(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113190860 B
(45)授权公告日 2024.03.01

(21)申请号 202110494588.0
(22)申请日 2021.05.07
(65)同一申请的已公布的文献号
申请公布号 CN 113190860 A
(43)申请公布日 2021.07.30
(73)专利权人 福建福链科技有限公司
地址 350001 福建省福州市高新区科技东路3号创新园一期14号楼2层212室
(72)发明人 谭焕明 斯雪明 朱永亮
(74)专利代理机构 福州市博深专利事务所(普通合伙) 35214
专利代理师 颜丽蓉
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06F 16/27(2019.01)
(56)对比文件
CN 108768992 A,2018.11.06
CN 110011810 A,2019.07.12
CN 111769938 A,2020.10.13
审查员 潘秋羽

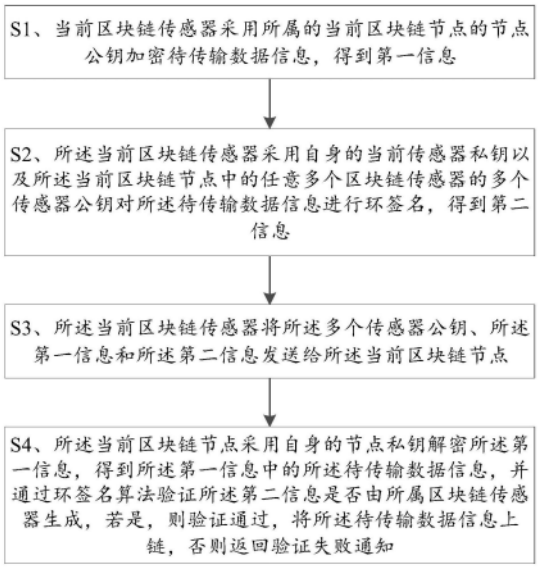
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种基于环签名的区块链传感器数据认证方法及系统

(57)摘要

本发明提供了一种基于环签名的区块链传感器数据认证方法及系统,区块链传感器采用所属的区块链节点的节点公钥加密待传输数据信息,得到第一信息,并采用自身的传感器私钥以及所属区块链节点中的任意多个区块链传感器的多个传感器公钥对待传输数据信息进行环签名,得到第二信息;将多个传感器公钥、第一信息和第二信息发送给所属的区块链节点;区块链节点采用节点私钥解密第一信息,得到待传输数据信息,并通过环签名算法验证第二信息是否由所属区块链传感器生成,若是,则将待传输数据信息上链。本发明有效地解决了目前区块链传感器传输的数据无法得到有效验证的问题,保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。



CN 113190860 B

1.一种基于环签名的区块链传感器数据认证方法,其特征在于,包括步骤:

S1、当前区块链传感器采用所属的当前区块链节点的节点公钥加密待传输数据信息,得到第一信息;

S2、所述当前区块链传感器采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名,得到第二信息;

S3、所述当前区块链传感器将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点;

S4、所述当前区块链节点采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知;

所述步骤S2具体为:

对所述待传输数据信息进行哈希值计算,得到第二哈希值;

所述当前区块链传感器采用所述当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述第二哈希值进行环签名,得到第二信息;

所述步骤S4中的并通过环签名算法验证所述第二信息是否由所属区块链传感器生成具体为:

首先验证所述多个传感器公钥是否在所述当前区块链节点的数据库中存储有,若是,则通过所述多个传感器公钥将所述第二信息解为所述第二哈希值,再正向计算所述待传输数据信息的哈希值为第一哈希值,比对所述第一哈希值与所述第二哈希值是否相同,若是,则所述第二信息是由所属区块链传感器生成,否则所述第二信息不是由所属区块链传感器生成。

2.根据权利要求1所述的一种基于环签名的区块链传感器数据认证方法,其特征在于,所述步骤S1之前还包括步骤:

S01、所述当前区块链传感器生成并存储所述当前传感器公钥和所述当前传感器私钥,并将所述当前传感器公钥和自身的当前传感器物理标识存储在所述当前区块链节点中,同时将所述当前传感器公钥存储在所述当前区块链节点的所有所属区块链传感器中;

S02、所述当前区块链节点生成并存储所述节点公钥和所述节点私钥,并将所述节点公钥和自身的节点物理标识存储在所述区块链节点中的每个所属区块链传感器中。

3.根据权利要求2所述的一种基于环签名的区块链传感器数据认证方法,其特征在于,所述步骤S3具体为:

所述当前区块链传感器将所述多个传感器公钥、所述节点物理标识、所述当前传感器物理标识、所述第二信息和所述第一信息发送给所述当前区块链节点。

4.根据权利要求3所述的一种基于环签名的区块链传感器数据认证方法,其特征在于,所述步骤S4具体包括以下步骤:

S41、所述当前区块链节点验证所述节点物理标识是否存储在所述当前区块链节点中,若是则执行步骤S42,否则返回验证失败通知;

S42、所述当前区块链节点验证所述当前传感器物理标识是否存储在所述当前区块链节点中,若是则执行步骤S43,否则返回验证失败通知;

S43、所述当前区块链节点采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知。

5.一种基于环签名的区块链传感器数据认证系统,其特征在于,包括当前区块链传感器以及当前区块链节点子系统,所述当前区块链传感器包括第一存储器、第一处理器以及存储在第一存储器上并可在第一处理器上运行的第一计算机程序,所述当前区块链节点子系统包括第二存储器、第二处理器以及存储在第二存储器上并可在第二处理器上运行的第二计算机程序;

所述第一处理器执行所述第一计算机程序时实现以下步骤:

S1、采用所属的当前区块链节点的节点公钥加密待传输数据信息,得到第一信息;

S2、采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名,得到第二信息;

S3、将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点;

所述第二处理器执行所述第二计算机程序时实现以下步骤:

S4、采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知;

所述第一处理器执行所述第一计算机程序的所述步骤S2时具体为:

对所述待传输数据信息进行哈希值计算,得到第二哈希值;

采用所述当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述第二哈希值进行环签名,得到第二信息;

所述第二处理器执行所述第二计算机程序的所述步骤S4中的并通过环签名算法验证所述第二信息是否由所属区块链传感器生成具体为:

首先验证所述多个传感器公钥是否在所述当前区块链节点的数据库中存储有,若是,则通过所述多个传感器公钥将所述第二信息解为所述第二哈希值,再正向计算所述待传输数据信息的哈希值为第一哈希值,比对所述第一哈希值与所述第二哈希值是否相同,若是,则所述第二信息是由所属区块链传感器生成,否则所述第二信息不是由所属区块链传感器生成。

6.根据权利要求5所述的一种基于环签名的区块链传感器数据认证系统,其特征在于,在所述步骤S1之前,所述第一处理器执行所述第一计算机程序还包括步骤:

S01、生成并存储所述当前传感器公钥和所述当前传感器私钥,并将所述当前传感器公钥和自身的当前传感器物理标识存储在所述当前区块链节点中,同时将所述当前传感器公钥存储在所述当前区块链节点的所有所属区块链传感器中;

所述第二处理器执行所述第二计算机程序还包括步骤:

S02、生成并存储所述节点公钥和所述节点私钥,并将所述节点公钥和自身的节点物理标识存储在所述区块链节点中的每个所属区块链传感器中。

7.根据权利要求6所述的一种基于环签名的区块链传感器数据认证系统,其特征在于,所述第一处理器执行所述第一计算机程序的所述步骤S3时具体为:

将所述多个传感器公钥、所述节点物理标识、所述当前传感器物理标识、所述第二信息和所述第一信息发送给所述当前区块链节点。

8.根据权利要求7所述的一种基于环签名的区块链传感器数据认证系统,其特征在于,所述第二处理器执行所述第二计算机程序的所述步骤S4时具体包括以下步骤:

S41、验证所述节点物理标识是否存储在所述当前区块链节点中,若是则执行步骤S42,否则返回验证失败通知;

S42、验证所述当前传感器物理标识是否存储在所述当前区块链节点中,若是则执行步骤S43,否则返回验证失败通知;

S43、采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知。

一种基于环签名的区块链传感器数据认证方法及系统

技术领域

[0001] 本发明涉及区块链技术领域,特别涉及一种基于环签名的区块链传感器数据认证方法及系统。

背景技术

[0002] 随着全球物联网技术的逐渐发展和各国政策的大力扶持,物联网芯片、信息传感器等先进产品不断推出,有力地促进了物联网的应用和普及。其中,区块链网络集成了分布式数据存储、点对点传输、共识机制、加密算法等技术,具有去中心化、去信任化、数据不可篡改、可追溯等特点,可以为物联网提供信任、所有权记录、透明性和通信支持,从而为解决物联网产业发展难题、拓展物联网产业发展空间提供了新的思路。

[0003] 而为了保证区块链网络的安全,区块链传感器在接入区块链网络时,可靠可信的认证和数据传输至关重要。在区块链传感器需求的分析中,安全是一个重要的参数。

[0004] 区块链传感器的安全隐患主要来源于三个方面:资源非常有限、不可靠的通信以及无人管理。这些缺陷使得区块链网络容易遭受各种攻击,而遭受攻击的区块链传感器,其传输出去的数据一般没有行之有效的检验机制来进行验证。

发明内容

[0005] 本发明所要解决的技术问题是:提供一种基于环签名的区块链传感器数据认证方法及系统,解决目前区块链传感器传输的数据无法得到有效验证的问题,保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。

[0006] 为了解决上述技术问题,本发明采用的技术方案为:

[0007] 一种基于环签名的区块链传感器数据认证方法,包括步骤:

[0008] S1、当前区块链传感器采用所属的当前区块链节点的节点公钥加密待传输数据信息,得到第一信息;

[0009] S2、所述当前区块链传感器采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名,得到第二信息;

[0010] S3、所述当前区块链传感器将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点;

[0011] S4、所述当前区块链节点采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知。

[0012] 为了解决上述技术问题,本发明采用的另一种技术方案为:

[0013] 一种基于环签名的区块链传感器数据认证系统,包括当前区块链传感器以及当前区块链节点子系统,所述当前区块链传感器包括第一存储器、第一处理器以及存储在第一存储器上并可在第一处理器上运行的第一计算机程序,所述当前区块链节点子系统包括第

二存储器、第二处理器以及存储在第二存储器上并可在第二处理器上运行的第二计算机程序；

[0014] 所述第一处理器执行所述第一计算机程序时实现以下步骤：

[0015] S1、采用所属的当前区块链节点的节点公钥加密待传输数据信息，得到第一信息；

[0016] S2、采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名，得到第二信息；

[0017] S3、将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点；

[0018] 所述第二处理器执行所述第二计算机程序时实现以下步骤：

[0019] S4、采用自身的节点私钥解密所述第一信息，得到所述第一信息中的所述待传输数据信息，并通过环签名算法验证所述第二信息是否由所属区块链传感器生成，若是，则验证通过，将所述待传输数据信息上链，否则返回验证失败通知。

[0020] 本发明的有益效果在于：本发明提供一种基于环签名的区块链传感器数据认证方法及系统，当当前区块链传感器传输数据时，通过采用所属的当前区块链节点的节点公钥对数据进行加密，并采用自身的私钥和同属于当前区块链节点中的任一多个区块链传感器的公钥对数据进行环签名，并将进行环签名的多个传感器公钥、加密的数据以及环签名的数据一起发送给当前区块链节点，从而通过节点私钥解密获得数据及通过环签名算法验证环签名是否是由自己的区块链传感器所签，保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。

附图说明

[0021] 图1为本实施例中的一种基于环签名的区块链传感器数据认证方法的流程示意图；

[0022] 图2为本实施例中的一种基于环签名的区块链传感器数据认证方法的框架示意图；

[0023] 图3为本实施例中的一种基于环签名的区块链传感器数据认证系统的结构示意图。

[0024] 标号说明：

[0025] 10、一种基于环签名的区块链传感器数据认证系统；20、当前区块链传感器；21、第一存储器；22、第一处理器；30、当前区块链节点子系统；31、第二存储器；32、第二处理器。

具体实施方式

[0026] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图予以说明。

[0027] 请参照图1及图2，一种基于环签名的区块链传感器数据认证方法，包括步骤：

[0028] S1、当前区块链传感器采用所属的当前区块链节点的节点公钥加密待传输数据信息，得到第一信息；

[0029] S2、所述当前区块链传感器采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名，得到第

二信息；

[0030] S3、所述当前区块链传感器将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点；

[0031] S4、所述当前区块链节点采用自身的节点私钥解密所述第一信息，得到所述第一信息中的所述待传输数据信息，并通过环签名算法验证所述第二信息是否由所属区块链传感器生成，若是，则验证通过，将所述待传输数据信息上链，否则返回验证失败通知。

[0032] 由上述描述可知，本发明的有益效果在于：当当前区块链传感器传输数据时，通过采用所属的当前区块链节点的节点公钥对数据进行加密，并采用自身的私钥和同属于当前区块链节点中的任一多个区块链传感器的公钥对数据进行环签名，并将进行环签名的多个传感器公钥、加密的数据以及环签名的数据一起发送给当前区块链节点，从而通过节点私钥解密获得数据及通过环签名算法验证环签名是否是由自己的区块链传感器所签，保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。

[0033] 进一步地，所述步骤S1之前还包括步骤：

[0034] S01、所述当前区块链传感器生成并存储所述当前传感器公钥和所述当前传感器私钥，并将所述当前传感器公钥和自身的当前传感器物理标识存储在所述当前区块链节点中，同时将所述当前传感器公钥存储在所述当前区块链节点的所有所属区块链传感器中；

[0035] S02、所述当前区块链节点生成并存储所述节点公钥和所述节点私钥，并将所述节点公钥和自身的节点物理标识存储在所述区块链节点中的每个所属区块链传感器中。

[0036] 由上述描述可知，每个传感器都生成一对公钥和私钥，其中公钥可存储在同在一个节点下的其他传感器中，方便每个传感器进行数据传输时通过公钥进行环签名，同时公钥还存在所属的当前节点的数据库中，方便后续节点通过数据库中的所有传感器公钥验证传感器上传的进行环签名的多个公钥是否在节点数据库中存储有，从而认证环签名来源于该节点下的一个区块链传感器。每个节点也生成一对公钥和私钥，其中公钥存储在其节点下的所有传感器中，用于传感器加密待传输数据，进一步保证数据传输的安全性。

[0037] 进一步地，所述步骤S3具体为：

[0038] 所述当前区块链传感器将所述多个传感器公钥、所述节点物理标识、所述当前传感器物理标识、所述第二信息和所述第一信息发送给所述当前区块链节点。

[0039] 由上述描述可知，通过物理标识进一步保证数据传输的安全性和可靠性。

[0040] 进一步地，所述步骤S4具体包括以下步骤：

[0041] S41、所述当前区块链节点验证所述节点物理标识是否存储在所述当前区块链节点中，若是则执行步骤S42，否则返回验证失败通知；

[0042] S42、所述当前区块链节点验证所述当前传感器物理标识是否存储在所述当前区块链节点中，若是则执行步骤S43，否则返回验证失败通知；

[0043] S43、所述当前区块链节点采用自身的节点私钥解密所述第一信息，得到所述第一信息中的所述待传输数据信息，并通过环签名算法验证所述第二信息是否由所属区块链传感器生成，若是，则验证通过，将所述待传输数据信息上链，否则返回验证失败通知。

[0044] 由上述描述可知，采用先验证物理标识再验证环签名的方式，从而达到高效的数据认证。

[0045] 进一步地，所述步骤S2具体为：

[0046] 对所述待传输数据信息进行哈希值计算,得到第二哈希值;

[0047] 所述当前区块链传感器采用所述当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述第二哈希值进行环签名,得到第二信息;

[0048] 所述步骤S4中的并通过环签名算法验证所述第二信息是否由所属区块链传感器生成具体为:

[0049] 首先验证所述多个传感器公钥是否在所述当前区块链节点的数据库中存储有,若是,则通过所述多个传感器公钥将所述第二信息解为所述第二哈希值,再正向计算所述待传输数据信息的哈希值为第一哈希值,比对所述第一哈希值与所述第二哈希值是否相同,若是,则所述第二信息是由所属区块链传感器生成,否则所述第二信息不是由所属区块链传感器生成。

[0050] 由上述描述可知,签名一般都是对哈希值进行签名,在当前区块链传感器中对待传输数据信息的哈希值进行环签名之后再传输,由于哈希值是不能得到原始消息的,结合节点公钥加密的待传输数据信息,由于只有节点私钥能够解密得到待传输数据信息,所以即使数据被窃取,窃取方也只能得到加密的待传输数据信息和哈希值,而无法得到原始的待传输数据信息,保证了数据传输的安全性。同时,结合环签名算法,先通过节点数据库中预先存储的所有传感器公钥验证进行环签名的多个传感器公钥是否在数据库中存储有,以保证环签名来源于该节点下的一个传感器,并比对第一哈希值与第二哈希值是否相同再对待传输数据信息进行上链的方式,即保证了数据来源的可靠性,也保证了数据的有效性。

[0051] 请参照图3,一种基于环签名的区块链传感器数据认证系统,包括当前区块链传感器以及当前区块链节点子系统,所述当前区块链传感器包括第一存储器、第一处理器以及存储在第一存储器上并可在第一处理器上运行的第一计算机程序,所述当前区块链节点子系统包括第二存储器、第二处理器以及存储在第二存储器上并可在第二处理器上运行的第二计算机程序;

[0052] 所述第一处理器执行所述第一计算机程序时实现以下步骤:

[0053] S1、采用所属的当前区块链节点的节点公钥加密待传输数据信息,得到第一信息;

[0054] S2、采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名,得到第二信息;

[0055] S3、将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点;

[0056] 所述第二处理器执行所述第二计算机程序时实现以下步骤:

[0057] S4、采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知。

[0058] 由上述描述可知,本发明的有益效果在于:基于同一技术构思,配合上述一种基于环签名的区块链传感器数据认证方法,提供一种基于环签名的区块链传感器数据认证系统,当当前区块链传感器传输数据时,通过采用所属的当前区块链节点的节点公钥对数据进行加密,并采用自身的私钥和同属于当前区块链节点中的任一多个区块链传感器的公钥对数据进行环签名,并将进行环签名的多个传感器公钥、加密的数据以及环签名的数据一起发送给当前区块链节点,从而通过节点私钥解密获得数据及通过环签名算法验证环签名

是否是由自己的区块链传感器所签,保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。

[0059] 进一步地,在所述步骤S1之前,所述第一处理器执行所述第一计算机程序还包括步骤:

[0060] S01、生成并存储所述当前传感器公钥和所述当前传感器私钥,并将所述当前传感器公钥和自身的当前传感器物理标识存储在所述当前区块链节点中,同时将所述当前传感器公钥存储在所述当前区块链节点的所有所属区块链传感器中;

[0061] 所述第二处理器执行所述第二计算机程序还包括步骤:

[0062] S02、生成并存储所述节点公钥和所述节点私钥,并将所述节点公钥和自身的节点物理标识存储在所述区块链节点中的每个所属区块链传感器中。

[0063] 由上述描述可知,每个传感器都生成一对公钥和私钥,其中公钥可存储在同在一个节点下的其他传感器中,方便每个传感器进行数据传输时通过公钥进行环签名,同时公钥还存在所属的当前节点的数据库中,方便后续节点通过数据库中的所有传感器公钥验证传感器上传的进行环签名的多个公钥是否在节点数据库中存储有,从而认证环签名来源于该节点下的一个区块链传感器。每个节点也生成一对公钥和私钥,其中公钥存储在其节点下的所有传感器中,用于传感器加密待传输数据,进一步保证数据传输的安全性。

[0064] 进一步地,所述第一处理器执行所述第一计算机程序的所述步骤S3时具体为:

[0065] 将所述多个传感器公钥、所述节点物理标识、所述当前传感器物理标识、所述第二信息和所述第一信息发送给所述当前区块链节点。

[0066] 由上述描述可知,通过物理标识进一步保证数据传输的安全性和可靠性。

[0067] 进一步地,所述第二处理器执行所述第二计算机程序的所述步骤S4时具体包括以下步骤:

[0068] S41、验证所述节点物理标识是否存储在所述当前区块链节点中,若是则执行步骤S42,否则返回验证失败通知;

[0069] S42、验证所述当前传感器物理标识是否存储在所述当前区块链节点中,若是则执行步骤S43,否则返回验证失败通知;

[0070] S43、采用自身的节点私钥解密所述第一信息,得到所述第一信息中的所述待传输数据信息,并通过环签名算法验证所述第二信息是否由所属区块链传感器生成,若是,则验证通过,将所述待传输数据信息上链,否则返回验证失败通知。

[0071] 由上述描述可知,采用先验证物理标识再验证环签名的方式,从而达到高效的数据认证。

[0072] 进一步地,所述第一处理器执行所述第一计算机程序的所述步骤S2时具体为:

[0073] 对所述待传输数据信息进行哈希值计算,得到第二哈希值;

[0074] 采用所述当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述第二哈希值进行环签名,得到第二信息;

[0075] 所述第二处理器执行所述第二计算机程序的所述步骤S4中的并通过环签名算法验证所述第二信息是否由所属区块链传感器生成具体为:

[0076] 首先验证所述多个传感器公钥是否在所述当前区块链节点的数据库中存储有,若是,则通过所述多个传感器公钥将所述第二信息解为所述第二哈希值,再正向计算所述待

传输数据信息的哈希值为第一哈希值,比对所述第一哈希值与所述第二哈希值是否相同,若是,则所述第二信息是由所属区块链传感器生成,否则所述第二信息不是由所属区块链传感器生成。

[0077] 由上述描述可知,签名一般都是对哈希值进行签名,在当前区块链传感器中对待传输数据信息的哈希值进行环签名之后再传输,由于哈希值是不能得到原始消息的,结合节点公钥加密的待传输数据信息,由于只有节点私钥能够解密得到待传输数据信息,所以即使数据被窃取,窃取方也只能得到加密的待传输数据信息和哈希值,而无法得到原始的待传输数据信息,保证了数据传输的安全性。同时,结合环签名算法,先通过节点数据库中预先存储的所有传感器公钥验证进行环签名的多个传感器公钥是否在数据库中存储有,以保证环签名来源于该节点下的一个传感器,并比对第一哈希值与第二哈希值是否相同再对待传输数据信息进行上链的方式,即保证了数据来源的可靠性,也保证了数据的有效性。

[0078] 请参照图1及图2,本发明的实施例一为:

[0079] 一种基于环签名的区块链传感器数据认证方法,包括步骤:

[0080] S01、当前区块链传感器生成并存储当前传感器公钥和当前传感器私钥,并将当前传感器公钥和自身的当前传感器物理标识存储在当前区块链节点中,同时将当前传感器公钥存储在当前区块链节点的所有所属区块链传感器中;

[0081] 在本实施例中,每个传感器都生成一对公钥和私钥,其中公钥可存储在同在一个节点下的其他传感器中,方便每个传感器进行数据传输时通过公钥进行环签名,同时公钥还存在所属的当前节点的数据库中,方便后续节点通过数据库中的所有传感器公钥验证传感器上传的进行环签名的多个公钥是否在节点数据库中存储有,从而认证环签名来源于该节点下的一个区块链传感器。

[0082] S02、当前区块链节点生成并存储节点公钥和节点私钥,并将节点公钥和自身的节点物理标识存储在区块链节点中的每个所属区块链传感器中;

[0083] 在本实施例中,每个节点也生成一对公钥和私钥,其中公钥存储在其节点下的所有传感器中,用于传感器加密待传输数据,从而保证数据传输的安全性。

[0084] S1、当前区块链传感器采用所属的当前区块链节点的节点公钥加密待传输数据信息,得到第一信息;

[0085] 在本实施例中,如图2所示,该系统中共有n个区块链节点,记第i(i=1,2,...,n)个区块链节点为当前区块链节点,与当前区块链节点连接的共有m个区块链传感器,这m个区块链传感器通过当前区块链节点将数据传输到该区块链系统中,其中,记第j(j=1,2,...,m_i)个区块链传感器为当前区块链传感器。

[0086] 其中,记当前区块链节点的公私钥对为{Mpk_i,Msk_i},当前区块链传感器的公私钥对为$\{pk_j^i, sk_j^i\}$,当前区块链节点的物理标识为$MIden_i$,当前区块链传感器的物理标识为$Iden_j^i$,则第一消息的格式为:

[0087] $$Enc_{Mpk_i}(Message)$$

[0088] 其中,Message为待传输数据信息,Enc为对称加密算法。

[0089] S2、当前区块链传感器采用自身的当前传感器私钥以及当前区块链节点中的任意多个区块链传感器的多个传感器公钥对待传输数据信息进行环签名,得到第二信息;

[0090] 具体为:对待传输数据信息进行哈希值计算,得到第二哈希值;当前区块链传感器采用当前传感器私钥以及当前区块链节点中的任意多个区块链传感器的多个传感器公钥对第二哈希值进行环签名,得到第二信息。

[0091] 在本实施例中,具体为采用(t-1)个传感器公钥对待传输数据进行环签名,第二信息的格式为:

[0092] $$RSig_{\{sk_j^i,pk_1^i,pk_1^i.....pk_{t-1}^i\}}(sha(Message))$$

[0093] 其中,sha为哈希值算法,RSig为环签名算法。

[0094] S3、当前区块链传感器将多个传感器公钥、第一信息和第二信息发送给当前区块链节点;

[0095] 具体为:当前区块链传感器将多个传感器公钥、节点物理标识、当前传感器物理标识、第二信息和第一信息发送给当前区块链节点;其中物理标识能够进一步保证数据传输的安全性和可靠性。

[0096] 在本实施例中,发送的具体格式为:

[0097] $$\{MIden_i\left|Iden_j^i\right|Enc_{Mpk_i}(Message)\left|RSig_{\{sk_j^i,pk_1^i,pk_1^i.....pk_{t-1}^i\}}(sha(Message)\}\right.$$

[0098] S4、当前区块链节点采用自身的节点私钥解密第一信息,得到第一信息中的待传输数据信息,并通过环签名算法验证第二信息是否由所属区块链传感器生成,若是,则验证通过,将待传输数据信息上链,否则返回验证失败通知;

[0099] 具体为:

[0100] S41、当前区块链节点验证节点物理标识是否存储在当前区块链节点中,若是则执行步骤S42,否则返回验证失败通知;即验证$MIden_i$是否在当前区块链节点中;

[0101] S42、当前区块链节点验证当前传感器物理标识是否存储在当前区块链节点中,若是则执行步骤S43,否则返回验证失败通知;即验证$Iden_j^i$是否在当前区块链节点中;

[0102] 在本实施例中,采用先验证物理标识再验证环签名的方式,能够达到高效的数据认证。

[0103] S43、当前区块链节点采用自身的节点私钥解密第一信息,得到第一信息中的待传输数据信息,并通过环签名算法验证第二信息是否由所属区块链传感器生成,若是,则验证通过,将待传输数据信息上链,否则返回验证失败通知;

[0104] 即在本实施例中,通过采用当前区块链节点的节点私钥Msk_i,解密第一信息得到待传输数据信息Message。

[0105] 其中,通过环签名算法验证第二信息是否由所属区块链传感器生成具体为:

[0106] 首先验证多个传感器公钥是否在当前区块链节点的数据库中存储有,若是,则通过当前区块链节点的数据库的任意多个区块链传感器的多个传感器公钥将第二信息解为第二哈希值,再正向计算待传输数据信息的哈希值为第一哈希值,比对第一哈希值与第二哈希值是否相同,若是,则第二信息是由所属区块链传感器生成,否则第二信息不是由所属区块链传感器生成;

[0107] 即在本实施例中,首先通过节点数据库中预先存储的所有传感器公钥验证进行环签名的(t-1)个传感器公钥是否在数据库中存储有,以保证环签名来源于该节点下的一个

传感器,当验证通过时通过采用这(t-1)个传感器公钥,对第二信息进行解环签名,得到sha(Message),然后再对通过节点私钥解密得到的待传输数据信息Message进行哈希值计算并与sha(Message)进行比对验证是否一样。

[0108] 由于哈希值是不能得到原始消息的,结合节点公钥加密的待传输数据信息,由于只有节点私钥能够解密得到待传输数据信息,所以即使数据被窃取,窃取方也只能得到加密的待传输数据信息和哈希值,而无法得到原始的待传输数据信息,保证了数据传输的安全性。同时,结合环签名算法,先通过节点数据库中预先存储的所有传感器公钥验证进行环签名的多个传感器公钥是否在数据库中存储有,以保证环签名来源于该节点下的一个传感器,并比对在当前区块链节点中再进行哈希值计算后得到的第一哈希值与解环签名得到的第二哈希值是否相同再对待传输数据信息进行上链的方式,即保证了数据来源的可靠性,也保证了数据的有效性。

[0109] 请参照图3,本发明的实施例二为:

[0110] 配合上述实施例一的一种基于环签名的区块链传感器数据认证方法,如图2所示,提供一种基于环签名的区块链传感器数据认证系统10,包括当前区块链传感器20以及当前区块链节点子系统30,当前区块链传感器20包括第一存储器21、第一处理器22以及存储在第一存储器21上并可在第一处理器22上运行的第一计算机程序,当前区块链节点子系统30包括第二存储器31、第二处理器32以及存储在第二存储器31上并可在第二处理器32上运行的第二计算机程序。

[0111] 其中,第一处理器22执行第一计算机程序时实现上述实施例一中的步骤S01、S1、S2和S3,第二处理器32执行第二计算机程序时实现上述实施例一中的步骤S02、S4及其对应的子步骤S41、S42和S43。

[0112] 综上所述,本发明提供的一种基于环签名的区块链传感器数据认证方法及系统,当当前区块链传感器传输数据时,通过采用所属的当前区块链节点的节点公钥对数据进行加密,并采用自身的私钥和同属于当前区块链节点中的任一多个区块链传感器的公钥对数据进行环签名,并将进行环签名的多个传感器公钥、加密的数据、环签名的数据、当前区块链传感器的物理标识以及当前区块链节点的物理标识一起发送给当前区块链节点。首先通过先依次验证当前区块链节点的物理标识和当前区块链传感器的物理标识是否存储在当前区块链节点中,保证数据传输的安全性和可靠性的同时达到高效的数据认证;其次通过利用节点私钥解密得到待传输的数据信息,再通过环签名算法验证环签名是否是由自己的区块链传感器所签,其中,对待传输数据信息进行环签名时是对其的哈希值进行环签名,由于哈希值是不能得到原始消息的,故而在传输过程中就算环签名被窃取,窃取方也无法得到原始的待传输数据信息,保证了数据传输的安全性,同时由于节点公钥加密的待传输数据信息只有节点私钥能够进行解密,而节点私钥只有区块链节点拥有,所以在传输过程中如果加密的待传输数据信息也被窃取,窃取方也无法得到原始的待传输数据信息,更进一步保证了数据传输的安全性;最后通过环签名算法,先通过节点数据库中预先存储的所有传感器公钥验证进行环签名的多个传感器公钥是否在数据库中存储有,以保证环签名来源于该节点下的一个传感器,再将节点私钥解密得到的待传输数据信息再计算哈希值,与解环签名得到的哈希值进行比对是否相同而决定是否对待传输数据信息进行上链的方式,在保证数据传输的安全性的同时也保证了数据来源的真实性和有效性。

[0113] 以上所述仅为本发明的实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等同变换,或直接或间接运用在相关的技术领域,均同理包括在本发明的专利保护范围内。

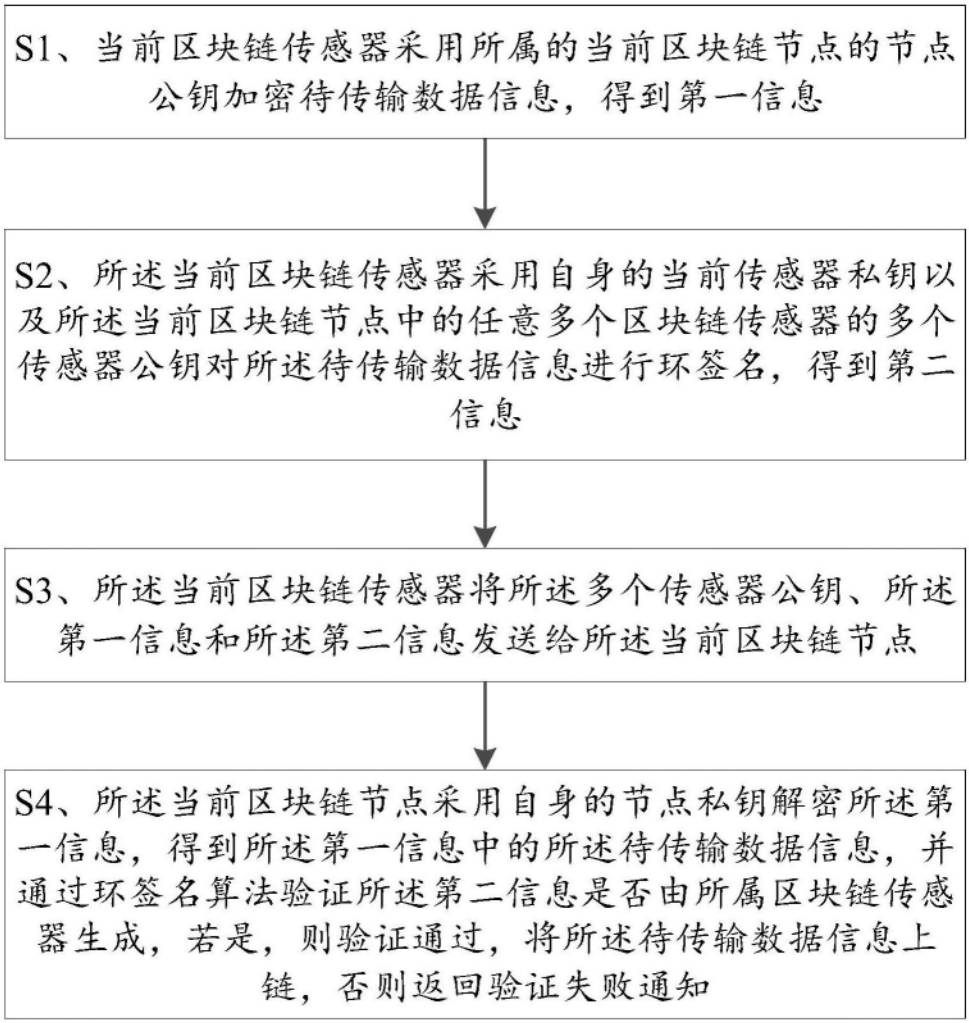

S1、当前区块链传感器采用所属的当前区块链节点的节点公钥加密待传输数据信息，得到第一信息
S2、所述当前区块链传感器采用自身的当前传感器私钥以及所述当前区块链节点中的任意多个区块链传感器的多个传感器公钥对所述待传输数据信息进行环签名，得到第二信息
S3、所述当前区块链传感器将所述多个传感器公钥、所述第一信息和所述第二信息发送给所述当前区块链节点
S4、所述当前区块链节点采用自身的节点私钥解密所述第一信息，得到所述第一信息中的所述待传输数据信息，并通过环签名算法验证所述第二信息是否由所属区块链传感器生成，若是，则验证通过，将所述待传输数据信息上链，否则返回验证失败通知

图1

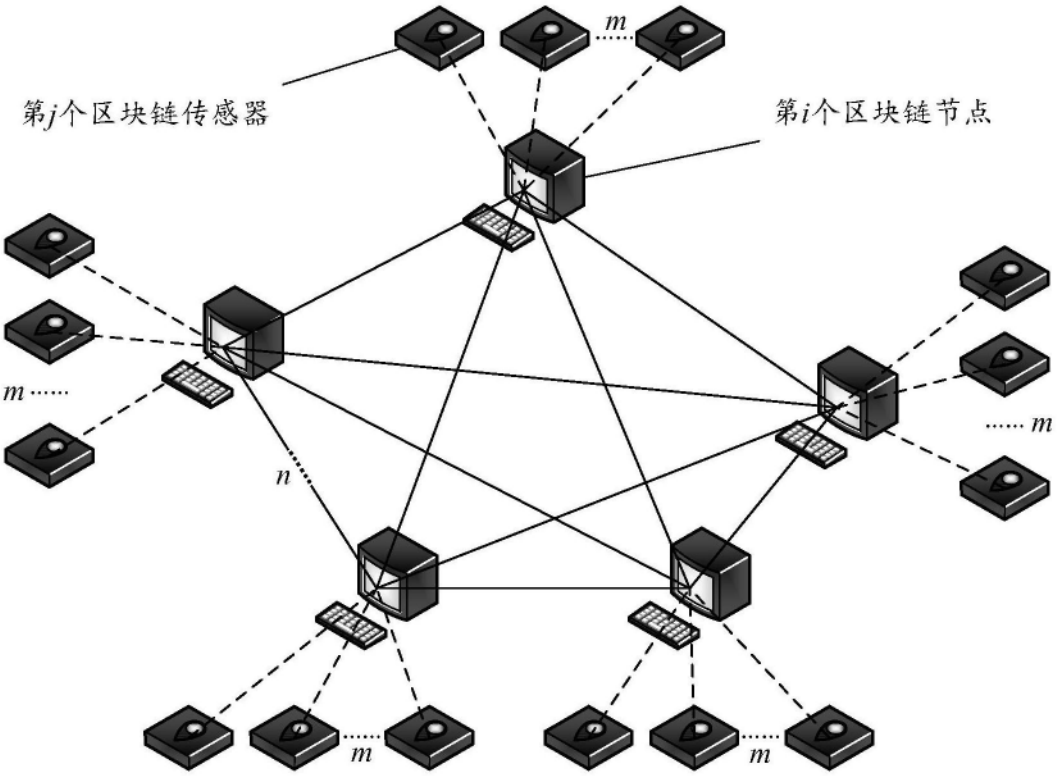

第j个区块链传感器
第i个区块链节点
m
m
m
n
m
m

图2

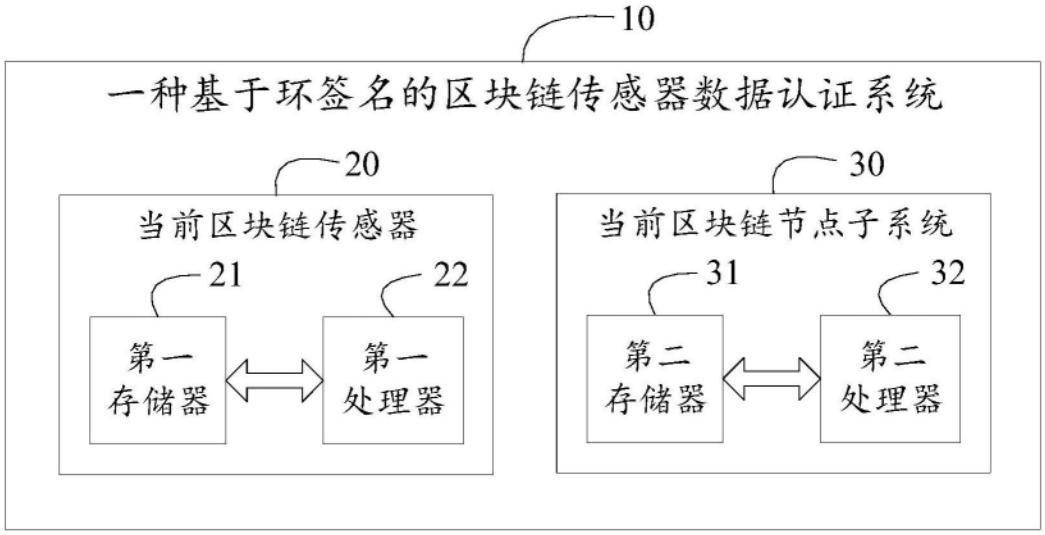

10
一种基于环签名的区块链传感器数据认证系统
20
当前区块链传感器
21
第一存储器
22
第一处理器
30
当前区块链节点子系统
31
第二存储器
32
第二处理器

图3