基于无证书密码体制和区块链结合的物联网设备访问控制方案研究

Research on Access Control Scheme of IoT Device Based on Combination of Certificateless Cryptography and Blockchain

谢国涛，王首媛，陈礼波（中讯邮电咨询设计院有限公司，北京 100048）
Xie Guotao，Wang Shouyuan，Chen Libo（China Information Technology Designin & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
针对物联网场景中的设备细粒度访问控制，提出一种高效实现方案，采用基于无证书密码体制和区块链访问控制相结合的方式，利用高效的无证书密码技术实现区块链中各种节点的身份管理，通过区块链维护节点关系和访问权限，通过基于智能合约的访问验证体系实现访问管控，形成安全的物联网细粒度访问控制体系；采用契合区块链和物联网的无证书密钥体系，设计高效的基于区块链的访问控制，提高访问效率、动态性、系统扩展性和伸缩性，降低部署成本。

关键词：
无证书密码体制；物联网；访问控制；密码算法
doi：10.12045/j.issn.1007-3043.2021.07.008
文章编号：1007-3043（2021）07-0031-05
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Aiming at the fine-grained access control of devices in the Internet of Things scenario，it proposes an efficient implementation scheme. It adopt.combination of certificate-free cryptosystem and blockchain access control，and uses efficient certificate-free cryptography to implement the identity management of various nodes in the blockchain. The node relationship and access authority are maintained through the blockchain，the access management and control is realized through the smart contract-based access verification system，which form.secure Internet of Things fine-grained access control system. The certificate-less key system that fits blockchain and Internet of things is adopted，and the efficient access control system based on blockchain is designed，which could improve access efficiency，dynamism，system scalability and scalability，and reduce deployment cost.

Keywords：
Certificateless cryptography；Internet of things；Access control；Cryptographic algorithm

引用格式：谢国涛，王首媛，陈礼波. 基于无证书密码体制和区块链结合的物联网设备访问控制方案研究[J]. 邮电设计技术，2021(7)：31-35.

1 概述

随着信息化的深入发展和“中国制造2025”计划的提出，物联网迎来了快速发展阶段，但要实现资源共享和协同，还面临细粒度的权限控制和安全问题。

本文基于区块链实现的细粒度访问控制体系[1]以及无证书密钥体制[2]的结合，针对物联网访问控制，提出技术解决方案。重点解决物联网细粒度访问控制的效率问题，包括CA体系存在的效率问题和区块链细粒度访问控制的效率问题。

本方案利用无证书密码技术提供可信执行环境，通过区块链统一管理设备生命周期内的所有者关系和访问权限，构建物联网设备细粒度访问控制系统。利用高效的无证书密码体制实现区块链节点身份管理，通过区块链维护节点关系和访问权限，通过基于智能合约的访问验证体系实现访问管控，形成安全高

收稿日期：2021-05-24

效的物联网访问控制。

2 物联网区块链访问控制现状

2.1 区块链现状

区块链是一种去中心化的分布式技术，是一种以密码学算法为基础的点对点分布式账本技术，是一种互联网上的共享数据库技术。区块链从技术上解决了基于信任的中心化模型带来的安全问题，它基于密码学算法保证价值的安全转移，基于哈希链及时间戳机制保证数据的可追溯、不可篡改特性，基于共识算法保证节点间区块数据的一致性，基于自动化的脚本代码和图灵完备的虚拟机保证可编程的智能合约。技术架构如图1所示，其主要特征为：智能合约、DAPP和虚拟机。[3]

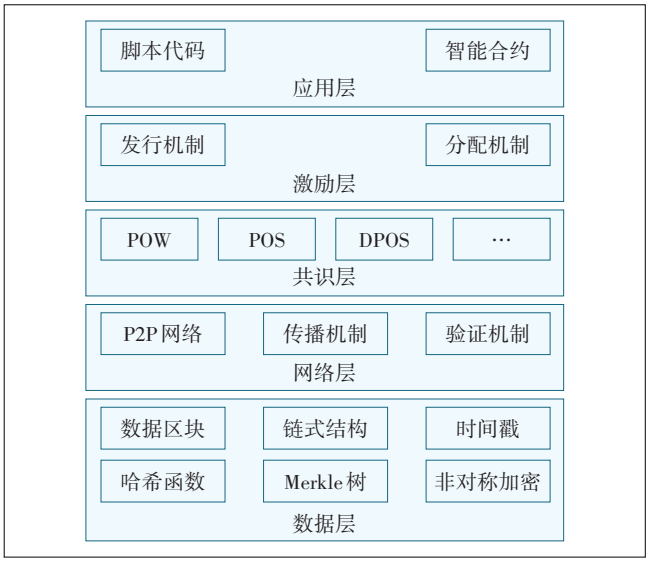


图1 区块链技术架构

2.2 基于区块链构建的访问控制现状

物联网已经可以实现物与物、物与人、人与人之间在任何时候、任何地点的有效连接；物联网中会产生海量的数据，其中具有大量的个人隐私，这些隐私信息一旦泄漏，会给用户带来巨大的损失。作为数据保护的基础技术之一，访问控制可保障数据仅能被拥有相应权限的用户访问。因此，物联网的访问控制机制也就成为了物联网安全和隐私保护的重要研究内容之一[3]。

当将区块链技术与物联网相结合时，访问控制作为物联网数据保护的关键技术之一，成为了主要的结合领域。目前有2种结合方式：一种是区块链技术与现有的物联网访问控制模型结合，区块链充当现有访问控制模型的可信实体，目前主要包括区块链与基于角色的访问控制（role-based access control，RBAC）模型结合、区块链与基于属性的访问控制（attributes based access control，ABAC）模型结合和区块链与基于权能的访问控制（capability-based access control，CapBAC）结合以及其他物联网场景下模型的结合；另一种是提出一种新的完全基于区块链的物联网访问控制模型，区块链作为可信实体的同时，基于区块链的特性设计了基于交易或者智能合约的访问控制方法，按照区块链架构的不同可以分为基于比特币区块链改进的访问控制模型和基于以太坊区块链的具有智能合约的访问控制模型。基于以太坊的区块链具有图灵完备的以太坊虚拟机，可以执行任意复杂算法的智能合约，因此，利用智能合约来实现物联网访问控制将是未来的研究方向[3]。

物联网的发展，将导致接入节点数量的增大，也将伴随归属权和访问的动态化、访问量的增大，如何在兼顾效率和安全的同时，实现访问控制的动态化，是对物联网访问控制提出的一大挑战。

2.3 现有基于PKI/CA的区块链构建的物联网访问控制体系存在的问题

对于基于区块链构建的物联网访问控制体系，当前的主要研究点为智能合约的设计、节点数据的压缩以及应对物联网场景接入节点量级较大的挑战，对物联网中的身份认证涉及较少，通常采用PKI/CA实现。虽然理论可行，但实际应用存在下列问题。

a）CA效率低下，对网络传输要求高，不适合物联网场景下终端计算、密钥管理的高效要求。

b）CA管理的中心化与区块链去中心化不契合。

c）基于区块链的访问控制体系在效率、安全、细粒度、动态性、系统扩展性和伸缩性方面不能全面兼顾。

d）缺乏适应物联网场景，融合身份认证体系和去中心化区块链的访问控制体系。

本文在此基础上提出无证书密码体制和区块链结合的方案可以解决以上技术应用的问题，为物联网访问控制提供高效、安全、细粒度的访问控制实现。

3 无证书密码体制

无证书密码体制介于传统PKI和标识密码技术之间，这种机制中用户私钥由2个秘密因素决定：一个是从密钥生成中心中提取的与用户身份相关的密钥，另

一个是由用户自己生成的密钥。从一个秘密元素不能计算另一个，即密钥生成中心不能算出用户的部分密钥，用户也算不出密钥生成中心生成的部分密钥。因此，无证书密码系统没有密钥托管的功能。无证书密码系统保证即使是攻击人成功地用自己的公钥代替了受害者的公钥，攻击人仍然无法伪造一个受害者的签名，或者解密一段加密给受害者的密文信息。将增加恶意攻击者的攻击难度。这种密码机制在加密过程中仍然提前需要获取接收方公钥（实际为公钥还原数据），然后使用接收方标识和系统参数计算接收方完整公钥。因此这类密码系统在加密应用中面临传统PKI类似的挑战，即需要预先获得接收方的公钥还原数据。对于签名过程，签名方可以将其公钥还原数据作为签名的一部分一起传递，验签方从签名结果中提取签名人的公钥还原数据，然后使用签名方标识和系统参数计算签名方的完整公钥，验证签名的正确性。因此这类系统在签名应用中具有无证书管理、系统轻量、通信开销低、具有强不可抵赖性等众多优点，非常适合物联网等领域的身份认证应用[5]。

4 无证书密码体制和区块链结合在物联网设备访问控制中的应用

物联网设备访问控制中，利用无证书密码体制为物联网系统所有接入节点提供身份认证，在此基础上，利用区块链技术维护设备整个生命周期内任意时刻的拥有者关系和访问权限信息。

4.1 物联网设备访问控制涉及节点定义

在访问控制区块链中，对区块链中目标访问设备而言，包括4种角色：被访问者（终端、或者代理终端访问的网关）、访问者、被访问资源的所有者、区块链中间节点，如图2所示。当然角色划分是相对于目标访问设备而言，如果没有指定目标访问设备（被访问者），访问者、资源所有者、中间节点是等同的。同时被访问者作为一种访问资源，并不一定以独立节点的形式存在。

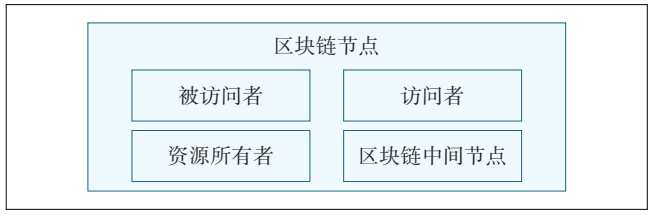
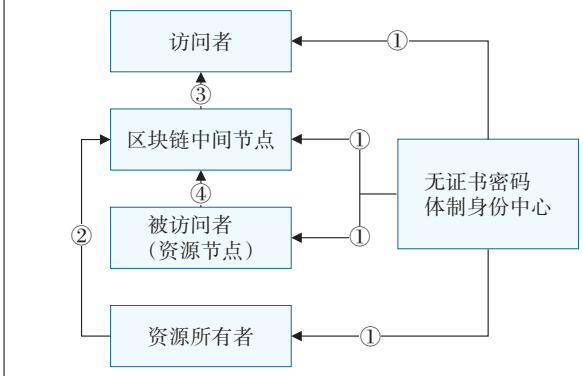


图2　区块链涉及节点

4.2 基于无证书密码体制和区块链结合实现的访问控制总体方案

利用无证书密码体制为物联网访问控制中的各种节点提供身份凭证，借此身份凭证，物联网访问控制中涉及的各种节点，能够对请求和回复中的角色进行身份认证，同时无证书密码体制为物联网访问控制中各种节点提供部分密钥对，在节点合成完整密钥对，并公布于区块链中，用于对信息的加解密处理等；同时区块链各节点通过共识机制和智能合约，实现资源所有权的发布与更新、访问权限的发布与更新、访问控制的验证与路由等，整体方案如图3所示。



注：
①无证书密码体制身份中心为物联网访问控制中各种节点（包括访问者、区块链中间节点、被访问者（资源节点）、资源所有者）等，通过区块链提供的系统唯一身份ID，提供部分密钥对，将用于完整密钥对的合成。
②资源所有者向区块链发布或更新资源所有权、发布或更新资源访问权限；区块链验证资源所有者身份后，形成不可篡改的资源归属关系和资源访问权限。
③访问者向区块链发出访问请求；区块链验证访问者身份后，通过智能合约强制执行访问控制，验证合法进行路由，同时保存访问请求或摘要。
④被访问者接收到区块链发来的访问请求后，验证访问者身份，结合自身状态，发回请求答复，区块链验证被访问者身份后，记录请求答复或摘要。

图3　基于无证书密码体制和区块链结合实现的访问控制总体方案

4.3 无证书密码体制密钥分发或更新

利用无证书密码体制身份中心，为物联网系统所有接入节点提供身份，使访问者、所有者、被访问者、区块链中间节点之间能够双向认证，搭建可信执行环境，如图4所示。

访问者、所有者、被访问者、区块链中间节点均利用CLA身份中心通过系统唯一身份ID获取部分密钥对；访问者、所有者、被访问者、区块链中间节点应当

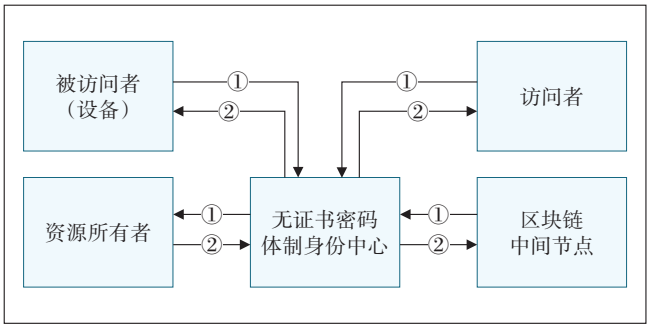


图4 无证书密码体制身份中心为区块链所有节点提供身份

具有密钥存储、密钥对合成、签名验签、加密解密等能力，能够将从无证书密码体制身份中心获取的部分密钥对与自身生成的部分密钥对合成，生成完整密钥对；当密钥对需要重置或超过有效期，可以利用无证书密码体制身份中心通过系统唯一身份ID获取部分密钥对。图4中①表示节点向无证书密码体制身份中心申请取得或更新密钥对；图4中②表示无证书密码体制身份中心发放部分密钥对，或发送因申请出错而导致的错误消息。

其中访问者、所有者、被访问者、区块链中间节点的“系统唯一身份ID”，可基于物联网访问控制区块链中的智能合约所制定规则生成，保证整个系统唯一性。

因无证书密码体制的密钥分发或更新，与基于无证书密码体制的双向认证可以独立，所以无证书密码体制身份中心不必处于区块链所在网络中，甚至无证书密码体制密钥分发或更新可离线进行。

4.4 访问控制区块链设计

访问控制区块链，主要基于图灵完备的智能合约，制定规则，实现节点注册、设备注册、归属数据、权限数据，维护访问控制基础数据，在此基础之上，通过身份认证、检索机制、路由策略、统计分析，达到访问控制业务的验证、快速处理、统计分析，如图5所示。

访问控制区块链中，主要涉及如下业务流程。

a）节点注册。包括访问者、资源所有者、区块链中间节点的注册，在符合约定规则的情况下，任何接入系统的服务，都能够成为区块链节点；节点通过注册获取系统唯一身份ID。

b）设备注册。或称被访问者注册，设备作为区块链中的资源，需要通过资源所有者进行注册，并获取系统唯一身份ID。设备只有通过注册，才能被资源所有者节点转移所有权、发布资源访问权限，继而能够被访问者所访问。

图5 访问控制区块链基础架构

c）归属数据。已注册的资源所有者，将设备在区块链注册成功，意味着区块链中的设备资源具有归属权，形如“资源-归属于-资源所有者”；归属定义在注册成功后上链；资源所有者能够转移所有权，区块链中记录资源生命周期内的所有权变更，形成不可篡改的资源归属关系。同时归属权变更将导致所有前资源所有者发布的关于资源的访问权限，需要根据基于智能合约定义的权限变更协议进行更新。

d）权限数据。即对资源的访问权限；资源所有者能够定义，访问者以何种方式、时机等访问（或不允许访问）资源，形如“访问者-允许（不允许）-访问机制-资源”；权限定义在遵守合约的情况下上链；并在访问者对资源进行访问时，通过基于智能合约的规则强制执行验证，验证符合的情况下，执行访问控制权限的结果，即在允许的情况下路由访问，或在不允许的情况下告知访问者结果，采用如下流程。

（a）访问者签名访问申请，通过被访问者公钥加密访问申请，并发送访问申请。

（b）区块链中间节点通过无证书密码体制对访问者身份进行认证，认证符合继续，否则返回给访问者身份认证失败信息。

（c）区块链中间节点验证访问权限符合情况，符合访问权限的访问继续，否则返回给访问者权限验证不符合信息。

（d）区块链中间节点通过路由策略配置，将访问请求快速路由到下一个区块链节点，或直接路由到资源节点，并记录访问请求到区块中（或仅记录访问请求摘要信息到区块中）。

（e）区块链中间路由节点均可通过无证书密码体制对访问者身份进行认证、或对访问信息进行权限符合性判断，通过共识机制达成一致。

（f）被访问者（资源）通过无证书密码体制对访问者身份进行认证，并通过被访问者私钥解密请求。

（g）被访问者（资源）根据自身情况答复访问请求，并通过访问者公钥加密请求答复。

（h）区块链中间节点通过无证书密码体制对资源身份进行认证，认证符合，记录访问答复到区块中（或仅记录访问答复摘要到区块中），并将访问答复路由给访问者。

（i）访问者通过无证书密码体制对资源身份进行认证，并通过访问者私钥解密请求答复。

（j）归属权变更将导致所有前资源所有者发布的关于资源的访问权限，需要根据基于智能合约定义的权限变更协议进行更新；通过共识机制达成一致后，新访问权限立即生效。

e）身份认证。即基于无证书密码体制的身份认证，在节点注册、设备注册、归属权变更、权限更新等过程中，均需要验证信息变动发生的来源身份，及其权限是否符合合约规定。

f）检索机制。访问控制中的权限判断涉及大量数据检索和计算，通过检索机制的合理配置，实现数据高效检索、避免重复计算。

g）路由策略。随着区块链网络接入量的增大，为提高访问效率，需要配置路由策略，减少访问节点，降低损耗。

h）统计分析。通过对主要业务（如节点注册、设备注册、归属权变更、权限更新、资源访问请求与结构等）的统计分析，发现系统异常、预期业务发展，提高系统表现。

4.5 区块链与无证书密码体制结合的方案优点

基于无证书密码体制和区块链技术相结合的方法，借助无证书密码体制提供可信执行环境，通过区块链统一管理设备生命周期内的所有者关系和访问权限，构建物联网设备访问控制系统。一方面，区块链非常适合解决工业互联网的访问安全问题[1]，同时，通过在区块链应用层中，数据层和业务层的设计，安全高效地解决应用过程中的问题；另一方面无证书密码体制的去中心化、离线认证特性非常契合区块链技术的应用，其轻量级灵活性强、低成本易部署、无证书体系的特点，将大大降低密钥管理和传输成本，支持海量设备的接入认证和密钥管理。

5 结束语

利用无证书密码体制的优势，通过区块链构建的物联网访问控制体系，在物联网可信执行环境的基础上，提供更加细粒度的访问控制机制；在提供安全的细粒度访问控制中，提高访问效率、动态性、系统扩展性和伸缩性，降低部署成本。

参考文献：

[1] 工业区块链应用白皮书（1.0版）[EB/OL]. [2021-05-10]. https://baijiahao.baidu.com/s?id=1680069264054446848&wfr=spider&for=pc.
[2] 熊荣华. 一种无双线性对运算的无证书公钥密码体制的实现方法：104539423.3[P]. 2015-04-22.
[3] 史锦山，李茹. 物联网下的区块链访问控制综述[J]. 软件学报，2019，30(6)：1632-1648.
[4] 樊建峰. 基于区块链技术的基站系统访问控制研究及应用[D]. 北京：中国科学院，2020.
[5] 程朝辉. 基于标准算法的高效无证书密码系统[J]. 中国信息安全，2019，118(10)：93-97.
[6] 陈家琪，冯俊，郝妍. 基于无证书密码学的可认证三方密钥协商协议[J]. 计算机应用研究，2010(5)：1902-1904.
[7] 孙磊，戴紫珊. 基于无证书密码学的移动自组网密钥管理[J]. 计算机工程，2009，35(10)：150-151.
[8] 杨小东，王美丁，裴喜祯，等. 一种标准模型下无证书签名方案的安全性分析与改进[J]. 电子学报，2019，439(9)：166-172.
[9] 曹素珍，王斐，郎晓丽，等. 基于无证书的多方合同签署协议[J]. 电子与信息学报，2019，41(11).
[10] 周艺华，李洪明. 基于区块链的数据管理方案[J]. 信息安全研究，2020(1).

作者简介：
谢国涛，毕业于浙江大学，硕士，主要从事5G物联网密码创新技术研究与应用工作；王首媛，毕业于北京邮电大学，工程师，硕士，主要从事5G物联网密码创新技术研究与应用工作；陈礼波，中讯有限咨询设计院创新业务部副总工程师，高级工程师，硕士，主要从事政企创新业务规划、光通信网络规划咨询设计工作。