(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111241569 B
(45)授权公告日 2021.03.30

(21)申请号 202010329555.6
(22)申请日 2020.04.24
(65)同一申请的已公布的文献号
申请公布号 CN 111241569 A
(43)申请公布日 2020.06.05
(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11
(72)发明人 韩喆 黄琪
(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 王戈
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/64(2013.01)

(56)对比文件
CN 110535647 A,2019.12.03
CN 106973054 A,2017.07.21

审查员 李佳曦

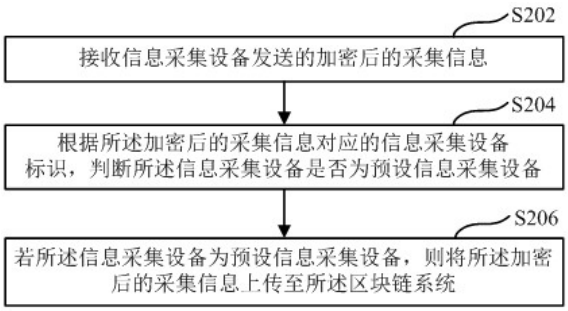
权利要求书6页 说明书17页 附图4页

(54)发明名称

一种信息处理的方法、装置及设备

(57)摘要

本说明书实施例公开了一种信息处理方法、装置及设备。方案包括:接收信息采集设备发送的加密后的采集信息;根据所述加密后的采集信息对应的信息采集设备标识,判断所述信息采集设备是否为预设信息采集设备;若所述信息采集设备为预设信息采集设备,则将所述加密后的采集信息上传至所述区块链系统。



CN 111241569 B

1.一种信息处理方法,包括:

信息管理设备接收信息采集设备发送的加密后的采集信息;所述信息采集设备包括用于进行仓储管理的采集货物信息的设备;

根据所述加密后的采集信息对应的信息采集设备标识,判断所述信息采集设备是否为预设信息采集设备;所述信息采集设备标识包括设备ID、设备序列号中至少一种;所述预设信息采集设备是与所述信息管理设备具有绑定关系的设备;所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的,具体包括:所述信息管理设备接收所述信息采集设备发送的第一绑定码;判断所述第一绑定码是否与预设绑定码相同;若所述第一绑定码与所述预设绑定码相同,将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识;按照预设规则,根据所述第一绑定码生成第二绑定码;将所述第二绑定码发送给所述信息采集设备,所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证,若验证通过,则所述信息采集设备与所述信息管理设备建立所述绑定关系;其中,所述按照预设规则,根据所述第一绑定码生成第二绑定码,具体包括:在所述第一绑定码的基础上添加特定信息构成所述第二绑定码;

若所述信息采集设备为预设信息采集设备,则将所述加密后的采集信息上传至区块链系统;所述区块链系统不包括所述信息采集设备。

2.根据权利要求1所述的方法,所述判断所述信息采集设备是否为预设信息采集设备,具体包括:

判断所述信息采集设备的信息采集设备标识是否与所述预设信息采集设备标识相同。

3.根据权利要求1所述的方法,所述将所述加密后的采集信息上传至区块链系统之前,还包括:

获取所述信息采集设备的所述信息采集设备标识;

基于所述信息采集设备标识,查找所述信息采集设备的公钥;

基于所述公钥,对所述加密后的采集信息进行签名验证,用于判断所述加密后的采集信息是否为所述信息采集设备传输给所述信息管理设备的;

若所述签名验证通过,则将所述加密后的采集信息上传至区块链系统。

4.根据权利要求1所述的方法,所述将所述加密后的采集信息上传至区块链系统之前,还包括:

获取所述加密后的采集信息的时间戳;

判断所述时间戳表示的时间与所述信息管理设备获取所述时间戳的时间的时间差值是否小于或等于预设时间差值;

若所述时间戳表示的时间与所述信息管理设备获取所述时间戳的时间的时间差值小于或等于所述预设时间差值,则将所述加密后的采集信息上传至区块链系统。

5.根据权利要求1所述的方法,还包括:

获取根据所述加密后的采集信息生成的链上数据的哈希值;

生成所述哈希值、所述信息采集设备标识与信息管理设备标识之间的关联关系数据;

存储所述关联关系数据。

6.根据权利要求1所述的方法,所述采集信息具体包括图像采集设备采集的图像信息,以及所述图像信息中的目标物信息、目标物数量信息、目标物位置信息中至少一种信息。

7.根据权利要求1所述的方法，所述信息采集设备包括扫码模块，所述采集信息具体包括所述扫码模块采集的码信息。

8.根据权利要求1所述的方法，所述信息采集设备为用于进行仓储管理的采集货物信息的设备，所述货物信息包括货物的数量信息、名称信息、位置信息中的至少一种信息。

9.一种信息处理方法，包括：

区块链系统获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；所述信息采集设备包括用于进行仓储管理的采集货物信息的设备；所述信息采集设备是与所述信息管理设备具有绑定关系的设备；所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的，具体包括：所述信息管理设备接收所述信息采集设备发送的第一绑定码；判断所述第一绑定码是否与预设绑定码相同；若所述第一绑定码与所述预设绑定码相同，将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；按照预设规则，根据所述第一绑定码生成第二绑定码；将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证，若验证通过，则所述信息采集设备与所述信息管理设备建立所述绑定关系；其中，所述信息采集设备标识包括设备ID、设备序列号中至少一种；所述区块链系统不包括所述信息采集设备；其中，所述按照预设规则，根据所述第一绑定码生成第二绑定码，具体包括：在所述第一绑定码的基础上添加特定信息构成所述第二绑定码；

对所述采集信息进行验签处理；

将通过验签的所述加密后的采集信息保存至区块链。

10.根据权利要求9所述的方法，所述对所述采集信息进行验签处理，具体包括：

确定所述信息采集设备的信息采集设备标识；

基于所述信息采集设备标识，查找所述信息采集设备的公钥；

利用所述公钥对所述加密后的采集信息进行签名验证；

若所述签名验证通过，则调用智能合约将所述加密后的采集信息保存至区块链。

11.一种信息处理方法，包括：

获取采集信息；

对所述采集信息进行加密，得到加密后的采集信息；

发送所述加密后的采集信息给信息管理设备；所述加密后的采集信息与信息采集设备标识相对应，所述信息采集设备标识用于所述信息管理设备判断信息采集设备为预设信息采集设备时，将所述加密后的采集信息上传至区块链系统；所述信息采集设备包括用于进行仓储管理的采集货物信息的设备；所述信息采集设备标识包括设备ID、设备序列号中至少一种；所述区块链系统不包括所述信息采集设备；所述预设信息采集设备是与所述信息管理设备具有绑定关系的设备；所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的，具体包括：所述信息管理设备接收所述信息采集设备发送的第一绑定码；判断所述第一绑定码是否与预设绑定码相同；若所述第一绑定码与所述预设绑定码相同，将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；按照预设规则，根据所述第一绑定码生成第二绑定码；将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证，若验证通过，则所述信息采集设备与所述信息管理设备建立所述绑定关系；其中，所述按照预设规则，根据所

述第一绑定码生成第二绑定码，具体包括：在所述第一绑定码的基础上添加特定信息构成所述第二绑定码。

12.根据权利要求11所述的方法，还包括：

发送信息采集设备标识给所述信息管理设备，以便所述信息管理设备基于所述信息采集设备标识查找所述信息采集设备的公钥。

13.根据权利要求11所述的方法，所述获取采集信息之后，还包括：

对所述采集信息添加时间戳，所述时间戳表征所述采集信息被采集的时间，用于所述信息管理设备对所述采集信息进行验证。

14.根据权利要求11所述的方法，所述采集信息具体包括图像采集设备采集的图像信息，以及所述图像信息中的目标物信息、目标物数量信息、目标物位置信息中至少一种信息。

15.根据权利要求11所述的方法，所述信息采集设备包括扫码模块，所述采集信息具体包括所述扫码模块采集的码信息。

16.根据权利要求11所述的方法，所述信息采集设备为用于进行仓储管理的采集货物信息的设备，所述货物信息包括货物的数量信息、名称信息、位置信息中的至少一种信息。

17.一种信息处理装置，包括：

采集信息接收模块，用于接收信息采集设备发送的加密后的采集信息；所述信息采集设备包括用于进行仓储管理的采集货物信息的设备；

采集设备判断模块，用于根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；所述信息采集设备标识包括设备ID、设备序列号中至少一种；所述预设信息采集设备是与信息管理设备具有绑定关系的设备；所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的，具体包括：所述信息管理设备接收所述信息采集设备发送的第一绑定码；判断所述第一绑定码是否与预设绑定码相同；若所述第一绑定码与所述预设绑定码相同，将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；按照预设规则，根据所述第一绑定码生成第二绑定码；将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证，若验证通过，则所述信息采集设备与所述信息管理设备建立所述绑定关系；其中，所述按照预设规则，根据所述第一绑定码生成第二绑定码，具体包括：在所述第一绑定码的基础上添加特定信息构成所述第二绑定码；

信息上链模块，用于若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至区块链系统，所述区块链系统不包括所述信息采集设备。

18.一种信息处理装置，包括：

采集信息获取模块，用于获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；所述信息采集设备包括用于进行仓储管理的采集货物信息的设备；所述信息采集设备是与所述信息管理设备具有绑定关系的设备；所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的，具体包括：所述信息管理设备接收所述信息采集设备发送的第一绑定码；判断所述第一绑定码是否与预设绑定码相同；若所述第一绑定码与所述预设绑定码相同，将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；按照预设规则，根据所述第一绑定码

生成第二绑定码;将所述第二绑定码发送给所述信息采集设备,所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证,若验证通过,则所述信息采集设备与所述信息管理设备建立所述绑定关系;其中,所述信息采集设备标识包括设备ID、设备序列号中至少一种;获取所述加密后的采集信息的区块链系统不包括所述信息采集设备;其中,所述按照预设规则,根据所述第一绑定码生成第二绑定码,具体包括:在所述第一绑定码的基础上添加特定信息构成所述第二绑定码;

信息验签模块,用于对所述采集信息进行验签处理;

信息保存模块,用于将通过验签的所述加密后的采集信息保存至区块链。

19.根据权利要求18所述的装置,所述信息验签模块,具体用于:

确定所述信息采集设备的信息采集设备标识;

基于所述信息采集设备标识,查找所述信息采集设备的公钥;

利用所述公钥对所述加密后的采集信息进行签名验证;

若所述签名验证通过,则调用智能合约将所述加密后的采集信息保存至区块链。

20.一种信息处理装置,包括:

信息获取模块,用于获取采集信息;

信息加密模块,用于对所述采集信息进行加密,得到加密后的采集信息;

信息发送模块,用于发送所述加密后的采集信息给信息管理设备;所述加密后的采集信息与信息采集设备标识相对应,所述信息采集设备标识用于所述信息管理设备判断信息采集设备为预设信息采集设备时,将所述加密后的采集信息上传至区块链系统;所述信息采集设备包括用于进行仓储管理的采集货物信息的设备;所述信息采集设备标识包括设备ID、设备序列号中至少一种;所述区块链系统不包括所述信息采集设备;所述预设信息采集设备是与所述信息管理设备具有绑定关系的设备;所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的,具体包括:所述信息管理设备接收所述信息采集设备发送的第一绑定码;判断所述第一绑定码是否与预设绑定码相同;若所述第一绑定码与所述预设绑定码相同,将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识;按照预设规则,根据所述第一绑定码生成第二绑定码;将所述第二绑定码发送给所述信息采集设备,所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证,若验证通过,则所述信息采集设备与所述信息管理设备建立所述绑定关系;其中,所述按照预设规则,根据所述第一绑定码生成第二绑定码,具体包括:在所述第一绑定码的基础上添加特定信息构成所述第二绑定码。

21.一种信息处理设备,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

接收信息采集设备发送的加密后的采集信息;所述信息采集设备包括用于进行仓储管理的采集货物信息的设备;

根据所述加密后的采集信息对应的信息采集设备标识,判断所述信息采集设备是否为预设信息采集设备;所述信息采集设备标识包括设备ID、设备序列号中至少一种;所述预设

信息采集设备是与信息管理设备具有绑定关系的设备;所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的,具体包括:所述信息管理设备接收所述信息采集设备发送的第一绑定码;判断所述第一绑定码是否与预设绑定码相同;若所述第一绑定码与所述预设绑定码相同,将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识;按照预设规则,根据所述第一绑定码生成第二绑定码;将所述第二绑定码发送给所述信息采集设备,所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证,若验证通过,则所述信息采集设备与所述信息管理设备建立所述绑定关系;其中,所述按照预设规则,根据所述第一绑定码生成第二绑定码,具体包括:在所述第一绑定码的基础上添加特定信息构成所述第二绑定码;

若所述信息采集设备为预设信息采集设备,则将所述加密后的采集信息上传至区块链系统,所述区块链系统不包括所述信息采集设备。

22.一种信息处理设备,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

获取信息管理设备上传的加密后的采集信息;所述采集信息是信息采集设备采集后上传至所述信息管理设备的;所述信息采集设备包括用于进行仓储管理的采集货物信息的设备;所述信息采集设备是与所述信息管理设备具有绑定关系的设备;所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的,具体包括:所述信息管理设备接收所述信息采集设备发送的第一绑定码;判断所述第一绑定码是否与预设绑定码相同;若所述第一绑定码与所述预设绑定码相同,将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识;按照预设规则,根据所述第一绑定码生成第二绑定码;将所述第二绑定码发送给所述信息采集设备,所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证,若验证通过,则所述信息采集设备与所述信息管理设备建立所述绑定关系;其中,所述信息采集设备标识包括设备ID、设备序列号中至少一种;获取所述加密后的采集信息的区块链系统不包括所述信息采集设备;其中,所述按照预设规则,根据所述第一绑定码生成第二绑定码,具体包括:在所述第一绑定码的基础上添加特定信息构成所述第二绑定码;

对所述采集信息进行验签处理;

将通过验签的所述加密后的采集信息保存至区块链。

23.一种信息处理设备,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

获取采集信息;

对所述采集信息进行加密,得到加密后的采集信息;

发送所述加密后的采集信息给信息管理设备;所述加密后的采集信息与信息采集设备

标识相对应，所述信息采集设备标识用于所述信息管理设备判断信息采集设备为预设信息采集设备时，将所述加密后的采集信息上传至区块链系统；所述信息采集设备包括用于进行仓储管理的采集货物信息的设备；所述信息采集设备标识包括设备ID、设备序列号中至少一种；所述区块链系统不包括所述信息采集设备；所述预设信息采集设备是与所述信息管理设备具有绑定关系的设备；所述绑定关系为所述信息采集设备与所述信息管理设备完成双方验证后确定的，具体包括：所述信息管理设备接收所述信息采集设备发送的第一绑定码；判断所述第一绑定码是否与预设绑定码相同；若所述第一绑定码与所述预设绑定码相同，将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；按照预设规则，根据所述第一绑定码生成第二绑定码；将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证，若验证通过，则所述信息采集设备与所述信息管理设备建立所述绑定关系；其中，所述按照预设规则，根据所述第一绑定码生成第二绑定码，具体包括：在所述第一绑定码的基础上添加特定信息构成所述第二绑定码。

一种信息处理的方法、装置及设备

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及一种信息处理的方法、装置及设备。

背景技术

[0002] 随着计算机技术的发展，先进的技术给我们带来了便利，同样也带来了新的问题。例如，在仓储管理方面，传统的仓储管理一般主要依靠人工管理，例如，依靠人工清点货物数量、填写货物清单等，而随着科技水平的不断提高，目前通常可以使用扫码器、摄像头或传感器等设备对仓库中货物信息进行采集，可以减少了人工，提高数据采集的效率，但通常采集的信息是通过网络进行传输，在传输过程中可能会遭到非法攻击，威胁信息的安全性。

[0003] 因此，如何确保信息安全性是本领域亟待解决的技术问题。

发明内容

[0004] 有鉴于此，本申请实施例中提供了一种信息处理方法、装置及设备，可用于提高信息的安全性。

[0005] 为解决上述技术问题，本说明书实施例是这样实现的：

[0006] 本说明书实施例中提供的一种信息处理方法，包括：

[0007] 接收信息采集设备发送的加密后的采集信息；

[0008] 根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0009] 若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0010] 本说明书实施例中提供的一种信息处理方法，包括：

[0011] 获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0012] 对所述采集信息进行验签处理；

[0013] 将通过验签的所述加密后的采集信息保存至区块链。

[0014] 本说明书实施例中提供的一种信息处理方法，包括：

[0015] 获取采集信息；

[0016] 对所述采集信息进行加密，得到加密后的采集信息；

[0017] 发送所述加密后的采集信息给信息管理设备；所述加密后的采集信息与信息采集设备标识相对应，所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备时，将所述加密后的采集信息上传至区块链系统。

[0018] 本说明书实施例中提供的一种信息处理装置，包括：

[0019] 采集信息接收模块，用于接收信息采集设备发送的加密后的采集信息；

[0020] 采集设备判断模块，用于根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0021] 信息上链模块，用于若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0022] 本说明书实施例中提供的一种信息处理装置，包括：

[0023] 采集信息获取模块，用于获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0024] 信息验签模块，用于对所述采集信息进行验签处理；

[0025] 信息保存模块，用于将通过验签的所述加密后的采集信息保存至区块链。

[0026] 本说明书实施例中提供的一种信息处理装置，包括：

[0027] 信息获取模块，用于获取采集信息；

[0028] 信息加密模块，用于对所述采集信息进行加密，得到加密后的采集信息；

[0029] 信息发送模块，用于发送所述加密后的采集信息给信息管理设备；所述加密后的采集信息与信息采集设备标识相对应，所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备，将所述加密后的采集信息上传至区块链系统。

[0030] 本说明书实施例中提供的一种信息处理设备，包括：

[0031] 至少一个处理器；以及，

[0032] 与所述至少一个处理器通信连接的存储器；其中，

[0033] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0034] 接收信息采集设备发送的加密后的采集信息；

[0035] 根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0036] 若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0037] 本说明书实施例中提供的一种信息处理设备，包括：

[0038] 至少一个处理器；以及，

[0039] 与所述至少一个处理器通信连接的存储器；其中，

[0040] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0041] 获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0042] 对所述采集信息进行验签处理；

[0043] 将通过验签的所述加密后的采集信息保存至区块链。

[0044] 本说明书实施例中提供的一种信息处理设备，包括：

[0045] 至少一个处理器；以及，

[0046] 与所述至少一个处理器通信连接的存储器；其中，

[0047] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0048] 获取采集信息；

[0049] 对所述采集信息进行加密，得到加密后的采集信息；

[0050] 发送所述加密后的采集信息给信息管理设备;所述加密后的采集信息与信息采集设备标识相对应,所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备时,将所述加密后的采集信息上传至区块链系统。

[0051] 本说明书实施例中采用的上述至少一个技术方案能够达到以下有益效果:

[0052] 本说明书实施例中,信息采集设备将采集信息加密后传输给信息管理设备,可有效提高信息的安全性,减少因网络攻击造成的信息错误,并且信息管理设备对信息采集设备进行验证,保证只有预设信息采集设备的采集信息才能上传至区块链系统,可减少干扰信息,进一步提高信息的安全性,因此,本说明书实施例中的方案可以从多角度保证信息安全性,进而也可以提高区块链中信息的可信度。

[0053] 另外,本说明书实施例中利用信息管理设备将信息采集设备获取的采集信息上传至区块链系统,无需将信息采集设备上链,可降低信息上链的成本,也可减少区块链系统中设备的连接数量,提高区块链系统的工作效率。

附图说明

[0054] 此处所说明的附图用来提供对本申请的进一步理解,构成本申请的一部分,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0055] 图1为本说明书实施例中提供的一种信息处理方法的应用场景的示意图;

[0056] 图2为本说明书实施例中提供的一种信息处理方法的流程示意图;

[0057] 图3为本说明书实施例中提供的一种信息处理方法的时序图;

[0058] 图4为本说明书实施例中提供的一种信息处理方法的流程示意图;

[0059] 图5为本说明书实施例中提供的一种信息处理方法的流程示意图;

[0060] 图6为本说明书实施例中提供的一种信息处理装置的结构示意图;

[0061] 图7为本说明书实施例中提供的一种信息处理装置的结构示意图;

[0062] 图8为本说明书实施例中提供的一种信息处理装置的结构示意图;

[0063] 图9为本说明书实施例中提供的一种信息处理设备的结构示意图。

具体实施方式

[0064] 为使本申请的目的、技术方案和优点更加清楚,下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然,所描述的实施例仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,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所有其他实施例,都属于本申请保护的范围。

[0065] 以下结合附图,详细说明本申请各实施例中提供的技术方案。

[0066] 图1为本说明书实施例中提供的一种信息处理方法的应用场景的示意图。如图1所示,整体架构中,主要包括被采集目标1、信息采集设备2、信息管理设备3以及区块链系统4。在实际应用中,被采集目标1可以包括仓库中存储的货物、设备中运行或存储的数据等可以被信息采集设备2采集的目标;信息采集设备2可以包括传感器、采集器、扫描器、摄像头等具有信息采集功能的设备;信息管理设备3可以是具有上链功能服务器类设备,可以将信息采集设备2采集的信息上传至区块链系统4,将采集的信息存储在区块链中。本说明书实施例中,信息采集设备2采集被采集目标1得到采集信息,将采集信息加密传输给信息管理设

备3，提高了采集信息的安全性；为进一步确保接收到的信息的安全性，信息管理设备3还可以对接收到的采集信息进行验证，确定接收到的采集信息是由信息采集设备2发送的；并且信息管理设备3可以接收多个信息采集设备2的信息，将采集的信息聚合后上传到区块链系统4中，可减少上链设备的数量，降低上链成本，并且可以减少区块链系统中设备的连接数量，提高区块链系统的工作效率。

[0067] 图2为本说明书实施例提供的一种信息处理方法的流程示意图。从程序角度而言，流程的执行主体可以为搭载于服务器或终端的程序。从功能角度而言，流程的执行主体对应的硬件设备可以是信息管理设备。

[0068] 如图2所示，该流程可以包括以下步骤：

[0069] 步骤202：接收信息采集设备发送的加密后的采集信息；

[0070] 实际应用中，信息采集设备通常可以采用蓝牙、无线、有线等传输方式将获取的采集信息传输给信息管理设备，还可以将采集信息加密后再进行传输，可减少网络攻击对采集信息的威胁，可提高信息的安全性。

[0071] 步骤204：根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0072] 实际应用中，加密后的采集信息中可以与信息采集设备标识相对应，具体的，加密后的采集信息中可以包含信息采集设备标识，信息采集设备标识也可以不包含于加密后的采集信息中，而是作为附加信息与加密后的采集信息一同发送给信息管理设备。所述信息采集设备标识可以用于指向发送采集信息的信息采集设备，其可以是信息采集设备的唯一标识符，如设备ID、设备序列号、MAC地址等，也可以是为信息采集设备预设的标识，如按照地理位置、排序等生成的标识信息，本说明书实施例中对信息采集设备标识的具体形式不作限定，只要能够将不同的信息采集设备区分，信息管理设备可以确定加密后的采集信息是由具体哪个信息采集设备发送的即可。

[0073] 实际应用中，为确保信息来源的可靠性，可以设置与信息管理设备对应的预设信息采集设备，信息管理设备可以将预设信息采集设备发送的采集信息上传至区块链系统，而对于预设信息采集设备之外的其他设备发送的采集信息不做上链处理，可以避免一些干扰设备发送的信息对真实采集信息的影响，提高信息来源的可靠性。例如，一些非法用户伪造了信息采集设备并伪造了采集信息，由于此信息采集设备是伪造的，是预设信息采集设备之外的设备，即使信息管理设备接收到此信息采集设备发送的伪造信息，也不会将伪造的信息上传至区块链系统，进一步保证信息的安全性。

[0074] 步骤206：若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0075] 实际应用中，信息管理设备可以将预设信息采集设备的采集信息上传至区块链系统，保证采集信息的真实有效性。

[0076] 本说明书实施例中信息采集设备可以是直接进行信息采集或者获取的设备，例如，摄像头、传感器、扫描器等设备，其数量可以很多，甚至可达到上万个，例如，大型仓库中的每个货架中通常都会布置多个传感器或摄像头用于对货架中货物情况进行监测，而在大型仓库中货架的数量通常会有成百上千个，这样整个仓库中信息采集设备的数量就会很多，如果将其获取的采集数据直接上传到区块链中，需要将所有信息采集设备配置为可上

链的设备，会增加成本，并且过多设备连接到区块链中，也会影响区块链对信息的处理效率。本说明书实施例中信息管理设备可以接收多个信息采集设备传输采集信息，利用信息管理设备将信息采集设备获取的采集信息聚合处理后，再上传到区块链中，可降低上链成本，提高区块链的处理效率，并且信息管理设备可以只将具有权限的信息采集设备发送的采集信息上传至区块链系统，可进一步保证上链信息的安全性。

[0077] 本说明书实施例中，信息采集设备将采集信息加密后传输给信息管理设备，可有效提高信息的安全性，减少因网络攻击造成的信息错误，并且信息管理设备对信息采集设备进行验证，保证只有预设信息采集设备的采集信息才能上传至区块链系统，可减少干扰信息，进一步提高信息的安全性，因此，本说明书实施例中的方案可以从多角度保证信息安全性，进而也可以提高区块链中信息的可信度。

[0078] 另外，本说明书实施例中利用信息管理设备将信息采集设备获取的采集信息上传至区块链系统，无需将信息采集设备上链，可降低信息上链的成本，也可减少区块链系统中设备的连接数量，提高区块链系统的工作效率。

[0079] 本说明书实施例中预设信息采集设备可以是满足预设条件的信息采集设备，也可以是与信息管理设备具有预设关系的信息采集设备，例如，将信息管理设备的设备列表中的信息采集设备设定为预设的信息采集设备，其中设备列表可以是预先设置的，也可以是根据与信息管理设备进行信息交互的信息采集设备生成的；又如，将某种型号的信息采集设备设定为预设的信息采集设备；又如，将与信息采集设备满足特定位置关系信息采集设备设定为预设的信息采集设备；又如，将与信息采集设备建立有绑定关系的信息采集设备设定为预设的信息采集设备，其中绑定关系可以理解为信息采集设备与信息管理设备互相进行了身份验证，两者之间允许进行信息交互。需要说明的是预信息采集设备的确定方式可以根据实际需要进行设定，这里不作具体限定。为更清楚的说明本说明书实施例中的方案，以预设信息采集设备为与信息采集设备建立有绑定关系的信息采集设备为例进行说明。

[0080] 图3为本说明书实施例提供的一种信息处理方法的时序图，如图3所示，本说明书实施例中的信息处理方法可以包括绑定阶段和信息处理阶段。

[0081] 其中，绑定阶段主要包括信息采集设备与信息管理设备建立绑定关系，信息管理设备可以对与其具有绑定关系的信息采集设备的采集信息进行上链处理，具体的绑定过程可以包括：信息采集设备可以向信息管理设备发送预先约定的第一绑定码，信息管理设备验证接收到的第一绑定码，验证通过后可向信息采集设备发送符合预定规则的第二验证码，信息采集设备可对第二验证码进行验证，验证通过则建立两者的绑定关系。

[0082] 信息处理阶段，主要是与信息管理设备建立绑定关系的信息采集设备将获取到的采集信息进行加密，将加密后的采集信息传输给信息管理设备，信息管理设备将接收到的加密后的采集信息上传至区块链系统。其中，信息采集设备可采用非对称加密方法对采集信息加密，并将公钥广播给信息管理设备，用于信息管理设备对加密后的采集信息进行验证。

[0083] 本说明书实施例中可以采用密钥机制对采集信息加密，具体的可采用非对称密钥技术，基于密码学的算法，每个信息采集设备和信息管理设备都可以具有两个独立的密钥，一个是公钥，一个是私钥，公钥与私钥在数学上是相关的，公钥可以用于加密一段信息或者

验证一个数字签名，私钥可以用来解密信息或者创建数字签名。在实际应用中，公钥不能反推得到私钥，所以公钥可以公开而不用担心信息的安全性，而私钥必须妥善保管，不得泄露，通常由私钥的所有者保管。信息的验证可以是私钥加工一段信息，得到一个数据签名，任何人都可以使用公钥来验证这个签名是不是属于签名人的，是不是未篡改的，使用私钥签名可以防止信息被篡改。

[0084] 说明书实施例中，所述接收信息采集设备发送的加密后的采集信息之前，还可以包括：

[0085] 接收所述信息采集设备发送的绑定请求；

[0086] 基于所述绑定请求，建立与所述信息采集设备的所述绑定关系。

[0087] 实际应用中，信息管理设备与信息采集设备建立绑定关系，可有效避免信息管理设备接收到具有干扰性的采集信息，例如，非法用户对信息管理设备进行网络攻击时，通过虚拟的或非法连接的信息采集设备向信息管理设备传输虚假信息，由于信息管理设备没有与这类信息采集设备建立绑定关系，也就不会将这类信息采集设备发送的信息上传至区块链系统，可确保上传至区块链系统的信息是可靠的。

[0088] 其中，绑定请求可以包括第一绑定码，所述基于所述绑定请求，建立与所述信息采集设备的绑定关系，具体可以包括：

[0089] 判断所述第一绑定码是否与预设绑定码相同；

[0090] 若所述第一绑定码与所述预设绑定码相同，则将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；所述预设信息采集设备标识为所述预设信息采集设备对应的用于区分不同预设信息采集设备的标识。

[0091] 本说明书实施例中信息管理设备可以通过从信息采集设备获取第一绑定码的方式建立与信采集设备的绑定关系，实际应用中，信息采集设备可以通过操作信息采集设备的操作面板向信息管理设备发送第一绑定码，也可以通过扫描信息管理设备出示的二维码、条形码等码图像向信息管理设备发送第一绑定码信息管理设备还可以通过扫描信息管理设备出示的二维码、条形码等码图像获取第一绑定码，具体形式，这里不作限定，只要信息管理设备可以获得信息采集设备发送的第一绑定码即可。实际应用中，在信息管理设备与信息采集设备建立绑定关系时，可以约定绑定码，也可称为预设绑定码，信息采集设备向信息管理设备发送第一绑定码，信息管理设备可以判断接收到的绑定码是否与预设绑定码相同，如果相同则可以与信息采集设备建立绑定关系。

[0092] 其中，第一绑定码可以是数字、文字、符合等多种形式，也可以包含表征信息采集设备身份特征的信息，例如设备名称、设备型号等。例如，预设绑定码为“113355”，信息采集设备可以向信息管理设备发送“113355”，信息管理设备确定信息采集设备发送的是与预设绑定码相同的第一绑定码，则确定可以与信息采集设备建立绑定关系。又如，第一绑定码包含信息采集设备的身份标识，如设备的编号“adc……”，预设绑定码可以包括全部或者部分可绑定设备的身份标识，如预设绑定码为“adc”，表示信息管理设备可以与设备编号前三位为“adc”的信息采集设备进行绑定，信息管理设备可以将接收到的信息采集设备的身份标识与预设的可绑定设备的身份标识进行比对，若预设的可绑定设备的身份标识中包含接收到的信息采集设备的身份标识，则表示第一绑定码与预设绑定码相同，则确定可以与此信息采集设备建立绑定关系。需要说明的是，上述内容仅是对第一绑定码进行的举例说明，并

不作为限定内容，第一绑定码可以根据实际需求设定，只要能够用于判断信息采集设备是否具有与信息管理设备进行绑定的权限即可。

[0093] 本说明书实施例中预设信息采集设备标识可以是预设信息采集设备对应的设备标识，所述判断所述信息采集设备是否为预设信息采集设备，具体可以包括：

[0094] 判断所述信息采集设备的信息采集设备标识是否与所述预设信息采集设备标识相同。

[0095] 本说明书实施例中，若信息采集设备信息采集设备标识与预设信息采集设备标识，则可以确定所述信息采集设备为预设信息采集设备，信息管理设备可以将其发送的采集信息上传至区块链系统。

[0096] 在实际应用中，可以将预设信息采集设备对应的预设信息采集设备标识保存在信息采集设备绑定列表中，信息采集设备绑定列表中可以记录有预设信息采集设备对应的预设信息采集设备标识，也可以是所有与信息管理设备具有绑定关系的信息采集设备的信息采集设备标识。在判断信息采集设备是否为预设信息采集设备时，可以将加密后的采集信息对应的信息采集设备标识与信息采集设备绑定列表中的内容进行比对，若此信息采集设备标识存在于列表中，则表示信息采集设备为预设信息采集设备。

[0097] 为进一步完善绑定关系，保证信息的安全性，所述则将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识之后，还可以包括：

[0098] 按照预设规则，根据所述第一绑定码生成第二绑定码；

[0099] 将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证。

[0100] 本说明书实施例中信息管理设备还可以按照预设规则，根据第一绑定码生成第二绑定码，反馈给信息采集设备，以便信息采集设备对信息管理设备进行验证，以确定此信息管理设备是接收到第一绑定码的信息管理设备，采用双方验证的方式，确保建立绑定关系的双方的合法性。例如，信息管理设备可以在第一绑定码的基础上添加特定信息构成第二绑定码，发送给信息采集设备，由于第一绑定码是由信息采集设备发送给信息管理设备的，收到第二绑定码的信息采集设备可以通过判断第二绑定码中是否包含之前发送给信息管理设备的第一绑定码对信息管理设备进行验证，若第二绑定码中包含之前发送给信息管理设备的第一绑定码，则表示此信息管理设备是信息采集设备想要进行信息传输的设备，可以与信息管理设备建立绑定关系，以便后续将采集信息传输给此信息管理设备。预设规则还可以是预设的算法，如，将第一绑定码与预设数值按照预设运算法则进行运算得到第二绑定码，信息采集设备接收到第二绑定码后可以进行逆运算来确定此信息管理设备是接收到第一绑定码的信息管理设备，等等。需要说明的是，本说明书实施例中预设规则可以根据实际需求进行设定，具体形式这里不作限定，只要能够用于信息采集设备对信息管理设备进行验证，完成双方验证即可。

[0101] 本说明书实施例中，信息采集设备在接收到第二验证码后还可以向信息管理设备反馈表示绑定成功或者不成功的信息，以便信息管理设备确定是否与信息采集设备绑定成功。若信息管理设备没有收到或者在预设时间段内没有收到信息采集设备反馈的表示绑定成功的信息，则可确定此次信息管理设备拒绝了本次绑定或者本次绑定过程存在某些问题，此时信息管理设备也不会将信息采集设备发送的采集信息上传至区块链系统。

[0102] 在实际应用中，在绑定过程中，还可以由信息管理设备向信息采集设备发起绑定请求，信息采集设备基于此绑定请求反馈给信息管理设备一反馈信息，此反馈信息中可以包含表征绑定请求的信息，也可以包含表征信息采集设备对应的设备标识的信息，信息管理设备基于此反馈信息建立与信息采集设备的绑定关系。在绑定过程中，绑定请求的发起方可以根据实际需求进行设定，这里不作具体限定。

[0103] 本说明书实施例中可以将表征与信息管理设备具有绑定关系的信息采集设备的身份标识的内容保存至信息管理设备中和/或区块链中，在将采集信息上传至区块链系统之前，可以将采集信息中表征信息采集设备的身份信息的内容与保存至信息管理设备中和/或区块链的表征与信息管理设备具有绑定关系的信息采集设备的身份标识的内容进行比对，判断采集信息是否为与信息管理设备具有绑定关系的设备发送的。当将表征与信息管理设备具有绑定关系的信息采集设备的身份标识的内容保存至区块链中时，还可以根据所述内容将采集信息存储至于所述内容对应的区块链中，以便后续对采集信息的查找。

[0104] 为进一步保证上传至区块链的信息的安全性，信息管理设备在将采集信息上传至区块链之前还可对采集信息进行签名验证，具体的，所述将所述加密后的采集信息上传至区块链系统之前，还可以包括：

[0105] 获取所述信息采集设备的所述信息采集设备标识；

[0106] 基于所述信息采集设备标识，查找所述信息采集设备对应的公钥；

[0107] 基于所述公钥，对所述加密后的采集信息进行签名验证，用于判断所述加密后的采集信息是否为所述信息采集设备传输给所述信息管理设备的；

[0108] 若所述签名验证通过，则将所述加密后的采集信息上传至区块链系统。

[0109] 本说明书实施例中信息采集设备可以生成公私钥对，加密的采集信息可以是利用信息采集设备的私钥签名处理过的信息，信息采集设备可以将公钥广播给信息管理设备，因此，在将采集信息上传至区块链之前，信息管理设备或者服务器还可以根据信息采集设备的设备标识，确定所述信息采集设备对应的公钥，利用公钥对加密后的采集信息进行签名验证，可以用于判断信息管理设备接收到的加密后的采集信息是否是发送所述加密后的采集信息的信息采集设备发送的，进一步提高加密后的采集信息来源的可靠性。

[0110] 本说明书实施例中信息管理设备也可以生成公私钥对，信息采集设备可以接收到信息管理设备广播的公钥。信息采集设备可以将获取到采集信息利用信息采集设备自身的私钥签名，然后利用接收到的信息管理设备的公钥加密，得到带有签名的加密后的采集信息；信息管理设备接收到所述加密后的采集信息后，可以利用信息管理设备自身的私钥对此加密后的采集信息进行解密，得到解密后的采集信息，还可以利用信息采集设备的公钥对其进行签名验证，验证是否此采集信息是否是信息采集设备发送的，是否被篡改。并且由于采集信息是利用信息管理设备的公钥加密处理的，只有信息管理设备的私钥才能解密，即使此加密后的采集信息被不法用户窃取，此不法用户也不能得到原始的采集信息，也可以保证信息不被泄露。

[0111] 为进一步确保获取到的信息的安全性，本说明书实施例中，所述将所述加密后的采集信息上传至区块链系统之前，还可以包括：

[0112] 获取所述加密后的采集信息的时间戳；

[0113] 判断所述时间戳表示的时间信息与所述信息管理设备获取所述时间戳的时间的

时间差值是否小于或等于预设时间差值；

[0114] 若所述时间戳表示的时间信息与所述信息管理设备获取所述时间戳的时间的时间差值小于或等于所述预设时间差值，则将所述加密后的采集信息上传至区块链系统。

[0115] 本说明书实施例中信息采集设备还可将获取的采集信息添加时间戳，信息管理设备可以通过验证时间戳来保证信息的安全性。例如，信息采集设备每10分钟获取一次信息，并将信息发送给信息管理设备，从而信息管理设备可以每10分钟接收到一次此信息采集设备的信息，当采集信息的时间戳中表征的时间信息与信息管理设备获取到所述时间戳的时间差值大于10分钟时，则表示此采集信息是之前的信息，可能是被重复处理的信息，也可能是非法用户进行重放攻击等网络攻击的信息，信息管理设备可以将这类信息筛选出来或者屏蔽掉或者删除掉，不将这些信息上传至区块链系统，可以避免将非法用户篡改或者伪造的信息上传至区块链，从而保证区块链系统中的信息时真实的信息，也保证了信息安全性。

[0116] 本说明书实施例中信息管理设备接收到的采集信息中可以包含获取所述采集信息的信息采集设备对应的信息采集设备标识，信息采集设备标识也可以作为附加信息与采集信息一同发送给信息管理设备，信息管理设备可以设定采集信息与信息采集设备的管理关系，在实际应用中，信息管理设备也可以有多个，多个信息管理设备获取的采集信息可以保存至同一个区块链系统中，为实现采集信息的追溯性，也可以将信息管理设备设置设备标识，根据此标识可以确定由此信息管理设备上传的采集信息。本说明书实施例中，信息管理设备可以当作是区块链系统的一个节点，所述方法，还可以包括：

[0117] 获取根据所述加密后的采集信息生成的链上数据的哈希值；

[0118] 生成所述哈希值、所述信息采集设备标识与信息管理设备标识之间的关联关系数据；所述信息管理设备标识为所述信息管理设备对应的用于区别不同信息管理设备的标识；

[0119] 存储所述关联关系数据。

[0120] 在实际应用中，将信息保存至区块链时，可以生成信息相应的哈希(hash)值，将哈希值存储到相应的区块中。本说明书实施例中存储的关联关系数据中可以包含所述信息采集设备标识与信息管理设备标识之间的关联数据，在获得新的采集信息后，还可以根据关联关系将新采集信息存储在获得此信息的信息采集设备对应的信息采集设备标识指向的区块中，可以使采集信息按照采集设备进行分类存储；同样，当有多个信息管理设备时，也可以将信息管理设备对应的信息管理设备标识指向不同的区块，将不同的信息管理设备获得的采集信息保存至对应的区块中。

[0121] 在实际应用中，还可以通过创建快照库的方式进行信息存储，创建信息采集设备快照库，例如，信息采集设备的信息采集设备标识可以指向区块链系统中的采集设备快照库，采集设备快照库中存储有表征所有信息采集设备的标识，每个信息采集设备的标识还可以指向存储加密后的采集信息的区块或者地址；信息管理设备的信息管理设备标识可以指向区块链系统中的管理设备快照库，管理设备快照库中存储有所有信息管理设备的标识，每个信息管理设备的标识还可以指向存储有与信息管理设备具有绑定关系的信息采集设备的标识的区块或者地址，进而信息管理设备可以将加密后的采集信息保存至对应的区块或者地址中。

[0122] 实际应用中可以通过调用智能合约对采集信息上传至区块链系统，利用智能合约

来维护信息处理的所有记录。其中智能合约可以包含多种逻辑函数，可以表征信息采集设备与信息管理设备的关联关系、信息采集设备与加密的采集信息对应的公钥的关联关系，等等。

[0123] 本说明书实施例中，所述采集信息具体可以包括图像采集设备采集的图像信息，以及所述图像信息中的目标物信息、目标物数量信息、目标物位置信息中至少一种信息。

[0124] 实际应用中，采集信息可以是图像信息，例如图片、视频等，还可以将图像信息进行处理，识别出其中包含的目标物信息、目标物数量信息、目标物位置信息中至少一种信息。例如，可以将摄像头拍摄的仓库货架存放货物的照片作为采集信息上传至区块链系统中，可以作为存证，以便后续使用；为更清楚的记录对货物情况，还可以对照片进行处理，识别出照片中具体货物的名称、数量、位置等信息，将识别出的信息上传至区块链系统中，以便对货物进行统计。

[0125] 本说明书实施例中，所述信息采集设备可以包括扫码模块，所述采集信息具体可以包括所述扫码模块采集的码信息。

[0126] 实际应用中，信息采集设备可以包括扫码模块，例如信息采集设备可以是是扫码枪等具有扫码功能的设备，扫码模块可以识别出码图像中的码信息，例如，存储在仓库中的货物通常会粘贴有二维码、条形码等码图像，码图像中可以记载有货物的名称、规格、产地、生产商、生产日期等信息，通过扫码模块，可以将这些信息识别出来，也可以借助信息管理模块将码图像中的码信息上传至区块链系统。需要说明的是，码图像的具体形式以及表征的具体码信息都是根据实际需要设定的，并且也可以根据实际需求，将码信息中的部分或者全部信息上传至区块链系统中，本说明书实施例对上述具体内容不作限定，只要能够满足需求即可。

[0127] 本说明书实施例中的信息处理方法可以应用于仓储管理的场景，具体的，所述信息采集设备可以为用于进行仓储管理的采集货物信息的设备，所述货物信息可以包括货物的数量信息、名称信息、位置信息中的至少一种信息。

[0128] 本说明书实施例中的信息处理方法还可以应用于其他场景，例如，用于健身房中健身器材本身以及健身器材中记录的用户信息等进行处理，等等。

[0129] 基于同样的原理，本说明书实施例还提供了一种信息处理方法，从程序角度而言，流程的执行主体可以为搭载于服务器或终端的程序。从功能角度而言，流程的执行主体对应的硬件设备可以是区块链系统。

[0130] 如图4所示，该流程可以包括以下步骤：

[0131] 步骤402：获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0132] 步骤404：对所述采集信息进行验签处理；

[0133] 步骤406：将通过验签的所述加密后的采集信息保存至区块链。

[0134] 本说明书实施例中信息管理设备可以将加密的采集信息上传至区块链系统，从区块链系统的角度而言，可以获取信息管理设备上传的加密后的采集信息，还可以将对加密的采集信息进行验签，进而保证区块链中存储的是没有被篡改的安全信息。

[0135] 其中，所述对所述采集信息进行验签处理，具体可以包括：

[0136] 确定所述信息采集设备的信息采集设备标识；

[0137] 基于所述信息采集设备标识，查找所述信息采集设备的公钥；

[0138] 利用所述公钥对所述加密后的采集信息进行签名验证；

[0139] 若所述签名验证通过，则调用智能合约将所述加密后的采集信息保存至区块链。

[0140] 本说明书实施例中，区块链系统还可以对上传的信息进行签名验证，为保证链上信息的安全性，可以将通过签名验证的信息保存至区块链，具体的，可以利用预先创建的智能合约进行签名验证，调用合约的处理函数，确定信息采集设备的设备标识，进而确定与此信息采集设备对应的公钥，利用此公钥对包含签名的加密后的采集信息进行签名验证，若验证通过还可以调用智能合约将加密后的采集信息保存至区块链。

[0141] 实际应用中，智能合约可以预先生成，其可以包含多种逻辑处理函数，例如，本说明书实施例中的智能合约可以是用于记录采集信息的合约，具体可以包括指向数据快照库的逻辑函数，所述数据快照库可以存储采集信息的相关内容，区块链系统可以根据采集信息、信息采集设备、信息管理设备之间的对应关系，将采集信息对应保存至对应的数据快照库中，还可以将验签所需的公钥保存至数据快照库中；智能合约还可以包括指向设备快照库的逻辑函数，所述设备快照库可以存储信息采集设备以及信息管理设备的相关内容，例如可以存储信息采集设备的设备标识、信息管理设备的设备标识以及信息采集设备与信息管理设备的绑定关系等等。

[0142] 智能合约还可以基于预设的用于处理采集信息的智能合约模板创建，智能合约模板中可以记载用于处理采集信息的处理逻辑，其可以包括，用于将公钥、信息采集设备的设备信息、信息管理设备的设备信息以及采集信息存储至区块链中的存储逻辑，还可以包括用于从区块链中查询已存储的公钥、信息采集设备的设备信息、信息管理设备的设备信息以及采集信息的查询逻辑，还可以包括对存储的信息进行更新的逻辑，等等。需要说明的是本说明书实施例中智能合约可以根据实际需求进行创建，具体形式这里不作限定，只要能够满足信息处理的需求即可。

[0143] 基于同样的原理，本说明书实施例中还提供另一种信息处理方法，图5为本说明书实施例中提供的一种信息处理方法，从程序角度而言，流程的执行主体可以为搭载于服务器或终端的程序。从功能性角度而言，流程的执行主体对应的硬件设备可以是信息采集设备。

[0144] 如图5所示，所述方法可以包括：

[0145] 步骤502：获取采集信息；

[0146] 步骤504：对所述采集信息进行加密，得到加密后的采集信息；

[0147] 步骤506：发送所述加密后的采集信息给信息管理设备；所述加密后的采集信息与信息采集设备标识相对应，所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备，将所述加密后的采集信息上传至区块链系统。

[0148] 本说明书实施例中信息采集设备可以将获取的采集信息加密传输给信息管理设备，以便信息管理设备将通过验证的信息上传至区块链系统。其中，信息采集设备可以是具有信息采集功能的设备，如扫码器、摄像头、传感器等，其可以包括同一种设备，也可以包括多种设备。

[0149] 其中，所述发送所述加密后的采集信息给信息管理设备之前，还可以包括：

[0150] 发送绑定请求给所述信息管理设备，以便所述信息管理设备与所述信息采集设备

建立绑定关系。

[0151] 其中，所述绑定请求包括第一绑定码，所述发送绑定请求给所述信息管理设备，具体可以包括：

[0152] 发送所述第一绑定码给所述信息管理设备，以便所述信息采集设备将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识。

[0153] 其中，所述发送第一绑定码给所述信息管理设备之后，还可以包括：

[0154] 接收所述信息管理设备发送的第二绑定码，所述第二绑定码为所述信息管理设备在所述第一绑定码的基础上按照预设规则生成的，用于对所述信息管理设备进行验证；

[0155] 判断所述第二绑定码中是否包含表征所述第一绑定码的信息，得到绑定判断结果；

[0156] 若所述绑定判断结果表示所述第二绑定码中包含表征所述第一绑定码的信息，则确定与所述信息管理设备建立绑定关系。

[0157] 其中，本说明书实施例中所述方法还可以包括：

[0158] 发送信息采集设备标识给所述信息管理设备，以便所述信息管理设备基于所述信息采集设备标识查找所述信息采集设备对应的公钥。

[0159] 实际应用中，所述信息采集设备标识可以在发送第一绑定码时发送给信息管理设备，还可以在给信息管理设备反馈绑定成功的信息时发送，还可以广播公钥时将信息擦剂设备标识一同进行广播，等等，具体方式这里不作限定，只要能够使信息管理设备获得即可。信息管理设备可以对获得的信息采集设备标识进行保存，并建立信息采集设备标识与信息采集设备广播的公钥之间的对应关系，以便能够根据信息采集设备标识确定与其对应的公钥。

[0160] 其中，所述获取采集信息之后，还可以包括：

[0161] 对所述采集信息添加时间戳，所述时间戳表征所述采集信息被采集的时间，用于所述信息管理设备对所述采集信息进行验证。

[0162] 在实际应用中，可采用非对称加密算法对采集信息进行签名和加密。本说明书实施例中可以将采集信息添加时间戳信息，利用信息采集设备的私钥进行签名，将签名后的添加有时间戳的采集信息加密后发送给信息管理设备，信息管理设备可以利用接收到的信息采集设备公钥对添加有时间戳的采集信息进行验签。在实际应用中，信息采集设备还可以将采集的信息签名后再添加时间戳信息，再进行加密处理等。需要说明的是，上述内容仅是为了更清楚的说明本说明书实施例的方案，对时间戳信息相关内容进行的举例说明，在实际应用中，还可以采用其他方式添加时间戳以及获取时间戳，具体方式这里不作限定，只要能够利用时间戳对所述采集信息进行验证即可。

[0163] 本说明书实施例中，所述采集信息具体可以包括图像采集设备采集的图像信息，以及所述图像信息中的目标物信息、目标物数量信息、目标物位置信息中至少一种信息。

[0164] 本说明书实施例中，所述信息采集设备可以包括扫码模块，所述采集信息具体可以包括所述扫码模块采集的码信息。

[0165] 本说明书实施例中，所述信息采集设备可以为用于进行仓储管理的采集货物信息的设备，所述货物信息包括货物的数量信息、名称信息、位置信息中的至少一种信息。

[0166] 基于同样的思路，本说明书实施例还提供了上述方法对应的装置。图6为本说明书

实施例提供的对应于图2的一种信息处理装置的结构示意图。如图6所示，该装置可以包括：

[0167] 采集信息接收模块602，用于接收信息采集设备发送的加密后的采集信息；

[0168] 采集设备判断模块604，用于根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0169] 信息上链模块606，用于若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0170] 其中，所述采集信息接收模块，还可以用于：

[0171] 接收所述信息采集设备发送的绑定请求；

[0172] 基于所述绑定请求，建立与所述信息采集设备的绑定关系。

[0173] 其中，所述绑定请求包括第一绑定码，所述基于所述绑定请求，建立与所述信息采集设备的绑定关系，具体可以包括：

[0174] 判断所述第一绑定码是否与预设绑定码相同；

[0175] 若所述第一绑定码与所述预设绑定码相同，则将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识；所述预设信息采集设备标识为所述预设信息采集设备对应的用于区分不同所述预设信息采集设备的标识。

[0176] 其中，所述采集信息接收模块，还可以用于：

[0177] 按照预设规则，根据所述第一绑定码生成第二绑定码；

[0178] 将所述第二绑定码发送给所述信息采集设备，所述第二绑定码用于所述信息采集设备对所述信息管理设备进行验证。

[0179] 基于同样的思路，本说明书实施例还提供了上述方法对应的装置。图7为本说明书实施例提供的对应于图4的一种信息处理装置的结构示意图。如图7所示，该装置可以包括：

[0180] 采集信息获取模块702，用于获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0181] 信息验签模块704，用于对所述采集信息进行验签处理；

[0182] 信息保存模块706，用于将通过验签的所述加密后的采集信息保存至区块链。

[0183] 其中，所述信息验签模块，具体可以用于：

[0184] 确定所述信息采集设备的信息采集设备标识；

[0185] 基于所述信息采集设备标识，查找所述信息采集设备的公钥；

[0186] 利用所述公钥对所述加密后的采集信息进行签名验证；

[0187] 若所述签名验证通过，则调用智能合约将所述加密后的采集信息保存至区块链。

[0188] 基于同样的思路，本说明书实施例还提供了上述方法对应的装置。图8为本说明书实施例提供的对应于图5的一种信息处理装置的结构示意图。如图8所示，该装置可以包括：

[0189] 信息获取模块802，用于获取采集信息；

[0190] 信息加密模块804，用于对所述采集信息进行加密，得到加密后的采集信息；

[0191] 信息发送模块806，用于发送所述加密后的采集信息给信息管理设备；所述加密后的采集信息与信息采集设备标识相对应，所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备时，将所述加密后的采集信息上传至区块链系统。

[0192] 其中，所述信息获取模块，还可以用于：

[0193] 发送所述第一绑定码给所述信息管理设备，以便所述信息采集设备将所述信息采集设备的信息采集设备标识确定为预设信息采集设备标识。

[0194] 其中，所述信息获取模块，还可以用于：

[0195] 接收所述信息管理设备发送的第二绑定码，所述第二绑定码为所述信息管理设备在所述第一绑定码的基础上按照预设规则生成的，用于所述信息采集设备对所述信息管理设备进行验证；

[0196] 判断所述第二绑定码中是否包含表征所述第一绑定码的信息，得到绑定判断结果；

[0197] 若所述绑定判断结果表示所述第二绑定码中包含表征所述第一绑定码的信息，则确定与所述信息管理设备建立绑定关系。

[0198] 基于同样的思路，本说明书实施例还提供了上述方法对应的设备。图9为本说明书实施例提供的一种信息处理设备的结构示意图，图9所示的设备可以执行上述图2、图4和图5所示方法中至少一种方法。

[0199] 当图9中所述设备与图2所示方法对应时，设备900可以包括：

[0200] 至少一个处理器910；以及，

[0201] 与所述至少一个处理器通信连接的存储器930；其中，

[0202] 所述存储器930存储有可被所述至少一个处理器910执行的指令920，所述指令被所述至少一个处理器910执行，以使所述至少一个处理器910能够：

[0203] 接收信息采集设备发送的加密后的采集信息；

[0204] 根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备；

[0205] 若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统。

[0206] 当图9中所述设备与图4所示方法对应时，设备900可以包括：

[0207] 至少一个处理器910；以及，

[0208] 与所述至少一个处理器通信连接的存储器930；其中，

[0209] 所述存储器930存储有可被所述至少一个处理器910执行的指令920，所述指令被所述至少一个处理器910执行，以使所述至少一个处理器910能够：

[0210] 获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的；

[0211] 对所述采集信息进行验签处理；

[0212] 将通过验签的所述加密后的采集信息保存至区块链。

[0213] 当图9中所述设备与图5所示方法对应时，设备900可以包括：

[0214] 至少一个处理器910；以及，

[0215] 与所述至少一个处理器通信连接的存储器930；其中，

[0216] 所述存储器930存储有可被所述至少一个处理器910执行的指令920，所述指令被所述至少一个处理器910执行，以使所述至少一个处理器910能够：

[0217] 获取采集信息；

[0218] 对所述采集信息进行加密，得到加密后的采集信息；

[0219] 发送所述加密后的采集信息给信息管理设备;所述加密后的采集信息与信息采集设备标识相对应,所述信息采集设备标识用于所述信息管理设备判断所述信息采集设备为预设信息采集设备时,将所述加密后的采集信息上传至区块链系统。

[0220] 本说明书实施例中还可以提供一种计算机可读介质,其上存储有计算机可读指令,所述计算机可读指令可被处理器执行以实现上述与图2、图4和图5所示的至少一种方法中对应的信息处理方法。

[0221] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0222] 本说明书实施例提供的装置、设备、非易失性计算机存储介质与方法是对应的,因此,装置、设备、非易失性计算机存储介质也具有与对应方法类似的有益技术效果,由于上面已经对方法的有益技术效果进行了详细说明,因此,这里不再赘述对应装置、设备、非易失性计算机存储介质的有益技术效果。

[0223] 在20世纪90年代,对于一个技术的改进可以很明显地区分是硬件上的改进(例如,对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而,随着技术的发展,当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此,不能说一个方法流程的改进就不能用硬件实体模块来实现。例如,可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array,FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language,HDL),而HDL也并非仅有一种,而是有许多种,如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等,目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[0224] 控制器可以按任何适当的方式实现,例如,控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320,

存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0225] 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。

[0226] 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，在实施本申请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。

[0227] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

[0228] 本发明是参照根据本发明实施例的方法、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。

[0229] 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。

[0230] 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。

[0231] 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。

[0232] 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。

[0233] 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，磁带式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。

[0234] 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。

[0235] 本申请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申请，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。

[0236] 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。

[0237] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

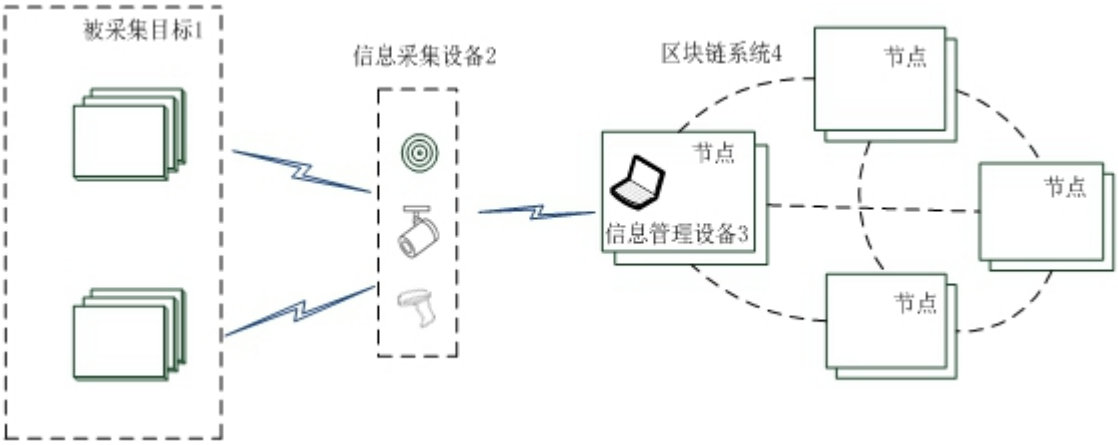

被采集目标1
信息采集设备2
区块链系统4
节点
节点
节点
节点
信息管理设备3

图1

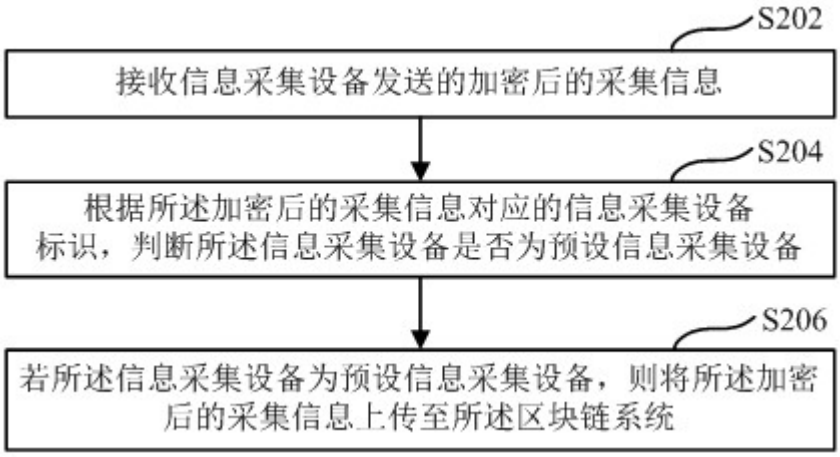

S202
接收信息采集设备发送的加密后的采集信息
S204
根据所述加密后的采集信息对应的信息采集设备标识，判断所述信息采集设备是否为预设信息采集设备
S206
若所述信息采集设备为预设信息采集设备，则将所述加密后的采集信息上传至所述区块链系统

图2

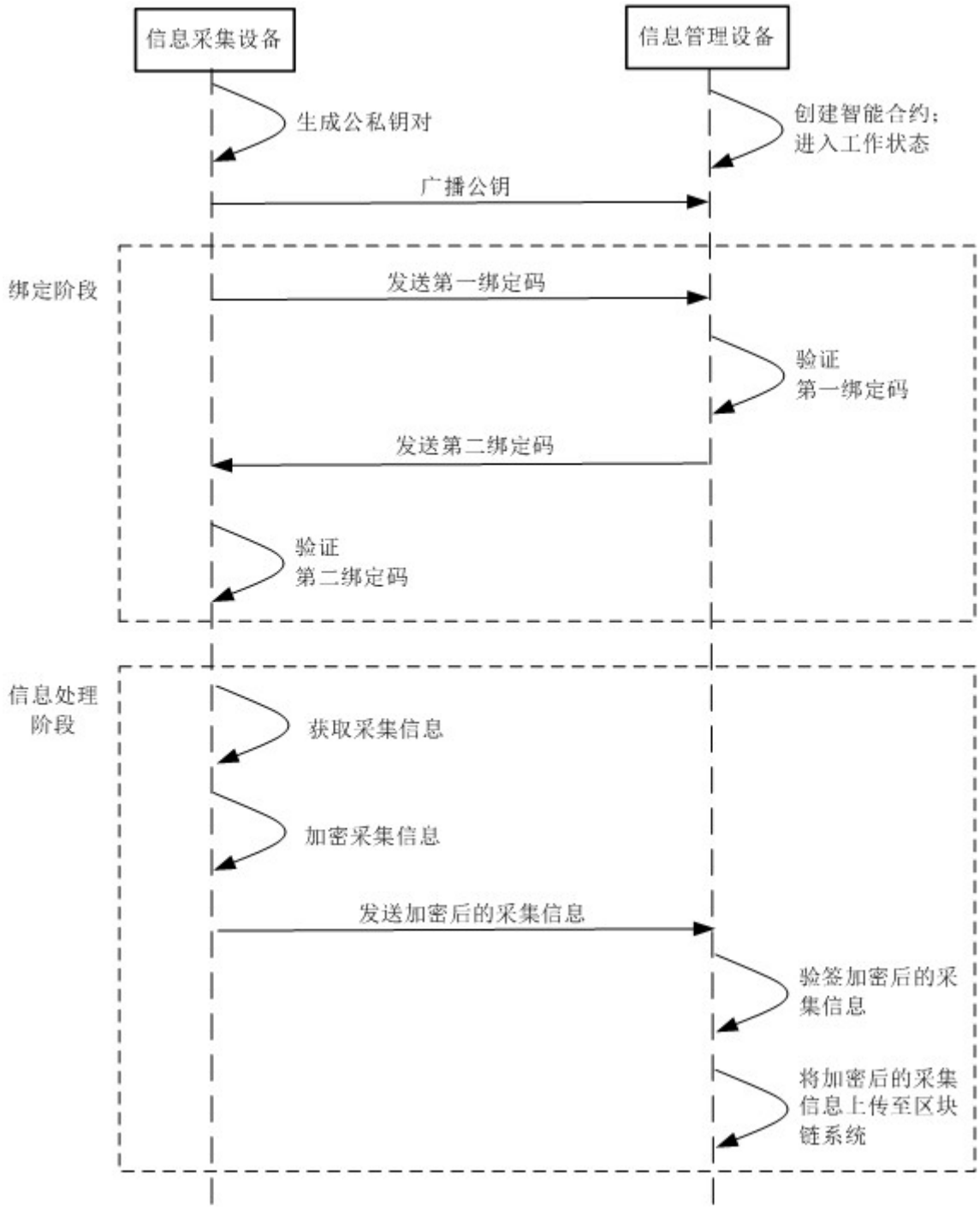

信息采集设备
信息管理设备
生成公私钥对
创建智能合约；
进入工作状态
广播公钥
绑定阶段
发送第一绑定码
验证
第一绑定码
发送第二绑定码
验证
第二绑定码
信息处理
阶段
获取采集信息
加密采集信息
发送加密后的采集信息
验签加密后的采
集信息
将加密后的采集
信息上传至区块
链系统

图3

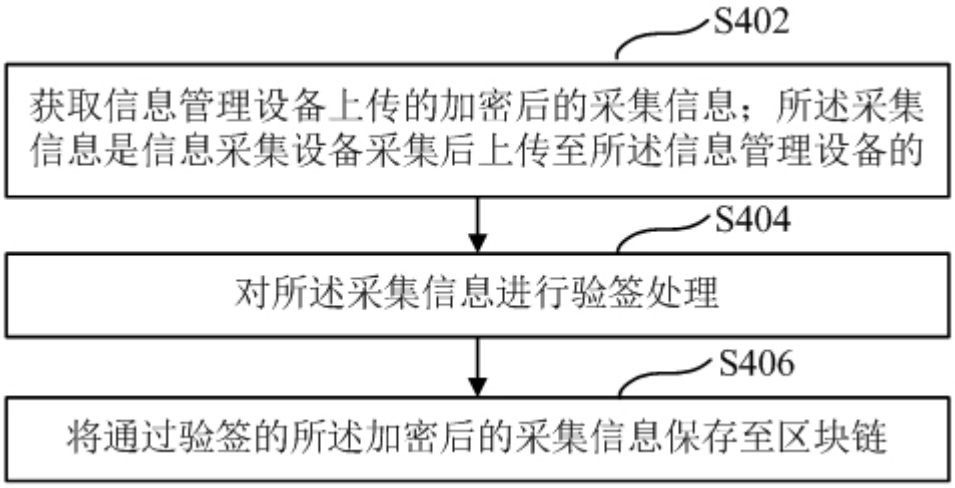

S402
获取信息管理设备上传的加密后的采集信息；所述采集信息是信息采集设备采集后上传至所述信息管理设备的
S404
对所述采集信息进行验签处理
S406
将通过验签的所述加密后的采集信息保存至区块链

图4

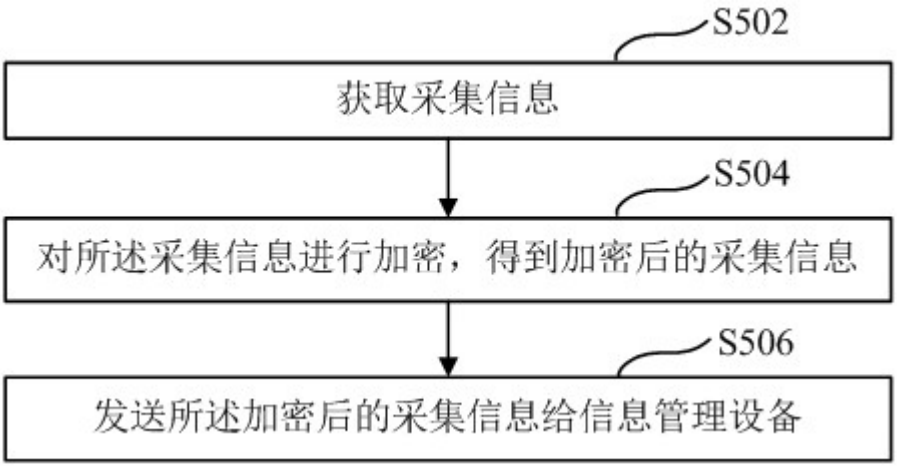

S502
获取采集信息
S504
对所述采集信息进行加密，得到加密后的采集信息
S506
发送所述加密后的采集信息给信息管理设备

图5

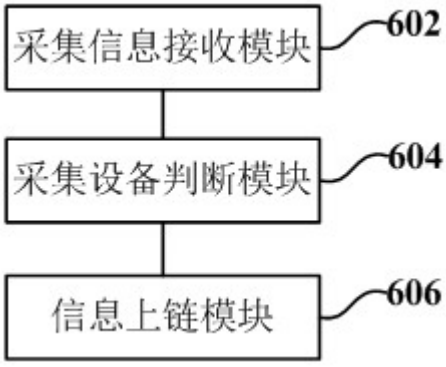

采集信息接收模块
602
采集设备判断模块
604
信息上链模块
606

图6

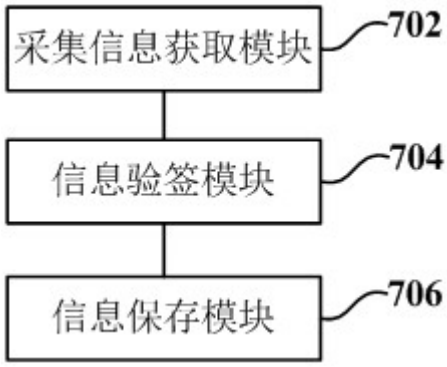

采集信息获取模块
702
信息验签模块
704
信息保存模块
706

图7

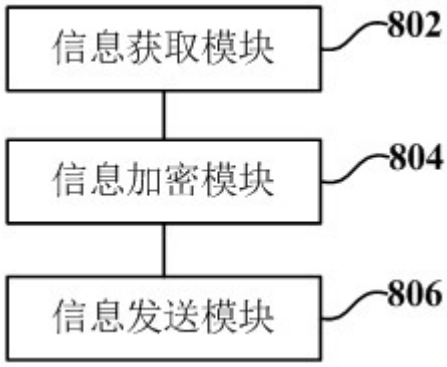

信息获取模块
802
信息加密模块
804
信息发送模块
806

图8

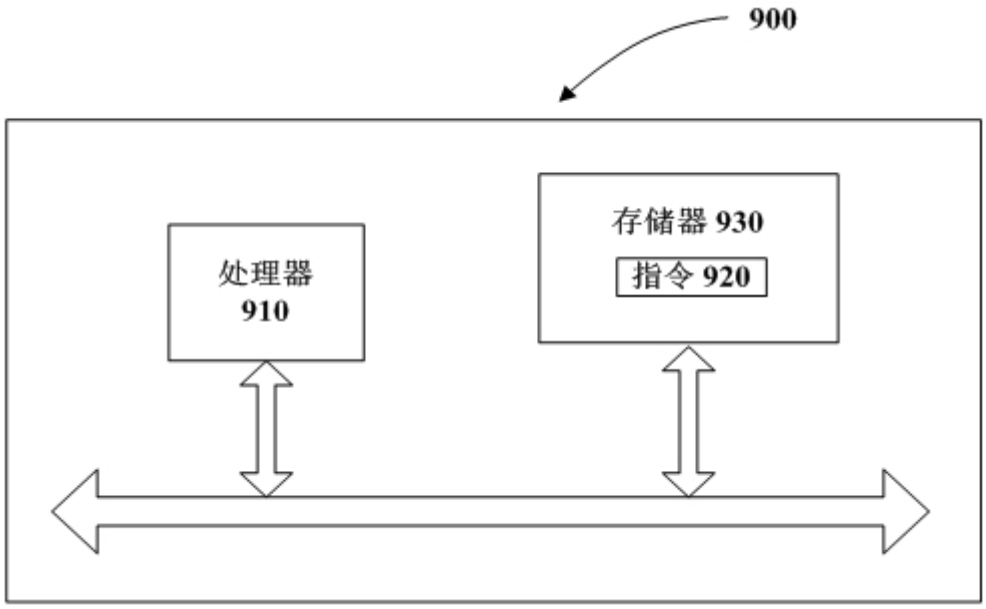

900
处理器
910
存储器 930
指令 920

图9