CLAIMS

What is claimed is

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

receiving a first verification code corresponding to a product sent by a user, wherein the product is an electronic product and the first verification code is displayed after the product is powered on;

performing verification on the product based on the first verification code, comprising:

returning traceability information corresponding to the first verification code to the user based on the first verification code by:

obtaining the traceability information corresponding to the first verification code from traceability information stored in a blockchain; and

returning the obtained traceability information to the user; and

receiving a verification result returned by the user based on the traceability information; and

returning permission information to the user if the verification succeeds, so that the user uses at least some of functions of the product by using the permission information.

2. The method according to claim 1, wherein the method further comprises receiving a second verification code corresponding to the product; and

performing verification on the product further comprises:

determining, based on the second verification code sent after the verification result returned by the user based on the traceability information is successful and pre-stored target verification codes, whether the second verification code is in the target verification codes; and

if the second verification code is in the target verification codes, determining that the verification succeeds, updating a recorded number of times verification has been performed on the second verification code, and returning the updated recorded number of verification times to the user; or

determining that the verification fails if the second verification code is not

in the target verification codes.

3. The method according to claim 2, wherein the first verification code is a plain code being a verification code not covered with a coating, and the second verification code is a secret code being a verification code covered with a coating.

4. The method according to claim 1, wherein

the first verification code is located on the product; and/or

the first verification code is located on a package of the product.

5. The method according to claim 4, wherein the first verification code is located on the package of the product, the package comprising a combination lock on the package, and wherein the combination lock is used to keep the package in a closed state, and the permission information is a password used to open the combination lock.

6. The method according to claim 4, wherein the permission information is an activation code, and wherein the activation code is used to activate the at least some of the functions of the product after the user enters the activation code on the product.

7. The method according to claim 4, wherein the returning permission information to the user comprises:

determining an identifier corresponding to the product based on the first verification code; and

communicating with the product based on the identifier, and sending the permission information to the product, wherein the permission information is used to activate the at least some of the functions of the product.

8. The method according to claim 1, wherein the method further comprises:

refusing to return the permission information to the user if the verification fails.

9. A product anti-counterfeiting verification apparatus comprising a plurality of modules for performing the method according to any one of claims 1 to 8, the plurality of modules comprising a receiving module, a verification module, and a first processing module.

10. An anti-counterfeiting verification device, comprising one or more processors and one or more memories, wherein the memory stores a program, and the program is executed by the one or more processors to perform the method according to any one of claims 1 to 8.