(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111865586 A
(43)申请公布日 2020.10.30

(21)申请号 202010764583.0
(22)申请日 2017.11.23
(62)分案原申请数据
201711183121.4 2017.11.23
(71)申请人 创新先进技术有限公司
地址 英属开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 王虎森
(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 徐晨影 许振新
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/14(2006.01)
G06Q 30/00(2012.01)
G06F 21/60(2013.01)

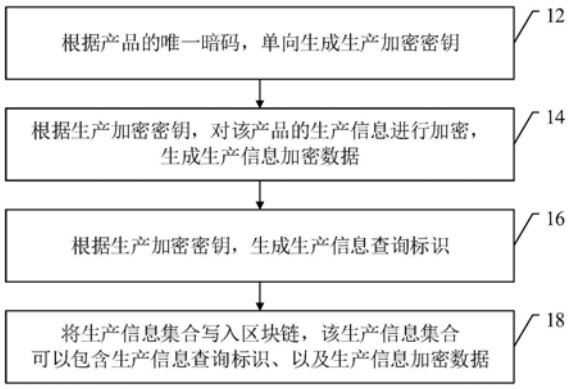
权利要求书2页 说明书20页 附图12页

(54)发明名称

一种产品信息的加密方法及装置

(57)摘要

本说明书公开一种基于区块链的产品信息加密、解密方法及装置，可以由生产方以产品唯一暗码为基础，对生产信息进行加密，当存在流通方时可以根据唯一暗码单向生成流通密钥，而流通方可以继续根据流通密钥生成流通信息加密密钥，对流通信息进行加密，根据流通信息加密密钥再生成下一个流通密钥。也就是以链式连环单向生成密钥的方式，对产品信息进行加密，利用产品唯一暗码除生产方和购买方以外无法获知的特性，以及区块链不可篡改不可伪造的特性，对生产信息进行加密和存储，使得生产信息有很高的保密性。



CN 111865586 A

1.一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:

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流通密钥加密数据;

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;

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。

2.如权利要求1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:

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。

3.如权利要求2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。

4.如权利要求3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:

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流通密钥查询标识、第n流通信息查询标识、第n+1流通密钥加密数据以及第n流通信息加密数据。

5.如权利要求4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。

6.如权利要求4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;

将签名后的第n信息集合写入区块链。

7.如权利要求1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。

8.一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;

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流通密钥加密数据；

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；

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；

其中，n为大于0的自然数。

9.一种电子设备，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流通密钥加密数据

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；

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。

10.一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流通密钥加密数据

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；

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。

一种产品信息的加密方法及装置

[0001] 本申请是申请号为"201711183121.4"、申请日为"2017年11月23日"、申请名称为"一种产品信息的加密方法、解密方法及装置"的专利申请的分案申请。

技术领域

[0002] 本说明书涉及计算机技术领域，尤其涉及一种产品信息的加密方法及装置、以及一种产品信息的解密方法及装置。

背景技术

[0003] 目前，随着各行各业的发展，包括线上线下各种产品的交易、流通已经非常普遍，这里所说的产品可以是实体产品，比如工业制品、工艺品等；也可以是计算机产品，比如软件、网络存储空间等。

[0004] 对于一个产品，通常存在一个生产方和一个购买方，即生产产品的一方和购买产品的一方，且多数情况下还存在流通方，即流通产品的一方或多方。比如，对于一批饮料产品，可以有一个生产方(饮料的生产厂商)，以及一个购买方(消费者)，或者在生产方和购买方之间存在至少一个流通方(代理商、零售商等)，在整个流通的过程中，除购买方的每一方均会为产品生成一个产品信息(生产方可以生成生产信息，而流通方可以生成流通信息)，这些信息串联到一起，就可以是由生产方到购买方的全过程，即的产品信息就是对产品进行溯源的依据。

[0005] 而通常情况下，需要对各产品信息进行保密，即每一方的产品信息只能由生产方和购买方获取到，而需要对流通方或窃取者保密。所以需要提供一种为各方生成的产品信息进行保密的方案，并确保购买方能够对产品进行溯源。

发明内容

[0006] 本说明书实施例提供一种基于区块链的产品信息加密、解密方法，用于在产品流通过程中，对产品信息进行保密，且确保购买方能够获得产品信息。

[0007] 本说明书实施例提供一种基于区块链的产品信息加密、解密装置，用于在产品流通过程中，对产品信息进行保密，且确保购买方能够获得产品信息。

[0008] 为解决上述技术问题，本说明书实施例是这样实现的：

[0009] 本说明书实施例采用下述技术方案：

[0010] 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：

[0011] 根据产品的唯一暗码，单向生成生产加密密钥；

[0012] 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；

[0013] 根据所述生产加密密钥，生成生产信息查询标识；

[0014] 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。

[0015] 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：

[0016] 根据第n公钥，单向生成第n流通密钥查询标识；

[0017] 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；

[0018] 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；

[0019] 根据所述第n流通密钥，单向生成第n加密密钥；

[0020] 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；

[0021] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0022] 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；

[0023] 其中，n为大于0的自然数。

[0024] 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：

[0025] 根据产品的唯一暗码，单向生成生产加密密钥；

[0026] 根据所述生产加密密钥，生成生产信息查询标识；

[0027] 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；

[0028] 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。

[0029] 一种基于区块链的产品信息加密装置，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，

[0030] 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；

[0031] 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；

[0032] 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；

[0033] 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。

[0034] 一种基于区块链的产品信息加密装置，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，

[0035] 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；

[0036] 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；

[0037] 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；

[0038] 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；

[0039] 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；

[0040] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0041] 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；

[0042] 其中，n为大于0的自然数。

[0043] 一种基于区块链的产品信息解密装置，所述方法应用于购买方，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，

[0044] 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；

[0045] 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；

[0046] 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；

[0047] 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。

[0048] 一种电子设备，包括：

[0049] 处理器；以及

[0050] 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：

[0051] 根据产品的唯一暗码，单向生成生产加密密钥；

[0052] 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；

[0053] 根据所述生产加密密钥，生成生产信息查询标识；

[0054] 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。

[0055] 一种电子设备，包括：

[0056] 处理器；以及

[0057] 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：

[0058] 根据第n公钥，单向生成第n流通密钥查询标识；

[0059] 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；

[0060] 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；

[0061] 根据所述第n流通密钥，单向生成第n加密密钥；

[0062] 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；

[0063] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0064] 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；

[0065] 其中，n为大于0的自然数。

[0066] 一种电子设备，包括：

[0067] 处理器；以及

[0068] 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：

[0069] 根据产品的唯一暗码，单向生成生产加密密钥；

[0070] 根据所述生产加密密钥，生成生产信息查询标识；

[0071] 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；

[0072] 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。

[0073] 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：

[0074] 根据产品的唯一暗码，单向生成生产加密密钥；

[0075] 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；

[0076] 根据所述生产加密密钥，生成生产信息查询标识；

[0077] 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。

[0078] 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：

[0079] 根据第n公钥，单向生成第n流通密钥查询标识；

[0080] 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；

[0081] 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；

[0082] 根据所述第n流通密钥，单向生成第n加密密钥；

[0083] 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；

[0084] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0085] 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；

[0086] 其中，n为大于0的自然数。

[0087] 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：

[0088] 根据产品的唯一暗码，单向生成生产加密密钥；

[0089] 根据所述生产加密密钥，生成生产信息查询标识；

[0090] 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；

[0091] 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。

[0092] 由以上实施例提供的技术方案可见，本说明书提供的实施例生产方可以利用产品的唯一暗码，单向生成生产加密密钥，再根据生产加密密钥，对产品的生产信息进行加密，生成生产信息加密数据，根据生产加密密钥，生成生产信息查询标识，将包含生产信息查询标识、以及生产信息加密数据的生产信息集合写入区块链。购买方可以利用产品的唯一暗码，单向生成生产加密密钥，再根据生产加密密钥生成生产信息查询标识，对从区块链读取到的生产信息加密数据进行解密，获得生产信息。而在产品流通过程中出现流通方的情况，可以根据生产加密密钥，单向生成用于流通至第1次序流通方的第1流通密钥，再单向生成生产信息查询标识，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，根据第1公钥，单向生成第1流通密钥查询标识，将包含所述第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生产信息集合写入区块链。利用产品唯一暗码在购买方破坏产品完整性后才能获知的特性，以及区块链不可篡改不可伪造的特性，对生产信息进行加密解密，使得生产信息有很高的保密性，且将生产信息写入区块链，使得下个流通方能够通过链式连续加密的方式，将产品信息写入区块链。

附图说明

[0093] 为了更清楚地说明本说明书实施例或现有的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0094] 图1为实施例1提供的基于区块链的产品信息加密方法的流程示意图；

[0095] 图2为实施例1提供的基于区块链的产品信息加密方法的示意图；

[0096] 图3为实施例1提供的基于区块链的产品信息加密方法的示意图；

[0097] 图4为实施例2提供的基于区块链的产品信息解密方法的流程示意图；

[0098] 图5为实施例2提供的基于区块链的产品信息解密方法的示意图；

[0099] 图6为实施例2提供的基于区块链的产品信息解密方法的示意图；

[0100] 图7为实施例3提供的基于区块链的产品信息加密方法的流程示意图；

[0101] 图8为实施例3提供的基于区块链的产品信息加密方法的示意图；

[0102] 图9为实施例4提供的基于区块链的产品信息加密方法的流程示意图；

[0103] 图10为实施例4提供的基于区块链的产品信息加密方法的示意图；

[0104] 图11为实施例5提供的基于区块链的产品信息解密方法的流程示意图；

[0105] 图12为实施例5提供的基于区块链的产品信息解密方法的示意图；

[0106] 图13为实施例6提供的基于区块链的产品信息加密装置的结构示意图；

[0107] 图14为实施例7提供的基于区块链的产品信息加密装置的结构示意图；

[0108] 图15为实施例8提供的基于区块链的产品信息解密装置的结构示意图；

[0109] 图16为本说明书实施例提供的一种电子设备的结构示意图。

具体实施方式

[0110] 为使本说明书的目的、技术方案和优点更加清楚，下面将结合具体实施例及相应的附图对本说明书的技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的其他实施例，都属于本说明书保护的范围。

[0111] 以下结合附图，详细说明本说明书中各实施例提供的技术方案。

[0112] 实施例1

[0113] 如前所述，在产品的整个流通过程中，除购买方的任一方均会为产品生成一个产品信息，比如生产方(产品厂商)可以在生产过程中，为产品生成一个生产信息(可以包含该产品、厂商等特征信息)，而流通方可以在接收到产品后，生成一个流通信息(可以包含流通方的时间、价格、地址等特征信息)，这些信息串联到一起，可以是对产品进行溯源的依据，溯源可以是指跟踪特定产品从生产、经过流通等中间环节，到购买方的整个流通过程。而对于非购买方和生产方而言(流通方和窃取者)，都需要对产品信息进行保密，并确保购买方可以查看产品信息，所以需要提供一种为各方生成的产品信息进行保密的方案，并确保购买方能够对产品进行溯源。

[0114] 本说明书提供一种基于区块链的产品信息加密、解密方法，用于在产品流通过程中，对产品信息进行保密，且确保购买方能够获得产品信息。该方法可以适用于流通过程

中，存在生产方和购买方的情况，也可以适用于流通过程中，存在购买方、一个或多个流通方，以及购买方的情况。

[0115] 而本实施例1以流通过程中，可以是存在生产方和购买方的情况为例，介绍产品信息的加密方法。具体地，先介绍一种基于区块链的产品信息加密方法，应用于存在生产方和购买方中的生产方。该方法的流程如图1所示，包括下述步骤：

[0116] 步骤12：根据产品的唯一暗码，单向生成生产加密密钥；

[0117] 产品的唯一暗码，可以是指暗藏在产品内部的识别码，只有购买方在破坏产品完整性，开始使用产品后，才能够找到唯一暗码，产品唯一暗码的意义在于除了生产方和购买方以外，均无法获取产品的唯一暗码。比如，对于瓶装饮料而言，只有开启瓶盖，即破坏了产品的完整后，才可以从瓶盖内侧找到产品的唯一暗码。所以作为生产方，可以以唯一暗码作为依据，对产品信息进行加密，以致只有购买方在破坏产品完整性开始使用后，才可以找到唯一暗码。

[0118] 具体地，可以通过单向函数的方式，对产品的唯一暗码生成生产加密密钥，其中，单向函数可以是指对于任何输入计算输出，但已知输出却无法确定输入，也可以通过单向散列函数的方式，对产品的唯一暗码生成生产加密密钥，单向散列函数，又称单向Hash函数、杂凑函数，就是把任意长的输入消息串变化成固定长的输出串且由输出串难以得到输入串的一种函数。所以，在无法获取到唯一暗码的情况下，无法确定出生产加密密钥。这里唯一暗码可以由pincode表示，而单向函数可以由hash表示，则根据产品唯一暗码单向生成的生产加密密钥可以由$key_{生产加密}$表示，则可以有$key_{生产加密}$=hash(pincode)的表达方式。

[0119] 在实际应用中，为了进一步加强的$key_{生产加密}$的安全性，在一种实施方式中，本步骤可以包括：接收生产方在生产该产品时生成的生产随机数；根据唯一暗码与生产随机数的组合，单向生成生产加密密钥。具体地，生产方在生产产品时可以生成一个生产随机数，该生产随机数可以用于对pincode进行单向计算，生成随机数可以用$nonce_{生产}$表示。唯一暗码与生产随机数的组合可以以(pincode||$nonce_{生产}$)表示，也就是可以有$key_{生产加密}$=hash(pincode||$nonce_{生产}$)，需要说明的是，这里所指的pincode与$nonce_{生产}$的组合，可以是简单的字符串先后串联，即pincode字符串在前、$nonce_{生产}$字符串在后，也可以是预设的字符串穿插串联的方式，比如pincode可以有6位字符串，而$nonce_{生产}$可以有4位字符串，预设的字符串穿插串联的方式可以是pincode前3位+$nonce_{生产}$前2位+pincode后3位+$nonce_{生产}$后2位，等。

[0120] 步骤14：根据生产加密密钥，对该产品的生产信息进行加密，生成生产信息加密数据。

[0121] 由于在前一步骤中，生成的生产加密密钥$key_{生产加密}$需要pincode的支持，而除购买方以外均无法得到pincode，所以本步骤就可以根据$key_{生产加密}$对产品的生产信息进行加密，生成生产信息加密数据。具体地，生产信息可以是指生产方在生产产品时生成的产品信息，其中，产品信息可以通过m表示，则生产信息可以通过$m_{生产}$表示。在实际应用中，通常需要保护$m_{生产}$的隐私，也可以理解为保护生产方的隐私，所以根据除购买方以外无法获知的pincode对生产信息进行加密，安全性很高。

[0122] 对于加密，可以通过加密函数实现，加密函数enc可以是指对信息进行加密的函数，函数中有两个输入，密钥和信息，加密后可以生成信息加密数据(在本实施例中，加密的信息即为产品信息m)，可以通过enc(加密密钥key，产品信息m)表示。而对于获取到信息加

密数据enc，但不知道key，无法解析出m；对于获取到enc和m，也无法得知key，此处的key若是非对称密钥，那么enc即为非对称加密；若key是对称密钥，那么enc即为对称加密。非对称加密的情况可以存在公钥pk和私钥sk。在本步骤中，可以将生成生产信息加密数据表示为enc(key$_{生产加密}$，m$_{生产}$)。

[0123] 在前文已经介绍，key$_{生产加密}$可以由pincode单向生成，也可以由pincode||nonce$_{生产}$单向生成，可见在加入nonce$_{生产}$的情况下，pincode与nonce$_{生产}$是得到key$_{生产加密}$的关键，而pincode只有购买方能够获得，所以为了达到保护nonce$_{生产}$的目的，本方法还可以包括：

[0124] 根据唯一暗码，单向生成随机数查询标识；在可信存储库中为该产品创建唯一标识；将随机数查询标识以及生产随机数发送至可信存储库，并均与唯一标识关联。

[0125] 具体地，为了达到保护nonce$_{生产}$的目的，可以将该nonce$_{生产}$发送至一个可信存储库中，当购买方需要生成key$_{生产加密}$，并对enc(key$_{生产加密}$，m$_{生产}$)进行解密时，可以从可信存储库中，查找到nonce$_{生产}$。该可信存储库，可以是高度安全的国家机构或企业，为在可信存储库中，可以存储针对不同产品的生产随机数，所以可以为不同产品分别创建一个唯一标识，对于如何查找nonce$_{生产}$，可以根据唯一暗码，单向生成随机数查询标识hash(pincode)，在将nonce$_{生产}$发送至可信存储库时，可以将hash(pincode)以及nonce$_{生产}$共同发送至可信存储库，并均与唯一标识关联，以便购买方可以通过hash(pincode)查找到nonce$_{生产}$。而在加入nonce$_{生产}$的情况下，key$_{生产加密}$＝hash(pincode||nonce$_{生产}$)，对于随机数查询标识hash(pincode)，也不会影响的key$_{生产加密}$安全性。

[0126] 根据本实施例的前提，在产品流通过程中，只存在生产方和购买方的情况下，实际应用中，可以由生产方将enc(key$_{生产加密}$，m$_{生产}$)发送至购买方，以便购买方解析m$_{生产}$。

[0127] 步骤16：根据生产加密密钥，生成生产信息查询标识。

[0128] 步骤18：将生产信息集合写入区块链，该生产信息集合可以包含生产信息查询标识、以及生产信息加密数据。

[0129] 区块链，可以是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式数据库。而将enc(key$_{生产加密}$，m$_{生产}$)写入区块链中，可以有效地防止篡改和伪造，具有较高的安全性和隐私性。由于区块链中，有大量的数据，所以为了使购买方能够快速地查找到enc(key$_{生产加密}$，m$_{生产}$)，可以根据key$_{生产加密}$，生成一个生产信息查询标识，比如，就可以通过单向函数生成，还可以根据key$_{生产加密}$中特定个字符位数生成，又或结合特定个字符位数以及单向函数生成，又或对进行二次单向计算，生成生产信息查询标识。可以包含生产信息查询标识以及enc(key$_{生产加密}$，m$_{生产}$)的生产信息集合写入区块链，以便购买方可以读取。

[0130] 如图2所示，为本方法的一个实施方式的示意图；如图3所示，为本方法的另一个实施例方式的示意图，区别在于如图3所示的实施方式中对key$_{生产加密}$的生成过程加入nonce$_{生产}$，更加有利于对enc(key$_{生产加密}$，m$_{生产}$)进行保护。

[0131] 需要说明的是，在本实施例以及下文的描述中，所指的"产品"均为同一产品，即生产方生成出的产品，比如，本说明书中的产品可以为"一批饮料"或"一个50GB的网络存储空间"，围绕产品的信息、密钥、公钥、私钥等，均对应同一产品。

[0132] 采用实施例1提供的方法，生产方利用产品的唯一暗码，单向生成生产加密密钥，再根据生产加密密钥，对产品的生产信息进行加密，生成生产信息加密数据，根据生产加密

密钥,生成生产信息查询标识,将包含生产信息查询标识、以及生产信息加密数据的生产信息集合写入区块链。利用产品唯一暗码除生产方和购买方以外无法获知的特性,以及区块链不可篡改不可伪造的特性,对生产信息进行加密和存储,使得生产信息有很高的保密性。此外,还可以通过生产随机数,进一步加强生产信息的保密性。

[0133] 实施例2

[0134] 基于与实施例1相同的发明思路,本实施例以流通过程中,存在生产方和购买方的情况为例,介绍基于区块链的产品信息加密、解密方法,用于在产品流通过程中,对产品信息进行保密,且确保购买方能够获得产品信息。具体地,本实施例介绍一种基于区块链的产品信息解密方法,应用于存在生产方和购买方中的购买方。该方法的流程如图4所示,包括下述步骤:

[0135] 步骤22:根据产品的唯一暗码,单向生成生产加密密钥。

[0136] 在实施例1中已经介绍,生产方可以根据pincode,单向生成$key_{生产加密}$,即有$key_{生产加密}$=hash(pincode),还介绍了pincode的特性,即购买方在破坏产品完整性,开始使用产品后,能够找到pincode,所以,购买方也就可以根据pincode,单向生成$key_{生产加密}$。

[0137] 在实施例1中还介绍了,为了进一步加强的$key_{生产加密}$的安全性,生产方在生产产品时,可以生成$nonce_{生产}$,所以在一种实施方式中,本步骤可以包括: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随机数查询标识对应的生产随机数;根据唯一暗码与生产随机数的组合,单向生成生产加密密钥。

[0138] 具体地,在加入$nonce_{生产}$的情况下,$key_{生产加密}$=hash(pincode||$nonce_{生产}$),由于生产方根据pincode生成了随机数查询标识hash(pincode),并将hash(pincode)以及$nonce_{生产}$共同发送至可信存储库,且均与为产品创建的唯一标识关联。所以购买方也可以根据pincode,单向生成hash(pincode),可以在可信存储库中通过hash(pincode)查找到$nonce_{生产}$,再单向生成$key_{生产加密}$=hash(pincode||$nonce_{生产}$),在实施例1中介绍pincode的$nonce_{生产}$的组合,本步骤中可以通过相同的组合方式进行组合,以便生成的$key_{生产加密}$与生产方生成的$key_{生产加密}$一致。

[0139] 步骤24:根据生产加密密钥,生成生产信息查询标识。

[0140] 在实施例1中介绍了生成生产信息查询标识的方式,本步骤中,购买方也可以按照生产方生成生产信息查询标识的方式进行生成,确保一致性。

[0141] 步骤26:根据生产信息查询标识,从区块链中读取产品的生产信息加密数据。

[0142] 在实施例中生产方将包含生产信息查询标识以及enc($key_{生产加密}$,$m_{生产}$)的生产信息集合写入区块链,本步骤就可以根据生产信息查询标识,读取到enc($key_{生产加密}$,$m_{生产}$)。

[0143] 步骤28:根据生产加密密钥,对生产信息加密数据进行解密,获得生产信息。

[0144] 在本步骤,根据加密函数的特性,可以根据$key_{生产加密}$,对enc($key_{生产加密}$,$m_{生产}$)进行解密,获得$m_{生产}$。由于购买方在破坏产品完整性,开始使用产品后,才能够找到pincode。盗窃方即使得到enc($key_{生产加密}$,$m_{生产}$),也由于无法得知pincode,无法进行解密,如果在加上$nonce_{生产}$的情况,由于无法得知pincode也就无法得知hash(pincode),更无法确定出$key_{生产加密}$=hash(pincode||$nonce_{生产}$)。

[0145] 如图5所示,为本方法的一个实施方式的示意图;如图6所示,为本方法的另一个实施例方式的示意图,区别在于如图6所示的实施方式中对$key_{生产加密}$的生成过程加入$nonce_{生产}$,

增加了解析$m_{生产}$的难度。

[0146] 采用实施例2提供的方法，购买方利用产品的唯一暗码，单向生成生产加密密钥，再根据生产加密密钥生成生产信息查询标识，对从区块链读取到的生产信息加密数据进行解密，获得生产信息。利用产品唯一暗码在购买方破坏产品完整性后才能获知的特性，以及区块链不可篡改不可伪造的特性，对生产信息进行解密，使得生产信息有很高的保密性。此外，还可以通过生产随机数，进一步加强生产信息的保密性。

[0147] 实施例3

[0148] 在前述两个实施例中，已经介绍了流通过程中，存在生产方和购买方的情况，而在实际应用中，也很可能存在一个或多个流通方，即可以使产品便捷地从生产方流通到购买方，比如代理商、批发商、零售商等。而流通方也会在流通过程中，为产品生成流通信息，而流通信息中可以包含流通方的隐私信息，所以也需要进行保密，即对于对其他流通方以及窃取者而言，需要对产品信息进行保密，并确保购买方可以查看产品信息，其他流通方无法获知生产信息以及其他流通方的流通信息。

[0149] 所以基于与前述两个实施例相同的发明思路，本实施例以流通过程中存在生产方、流通方和购买方的情况为例，介绍一种基于区块链的产品信息加密、解密方法，具体地，先介绍一种基于区块链的产品信息的加密方法，应用于存在生产方、流通方和购买方中的生产方。该方法的流程如图7所示，包括下述步骤：

[0150] 步骤32：根据产品的唯一暗码，单向生成生产加密密钥；

[0151] 步骤34：根据生产加密密钥，对该产品的生产信息进行加密，生成生产信息加密数据。

[0152] 前两步骤中，与实施例1类似，此处不再赘述，可以根据如图2或图3所示的实施方式生成$enc(key_{生产加密}, m_{生产})$。

[0153] 步骤36：根据生产加密密钥，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。

[0154] 这里所指的第1流通密钥，可以作用于第1次序流通方进行流通，比如批发商作为生产方后的第一个流通方，那么批发商就可以是指第1次序流通方。考虑到pincode的特性，即生产方和破坏产品完整性后的购买方才能获知，可以以pincode作为基础，在流通过程中进行链式连续生成加密密钥。具体地，可以利用单向函数的特性，即得知结果无法逆向解析输入的特性，根据生产加密密钥，单向生成第1流通密钥，该第1流通密钥可以$key_{第1流通}$表示。

[0155] 在实施例1中已经介绍，可以将信息加密数据写入区块链，购买方可以通过$key_{生产加密}$生成生产信息查询标识，且便于从区块链中读取$enc(key_{生产加密}, m_{生产})$。但针对流通方而言，为了达到对生产信息保密的目的，可以无需流通方获知$key_{生产加密}$，但流通方也需要在区块链中读取数据，所以可以为流通方也生成一个生产信息查询标识，且避免由$key_{生产加密}$直接生成，即根据$key_{第1流通}$，单向生成生产信息查询标识，可以表示为$hash(key_{第1流通})$。

[0156] 步骤38：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。

[0157] 由于是$key_{第1流通}$通过$key_{生产加密}$生成的，而$key_{第1流通}$又可以作用于第1次序流通方进行流通，可以考虑让第1次序流通方获知$key_{第1流通}$，但无法获知$key_{生产加密}$，所以可以通过第1公钥对$key_{第1流通}$进行加密，第1公钥可以表示为pk_1，可以是指第1次序流通方的流通公钥。具体

地，用第1次序流通方的pk_1对$key_{第1流通}$进行加密，可以生成第1流通密钥加密数据$enc(pk_1, key_{第1流通})$。从而使得第1次序流通方可以根据第1私钥sk_1进行解密。

[0158] 在实际应用中，为了进一步保护产品流通过程的隐私性，可以在生成$enc(pk_1, key_{第1流通})$的过程中，加入产品的公开明码，在一种实施方式中，本步骤可以包括：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流通密钥加密数据。公开明码qcode，可以在产品外部且全局唯一，任何一方在接收到产品后，均可以获得qcode，但对于未拿到产品的任何对象不容易获得(比如窃取者，但也可以通过非正常手段窃取)，所以可以将qcode加入到流通过程中，进一步加强流通的隐私性。具体地，可以有$enc(pk_1, qcode||key_{第1流通})$。

[0159] 步骤310：根据第1公钥，单向生成第1流通密钥查询标识。

[0160] 上一步骤中，生成了$enc(pk_1, key_{第1流通})$，而为了保证数据安全性，本方法也可以将信息集合写入区块链，所以为了使第1流通方便捷地找到$enc(pk_1, key_{第1流通})$，可以为流通方生成单向一个密钥查询标识，即第1流通密钥查询标识，可以表示为$hash(pk_1)$，以便第1流通可以通过pk_1从区块链中读取到$enc(pk_1, key_{第1流通})$。

[0161] 步骤312：将生产信息集合写入区块链，该生产信息集合可以包含第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。

[0162] 本步骤可以将生产信息写入区块链(上链)，以便流通方和购买方可以获取到$enc(pk_1, key_{第1流通})$以及$enc(key_{生产加密}, m_{生产})$，对于如何查找，可以通过$hash(pk_1)$，以及$hash(key_{第1流通})$。

[0163] 在实际应用中，为了进一步加强隐私性，本步骤可以包括：根据生产私钥，对生产信息集合进行签名，该生产私钥为生产方在生产产品时生成的私钥；将签名后的生产信息集合写入区块链。如图8所示，为本方法的一个实施方式的示意图。

[0164] 采用实施例3提供的方法，在实施例1的基础上，根据生产加密密钥，单向生成用于流通至第1次序流通方的第1流通密钥，再单向生成生产信息查询标识，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，根据第1公钥，单向生成第1流通密钥查询标识，将包含所述第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生产信息集合写入区块链。利用产品唯一暗码在购买方破坏产品完整性后才能获知的特性，以及区块链不可篡改不可伪造的特性，对生产信息进行加密，使得生产信息有很高的保密性，且将生产信息写入区块链，使得下个流通方能够通过链式连续加密的方式，将产品信息写入区块链。

[0165] 实施例4

[0166] 基于与前述两个实施例相同的发明思路，本实施例以流通过程中存在生产方、流通方和购买方的情况为例，介绍一种基于区块链的产品信息加密、解密方法，具体地，介绍一种基于区块链的产品信息的加密方法，应用于存在生产方、流通方和购买方中的流通方。该方法的流程如图9所示，包括下述步骤：

[0167] 步骤42：根据第n公钥，单向生成第n流通密钥查询标识。

[0168] 在实施例3中，介绍了流通方公钥的作用，本步骤可以根据pk_n，单向生成第n流通密钥查询标识$hash(pk_n)$，其中，n可以是大于0的自然数，比如1、2、3、4.....等。

[0169] 步骤44：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。

[0170] 如图8所示，在将生产信息集合写入区块链时，第1次序流通方可以根据hash(pk_1)，查找到enc(pk_1，$key_{第1流通}$)，类似地，第n次序流通方可以根据hash(pk_n)，查找到enc(pk_n，$key_{第n流通}$)。

[0171] 在实施例3中已经介绍，可以实际应用中，对生产信息集合进行签名，而对于流通方，可以有多个流通方，每个流通方均以各自的私钥进行签名，所以在本步骤之后，还可以包括：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。当验证成功后，再执行下个步骤。

[0172] 步骤46：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。

[0173] 在实施例3中已经介绍，第1次序流通方可以根据第1私钥sk_1对enc(pk_1，$key_{第1流通}$)进行解密，类似地，本步骤中，也可以根据第n私钥sk_n对enc(pk_n，$key_{第n流通}$)进行解密。

[0174] 步骤48：根据第n流通密钥，单向生成第n加密密钥。

[0175] 在实施例3(可以参考实施例1)中介绍了根据产品的pincode，单向生成$key_{生产加密}$，而作为流通方无法获取到pincode，而本说明书提供的加密方法，就可以对pincode进行链式连续生成加密密钥作为核心，所以本步骤中，流通方，可以根据$key_{第n流通}$，单向生成$key_{第n加密}$，与生产方关联到一起，就是可以是生产方根据pincode生成$key_{生产加密}$，而各个流通方链式连续生成$key_{第1加密}$、$key_{第2加密}$、$key_{第3加密}$等，即$key_{第n加密}$＝hash($key_{第n流通}$)。

[0176] 在实际应用中，为了进一步加强隐私性，也可以与生产方类似，流通方也可以生成一个随机数，所以在一种实施方式中，本步骤可以包括：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。具体地，可以有$key_{第n加密}$＝hash($key_{第n流通}$||$nonce_{第n}$)。

[0177] 与实施例1类似的，本步骤还可以包括：将第n随机数发送至可信存储库，并与产品的唯一标识关联，以便购买方可以通过产品的唯一标识，找到各个流通方的随机数，而其他流通方，由于无法得知pincode，也就无法获得其他流通方的随机数。

[0178] 步骤410：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。

[0179] 生产方可以生成一个生产信息$m_{生产}$，则流通方就可以在流通过程中生成各自的流通信息$m_{第n}$，比如，第1次序流通方可以生成$m_{第1}$，第1次序流通方可以生成$m_{第2}$，等。从而本步骤可以根据$key_{第n加密}$对$m_{第n}$进行加密，生成enc($key_{第n加密}$，$m_{第n}$)。

[0180] 步骤412：根据第n加密密钥，生成第n流通信息查询标识。

[0181] 在实施例1中已经介绍，生成信息查询标识的方式，在本步骤中，也可以根据实施例1介绍的方式，由$key_{第n加密}$生成第n流通信息查询标识。

[0182] 而在实际应用中，可以有下一个流通方，则与实施例3中步骤36类似地的，本步骤还可以包括：根据第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。而第n+1流通密钥，就可以是相对于第n次序流通方而言的下一次序的流通方。即$key_{第n+1流通}$＝hash($key_{第n流通}$)，第n流通信息查询标识可以是hash($key_{第n+1流通}$)，以便第n+1次序流通方可以根据hash($key_{第n+1流通}$)，读取区块链中的数据。

[0183] 步骤414：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。

[0184] 如图2或3所示，本步骤可以类似地，将包含第n流通信息查询标识以及enc

($key_{第n加密}$，$m_{第n}$)的第n信息集合写入区块链中。

[0185] 在有下一个流通方的情况下，本步骤可以包括

[0186] 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，该第n+1公钥可以是第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，该第n信息集合包含第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。

[0187] 具体地，可以是与前述类似地，

[0188] 可以根据pk_{n+1}，对$key_{第n+1流通}$进行加密，生成enc(pk_{n+1}，$key_{第n+1流通}$)，生成hash(pk_{n+1})作为第n+1流通密钥查询标识。将包含hash(pk_{n+1})、hash($key_{第n+1流通}$)、enc(pk_{n+1}，$key_{第n+1流通}$)、以及enc($key_{第n加密}$，$m_{第n}$)的第n信息集合写入区块链。

[0189] 而在实际应用中，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，可以包括：

[0190] 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，即可以有enc(pk_{n+1}，qcode||$key_{第n+1流通}$)。

[0191] 而在实际应用中，与前述类似地，可以根据第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，以便下个流通方可以根据公钥进行签名验证。如图10所示，为本实施例的示意图。

[0192] 采用实施例4的方法，在实施例3的生产方的基础上，根据第n私钥，解析出第n流通密钥，最终将包含第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流通信息加密数据的第n信息集合写入区块链。利用产品唯一暗码在购买方破坏产品完整性后才能获知的特性，以及区块链不可篡改不可伪造的特性，对第n流通信息进行加密，使得第n流通信息有很高的保密性，且将第n流通信息写入区块链，使得下个流通方能够通过链式连续加密的方式，将产品信息写入区块链。若没有下个流通方，也可以通过将包含第n流通信息查询标识以及第n流通信息加密数据的第n信息集合写入区块链。

[0193] 实施例5

[0194] 基于与前述实施例相同的发明思路，本实施例以流通过程中存在生产方、流通方和购买方的情况为例，介绍一种基于区块链的产品信息加密、解密方法，具体地，介绍一种基于区块链的产品信息的加密方法，应用于存在生产方、流通方和购买方中的购买方。该方法的流程如图11所示，包括下述步骤：

[0195] 步骤52：根据产品的唯一暗码，单向生成生产加密密钥。

[0196] 步骤54：根据生产加密密钥，生成生产信息查询标识。

[0197] 步骤56：根据生产信息查询标识，从区块链中读取产品的生产信息加密数据。

[0198] 在一种实施方式中，本步骤可以包括：

[0199] 根据唯一暗码与生产随机数的组合，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。

[0200] 具体地，本步骤可以加入随机数的组合，即可以有$key_{生产加密}$=hash(pincode||$nonce_{生产}$)，$key_{第1流通}$=hash($key_{生产加密}$)，单向生成生产信息查询标识hash($key_{第1流通}$)，从而可以从区块链中读取生产信息集合中的enc($key_{生产加密}$，$m_{生产}$)。

[0201] 步骤58:根据生产加密密钥,对生产信息加密数据进行解密,获得生产信息。

[0202] 上述步骤与实施例2中介绍的实施方式类似,此处不再赘述。

[0203] 步骤510:根据生产加密密钥,单向生成第1流通密钥,根据第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。

[0204] 购买方可以根据$key_{生产加密}$单向生成$key_{第1流通}$。即$key_{第1流通}=hash(key_{生产加密})$。根据链式连续生成的方式,可以根据$key_{第n流通}$生成$key_{第n加密}$,在前文已经介绍了,可以在生成加密密钥时,加入随机数,所以根据第n流通密钥,单向生成第n加密密钥,可以包括:从可信存储库中获取与随机数查询密钥对应的第n随机数;根据第n流通密钥与第n随机数的组合,单向生成第n加密密钥。具体地,由于购买方获知了pincode,所以可以单向生成随机数查询密钥hash(pincode),根据前述实施例的介绍,生产方和流通方,均可以将随机数发送至可信存储库,且可以与产品的唯一标识关联,也即唯一标识可以关联hash(pincode)、生产随机数、以及第n随机数,此时可以将可信存储库设置为,只允许通过唯一标识关联随机数而不能读取,而hash(pincode)可以进行读取,就有效防止流通方通过唯一标识获取随机数。而购买方通过hash(pincode)获取到对应的第n随机数(包括第1随机数、第2随机数.....第n随机数)后,就可以单向生成第n加密密钥,可以有$key_{第n加密}=hash(key_{第n流通}||nonce_{第n})$。而对于流通密钥,可以根据第n加密密钥,单向生成第n+1流通密钥,可以有$key_{第n+1流通}=hash(key_{第n加密})$。具体比如,购买方在步骤52中生成了$key_{生产加密}$,则本步骤可以有$key_{第1流通}=hash(key_{生产加密})$、再可以生成$key_{第1加密}=hash(key_{第1流通}||nonce_{第1})$、以及还可以生成$key_{第2流通}=hash(key_{第1加密})$,如此往复,可以得到全部的流通方的流通密钥。

[0205] 本实施例中,n可以是大于0的自然数。

[0206] 步骤512:根据第n流通信息查询标识,从区块链中读取产品的第n流通信息加密数据。

[0207] 若对于最后一个流通方,可以根据第n加密密钥,根据预设方式生成第n流通信息查询标识,比如实施例1中步骤18介绍的方式,根据$key_{第n加密}$中特定个字符位数生成,又或结合特定个字符位数以及单向函数生成,又或对进行二次单向计算,生成第n流通信息查询标识。

[0208] 而对于非最后一个流通方而言,则本步骤可以包括:根据第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$enc(key_{第n加密},m_{第n})$。

[0209] 具体地,可以有$key_{第n加密}=hash(key_{第n流通}||nonce_{第n})$,$key_{第n+1流通}=hash(key_{第n加密})$,此后可以生成第n流通信息查询标识$hash(key_{第n+1流通})$。如图10所示,可以根据$hash(key_{第n+1流通})$,从区块链中读取$enc(key_{第n加密},m_{第n})$。

[0210] 步骤514:根据第n加密密钥,对第n流通信息加密数据进行解密,获得第n流通信息。

[0211] 具体地,可以与实施例2的介绍类似,根据$key_{第n加密}$,对$enc(key_{第n加密},m_{第n})$进行解密,获取$m_{第n}$。如图12为本实施例的示意图。

[0212] 采用实施例5提供的方法,购买方利用产品的唯一暗码,单向生成生产加密密钥,再根据生产加密密钥生成生产信息查询标识,对从区块链读取到的生产信息加密数据进行

解密，获得生产信息。通过链式连续加密的方式，根据生产加密密钥，生成第1流通密钥，再生成第1加密密钥、从而持续生成第n加密密钥，再生成第n+1流通密钥、第n信息查询标识，进而根据第n加密密钥对根据第n信息查询标识获取到的第n流通信息加密数据进行解密，得到第n流通信息。

[0213] 实施例6

[0214] 基于相同的发明构思，实施例6提供了一种基于区块链的产品信息加密装置，所述装置可以应用于生产方，用于实现实施例1和实施例3所述的方法。该装置的结构框图如图13所示，为该装置的结构图，包括：

[0215] 密钥生成单元61、数据生成单元62、标识生成单元63、数据写入单元64，其中，

[0216] 所述密钥生成单元61，可以根据产品的唯一暗码，单向生成生产加密密钥；

[0217] 所述数据生成单元62，可以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；

[0218] 所述标识生成单元63，可以根据所述生产加密密钥，生成生产信息查询标识；

[0219] 所述数据传输单元64，可以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。

[0220] 在一种实施方式中，所述密钥生成单元61，可以

[0221] 接收生产方在生产所述产品时生成的生产随机数；

[0222] 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。

[0223] 在一种实施方式中，

[0224] 所述标识生成单元63，可以根据所述唯一暗码，单向生成随机数查询标识；

[0225] 所述数据传输单元64，可以

[0226] 在可信存储库中为所述产品创建唯一标识；

[0227] 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。

[0228] 在一种实施方式中，所述标识生成单元63，可以

[0229] 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

[0230] 所述数据生成单元62，可以

[0231] 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；

[0232] 根据第1公钥，单向生成第1流通密钥查询标识；

[0233] 所述数据传输单元64，可以

[0234] 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。

[0235] 在一种实施方式中，所述数据生成单元62，

[0236] 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。

[0237] 在一种实施方式中，所述数据传输单元64，可以

[0238] 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；

[0239] 将签名后的生产信息集合写入区块链。

[0240] 实施例7

[0241] 基于相同的发明构思，实施例7提供了一种基于区块链的产品信息加密装置，所述装置可以应用于流通方，用于实现实施例4所述的方法。该装置的结构框图如图14所示，为该装置的结构图，包括：

[0242] 标识生成单元71、数据读取单元72、数据解析单元73、密钥生成单元74、数据加密单元75、数据传输单元76，其中，

[0243] 所述标识生成单元71，可以根据第n公钥，单向生成第n流通密钥查询标识；

[0244] 所述数据读取单元72，可以根据第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；

[0245] 所述数据解析单元73，可以根据第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；

[0246] 所述密钥生成单元74，可以根据所述第n流通密钥，单向生成第n加密密钥；

[0247] 所述数据加密单元75，可以根据第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；

[0248] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0249] 所述数据传输单元76，可以将第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；

[0250] 其中，n为大于0的自然数。

[0251] 在一种实施方式中，所述密钥生成单元74，可以

[0252] 接收第n次序流通方在接收产品时生成的第n随机数；

[0253] 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。

[0254] 在一种实施方式中，所述数据传输单元76，可以

[0255] 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。

[0256] 在一种实施方式中，所述标识生成单元71，可以

[0257] 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

[0258] 所述密钥生成单元74，可以根据第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；

[0259] 所述标识生成单元71，可以根据第n+1公钥，单向生成第n+1流通密钥查询标识；

[0260] 所述数据传输单元76，可以将第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。

[0261] 在一种实施方式中，所述数据加密单元75，可以

[0262] 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。

[0263] 在一种实施方式中，所述数据传输单元76，可以

[0264] 根据第n私钥，对所述第n信息集合进行签名；

[0265] 将签名后的第n信息集合写入区块链。

[0266] 在一种实施方式中，所述数据解析单元73，可以根据第n私钥，对所述第n流通密钥加密数据进行解密之前，

[0267] 根据生产公钥，对签名后的生产信息集合进行签名验证；或

[0268] 根据第n公钥，对签名后的第n信息集合进行签名验证。

[0269] 实施例8

[0270] 基于相同的发明构思，实施例8提供了一种基于区块链的产品信息解密装置，所述装置可以应用于购买方，用于实现实施例3和5所述的方法。该装置的结构框图如图15所示，为该装置的结构图，包括：

[0271] 密钥生成单元81、标识生成单元82、数据读取单元83、以及数据解析单元84，其中，

[0272] 所述密钥生成单元81，可以根据产品的唯一暗码，单向生成生产加密密钥；

[0273] 所述标识生成单元82，可以根据所述生产加密密钥，生成生产信息查询标识；

[0274] 所述数据读取单元83，可以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；

[0275] 所述数据解析单元84，可以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。

[0276] 在一种实施方式中，

[0277] 所述密钥生成单元81，可以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；

[0278] 所述数据读取单元83，可以根据所述第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；

[0279] 所述数据解析单元84，可以根据所述第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；

[0280] 其中，n为大于0的自然数。

[0281] 在一种实施方式中，

[0282] 所述密钥生成单元81，可以根据产品的唯一暗码，单向生成随机数查询标识；

[0283] 所述数据读取单元83，可以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；

[0284] 所述密钥生成单元81，可以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。

[0285] 在一种实施方式中，

[0286] 所述数据读取单元83，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；

[0287] 所述密钥生成单元81，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，

[0288] 其中，n为大于0的自然数。

[0289] 在一种实施方式中，

[0290] 所述密钥生成单元81，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；

[0291] 所述数据读取单元83，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

[0292] 所述密钥生成单元81，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；

[0293] 所述数据读取单元83，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。

[0294] 图16是本说明书的一个实施例电子设备的结构示意图。在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少1个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[0295] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或EISA(Extended Industry Standard Architecture，扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图16中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[0296] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[0297] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成会话窗口中信息对话框的渲染装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

[0298] 根据产品的唯一暗码，单向生成生产加密密钥；

[0299] 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；

[0300] 根据所述生产加密密钥，生成生产信息查询标识；

[0301] 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。

[0302] 还可以用于执行以下操作：

[0303] 根据第n公钥，单向生成第n流通密钥查询标识；

[0304] 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；

[0305] 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；

[0306] 根据所述第n流通密钥，单向生成第n加密密钥；

[0307] 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；

[0308] 根据所述第n加密密钥，生成第n流通信息查询标识；

[0309] 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；

[0310] 其中，n为大于0的自然数。

[0311] 还可以用于执行以下操作：

[0312] 根据产品的唯一暗码,单向生成生产加密密钥;

[0313] 根据所述生产加密密钥,生成生产信息查询标识;

[0314] 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;

[0315] 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。

[0316] 上述如本说明书图16所示实施例提供的业务反馈装置执行的方法可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field -Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本说明书实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本说明书实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0317] 该电子设备还可执行图13至图15中的基于区块链的产品信息加密、解密装置执行的方法,并实现基于区块链的产品信息加密、解密装置在图16所示实施例的功能,本说明书实施例在此不再赘述。

[0318] 本说明书实施例还提出了一种计算机可读存储介质,该计算机可读存储介质存储一个或多个程序,该一个或多个程序包括指令,该指令当被包括多个应用程序的电子设备执行时,能够使该电子设备执行图16所示实施例中业务反馈装置执行的方法,并具体用于执行:

[0319] 根据产品的唯一暗码,单向生成生产加密密钥;

[0320] 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;

[0321] 根据所述生产加密密钥,生成生产信息查询标识;

[0322] 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。

[0323] 还可以用于执行:

[0324] 根据第n公钥,单向生成第n流通密钥查询标识;

[0325] 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;

[0326] 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;

[0327] 根据所述第n流通密钥,单向生成第n加密密钥;

[0328] 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;

[0329] 根据所述第n加密密钥,生成第n流通信息查询标识;

[0330] 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；

[0331] 其中，n为大于0的自然数。

[0332] 还可以用于执行：

[0333] 根据产品的唯一暗码，单向生成生产加密密钥；

[0334] 根据所述生产加密密钥，生成生产信息查询标识；

[0335] 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；

[0336] 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。

[0337] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0338] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0339] 本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0340] 本说明书是参照根据本说明书实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0341] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0342] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0343] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0344] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0345] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0346] 还需要说明的是，术语"包括"、"包含"或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句"包括一个……"限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0347] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0348] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0349] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0350] 以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

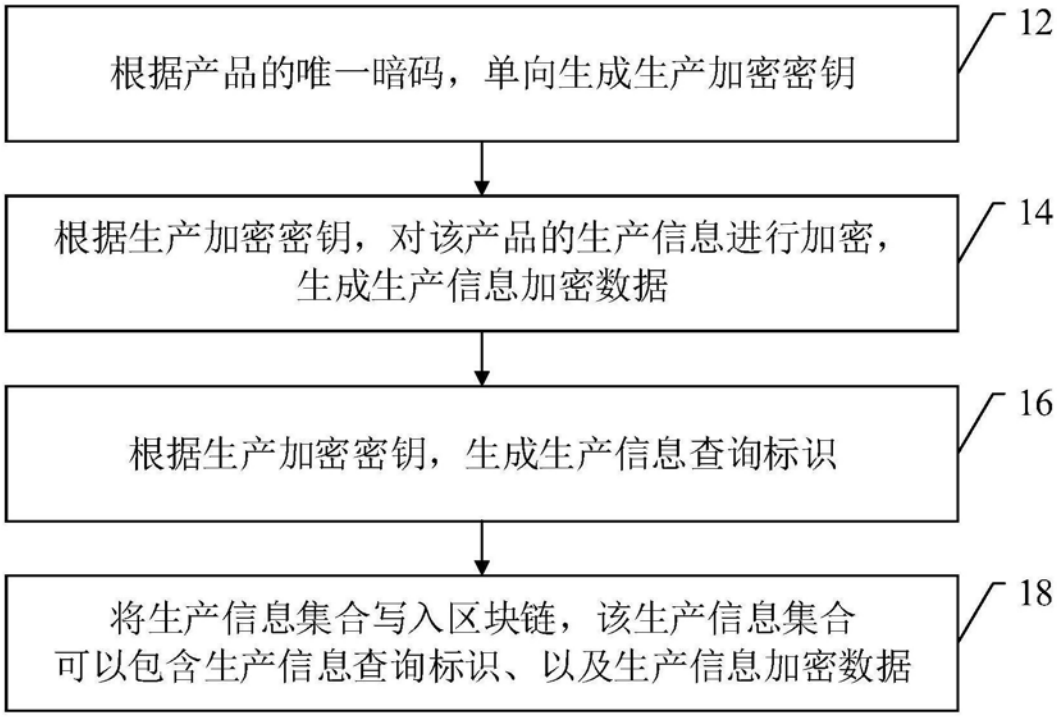

根据产品的唯一暗码，单向生成生产加密密钥
12
根据生产加密密钥，对该产品的生产信息进行加密，
生成生产信息加密数据
14
根据生产加密密钥，生成生产信息查询标识
16
将生产信息集合写入区块链，该生产信息集合
可以包含生产信息查询标识、以及生产信息加密数据
18

图1

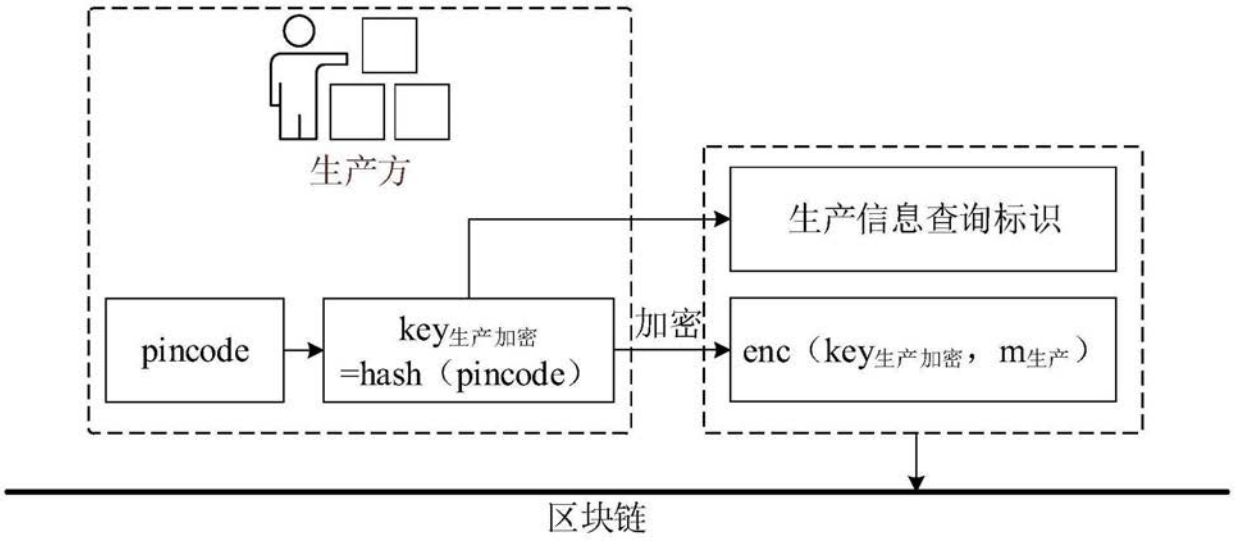

生产方
生产信息查询标识
pincode
key生产加密
=hash（pincode）
加密
enc（key生产加密，m生产）
区块链

图2

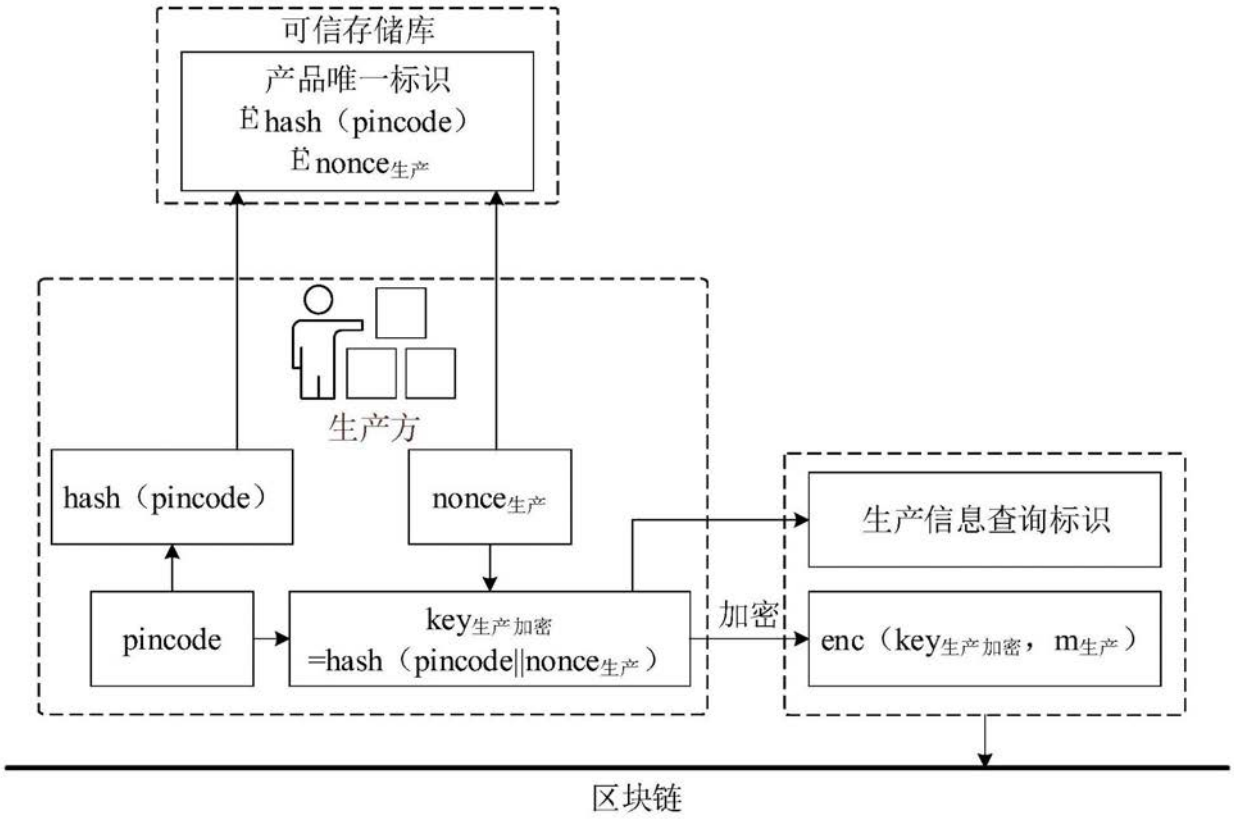

可信存储库
产品唯一标识
Ê hash（pincode）
Ê nonce生产
生产方
hash（pincode）
nonce生产
pincode
key生产加密
=hash（pincode||nonce生产）
加密
生产信息查询标识
enc（key生产加密，m生产）
区块链

图3

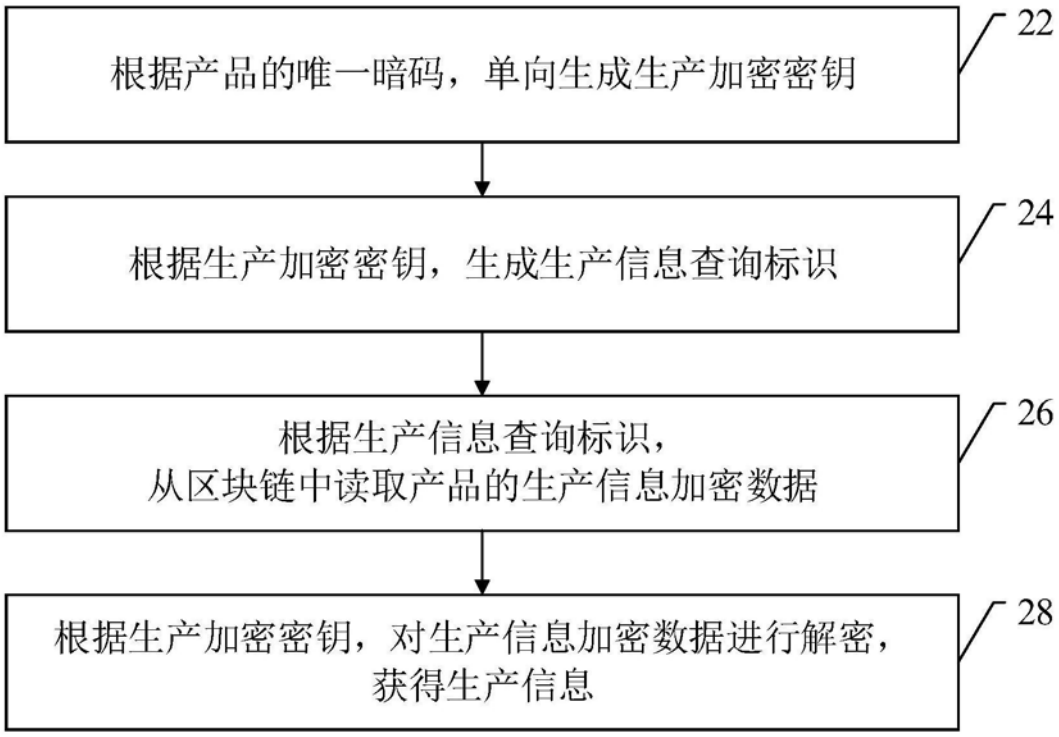

根据产品的唯一暗码，单向生成生产加密密钥
22
根据生产加密密钥，生成生产信息查询标识
24
根据生产信息查询标识，
从区块链中读取产品的生产信息加密数据
26
根据生产加密密钥，对生产信息加密数据进行解密，
获得生产信息
28

图4

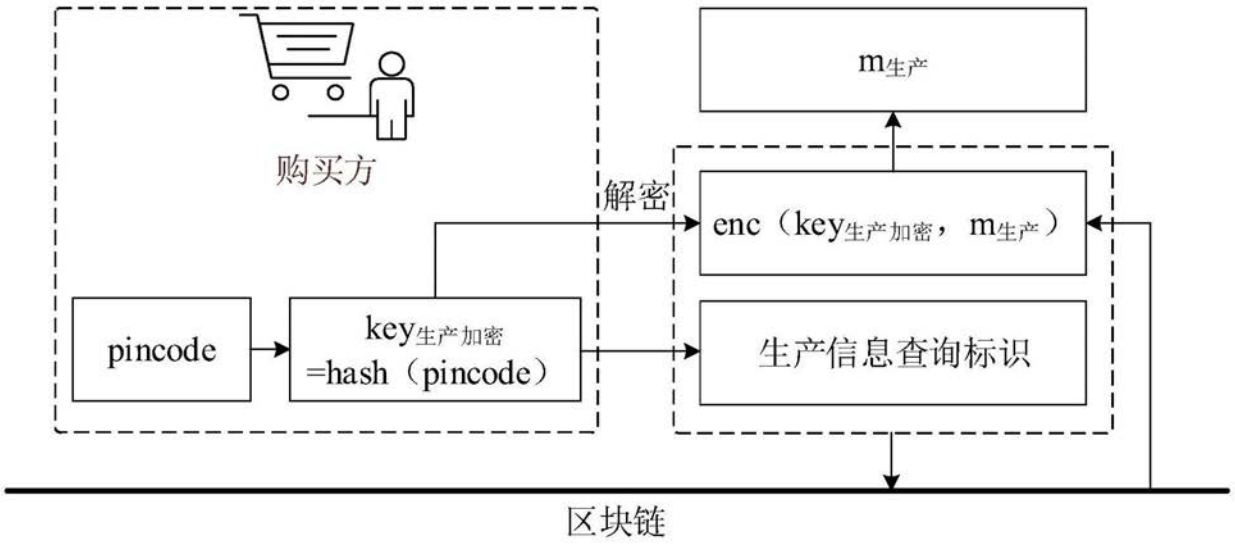

m生产
购买方
解密
enc（key生产加密，m生产）
pincode
key生产加密
=hash（pincode）
生产信息查询标识
区块链

图5

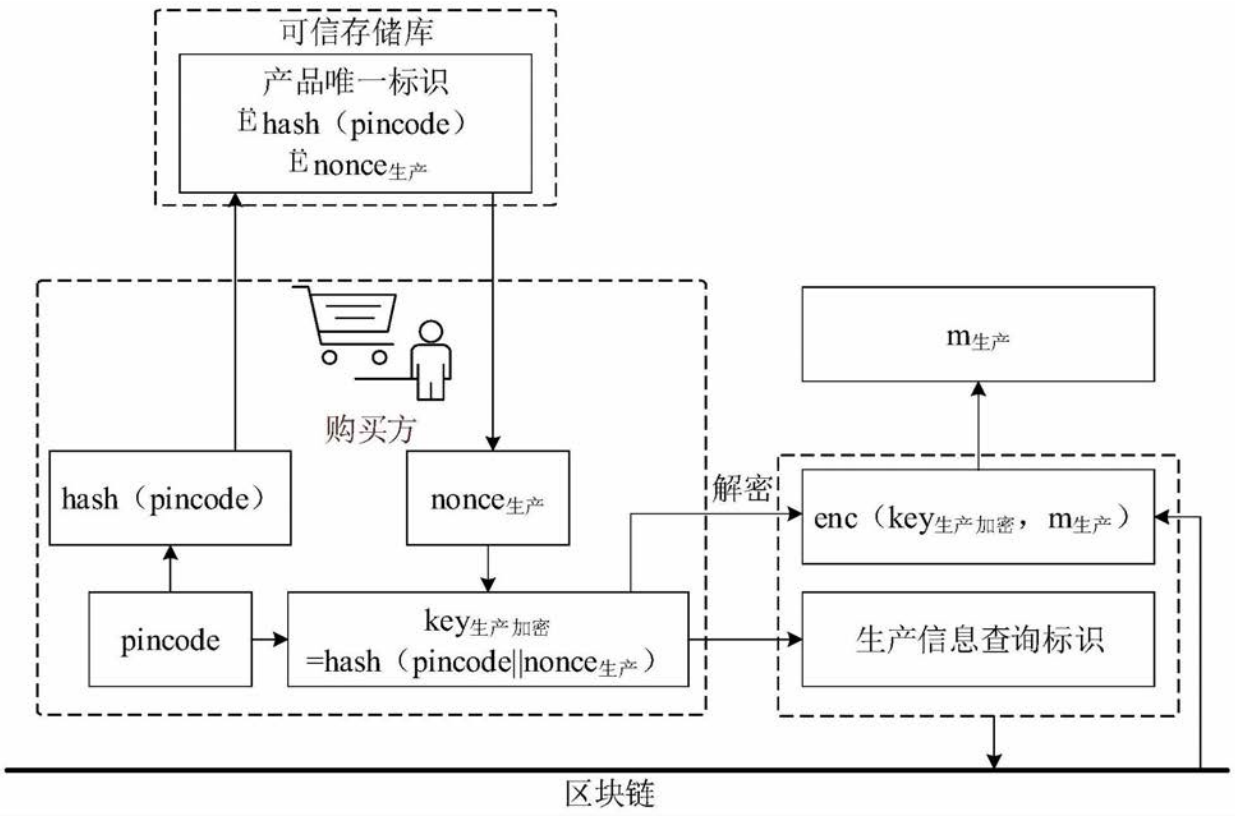

可信存储库
产品唯一标识
hash（pincode）
nonce生产
m生产
购买方
hash（pincode）
nonce生产
解密
enc（key生产加密，m生产）
pincode
key生产加密
=hash（pincode||nonce生产）
生产信息查询标识
区块链

图6

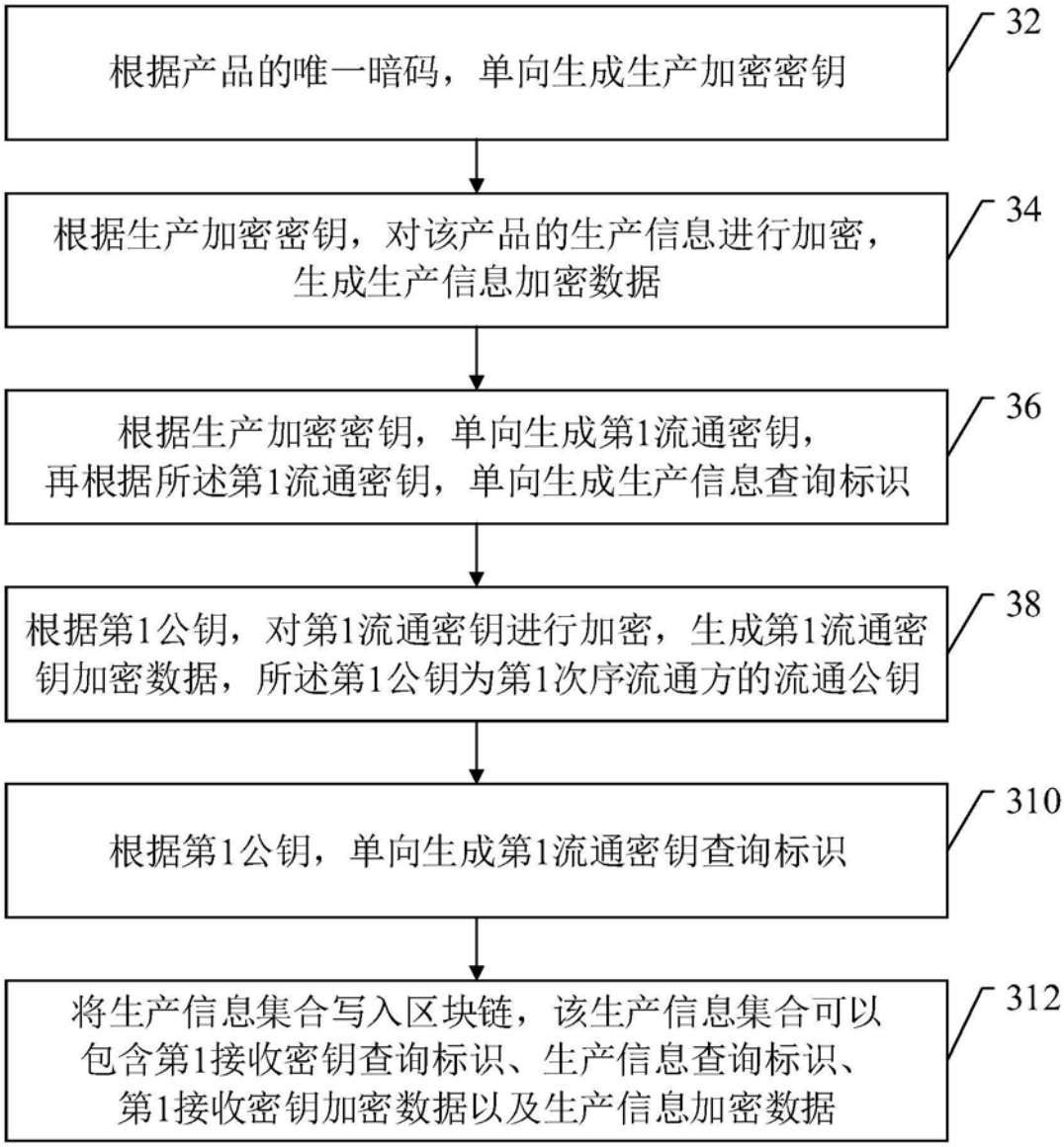

根据产品的唯一暗码，单向生成生产加密密钥
32
根据生产加密密钥，对该产品的生产信息进行加密，
生成生产信息加密数据
34
根据生产加密密钥，单向生成第1流通密钥，
再根据所述第1流通密钥，单向生成生产信息查询标识
36
根据第1公钥，对第1流通密钥进行加密，生成第1流通密
钥加密数据，所述第1公钥为第1次序流通方的流通公钥
38
根据第1公钥，单向生成第1流通密钥查询标识
310
将生产信息集合写入区块链，该生产信息集合可以
包含第1接收密钥查询标识、生产信息查询标识、
第1接收密钥加密数据以及生产信息加密数据
312

图7

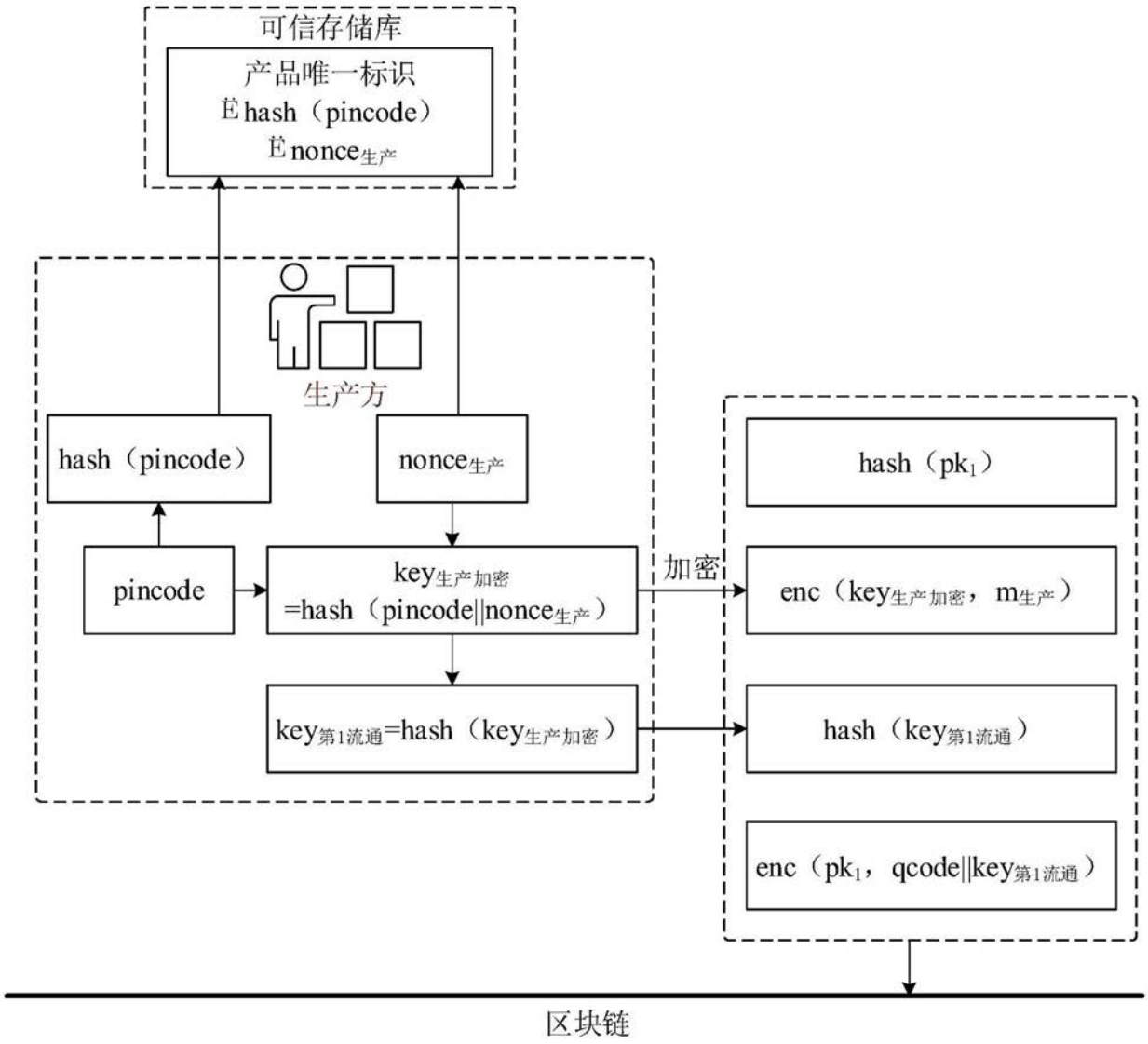

可信存储库
产品唯一标识
Ê hash（pincode）
Ê nonce生产
生产方
hash（pincode）
nonce生产
pincode
key生产加密
=hash（pincode||nonce生产）
key第1流通=hash（key生产加密）
加密
hash（pk1）
enc（key生产加密，m生产）
hash（key第1流通）
enc（pk1，qcode||key第1流通）
区块链

图8

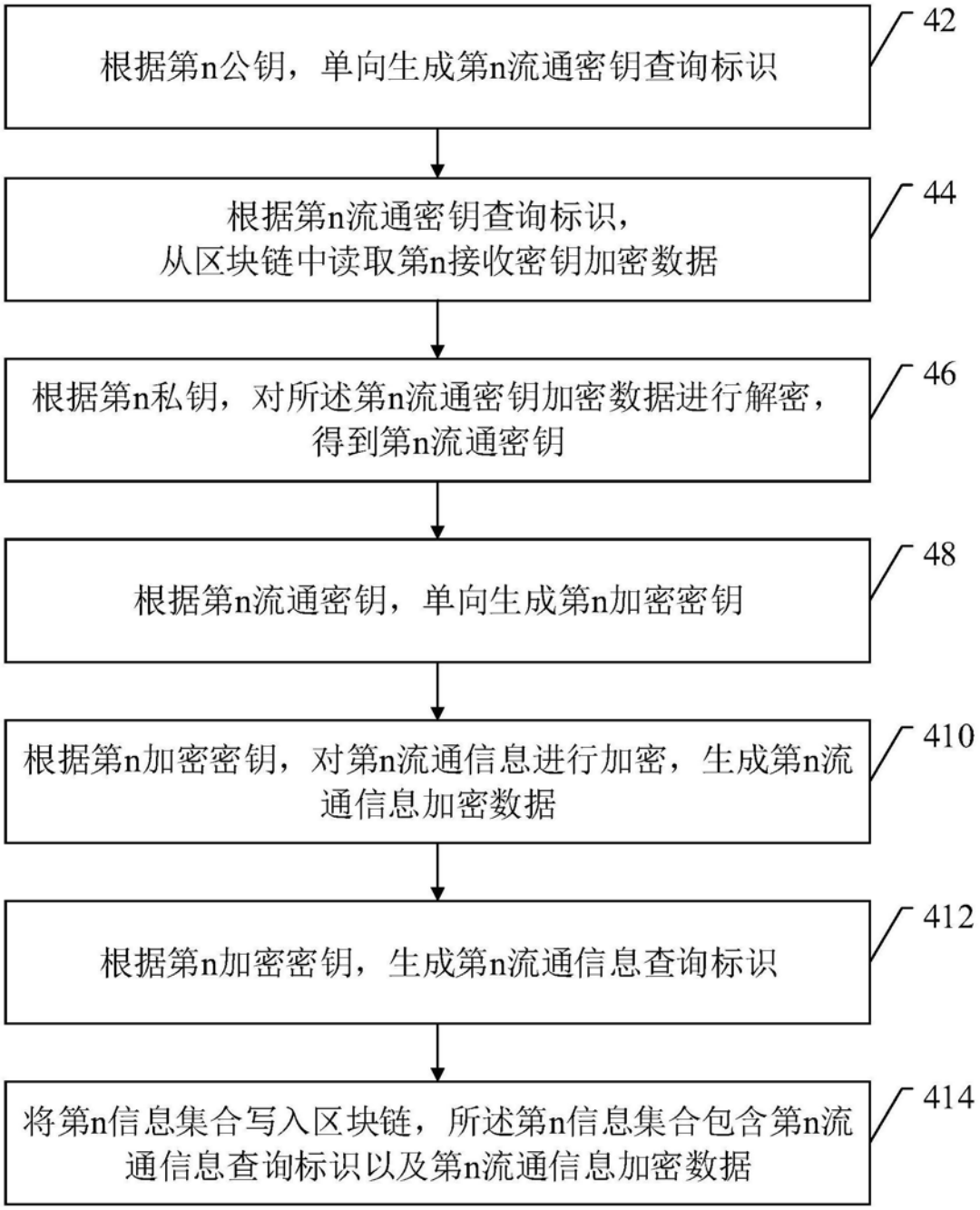

根据第n公钥，单向生成第n流通密钥查询标识
42
根据第n流通密钥查询标识，
从区块链中读取第n接收密钥加密数据
44
根据第n私钥，对所述第n流通密钥加密数据进行解密，
得到第n流通密钥
46
根据第n流通密钥，单向生成第n加密密钥
48
根据第n加密密钥，对第n流通信息进行加密，生成第n流
通信息加密数据
410
根据第n加密密钥，生成第n流通信息查询标识
412
将第n信息集合写入区块链，所述第n信息集合包含第n流
通信息查询标识以及第n流通信息加密数据
414

图9

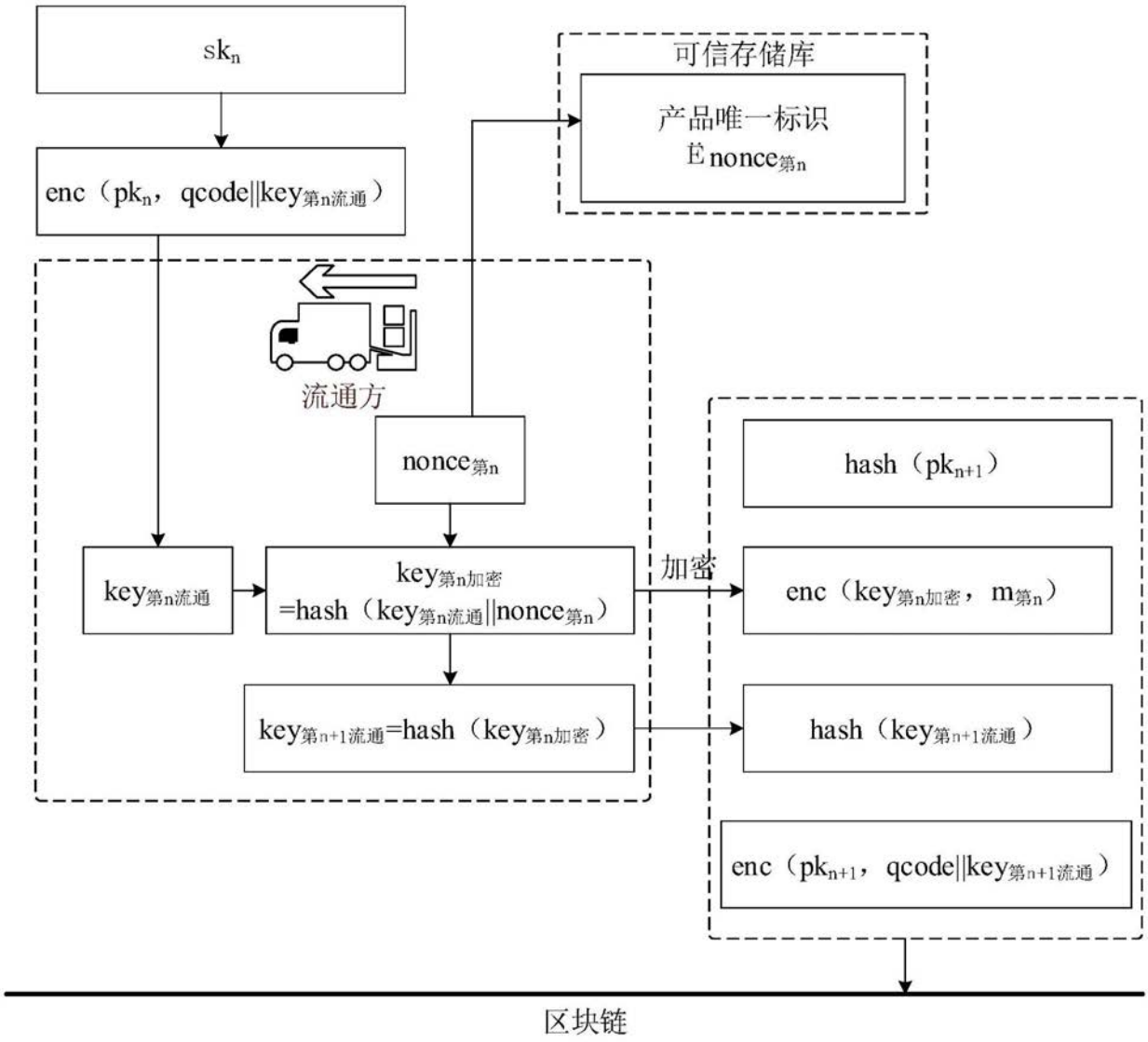

sk_n
enc（pk_n，qcode||$key_{第n流通}$）
可信存储库
产品唯一标识
$nonce_{第n}$
流通方
$nonce_{第n}$
$key_{第n流通}$
$key_{第n加密}$
=hash（$key_{第n流通}$||$nonce_{第n}$）
加密
$key_{第n+1流通}$=hash（$key_{第n加密}$）
hash（pk_{n+1}）
enc（$key_{第n加密}$，$m_{第n}$）
hash（$key_{第n+1流通}$）
enc（pk_{n+1}，qcode||$key_{第n+1流通}$）
区块链

图10

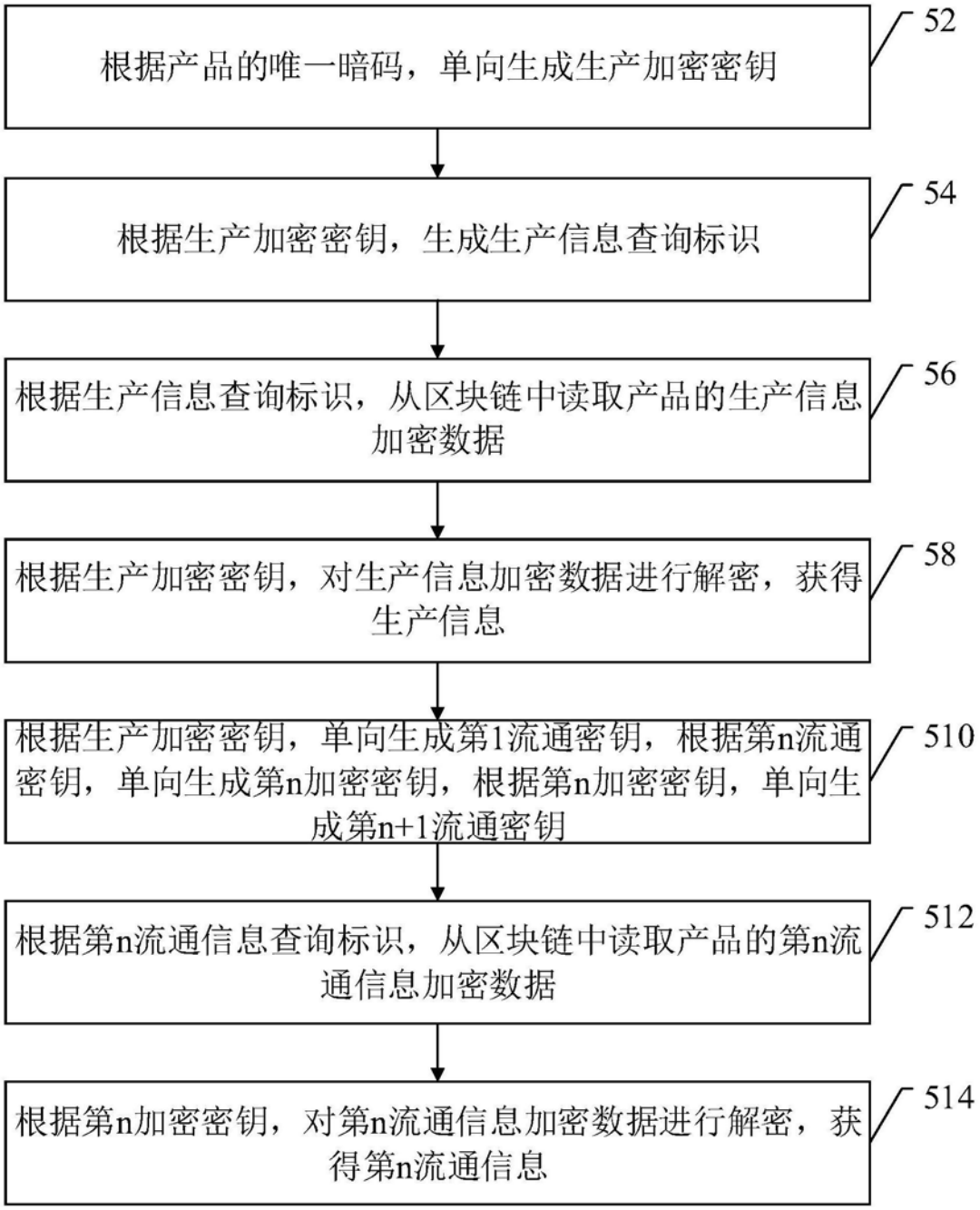

根据产品的唯一暗码，单向生成生产加密密钥
52
根据生产加密密钥，生成生产信息查询标识
54
根据生产信息查询标识，从区块链中读取产品的生产信息加密数据
56
根据生产加密密钥，对生产信息加密数据进行解密，获得生产信息
58
根据生产加密密钥，单向生成第1流通密钥，根据第n流通密钥，单向生成第n加密密钥，根据第n加密密钥，单向生成第n+1流通密钥
510
根据第n流通信息查询标识，从区块链中读取产品的第n流通信息加密数据
512
根据第n加密密钥，对第n流通信息加密数据进行解密，获得第n流通信息
514

图11

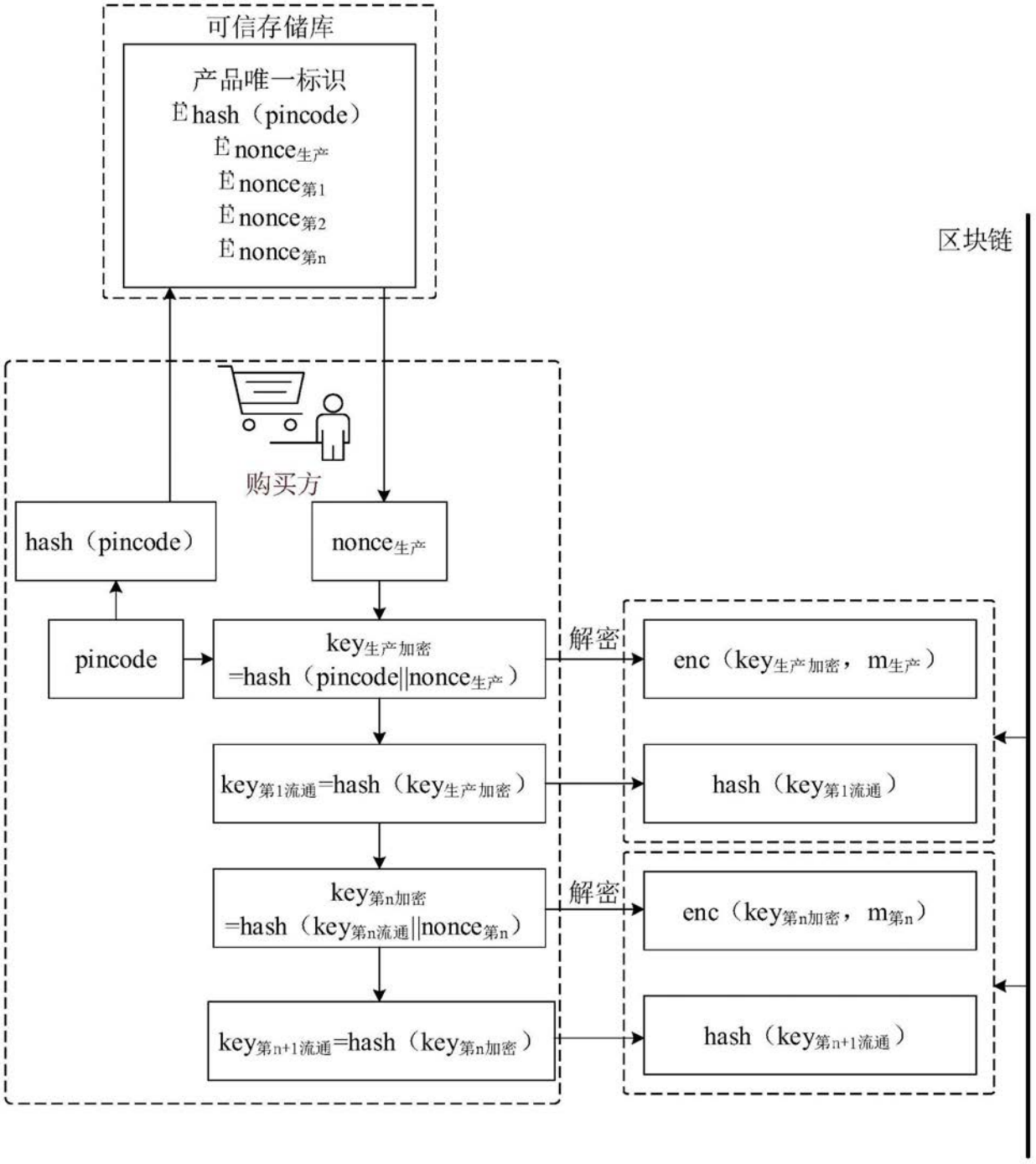

可信存储库
产品唯一标识
hash（pincode）
nonce生产
nonce第1
nonce第2
nonce第n
区块链
购买方
hash（pincode）
nonce生产
pincode
key生产加密
=hash（pincode||nonce生产）
解密
enc（key生产加密，m生产）
key第1流通=hash（key生产加密）
hash（key第1流通）
key第n加密
=hash（key第n流通||nonce第n）
解密
enc（key第n加密，m第n）
key第n+1流通=hash（key第n加密）
hash（key第n+1流通）

图12

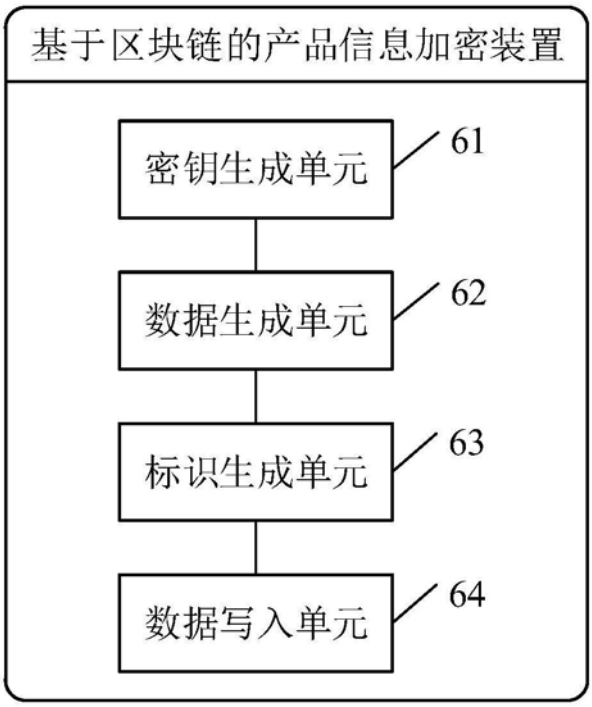


图13

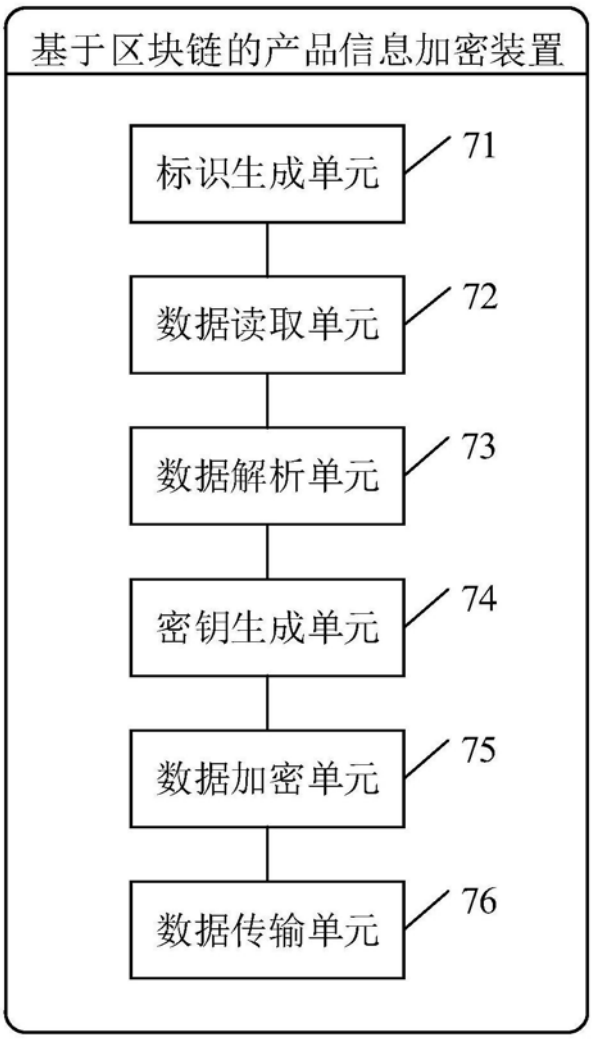

基于区块链的产品信息加密装置
标识生成单元
71
数据读取单元
72
数据解析单元
73
密钥生成单元
74
数据加密单元
75
数据传输单元
76

图14

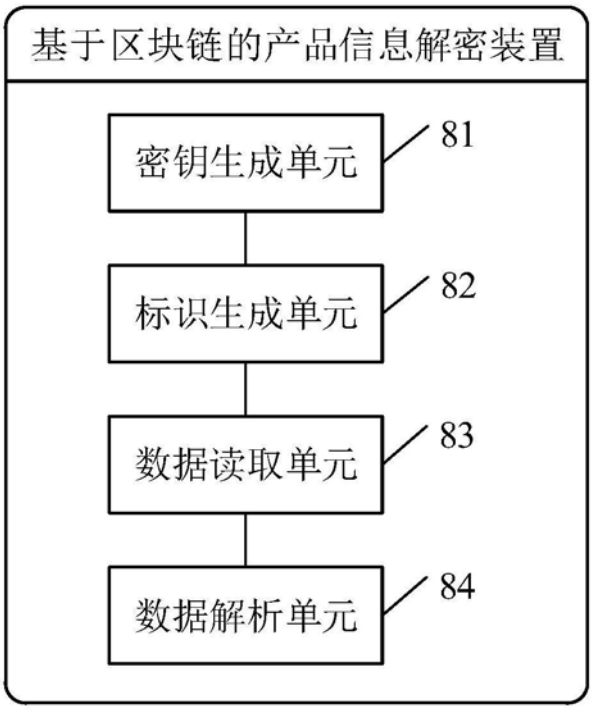

基于区块链的产品信息解密装置
密钥生成单元
81
标识生成单元
82
数据读取单元
83
数据解析单元
84

图15

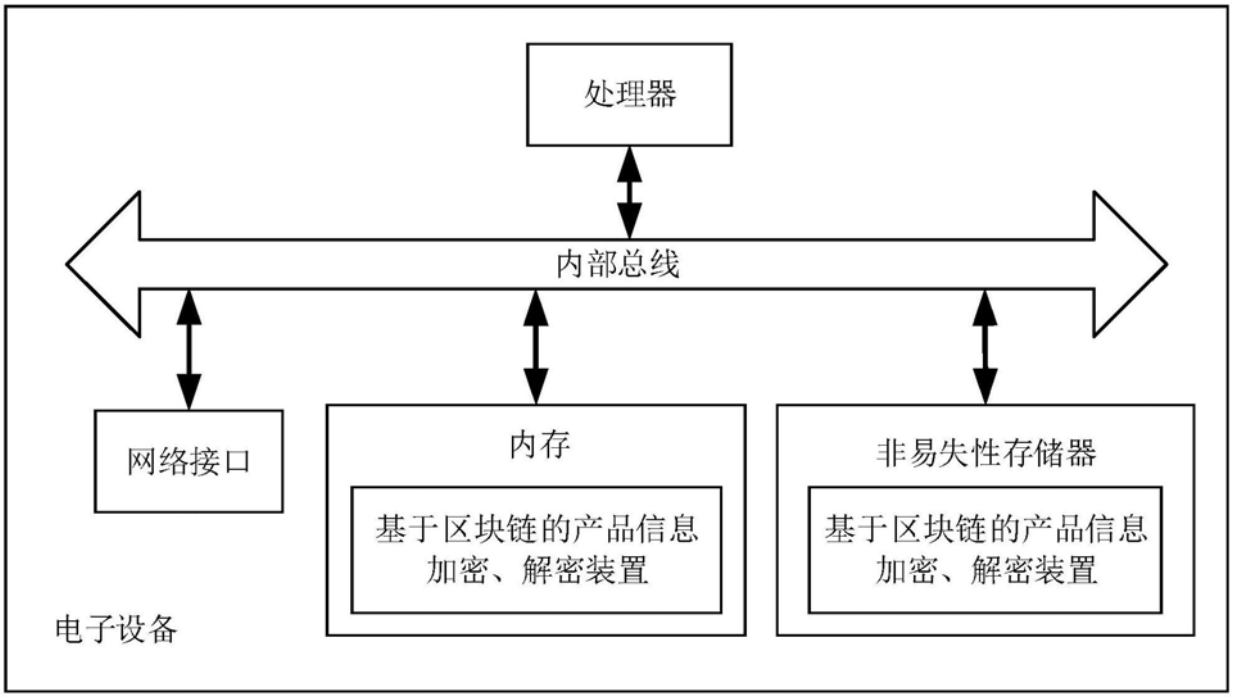

处理器
内部总线
网络接口
内存
基于区块链的产品信息加密、解密装置
非易失性存储器
基于区块链的产品信息加密、解密装置
电子设备

图16