

CLAIMS

What is claimed is:

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

~~receiving, by a client device, an anti-counterfeiting verification request submitted by a user for a product, wherein the blockchain stores~~ 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 ~~corresponding to a target product, and recorded on a blockchain, wherein~~ the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information ~~that correspond~~ corresponding to the target product and are stored in the blockchain by a plurality of participants maintaining the blockchain, wherein the plurality of types of anti-counterfeiting participants; ~~and identification information comprise the method comprises:~~ anti-counterfeiting identification code;

~~obtaining an anti-counterfeiting verification request submitted by a user for the target product;~~

~~initiating an anti-counterfeiting~~ 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 on the target product of the first data digest and the second data digest;

in response to the anti-counterfeiting successful verification request, wherein the anti-counterfeiting 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 at least an integrity verification on the anti-counterfeiting information the first data digest; and

returning an anti-counterfeiting verification result for sending, by the target client device, the product information to the user.

2. The computer-implemented method according to claim 1, wherein the anti-counterfeiting ~~information comprises an anti-counterfeiting~~ identification code is generated by ~~the anti-counterfeiting an~~ authority ~~for party associated with~~ the ~~target~~ product, and at least one type of the plurality of types of anti-counterfeiting identification information ~~that~~ is generated by ~~other anti-counterfeiting participants~~ 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 ~~the target product is attached with~~ 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 ~~the~~an anti-counterfeiting identification code ~~obtained by a user by scanning the anti-counterfeiting label;~~ and;

initiating 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 target product in response to the anti-counterfeiting verification request comprises~~comprising:

~~initiating performing an integrity verification of anti-counterfeiting information recorded on a query in the 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 in the anti-counterfeiting verification request in response to the anti-counterfeiting verification request, a first data digest, wherein the first data digest corresponds to detect the at least one a first type of the plurality of types of anti-counterfeiting identification information that is generated by other anti-counterfeiting, 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 stored in association with the anti-counterfeiting identification code; and wherein the first participant maintains a first service node of a blockchain network for the blockchain;~~

~~determining that the target product passes the anti-counterfeiting verification if the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants 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 ~~is detected~~on the blockchain.

~~4. The method according to claim 3, wherein before initiating a query in the blockchain based on the anti-counterfeiting identification code in the anti-counterfeiting verification request, the method further comprises:~~

~~performing a validity verification on the anti-counterfeiting identification code in the anti-counterfeiting verification request; and~~

~~further initiating a query in the blockchain based on the anti-counterfeiting identification code if the anti-counterfeiting identification code passes the validity verification.~~

~~5. The method according to claim 3, wherein determining that the target product passes the anti-counterfeiting verification if the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants and stored in association with the anti-counterfeiting identification code is detected further comprises:~~

~~further performing a validity verification on the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants if the blockchain stores the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants and stored in association with the anti-counterfeiting identification code; and~~

~~determining that the target product passes the anti-counterfeiting verification if the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants passes the validity verification.~~

~~6. The method according to claim 2, further comprising:~~

~~generating a user scanning record for the anti-counterfeiting label in response to the user scanning operation for the anti-counterfeiting label; and~~

~~publishing the generated scanning record to the blockchain for storage.~~

~~7. The method according to claim 2, wherein other anti-counterfeiting participants comprise key participants corresponding to all stages in the product life cycle of the target product; and the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants comprises product descriptions related to all stages in the product life cycle of the target product.~~

~~8. The method according to claim 7, wherein the key participants comprise a production organization and an inspection organization of the target product; and the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants comprises a data digest of production information of the target product and a data digest of an inspection report of the target product.~~

~~9. The method according to claim 8, wherein the production information of the target product and the inspection report of the target product are stored in a third-party storage system interfaced with the blockchain, wherein the third-party storage system is a content addressable storage system.~~

~~10. The method according to claim 8, wherein the blockchain is a consortium blockchain.~~

~~11. A blockchain-based anti-counterfeiting apparatus, wherein the blockchain stores anti-counterfeiting information corresponding to a target product, and the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information that correspond to the target product and are stored in the blockchain by a plurality of anti-counterfeiting participants; and the apparatus comprises:~~

~~an acquisition module, configured to obtain an anti-counterfeiting verification request submitted by a user for the target product;~~

~~a verification module, configured to initiate an anti-counterfeiting verification on the target product in response to the anti-counterfeiting verification request, wherein the anti-counterfeiting verification comprises at least an integrity verification on the anti-counterfeiting information; and~~

~~a return module, configured to return an anti-counterfeiting verification result for the target product to the user.~~

~~12. The apparatus according to claim 11, wherein the anti-counterfeiting information comprises an anti-counterfeiting identification code generated by the anti-counterfeiting authority for the target product, and at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants and stored in association with the anti-counterfeiting identification code.~~

~~13. The apparatus according to claim 12, wherein the target product is attached with an anti-counterfeiting label generated based on the anti-counterfeiting identification code; and the anti-~~

~~counterfeiting verification request comprises the anti-counterfeiting identification code obtained by a user by scanning the anti-counterfeiting label; and~~

~~the verification module is configured to:~~

~~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 initiate a query in the blockchain based on the anti-counterfeiting identification code in, the anti-counterfeiting verification request in response to identification code is obtained by scanning the anti-counterfeiting verification request, to detect the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants and stored in association with the anti-counterfeiting identification code; and label, and initiating the anti-counterfeiting verification on the product comprises:~~

~~determine that the target product passes initiating a query on the blockchain based on the anti-counterfeiting identification code in response to receiving the anti-counterfeiting verification if 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 is generated by other anti-counterfeiting participants and stored in association with the at least one type of the plurality of types of anti-counterfeiting identification code information is detected on the blockchain.~~

14

~~16. The apparatus computer-implemented system according to claim 13 15, wherein determining that the anti-counterfeiting verification module of the product is further configured to successful comprises:~~

~~before initiating a query in the blockchain based on the performing a validity verification of the at least one type of the plurality of types of anti-counterfeiting identification code in information generated by the at least one participant; and~~

~~determining that the anti-counterfeiting verification request, perform a is successful based on the validity verification on the 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 code in the anti-counterfeiting verification request; and further initiate a query in the blockchain based on the anti-counterfeiting identification code if the anti-counterfeiting identification code passes the validity verification information comprises a data digest of an inspection report of the product.

1815. The apparatuscomputer-implemented system according to claim 1317, wherein the inspection report is stored in the third-party content addressable storage device accessible to the blockchain. verification module is further configured to:

further perform a validity verification on the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants if the blockchain stores the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants and stored in association with the anti-counterfeiting identification code; and determine that the target product passes the anti-counterfeiting verification if the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants passes the validity verification.

16. The apparatus according to claim 12, further comprising:

a generation module, configured to: generate a user scanning record for the anti-counterfeiting label in response to the user scanning operation for the anti-counterfeiting label; and publish the generated scanning record to the blockchain for storage.

17. The apparatus according to claim 12, wherein other anti-counterfeiting participants comprise key participants corresponding to all stages in the product life cycle of the target product; and the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants comprises product descriptions related to all stages in the product life cycle of the target product.

18. The apparatus according to claim 17, wherein the key participants comprise a production organization and an inspection organization of the target product; and the at least one type of anti-counterfeiting identification information that is generated by other anti-counterfeiting participants comprises a data digest of production information of the target product and a data digest of an inspection report of the target product.

~~19. The apparatus according to claim 18, wherein the production information of the target product and the inspection report of the target product are stored in a third-party storage system interfaced with the blockchain, wherein the third-party storage system is a content addressable storage system.~~

~~20. The apparatus according to claim 18, wherein the blockchain is a consortium blockchain.~~

~~21. An electronic device, comprising:~~

~~a processor; and~~

~~a memory, configured to store machine-executable instructions; wherein~~

~~by reading and executing the machine-executable instructions that are stored in the memory and that correspond to an anti-counterfeiting logic for blockchain-based anti-counterfeiting, the processor is enabled to:~~

~~obtain an anti-counterfeiting verification request submitted by a user for the target product, wherein the blockchain stores anti-counterfeiting information corresponding to a target product, and the anti-counterfeiting information comprises a plurality of types of anti-counterfeiting identification information that correspond to the target product and are stored in the blockchain by a plurality of anti-counterfeiting participants.~~

~~initiate an anti-counterfeiting verification on the target product in response to the anti-counterfeiting verification request, wherein the anti-counterfeiting verification comprises at least an integrity verification on the anti-counterfeiting information; and~~

~~return an anti-counterfeiting verification result for the target product to the user.~~