request comprises asset transfer information;

a locking module, configured to invoke a first smart contract in a blockchain, and lock a to-be-transferred asset based on the first smart contract and the asset transfer information;

a sending module, configured to send asset information of the to-be-transferred asset to a designated trading platform, so that the trading platform determines, based on the asset information, a second user who trades with the first user;

an acquisition module, configured to obtain asset transfer confirmation information from the first client device; and

a transfer module, configured to perform transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information, so as to transfer the to-be-transferred asset to the second user, wherein the asset transfer confirmation information comprises information about the second user,

wherein the asset transfer information comprises first identification information of the to-be-transferred asset; and

the acquisition module is configured to: obtain a first possessing code of the first user regarding the to-be-transferred asset and a first public key corresponding to the first possessing code from the blockchain based on the first identification information, wherein the first possessing code represents that the to-be-transferred asset belongs to the first user;

encrypt the first possessing code based on the first public key to obtain a ciphertext of the first possessing code;

send the ciphertext of the first possessing code to the first client device, so that the first client device decrypts the ciphertext of the first possessing code based on a first private key corresponding to the first public key to obtain the first possessing code, and generate the asset transfer confirmation information based on the first possessing code; and

receive the asset transfer confirmation information sent by the first client device.

10. The apparatus according to claim 9, wherein

the transfer module is configured to: invoke a second smart contract in the blockchain, and generate a second possessing code based on the second smart contract; and

receive asset transfer verification information sent by the second client device, wherein the asset transfer verification information is generated based on the obtained first possessing code; and

if verification of the asset transfer verification information succeeds, send the second possessing code to the second client device to represent that the to-be-transferred asset belongs to the second user.

11. The apparatus according to claim 10, wherein the asset transfer confirmation information further comprises a second public key of the second user; the asset transfer verification information comprises the following: the first identification information,

and second signature data obtained by signing the first possessing code based on a second private key corresponding to the second public key; and

the transfer module is further configured to: after the generating a second possessing code based on the second smart contract, store the second possessing code, the second public key, and the first identification information in association with the blockchain; and

obtain the second public key stored in association with the blockchain based on the first identification information in the asset transfer verification information; and

if verification of the second signature data based on the second public key succeeds, determine that the verification of the asset transfer verification information succeeds.

12. A system for asset transfer, comprising a first client device, a blockchain, and a trading platform, wherein

the first client device is configured to: send an asset transfer request to a blockchain node connected to the blockchain in response to an asset transfer operation of a first user, wherein the asset transfer request comprises asset transfer information; and send asset transfer confirmation information to the blockchain node based on information about a second user, wherein the second user is a user who trades with the first user and is determined by the trading platform;

the blockchain node connected to the blockchain is configured to: receive the asset transfer request sent by the first client device; invoke a first smart contract in the blockchain, and lock a to-be-transferred asset based on the first smart contract and the asset transfer information; send asset information of the to-be-transferred asset to the trading platform; and obtain the asset transfer confirmation information from the first client device, and perform transfer processing on the locked to-be-transferred asset based on the asset transfer confirmation information, so as to transfer the to-be-transferred asset to the second user; and

the trading platform is configured to: receive the asset information sent by the blockchain node, publish the asset information, and determine the second user who trades with the first user,

wherein the system further comprises a second client device of the second user;

the second client device is configured to: obtain a first possessing code in response to an asset acquisition operation of the second user; generate asset transfer verification information based on the first possessing code, and send the asset transfer verification

information to the blockchain node, wherein the first possessing code represents that the to-be-transferred asset belongs to the first user;

the blockchain node is configured to: invoke a second smart contract in the blockchain, and generate a second possessing code based on the second smart contract; and

receive the asset transfer verification information sent by the second client device, and if verification of the asset transfer verification information succeeds, send the second possessing code to the second client device to represent that the to-be-transferred asset belongs to the second user; and

the second client device is configured to receive the second possessing code sent by the blockchain node.