(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 110012015 A
(43)申请公布日 2019.07.12

(21)申请号 201910280490.8

(22)申请日 2019.04.09

(71)申请人 中国科学院沈阳计算技术研究所有限公司
地址 110168 辽宁省沈阳市东陵区南屏东路16号

(72)发明人 于金刚 张弘 李航宇 孙建伟 于波 毛立爽 姬鹏翔

(74)专利代理机构 沈阳科苑专利商标代理有限公司 21002
代理人 李巨智

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)

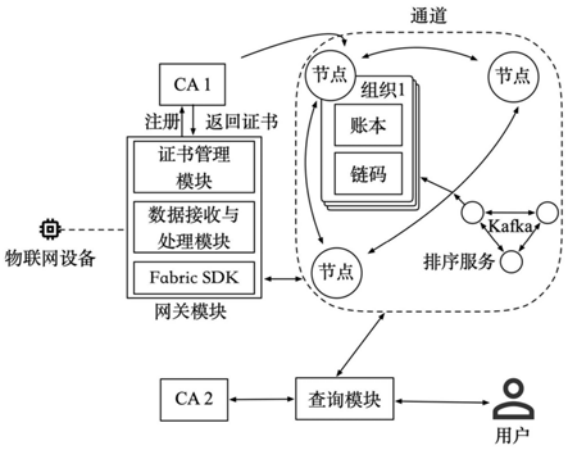
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于区块链的物联网数据共享方法及系统

(57)摘要

本发明涉及一种基于区块链的物联网数据共享方法及系统，系统包括证书管理模块、网关模块和通道；方法包括物联网设备通过网关模块向CA申请注册，CA向网关模块返回证书，并存储于网关模块内的证书管理模块；网关模块接收数据信息进行处理，通过Fabric SDK发送给节点；节点进行背书，返回给Fabric SDK；Fabric SDK根据背书策略将收集到的数据信息发送给排序服务，排序服务按时间顺序进行排序后打包成区块，广播给通道内的节点；节点收到区块后，对其进行验证，将区块写入本地账本。本发明在不借助单一可信中心化机构的前提下，帮助参与方直接建立信任，保障数据能够安全共享，提升价值传递效率，区块链数据结构降低了数据被篡改的风险。



CN 110012015 A

1.一种基于区块链的物联网数据共享方法,其特征在于,包括以下步骤:

步骤1:物联网设备通过网关模块向第一CA申请注册,第一CA向网关模块返回证书,并存储于网关模块内的证书管理模块;

步骤2:网关模块接收物联网设备的数据信息,对数据信息进行处理,并将处理后的数据信息通过Fabric SDK发送给通道内的节点;

步骤3:通道内的节点收到Fabric SDK发送的数据信息后,对数据信息进行背书,并将背书后的数据信息返回给Fabric SDK;

步骤4:Fabric SDK根据背书策略将收集到的背书后的数据信息发送给排序服务,排序服务对收到的数据信息按时间顺序进行排序后打包成区块,广播给通道内的节点;

步骤5:通道内的节点收到区块后,对其进行验证,将通过验证后的区块写入本地账本。

2.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:所述物联网设备通过网关模块向第一CA申请注册包括以下过程:

网关模块向第一CA的enroll接口发送HTTP POST请求,第一CA收到请求后进行验证,如果合法,在本地生成证书,返回给网关,如果不合法,向网关模块发回非法提示。

3.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:所述对数据信息进行处理包括:格式转化、数据清洗、数据归一化。

4.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:所述背书为:节点对Fabric SDK发送的数据信息的合法性和权限进行检查,如果检查通过,则对收到该数据信息产生的状态变化进行模拟,如果模拟的数据结果合法,则对该数据信息进行保证。

5.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:所述验证包括:交易消息结构、签名完整性、是否重复、读写集合版本是否匹配。

6.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:查询模块向第二CA申请证书,并携带证书通过调用链码对通道内的账本进行访问。

7.根据权利要求1或2所述的基于区块链的物联网数据共享方法,其特征在于:所述网关模块包括:

证书管理模块,用于存储物联网设备的证书;

数据接收与处理模块,用于接收物联网设备的数据信息并对其进行处理,将处理后的数据信息发送给Fabric SDK;

Fabric SDK,用于与通道进行交互。

8.根据权利要求1所述的基于区块链的物联网数据共享方法,其特征在于:所述排序服务为:为网络中所有合法的数据信息进行全局排序,并分批次将其中排序后的数据信息组合生成区块结构。

9.一种基于权利要求1～8任一项所述方法的物联网数据共享系统,其特征在于,包括:

物联网设备,用于向网关模块发送注册申请以及数据信息;

网关模块,用于根据物联网设备的注册申请向第一CA申请注册,网关模块内的证书管理模块接收第一CA返回的证书;网关模块内的数据接收与处理模块接收物联网设备的数据信息,对数据信息进行处理;网关模块内的Fabric SDK将处理后的数据信息发送给通道内的节点,并根据背书策略将收集到的背书后的数据信息发送给通道内的排序服务;

通道,包括若干节点和排序服务,其中节点收到Fabric SDK发送的数据信息后,对数据信息进行背书,并将背书后的数据信息返回给Fabric SDK;排序服务对收到的数据信息按时间顺序进行排序后打包成区块,广播给通道内的节点;通道内的节点收到区块后,对其进行验证,将通过验证后的区块写入本地账本。

10.根据权利要求9所述的基于区块链的物联网数据共享系统,其特征在于,还包括查询模块,向第二CA申请证书,并携带证书通过调用链码对通道内的账本进行访问。

一种基于区块链的物联网数据共享方法及系统

技术领域

[0001] 本发明涉及区块链技术领域以及物联网技术领域，具体地说是一种基于区块链的物联网数据共享方法及系统。

背景技术

[0002] 物联网是物品之间通过互联网连接起来共享信息的网络。随着物联网技术的发展，网络的结构日益复杂，采集的数据量呈现爆发式增长，信息孤岛问题日益突出，如何在不同的参与方间安全地共享数据成为了一个巨大的挑战。一种典型的方式是引入可信的中心化机构，由该机构负责收集、传输和管理数据，但这种方案有一些显著的缺陷：

[0003] 1.中心化机构需要负责设备的管理、数据的存储和传输，一旦其出现故障，整个系统将陷入瘫痪。

[0004] 2.中心化机构对参与方不透明，权力过大，如果遭到外部攻击，数据可能会被篡改。

[0005] 3.数据传输必须经过中心化机构，而数据提供方的一些隐私数据可能更希望直接与数据需求方共享。

[0006] 区块链起源于比特币，是一种由多方维护、数据无法更改的分布式账本技术，具有去中心化、共同维护、不可篡改、加密安全等特征。它能够在脱离中心化机构的情况下使参与方建立互信，这一优势适合于改进物联网现有架构。区块链通过共识机制确保账本数据的一致性，任何参与者都无法绝对获得账本的控制权。它将数据按时间顺序打包至区块，每个区块均包含前一区块的摘要信息，从而形成链式的数据结构，并以密码学方式保证上链数据不被篡改和伪造。区块链一般还包含智能合约(也称作链码)，可以将规则或合同编码为程序部署到区块链上，触发条件后按事先的约定自动执行。

[0007] 根据参与者权限的不同，区块链一般分为公有链、私有链和联盟链。开源的Hyperledger Fabric是联盟链的代表，它在最大程度保留区块链优点的基础上，增加支持了权限管理和身份认证，设计上可插拔、可扩展，其共识机制、成员服务、加密算法、底层数据库等均可灵活替换，方便满足不同场景的使用需求。Hyperledger Fabric借助CA(Certificate Authority，证书颁发机构)实现了权限的管理，采用通道机制隔离了不同的参与方。

[0008] 现有技术由于引入中心化机构，普遍存在单点故障问题，数据共享不透明，存在被篡改的风险，数据的可用性和安全性得不到保障。本申请的技术方案利用区块链去中心化的特征，分散了提供服务的节点，降低了单点故障风险；利用区块链这一不可篡改的数据结构，提高了共享时的透明度，保证了数据的完整可靠。

发明内容

[0009] 针对现有技术的不足，本发明提供一种基于区块链的物联网数据共享方法及系统，有效避免了单点故障问题，提高了数据共享效率，其权限管理方案保证了系统的安全性

和隐私性,区块链数据结构降低了数据被篡改的风险。

[0010] 本发明为实现上述目的所采用的技术方案是:

[0011] 一种基于区块链的物联网数据共享方法,包括以下步骤:

[0012] 步骤1:物联网设备通过网关模块向第一CA申请注册,第一CA向网关模块返回证书,并存储于网关模块内的证书管理模块;

[0013] 步骤2:网关模块接收物联网设备的数据信息,对数据信息进行处理,并将处理后的数据信息通过Fabric SDK发送给通道内的节点;

[0014] 步骤3:通道内的节点收到Fabric SDK发送的数据信息后,对数据信息进行背书,并将背书后的数据信息返回给Fabric SDK;

[0015] 步骤4:Fabric SDK根据背书策略将收集到的背书后的数据信息发送给排序服务,排序服务对收到的数据信息按时间顺序进行排序后打包成区块,广播给通道内的节点;

[0016] 步骤5:通道内的节点收到区块后,对其进行验证,将通过验证后的区块写入本地账本。

[0017] 所述物联网设备通过网关模块向第一CA申请注册包括以下过程:

[0018] 网关模块向第一CA的enroll接口发送HTTP POST请求,第一CA收到请求后进行验证,如果合法,在本地生成证书,返回给网关,如果不合法,向网关模块发回非法提示。

[0019] 所述对数据信息进行处理包括:格式转化、数据清洗、数据归一化。

[0020] 所述背书为:节点对Fabric SDK发送的数据信息的合法性和权限进行检查,如果检查通过,则对收到该数据信息产生的状态变化进行模拟,如果模拟的数据结果合法,则对该数据信息进行保证。

[0021] 所述验证包括:交易消息结构、签名完整性、是否重复、读写集合版本是否匹配。

[0022] 还包括查询模块向第二CA申请证书,并携带证书通过调用链码对通道内的账本进行访问。

[0023] 所述网关模块包括:

[0024] 证书管理模块,用于存储物联网设备的证书;

[0025] 数据接收与处理模块,用于接收物联网设备的数据信息并对其进行处理,将处理后的数据信息发送给Fabric SDK;

[0026] Fabric SDK,用于与通道进行交互。

[0027] 所述排序服务为:为网络中所有合法的数据信息进行全局排序,并分批次将其中排序后的数据信息组合生成区块结构。

[0028] 一种基于区块链的物联网数据共享系统,包括:

[0029] 物联网设备,用于向网关模块发送注册申请以及数据信息;

[0030] 网关模块,用于根据物联网设备的注册申请向第一CA申请注册,网关模块内的证书管理模块接收第一CA返回的证书;网关模块内的数据接收与处理模块接收物联网设备的数据信息,对数据信息进行处理;网关模块内的Fabric SDK将处理后的数据信息发送给通道内的节点,并根据背书策略将收集到的背书后的数据信息发送给通道内的排序服务;

[0031] 通道,包括若干节点和排序服务,其中节点收到Fabric SDK发送的数据信息后,对数据信息进行背书,并将背书后的数据信息返回给Fabric SDK;排序服务对收到的数据信息按时间顺序进行排序后打包成区块,广播给通道内的节点;通道内的节点收到区块后,对

其进行验证,将通过验证后的区块写入本地账本。

[0032] 还包括查询模块,向第二CA申请证书,并携带证书通过调用链码对通道内的账本进行访问。

[0033] 本发明具有以下有益效果及优点:

[0034] 1.物联网拓扑去中心化,节点高度自治,即使某些节点发生故障,系统整体仍然能够正常工作;

[0035] 2.由CA提供安全灵活的权限管理方案,保证只有授权成员读写数据,数据在不同的参与方之间可以被安全共享;

[0036] 3.数据由多个参与方共同维护,某一方对数据的篡改不会被系统整体所接受,已写入的数据不可更改。

附图说明

[0037] 图1是本发明的系统示意图。

具体实施方式

[0038] 下面结合附图及实施例对本发明做进一步的详细说明。

[0039] 为使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图对本发明的具体实施方式做详细的说明。在下面的描述中阐述了很多具体细节以便于充分理解本发明。但本发明能够以很多不同于在此描述的其他方式来实施,本领域技术人员可以在不违背发明内涵的情况下做类似改进,因此本发明不受下面公开的具体实施的限制。

[0040] 除非另有定义,本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在发明的说明书中所使用的术语只是为了描述具体的实施例的目的,不是旨在于限制本发明。

[0041] 如图1所示为本发明的系统示意图。

[0042] 一种基于区块链的物联网数据共享方法,其特征在于:

[0043] 区块链网络,基于Hyperledger Fabric构建,由物联网参与方协商该网络的配置,共同维护;参与方从属于各自的组织,组织通过CA进行成员身份管理,并维护排序服务和节点,节点中的账本利用区块链这一数据结构以不可篡改的方式存储数据;组织间通过建立通道与外部隔离,以便在通道内部共享数据;这些数据不由单一方控制,而是基于协商的通道策略集体维护;

[0044] 网关模块,负责在物联网设备及所述区块链网络间处理和传输数据,包括证书管理模块、数据接收与处理模块、Fabric SDK;所述证书管理模块帮助新加入的物联网设备向CA申请证书,收到CA返回的证书后,将其加密存储于本地数据库,并记录证书与物联网设备的对应关系;所述数据接收与处理模块对物联网设备采集的数据进行必要的清洗、格式转换、打包等处理;所述Fabric SDK 使用对应物联网设备的证书为上一步处理完的数据进行签名,将其封装后发送至对应的通道;所述Fabric SDK为一套开发工具,封装了节点提供的服务接口。

[0045] 查询模块,供数据需求方对数据进行查询;所述查询模块携带自身证书,调用链码访问账本上记录的数据,相关人员或设备可以进一步利用。

[0046] 所述网关模块对所述区块链网络中的各类事件进行监听，基于事件采取下一步的操作。

[0047] 为所述通道创建能够记录查询日志的附属通道，形成双链体系；所述通道上对数据的每一次查询，都通过在链码中调用附属通道的链码，将查询项目和查询时间等信息写入附属通道；一旦所述通道的数据发生泄露，通过分析附属通道的记录，可以追查到薄弱环节和泄露的范围。

[0048] 对隐私数据进行更细粒度的控制，在所述网关模块向所述通道发送数据时，将隐私数据存储在特殊域中，节点上的链码探测到该特殊域，自动计算隐私数据的散列值，后续仅向所述通道广播散列值，真实值存储在节点本地数据库；当数据需求方希望访问隐私数据时，可以向节点请求，如果该数据需求方被授予了权限，节点从本地读取或向其他存有数据的节点请求后将数据返回，数据需求方对收到的数据计算散列值，将该值与记入账本的值做对比以确认数据的真实性。

[0049] 实施例：

[0050] 物联网设备在实施例中使用DHT22温湿度传感器，通过GPIO针脚连接到网关。

[0051] 网关使用树莓派3B，装有Raspbian Stretch Lite系统，通过无线网络与CA 及区块链网络相连接。其中，CA采用Fabric CA实现，运行在服务器上。网关上运行Python脚本，用于从GPIO针脚接收数据并进行处理。网关后续与CA交互的步骤如下：

[0052] 1.网关确认新加入物联网设备的身份，获取其设备类型等元数据，设置设备 ID。

[0053] 2.若确认无误，网关调用Fabric CA的RESTful API，向所在组织的CA申请该设备的身份证书。

[0054] 3.CA收到申请后，生成必要的证书材料，返回给网关。CA事先已经在区块链网络中的通道、排序服务、节点等组件的配置中获得了授权，因此其颁发的ECerts(登记证书)、TCerts(交易证书)等能够在网络中使用。

[0055] 4.网关收到证书后，将其交给本地的证书管理模块，由证书管理模块加密存储于本地数据库，并记录证书与物联网设备的对应关系。

[0056] 前述区块链网络包含1个通道，1组在Apache Kafka上的排序服务，分属于 Org1和Org2组织的若干节点，Org1提供数据，Org2获取数据。这些组件部署在不同的服务器上，通过gRPC协议通信。

[0057] 区块链网络和通道的配置文件中设有权限策略，限定了成员具备那些特定的权限。

[0058] 网关使用对应物联网设备的证书将处理后的数据进行签名，封装成交易提案后通过Fabric SDK发送至通道内的节点。

[0059] 节点和排序服务对收到的交易进行背书、排序，最终广播至通道内全部节点，写入本地账本。

[0060] 优选地，网关对区块链网络中的各类事件进行监听，基于事件采取下一步的操作。

[0061] 优选地，为通道创建能够记录查询日志的附属通道，进而在通道上实例化调用附属通道链码的相关链码，使得对数据的每一次查询，都将查询的范围和查询者的信息记录到附属通道。

[0062] 优选地，在网关模块向通道的节点发送数据时，将隐私数据存储在transient 这

一特殊域中，节点上的链码探测到该特殊域，自动计算隐私数据的散列值，后续仅向通道广播散列值，真实值存储在节点本地私有数据库。当数据需求方希望访问隐私数据时，可以向节点请求，如果该数据需求方被授予了权限，节点从本地读取或向其他存有数据的节点请求后将数据返回，数据需求方对收到的数据计算散列值，将该值与记入账本的值做对比以确认数据的真实性。

[0063] 查询模块是Web应用程序，底层通过Fabric SDK提供的API调用查询链码，为数据需求方提供通道策略所允许数据。

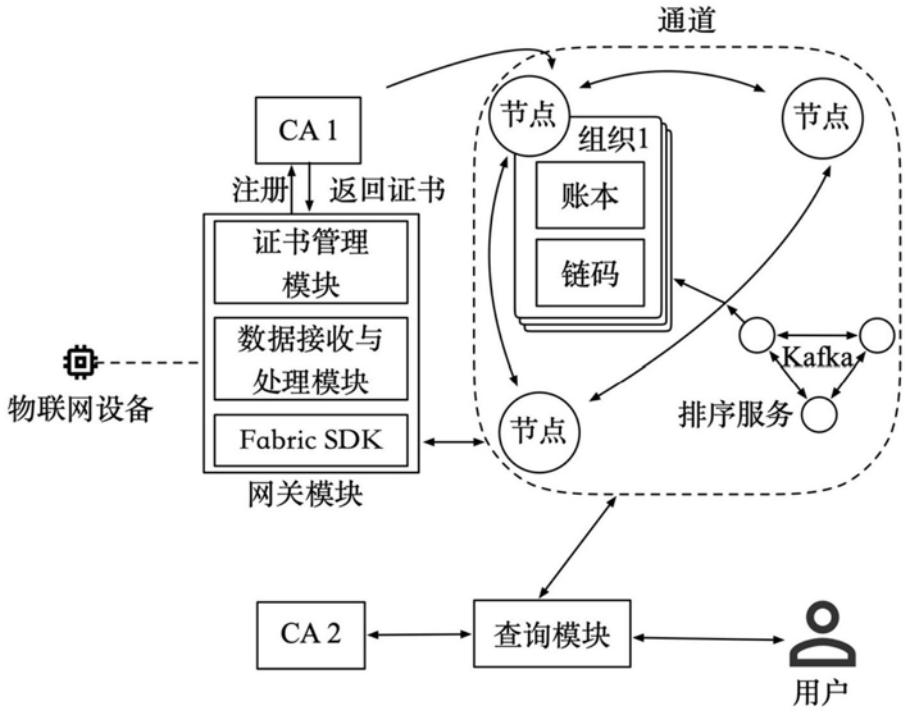

通道
CA 1
注册
返回证书
证书管理模块
数据接收与处理模块
Fabric SDK
网关模块
物联网设备
节点
组织1
账本
链码
节点
节点
Kafka
排序服务
CA 2
查询模块
用户

图1