(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 107528856 A
(43)申请公布日 2017.12.29

(21)申请号 201710887115.0

(22)申请日 2017.09.27

(71)申请人 福建实达电脑设备有限公司
地址 350015 福建省福州市马尾区君竹路（自贸试验区内）

(72)发明人 邱霖恺 王贤俊 高刚强 郑文侃 刘维 何逞

(74)专利代理机构 福州元创专利商标代理有限公司 35100
代理人 蔡学俊

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

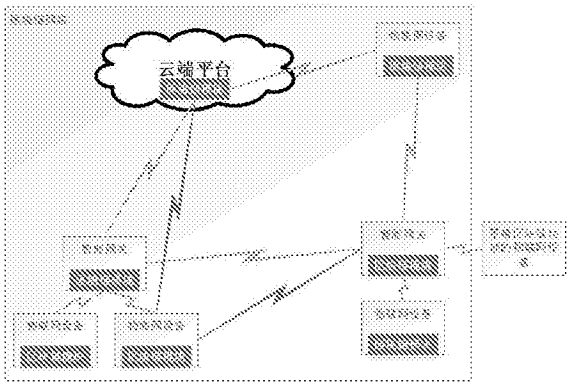
权利要求书1页 说明书4页 附图4页

(54)发明名称

基于区块链的物联网雾端设备在云端平台接入认证方法

(57)摘要

本发明涉及一种基于区块链的物联网雾端设备在云端平台接入认证方法。物联网设备通过通过设备认证手段向带有区块链模块的智能网关发起接入云端平台的代理请求；智能网关的区块链模块接入区块链网络，并向区块链网络给出物联网设备的设备证书和智能网关的设备证书请求认证：区块链网络通过先判断该智能网关的请求链路是否在短期内频繁变化或者存在安全风险，然后再验证智能网关证书的合法性；同理采用相同方式验证物联网设备的设备证书的合法性；若物联网设备带区块链模块也可直接发起接入云端平台的代理请求，其接入认证方式同智能网关的认证方式。本发明降低对云端平台的依赖性和使用频度，降低在设备接入方面云端平台被嗅探和注入的风险。




CN 107528856 A

1.一种基于区块链的物联网雾端设备在云端平台接入认证方法，其特征在于：首先，物联网设备通过通过设备认证手段向带有区块链模块的智能网关发起接入云端平台的代理请求；而后，智能网关的区块链模块接入区块链网络，并向区块链网络给出物联网设备的设备证书和智能网关的设备证书，并请求认证，即：区块链网络首先先判断该智能网关的请求链路是否在短期内频繁变化或者存在安全风险，保证该智能网关节点没有被污染，然后再发起智能网关设备证书的认证请求，通过包括投票、挖矿的共识算法，验证智能网关证书的合法性；若智能网关节点没有存在安全风险且设备证书合法，则区块链网络再先判断该智能网关代理的物联网设备请求链路是否在短期内频繁变化或者存在安全风险，保证该物联网设备节点没有被污染，然后再发起请求设备证书的认证请求，通过包括投票、挖矿的共识算法，验证物联网设备的设备证书的合法性，并告知智能网关；物联网设备的设备证书和智能网关的设备证书认证通过后，智能网关将结果通知给对应的物联网设备；若智能网关节点和对应的物联网设备节点均没有存在安全风险且相应的设备证书合法，则该物联网设备节点后续能够通过该智能网关代理通讯和云端平台进行接入并执行后续的数据交互或者业务处理。

2.根据权利要求1所述的基于区块链的物联网雾端设备在云端平台接入认证方法，其特征在于：所述物联网设备为带区块链的物联网设备或不带区块链的物联网设备。

3.根据权利要求2所述的基于区块链的物联网雾端设备在云端平台接入认证方法，其特征在于：所述物联网设备为带区块链的物联网设备时，所述带区块链的物联网设备能够不通过智能网关直接发起接入云端平台的代理请求，其认证过程如下：首先先由带区块链的物联网设备的区块链模块接入区块链网络，并向网络给出带区块链的物联网设备的设备证书，并请求认证；区块链网络首先先判断该带区块链的物联网设备的请求链路是否在短期内频繁变化或者存在安全风险，保证该节点没有被污染，然后再发起证书的认证请求，通过包括投票、挖矿的共识算法，验证证书的合法性，并告知带区块链的物联网设备；若节点没有存在安全风险且带区块链的物联网设备的设备证书合法，则该节点后续可以和云端平台进行接入并执行后续的数据交互或者业务处理。

4.根据权利要求1所述的基于区块链的物联网雾端设备在云端平台接入认证方法，其特征在于：所述云端平台为带区块链模块的云端平台。

# 基于区块链的物联网雾端设备在云端平台接入认证方法

## 技术领域

[0001] 本发明涉及一种基于区块链的物联网雾端设备在云端平台接入认证方法。

## 背景技术

[0002] 同类物联网雾端设备接入到云端平台的认证方案中，一般是由雾端设备直接向云端平台发起请求，或者是由雾端设备向一个智能网关授权代理向云端平台发起请求。这种方式有几个缺点：

首先，这种模式增加了增加云端遭受大量的无效认证请求而出现有效请求不被响应的风险；

其次，这种模式对于设备认证的模式可以实现就近认证和分布式认证，有效利用了区块链特性实现雾端认证；

最后，当雾端设备数量增加到一定界限的时候，如果云端认证体系不进行相应的扩容，则无法满足原有的认证需求，认证速度和认证的响应率也会随之降低。

而本技术针对这些缺点，同时利用了区块链一些特性，同时针对已有不带区块链设备做出兼容方案，实现了带区块链和不带区块链功能的设备接入云端平台时不需要立即直接访问云端，可以先通过区块链网络进行接入认证和授权，分担云端平台的认证请求处理负担，并通过区块链网络保存本次认证的流程和凭据，利用区块链的特性保证数据不会被篡改。

## 发明内容

[0003] 本发明的目的在于提供一种基于区块链的物联网雾端设备在云端平台接入认证方法，该方法通过使用临近节点有效提升完成认证的需求，降低在设备接入方面云端平台被嗅探和注入的风险；在文件打印时可有效的提高文件传输及答应的安全性及可靠性，防止数据泄密现象发生。

为实现上述目的，本发明的技术方案是：一种基于区块链的物联网雾端设备在云端平台接入认证方法，首先，物联网设备通过通过设备认证手段向带有区块链模块的智能网关发起接入云端平台的代理请求；而后，智能网关的区块链模块接入区块链网络，并向区块链网络给出物联网设备的设备证书和智能网关的设备证书，并请求认证，即：区块链网络首先先判断该智能网关的请求链路是否在短期内频繁变化或者存在安全风险，保证该智能网关节点没有被污染，然后再发起智能网关设备证书的认证请求，通过包括投票、挖矿的共识算法，验证智能网关证书的合法性；若智能网关节点没有存在安全风险且设备证书合法，则区块链网络再先判断该智能网关代理的物联网设备请求链路是否在短期内频繁变化或者存在安全风险，保证该物联网设备节点没有被污染，然后再发起请求设备证书的认证请求，通过包括投票、挖矿的共识算法，验证物联网设备的设备证书的合法性，并告知智能网关；物联网设备的设备证书和智能网关的设备证书认证通过后，智能网关将结果通知给对应的物联网设备；若智能网关节点和对应的物联网设备节点均没有存在安全风险且相应的设备证

书合法，则该物联网设备节点后续能够通过该智能网关代理通讯和云端平台进行接入并执行后续的数据交互或者业务处理。

[0004] 在本发明一实施例中，所述物联网设备为带区块链的物联网设备或不带区块链的物联网设备。

[0005] 在本发明一实施例中，所述物联网设备为带区块链的物联网设备时，所述带区块链的物联网设备能够不通过智能网关直接发起接入云端平台的代理请求，其认证过程如下：首先先由带区块链的物联网设备的区块链模块接入区块链网络，并向网络给出带区块链的物联网设备的设备证书，并请求认证；区块链网络首先先判断该带区块链的物联网设备的请求链路是否在短期内频繁变化或者存在安全风险，保证该节点没有被污染，然后再发起证书的认证请求，通过包括投票、挖矿的共识算法，验证证书的合法性，并告知带区块链的物联网设备；若节点没有存在安全风险且带区块链的物联网设备的设备证书合法，则该节点后续可以和云端平台进行接入并执行后续的数据交互或者业务处理。

[0006] 在本发明一实施例中，所述云端平台为带区块链模块的云端平台。

[0007] 相较于现有技术，本发明具有以下有益效果：

1)通过使用临近节点有效提升完成认证的需求；

2)通过区块链特性，降低对云端平台的依赖性和使用频度，降低在设备接入方面云端平台被嗅探、渗透和注入的风险；

3)在设备认证时可有效的提高认证数据传输及应答的安全性及可靠性，防止数据泄密现象发生；

4)实现了对不包含区块链模块的物联网设备接入云端平台的认证方法。

## 附图说明

[0008] 图1为本发明系统整体框架图。

[0009] 图2为本发明网络拓扑图。

[0010] 图3为本发明带区块链模块的物联网设备/智能网关接入云端平台认证流程。

[0011] 图4为本发明不带区块链模块的物联网设备接入云端平台认证流程。

## 具体实施方式

[0012] 下面结合附图，对本发明的技术方案进行具体说明。

[0013] 本发明的一种基于区块链的物联网雾端设备在云端平台接入认证方法，首先，物联网设备通过通过设备认证手段向带有区块链模块的智能网关发起接入云端平台(带区块链模块的云端平台)的代理请求；而后，智能网关的区块链模块接入区块链网络，并向区块链网络给出物联网设备的设备证书和智能网关的设备证书，并请求认证，即：区块链网络首先先判断该智能网关的请求链路是否在短期内频繁变化或者存在安全风险，保证该智能网关节点没有被污染，然后再发起智能网关设备证书的认证请求，通过包括投票、挖矿的共识算法，验证智能网关证书的合法性；若智能网关节点没有存在安全风险且设备证书合法，则区块链网络再先判断该智能网关代理的物联网设备请求链路是否在短期内频繁变化或者存在安全风险，保证该物联网设备节点没有被污染，然后再发起请求设备证书的认证请求，通过包括投票、挖矿的共识算法，验证物联网设备的设备证书的合法性，并告知智能网关；

物联网设备的设备证书和智能网关的设备证书认证通过后，智能网关将结果通知给对应的物联网设备；若智能网关节点和对应的物联网设备节点均没有存在安全风险且相应的设备证书合法，则该物联网设备节点后续能够通过该智能网关代理通讯和云端平台进行接入并执行后续的数据交互或者业务处理。所述物联网设备为带区块链的物联网设备时，所述带区块链的物联网设备能够不通过智能网关直接发起接入云端平台的代理请求，其认证过程如下：首先先由带区块链的物联网设备的区块链模块接入区块链网络，并向网络给出带区块链的物联网设备的设备证书，并请求认证；区块链网络首先先判断该带区块链的物联网设备的请求链路是否在短期内频繁变化或者存在安全风险，保证该节点没有被污染，然后再发起证书的认证请求，通过包括投票、挖矿的共识算法，验证证书的合法性，并告知带区块链的物联网设备；若节点没有存在安全风险且带区块链的物联网设备的设备证书合法，则该节点后续可以和云端平台进行接入并执行后续的数据交互或者业务处理。

[0014] 以下为本发明的具体实现过程。

[0015] 本发明可以分为以下几个部分（系统框架图见附图1）：

1．云端平台主要实现了设备认证过后的正常雾端物联网设备和云端平台的交互流程。

[0016] 2．带区块链模块的智能网关，首先智能网关拥有带区块链模块的物联网设备的基础功能，在代理其他设备接入区块链网络或者云端平台的请求之前，需要先对自己进行接入认证，此流程可以参考

带区块链模块的物联网设备/智能网关接入云端平台认证流程（见附图3）。

[0017] 3．不带区块链模块的物联网设备，需要通过已经认证的带区块链模块的智能网关代理，经过区块链网络的认证，才能通过智能网关代理实现和云端平台建立连接并执行交互，此流程可以参考

不带区块链模块的物联网设备接入云端平台认证流程（见附图4）。

[0018] 4．带区块链模块的物联网设备，则可以选择自己接入区块链网络进行接入云端平台的设备认证（见附录图-3），或者也通过区块链智能网关代理接入请求从而接入区块链网络实现设备认证（见附录图-4）。

[0019] 从网络拓扑结构上看，可以分为以下几个部分（网络拓扑图见附图2）：

1．区块链模块，即能够接入区块链网络并执行相应的业务的模块，其在整个区块链网络中是一个节点，多个节点形成区块链集群网络，网络中的单个节点都能够发起认证请求或者响应一次认证请求并给出结果。通过挖矿、投票等共识算法保障节点安全和数据不被篡改的特点。其中区块链模块在出厂之前都应该有一个预置的证书，是由整个区块链网络的根证书签发，并能查证其证书链。

[0020] 其中，如果出现不带区块链模块的物联网设备，其证书应该存储在对应的智能网关内，并通过设备原先的验证方式，保证设备的合法性之后才能发起证书在区块链网络认证的请求。

[0021] 2．区块链网络，是多个区块链模块节点形成的一个集群网络，通过挖矿、投票等共识算法保障节点安全和数据不被篡改的特点。

[0022] 3．云端平台，本身拥有区块链模块，能够接入区块链网络，并且拥有一些侧链业务处理系统，能够依赖区块链认证机制与物联网雾端设备或者网关执行一些相应的业务和

数据交互。

[0023] 4．物联网设备和智能网关，通过智能网关代理或物联网设备自带的区块链模块接入区块链网络，共享网络认证机制并响应认证的请求，同时参与相应的认证业务和认证数据存储，保障整个区块链网络链路数据的安全性和唯一性。

[0024] 针对上述框图及网络结构，本发明基于区块链的物联网雾端设备在云端平台接入认证方法，提供了2种针对是否包含区块链模块的物联网设备接入云端平台的认证方案。

[0025] 1．带区块链模块的物联网设备/智能网关接入云端平台认证流程(见附图3)

当一个物联网设备或智能网关已经带有区块链模块，则可以采用此流程进行接入云端平台的认证。首先先由设备的区块链模块接入区块链网络，并向网络给出自己的设备证书，并请求认证。区块链网络首先先判断该设备的请求链路是否在短期内频繁变化或者存在其他安全风险，保证该节点没有被污染，然后再发起证书的认证请求，通过相应的投票、挖矿等共识算法，验证证书的合法性，并告知请求者。如果节点没有存在安全风险且设备证书合法，则该节点后续可以和云端平台进行接入并执行后续的数据交互或者业务处理。

[0026] 2．不带区块链模块的物联网设备接入云端平台认证流程(见附图4)

当一个物联网设备并不带有区块链模块，则可以采用此流程进行接入云端平台的认证。首先先由设备通过原有的设备认证手段向带有区块链模块的智能网关发起接入云端平台的代理请求。智能网关的区块链模块接入区块链网络，并向网络给出将请求者的设备证书和智能网关自己的设备证书，并请求认证。

[0027] 区块链网络首先先判断该智能网关的请求链路是否在短期内频繁变化或者存在其他安全风险，保证该智能网关节点没有被污染，然后再发起智能网关设备证书的认证请求，通过相应的投票、挖矿等共识算法，验证智能网关证书的合法性。

[0028] 如果智能网关节点没有存在安全风险且设备证书合法，则网络再先判断该智能网关代理的设备请求链路是否在短期内频繁变化或者存在其他安全风险，保证该请求设备节点没有被污染，然后再发起请求设备证书的认证请求，通过相应的投票、挖矿等共识算法，验证请求设备证书的合法性，并告知智能网关。

[0029] 智能网关将结果通知给对应的请求设备。

[0030] 如果智能网关节点和对应的请求设备节点均没有存在安全风险且相应的设备证书合法，则该请求设备节点后续可以通过该智能网关代理通讯和云端平台进行接入并执行后续的数据交互或者业务处理。

[0031] 以上是本发明的较佳实施例，凡依本发明技术方案所作的改变，所产生的功能作用未超出本发明技术方案的范围时，均属于本发明的保护范围。

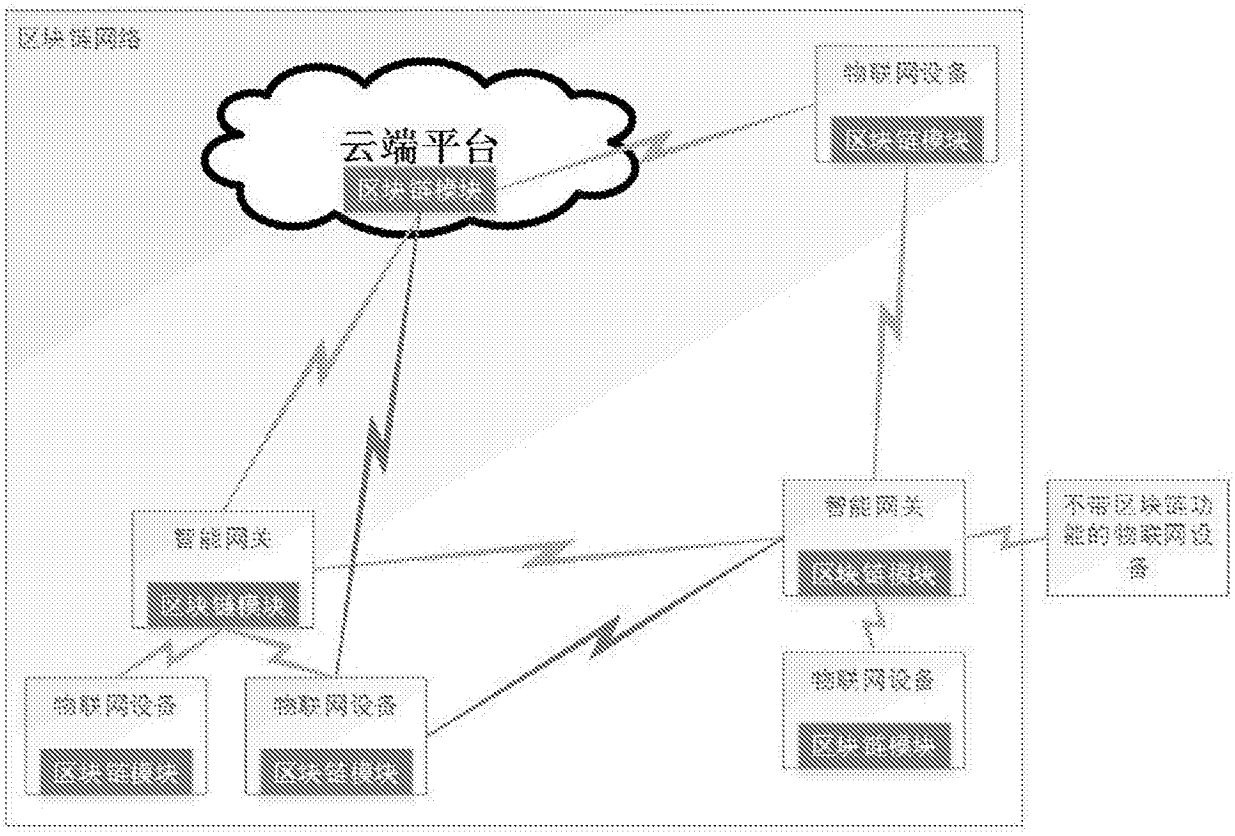

区块链网络
云端平台
物联网设备
智能网关
智能网关
不带区块链功能的物联网设备
物联网设备
物联网设备
物联网设备

图1

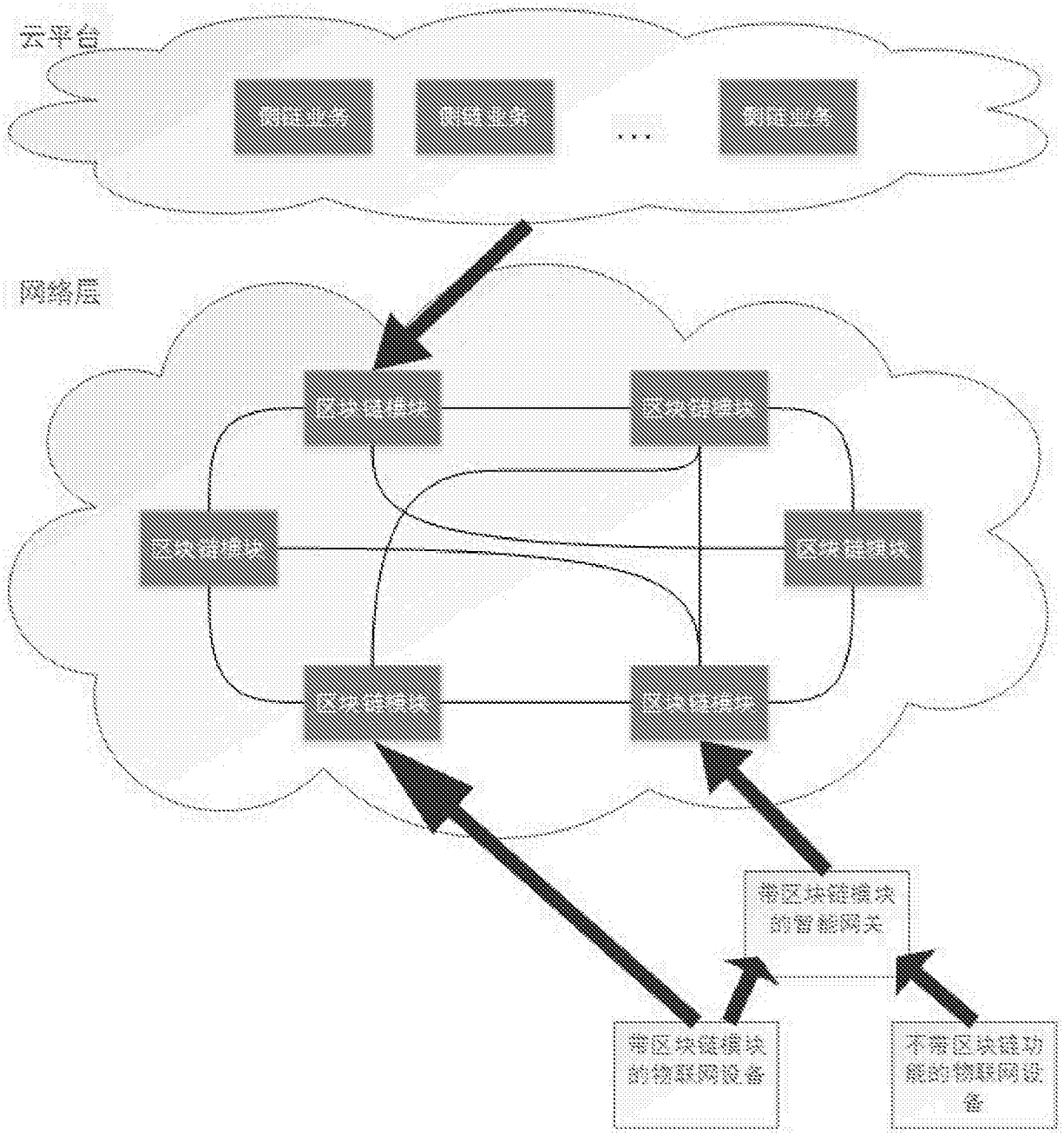

云平台
网络层
区块链模块
区块链模块
区块链模块
区块链模块
区块链模块
区块链模块
带区块链模块的智能网关
带区块链模块的物联网设备
不带区块链功能的物联网设备

图2

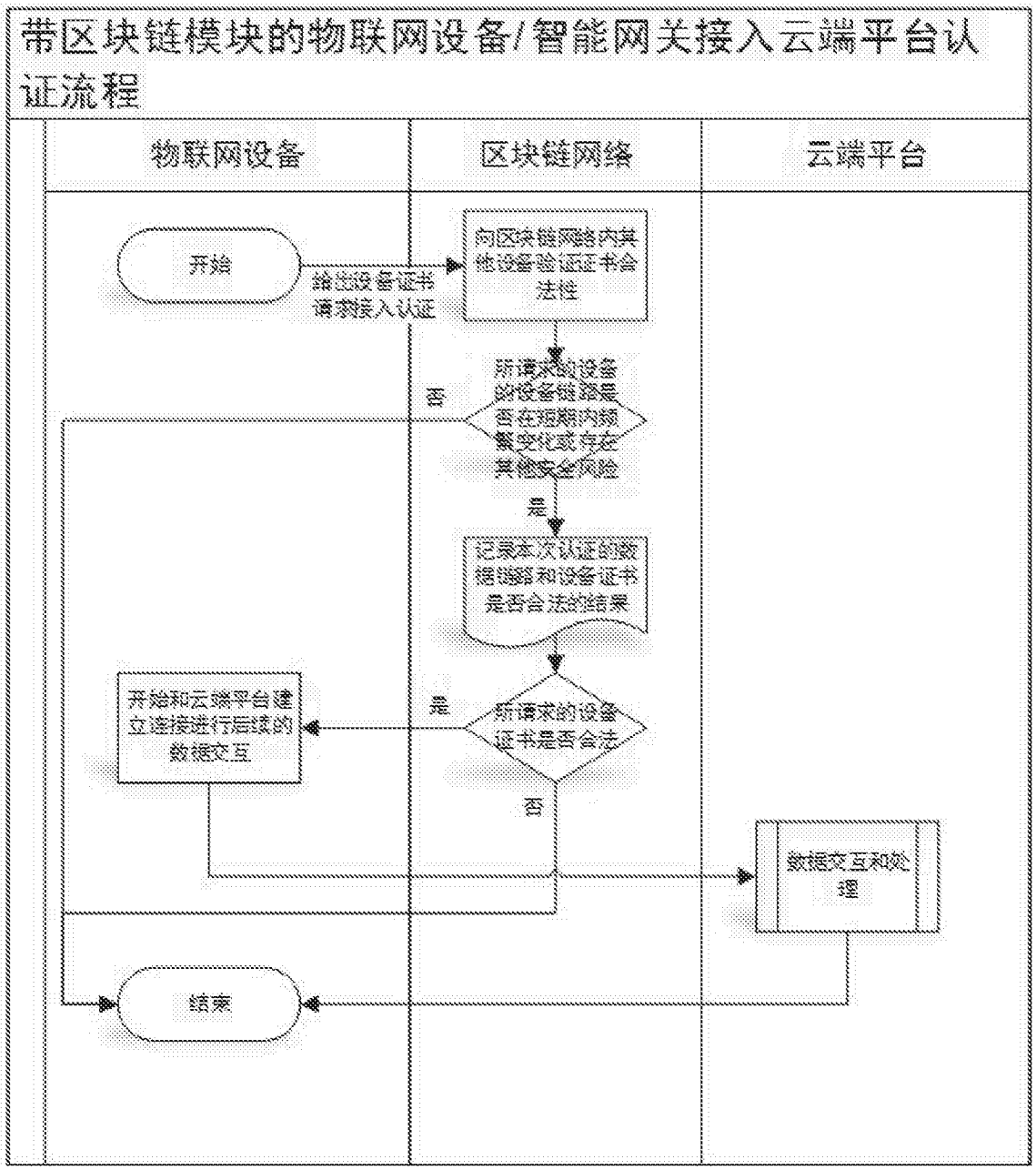

带区块链模块的物联网设备/智能网关接入云端平台认证流程
物联网设备
区块链网络
云端平台
开始
将当设备证书请求接入认证
向区块链网络内其他设备验证证书合法性
所请求的设备的设备链路是否在短期内频繁变化或存在其他安全风险
否
是
记录本次认证的数据包和设备证书是否合法的结果
所请求的设备证书是否合法
是
否
开始和云端平台建立连接进行后续的数据交互
数据交互和处理
结束

图3

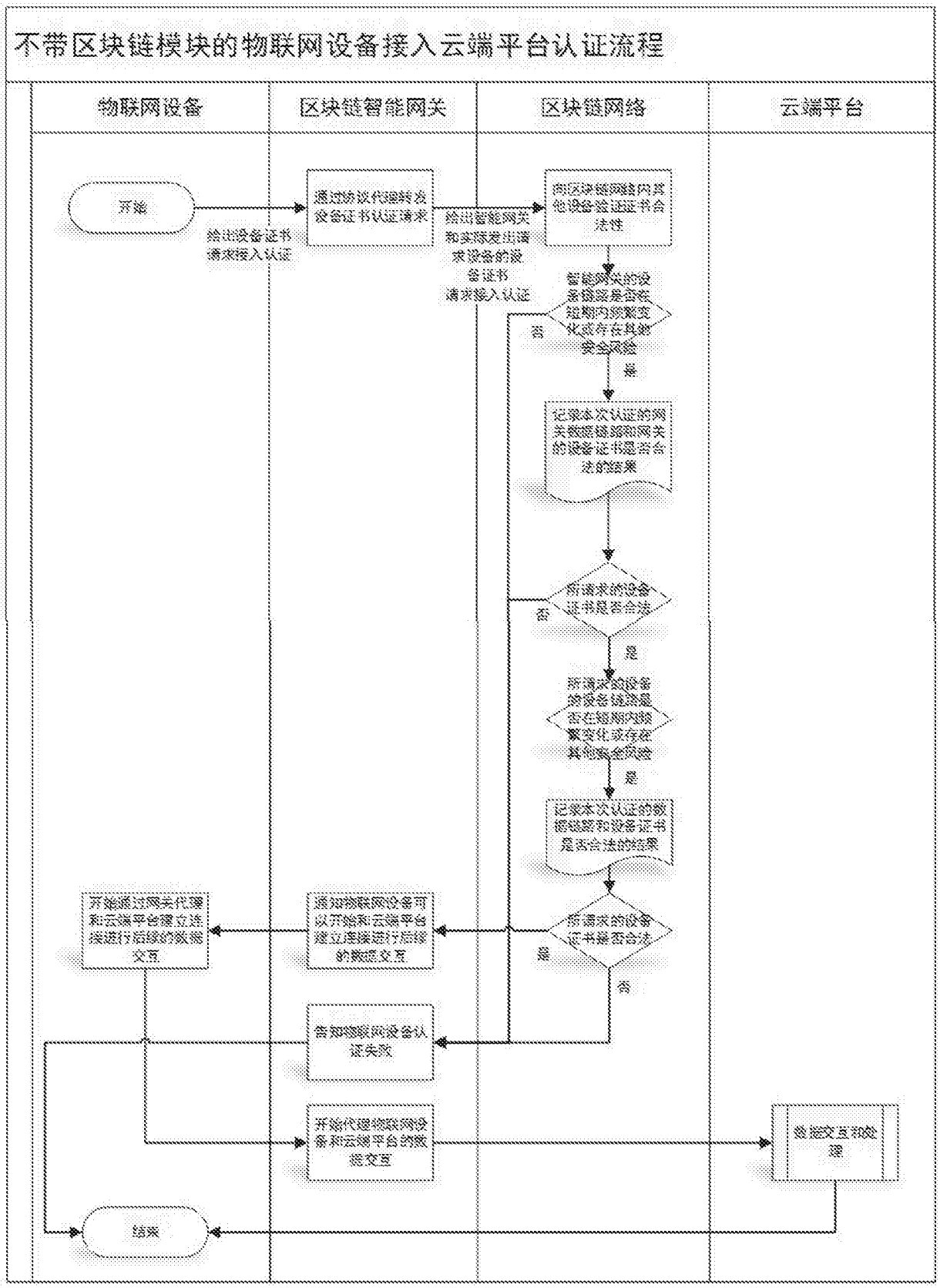

不带区块链模块的物联网设备接入云端平台认证流程
物联网设备
区块链智能网关
区块链网络
云端平台
开始
给出设备证书请求接入认证
通过协议代理转发设备证书认证请求
给出智能网关和实际发出请求设备的设备证书请求接入认证
向区块链网络内其他设备验证证书合法性
智能网关的设备链路是否在短期内频繁变化或存在其他安全风险
否
是
记录本次认证的网关数据链路和网关的设备证书是否合法的结果
所请求的设备证书是否合法
否
是
所请求的设备的设备链路是否在短期内频繁变化或存在其他安全风险
是
记录本次认证的数据链路和设备证书是否合法的结果
所请求的设备证书是否合法
是
否
开始通过网关代理和云端平台建立连接进行后续的数据交互
通知物联网设备可以开始和云端平台建立连接进行后续的数据交互
告知物联网设备认证失败
开始代理物联网设备和云端平台的数据交互
数据交互和处理
结束

图4