

权利要求书

- 1、一种基于区块链的产品信息加密方法，所述方法应用于生产方，包括：
根据产品的唯一暗码，单向生成生产加密密钥；
根据所述生产加密密钥，对所述产品的生产信息进行加密，生成生产信息加密数据；
5 根据所述生产加密密钥，生成生产信息查询标识；
将生产信息集合写入区块链，所述生产信息集合包含生产信息查询标识、以及生产信息加密数据。
- 2、如权利要求 1 所述的方法，根据产品的唯一暗码，单向生成生产加密密钥，具体包括：
10 接收生产方在生产所述产品时生成的生产随机数；
根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥。
- 3、如权利要求 2 所述的方法，所述方法还包括：
根据所述唯一暗码，单向生成随机数查询标识；
在可信存储库中为所述产品创建唯一标识；
15 将所述随机数查询标识以及所述生产随机数发送至所述可信存储库，并均与所述唯一标识关联。
- 4、如权利要求 1 所述的方法，根据所述生产加密密钥，生成生产信息查询标识，具体包括：
根据所述生产加密密钥，单向生成第 1 流通密钥，再根据所述第 1 流通密钥，单向
20 生成生产信息查询标识；则
将生产信息集合写入区块链，具体包括：
根据第 1 公钥，对第 1 流通密钥进行加密，生成第 1 流通密钥加密数据，所述第 1 公钥为第 1 次序流通方的流通公钥；
根据第 1 公钥，单向生成第 1 流通密钥查询标识；
25 将生产信息集合写入区块链，所述生产信息集合包含所述第 1 接收密钥查询标识、生产信息查询标识、第 1 接收密钥加密数据以及生产信息加密数据。
- 5、如权利要求 4 所述的方法，根据第 1 公钥，对第 1 流通密钥进行加密，生成第 1 流通密钥加密数据，具体包括：
根据第 1 公钥，对产品的公开明码与第 1 流通密钥的组合进行加密，生成第 1 流通
30 密钥加密数据。
- 6、如权利要求 4 所述的方法，将生产信息集合写入区块链，具体包括：

根据生产私钥, 对所述生产信息集合进行签名, 所述生产私钥为生产方在生产所述产品时生成的私钥;

将签名后的生产信息集合写入区块链。

7、一种基于区块链的产品信息加密方法, 所述方法应用于流通方, 包括:

5 根据第 n 公钥, 单向生成第 n 流通密钥查询标识;

根据第 n 流通密钥查询标识, 从区块链中读取第 n 接收密钥加密数据;

根据第 n 私钥, 对所述第 n 流通密钥加密数据进行解密, 得到第 n 流通密钥;

根据所述第 n 流通密钥, 单向生成第 n 加密密钥;

根据第 n 加密密钥, 对第 n 流通信息进行加密, 生成第 n 流通信息加密数据;

10 根据所述第 n 加密密钥, 生成第 n 流通信息查询标识;

将第 n 信息集合写入区块链, 所述第 n 信息集合包含第 n 流通信息查询标识以及第 n 流通信息加密数据;

其中, n 为大于 0 的自然数。

8、如权利要求 7 所述的方法, 根据所述第 n 流通密钥, 单向生成第 n 加密密钥,

15 具体包括:

接收第 n 次序流通方在接收产品时生成的第 n 随机数;

根据所述第 n 流通密钥与所述第 n 随机数的组合, 单向生成第 n 加密密钥。

9、如权利要求 8 所述的方法, 所述方法还包括:

将所述第 n 随机数发送至可信存储库, 并与所述产品的唯一标识关联。

20 10、如权利要求 9 所述的方法, 根据所述第 n 加密密钥, 生成第 n 流通信息查询标识, 具体包括:

根据所述第 n 加密密钥, 单向生成第 $n+1$ 流通密钥, 再根据第 $n+1$ 流通密钥, 单向生成第 n 流通信息查询标识; 则

将第 n 信息集合写入区块链, 具体包括:

25 根据第 $n+1$ 公钥, 对第 $n+1$ 流通密钥进行加密, 生成第 $n+1$ 流通密钥加密数据, 所述第 $n+1$ 公钥为第 $n+1$ 次序流通方的流通公钥;

根据第 $n+1$ 公钥, 单向生成第 $n+1$ 流通密钥查询标识;

将第 n 信息集合写入区块链, 所述第 n 信息集合包含所述第 $n+1$ 接收密钥查询标识、第 n 流通信息查询标识、第 $n+1$ 接收密钥加密数据以及第 n 流通信息加密数据。

30 11、如权利要求 10 所述的方法, 根据第 $n+1$ 公钥, 对第 $n+1$ 流通密钥进行加密, 生成第 $n+1$ 流通密钥加密数据, 具体包括:

根据第 $n+1$ 公钥，对产品的公开明码与第 $n+1$ 流通密钥的组合进行加密，生成第 $n+1$ 流通密钥加密数据。

12、如权利要求 10 所述的方法，将第 n 信息集合写入区块链，具体包括：

根据第 n 私钥，对所述第 n 信息集合进行签名；

5 将签名后的第 n 信息集合写入区块链。

13、如权利要求 7 所述的方法，根据第 n 私钥，对所述第 n 流通密钥加密数据进行解密之前，所述方法还包括：

根据生产公钥，对签名后的生产信息集合进行签名验证；或

根据第 n 公钥，对签名后的第 n 信息集合进行签名验证。

10 14、一种基于区块链的产品信息解密方法，所述方法应用于购买方，包括：

根据产品的唯一暗码，单向生成生产加密密钥；

根据所述生产加密密钥，生成生产信息查询标识；

根据所述生产信息查询标识，从区块链中读取所述产品的生产信息加密数据；

根据所述生产加密密钥，对所述生产信息加密数据进行解密，获得生产信息。

15 15、如权利要求 14 所述的方法，所述方法还包括：

根据所述生产加密密钥，单向生成第 1 流通密钥，根据所述第 n 流通密钥，单向生成第 n 加密密钥，根据第 n 加密密钥，单向生成第 $n+1$ 流通密钥；

根据所述第 n 流通信息查询标识，从区块链中读取所述产品的第 n 流通信息加密数据；

20 根据所述第 n 加密密钥，对所述第 n 流通信息加密数据进行解密，获得第 n 流通信息；

其中， n 为大于 0 的自然数。

16、如权利要求 14 所述的方法，根据产品的唯一暗码，单向生成生产加密密钥，具体包括：

25 根据产品的唯一暗码，单向生成随机数查询标识；

从可信存储库中获取与所述随机数查询标识对应的生产随机数；

根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥。

17、如权利要求 15 所述的方法，根据所述第 n 流通密钥，单向生成第 n 加密密钥，具体包括：

30 从可信存储库中获取与所述随机数查询密钥对应的第 n 随机数；

根据所述第 n 流通密钥与所述第 n 随机数的组合，单向生成第 n 加密密钥，

其中， n 为大于 0 的自然数。

18、如权利要求 17 所述的方法，从区块链中读取所述产品的生产信息加密数据，具体包括：

根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥，再单向生成第 1 流通密钥，再单向生成生产信息查询标识；

根据所述生产信息查询标识，从区块链中读取生产信息集合中的生产信息加密数据；则

从区块链中读取所述产品的第 n 流通信息加密数据，具体包括：

根据所述第 n 流通密钥与所述第 n 随机数的组合，单向生成第 n 加密密钥，再单向生成第 $n+1$ 流通密钥，再单向生成第 n 流通信息查询标识；

根据所述第 n 流通信息查询标识，从区块链中读取第 n 信息集合中的第 n 流通信息加密数据。

19、一种基于区块链的产品信息加密装置，所述装置应用于生产方，包括：密钥生成单元、数据生成单元、标识生成单元、数据写入单元，其中，

15 所述密钥生成单元，根据产品的唯一暗码，单向生成生产加密密钥；

所述数据生成单元，根据所述生产加密密钥，对所述产品的生产信息进行加密，生成生产信息加密数据；

所述标识生成单元，根据所述生产加密密钥，生成生产信息查询标识；

20 所述数据传输单元，将生产信息集合写入区块链，所述生产信息集合包含生产信息查询标识、以及生产信息加密数据。

20、如权利要求 19 所述的装置，所述密钥生成单元，

接收生产方在生产所述产品时生成的生产随机数；

根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥。

21、如权利要求 20 所述的装置，

25 所述标识生成单元，根据所述唯一暗码，单向生成随机数查询标识；

所述数据传输单元，

在可信存储库中为所述产品创建唯一标识；

将所述随机数查询标识以及所述生产随机数发送至所述可信存储库，并均与所述唯一标识关联。

30 22、如权利要求 19 所述的装置，所述标识生成单元，

根据所述生产加密密钥，单向生成第 1 流通密钥，再根据所述第 1 流通密钥，单向

生成生产信息查询标识；则

所述数据生成单元，

根据第 1 公钥，对第 1 流通密钥进行加密，生成第 1 流通密钥加密数据，所述第 1 公钥为第 1 次序流通方的流通公钥；

5 根据第 1 公钥，单向生成第 1 流通密钥查询标识；

所述数据传输单元，

将生产信息集合写入区块链，所述生产信息集合包含所述第 1 接收密钥查询标识、生产信息查询标识、第 1 接收密钥加密数据以及生产信息加密数据。

23、如权利要求 22 所述的装置，所述数据生成单元，

10 根据第 1 公钥，对产品的公开明码与第 1 流通密钥的组合进行加密，生成第 1 流通密钥加密数据。

24、如权利要求 22 所述的装置，所述数据传输单元，

根据生产私钥，对所述生产信息集合进行签名，所述生产私钥为生产方在生产所述产品时生成的私钥；

15 将签名后的生产信息集合写入区块链。

25、一种基于区块链的产品信息加密装置，所述装置应用于流通方，包括：标识生成单元、数据读取单元、数据解析单元、密钥生成单元、数据加密单元、数据传输单元，其中，

所述标识生成单元，根据第 n 公钥，单向生成第 n 流通密钥查询标识；

20 所述数据读取单元，根据第 n 流通密钥查询标识，从区块链中读取第 n 接收密钥加密数据；

所述数据解析单元，根据第 n 私钥，对所述第 n 流通密钥加密数据进行解密，得到第 n 流通密钥；

所述密钥生成单元，根据所述第 n 流通密钥，单向生成第 n 加密密钥；

25 所述数据加密单元，根据第 n 加密密钥，对第 n 流通信息进行加密，生成第 n 流通信息加密数据；

根据所述第 n 加密密钥，生成第 n 流通信息查询标识；

所述数据传输单元，将第 n 信息集合写入区块链，所述第 n 信息集合包含第 n 流通信息查询标识以及第 n 流通信息加密数据；

30 其中，n 为大于 0 的自然数。

26、如权利要求 25 所述的装置，所述密钥生成单元，

- 接收第 n 次序流通方在接收产品时生成的第 n 随机数；
根据所述第 n 流通密钥与所述第 n 随机数的组合，单向生成第 n 加密密钥。
- 27、如权利要求 26 所述的装置，所述数据传输单元，
将所述第 n 随机数发送至可信存储库，并与所述产品的唯一标识关联。
- 5 28、如权利要求 27 所述的装置，所述标识生成单元，
根据所述第 n 加密密钥，单向生成第 $n+1$ 流通密钥，再根据第 $n+1$ 流通密钥，单向生成第 n 流通信息查询标识；则
所述密钥生成单元，根据第 $n+1$ 公钥，对第 $n+1$ 流通密钥进行加密，生成第 $n+1$ 流通密钥加密数据，所述第 $n+1$ 公钥为第 $n+1$ 次序流通方的流通公钥；
- 10 所述标识生成单元，根据第 $n+1$ 公钥，单向生成第 $n+1$ 流通密钥查询标识；
所述数据传输单元，将第 n 信息集合写入区块链，所述第 n 信息集合包含所述第 $n+1$ 接收密钥查询标识、第 n 流通信息查询标识、第 $n+1$ 接收密钥加密数据以及第 n 流通信息加密数据。
- 29、如权利要求 28 所述的装置，所述数据加密单元，
- 15 根据第 $n+1$ 公钥，对产品的公开明码与第 $n+1$ 流通密钥的组合进行加密，生成第 $n+1$ 流通密钥加密数据。
- 30、如权利要求 28 所述的装置，所述数据传输单元，
根据第 n 私钥，对所述第 n 信息集合进行签名；
将签名后的第 n 信息集合写入区块链。
- 20 31、如权利要求 25 所述的装置，所述数据解析单元，根据第 n 私钥，对所述第 n 流通密钥加密数据进行解密之前，
根据生产公钥，对签名后的生产信息集合进行签名验证；或
根据第 n 公钥，对签名后的第 n 信息集合进行签名验证。
- 32、一种基于区块链的产品信息解密装置，所述装置应用于购买方，包括：密钥生成单元、标识生成单元、数据读取单元、以及数据解析单元，其中，
- 25 所述密钥生成单元，根据产品的唯一暗码，单向生成生产加密密钥；
所述标识生成单元，根据所述生产加密密钥，生成生产信息查询标识；
所述数据读取单元，根据所述生产信息查询标识，从区块链中读取所述产品的生产信息加密数据；
- 30 所述数据解析单元，根据所述生产加密密钥，对所述生产信息加密数据进行解密，获得生产信息。

33、如权利要求 32 所述的装置，

所述密钥生成单元，根据所述生产加密密钥，单向生成第 1 流通密钥，根据所述第 n 流通密钥，单向生成第 n 加密密钥，根据第 n 加密密钥，单向生成第 n+1 流通密钥；

所述数据读取单元，根据所述第 n 流通信息查询标识，从区块链中读取所述产品的第 n 流通信息加密数据；

所述数据解析单元，根据所述第 n 加密密钥，对所述第 n 流通信息加密数据进行解密，获得第 n 流通信息；

其中，n 为大于 0 的自然数。

34、如权利要求 32 所述的装置，

所述密钥生成单元，根据产品的唯一暗码，单向生成随机数查询标识；

所述数据读取单元，从可信存储库中获取与所述随机数查询标识对应的生产随机数；

所述密钥生成单元，根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥。

35、如权利要求 33 所述的装置，

所述数据读取单元，从可信存储库中获取与所述随机数查询密钥对应的第 n 随机数；

所述密钥生成单元，根据所述第 n 流通密钥与所述第 n 随机数的组合，单向生成第 n 加密密钥，

其中，n 为大于 0 的自然数。

36、如权利要求 35 所述的装置，

所述密钥生成单元，根据所述唯一暗码与所述生产随机数的组合，单向生成生产加密密钥，再单向生成第 1 流通密钥，再单向生成生产信息查询标识；

所述数据读取单元，根据所述生产信息查询标识，从区块链中读取生产信息集合中的生产信息加密数据；则

所述密钥生成单元，根据所述第 n 流通密钥与所述第 n 随机数的组合，单向生成第 n 加密密钥，再单向生成第 n+1 流通密钥，再单向生成第 n 流通信息查询标识；

所述数据读取单元，根据所述第 n 流通信息查询标识，从区块链中读取第 n 信息集合中的第 n 流通信息加密数据。

37、一种电子设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理

器执行以下操作:

根据产品的唯一暗码, 单向生成生产加密密钥;

根据所述生产加密密钥, 对所述产品的生产信息进行加密, 生成生产信息加密数据;

根据所述生产加密密钥, 生成生产信息查询标识;

- 5 将生产信息集合写入区块链, 所述生产信息集合包含生产信息查询标识、以及生产信息加密数据。

38、一种电子设备, 包括:

处理器; 以及

被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理

- 10 器执行以下操作:

根据第 n 公钥, 单向生成第 n 流通密钥查询标识;

根据第 n 流通密钥查询标识, 从区块链中读取第 n 接收密钥加密数据;

根据第 n 私钥, 对所述第 n 流通密钥加密数据进行解密, 得到第 n 流通密钥;

根据所述第 n 流通密钥, 单向生成第 n 加密密钥;

- 15 根据第 n 加密密钥, 对第 n 流通信息进行加密, 生成第 n 流通信息加密数据;

根据所述第 n 加密密钥, 生成第 n 流通信息查询标识;

将第 n 信息集合写入区块链, 所述第 n 信息集合包含第 n 流通信息查询标识以及第 n 流通信息加密数据;

其中, n 为大于 0 的自然数。

- 20 39、一种电子设备, 包括:

处理器; 以及

被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理

器执行以下操作:

根据产品的唯一暗码, 单向生成生产加密密钥;

- 25 根据所述生产加密密钥, 生成生产信息查询标识;

根据所述生产信息查询标识, 从区块链中读取所述产品的生产信息加密数据;

根据所述生产加密密钥, 对所述生产信息加密数据进行解密, 获得生产信息。

40、一种计算机可读存储介质, 所述计算机可读存储介质存储一个或多个程序, 所述一个或多个程序当被包括多个应用程序的电子设备执行时, 使得所述电子设备执行以

- 30 下操作:

根据产品的唯一暗码, 单向生成生产加密密钥;

根据所述生产加密密钥,对所述产品的生产信息进行加密,生成生产信息加密数据;

根据所述生产加密密钥,生成生产信息查询标识;

将生产信息集合写入区块链,所述生产信息集合包含生产信息查询标识、以及生产信息加密数据。

- 5 41、一种计算机可读存储介质,所述计算机可读存储介质存储一个或多个程序,所述一个或多个程序当被包括多个应用程序的电子设备执行时,使得所述电子设备执行以下操作:

根据第 n 公钥,单向生成第 n 流通密钥查询标识;

根据第 n 流通密钥查询标识,从区块链中读取第 n 接收密钥加密数据;

- 10 根据第 n 私钥,对所述第 n 流通密钥加密数据进行解密,得到第 n 流通密钥;

根据所述第 n 流通密钥,单向生成第 n 加密密钥;

根据第 n 加密密钥,对第 n 流通信息进行加密,生成第 n 流通信息加密数据;

根据所述第 n 加密密钥,生成第 n 流通信息查询标识;

将第 n 信息集合写入区块链,所述第 n 信息集合包含第 n 流通信息查询标识以及第

- 15 n 流通信息加密数据;

其中, n 为大于 0 的自然数。

42、一种计算机可读存储介质,所述计算机可读存储介质存储一个或多个程序,所述一个或多个程序当被包括多个应用程序的电子设备执行时,使得所述电子设备执行以下操作:

- 20 根据产品的唯一暗码,单向生成生产加密密钥;

根据所述生产加密密钥,生成生产信息查询标识;

根据所述生产信息查询标识,从区块链中读取所述产品的生产信息加密数据;

根据所述生产加密密钥,对所述生产信息加密数据进行解密,获得生产信息。