

基于区块链的数据验证方法及装置、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数据验证方法及装置、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数据验证方法，所述方法包括：

[04]获取数据提供方公布的目标数据在区块链上的数据标识；其中，所述数据标识指示所述目标数据在所述区块链上的存储位置；

[05]基于所述数据标识确定所述目标数据是否已存储至所述区块链；

- 15 [06]如果所述目标数据已存储至所述区块链，从所述数据标识指示的存储位置上获取所述目标数据；其中，所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息；

[07]基于所述校验信息对获取到的所述目标数据进行真实性验证，并向数据验证方输出验证结果。

- 20 [08]可选的，数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码；

[09]所述获取数据提供方公布的目标数据在区块链上的数据标识，包括：

[10]扫描并解析所述图形编码，以获取所述目标数据在区块链上的数据标识。

[11]可选的，所述数据标识为收录所述目标数据的交易的交易 hash 值；

- [12]所述基于所述数据标识确定所述目标数据是否已存储至所述区块链, 包括:
- [13]基于收录所述目标数据的交易的交易 hash 值针对所述交易进行 SPV 验证, 以确定所述交易是否已存储至所述区块链。
- [14]可选的, 所述基于所述校验信息对获取到的所述目标数据进行真实性验证, 包括:
- 5 [15]执行搭载的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证;
- [16]或者, 调用发布在所述区块链上的智能合约, 执行所述智能合约中声明的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证。
- [17]可选的, 所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息; 所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行 hash 计算
- 10 得到的 hash 值;
- [18]所述基于所述校验信息对获取到的所述目标数据进行真实性验证, 包括:
- [19]针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值; 确定计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同; 如果相同, 确定获取到的所述目标数据通过真实性验证; 如果不相同, 确定获取到的所述
- 15 目标数据未通过真实性验证。
- [20]可选的, 所述辅助信息包括以下信息中的任一或者多个的组合:
- [21]数据上传方的身份标识;
- [22]所述目标数据的上传时间戳;
- [23]所述目标数据的上传地点。
- 20 [24]可选的, 还包括:
- [25]将从所述数据标识指示的存储位置上获取到的所述目标数据, 向所述数据验证方输出, 以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行比对。
- [26]本说明书还提出一种基于区块链的数据验证装置, 所述装置包括:
- 25 [27]第一获取模块, 获取数据提供方公布的目标数据在区块链上的数据标识; 其中, 所述数据标识指示所述目标数据在所述区块链上的存储位置;
- [28]确定模块, 基于所述数据标识确定所述目标数据是否已存储至所述区块链;

- [29]第二获取模块, 如果所述目标数据已存储至所述区块链, 从所述数据标识指示的存储位置上获取所述目标数据; 其中, 所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息;
- [30]验证模块, 基于所述校验信息对获取到的所述目标数据进行真实性验证, 并向数据
- 5 验证方输出验证结果。
- [31]可选的, 数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码;
- [32]所述第一获取模块:
- [33]扫描并解析所述图形编码, 以获取所述目标数据在区块链上的数据标识。
- [34]可选的, 所述数据标识为收录所述目标数据的交易的交易 hash 值;
- 10 [35]所述确定模块:
- [36]基于收录所述目标数据的交易的交易 hash 值针对所述交易进行 SPV 验证, 以确定所述交易是否已存储至所述区块链。
- [37]可选的, 所述验证模块:
- [38]执行搭载的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证;
- 15 [39]或者, 调用发布在所述区块链上的智能合约, 执行所述智能合约中声明的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证。
- [40]可选的, 所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息; 所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到的 hash 值;
- 20 [41]所述验证模块进一步:
- [42]针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值; 确定计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同; 如果相同, 确定获取到的所述目标数据通过真实性验证; 如果不相同, 确定获取到的所述目标数据未通过真实性验证。
- 25 [43]可选的, 所述辅助信息包括以下信息中的任一或者多个的组合:
- [44]数据上传方的身份标识;
- [45]所述目标数据的上传时间戳;

[46]所述目标数据的上传地点。

[47]可选的，所述第二获取模块进一步：

[48]将从所述数据标识指示的存储位置上获取到的所述目标数据，向所述数据验证方输出，以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行
5 比对。

[49]本说明书还提出一种电子设备，包括：

[50]处理器；

[51]用于存储机器可执行指令的存储器；

[52]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数据验证的
10 控制逻辑对应的机器可执行指令，所述处理器被促使：

[53]获取数据提供方公布的目标数据在区块链上的数据标识；其中，所述数据标识指示
所述目标数据在所述区块链上的存储位置；

[54]基于所述数据标识确定所述目标数据是否已存储至所述区块链；

[55]如果所述目标数据已存储至所述区块链，从所述数据标识指示的存储位置上获取所
15 述目标数据；其中，所述区块链上存储的所述目标数据中携带用于对所述目标数据进行
真实性验证的校验信息；

[56]基于所述校验信息对获取到的所述目标数据进行真实性验证，并向数据验证方输出
验证结果。

[57]通过以上技术方案，一方面，基于数据提供方公布的数据标识，来确定上述目标数
20 据是否已存储至所述区块链，可以对数据提供方发布的信息的真实性进行验证，使得数
据验证方可以及时的发现数据提供方发布的，在区块链上并不存在真实的数据存储记录
的虚假数据标识

[58]另一方面，在确定上述目标数据已存储至区块链的前提下，基于区块链上存储的上
述目标数据中携带的校验信息，对区块链上的目标数据进行真实性验证，使得数据验证
25 方可以确认出区块链上的目标数据的内容是否发生过篡改，及时的发现数据内容的异常。

附图说明

[59]图 1 是一示例性实施例提供的一种基于区块链的数据验证方法的流程图；

[60]图 2 是一示例性实施例提供的一种联盟链的示意图;

[61]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;

[62]图 4 是一示例性实施例提供的一种基于区块链的数据验证装置的框图。

具体实施方式

5 [63]随着社会信息化程度越来越高,如何连接真实世界与数字世界,已经逐渐演变成互联网向更多的生活领域和产业中深入时的关键议题。

[64]例如,在一个典型的场景中,在一些电商网站上出售的一些商品,由于用户只能在网站上看到一些图片(数字信息),因此在实际应用中,通常需要让消费者相信看到的数字信息在真实世界中存在唯一对应的实物。

10 [65]而在本说明书中,正是在以上的业务背景下,提出的一种对收录在区块链的分布式数据库中的数字信息进行真实性验证的技术方案。

[66]在实现时,可以针对目标数据定义一种标准的数据存储格式,并通过上传客户端将上述目标数据按照定义的数据存储格式,上传至该上传客户端接入的区块链节点设备。其中,在定义的数据存储格式中,可以包括用于对上述目标数据进行真实性验证的校验
15 信息。

[67]该节点设备收到上传客户端上传的目标数据后,可以将该目标数据在区块链中进行发布,在经过区块链中的节点设备的共识处理后,将上述目标数据存储至区块链的分布式数据库。

[68]而上述目标数据在被成功存储至区块链的分布式数据库后,区块链中的节点设备可
20 以通过上传客户端向数据提供方返回一个能够指示上述目标数据在区块链上的存储位置的数据标识;例如,在实际应用中,上述数据标识具体可以是收录了该目标数据的交易的交易 hash 值。

[69]进一步的,在将上述目标数据成功存储至区块链的分布式数据库后,数据提供方可以将该目标数据以及区块链中的节点设备返回的该目标数据在区块链上的数据标识进行公开发布;例如,通过网站进行公开发布。
25

[70]而数据验证方在查看到数据提供方公开发布的目标数据,以及该目标数据在区块链上的数据标识后,可以通过验证客户端对数据提供方公布的该目标数据的真实性进行验

证。

[71]首先，验证客户端可以获取数据提供方发布的上述数据标识，基于该数据标识验证上述目标数据是否已被存储至区块链的分布式数据库。

[72]进一步的，如果经过验证，确定该目标数据已经被存储至区块链的分布式数据库，

- 5 可以进一步从上述数据标识指示的存储位置上，获取区块链上已经存储的上述目标数据，然后基于该目标数据中携带的上述校验信息，对该目标数据进行真实性验证，并通过上述验证客户端向数据验证方输出验证结果。

[73]通过以上技术方案，一方面，基于数据提供方公布的数据标识，来确定上述目标数据是否已存储至所述区块链，可以对数据提供方发布的信息的真实性进行验证，使得数

- 10 据验证方可以及时的发现数据提供方发布的，在区块链上并不存在真实的数据存储记录的虚假数据标识

[74]另一方面，在确定上述目标数据已存储至区块链的前提下，基于区块链上存储的上述目标数据中携带的校验信息，对区块链上的目标数据进行真实性验证，使得数据验证方可以确认出区块链上的目标数据的内容是否发生过篡改，及时的发现数据内容的异常。

- 15 [75]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。

[76]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数据验证方法，应用于验证客户端，执行以下步骤：

[77]步骤 102，获取数据提供方公布的目标数据在区块链上的数据标识；其中，所述数据标识指示所述目标数据在所述区块链上的存储位置；

- 20 [78]步骤 104，基于所述数据标识确定所述目标数据是否已存储至所述区块链；

[79]步骤 106，如果所述目标数据已存储至所述区块链，从所述数据标识指示的存储位置上获取所述目标数据；其中，所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息；

[80]步骤 108，基于所述校验信息对获取到的所述目标数据进行真实性验证，并向数据

- 25 验证方输出验证结果。

[81]上述目标数据，具体可以包括任意形式的能够在区块链上进行存证，并且可以通过互联网进行公开发布的与真实世界中的实物对应的数字信息；

[82]例如，在一种场景中，上述目标数据具体可以是由线下的质检机构出具的商品质检

报告，而商家在通过电商平台发布商品时，可以将商品的图片与该商品的商品质检报告的图片一起进行公开发布。

[83]上述数据标识，具体可以包括能够指示区块链上存储的数据在区块链上的存储位置的任意形式的标识信息；

- 5 [84]例如，在示出的一种实施方式中，在区块链的分布式数据库中，数据通常是被收录在交易中，在区块链上的区块中进行存储，并且区块中存储的交易，通常会基于交易的交易 hash 值组织成 Merkle 树，因此为了便于数据检索，上述数据标识具体可以是收录数据的交易的交易 hash。通过交易 hash 可以快速定位到收录该数据的交易。当然，在实际应用中，上述数据标识具体也可以采用收录数据的交易的交易编号。

- 10 [85]在本说明书描述的区块链，具体可以包括任意类型的区块链网络。

[86]例如，在示出的一种实施方式中，上述区块链具体可以是一个由若干商家、质检机构、以及若干普通消费者组成的联盟链。质检机构作为数据上传方，可以通过上传客户端接入到联盟链上的任一节点设备，将商品质检报告以数字信息的形式上传至该节点设备，由该节点设备在区块链中发起针对该商品质检报告共识处理，并在共识通过后，将
15 该商品质检报告收录存储至区块链的分布式数据库。商家可以作为数据提供方，将由质检机构出具的商品质检报告通过电商平台进行公开发布；而普通的消费者在查看到商家公布的商品质检报告时，也可以通过验证客户端接入到联盟链上的任一节点设备，发起针对该商品质检报告的真实验证。

- [87]以下以上述目标数据为商品质检报告，上述区块链为由若干商家、质检机构、以及
20 若干普通消费者组成的联盟链构成的联盟链为例，对本说明书的技术方案进行详细说明。

[88]请参见图 2，图 2 为本说明书示出的一种联盟链的示意图。

- [89]如图 2 所示，区块链的运营方可以预先搭建一个由若干节点设备组成的联盟链，而商家、商品质检机构以及普通消费者，都可以在联盟链中进行注册，在取得在联盟链上的合法身份（比如取得联盟链为其分配的私钥公钥对）后，作为联盟成员接入上述联盟
25 链。

[90]其中，商家、商品质检机构以及普通消费者在联盟链中进行注册，以及作为联盟成员加入联盟链的具体实施过程，在本说明书中不再进行详述。

[91]请参见图 2，商品质检机构作为数据上传方，可以通过上传客户端接入到联盟链中的节点设备，将为商家委托的商品出具的商品质检报告以数字信息的形式上传至该节点

设备。

[92]而普通消费者作为数据验证方，可以通过验证客户端接入到联盟链中的节点设备，当普通的消费者在查看到商家公布的商品质检报告时，可以通过验证客户端发起针对该商品质检报告的真实性的验证。

5 [93]其中，需要说明的是，以上描述的上传客户端以及验证客户端，可以是 web 客户端（比如区块链浏览器）也可以是原生的 APP 应用，在本说明书中不进行特别限定。

[94]在本说明书中，商品质检机构可以针对需要上传的商品质检报告定义一种标准的数据存储格式。当商品质检机构在为商家委托的商品出具了商品质检报告后，可以将该商品质检报告组织成标准的数据存储格式，并基于商品质检机构持有的私钥进行签名后，
10 上传至该上传客户端接入的区块链节点设备。

[95]其中，在为商品质检报告定义的数据存储格式中，可以包含数据的原始内容、校验信息、以及辅助信息等三部分。上述校验信息，具体用于对数据进行真实性验证。而上述辅助信息，则可以是与上述真实性验证相关的辅助参数。

[96]在示出的一种实施方式中，上述校验信息具体可以为基于商品质检报告的原始内容
15 以及上述辅助信息进行 hash 计算得到的 hash 值。而上述辅助信息，具体可以包括数据上传方的身份标识、上传时间戳、上传地点等信息中的任一或者多个的组合。

[97]在这种情况下，为商品质检报告定义的数据存储格式，可以如下表 1 所示：

序号	字段名称	字段内容
1	内容字段	填充数据的原始内容
2	上传者身份字段	填充上传者的身份标识
3	上传时间字段	填充数据的上传时间戳
4	上传地点字段	填充数据的上传地点
5	校验信息字段	填充基于字段 1-4 计算出的 hash 值

表 1

[98]其中，上述内容字段中填充的数据的原始内容的具体形式，在本说明书中不进行特
20 别限定；例如，可以是图片的形式。

[99]上述上传者身份字段中填充的身份标识，具体可以采用任意形式的能够指示上传者身份的信息；例如，身份证号码、指纹信息、数字证书签名，等等。

[100] 上述上传时间字段中填充的时间标识,要以公认的世界时间为准，防止使用某地区时间相对其他不同时区的人,对同一时间理解不一致而引起的歧义；比如,北京时区相

对纽约时区，对同一时间的理解就会引起歧义。

[101] 上述上传地点字段中也要防止使用，可能引起歧义的地址描述；例如“中山路”，可能有很多城市都有中山路，最恰当的做法是使用经纬度坐标、GeoHash 等没有歧义的地址表达方式。

5 [102] 在本说明书中，当联盟链中的节点设备收到上述上传客户端上传的商品质检报告后，首先可以基于上述商品质检机构持有的私钥对应的公钥，对该商品质检报告的签名进行验证；如果签名验证通过，表明该商品质检报告为合法的商品质检机构上传的信息，此时可以进一步可以将该目标数据在区块链中进行发布，在经过联盟链中的节点设备的共识处理后，将上述商品质检报告存储至区块链的分布式数据库。

10 [103] 其中，联盟链中采用的共识算法，在本说明书中不进行特别限定；例如，可以采用诸如 pbft 等主流的适宜在联盟链中使用的共识算法，也可以由联盟链的运营方独立的开发相关的共识算法。

[104] 当上述商品质检报告被成功存储至区块链的分布式数据库后，区块链中的节点设备还可以通过上传客户端向商品质检机构，返回一个能够指示上述商品质检报告在区

15 块链上的存储位置的数据标识。

[105] 例如，在示出的一种实施方式中，上述数据标识具体可以是收录了该商品质检报告的交易的交易 hash 值。

[106] 在本说明书中，商品质检机构还可以将生成的商品质检报告，以及由联盟链中的节点设备返回的上述数据标识，发送给商家。而商家在收到商品质检机构发送的商品
20 质检报告以及上述数据标识后，可以通过网站向普通的消费者进行公布；例如，可以在电商平台中，与商品图片一起向消费者公布。

[107] 普通消费者在查看到商家公开发布的商品质检报告，以及该商品质检报告在区块链上的数据标识后，可以通过上述验证客户端对商家公布的该商品质检报告的真实

25 [108] 在示出的一种实施方式中，消费者在查看到商家公布的商品质检报告在区块链上的数据标识后，可以在上述验证客户端提供的用户界面中手动输入提交查看到的数据标识。而上述验证客户端可以获取用户手动输入的数据标识，然后基于获取到的数据标识，发起对上述商品质检报告的验证。

[109] 在示出的另一种实施方式中，商家在发布上述商品质检报告时，可以将该商品

质检报告以图形编码（比如二维码或者条形码）的形式，携带在公开发布的商品质检报告上；

[110] 例如，以上述数据标识为收录了该商品质检报告的交易的交易 hash 值为例，商家可以将该交易 hash 值对应的字符串作为编码信息，生成相应的图形编码，然后将生成的图形编码附着在公开发布的商品质检报告的图片之上。

[111] 在这种情况下，普通消费者可以通过上述验证客户端针对该图形编码进行扫描操作，由上述验证客户端对扫描得到的图形编码进行解析，来获取该图形编码中携带的上述数据标识，然后基于解析得到的数据标识，发起对上述商品质检报告的验证。

[112] 在本说明书中，当上述验证客户端获取到商家公布的商品质检报告在联盟链上的数据标识后，可以基于该数据标识来确定该商品质检报告，是否已经存储至联盟链的分布式数据库。

[113] 在示出的一种实施方式中，以上述数据标识为收录了该商品质检报告的交易的交易 hash 值为例，可以基于该交易 hash 值针对收录该商品质检报告的交易进行 SPV（Simplified Payment Verification, 简单支付验证）验证，来确定该交易是否已经被存储至联盟链的分布式数据库。

[114] 其中，SPV 是一种用于验证一笔交易是否已经在区块链的分布式数据库中已经存在的协议，以下对基于交易 hash 对交易进行 SPV 认证的具体过程进行详细描述。

[115] 在实际应用中，区块链中的区块，通常由区块头和区块体（包含交易）两部分组成。区块中收录的交易，通常会以交易的 hash 值的形式，组织成 Merkle 树。

[116] 其中，将区块中收录的交易的 hash 值组织成 Merkle 树的具体过程，在本说明书中不进行特别限定，本领域技术人员在将本说明书的技术方案付诸实现时，可以参考相关技术中的记载。

[117] 在基于交易 hash 值对交易进行 SPV 验证时，首先可以获取该交易在包含该交易的目标区块的 Merkle 树中的 Merkle 认证路径；

[118] 其中，上述 Merkle 认证路径，具体是指一笔交易的交易 hash 值，在上述 Merkle 树中进行逐级遍历查找经过的路径上的节点所对应的兄弟节点（即相邻节点）所组成的路径。在针对一笔交易进行 SPV 认证的过程中，该交易的 Merkle 认证路径可以作为反向计算该交易所在的 Merkle 树的根节点对应的 hash 值的计算参数。

[119] 需要说明的是，上述 Merkle 认证路径，具体可以由用户手动提交，也可以是由上述验证客户端向区块链主动查询；

[120] 例如，上述验证客户端主动查询获取该交易在包含该交易的目标区块的 Merkle 树中的 Merkle 认证路径时，首先可以基于交易的交易 hash 值定位该交易所在的目标区块；

[121] 其中，基于交易 hash 值定位交易所在的区块的过程，在本说明书中不再进行详述；比如，在相关技术中，可以通过部署布隆过滤器，来定位交易的 hash 值所在的区块。当定位出交易所在的区块后，可以进一步从定位出的该区块的 Merkle 树中，查找出该交易在该 Merkle 树中的 Merkle 认证路径。

10 [122] 在本说明书中，当获取到该交易在包含该交易的目标区块的 Merkle 树中的 Merkle 认证路径后，可以基于 SPV 协议规定的计算过程，来计算出上述目标区块的区块头的 hash 值（即上述目标区块的 Merkle 树的根节点的 hash 值）；然后，确定计算出的上述目标区块的区块头的 hash 值，与该目标区块的区块头中保存的 hash 值是否匹配；如果匹配，可以确定该交易包含在该目标区块中；也即，上述商品质检报告已经成功收
15 录存储至联盟链的分布式数据库。反之，如果不匹配，表明该交易并未包含在目标区块中；也即，上述商品质检报告未成功收录存储至联盟的分布式数据库。

[123] 在本说明书中，当通过以上的实施过程，确认上述商品质检报告，已经存储至联盟链的分布式数据库，此时可以进一步从上述数据标识指示的存储位置上获取上述商品质检报告。

20 [124] 例如，仍以上述数据标识为收录了该商品质检报告的交易的交易 hash 值为例，可以基于该交易 hash 定位出对应的交易，然后从定位出的该交易中读取收录在该交易中的商品质检报告。

[125] 当从上述数据标识指示的存储位置上获取到上述商品质检报告后，可以进一步读取该商品质检报告的标准存储格式中所携带的上述校验信息，然后基于上述校验信息，
25 对从联盟链的分布式数据库中获取到的商品质检报告进行真实性验证。

[126] 其中，在本说明书中，上述真实性验证，具体是指对上述商品质检报告中记录的原始内容是否被篡改进行验证；

[127] 例如，在一些场景下，商品质检机构在出具了商品质检报告后，可以将商品质检报告组织成标准的数据存储格式后发送给商家，由商家进行上传；在这种情况下，一

些信誉较差的商家，可能对商品质检报告中的某些字段在上传之前进行恶意修改。

[128] 又如，在另一些场景下，上述商品质检报告在上传传输的过程中，也可能被非法截获后，对其中的某些字段进行恶意修改。

[129] 通过引入对链上的商品质检报告的真实验证过程，可以让普通的消费者及时的发现以上列举出的对商品质检报告进行恶意修改的情形。

[130] 在本说明书中，上述校验客户端在基于上述商品质检报告中携带的校验信息，对从联盟链的分布式数据库中获取到的商品质检报告进行真实性验证时，具体可以执行本地搭载的校验程序来实现，也可以通过远程调用联盟链上部署的智能合约来实现。

[131] 在示出的一种实施方式中，上述校验客户端上可以搭载用于对上述商品质检报告进行真实性验证的验证程序；

[132] 例如，针对上述商品质检报告的真实验证规则，可以由作为数据上传方的商品质检机构进行公开发布，而上述验证客户端的开发人员，可以根据上述商品质检机构发布的验证规则，在上述验证客户端的软件环境中开发相应的程序执行代码（比如，与上述验证规则的执行逻辑对应的功能函数）。

[133] 当上述校验客户端确认上述商品质检报告，已经存储至联盟链的分布式数据库上，并获取到联盟链上存储的商品质检报告后，可以从获取到的上述商品质检报告中读取上述校验信息；例如，以上述表 1 示出的数据存储格式为例，可以从表 1 中示出的字段 5 中读取上述校验信息。

[134] 进一步的，可以执行本地搭载的上述验证程序，基于读取到的校验信息对从联盟链上获取到的商品质检报告进行真实性验证。

[135] 在示出的一种实施方式中，上述联盟链中也可以预先部署智能合约，并在该智能合约中声明用于对上述商品质检报告进行真实性验证的验证程序；

[136] 例如，联盟链的运营方，可以基于作为数据上传方的商品质检机构公开发布的针对上述商品质检报告的真实验证规则，来开发相应的合约代码，并部署智能合约，然后将智能合约在联盟链中进行发布，由联盟链中的节点设备进行共识处理，并在共识通过后存储至联盟链的分布式数据库，供接入联盟链的客户端进行远程调用。

[137] 当上述校验客户端确认上述商品质检报告，已经存储至联盟链的分布式数据库上，并获取到联盟链上存储的商品质检报告后，可以从获取到的上述商品质检报告中读

取上述校验信息，并基于上述校验信息构建一笔交易提交给上述智能合约，发起针对上述智能合约的调用，执行上述智能合约中声明的验证程序，基于读取到的校验信息对从联盟链上获取到的商品质检报告进行真实性验证。

5 [138] 在示出的一种实施方式中，以上述校验信息为基于商品质检报告的原始内容以及上述商品质检报告的数据存储格式中携带的上述辅助信息进行 hash 计算得到的 hash 值为例，在这种情况下，通过执行上述验证客户端本地搭载的验证程序，或者远程调用上述智能合约，执行上述智能合约中声明的验证程序，对上述商品质检报告进行真实性验证时，可以针对从联盟链上获取到的上述商品质检报告的数据存储格式中携带的，上述商品质检报告的原始内容以及上述辅助信息重新进行 hash 计算得到 hash 值。

10 [139] 进一步的，可以将计算出的 hash 值和上述商品质检报告的数据存储格式中携带的作为上述校验信息的 hash 值进行匹配，以确定计算出的 hash 值与上述商品质检报告的数据存储格式中携带的作为上述校验信息的 hash 值是否相同；如果二者相同，表明联盟链上存储的上述商品质检报告中携带的内容并未被篡改，此时上述商品质检报告通过真实性验证；当然，如果二者不相同，表明联盟链上存储的上述商品质检报告中携带的内容发生了篡改，此时上述商品质检报告未通过真实性验证。

[140] 当完成针对上述商品质检报告的真实验证后，可以将真实性验证结果，通过上述验证客户端向普通的消费者进行输出，此时该消费者可以参照验证客户端输出的针对上述商品质检报告的真实验证结果，来确定是否购买该商品。

20 [141] 在本说明书中，对于从联盟链上获取到的上述商品质检报告，还可以通过上述验证客户端向普通的消费者进行输出，使得普通的消费者可以将联盟链上的存储的商品质检报告，与商家公布的商品质检报告进行比对。

[142] 通过这种方式，使得消费者可以直观的查看到，商家公布的商品质检报告中记录的信息，是否与商品质检机构上传的商品质检报告记录的信息一致。

25 [143] 其中，在实际应用中，可以在从联盟链上获取到上述商品质检报告之时，立即向消费者输出上述商品质检报告；也可以在完成针对上述商品质检报告的真实验证，并且通过上述验证客户端将真实性验证结果向普通的消费者进行输出之后，有选择性的向消费者进行输出；

[144] 例如，可以在上述真实性验证结果表明，上述商品质检报告通过了真实性验证的情况下，再将从联盟链上获取到的上述商品质检报告向消费者输出展示。相反的，如

果上述商品质检报告并没有通过真实性验证,则不再将上述商品质检报告向消费者进行输出。通过这种方式,可以确保让消费者只能查看到通过了真实性验证的商品质检报告。

[145] 需要强调的是,以上实施例仅以上述述目标数据为商品质检报告为例进行了说明;显然,在实际应用中,上述目标数据也可以是商品质检报告以外的其它形式的数据。

- 5 当上述目标数据为商品质检报告以外的其它形式的数据时,本领域技术人员完全可以参照以上实施例中记载的实施过程,来等同实施本说明书中记载的技术方案,在本说明书中不再进行赘述。

- [146] 通过以上技术方案可见,一方面,基于数据提供方公布的数据标识,来确定上述目标数据是否已存储至所述区块链,可以对数据提供方发布的信息的真实性进行验证,使得数据验证方可以及时的发现数据提供方发布的,在区块链上并不存在真实的数据存储记录的虚假数据标识;
- 10

[147] 例如,如果通过商家公布的上述数据标识,确定出区块链上并未存储与该数据标识对应的商品质检报告,表明该商家公布的该数据标识,可能为一个虚假的数据标识,也即商家公布的商品质检报告可能并不是真实存在的。

- 15 [148] 另一方面,在确定上述目标数据已存储至区块链的前提下,基于区块链上存储的上述目标数据中携带的校验信息,对区块链上的目标数据进行真实性验证,使得数据验证方可以确认出区块链上的目标数据的内容是否发生过篡改,及时的发现数据内容的异常。

- [149] 例如,如果区块链上存储的商品质检报告并未通过真实性验证,表明该商品质检报告,可能在上传之前或者在上传的传输过程中被非法篡改,从而使得消费者可以及时的得知这一异常。
- 20

- [150] 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数据验证装置的实施例。本说明书的基于区块链的数据验证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数据验证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。
- 25

[151] 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数据验证装置的框图。

[152] 请参考图4, 所述基于区块链的数据验证装置40可以应用在前述图3所示的电子设备中, 包括有: 第一获取模块401、确定模块402、第二获取模块403和验证模块403。

5 [153] 第一获取模块401, 获取数据提供方公布的目标数据在区块链上的数据标识; 其中, 所述数据标识指示所述目标数据在所述区块链上的存储位置;

[154] 确定模块402, 基于所述数据标识确定所述目标数据是否已存储至所述区块链;

[155] 第二获取模块403, 如果所述目标数据已存储至所述区块链, 从所述数据标识指示的存储位置上获取所述目标数据; 其中, 所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息;

10 [156] 验证模块404, 基于所述校验信息对获取到的所述目标数据进行真实性验证, 并向数据验证方输出验证结果。

[157] 在本实施例中, 数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码;

15 [158] 所述第一获取模块401:

[159] 扫描并解析所述图形编码, 以获取所述目标数据在区块链上的数据标识。

[160] 在本实施例中, 所述数据标识为收录所述目标数据的交易的交易hash值;

[161] 所述确定模块402:

[162] 基于收录所述目标数据的交易的交易hash值针对所述交易进行SPV验证, 以确
20 定所述交易是否已存储至所述区块链。

[163] 在本实施例中, 所述验证模块404:

[164] 执行搭载的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证;

[165] 或者, 调用发布在所述区块链上的智能合约, 执行所述智能合约中声明的验证
25 程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证。

[166] 在本实施例中, 所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息; 所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行

hash 计算得到的 hash 值;

[167] 所述验证模块 404 进一步:

[168] 针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值; 确定计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同;

- 5 如果相同, 确定获取到的所述目标数据通过真实性验证; 如果不相同, 确定获取到的所述目标数据未通过真实性验证。

[169] 在本实施例中, 所述辅助信息包括以下信息中的任一或者多个的组合:

[170] 数据上传方的身份标识;

[171] 所述目标数据的上传时间戳;

- 10 [172] 所述目标数据的上传地点。

[173] 在本实施例中, 所述第二获取模块 403 进一步:

[174] 将从所述数据标识指示的存储位置上获取到的所述目标数据, 向所述数据验证方输出, 以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行比对。

- 15 [175] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程, 在此不再赘述。

[176] 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。

- 20 [177] 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。

[178] 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。

5 [179] 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数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[180] 获取数据提供方公布的目标数据在区块链上的数据标识；其中，所述数据标识指示所述目标数据在所述区块链上的存储位置；

[181] 基于所述数据标识确定所述目标数据是否已存储至所述区块链；

10 [182] 如果所述目标数据已存储至所述区块链，从所述数据标识指示的存储位置上获取所述目标数据；其中，所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息；

[183] 基于所述校验信息对获取到的所述目标数据进行真实性验证，并向数据验证方输出验证结果。

15 [184] 在本实施例中，数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码；

[185] 通过读取并执行所述存储器存储的与基于区块链的数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[186] 扫描并解析所述图形编码，以获取所述目标数据在区块链上的数据标识。

[187] 在本实施例中，所述数据标识为收录所述目标数据的交易的交易 hash 值；

20 [188] 通过读取并执行所述存储器存储的与基于区块链的数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[189] 基于收录所述目标数据的交易的交易 hash 值针对所述交易进行 SPV 验证，以确定所述交易是否已存储至所述区块链。

25 [190] 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数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[191] 执行搭载的验证程序，基于所述校验信息对获取到的所述目标数据进行真实性验证；

[192] 或者，调用发布在所述区块链上的智能合约，执行所述智能合约中声明的验证程序，基于所述校验信息对获取到的所述目标数据进行真实性验证。

[193] 在本实施例中，所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息；所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行
5 hash 计算得到的 hash 值；

[194] 通过读取并执行所述存储器存储的与基于区块链的数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[195] 针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值；确定计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同；
10 如果相同，确定获取到的所述目标数据通过真实性验证；如果不相同，确定获取到的所述目标数据未通过真实性验证。

[196] 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数据验证的控制逻辑对应的机器可执行指令，所述处理器被促使：

[197] 将从所述数据标识指示的存储位置上获取到的所述目标数据，向所述数据验证
15 方输出，以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行比对。

[198] 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
20 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，本说明书的真正范围和精神由下面的权利要求指出。

[199] 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。

25 [200] 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护的范围之内。

权利要求书

1. 一种基于区块链的数据验证方法, 所述方法包括:
获取数据提供方公布的目标数据在区块链上的数据标识; 其中, 所述数据标识指示所述目标数据在所述区块链上的存储位置;
- 5 基于所述数据标识确定所述目标数据是否已存储至所述区块链;
如果所述目标数据已存储至所述区块链, 从所述数据标识指示的存储位置上获取所述目标数据; 其中, 所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息;
基于所述校验信息对获取到的所述目标数据进行真实性验证, 并向数据验证方输出
10 验证结果。
2. 根据权利要求 1 所述的方法, 数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码;
所述获取数据提供方公布的目标数据在区块链上的数据标识, 包括:
扫描并解析所述图形编码, 以获取所述目标数据在区块链上的数据标识。
- 15 3. 根据权利要求 1 或 2 所述的方法, 所述数据标识为收录所述目标数据的交易的交易 hash 值;
所述基于所述数据标识确定所述目标数据是否已存储至所述区块链, 包括:
基于收录所述目标数据的交易的交易 hash 值针对所述交易进行 SPV 验证, 以确定所述交易是否已存储至所述区块链。
- 20 4. 根据权利要求 1 所述的方法, 所述基于所述校验信息对获取到的所述目标数据进行真实性验证, 包括:
执行搭载的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证;
或者, 调用发布在所述区块链上的智能合约, 执行所述智能合约中声明的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证。
- 25 5. 根据权利要求 4 所述的方法, 所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息; 所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到的 hash 值;
所述基于所述校验信息对获取到的所述目标数据进行真实性验证, 包括:
针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值; 确定
30 计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同; 如果相同, 确定获取到的所述目标数据通过真实性验证; 如果不相同, 确定获取到的所述

目标数据未通过真实性验证。

6. 根据权利要求 5 所述的方法, 所述辅助信息包括以下信息中的任一或者多个的组合:

数据上传方的身份标识;

5 所述目标数据的上传时间戳;

所述目标数据的上传地点。

7. 根据权利要求 1 所述的方法, 还包括:

将从所述数据标识指示的存储位置上获取到的所述目标数据, 向所述数据验证方输出, 以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行
10 比对。

8. 一种基于区块链的数据验证装置, 所述装置包括:

第一获取模块, 获取数据提供方公布的目标数据在区块链上的数据标识; 其中, 所述数据标识指示所述目标数据在所述区块链上的存储位置;

确定模块, 基于所述数据标识确定所述目标数据是否已存储至所述区块链;

15 第二获取模块, 如果所述目标数据已存储至所述区块链, 从所述数据标识指示的存储位置上获取所述目标数据; 其中, 所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息;

验证模块, 基于所述校验信息对获取到的所述目标数据进行真实性验证, 并向数据验证方输出验证结果。

20 9. 根据权利要求 8 所述的装置, 数据提供方公布的目标数据上携带基于所述数据标识生成的图形编码;

所述第一获取模块:

扫描并解析所述图形编码, 以获取所述目标数据在区块链上的数据标识。

25 10. 根据权利要求 8 或 9 所述的方法, 所述数据标识为收录所述目标数据的交易的交易 hash 值;

所述确定模块:

基于收录所述目标数据的交易的交易 hash 值针对所述交易进行 SPV 验证, 以确定所述交易是否已存储至所述区块链。

11. 根据权利要求 8 所述的装置, 所述验证模块:

30 执行搭载的验证程序, 基于所述校验信息对获取到的所述目标数据进行真实性验证; 或者, 调用发布在所述区块链上的智能合约, 执行所述智能合约中声明的验证程序,

基于所述校验信息对获取到的所述目标数据进行真实性验证。

12. 根据权利要求 11 所述的装置, 所述区块链上存储的所述目标数据中还包括与所述真实性验证相关的辅助信息; 所述校验信息为基于所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到的 hash 值;

5 所述验证模块进一步:

针对所述目标数据的原始内容以及所述辅助信息进行 hash 计算得到 hash 值; 确定计算出的 hash 值与在所述区块链上存储的所述目标数据中携带的 hash 值是否相同; 如果相同, 确定获取到的所述目标数据通过真实性验证; 如果不相同, 确定获取到的所述目标数据未通过真实性验证。

10 13. 根据权利要求 12 所述的装置, 所述辅助信息包括以下信息中的任一或者多个的组合:

数据上传方的身份标识;

所述目标数据的上传时间戳;

所述目标数据的上传地点。

15 14. 根据权利要求 8 所述的装置, 所述第二获取模块进一步:

将从所述数据标识指示的存储位置上获取到的所述目标数据, 向所述数据验证方输出, 以由所述数据验证方将输出的所述目标数据与所述数据提供方公布的目标数据进行比对。

15. 一种电子设备, 包括:

20 处理器;

用于存储机器可执行指令的存储器;

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数据验证的控制逻辑对应的机器可执行指令, 所述处理器被促使:

获取数据提供方公布的目标数据在区块链上的数据标识; 其中, 所述数据标识指示

25 所述目标数据在所述区块链上的存储位置;

基于所述数据标识确定所述目标数据是否已存储至所述区块链;

如果所述目标数据已存储至所述区块链, 从所述数据标识指示的存储位置上获取所述目标数据; 其中, 所述区块链上存储的所述目标数据中携带用于对所述目标数据进行真实性验证的校验信息;

30 基于所述校验信息对获取到的所述目标数据进行真实性验证, 并向数据验证方输出验证结果。