

基于区块链的防伪方法及装置、电子设备

技术领域

[01] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的防伪方法及装置、电子设备。

5 背景技术

[02] 区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，使得区块链技术已在众多的领域中广泛的进行应用。

10 发明内容

[03] 本说明书提出一种基于区块链的防伪方法，所述区块链中存储了与目标产品对应的防伪信息；其中，所述防伪信息由多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；所述方法包括：

[04] 获取用户提交的针对所述目标产品的防伪验证请求；

15 [05] 响应于所述防伪校验请求，发起针对所述目标产品的防伪校验；其中，所述防伪校验至少包括针对所述防伪信息的完整性校验；

[06] 向所述用户返回针对所述目标产品的防伪校验结果。

[07] 可选的，所述防伪信息包括由防伪机构为所述目标产品生成的防伪识别码、以及与所述防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息。

20 [08] 可选的，所述目标产品附着了基于所述防伪识别码生成的防伪标签；所述防伪验证请求包括用户通过扫描识别所述防伪标签获取到的所述防伪识别码；

[09] 所述响应于所述防伪校验请求，发起针对所述目标产品的防伪校验，包括：

[10] 响应于所述防伪校验请求，基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询，以确定是否查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参

与方生成的防伪识别信息;

[11]如果查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息,确定所述目标产品通过防伪校验。

5 [12]可选的,所述基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询之前,还包括:

[13]针对所述防伪验证请求中的防伪识别码进行合法性验证;

[14]如果所述防伪识别码通过合法性验证,进一步基于所述防伪识别码在所述区块链中发起查询。

10 [15]可选的,所述如果所述区块链中存储了与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息,确定所述目标产品通过防伪校验,还包括:、

[16]如果所述区块链中存储了与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息,进一步针对所述至少一种由其它防伪参与方生成的防伪识别信息进行合法性验证;

15 [17]如果所述至少一种由其它防伪参与方生成的防伪识别信息通过合法性验证,确定所述目标产品通过防伪校验。

[18]可选的,所述方法还包括:

[19]响应于用户针对所述防伪标签的扫描操作,生成用户针对所述防伪标签的扫描记录;

[20]将生成的扫描记录发布至所述区块链进行存储。

20 [21]可选的,所述其它防伪参与方,包括所述目标产品的产品生命周期中的各个环节对应的关键参与方;所述至少一种由其它防伪参与方生成的防伪识别信息,包括与所述目标产品的产品生命周期中的各个环节相关的产品描述信息。

[22]可选的,所述关键参与方,包括所述目标产品的生产机构、以及检验机构;所述至少一种由其它防伪参与方生成的防伪识别信息包括,所述目标产品的生产信息的数据摘要、所述目标产品的检验报告的数据摘要。

25 [23]可选的,所述目标产品的生产信息以及所述目标产品的检验报告,存储在与所述区块链对接的第三方存储系统;其中,所述第三方存储系统为内容可寻址存储系统。

[24]可选的,所述区块链为联盟链。

[25]本申请还提出一种基于区块链的防伪装置，所述区块链中存储了与目标产品对应的防伪信息；其中，所述防伪信息由多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；所述装置包括：

[26]获取模块，获取用户提交的针对所述目标产品的防伪验证请求；

- 5 [27]校验模块，响应于所述防伪校验请求，发起针对所述目标产品的防伪校验；其中，所述防伪校验至少包括针对所述防伪信息的完整性校验；

[28]返回模块，向所述用户返回针对所述目标产品的防伪校验结果。

[29]可选的，所述防伪信息包括由防伪机构为所述目标产品生成的防伪识别码、以及与所述防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息。

- 10 [30]可选的，所述目标产品附着了基于所述防伪识别码生成的防伪标签；所述防伪验证请求包括用户通过扫描识别所述防伪标签获取到的所述防伪识别码；

[31]所述校验模块：

[32]响应于所述防伪校验请求，基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询，以确定是否查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息；

15

[33]如果查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息，确定所述目标产品通过防伪校验。

[34]可选的，所述校验模块进一步：

- [35]在基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询之前，针对所述
- 20 防伪验证请求中的防伪识别码进行合法性验证；如果所述防伪识别码通过合法性验证，进一步基于所述防伪识别码在所述区块链中发起查询。

[36]可选的，所述校验模块进一步：

- [37]如果所述区块链中存储了与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息，进一步针对所述至少一种由其它防伪参与方生成的防伪识别
- 25 信息进行合法性验证；如果所述至少一种由其它防伪参与方生成的防伪识别信息通过合法性验证，确定所述目标产品通过防伪校验。

[38]可选的，所述装置还包括：

[39]生成模块，响应于用户针对所述防伪标签的扫描操作，生成用户针对所述防伪标签的扫描记录；将生成的扫描记录发布至所述区块链进行存储。

[40]可选的，所述其它防伪参与方，包括所述目标产品的产品生命周期中的各个环节对应的关键参与方；所述至少一种由其它防伪参与方生成的防伪识别信息，包括与所述目标产品的产品生命周期中的各个环节相关的产品描述信息。

[41]可选的，所述关键参与方，包括所述目标产品的生产机构、以及检验机构；所述至少一种由其它防伪参与方生成的防伪识别信息包括，所述目标产品的生产信息的数据摘要、所述目标产品的检验报告的数据摘要。

[42]可选的，所述目标产品的生产信息以及所述目标产品的检验报告，存储在与所述区块链对接的第三方存储系统；其中，所述第三方存储系统为内容可寻址存储系统。

[43]可选的，所述区块链为联盟链。

[44]本说明书还提出一种电子设备，包括：

[45]处理器；

[46]用于存储机器可执行指令的存储器；

[47]其中，通过读取并执行所述存储器存储的与基于区块链的基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

[48]获取用户提交的针对所述目标产品的防伪验证请求；所述区块链中存储了与目标产品对应的防伪信息；其中，所述防伪信息由多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；

[49]响应于所述防伪校验请求，发起针对所述目标产品的防伪校验；其中，所述防伪校验至少包括针对所述防伪信息的完整性校验；

[50]向所述用户返回针对所述目标产品的防伪校验结果。

[51]通过以上实施例，由于在区块链中存储的与目标产品相关的防伪信息，是基于多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；并且，在针对该目标产品的防伪校验中，引入了针对区块链上存储的上述防伪信息的完整性校验；因此，即便上述多种防伪识别信息中的部分真实的防伪识别信息发生泄露，基于这部分泄露的防伪识别信息为假冒伪劣产品所生成的防伪信息，也仍然无法通过针对该产品的防伪信息的完整性校验，从而可以显著的提升产品防伪的安全等级。

附图说明

[52]图 1 是一示例性实施例提供的一种基于区块链的防伪方法的流程图。

[53]图 2 是一示例性实施例提供的一种联盟链的架构图。

[54]图 3 是一示例性实施例提供的一种电子设备的结构示意图。

5 [55]图 4 是一示例性实施例提供的一种基于区块链的防伪装置的框图。

具体实施方式

[56]在一些场景下,产品的生产机构在对产品进行防伪时,通常会基于第三方的权威机构(比如防伪机构)为产品生成的防伪识别信息(比如防伪识别码),来为产品构建防伪标签,并将防伪标签附着于产品的外表面。

10 [57]当产品流转 to 消费者手中后,消费者可以通过终端设备对附着于产品外表面的防伪标签进行扫描识别,来获取防伪识别信息,然后发起对获取到的防伪识别信息进行合法性验证,来确认所持有的产品是否为假冒伪劣的产品。

[58]在这种场景下,一旦第三方的权威机构用于生成防伪识别信息的相关数据发生泄露,则产品的造假者就可能利用发生泄露的数据,为假冒伪劣产品生成合法的防伪标签,而
15 将一些假冒伪劣产品作为真品销售给消费者,对消费者造成损失。

[59]基于此,在本说明书中,提出一种基于多个防伪参与方在区块链上存储的多种防伪识别信息来构造与目标产品相关的防伪信息,并通过在针对该目标产品的防伪校验中,引入针对上述防伪信息的完整性校验,来提升产品防伪的安全等级的技术方案。

[60]在实现时,上述目标产品的防伪参与方,可以不再仅涵盖单一的权威机构,而是由
20 多个防伪参与方组成。该多个防伪参与方可以将各自为上述目标产品生成的防伪识别信息,以交易的形式在区块链中进行存储。而应用客户端可以利用多个防伪参与方在区块链上存储的,与目标产品对应的多种防伪识别信息,来构成与目标产品对应的防伪信息;

[61]例如,上述多个防伪参与方具体可以包括防伪机构、以及至少一种其它防伪参与方;在这种场景下,上述防伪信息则具体可以包括由上述防伪机构为该目标产品生成的防伪
25 识别码、以及与该防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息;

[62]其中,上述其它防伪参与方,具体可以是上述目标产品的产品生命周期中的各个环

节对应的关键参与方；比如，上述关键参与方具体可以是上述目标产品的生产机构、检验机构等等。在这种场景下，上述防伪信息具体可以包括，上述目标产品的防伪识别码、上述目标产品的生产信息的数据摘要、上述目标产品的检验报告的数据摘要。

5 [63]当上述目标产品流转 to 消费者手中后，消费者可以通过持有的终端设备来获取上述多种防伪识别信息中的至少一种防伪识别信息，然后基于获取到的防伪识别信息，来构建针对该目标产品的防伪校验请求；

10 [64]例如，在实际应用中，上述目标产品的生产机构，可以基于上述防伪机构为该目标产品生成的防伪识别码，为该目标产品构建防伪标签（比如，该防伪标签具体可以是 RFID 电子标签、二维码标签等），并在该目标产品出厂时，将该防伪标签附着在该目标产品外表面。

[65]当该目标产品流转 to 消费者手中后，消费者可以通过持有的终端设备对该防伪标签进行扫描识别，来获取上述防伪识别码，并基于获取到的防伪识别码来构建针对上述目标产品的防伪验证请求，然后将该防伪验证请求提交给应用客户端。

15 [66]应用客户端在收到针对上述目标产品的防伪验证请求之后，可以基于该防伪验证请求中携带的防伪识别信息，发起针对上述目标产品的防伪校验；其中，针对上述目标产品的防伪校验至少需要包括针对已经在区块链上存储的与上述目标产品对应的防伪信息的完整性校验。当完成针对上述目标产品的防伪校验之后，应用客户端可以向用户返回防伪校验结果。

20 [67]在以上技术方案中，由于在区块链中存储的与目标产品相关的防伪信息，是基于多个防伪参与方在区块链上存储的与上述目标产品对应的多种防伪识别信息构成；并且，在针对该目标产品的防伪校验中，引入了针对区块链上存储的上述防伪信息的完整性校验；因此，即便上述多种防伪识别信息中的部分真实的防伪识别信息发生泄露，基于这部分泄露的防伪识别信息为假冒伪劣产品所生成的防伪信息，也仍然无法通过针对该产品的防伪信息的完整性校验，从而可以显著的提升产品防伪的安全等级。

25 [68]下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[69]请参考图 1，图 1 是本说明书一实施例提供的一种基于区块链的防伪方法，应用于应用客户端；其中，所述区块链中存储了与目标产品对应的防伪信息；所述防伪信息由多个防伪参与方在区块链上存储的与上述目标产品对应的多种防伪识别信息构成；上述方法执行以下步骤：

[70]步骤 102, 获取用户提交的针对所述目标产品的防伪验证请求;

[71]步骤 104, 响应于所述防伪校验请求, 发起针对所述目标产品的防伪校验; 其中, 所述防伪校验至少包括针对所述防伪信息的完整性校验;

[72]步骤 106, 向所述用户返回针对所述目标产品的防伪校验结果。

- 5 [73]在本说明书所描述的区块链, 具体可以包括私有链、共有链以及联盟链等, 在本说明书中不进行特别限定。

[74]例如, 在一个场景中, 上述区块链具体可以是由目标产品的防伪机构、生产机构、检验机构 (或者管理机构) 作为联盟成员组成的一个联盟链; 该联盟链的运营方可以依托于该联盟链, 来部署针对上述目标产品的防伪校验业务; 而以上所描述的作为联盟成员
10 的防伪机构、生产机构、检验机构都可以作为上述防伪校验业务的一个业务节点。各个业务节点可以将自身所产生的与上述目标产品相关的防伪识别信息以交易的形式在联盟链中进行发布, 并在该交易经过联盟链中的共识节点的共识处理之后, 在联盟链中的分布式数据库进行存储, 完成上述防伪识别信息的“上链”存证。

[75]其中, 需要说明的是, 在本说明书中所描述的交易 (Transaction), 是指用户通过
15 区块链的客户端创建, 并需要最终发布至区块链的分布式数据库中的一笔数据。

[76]区块链中的交易, 通常存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移; 例如, 在传统的比特币区块链网络中, 交易可以是用户向区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据; 例如, 运营方可以基于实际的业务需求搭建一个联盟链, 依托于联盟链部署
20 一些与价值转移无关的其它类型的在线业务 (比如, 防伪校验业务、租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等), 而在这类联盟链中, 交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[77]上述应用客户端, 可以包括任意类型的以区块链中存储的底层业务数据作为数据支撑, 来实现特定的业务功能的上层应用;

25 [78]例如, 以在区块链中部署防伪校验业务为例, 上述应用客户端具体可以是, 以区块链中存储的与上述目标产品对应的防伪数据作为数据支撑, 来实现对该目标产品的防伪验证的 APP 客户端。

[79]上述防伪信息, 具体可以包括用于对目标产品进行防伪校验的任意形式的数据; 在传统的防伪校验场景中, 上述防伪信息通常可以是由与产品的生产机构具有合作关系的

防伪机构，生成的具有唯一性的防伪识别码；而在本说明书中，上述防伪信息，则可以是由多个防伪参与方在区块链上存储的，与上述目标产品对应的多种防伪识别信息构成。

[80]其中，上述多个防伪参与方的具体类型，在本说明书中都不进行具体的限定，与上述目标产品相关的任意机构，都可以加入到上述多个防伪参与方；

- 5 [81]例如，在示出的一种实施方式中，上述多个防伪参与方，具体可以包括上述防伪机构，以及至少一种与上述防伪机构共同参与针对上述目标产品的防伪校验的其它防伪参与方。

[82]在这种场景下，上述防伪信息则具体可以包括由上述防伪机构为该目标产品生成的防伪识别码、以及与该防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息；

[83]其中，在示出的一种实施方式中，上述其它防伪参与方，具体可以包括上述目标产品的产品生命周期中的各个环节对应的关键参与方；相应的，上述至少一种由其它防伪参与方生成的防伪识别信息，则可以包括与上述目标产品的产品生命周期中的各个环节相关的产品描述信息。

- 15 [84]其中，上述产品生命周期，具体可以涵盖产品从生产到投入市场，以及从投入市场到更新换代和退出市场，所经历的所有环节；

[85]例如，在示出的一种实现方式中，上述目标产品的产品生命周期通常可以包括产品的生产、检验等环节等；在这种情况下，上述关键参与方，具体可以包括上述目标产品的生产机构、检验机构等等；相应的，上述至少一种由其它防伪参与方生成的防伪识别信息，则可以包括上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要等等。

[86]通过这种方式，由于单一防伪参与方不能篡改区块链上的存储的数据，也不能由单一防伪参与方基于自身生成的单一一种防伪识别信息，为上述目标产品构造成完整的防伪信息；因此，可以保证上述防伪信息的唯一性、可信性；而且，还可以将上述目标产品的防伪识别码，与该目标产品的产品生命周期中的诸如生产、检验等各个关键环节关联，从而基于上述目标产品的防伪识别码，就可以在区块链中查询到各个关键环节的产品描述信息。

[87]其中，需要说明的是，上述多个防伪参与方的具体数量，在本说明书中不进行特别限定；在实际应用中，上述多个防伪参与方的数量越多，最终基于上述多个防伪参与方

在区块链中存储的多种防伪识别信息构成的防伪信息的防伪能力,也会进一步得到提升。

[88]例如,在示出的一种实施方式中,上述多个防伪参与方的具体数量,可以是动态变化的;也即,上述目标产品的产品生命周期中的任意一个环节对应的运营方,都可以作为防伪参与方,动态加入或者退出上述多个防伪参与方。

- 5 [89]以下以上述区块链为联盟链,上述多个防伪参与方包括防伪机构、生产机构以及检验机构为例,对本说明书的技术方案进行详细说明;

[90]其中,需要强调的是,以上述多个防伪参与方包括上述目标产品的防伪机构、生产机构以及检验机构为例仅为示例性说明;

- [91]显然,在本说明书中,上述多个防伪参与方也可以包括防伪机构、生产机构以及检验机构以外的能够参与上述目标产品的防伪校验的其它类型的运营机构;比如,上述目标产品的销售机构、代理机构、管理机构等等,在本说明书中不再进行一一列举。、
- 10

[92]请参见图2,图2为本说明书示出的一种联盟链的架构图。

- [93]如图2所示,上述目标产品的防伪机构、生产机构以及检验机构,均可以作为联盟成员加入到联盟链,并将各自产生的与上述目标产品相关的产品数据作为防伪识别信息,以交易的形式发布至联盟链,并在该交易经过联盟链中的共识节点的共识处理之后,在联盟链中的分布式数据库进行存储,完成上述防伪识别信息的“上链”存证。
- 15

- [94]上述防伪机构,可以独立开发和设计具有唯一性的防伪验证码,并将开发和设计的防伪验证码,以交易的形式发布至联盟链,在上述联盟链的分布式数据库中进行“上链”存证;同时,上述防伪机构,还可以基于开发和设计的防伪验证码,来为上述生产机构所生产的产品构建防伪标签;其中,上述防伪标签的具体类型在本说明书不进行特别限定;比如,可以是基于上述防伪验证码生成的RFID标签、或者二维码标签,等等。
- 20

- [95]上述生产机构,在完成产品的制造生产后,可以在出库的产品的外表面上,附着由上述防伪机构生成的防伪标签;同时,可以将该产品的诸如产品名称,生产日期,出库日期,批次,包装批号等产品的生产信息,保存在与上述联盟链对应的第三方存储系统,并基于持有的私钥对该产品的生产信息的数据摘要(比如hash值)进行签名后,以交易的形式发布至联盟链,在上述联盟链的分布式数据库中进行“上链”存证;
- 25

[96]上述检验机构,可以对上述生产机构上市的各个批次的产品进行检验,并将检验报告的详细内容保存至与上述联盟链对应的第三方存储系统,同时还可以基于持有的私钥对该产品的生产信息的数据摘要进行签名后,以交易的形式发布至联盟链,在上述联盟

链的分布式数据库中进行“上链”存证。

[97]其中，在示出的一种实施方式中，上述第三方存储系统，具体可以是 CAS（content-addressable-storage，内容可寻址存储）系统。

5 [98]所谓内容可寻址存储系统，是指基于所存储的数据的内容（比如基于数据的内容生成的数据摘要）来唯一标识数据，而不再采用基于所存储的数据的保存位置来标识数据的存储系统；例如，在实际应用中，上述第三方存储系统具体可以是 IPFS 等 CAS 系统；

[99]通过这种方式，用户后续在需要查看产品的生产信息以及校验报告时，可以通过应用客户端，基于该产品的防伪信息中的数据摘要，向上述 CAS 系统发起查询，来获得产品的生产信息以及检验报告的原始内容。

10 [100] 请继续参见图 2，在本说明书中，在上述联盟链上存证的与需要进行防伪验证的目标产品相关的防伪数据，具体可以由上述目标产品的防伪验证码、上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要等三部分组成。

15 [101] 而上述防伪机构、生产机构以及检验机构，在将各自产生的与上述目标产品相关的防伪识别信息，在联盟链中进行“上链”存证之后，上述应用客户端可以获取已经在联盟链上存证的与上述目标产品对应的防伪识别码、上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要，并将在联盟链上存证的上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要，与在联盟链上存证的上述目标产品的防伪识别码进行关联存储，以将以上三方在联盟链上存证的防伪识别信息，组织成为该目标产品的防伪信息。

20 [102] 例如，在实现时，上述防伪机构、生产机构以及检验机构在联盟链上存证各自为目标产品生成的防伪识别信息时，可以将该目标产品的产品标识与对应的防伪识别信息一起在联盟链中进行存证，从而应用客户端可以在联盟链中查询对应相同的产品标识的防伪识别码、生产信息的数据摘要、以及检验报告的数据摘要，来为该目标产品生成防伪信息。

25 [103] 在本说明书中，上述联盟链的运营方，在联盟链上部署上述防伪校验业务时，具体可以通过向联盟链发布与防伪校验业务相关的智能合约来实现。

[104] 在这种情况下，上述运营方可以预先开发与防伪校验业务相关的智能合约，并在智能合约中声明需要触发执行的防伪校验业务逻辑。

[105] 而对于开发完成的智能合约，运营方可以通过联盟链中的任一节点设备将该智

能合约发布至联盟链，并在该智能合约由该联盟链中的共识节点完成共识后，收录至该联盟链的分布式数据库。

5 [106] 后续，普通的消费者可以通过应用客户端接入任一节点设备，发起对该智能合约的合约调用，在联盟链上触发执行相关的防伪校验业务逻辑，完整针对上述目标产品的防伪校验。

[107] 其中，需要说明的是，联盟链中的成员节点设备在对发布至区块链的智能合约进行共识处理时，所采用的共识算法，以及具体的共识过程，在本说明书中不再进行详述，本领域技术人员在将本说明书记载的技术方案付诸实现时，可以参考相关技术中的记载。例如，对于联盟链而言，可以采用诸如 PBFT 算法，或者其它类似的共识算法。

10 [108] 在本说明书中，当上述目标产品流转 to 消费者手中后，消费者可以通过终端设备对附着于产品外表面的防伪标签进行扫描识别，来获取该防伪标签中携带的防伪识别码，然后基于获取到的防伪识别码来构建针对上述目标产品的防伪校验请求。

15 [109] 其中，需要说明的是，在实际应用中，防伪机构在构建针对上述目标产品的防伪校验请求时，所使用的防伪识别信息，除了可以包括通过扫描识别上述防伪标签获取到的防伪识别码以外，还可以包括上述多种防伪识别信息中除了上述防伪识别码以外的任意一种或者几种，在本说明书中不进行特别限定。

[110] 也即，在上述防伪校验请求中，除了可以包括从上述防伪标签中扫描识别出的防伪识别码以外，还可以包含上述多种防伪识别信息中除了上述防伪识别码以外的其它种类的防伪识别信息。

20 [111] 而上述应用客户端在收到上述防伪验证请求后，可以响应该防伪验证请求，发起针对上述智能合约的合约调用，以完成针对上述目标产品的防伪校验。

25 [112] 其中，需要说明的是，在本说明书中，针对上述目标产品的防伪校验，至少需要包括针对已经在联盟链上存证的上述目标产品的防伪信息的完整性校验。所述完整性校验，是指校验已经在联盟链上存证的，构成上述目标产品的防伪信息的多种防伪识别信息中，是否存在缺失。

[113] 在示出的一种实施方式中，针对上述目标产品的防伪校验，具体可以包括针对上述目标产品的防伪信息的完整性校验和合法性校验两部分。

[114] 在实现时，上述应用客户端在收到上述防伪验证请求后，可以读取该防伪验证请求中携带的防伪识别码，并将该防伪验证码提交至上述智能合约的公共合约地址，来

发起针对上述智能合约的合约调用，以触发执行上述智能合约中声明的防伪校验业务逻辑，完成上述目标产品的防伪校验。

[115] 而上述智能合约在收到上述应用客户端提交的防伪识别码后，首先可以针对读取到的防伪识别码进行合法性验证；其中，针对该防伪识别码的合法性验证，通常可以
5 包括针对该防伪识别码的唯一性验证；

[116] 例如，在实际应用中，可以计算读取到的防伪识别码的 hash 值，基于该 hash 值在联盟链中发起查询，以确定联盟链中是否存证了与该 hash 值对应的唯一的防伪识别码；如果是，可以认为该防伪识别码通过了合法性验证。

[117] 当该防伪验证请求中携带的防伪识别码通过了合法性验证之后，上述智能合约
10 可以进一步针对上述目标产品的防伪信息进行完整性校验，基于该防伪验证请求中的防伪识别码在联盟链中发起查询，以确定是否查询到与该防伪识别码关联存储的上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要；

[118] 如果查询到了与该防伪识别码关联存储的上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要，表明已经在联盟链上存证的，构成上述目标
15 产品的防伪信息的多种防伪识别信息完整，并不存在缺失，此时上述目标产品的防伪信息通过完整性验证；

[119] 如果未查询到了与该防伪识别码关联存储的上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要，此时上述目标产品的防伪信息未通过完整性验证，可以通过上述应用客户端向用户返回上述防伪产品为假冒伪劣产品的防伪校
20 验结果；比如，该防伪校验结果具体可以是一条 “该产品为假冒产品” 的文本提示。

[120] 进一步的，如果上述目标产品的防伪信息通过完整性验证之后，上述智能合约可以进一步针对查询到的，与上述防伪识别码关联存储的上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要进行合法性验证；

[121] 其中，针对上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要的合法性验证，通常可以包括针对上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要所携带的签名进行验证；
25

[122] 例如，上述智能合约可以基于与上述生产机构和上述检验机构持有的私钥对应的公钥，针对上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要所携带的签名分别进行验证；如果验证通过，表明上述目标产品的生产信息的数

据摘要，以及上述目标产品的检验报告的数据摘要通过合法性验证。

[123] 如果上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要通过了合法性验证，此时针对该目标产品的防伪校验完成，该目标产品通过了防伪校验。在这种情况下，可以通过上述应用客户端向用户返回上述防伪产品为真品的防伪校验结果；比如，该防伪校验结果具体可以是一条“该产品为真品”的文本提示；

[124] 相应的，如果上述目标产品的生产信息的数据摘要，以及上述目标产品的检验报告的数据摘要未通过合法性验证（比如签名不正确），此时该目标产品未通过防伪校验。在这种情况下，可以通过上述应用客户端向用户返回上述防伪产品为假冒伪劣产品的防伪校验结果。

10 [125] 其中，需要补充说明的是，当有新的机构作为上述防伪参与方，加入至上述多个防伪参与方，此时上述应用客户端可以按照以上描述的方式，将在联盟链上存证的多种防伪识别信息，重新组织成为该目标产品的防伪信息，对原有的防伪信息进行更新；

[126] 例如，假设上述目标产品的销售机构也将作为防伪参与方加入至上述多个防伪参与方，此时该目标产品的销售机构所生成的销售信息，也将作为构成上述防伪信息的防伪识别信息加入至上述防伪信息。

[127] 相应的，如果防伪参与方的数量发生变化，构成上述防伪信息的防伪识别信息中加入了新的防伪识别信息，此时针对上述防伪信息的防伪校验逻辑，也会同步的变化；在这种情况下，上述联盟链的运营方，可以重新在联盟链中部署新的智能合约，来对上述目标产品的防伪信息进行防伪校验。

20 [128] 在示出的另一种实施方式中，用户在通过终端设备针对上述防伪标签进行识别扫描时，上述应用客户端还可以对用户针对上述防伪标签的扫描操作进行响应，生成用户针对上述防伪标签的扫描记录，然后将生成的扫描记录以交易的形式，在联盟链中进行存储。

[129] 通过这种方式，可以将用户针对上述防伪标签的扫描记录，在联盟链中进行存
25 证，以便能够在目标商品在流转的过程中，对该目标商品的防伪标签的扫描记录进行追溯查询。

[130] 通过以上实施例可见，由于在本说明书中，在区块链中存储的与目标产品相关的防伪信息，是基于多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成，不再采用单一的防伪识别码作为防伪信息；

[131] 并且，在针对该目标产品的防伪校验中，引入了针对区块链上存储的上述防伪信息的完整性校验；

[132] 因此，即便上述多种防伪识别信息中的部分真实的防伪识别信息发生泄露，基于这部分泄露的防伪识别信息为假冒伪劣产品所生成的防伪信息，也仍然无法通过针对该产品的防伪信息的完整性校验，从而可以显著的提升产品防伪的安全等级。

[133] 例如，以上述防伪信息具体由，上述目标产品的防伪识别码、上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要等三部分组成为例，即便上述目标产品的防伪识别码泄露，产品的造假者基于发生泄露的防伪识别码构建出了合法的防伪标签；但在基于从该目标产品上的防伪标签中扫描识别出的防伪识别码，对该目标产品进行防伪校验的阶段，此时由于联盟链上可能并不没有存证与该防伪识别码关联存储的上述目标产品的生产信息的数据摘要、以及上述目标产品的检验报告的数据摘要，因此无法通过针对上述防伪信息的完整性校验，从而在防伪校验阶段，仍然能够将这类包含合法的防伪标签的假冒伪劣产品识别为假冒伪劣产品。

[134] 与上述方法实施例相对应，本说明书还提供了一种基于区块链的防伪装置的实施例。本说明书的基于区块链的防伪装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 3 所示，为本说明书的基于区块链的防伪装置所在电子设备的一种硬件结构图，除了图 3 所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的电子设备通常根据该电子设备的实际功能，还可以包括其他硬件，对此不再赘述。

[135] 图 4 是本说明书一示例性实施例示出的一种基于区块链的防伪装置的框图。

[136] 请参考图 4，所述基于区块链的防伪装置 40 可以应用在前述图 3 所示的电子设备中；所述区块链中存储了与目标产品对应的防伪信息；其中，所述防伪信息由多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；所述装置 40 包括有：获取模块 401、校验模块 402 和返回模块 403。

[137] 获取模块 401，获取用户提交的针对所述目标产品的防伪验证请求；

[138] 校验模块 402，响应于所述防伪校验请求，发起针对所述目标产品的防伪校验；其中，所述防伪校验至少包括针对所述防伪信息的完整性校验；

- [139] 返回模块 403, 向所述用户返回针对所述目标产品的防伪校验结果。
- [140] 在本实施例中, 所述防伪信息包括由防伪机构为所述目标产品生成的防伪识别码、以及与所述防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息。
- [141] 在本实施例中, 所述目标产品附着了基于所述防伪识别码生成的防伪标签; 所
5 述防伪验证请求包括用户通过扫描识别所述防伪标签获取到的所述防伪识别码;
- [142] 所述校验模块 402:
- [143] 响应于所述防伪校验请求, 基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询, 以确定是否查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息;
- 10 [144] 如果查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息, 确定所述目标产品通过防伪校验。
- [145] 在本实施例中, 所述校验模块 402 进一步:
- [146] 在基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询之前, 针对所述防伪验证请求中的防伪识别码进行合法性验证; 如果所述防伪识别码通过合法性
15 验证, 进一步基于所述防伪识别码在所述区块链中发起查询。
- [147] 在本实施例中, 所述校验模块 402 进一步:
- [148] 如果所述区块链中存储了与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息, 进一步针对所述至少一种由其它防伪参与方生成的防伪识别信息进行合法性验证; 如果所述至少一种由其它防伪参与方生成的防伪识别信息通
20 过合法性验证, 确定所述目标产品通过防伪校验。
- [149] 在本实施例中, 所述装置 40 还包括:
- [150] 生成模块 404 (图 4 中未示出), 响应于用户针对所述防伪标签的扫描操作, 生成用户针对所述防伪标签的扫描记录; 将生成的扫描记录发布至所述区块链进行存储。
- [151] 在本实施例中, 所述其它防伪参与方, 包括所述目标产品的产品生命周期中的
25 各个环节对应的关键参与方; 所述至少一种由其它防伪参与方生成的防伪识别信息, 包括与所述目标产品的产品生命周期中的各个环节相关的产品描述信息。
- [152] 在本实施例中, 所述关键参与方, 包括所述目标产品的生产机构、以及检验机构; 所述至少一种由其它防伪参与方生成的防伪识别信息包括, 所述目标产品的生产信

息的数据摘要、所述目标产品的检验报告的数据摘要。

[153] 在本实施例中，所述目标产品的生产信息以及所述目标产品的检验报告，存储在与所述区块链对接的第三方存储系统；其中，所述第三方存储系统为内容可寻址存储系统。

5 [154] 在本实施例中，所述区块链为联盟链。

[155] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

10

[156] 上述实施例阐明的系统、装置、模块或模块，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，计算机的具体形式可以是个人计算机、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、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

15

[157] 与上述方法实施例相对应，本说明书还提供了一种电子设备的实施例。该电子设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。

20

[158] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

[159] 获取用户提交的针对所述目标产品的防伪验证请求；所述区块链中存储了与目标产品对应的防伪信息；其中，所述防伪信息由多个防伪参与方在区块链上存储的与所述目标产品对应的多种防伪识别信息构成；

25

[160] 响应于所述防伪校验请求，发起针对所述目标产品的防伪校验；其中，所述防伪校验至少包括针对所述防伪信息的完整性校验；

[161] 向所述用户返回针对所述目标产品的防伪校验结果。

[162] 在本实施例中，所述防伪信息包括由防伪机构为所述目标产品生成的防伪识别码、以及与所述防伪识别码关联存储的至少一种由其它防伪参与方生成的防伪识别信息；所述目标产品附着了基于所述防伪识别码生成的防伪标签；所述防伪验证请求包括用户通过扫描识别所述防伪标签获取到的所述防伪识别码；

- 5 [163] 通过读取并执行所述存储器存储的与基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

[164] 响应于所述防伪校验请求，基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询，以确定是否查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息；

- 10 [165] 如果查询到与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息，确定所述目标产品通过防伪校验。

[166] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

- 15 [167] 基于所述防伪验证请求中的防伪识别码在所述区块链中发起查询之前，针对所述防伪验证请求中的防伪识别码进行合法性验证；如果所述防伪识别码通过合法性验证，进一步基于所述防伪识别码在所述区块链中发起查询。

[168] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

- 20 [169] 如果所述区块链中存储了与所述防伪识别码关联存储的所述至少一种由其它防伪参与方生成的防伪识别信息，进一步针对所述至少一种由其它防伪参与方生成的防伪识别信息进行合法性验证；

[170] 如果所述至少一种由其它防伪参与方生成的防伪识别信息通过合法性验证，确定所述目标产品通过防伪校验。

- 25 [171] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的防伪的控制逻辑对应的机器可执行指令，所述处理器被促使：

[172] 响应于用户针对所述防伪标签的扫描操作，生成用户针对所述防伪标签的扫描记录；

[173] 将生成的扫描记录发布至所述区块链进行存储。

[174] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的
5 真正范围和精神由下面的权利要求指出。

[175] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[176] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保
10 护的范围之内。