

CLAIMS

What is claimed is:

1. A computer-implemented method for anti-counterfeiting, comprising:

receiving, by a client device, an anti-counterfeiting verification request submitted by a user for a product, wherein the anti-counterfeiting verification request comprises an anti-counterfeiting identification code;

in response to receiving the anti-counterfeiting verification request, performing, by the client device based on invoking a smart contract, operations for an anti-counterfeiting verification of the product comprising:

performing an integrity verification of anti-counterfeiting information recorded on a blockchain, wherein the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information corresponding to a plurality of participants maintaining the blockchain, wherein the plurality of types of anti-counterfeiting identification information comprise the anti-counterfeiting identification code;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a first data digest, wherein the first data digest corresponds to a first type of the plurality of types of anti-counterfeiting identification information, wherein the first data digest uniquely corresponds to a first participant of the plurality of participants, wherein the first participant of the plurality of participants corresponds to a first stage of a product life cycle of the product, and wherein the first participant maintains a first service node of a blockchain network for the blockchain;

verifying, based on a first public key corresponding to the first participant, the first data digest, wherein the first data digest is signed using a first private key corresponding to the first participant;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a second data digest, wherein the second data digest corresponds to a second type of the plurality of types of anti-counterfeiting identification information, wherein the second data digest uniquely corresponds to a second participant of the plurality of participants, wherein the second participant of the plurality of participants corresponds to a second stage of the product life cycle of the product, and wherein the second participant maintains a second service node of the blockchain network; and

verifying, based on a second public key corresponding to the second participant, the second data digest, wherein the second data digest is signed using a second private key corresponding to the second participant;

sending, by the client device, an anti-counterfeiting verification result for the product to the user indicating successful verification of the first data digest and the second data digest;

in response to the successful verification, identifying, by the client device, product information from a third-party content addressable storage device accessible to the blockchain by using a user query to the third-party content addressable storage device, wherein the user query comprises the first data digest; and

sending, by the client device, the product information to the user.

2. The computer-implemented method according to claim 1, wherein the anti-counterfeiting identification code is generated by an authority party associated with the product, and at least one type of the plurality of types of anti-counterfeiting identification information is generated by at least one participant and stored in association with the anti-counterfeiting identification code on the blockchain.

3. The computer-implemented method according to claim 2, wherein an anti-counterfeiting label is attached to the product, wherein the anti-counterfeiting label is generated based on the anti-counterfeiting identification code, the anti-counterfeiting identification code is obtained by scanning the anti-counterfeiting label, and initiating the anti-counterfeiting verification on the product comprises:

initiating a query on the blockchain based on the anti-counterfeiting identification code in response to receiving the anti-counterfeiting verification request;

receiving the at least one type of the plurality of types of anti-counterfeiting identification information on the blockchain; and

determining that the anti-counterfeiting verification of the product is successful based on determining that the at least one type of the plurality of types of anti-counterfeiting identification information is on the blockchain.

4. The computer-implemented method according to claim 3, wherein determining that the anti-counterfeiting verification of the product is successful comprises:

performing a validity verification of the at least one type of the plurality of types of anti-counterfeiting identification information generated by the at least one participant; and

determining that the anti-counterfeiting verification is successful based on the validity verification being successful.

5. The computer-implemented method according to claim 2, wherein the plurality of participants comprise a product manufacturer and a product inspector, and the at least one type of the plurality of types of anti-counterfeiting identification information comprises a data digest of an inspection report of the product.

6. The computer-implemented method according to claim 5, wherein the inspection report is stored in the third-party content addressable storage device accessible to the blockchain.

7. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, by a client device, an anti-counterfeiting verification request submitted by a user for a product, wherein the anti-counterfeiting verification request comprises an anti-counterfeiting identification code;

in response to receiving the anti-counterfeiting verification request, performing, by the client device based on invoking a smart contract, operations for an anti-counterfeiting verification of the product comprising:

performing an integrity verification of anti-counterfeiting information recorded on a blockchain, wherein the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information corresponding to a plurality of participants maintaining the blockchain, wherein the plurality of types of anti-counterfeiting identification information comprise the anti-counterfeiting identification code;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a first data digest, wherein the first data digest corresponds to a first type of the plurality of types of anti-counterfeiting identification information, wherein the first data digest uniquely

corresponds to a first participant of the plurality of participants, wherein the first participant of the plurality of participants corresponds to a first stage of a product life cycle of the product, and wherein the first participant maintains a first service node of a blockchain network for the blockchain;

verifying, based on a first public key corresponding to the first participant, the first data digest, wherein the first data digest is signed using a first private key corresponding to the first participant;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a second data digest, wherein the second data digest corresponds to a second type of the plurality of types of anti-counterfeiting identification information, wherein the second data digest uniquely corresponds to a second participant of the plurality of participants, wherein the second participant of the plurality of participants corresponds to a second stage of the product life cycle of the product, and wherein the second participant maintains a second service node of the blockchain network; and

verifying, based on a second public key corresponding to the second participant, the second data digest, wherein the second data digest is signed using a second private key corresponding to the second participant;

sending, by the client device, an anti-counterfeiting verification result for the product to the user indicating successful verification of the first data digest and the second data digest;

in response to the successful verification, identifying, by the client device, product information from a third-party content addressable storage device accessible to the blockchain by using a user query to the third-party content addressable storage device, wherein the user query comprises the first data digest; and

sending, by the client device, the product information to the user.

8. The non-transitory, computer-readable medium according to claim 7, wherein the anti-counterfeiting identification code is generated by an authority party associated with the product, and at least one type of the plurality of types of anti-counterfeiting identification information is generated by at least one participant and stored in association with the anti-counterfeiting identification code on the blockchain.

9. The non-transitory, computer-readable medium according to claim 8, wherein an anti-counterfeiting label is attached to the product, wherein the anti-counterfeiting label is generated based on the anti-counterfeiting identification code, the anti-counterfeiting identification code is obtained by scanning the anti-counterfeiting label, and initiating the anti-counterfeiting verification on the product comprises:

initiating a query on the blockchain based on the anti-counterfeiting identification code in response to receiving the anti-counterfeiting verification request;

receiving the at least one type of the plurality of types of anti-counterfeiting identification information on the blockchain; and

determining that the anti-counterfeiting verification of the product is successful based on determining that the at least one type of the plurality of types of anti-counterfeiting identification information is on the blockchain.

10. The non-transitory, computer-readable medium according to claim 9, wherein determining that the anti-counterfeiting verification of the product is successful comprises:

performing a validity verification of the at least one type of the plurality of types of anti-counterfeiting identification information generated by the at least one participant; and

determining that the anti-counterfeiting verification is successful based on the validity verification being successful.

11. The non-transitory, computer-readable medium according to claim 8, wherein the plurality of participants comprise a product manufacturer and a product inspector, and the at least one type of the plurality of types of anti-counterfeiting identification information comprises a data digest of an inspection report of the product.

12. The non-transitory, computer-readable medium according to claim 11, wherein the inspection report is stored in the third-party content addressable storage device accessible to the blockchain.

13. A computer-implemented system, comprising:
one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving, by a client device, an anti-counterfeiting verification request submitted by a user for a product, wherein the anti-counterfeiting verification request comprises an anti-counterfeiting identification code;

in response to receiving the anti-counterfeiting verification request, performing, by the client device based on invoking a smart contract, operations for an anti-counterfeiting verification of the product comprising:

performing an integrity verification of anti-counterfeiting information recorded on a blockchain, wherein the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information corresponding to a plurality of participants maintaining the blockchain, wherein the plurality of types of anti-counterfeiting identification information comprise the anti-counterfeiting identification code;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a first data digest, wherein the first data digest corresponds to a first type of the plurality of types of anti-counterfeiting identification information, wherein the first data digest uniquely corresponds to a first participant of the plurality of participants, wherein the first participant of the plurality of participants corresponds to a first stage of a product life cycle of the product, and wherein the first participant maintains a first service node of a blockchain network for the blockchain;

verifying, based on a first public key corresponding to the first participant, the first data digest, wherein the first data digest is signed using a first private key corresponding to the first participant;

obtaining, from the blockchain and based on the anti-counterfeiting identification code, a second data digest, wherein the second data digest corresponds to a second type of the plurality of types of anti-counterfeiting identification information, wherein the second data digest uniquely corresponds to a second participant of the plurality of participants, wherein the second participant of the plurality of participants corresponds to a second stage of the product

life cycle of the product, and wherein the second participant maintains a second service node of the blockchain network; and

verifying, based on a second public key corresponding to the second participant, the second data digest, wherein the second data digest is signed using a second private key corresponding to the second participant;

sending, by the client device, an anti-counterfeiting verification result for the product to the user indicating successful verification of the first data digest and the second data digest;

in response to the successful verification, identifying, by the client device, product information from a third-party content addressable storage device accessible to the blockchain by using a user query to the third-party content addressable storage device, wherein the user query comprises the first data digest; and

sending, by the client device, the product information to the user.

14. The computer-implemented system according to claim 13, wherein the anti-counterfeiting identification code is generated by an authority party associated with the product, and at least one type of the plurality of types of anti-counterfeiting identification information is generated by at least one participant and stored in association with the anti-counterfeiting identification code on the blockchain.

15. The computer-implemented system according to claim 14, wherein an anti-counterfeiting label is attached to the product, wherein the anti-counterfeiting label is generated based on the anti-counterfeiting identification code, the anti-counterfeiting identification code is obtained by scanning the anti-counterfeiting label, and initiating the anti-counterfeiting verification on the product comprises:

initiating a query on the blockchain based on the anti-counterfeiting identification code in response to receiving the anti-counterfeiting verification request;

receiving the at least one type of the plurality of types of anti-counterfeiting identification information on the blockchain; and

determining that the anti-counterfeiting verification of the product is successful based on determining that the at least one type of the plurality of types of anti-counterfeiting identification information is detected on the blockchain.

16. The computer-implemented system according to claim 15, wherein determining that the anti-counterfeiting verification of the product is successful comprises:

performing a validity verification of the at least one type of the plurality of types of anti-counterfeiting identification information generated by the at least one participant; and

determining that the anti-counterfeiting verification is successful based on the validity verification being successful.

17. The computer-implemented system according to claim 14, wherein the at least one participant comprise a product manufacturer and a product inspector, and the at least one type of the plurality of types of anti-counterfeiting identification information comprises a data digest of an inspection report of the product.

18. The computer-implemented system according to claim 17, wherein the inspection report is stored in the third-party content addressable storage device accessible to the blockchain.