(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 112769894 A
(43)申请公布日 2021.05.07

(21)申请号 202011494197.0

(22)申请日 2020.12.17

(71)申请人 国网浙江省电力有限公司信息通信分公司
地址 310020 浙江省杭州市江干区市民街219号
申请人 国网浙江德清县供电有限公司
浙江工业大学
北京隐山科技有限公司

(72)发明人 李洋 胡凯 曹维珊 洪成 章振海 唐玉平 姚宸杨 张烨华 陈海龙 王凌 顾国民 陈铁明 宋琪杰 刘媛

(74)专利代理机构 杭州斯可睿专利事务所有限公司 33241
代理人 王利强

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

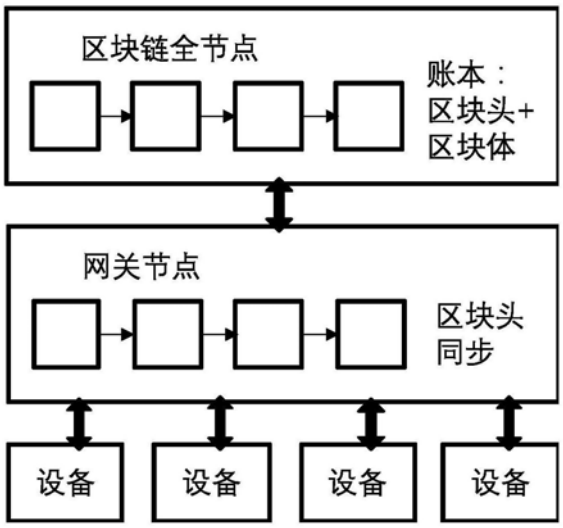
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种基于区块链Merkle树验证的设备认证方法

(57)摘要

一种基于区块链Merkle树验证的设备认证方法,包括如下步骤:步骤一:可编程网关通过区块链接口进行区块头同步。步骤二:设备提交注册信息后,由网关构建交易存入区块链,并返回交易hash值作为凭证;步骤三:设备携带注册交易hash向网关发起认证请求;步骤四:将注册hash与路径值中的hash进行一一运算,获得根hash值,并与网关区块头中同步的最长链中的区块Merkle根hash进行比较,找到相等区块,并获取已经确认数量,若大于设定确认,则认证有效通过;步骤五:网关将定时对设备进行认证。本发明可杜绝设备隐私信息的传播,并无需等待区块链确认进行交易信息,即认证信息的验证,提高设备认证安全性。



CN 112769894 A

1.一种基于区块链Merkle树验证的设备认证方法,其特征在于,所述方法包括如下步骤:

步骤一:网关接入区块链网络,当区块链生成新区块后,网关将对区块链中的区块头进行同步,区块头中包含前置区块hash,Merkle根hash值以及后置区块hash信息;

步骤二:设备提交注册信息,该信息中包含设备的基本信息,提交进行设备注册,网关接受到注册信息后,根据区块链要求构建交易对象Tx,并获取交易对象的hash值hash(Tx);

步骤三:网关将Tx提交区块链进行入链注册,并同步将hash(Tx)作为认证凭证下发给设备进行存储,区块链收到Tx后进行挖矿共识认证,认证完成后,入链记录,并返回回执给网关;

步骤四:设备发起认证请求,认证请求中仅包含hash(Tx),网关收到后,通过该值,向区块链获取该交易所在区块的Merkle树hash路径;

步骤五:网关通过路径与hash(Tx)计算,得到根hash值,并与同步区块头的最长链进行对比,获取得到与该hash值一致的区块头,并获取比该区块头高度高的区块数量,若大于设定次数,则认证成功;

步骤六:网关记录设备认证情况,并更新认证时间,构建设备的新认证信息进行入链更新,回到步骤三的过程,网关在等待认证有效期过后,回到步骤四的过程进行重新认证。

一种基于区块链Merkle树验证的设备认证方法

技术领域

[0001] 本发明涉及一种基于Merkle树验证的设备认证方法，更具体说，它涉及一种通过交易hash以及区块中的Merkle根路径进行验证的设备认证方法。

背景技术

[0002] 随着工业互联网的发展，物联网终端呈现海量增长的趋势。大部分设备是无人值守的，很多情况下需要特定用户通过网络远程管理控制设备，所以对于设备的身份识别认证等安全措施显得尤为重要。常用的安全机制是对每个设备进行身份标识，从而进行区分，当设备连接进入网络时，还需要一个特定的密码以防止恶意用户或身份伪造。在传统的认证系统中。使用认证服务器进行设备认证，但仅凭认证服务器生成的认证信息并不能很好的保证用户设备的唯一性，因为认证服务器发送的认证信息仍有可能被第三方进行劫持或攻击。

[0003] 而区块链的提出，为解决物联网设备认证提供了新的机会与挑战。区块链的本质是一个去中心化的分布式账本系统，具有去中心化、信息不可篡改、数据公开透明等基本特点以及共识机制、智能合约、非对称加密三大保障机制。Merkle树是区块链种一种数据结构，进行交易hash的存储。Merkle树大多用来进行交易信息的完整性验证。传统区块链应用于物联网设备主要用于存储设备的密钥以及相关信息，但是区块链共识验证需要一定时间，导致设备验证无法得到及时的回复。同时，验证信息会携带设备相关信息，导致信息泄漏。将设备认证信息与Merkle树认证相结合，为设备认证提供新思路。

发明内容

[0004] 为了克服现有设备认证信息入链验证慢、设备相关信息易泄漏等不足，本发明提供一种高效、保护设备隐私信息安全的基于基于区块链Merkle树验证的设备认证方法

[0005] 为解决上述技术问题本发明提供如下技术方案：

[0006] 一种基于区块链Merkle树验证的设备认证方法，包括如下步骤：

[0007] 步骤一：网关接入区块链网络，当区块链生成新区块后，网关将对区块链中的区块头进行同步，区块头中包含前置区块hash，Merkle根hash值以及后置区块hash等关键信息；

[0008] 步骤二：设备提交注册信息，该信息中包含设备的基本信息，提交进行设备注册，网关接受到注册信息后，根据区块链要求构建交易对象Tx，并获取交易对象的hash值hash(Tx)；

[0009] 步骤三：网关将Tx提交区块链进行入链注册，并同步将hash(Tx)作为认证凭证下发给设备进行存储，区块链收到Tx后进行挖矿共识认证，认证完成后，入链记录，并返回回执给网关；

[0010] 步骤四：设备发起认证请求，认证请求中仅包含hash(Tx)，网关收到后，通过该值，向区块链获取该交易所在区块的Merkle树hash路径；

[0011] 步骤五：网关通过路径与hash(Tx)计算，得到根hash值，并与同步区块头的最长链

进行对比，获取得到与该hash值一致的区块头，并获取比该区块头高度高的区块数量，若大于设定次数，则认证成功；

[0012] 步骤六：网关记录设备认证情况，并更新认证时间，构建设备的新认证信息进行入链更新，回到步骤三的过程，网关在等待认证有效期过后，回到步骤四的过程进行重新认证。

[0013] 本发明中，可编程网关通过区块链接口进行区块同步，同步的区块链仅仅只同步区块头，而不进行区块体的同步，减少网关数据的存储量；网关将定时对设备进行认证，认证后，同步修改在注册信息中的最新认证时间，相应的hash值也会进行变动，则重复上述过程，对下层设备进行认证。

[0014] 本发明的有益效果表现在：(1)与目前主流的认证方法相比，该发明通过区块链与Merkle根hash进行认证，减少通过数字证书等方式造成的密钥泄漏安全隐患。(2)将设备的注册认证信息存储在区块链，不可篡改，保证信息的安全存储。(3)使用同步区块头的方式进行认证，减少区块全账本同步的存储压力，网关通过同步区块头加入区块链网络，构建可信关系。(4)本发明通过验证hash进行设备注册和认证，减少设备信息在网络种的交互，避免设备隐私造成泄漏，同时，无需等待区块链对注册和认证信息的验证，提高了交互的效率，减少网络等待时间，增加系统吞吐量。(5)本发明实现了面向设备的区块链服务，具备一定计算能力的设备都可接入网关，具有较高的通用性。

附图说明

[0015] 图1为通过区块链进行设备认证的架构图；

[0016] 图2为通过交易构建Merkle根hash值的方法；

[0017] 图3为基于区块链Merkle树验证的设备认证方法时序图。

具体实施方式

[0018] 下面结合附图对本发明做进一步描述。

[0019] 参照图1～图3，一种基于区块链Merkle树验证的设备认证方法，本发明包含三部分，分别为区块链系统，网关节点以及设备，其中，区块链由全节点构成，记录同步的账本中包含区块头和区块体；网关节点关联区块链全节点，但是仅仅同步区块头；设备与网关相连，进行注册认证等相关操作。

[0020] 如图2所示，为Merkle树根hash的计算方式，TxA、TxB、TxC和TxD分别为一个时间段内产生的交易，通过hash(TxN)计算得到交易的hash值Hash0-0、Hash0-1、Hash1-0、Hash1-1，之后对其两两hash，得到Hash0、Hash1；以此循环，直到得到最后一个两两hash的值，即为最后的Merkle树根hash值，该值包含了该区块下的所有交易签名。

[0021] 如图3所示，一种基于区块链Merkle树验证的设备认证方法，包括如下步骤：

[0022] 步骤一：网关接入区块链网络，当区块链生成新区块后，网关将对区块链中的区块头进行同步，区块头中主要包含前置区块hash，Merkle根hash值以及后置区块hash等信息；

[0023] 步骤二：设备提交注册信息RegisterInfo，该信息中主要包含设备的基本信息，提交进行设备注册，网关接受到注册信息后，根据区块链要求构建交易对象Tx，并获取交易对象的hash值hash(Tx)；

[0024] 步骤三:网关将Tx提交区块链进行入链注册,并同步将hash(Tx)作为认证凭证下发给设备进行存储,区块链收到Tx后进行挖矿共识认证,认证完成后,入链记录,并返回回执给网关;

[0025] 步骤四:设备发起认证请求,认证请求中仅包含hash(Tx),网关收到后,通过该值,向区块链获取该交易所在区块的Merkle树hash路径;

[0026] 步骤五:网关通过路径与hash(Tx)计算,得到根hash值,并与同步区块头的最长链进行对比,获取得到与该hash值一致的区块头,并获取比该区块头高度高的区块数量,若大于设定次数(例如6),则认证成功;

[0027] 步骤六:网关记录设备认证情况,并更新认证时间,构建设备的新认证信息进行入链更新,回到步骤三的过程,网关在等待认证有效期过后,回到步骤四的过程进行重新认证。

[0028] 上述实施例的说明只是用于帮助理解本发明。应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以对本发明进行若干改进和修饰,这些改进和修饰也落入本发明权利要求的保护范围内。

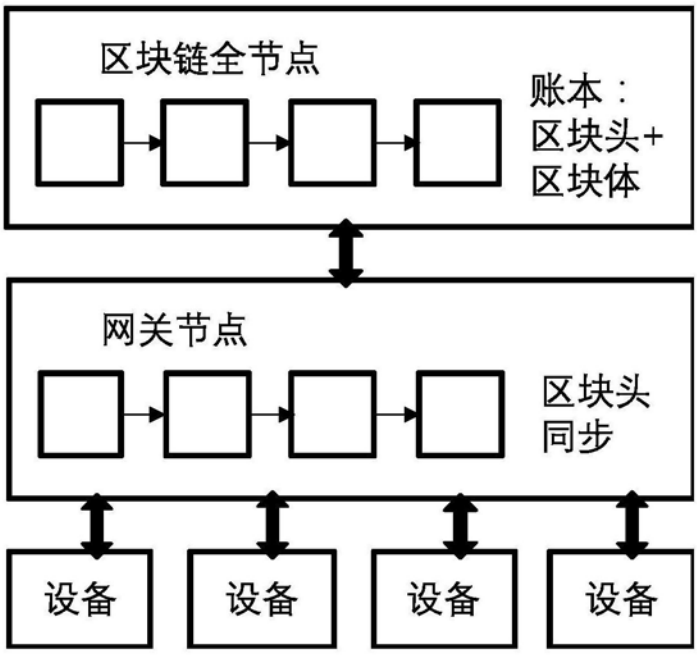

区块链全节点
账本：
区块头+
区块体
网关节点
区块头
同步
设备
设备
设备
设备

图1

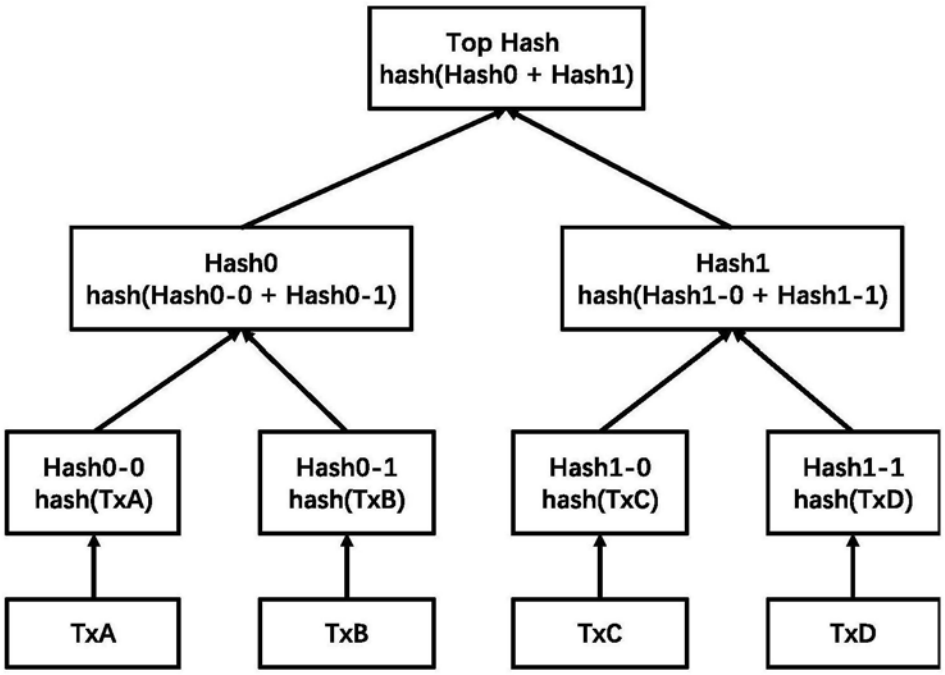

Top Hash
hash(Hash0 + Hash1)
Hash0
hash(Hash0-0 + Hash0-1)
Hash1
hash(Hash1-0 + Hash1-1)
Hash0-0
hash(TxA)
Hash0-1
hash(TxB)
Hash1-0
hash(TxC)
Hash1-1
hash(TxD)
TxA
TxB
TxC
TxD

图2

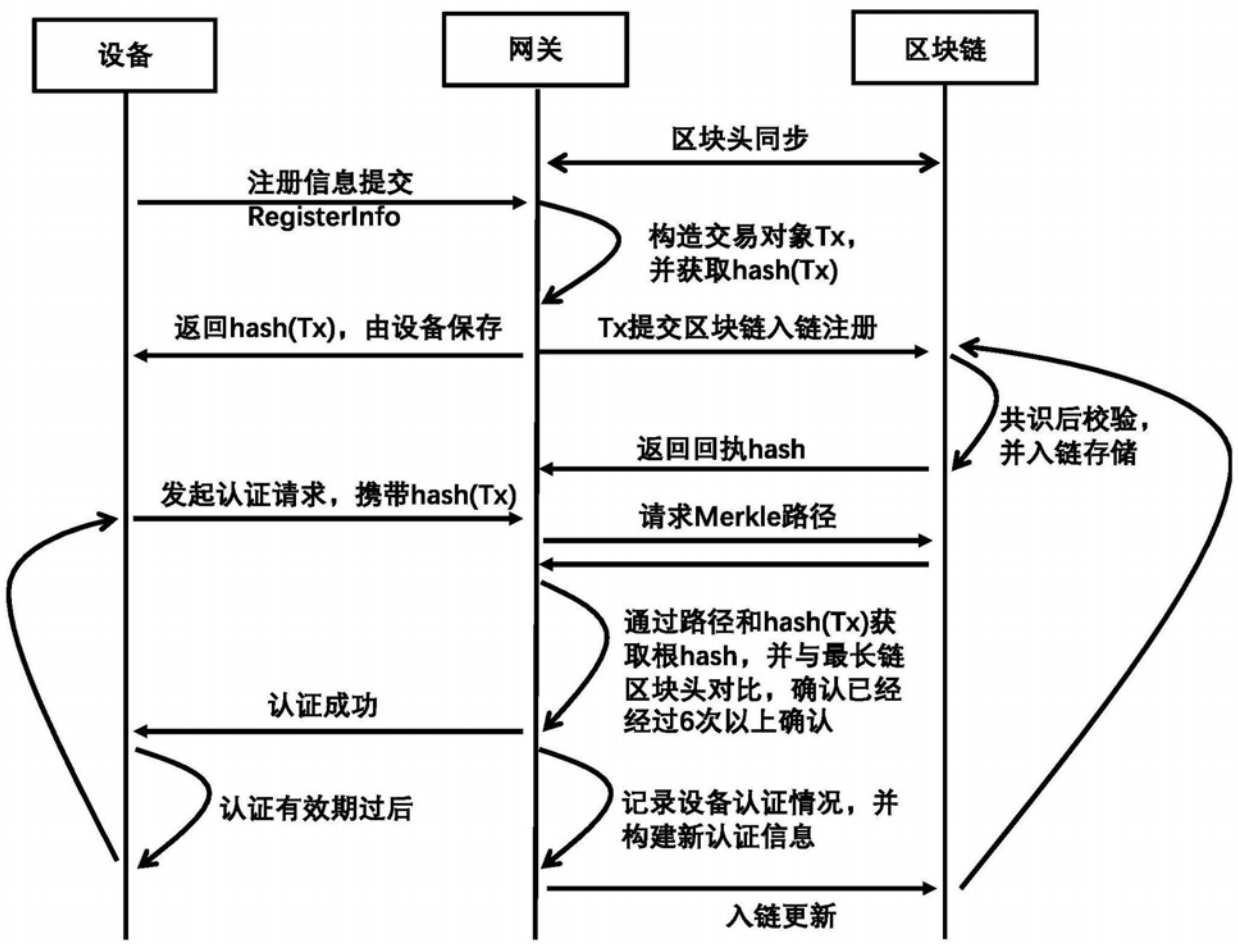

设备
网关
区块链
区块头同步
注册信息提交
RegisterInfo
构造交易对象Tx，
并获取hash(Tx)
返回hash(Tx)，由设备保存
Tx提交区块链入链注册
共识后校验，
并入链存储
返回回执hash
发起认证请求，携带hash(Tx)
请求Merkle路径
通过路径和hash(Tx)获
取根hash，并与最长链
区块头对比，确认已经
经过6次以上确认
认证成功
认证有效期过后
记录设备认证情况，并
构建新认证信息
入链更新

图3