软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1632−1648 [doi: 10.13328/j.cnki.jos.005740]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

物联网下的区块链访问控制综述*

史锦山[1,2], 李 茹[1,2]

[1](内蒙古大学 计算机学院,内蒙古 呼和浩特 010021)

[2](内蒙古自治区无线网络与移动计算重点实验室(内蒙古大学),内蒙古 呼和浩特 010021)

通讯作者: 李茹, E-mail: csliru@imu.edu.cn

摘 要: 随着物联网的不断发展,物联网的隐私保护问题引起了人们的重视,而访问控制技术是保护隐私的重要方法之一.物联网访问控制模型多基于中央可信实体的概念构建.去中心化的区块链技术解决了中心化模型带来的安全隐患.从物联网自身环境特点出发,提出物联网终端节点设备轻量级、物联网海量终端节点和物联网动态性这 3 个物联网下访问控制必须要解决的问题.然后,以这 3 个问题为核心,分析、总结了现有物联网中主流访问控制模型以及使用区块链后的访问控制模型分别是怎么解决这些问题的.最后总结出两类区块链访问控制模型以及将区块链用于物联网访问控制中的优势,并对基于区块链的物联网访问控制在未来需要解决的问题进行了展望.

关键词: 区块链;物联网;访问控制;智能合约;隐私保护

中图法分类号: TP309

中文引用格式: 史锦山,李茹.物联网下的区块链访问控制综述.软件学报,2019,30(6):1632−1648. http://www.jos.org.cn/1000-9825/5740.htm

英文引用格式: Shi JS, Li R. Survey of blockchain access control in Internet of things. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1632−1648 (in Chinese). http://www.jos.org.cn/1000-9825/5740.htm

Survey of Blockchain Access Control in Internet of Things

SHI Jin-Shan[1,2], LI Ru[1,2]

[1](College of Computer Science, Inner Mongolia University, Hohhot 010021, China)

[2](Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing (Inner Mongolia University), Hohhot 010021, China)

Abstract: With the development of the Internet of things, the privacy protection of the IoT has attracted people's attention, and access control technology is one of the important methods of privacy protection. The IoT access control model is based on the concept of a central trusted entity. The decentralized blockchain technology solves the security risks brought by the centralized model. This study proposes three issues that must be resolved according to the characteristics of the IoT environment. These three issues are: (1) IoT terminal device lightweight; (2) IoT has a large number of terminal nodes; and (3) dynamic issues under the IoT. Then, using these three issues as the core, it is analyzed and summarized that how the mainstream access control model in the existing IoT and blockchain-based access control model solves these problems. Finally, two types of blockchain access control models and the advantages of using blockchain for IoT access control are summarized, as well as the problems that need to be solved in the future for blockchain and IoT access control.

Key words: blockchain; Internet of things; access control; smart contract; privacy protection

自 1999 年麻省理工学院 Ashton 教授首次提出物联网概念发展至今,物联网已经可以实现物与物、物与人、

* 基金项目: 国家自然科学基金(61862046, 61363079)
Foundation item: National Natural Science Foundation of China (61862046, 61363079)
本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.
收稿时间: 2018-06-25; 修改时间: 2018-10-12; 采用时间: 2018-12-18; jos 在线出版时间: 2019-03-27
CNKI 网络优先出版: 2019-03-27 16:40:26, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.006.html

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.作为数据保护的基石性技术之一,访问控制可保障数据仅能被拥有相应权限的用户访问[1].因此,物联网下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.

随着物联网技术和应用的不断发展,物联网从早期依托射频识别(radio frequency identification,简称 RFID)技术的物流网络发展到目前万物皆可连的“智慧地球”,物联网环境下的访问控制也随之不断发展.主要的访问控制方法有:基于角色的访问控制(role-based access control,简称 RBAC)[2−5]、基于属性的访问控制(attributes based access control,简称 ABAC)[6−11]、基于使用控制模型(usage control,简称 UCON)的访问控制[12−15]和基于权能的访问控制(capability-based access control,简称 CapBAC)[16−20]等.

RBAC 在物联网概念出现之前已经被提出,最初是为了解决大型企业级系统的访问控制问题.RBAC 将角色和一组权限关联在一起,用户根据系统所赋予的角色获取相应的权限.随着物联网的发展,学者们将 RBAC 用于物联网中的访问控制中,可支持物联网环境的可扩展性[21]、跨域访问控制[22]和设备异构[23,24]等特性.但是 RBAC 作为一种静态的访问控制方法,无法提前预设{用户,角色}、{角色,权限}的对应关系,因此无法解决物联网节点动态接入的问题.ABAC 是一种动态的访问控制模型,与 RBAC 需要管理者提前预设{角色,权限}等对应关系不同,ABAC 使用属性作为访问控制的关键要素,而属性是主体和客体内在固有的,通过实体属性发现机制可以挖掘出独立、完备的主体、客体等的属性集合,因此不需要管理者手工输入,然后通过自动化的属性-权限关联关系发现机制可以快速挖掘出{属性,权限}.因此,ABAC 不仅可以解决物联网中节点的动态接入问题,而且对于节点移动和访问数据变化带来的动态性也可以完美解决.物联网下的 ABAC 考虑了节点轻量级[7,10]、动态性[8]的物联网特性做出了局部改进.在物联网中实现访问控制,不仅需要考虑节点的动态接入问题,还需要考虑访问过程中节点属性的可变性问题.而 UCON 不仅解决了节点动态接入问题[14],而且还在访问控制过程中考虑了连续性和可变性两个重要属性[15].连续性体现在访问控制会对请求者访问资源的整体过程进行实时监控,可以随时撤销其资源使用权限;可变性是指属性在访问控制过程中是可变的,在 UCON 中,一般将属性分为不变属性和可变属性两种,其中,可变属性会随着环境和行为等的变化而改变.

上述 RBAC,ABAC 和 UCON 这 3 个访问控制模型都由一个集中式的授权决策实体依据访问控制策略和其他属性信息进行访问控制决策,即以上方法均是引入中央可信实体的概念构建的.随着物联网在生活领域的深入应用,用户对数据隐私和个人隐私信息的保护提出了更高的要求.但是每个访问请求都指向同一个中央可信实体,由中央可信实体保存所有信息,并依据所保存的信息完成所有决策.这本身就是技术层面的不安全,需要依赖技术之外的法律层面来保障安全.而近年频出的隐私泄露事件,如韩国三大信用卡公司信息泄露事件、苹果 iCloud 云端系统漏洞风波等,都对中央可信实体的可信度提出了质疑.

RBAC,ABAC 和 UCON 这 3 种方法都需要一个集中式的服务器来完成授权决策,而 CapBAC 在物联网环境中已经实现了轻量级[18]的分布式[16,18,19]的访问控制,而且支持动态性[17,20]和可扩展性[17,20].虽然 CapBAC 分布式的设计避免了使用集中式服务器所带来的单点故障问题,但是 CapBAC 在物联网中轻量级的设备上实现分布式的访问控制决策时,轻量级设备并不能保证自己的安全性,有可能会被攻击者通过安全性薄弱的物联网设备作为突破口威胁到访问控制的安全,因此,分布式 CapBAC 无法解决在不可信环境下的物联网访问控制.

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.2015 年,区块链技术从金融领域扩展到物联网领域.主要的应用之一就是用于物联网访问控制,代替物联网访问控制的中央可信实体.

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.目前有两种结合方式: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,目前主要的研究见表 1,包括区块链与 RBAC 模型结合[25]、区块链与 ABAC 模型结合[26−28]和区块

链与 CapBAC 结合[29−31]以及其他物联网场景下模型的结合[32,33];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,见表 2,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[34−37]和基于以太坊区块链的具有智能合约的访问控制模型[38−40].

Table 1 Research on integrating blockchain into existing access control model

表 1 将区块链融入现有访问控制模型的研究

与区块链结合的模型或思想	相关文献	特点
RBAC	[25]	使用区块链解决 RBAC 中跨组织访问控制问题,实现了用户角色的跨组织认证
ABAC	[26−28]	使用区块链来确保用户身份属性和访问控制策略不能被恶意用户修改;策略和权限交换在区块链上是公开的,防止一方以欺诈方式拒绝执行政策授予的权利
CapBAC	[29−31]	文献[29]将区块链用在数据存储系统中,当作一个可信的数据库来存储物联网数据;文献[30,31]使用区块链记录权限的授予、使用、流通等操作
CP-ABE[41]	[32]	将区块链用于访问控制中的用户合法性检查
SmartOrBAC[42]	[33]	使用区块链记录访问权限的授予、使用、流通等操作

Table 2 New access control model based entirely on blockchain

表 2 基于区块链提出的访问控制模型

区块链类型	相关文献	特点
比特币	[34−37]	文献[34]将区块链用于存储访问权限;文献[35,36,37]将访问控制策略存储在区块链上,通过区块链交易对访问权限进行管理
以太坊	[38−40]	文献[38,39]将访问控制的主要功能都通过智能合约实现;文献[40]将区块链用在了数据来源管理中,通过智能合约记录所有对数据更改的信息

物联网环境下的访问控制需要考虑以下的问题.

物联网终端节点设备轻量级的问题.物联网终端设备的计算和存储能力一般较弱,而且这些计算和存储能力主要是为物联网设备自身功能服务,无法存储大量数据和进行大计算量任务,甚至有些传感器节点没有存储和计算能力;物联网海量终端节点的问题.物联网中具有大量终端节点,随之而来的还有终端节点种类和其产生的数据较多的问题;物联网动态性的问题.部分物联网终端节点具有移动性,因此需要考虑节点移动性和节点动态接入的问题.

下文将从这 3 个方面来分析物联网访问控制在没有使用区块链时是如何解决这些问题,以及使用区块链后如何解决这 3 个问题.

本文接下来的部分按如下组织:第 1 节从区块链的概念以及发展演进、区块链的链式结构、区块结构和共识机制这 4 个方面介绍区块链技术.第 2 节从物联网终端节点设备轻量级的角度,总结物联网访问控制在没有使用区块链时是如何解决这些问题,使用区块链后如何解决该问题.第 3 节从物联网海量终端节点的角度总结了物联网访问控制在没有使用区块链时是如何解决节点数量庞大所带来的一系列问题,使用区块链后如何解决这些问题.第 4 节从物联网动态性的角度总结了物联网访问控制在没有使用区块链时各个模型解决动态性的方法和侧重点以及使用区块链后如何解决动态性问题.第 5 节根据现有的研究提出了两类基于区块链的访问控制模型,然后对全文进行总结,并讨论了基于区块链的物联网访问控制在未来的发展中将面临的问题.

1 区块链概述

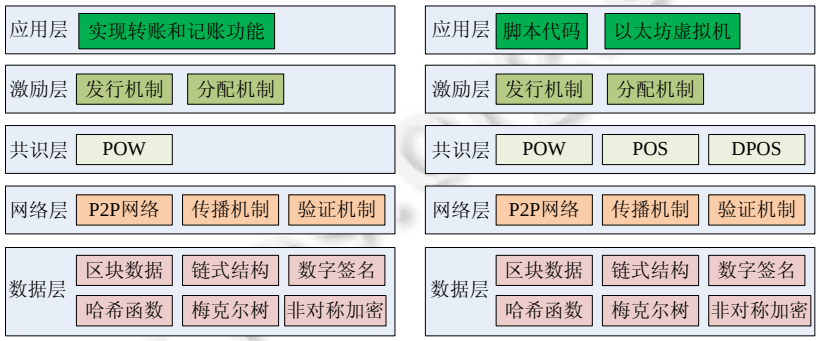
1.1 区块链概念以及发展演进

区块链最初作为比特币的底层记账系统而被人熟知,直到 2015 年,区块链才作为一个单独的概念被研究者关注.区块链并不单纯指其链式的数据结构,而是包括 P2P 网络技术、共识机制[43]、密码学技术、链上脚本[44−46]等一系列技术结合后的产物.虽然区块链目前并没有形成统一的定义,但是可以通过区块链的发展演进来理解区块链.

如图 1(a)所示,区块链起源于 2008 年中本聪发表的论文[47],当时的区块链是一种能在互不信任或者弱信任

的参与者之间维持一套不可篡改的去中心化的分布式记账系统,主要用于金融领域[48].学术界将其命名为区块链 1.0,主要用于数字货币中.其主要特征是:(1) 建立了以区块为单位的链状数据结构;(2) 全网共享账本;(3) 非对称加密;(4) 源代码开源.基于以上特征,区块链具有了账本公开透明、可追踪、不可篡改的性质.

随着研究者对区块链的思考与探索,2013 年末,以太坊的概念被 Buterin 提出,2014 年成立了以太坊基金会并创建了以太坊项目.以太坊的出现,标志着进入区块链 2.0 时代.区块链 2.0 中,区块链可以被看做一种分布式、去中心化的计算与存储架构.技术架构如图 1(b)所示,区块链 2.0 的主要特征有:(1) 智能合约;(2) DAPP;(3) 虚拟机.区块链 2.0 将区块链的应用范围扩展到金融领域之外,使其不仅仅是一个账本,而是具有了可观的计算能力.



(a) 区块链 1.0 技术架构 (b) 区块链 2.0 技术架构

Fig.1 Blockchain technology architecture

图 1 区块链技术架构[48]

1.2 区块链的链式结构

区块链的数据结构是以区块为单位的交易通过密码学算法连接起来的链状数据结构.如图 2 所示,区块分为区块头和区块体,通过区块头中封装的前一个区块的哈希值将区块链接起来形成一个链式结构.一个区块的改变会导致链在其后的所有区块的改变,因此区块链不可篡改,并且可追踪和保证安全.

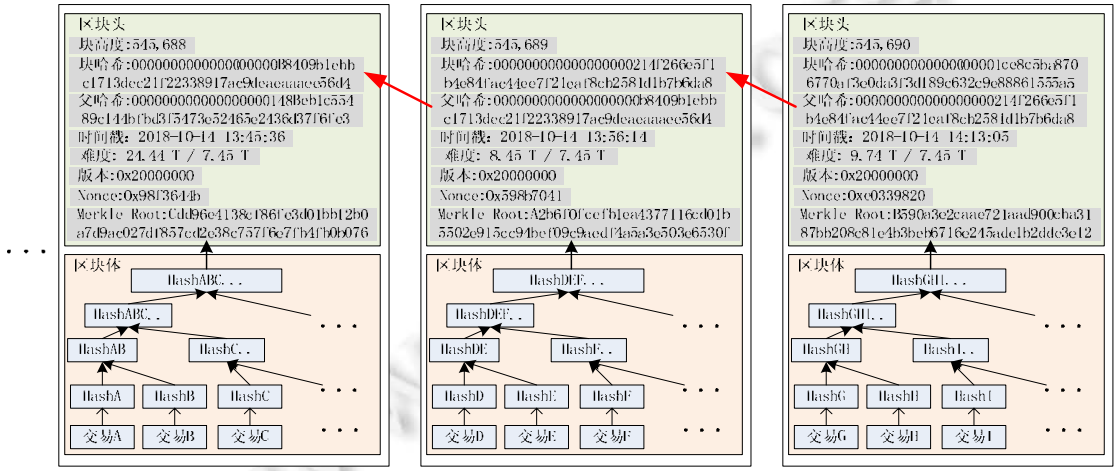


Fig.2 Data structure of the bitcoin blockchain

图 2 比特币区块链数据结构

1.3 区块内部结构

以图 2 的比特币区块为例,区块头中封装了块高度、时间戳、块哈希、前一个块的哈希、Merkle 根等数据,区块体中存储着本区块所有的交易信息.块高度指明了该区块在区块链中的位置;时间戳为该区块产生的时间;

块哈希为区块头的哈希值,比特币中通过求解一定难度的哈希值来满足工作量证明算法;Merkle 根是一个哈希值,通过该区块中的所有交易构成的 Merkle 树的根.区块体中存储着本区块中的所有交易数据.

区块是由挖矿节点构造的,挖矿节点首先会在区块头中填充版本、父哈希、Merkle 根、时间戳、难度和 Nonce 这 6 个字段,其中:版本号、父哈希和难度在构造区块时已经确定;Merkle 根需要将本区块中所有的交易组成一个 Merkle 树,然后在区块头中记录 Merkle 根,当 Merkle 根生成后,区块体也同时生成;时间戳是挖矿节点填充区块头字段时的时间,以 Unix 纪元时间编码;Nonce 用来改变块哈希的值,使其满足难度目标,比特币中挖矿就是不断改变 Nonce 来计算区块头的哈希值,直到找到一个哈希值满足难度目标.当挖矿节点找到满足难度的哈希值后,将该哈希值作为块哈希填充到区块头中,这样就生成了一个完整区块,然后将该区块发送给所有的邻居节点.

随着区块链的发展,对区块的功能提出了更多的要求.以太坊为了满足智能合约的需求,对 Merkle 树进行了改进,提出了 Merkle Patricia 树作为数据组织形式[49,50].而且与比特币保存一棵 Merkle 树不同,以太坊保存了 3 棵 Merkle Patricia 树,分别是状态树、交易树和收据树.其中:状态树用来记录各个账户的状态,交易树用来记录交易内容,收据树用来记录每笔交易相应的收据.区块链根据需求和应用领域的不同,实现方式也不同,其区块头和区块体中存储的数据也会有区别.

1.4 共识机制

区块链中的共识机制是为了解决区块分布式存储所产生的一致性问题,也就是拜占庭将军问题.根据区块链类型的不同,共识的环境和要求也不相同,所以使用的共识机制也各不相同.区块链按照访问和管理权限可以分为公有链、联盟链和私有链等 3 类.下文将按照区块链不同类型的特点来介绍各自类型下所使用的共识机制.

- 公有链中没有中心化的官方组织及管理机构,参与的节点可自由进出网络,读写数据的权限不受系统限制.公有链参与节点数量巨大,且对节点的信任度最低.典型的共识机制有工作量证明(proof of work,简称 PoW)[51]、权益证明(proof of stake,简称 PoS)和授权股份证明(delegated proof of stake,简称 DPoS);
- 联盟链是由若干机构联合发起组成,仅限于联盟成员参与,区块链上的读写权限、参与记账权限按联盟规则来制定.联盟链和公有链相比节点数量较少,且节点间有相当程度的信任.典型的共识机制有 BFT(Byzantine fault tolerance)机制[52]和实用拜占庭容错机制(practical Byzantine fault tolerance,简称 PBFT)[53,54]等;
- 私有链是由私有组织自己建立,不同节点具有不同的权限.私有链假设参与节点不进行攻击,进一步放宽共识机制的假设条件.典型的共识机制有不考虑拜占庭故障的 Paxos 机制[55,56]及 Raft 机制.

在实际应用中,共识机制的选择是根据区块链应用的场景决定的,表 3 为 3 种类型区块链中典型项目共识机制对比.以太坊针对矿池模式导致的算力集中问题而将 PoW 改进为 Ethash;而蚂蚁金服因为金融领域所需的高安全性而选择了 PBFT.

Table 3 Comparison of consensus mechanisms for blockchain projects

表 3 区块链项目的共识机制对比

类型	项目	共识机制	优点	缺点
公有链	比特币	PoW	去中心化,动态性,高可扩展性,支持 10 万以上节点共识	消耗大量算力和电力,低吞吐,高延迟,51%攻击
	以太坊	PoW/PoS 混合模式;PoW 的改进算法 Ethash,PoS 的改进算法 Casper	Ethash 算法相当程度地抵制了 PoW 算力集中问题;在 Casper 有可能做到秒级别的共识	正在从 PoW 向 PoS 过渡,所以依然需要消耗较多的算力和电力
联盟链	Hyperledger	推荐使用 PBFT,但支持名为 Solo 和 kafka 的另外两种共识方式	PBFT 能够解决拜占庭故障性问题,共识时间快;可插拔共识模式,支持多种共识算法	PBFT 适用于节点数少于 20 个的场景,节点过多时算法效率低,算法复杂度高
	quorum	Raft/BFT 混合模式,BFT 在拜占庭容错环境下使用	Raft 可达到秒级共识,共识结果的一致性和正确性高	算法复杂度较高,属于多中心化机制
私有链	蚂蚁金服	PBFT	能够解决拜占庭故障性问题,共识时间快	适用于节点数少于 20 个的场景,算法复杂度高

2 物联网终端节点设备轻量级

物联网中的终端设备如智能摄像头、传感器、可穿戴设备、智能家居、智能汽车等都有大小不一的计算和存储能力,但这些计算和存储能力主要是为物联网设备自身的功能服务的,无法为访问控制提供足够的计算和存储能力.因此,物联网中的访问控制多是将大数据量的计算和存储放在资源受限的物联网设备之外执行.

2.1 未使用区块链时的解决方法

物联网环境下基于RBAC[21−24],ABAC[6−11]和UCON[12−15]的访问控制模型在实现时都是由一个集中式的授权决策实体依据访问控制策略和其他属性信息进行访问控制决策,其访问控制中的计算和存储主要通过集中式的服务器执行.

- 在以RBAC为基础的物联网访问控制中,需要计算和保存{用户,角色}、{角色,权限}等大量信息,而物联网设备的计算和存储资源受限,无法承担起访问控制的需求,因此通过可信第三方服务器来维护和存储{用户,角色}、{角色,权限}信息;
- ABAC能够有效地解决动态大规模环境下的细粒度访问控制问题,是因为ABAC将主体和客体的属性作为基本的决策要素,利用用户所具有的属性集合决定是否赋予其访问权限,实现这一功能需要实体属性发现机制、{属性,权限}关联关系发现机制、访问控制策略描述机制、身份认证机制和权限实时更新机制等多种机制协同工作,因此所需的计算和存储能力是轻量级的物联网设备无法提供的,所以,以ABAC为基础的物联网访问控制需要利用第三方服务器挖掘和保存属性集和{属性,权限}关联关系,通过{属性,权限}来表达复杂的访问控制规则,从而实现物联网下的ABAC访问控制;
- UCON包括主体、客体和权限这3个基本元素以及授权规则、义务和条件这3个与授权有关的元素,同时考虑了连续和可变属性,实现这些功能所需的计算和存储能力物联网终端设备同样无法负担,所以需要由一个集中式的服务器为授权决策实体提供计算和存储资源,然后依据访问控制策略和其他属性信息进行访问控制决策.

上述这些访问控制模型都有一个集中的实体用于访问控制决策,考虑到集中式的实体是一个单点故障问题,随后有学者提出使用分布式方法解决该问题,其中典型代表是物联网环境下分布式的基于权能的访问控制(distributed capability-based access control,简称DCapBAC)[57,58],利用物联网设备组成的分布式平台实现访问控制.但是物联网设备的计算和存储能力较弱,很容易被恶意用户攻击,因此,单纯的物联网设备无法作为一个安全的决策实体[38].

综上所述,物联网设备无法为访问控制提供足够的计算和存储资源,所以需要引入可信第三方来协助进行访问控制,但是这个第三方机构的安全性却无法保证.因此,物联网访问控制需要一个完全可信的第三方机构来提供存储和计算能力.

2.2 使用区块链后的解决方法

由于区块链自身具有可以在假定参与者都不是可信的情况下在技术层面迫使所有参与者遵守诚信,而且具有不可篡改性和隐私保护性,所以区块链可以成为物联网访问控制中可信第三方的角色,为访问控制提供一个可信的环境.区块链在物联网访问控制中作为可信平台,为物联网访问控制提供了计算和存储两种能力.目前,研究者们对区块链计算和存储的使用方法各有不同,有的侧重于使用区块链的存储能力,有的侧重于利用区块链的计算能力,更多的是同时使用计算和存储能力.

(1) 区块链提供可信存储

有研究者侧重于使用区块链的可靠存储能力,利用区块链不可篡改和可审计等功能为访问控制提供一个安全的存储空间.目前,使用区块链存储能力的方法主要可以分为3类.

- 第1类是利用区块链存储访问控制策略,具体的研究有:Dorri等人将区块链用于存储访问控制策略,同时利用区块链不可篡改的特性生成一个时间顺序的不可变的事务历史[36];Alansari将区块链用于存储访问控制策略的同时还存储了用户属性,其计算密集的部分放在链外在安全硬件Intel SGX中执行,区

块链仅作为可信平台防止数据被篡改[26,27];Di Francesco 等人也是将区块链用于保存访问控制策略,同时考虑到区块链上的每一个块生成后都不能删除,会对网络照成永久的负担,因此还提出了一种自定义的高效格式编码用来压缩区块大小,提高了区块链存储的利用率[28];

- 第 2 类是存储物联网中产生的数据,Hashemi 将访问控制中的数据存储和数据管理分离,区块链用在数据存储系统中,当作一个可信的事务数据库来存储数据[29];Ramachandran 是将区块链用在了数据源管理中,将其作为一种安全媒介来存储数据源信息,然后通过智能合约记录对数据的更改信息,防止恶意用户直接破坏源数据[40];
- 第 3 类是直接存储访问权限,Shafagh 等人就是将区块链用于存储访问权限,保证权限不被篡改[34].

(2) 区块链提供可信计算

另外,有些研究者认为使用区块链来存储数据在效率和性能上都不好,所以将数据存储在链下,区块链上仅存储指向数据的哈希,区块链为访问控制提供一个可执行智能合约的可信平台.现有的研究有:Rifi 等人利用的是区块链计算能力,通过 3 种不同类型的智能合约维护不同节点间的规则、认证和通信,将交易的数据存储在另外的数据库中,区块链中仅保存指向该数据的哈希[39].

(3) 区块链提供可信的计算和存储

更多的研究者则是充分利用了区块链的计算和存储两种能力,将重要数据保存在区块链的同时,也利用区块链的计算能力进行访问控制决策.按照区块链所提供的计算能力的大小,可以分为基于比特币区块链的研究和基于以太坊区块链的研究这两类.

- 对于第 1 类基于比特币区块链的物联网访问控制研究,因为比特币区块链设计的目的是作为一种金融领域的交易平台,将其应用到物联网访问控制中时仅仅是利用了锁定脚本和解锁脚本提供的计算能力,所以比特币区块链能够提供的计算能力并不强.基于比特币区块链的研究有:Ouaddah 利用令牌表示访问权限,令牌传递时,将访问控制策略以锁定脚本的方式嵌入到交易中,用户通过解锁脚本证明其拥有令牌[30,31];随后,Outchakoucht 等人在文献[30]的基础上结合了机器学习算法,但是其区块链的使用方法没有改变[33];Jemel 将区块链用于访问控制中的用户合法性检查[32];Ying 提出一种基于区块链的访问控制架构,将访问控制策略存储在区块链上,通过区块链交易对这些策略进行管理[35];Zyskind 等人将访问控制策略存储在区块链中,将个人敏感数据存储在链下,通过区块链上的访问控制策略管理链下的数据[37];
- 第 2 类是基于以太坊区块链的物联网访问控制研究,其特点是支持智能合约,可以在智能合约中实现任意复杂的算法,计算能力相当可观,相关的研究有:Cruz、Paul 等人使用区块链解决跨组织的 RBAC 中验证用户角色真实性的问题,把区块链作为一个可信平台,通过智能合约创建、修改用户及其属性[25];Zhang 等人将访问控制的主要功能都通过智能合约实现,包括多个访问控制合约、一个法官合约和一个注册合约,充分利用了区块链的存储和计算能力[38].

综上所述,由于区块链自身的安全、可审计、不可篡改、匿名等特性,使其可以完美地胜任物联网访问控制中可信第三方的角色.在计算能力方面,基于比特币区块链的架构所能提供的计算能力并不多,而且在算法复杂性和可扩展性上都有很多限制,但文献[30,31]在其方案中融入了智能合约思想;基于以太坊的区块链具有图灵完备的太坊虚拟机,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.在存储能力方面,由于区块链只能添加区块,不能删除历史区块,而且作为一种分布式系统区块链会在每个完整节点上保存同样的内容,所以区块链的存储能力并不廉价.

随着区块链的发展,区块链已经从一个账本式的数据库发展成为一个安全可信的平台,与其代价高昂的存储能力相比,区块链提供的可信计算能力更值得大家利用.因此在使用区块链存储时,应该存储访问控制数据,而不是像文献[29]中那样存储物联网设备产生的数据.

3 物联网海量终端节点

随着物联网的发展,物联网终端节点的数量会变得非常庞大,同时,终端节点设备的种类及其产生数据类型的种类也非常多.大量的终端节点导致访问控制无法使用静态的方法直接将用户和权限绑定,同时,众多终端节点的类型代表着用户和节点属性的多元化,这都对物联网访问控制提出了新的挑战.

3.1 未使用区块链时的解决方法

物联网自身具有节点数量多、种类多、数据类型多的特点,因此,物联网中的访问控制需要适应这些情况.物联网中不同的访问控制模型,解决这些问题的方法也各有不同.

- RBAC 以角色和权限为核心,把一组权限与角色关联在一起,用户则根据所在系统中所指定的角色取得权限.虽然 RBAC 需要存储大量{用户,角色}、{角色,权限}的信息,无法满足物联网中海量的节点和数据的访问控制,但是通过用户和权限相分离、用户归属于某一角色等方法,RBAC 降低了访问控制表的存储数,使其扩展模型可以适用于少数物联网场景.相关研究有:Yavari 等人将实验场景设为医疗保健场景,通过基于RBAC的方式管理可穿戴式和固定式传感器获取的人体安全数据[21];Liu等人针对制造业物联网场景,提出了一种可以跨域访问的基于 RBAC 的访问控制方法[22];Zhang 等人提出了集成上下文相关信息的扩展 RBAC 物联网访问控制模型,将对象的操作转换为服务,以 Web 服务方式为基础管理物联网中的设备,根据一组收集的系统和用户环境上下文信息授予用户相应的权限[23];
- ABAC 将主体和客体的属性作为基本的决策要素,由于属性是主体和客体内在固有的,不需要手工分配,通过属性-权限关联关系发现机制构建{属性,权限}关联关系,然后根据每个访问请求者的属性以及所请求资源权限所需的属性完成访问授权,使得 ABAC 管理上相对简单.因此,ABAC 更加适用于节点数量多、种类多、数据类型多的物联网.针对物联网环境的 ABAC 改进模型也层出不穷,例如:针对物联网设备资源受限的特征,提出了物联网环境下 ABAC 的改进模型[7,8];Wu 等人针对物联网中的跨域访问控制,提出了基于 ABAC 的细粒度跨域访问控制机制[9];Ouechtati 等人将 ABAC 和信任概念结合,提出了针对物联网环境的 Trust-ABAC 访问控制模型[10];Sun 等人将 ABAC 和 RBAC 相结合,提出了针对物联网具有大规模动态环境的访问控制模型[11];
- CapBAC 将权限具现化为一种令牌,因此,CapBAC 中主体可以把访问权限授予另一个主体,该主体还可以进一步把全部或部分权限授予其他代理,每个阶段的授权深度可控,因此可以通过分布式的方法来解决物联网中节点多的问题.结合椭圆曲线密码学、身份认证和上下文等相关技术,多个文献研究了基于CapBAC的物联网环境下的访问控制模型.Sheng等人以权能为基础,结合上下文和椭圆密码体系构建了基于权能的物联网访问控制架构[16];Gusmeroli 等人提出了以权能为基础的细粒度的访问控制模型[17];Mahalle 等人针对物联网环境下动态的网络拓扑结构、受限的上下文环境和资源低功耗设备的弱物理安全特性,提出了一种身份认证和基于权能的物联网访问控制模型 IACAC(identity authentication and capability based access control)[18];Hernández-Ramos 等人针对物联网内部威胁,提出了结合标准椭圆曲线加密机制的物联网访问控制方案[19].

综上所述,基于 RBAC 的物联网访问控制虽然通过将用户权限分离、用户归属某个角色的方式降低了访问控制表的数据量,但是仍无法满足物联网的需求,仅适用于少量特定物联网场景.基于 ABAC 的物联网访问控制可以自动获取主、客体属性,自动建设属性-权限的关联关系,适用于节点数量多、种类多、数据类型多的物联网;基于 CapBAC 的物联网访问控制通过分布式的设计,解决了物联网节点数量多、种类多、数据类型多的特点.物联网环境下还有一些其他的访问控制模型,但是这些模型中有的是针对特定的场景[14,15],有的是针对特定的问题[12,13],但是并没有针对物联网节点数量多而做出专门的设计,这里就不再讨论了.

3.2 使用区块链后的解决方法

将区块链应用于物联网访问控制中,同样需要解决物联网由于海量终端节点所带来的一系列问题.本文从以下 3 个方面考虑区块链的解决方法:首先考虑如何管理物联网中数量庞大的终端节点;其次需要考虑庞大节

点数量给区块链带来的存储压力,因为访问控制策略以及相关事务会随着节点的增多而增多;第三需要考虑庞大数量的终端节点对访问控制性能的影响,因为目前比特币和以太坊确认一条交易的时间较长,无法直接用在物联网访问控制中.

(1) 分层管理

物联网具有数量庞大的终端节点,这些终端节点多是计算和存储能力较弱的轻量级设备,甚至有的传感器节点仅具有将收集到的环境数据输出的功能而没有技术和存储能力.因此,第一个解决思路是分层,在物联网的设备端将多个有关联的设备组成簇,由功能较强的簇头节点管理簇中所有终端节点.

这样的好处是一方面减少了访问控制直接管理物联网节点的数量,降低访问控制的负担;另一方面,在设备端由功能较强的设备帮助管理功能弱的设备,使弱设备不用直接暴露在网络中,提高了物联网设备的安全性.

这方面的研究有:Rifi 等人提出一个智能家居场景,智能建筑中的普通传感器能力较弱,无法直接连接到区块链,因此由功能强大的家庭网关安装区块链客户端与区块链相连,利用家庭网关管理智能建筑中的所有物联网设备[39];Dorri 等人同样是在智能家居场景中假设每个家庭都有一个总是在线的、高资源的设备负责处理家里和外部的所有通信,同时,这个设备也是区块链网络中的一个节点,存储着本地区块链(local private BC)并具有共识功能[36];Ouaddah 等人的区块链访问控制架构中,同样提出用户将区块链钱包(wallet)作为一个授权管理器(authorization manager point),使用这个钱包管理着多个资源[31];Zhang 等人同样将物联网设备连接到网关,有网关负责连接到 P2P 网络[38].

(2) 压缩存储

物联网数量庞大的终端节点导致区块链需要存储的数据也随之增加,但是区块链存储的代价较大,所以需要减少区块链的存储压力.

- 第 1 种解决方法是从区块链本身考虑,即:在不增加区块链块大小的情况下,使每个块存储更多的信息.Maesa 等人认为,区块链上的每一个块都不能删除,因此会对网络照成永久的负担.所以提出一种自定义的高效格式编码用来压缩上传到区块链中的访问控制策略的大小,具体方法是:定义一个协定的符号映射表,表示策略中可用操作数和数字代码之间的映射关系,将属性名称和操作映射到一个简短的数字值内,映射表会在将来的协议版本中不断更新[28];
- 第 2 种解决方法是将访问控制策略存储在链外,区块链中仅存储指向链外的哈希值.文献[28]认为:最简单的解决方案是在将访问控制策略存储在链外,区块链中仅存储指向链外的哈希值.这个解决方案的好处是可以尽量减少存储在区块链上的数据量,因为策略占用的空间是独立于策略大小的;主要缺点是策略本身存储在区块链之外不利于发挥区块链技术安全性、可用性等优势.Rifi 等人认为:将访问控制事务数据存储在区块链中代价太大,因为所有区块链网络中的节点都需要存储一个备份.所以,他们的方法是将包含大量数据的消息事务存储在链外数据库中,而不是将访问控制策略存储在链外,区块链中仅保存指向该数据的哈希[39].

(3) 性能优化

物联网中庞大数量的终端节点会对访问控制性能产生影响,目前的比特币和以太坊确认一条交易的时间较长,无法直接用在物联网访问控制中.对访问控制性能的优化主要从两个方面考虑:增加新区块产生的速度和增加单个区块中存储的数据量.

目前,增加新区块产生速度的一种方法是提高共识的速度,通过提出新的共识算法来提高共识速度.ByzCoin 采用多个领导者共同快速决定是否应该将区块添加到区块链中,领导者小组由近期时间窗口的矿工动态组成,每个矿工的投票能力与其在当前时间窗口的挖矿区块数量成正比[59],如图 3(a)所示,一组领导者可以在一个共识周期产生多个区块.Luu 等人将矿工节点分成称为“委员会”的组,每个委员会处理一组不相交的交易,在委员会内,节点运行拜占庭一致性协议以协定交易区块,委员会将该交易区块发送给最终委员会,最终委员会将收到的所有区块整理到一个最终区块中[60],如图 3(b)所示.增加新区块产生速度的另一种方法是并行地产生多个区块,最初在 Nxt 社区中提出将有向无环图(directed acyclic graph,简称 DAG)与区块链结合,将区块链由链

式结构改为有向无环图结构,可以并行产生多个区块.Boyen 等人提出以一种名为 Graphchain 的框架,通过放弃将“区块”“链”起来的概念来并行化的产生区块[61],如图 3(c)所示,Graphchain 将数据组织形式从链扩展到了图,挖矿节点可以并行产生区块,其中每个区块最少需要有两个父区块,从而使 Graphchain 是“瘦”的.Coelho 将 DAG 与区块链相结合,用基于 DAG 的账本来实现疾病监测[62].

增加区块中存储的数据量的研究有:Eyal 等人提出一种名为 Bitcoin-NG 的区块链架构,将时间划分为 epoch,并且提出了微区块的概念,微区块并不包含工作量证明.如图 3(d)所示,领导者节点可以在其 epoch 期间单方面向区块链追加多笔微区块,直到新领导者节点被选出[63].文献[59]的 ByzCoin 是在 Bitcoin-NG 基础上设计的,所以 ByzCoin 继承了 Bitcoin-NG 对区块链的改进.

综上所述,面对物联网海量终端节点所带来的问题,目前通过分层管理、压缩存储和性能优化这 3 个方面进行解决:分层管理的思想在未使用区块链时就已经被广泛使用;压缩存储是使用区块链所特有的问题,因为区块链只增不减的特性;性能问题是目前将区块链用于访问控制中最主要的挑战之一,多数物联网场景都对相应时间有要求,而目前区块链的性能并不高.

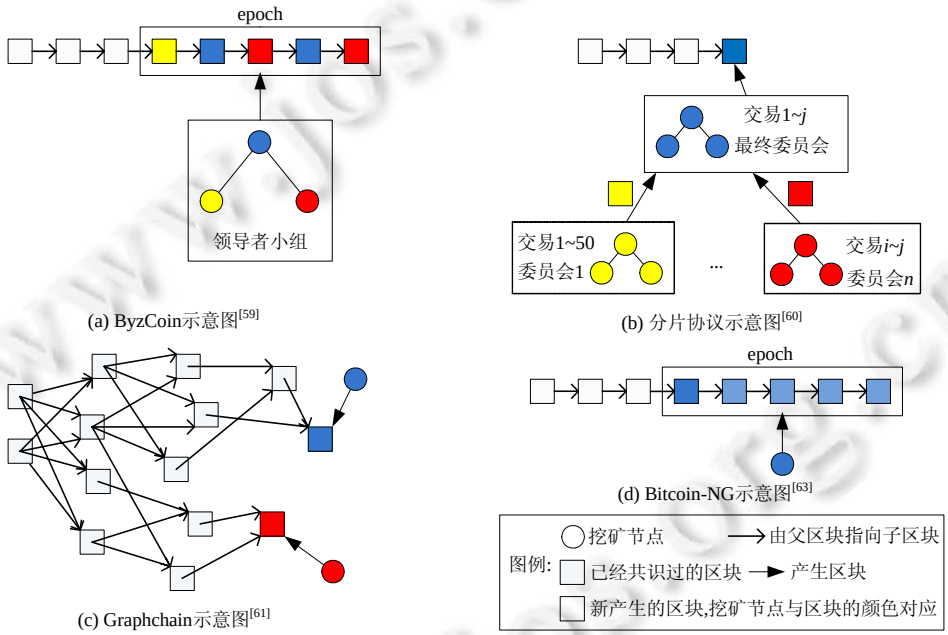


Fig.3 Blockchain performance optimization improvement scheme

图 3 区块链性能优化改进方案

4 物联网动态性

物联网环境下节点的动态性不仅包含节点的动态接入问题,而且还包含节点的移动性以及访问数据对象会实时变化等问题.这种动态性使得我们无法提前预知所有用户信息,也无法准确了解用户和权限结构,更无法提前预设用户与权限的对应关系.

4.1 未使用区块链时的解决方法

RBAC 是一种静态访问控制模型,最初并不支持节点的动态接入.随后,有研究者对 RBAC 进行改进,使其可以实现节点的动态接入.Zhang 等人在 RBAC 的基础上添加了上下文感知和上下文约束,实现了角色和权限的实时动态管理[64].

ABAC 作为动态的访问控制模型天然支持节点的动态接入,ABAC 以主体和客体的属性作为基本的访问

控制决策要素,通过实体属性发现机制,可以挖掘出独立、完备的主体属性、客体属性、权限属性和环境属性集合,因此不需要管理者手工输入主、客体属性.然后,通过自动化的属性-权限关联关系发现机制,可以快速挖掘出{属性,权限},通过主体属性、客体属性、权限属性和环境属性集合以及{属性,权限}关联关系实现动态性的访问控制.因此,ABAC 可以解决物联网中节点的动态接入问题[6,8].

UCON 对于动态性问题的考虑更加深入,通过在访问控制中加入连续性和可变性两个重要因素,不仅可以对访问请求者访问资源的整体过程进行实时监控,随时动态性地调整其资源使用权限,而且考虑了属性的动态性,访问控制中,实体的可变属性是随着环境和上下文变化的.物联网环境下的 UCON 研究有 Zhang 等人将 UCON 用于物联网场景[14]和车联网场景[15].

物联网环境下 CapBAC 对于动态性的支持主要体现在其分布式的设计上,基于分布式的设计,使其更适用于物联网中动态的网络拓扑结构.有学者对基于 CapBAC 进行改进,结合椭圆曲线密码学、身份认证和上下文等相关技术,提出了一种身份认证和基于权能的物联网访问控制模型,适用于动态的网络拓扑结构、受限的上下文环境和资源低功耗设备的弱物理安全的物联网环境[18].

上述 4 种访问控制模型在解决物联网动态性问题时都有各自的侧重点:RBAC 设计之初并不支持动态性,研究者将其应用到物联网环境时,通过对其拓展改进,使其可以实现节点的动态接入;ABAC 自身的设计就使其支持物联网的动态性;UCON 对于动态性的考虑更进了一步,不仅考虑了访问控制过程中权限控制的动态性,还考虑到了实体属性也具有动态性;物联网环境下,CapBAC 作为一种分布式的访问控制模型,更侧重于解决物联网动态的网络拓扑结构问题.

4.2 使用区块链后的解决方法

对于物联网环境下节点的动态性问题,区块链可以完美地解决.一方面是由于区块链中用户的身份是由其密钥来证明的,因此节点可以在任意时间、任意地点连接到区块链网络,只要节点的签名正确就可以进行操作;另一方面,区块链本身采用的是 P2P 的网络架构,当有用户节点需要接入网络时,只要连接到网络中其他区块链节点就可以了,而且由于区块链的 P2P 网络结构并不是基于节点间的地理位置,因此节点只需选择网络中存在的区块链节点并与其相连即可[65].因此,对于节点移动、频繁接入、退出等情况,区块链自身的特性就可以解决.

5 总结与展望

5.1 区块链访问控制模型小结

通过对上述使用区块链的访问控制模型的分析,总结出两类将区块链用于访问控制中的模型,模型中并没有详细的设计细节,仅仅表示出了他们的共同思想.

(1) 去中心的区块链访问控制模型

第 1 类是对文献[25,32,35−39]的总结,提取出他们提出模型的共同之处形成的模型,将其命名为去中心的区块链访问控制模型,其思想为:资源拥有者先将资源的访问控制策略发布在区块链中,然后,当资源请求者想要访问该资源时,直接向区块链中的访问控制策略请求权限,由区块链中运行的访问控制策略决定是否授予访问权限.区块链在访问控制中的作用不仅是存储访问控制策略和权限交易信息,而且提供自动执行访问控制策略进行权限授予等功能.具体流程如图 4 所示:(1) 资源拥有者 o 为资源 r 生成访问控制策略,并将其发布在区块链中;(2) 区块链收到访问控制策略后进行验证,验证通过后将其存储在区块链中;(3) 资源请求者 q 想要访问资源 r,向区块链发送请求访问交易;(4) 区块链收到请求访问交易后,根据访问控制策略决定是否授予 q 访问权限;(5) 若区块链中的访问控制策略同意授予 q 访问权限,则返回访问权限.

去中心的区块链访问控制模型的优点是:充分利用了区块链的计算和存储能力,将访问控制策略存储在区块链上,遏制了越权行为且便于审计;同时,去中心的架构避免了中心节点被破坏导致系统崩溃的情况.缺点是将策略和权限授予记录公开放在区块链上,容易被攻击者找到漏洞.

(2) 有中心的区块链访问控制模型

第 2 类是对文献[28,30,31,33,40]的总结,将其命名为有中心的区块链访问控制模型.模型思想为:仍然存在中心化的授权服务器,资源请求者先向授权服务器(文献[30]中资源拥有者作为授权服务器)发送访问请求,若策略同意,则向区块链发布授予访问权限的交易.区块链记录了该访问权限并通知资源请求者,资源请求者访问资源时,需先告诉区块链使用该访问权限.区块链在访问控制中的作用是记录权限拥有者以及提供权限转移功能.具体流程如图 5 所示:(1) 资源拥有者 *o* 向授权服务器发送资源 *r* 的访问控制策略;(2) 资源请求者 *q* 向资源 *r* 的授权服务器发送请求访问的消息;(3) 若授权服务器中的策略同意,则向区块链发送授予 *q* 访问资源 *r* 访问权限的交易;(4) 区块链对收到的授权或交易进行验证,验证通过后,存储在区块链中;(5) 区块链验证通过后,通知 *q* 取得访问权限;(6) *q* 向区块链发送交易使用访问权限.

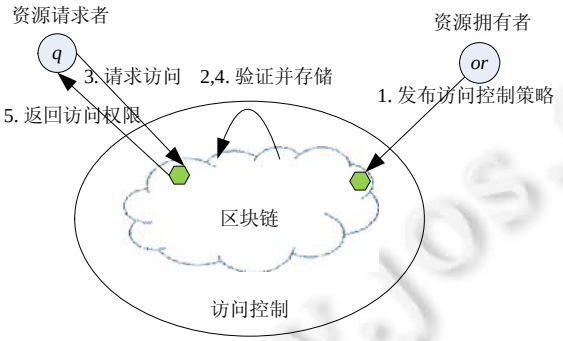


Fig.4 Decentralized blockchain access control model

图 4 去中心的区块链访问控制模型

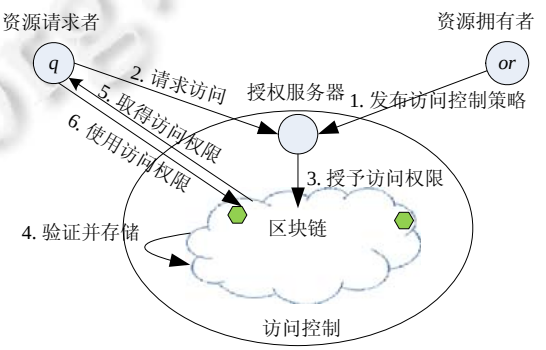


Fig.5 Centered blockchain access control model

图 5 有中心的区块链访问控制模型

有中心的区块链访问控制模型将区块链作为一个可信的存储平台,其访问控制策略运行在授权服务器中,这样做的优点是:权限的授予和使用都被永久性的记录在区块链中无法伪造,便于审计;同时,由于访问控制策略在授权服务器上运行,所以避免了区块链低效对访问控制的影响.缺点是无法保证授权服务器自身的公正性和安全性;依然存在单点故障问题.

5.2 总 结

综上所述,首先对物联网下常用的 4 种访问控制模型进行了分析,其中基于 RBAC,ABAC 和 UCON 的访问控制模型都需要一个集中式的服务器来完成授权决策;基于 CapBAC 的物联网访问控制模型实现了分布式的架构,但是将访问控制决策放在较弱的物联网设备上并不安全.去中心化的区块链从技术上解决了基于中心化模型带来的安全问题,同时也能保证自己的安全性,为物联网访问控制带来新的解决思路.本文从物联网终端节点设备轻量级、物联网海量终端节点、物联网的动态性这 3 个角度对现有物联网中主流访问控制模型以及使用区块链后的访问控制模型进行了总结.

- 首先,物联网设备无法为访问控制提供足够的计算和存储资源,所以需要引入可信第三方来协助进行访问控制,但是这个第三方机构的安全性却无法保证.区块链作为一种新兴的去中心化的分布式技术,从技术上解决了基于信任的中心化模型带来的安全问题,适合作为物联网访问控制的第三方机构.目前,对于区块链的使用逐渐从当作一个可信数据库保存访问控制策略转变为利用区块链智能合约实现自动化的访问控制;
- 其次,对于物联网海量终端节点所带来的问题,RBAC 作为一种静态的访问控制模型,无法满足物联网的需求,仅适用于少量特定物联网场景.基于 ABAC 的物联网访问控制属于动态的访问控制模型,适用于节点数量多、种类多、数据类型多的物联网.基于 CapBAC 的物联网访问控制通过分布式的设计,解决了物联网节点数量多、种类多、数据类型多的特点.使用区块链的物联网访问控制模型从以下 3 个角度解决节点的带来的问题:第一,通过分层的方式简化管理;第二,通过压缩数据或将数据保存到链

外等方法减小区块链存储压力;第三,通过改进区块链结构、改进共识算法等方法提高区块链性能;

- 最后,对于物联网动态性所带来的问题,RBAC 的原始模型并不支持动态性,后有学者将其应用到物联网环境中时,对 RBAC 进行了改进,使其可以实现节点的动态接入;ABAC 自身的设计就使其支持物联网的动态性;UCON 对于动态性的考虑更进了一步,不仅考虑了访问控制过程中权限控制的动态性,而且考虑到了实体属性也具有动态性;物联网环境下,CapBAC 作为一种分布式的访问控制模型,更侧重于解决物联网动态的网络拓扑结构问题.对于使用区块链的物联网访问控制,区块链本身结构的设计特点就支持动态性.

5.3 展 望

下面对基于区块链的物联网访问控制在未来的发展中将面临的问题和挑战进行讨论.

(1) 模型的设计

区块链可以为访问控制提供可信的计算和存储,但是实现可信的代价是存储在区块链上的数据会向所有人公开.对于使用智能合约实现访问控制策略的方案来说,将访问控制策略直接暴露给全网可能并不是一个很好的选择,因此,设计一种适合的智能合约隐私保护方案是一个值得研究的问题.目前,保证智能合约代码隐私性的技术有微软提出的 Confidential Consortium Blockchain,利用 Intel SGX 和 Windows 虚拟安全模式创建可信计算环境,在其中实现证明放入代码的安全性和保证内部数据对外界不可见以及不被篡改的功能[66].

另一种思路是在目前的区块链技术的基础上实现访问控制,因此,选择物联网访问控制中的哪些功能放在区块链中实现,也是一个值得研究的问题.

(2) 跨组织访问

目前研究的物联网场景都较为单一,但是在现实中会出现跨组织或者跨域的访问控制需求.这些组织或者域并不都相互信任,因此需要可信的第三方作为交流平台.而区块链恰好可以充当一个公开可信的平台.因此,通过区块链来解决跨组织或者跨链的访问控制,也是值得研究的问题.

(3) 跨链访问控制

区块链上的数据只增加不减少,使用一条链为全世界用户提供访问控制的可能性微乎其微,所以必然存在多条链并存的情况.在不同区块链间实现跨链的访问控制不仅需要解决区块链自身的差异性,而且需要解决访问控制策略冲突、智能合约适应性等一系列问题.因此,跨链的访问控制是一个挑战性的工作.

(4) 时间优化

目前的比特币和以太坊确认一条交易的时间较长,无法直接用在物联网访问控制中,因此需要设计满足物联网访问控制性能需求的区块链.物联网中的访问控制对时间的要求较高,多数物联网场景需要实时的访问控制,而区块链中出块的速度直接制约着访问控制的速度,因此,如何提高区块链的性能,是未来必须要解决的一个问题.

目前,提升区块链访问控制性能的方法主要有 3 种:第一,通过设计新的共识算法来提高共识速度,这样可以提高区块链产生区块的速度[59,60,63];第二,将区块链的链式结构改为网状结构,这样可以并行产生多个区块[61,62];第三,利用多个侧链和主链合作,主链保证安全性,侧链实现具体业务功能,通过多个链并行工作提高性能[67,68].

(5) 存储优化

区块链的存储是一个增量的过程,即只能增加而不能减少,所以会给存储带来巨大的负担.因此,如何降低区块链存储的代价,是物联网访问控制需要解决的另一个问题.目前的解决方法有两种:第一,压缩区块链中存储的数据,使相同大小的区块存储更多的内容[28];第二,将区块链与区块链存储解耦[69],区块链中存储的是指向某个内容的哈希值[39].

References:

[1] Fang L, Yin LH, Guo YC, Fang BX. A survey of key technologies in attribute-based access control scheme. Chinese Journal of Computers, 2017,40(7):1680−1698 (in Chinese with English abstract). http://cjc.ict.ac.cn/online/onlinepaper/fl-201773143716.pdf [doi: 10.11897/SP.J.1016.2017.01680]

[2] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. Computer, 1996,29(2):38−47. [doi: 10.1109/2.485845]

[3] Ferraiolo DF, Kuhn DR. Role-based access controls. Computer, 1992,4(3):554−563. [doi: 10.1007/978-1-4419-5906-5_829]

[4] Moyer MJ, Abamad M. Generalized role-based access control. In: Proc. of the 21st Int'l Conf. on Distributed Computing Systems. IEEE, 2001. 391−398. [doi: 10.1109/ICDSC.2001.918969]

[5] Bertino E, Bonatti PA, Ferrari E. TRBAC: A temporal role-based access control model. ACM Trans. on Information and System Security (TISSEC), 2001,4(3):191−233. [doi: 10.1145/501978.501979]

[6] Yuan E, Tong J. Attributed based access control (ABAC) for Web services. In: Proc. of the IEEE Int'l Conf. on Web Services. IEEE, 2005. [doi: 10.1109/ICWS.2005.25]

[7] Hemdi M, Deters R. Using REST based protocol to enable ABAC within IoT systems. In: Proc. of the Information Technology, Electronics and Mobile Communication Conf. IEEE, 2016. 1−7. [doi: 10.1109/IEMCON.2016.7746297]

[8] Han Q, Li J. An authorization management approach in the Internet of things. Journal of Information & Computational Science, 2012,9(6):1705−1713.

[9] Wu J, Dong M, Ota K, Pei B. A fine-grained cross-domain access control mechanism for social Internet of things. In: Proc. of the Ubiquitous Intelligence and Computing. IEEE, 2014. 666−671. [doi: 10.1109/UIC-ATC-ScalCom.2014.140]

[10] Ouechtati H, Azzouna NB. Trust-ABAC towards an access control system for the Internet of things. In: Proc. of the Int'l Conf. on Green, Pervasive, and Cloud Computing. Cham: Springer-Verlag, 2017. 75−89. [doi: 10.1007/978-3-319-57186-7_7]

[11] Sun K, Yin L. Attribute-role-based hybrid access control in the Internet of things. In: Proc. of the Asia-Pacific Web Conf. Springer Int'l Publishing, 2014. 333−343. [doi: 10.1007/978-3-319-11119-3_31]

[12] Park J, Sandhu R. Towards usage control models: Beyond traditional access control. In: Proc. of the ACM Symp. on Access Control Models and Technologies (SACMAT 2002). Association for Computing Machinery, 2002. 57−64. [doi: 10.1145/507711.507722]

[13] Park J, Sandhu R. The UCON ABC usage control model. ACM Trans. on Information & System Security, 2004,7(1):128−174. [doi: 10.1145/984334.984339]

[14] Zhang G, Gong W. The research of access control based on UCON in the Internet of things. Journal of Software, 2011,6(4):724−731. [doi: 10.4304/jsw.6.4.724-731]

[15] Zhang G, Gong W. The research of access control in the application of VANET based on UCON. Procedia Engineering, 2012,29:4091−4095. [doi: 10.1016/j.proeng.2012.01.625]

[16] Shen HB, Liu SB. A context-aware capability-based access control framework for the Internet of things. Journal of Wuhan University (Natural Science Edition), 2014,60(5):424−428 (in Chinese with English abstract). [doi: 10.14188/j.1671-8836.2014.05.008]

[17] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of things. Mathematical & Computer Modelling, 2013,58(5-6):1189−1205. [doi: 10.1016/j.mcm.2013.02.006]

[18] Mahalle PN, Anggorojati B, Prasad NR, Prasad R. Identity authentication and capability based access control (IACAC) for the Internet of things. Journal of Cyber Security and Mobility, 2013,1(4):309−348.

[19] Hernández-Ramos JL, Jara AJ, Marin L, Skarmeta A. Distributed capability-based access control for the Internet of things. Journal of Internet Services and Information Security (JISIS), 2013,3(3/4):1−16.

[20] Anggorojati B, Mahalle PN, Prasad NR, Prasad R. Capability-based access control delegation model on the federated IoT network. In: Proc. of the Int'l Symp. on Wireless Personal Multimedia Communications. IEEE Computer Society, 2012. 604−608.

[21] Yavari A, Panah AS, Georgakopoulos D, Jayaraman PP, Schyndel RV. Scalable role-based data disclosure control for the Internet of things. In: Proc. of the IEEE 37th Int'l Conf. on Distributed Computing Systems. IEEE, 2017. 2226−2233. [doi: 10.1109/ICDCS.2017.307]

[22] Liu Q, Zhang H, Wan J, Chen X. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing Internet of things. IEEE Access, 2017,PP(99):1−1. [doi: 10.1109/ACCESS.2017.2693380]

[23] Zhang G, Tian J. An extended role based access control model for the Internet of things. In: Proc. of the Int'l Conf. on Information, Networking and Automation (ICINA). IEEE, 2010. 319−323. [doi: 10.1109/ICINA.2010.5636381]

[24] Liu J, Xiao Y, Chen CLP. Authentication and access control in the Internet of things. In: Proc. of the Int'l Conf. on Distributed Computing Systems Workshops. IEEE, 2012. 588−592. [doi: 10.1109/ICDCSW.2012.23]

[25] Cruz JP, Kaji Y, Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access, 2018,6:12240−12251. [doi: 10.1109/ACCESS.2018.2812844]

[26] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations. In: Proc. of the 2017 IEEE 37th Int'l Conf. on Distributed Computing Systems (ICDCS). IEEE, 2017. 2131−2136. [doi: 10.1109/ICDCS.2017.241]

[27] Alansari S, Paci F, Margheri A, Sassone V. Privacy-preserving access control in cloud federations. In: Proc. of the 2017 IEEE 10th Int'l Conf. on Cloud Computing (CLOUD). IEEE, 2017. 757−760. [doi: 10.1109/CLOUD.2017.108]

[28] Maesa DDF, Mori P, Ricci L. Blockchain based access control. In: Proc. of the IFIP Int'l Conf. on Distributed Applications and Interoperable Systems. Cham: Springer-Verlag, 2017. 206−220. [doi: 10.1007/978-3-319-59665-5_15]

[29] Hashemi SH, Faghri F, Campbell RH. Decentralized user-centric access control using PubSub over blockchain. arXiv preprint arXiv:1710.00110, 2017.

[30] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Proc. of the Europe and Mena Cooperation Advances in Information and Communication Technologies. Cham: Springer-Verlag, 2017. 523−533. [doi: 10.1007/978-3-319-46568-5_53]

[31] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of things. Security and Communication Networks, 2016,9(18):5943−5964. [doi: 10.1002/sec.1748]

[32] Jemel M, Serhrouchni A. Decentralized access control mechanism with temporal dimension based on blockchain. In: Proc. of the 2017 IEEE 14th Int'l Conf. on e-Business Engineering (ICEBE). IEEE, 2017. 177−182. [doi: 10.1109/ICEBE.2017.35]

[33] Outchakoucht A, Hamza ESS, Leroy JP. Dynamic access control policy based on blockchain and machine learning for the Internet of things. Int'l Journal of Advanced Computer Science and Applications (IJACSA), 2017,8(7):417−424.

[34] Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S. Towards blockchain-based auditable storage and sharing of IoT data. In: Proc. of the 2017 on Cloud Computing Security Workshop. ACM Press, 2017. 45−50. [doi: 10.1145/3140649.3140656]

[35] Mei Y. Simplification model construction of Internet access control based on block chain. Journal of Communication University of China, 2017,24(5):7−12 (in Chinese with English abstract).

[36] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the 2017 IEEE Int'l Conf. on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017. 618−623.

[37] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the 2015 IEEE Security and Privacy Workshops (SPW). IEEE, 2015. 180−184. [doi: 10.1109/SPW.2015.27]

[38] Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the Internet of things. IEEE Internet of Things Journal, 2019,6(2):1594−1605. [doi: 10.1109/JIOT.2018.2847705]

[39] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for IoT data access protection. In: Proc. of the 2017 IEEE 17th Int'l Conf. on Ubiquitous Wireless Broadband (ICUWB). IEEE, 2017. 1−5. [doi: 10.1109/ICUWB.2017.8251003]

[40] Ramachandran A, Kantarcioglu D. Using blockchain and smart contracts for secure data provenance management. arXiv preprint arXiv:1709.10000, 2017.

[41] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proc. of the IEEE Symp. on Security and Privacy. Los Alam: IEEE Computer Society, 2007. [doi: 10.1109/SP.2007.11]

[42] Ouaddah A, Bouij-Pasquier I, Elkalam AA, Ouahman AA. Security analysis and proposal of new access control model in the Internet of thing. In: Proc. of the 2015 Int'l Conf. on Electrical and Information Technologies (ICEIT). IEEE, 2015. 30−35. [doi: 10.1109/EITech.2015.7162936]

[43] Mattila J. The blockchain phenomenon—The disruptive potential of distributed consensus architectures. ETLA Working Papers, The Research Institute of the Finnish Economy, 2016.

[44] Bhargavan K, Swamy N, Zanella-Béguelin S, Delignat-Lavaud A, Fournet C, Gollamudi A, Gonthier G, Kobeissi N, Kulatova N, Rastogi A. Formal verification of smart contracts: Short paper. In: Proc. of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM Press, 2016. 91–96.

[45] Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J. Blockchain contract: Securing a blockchain applied to smart contracts. In: Proc. of the 2016 IEEE Int'l Conf. on Consumer Electronics (ICCE). IEEE, 2016. 467–468. [doi: 10.1109/ICCE.2016.7430693]

[46] Peters GW, Panayi E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the Internet of money. In: Proc. of the Banking Beyond Banks and Money. Cham: Springer-Verlag, 2016. 239–278. [doi: 10.1007/978-3-319-42448-4_13]

[47] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[48] China Blockchain Technology and Industry Development Forum. China Blockchain Technology and Application Development White Paper (2016). 2016 (in Chinese). http://www.cbdforum.cn/bcweb/index/article/rsr-6.html

[49] Yan Y, Zheng K, Guo ZX. Ethereum Technical Details and Actual Combat. Beijing: Mechanical Industry Press, 2018. 24–30 (in Chinese).

[50] Ethereum block architecture. 2016. https://ethereum.stackexchange.com/questions/268/ethereum-block-architecture

[51] Garay JA, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications. In: Proc. of the Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2015. 281–310. [doi: 10.1007/978-3-662-46803-6_10]

[52] Lamport L, Shostak RE, Pease MC. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382–401. [doi: 10.1145/357172.357176]

[53] Castro M, Liskov B. Proactive recovery in a Byzantine-fault-tolerant system. In: Proc. of the 4th Conf. on Symp. on Operating System Design & Implementation, Vol.4. USENIX Association, 2000. 273–288.

[54] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems (TOCS), 2002, 20(4):398–461. [doi: 10.1145/571637.571640]

[55] Lamport L. The part-time parliament. ACM Trans. on Computer Systems, 1998,16(2):133–169. [doi: 10.1145/279227.279229]

[56] Lamport L. Fast paxos. Distributed Computing, 2006,19(2):79–103. [doi: 10.1007/s00446-006-0005-x]

[57] Hernandez-Ramos JL, Pawlowski MP, Jara AJ, Skarmeta AF. Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 2015,33(4):690–702. [doi: 10.1109/JSAC.2015.2393436]

[58] Hussein D, Bertin E, Frey V. A community-driven access control approach in distributed IoT environments. IEEE Communications Magazine, 2017,55(3):146–153. [doi: 10.1109/MCOM.2017.1600611CM]

[59] Kokoris-Kogias E, Jovanovic P, Gailly N, Khoffi I, Gasser L. Enhancing bitcoin security and performance with strong consistency via collective signing. Applied Mathematical Modelling, 2016,37(8):5723–5742. [doi: 10.1016/j.apm.2012.11.009]

[60] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. ACM Press, 2016. 17–30. [doi: 10.1145/2976749.2978389]

[61] Boyen X, Carr C, Haines T. Blockchain-free cryptocurrencies: a rational framework for truly decentralised fast transactions. In: Proc. of the IACR Cryptology ePrint Archive 2016. 2016. 871.

[62] Coelho FC. Optimizing disease surveillance by reporting on the blockchain. bioRxiv, 2018. [doi: 10.1101/278473.]

[63] Eyal I, Gencer AE, Renesse RV. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the Usenix Conf. on Networked Systems Design and Implementation. USENIX Association, 2016. 45–59.

[64] Zhang SS, Jiang H, Xie SX, Li QJ. Research of RBAC dynamic access control based on context-aware. Computer Security, 2009, 8:5–8 (in Chinese with English abstract).

[65] Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc., 2014.

[66] Sidkri. The confidential consortium blockchain framework technical overview. https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf

[67] Back A, Corallo M, Dashjr L. Enabling blockchain innovations with pegged sidechains. In: Proc. of the URL. 2014. http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains

[68] Hueber O. The blockchain and the sidechain innovations for the electronic commerce beyond the bitcoin's framework. Int'l Journal of Transitions and Innovation Systems, 2018,6(1):88−102.

[69] Yu FR, Liu J, He Y, Si P, Zhang Y. Virtualization for distributed ledger technology (vDLT). IEEE Access, 2018,6:25019−25028. [doi: 10.1109/ACCESS.2018.2829141]

附中文参考文献:

[1] 房梁,殷丽华,郭云川,方滨兴.基于属性的访问控制关键技术研究综述.计算机学报,2017,40(7):1680−1698. http://cjc.ict.ac.cn/online/onlinepaper/fl-201773143716.pdf [doi: 10.11897/SP.J.1016.2017.01680]

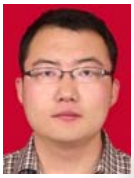
[16] 沈海波,刘少波.面向物联网的基于上下文和权能的访问控制架构.武汉大学学报(理学版),2014,60(5):424−428.

[35] 梅颖.基于区块链的物联网访问控制简化模型构建.中国传媒大学学报(自然科学版),2017,24(5):7−12.

[48] 中国区块链技术和产业发展论坛.中国区块链技术和应用发展白皮书(2016).2016. http://www.cbdforum.cn/bcweb/index/article/rsr-6.html

[49] 闫莺,郑凯,郭众鑫.以太坊技术详解与实战.北京:机械工业出版社,2018.24−30.

[64] 张沙沙,姜华,谢圣献,李秋静.基于上下文感知的 RBAC 动态访问控制研究.计算机安全,2009,8:5−8.



史锦山(1990−),男,内蒙古和林格尔人,博士生,CCF 学生会员,主要研究领域为区块链,访问控制,物联网.

李茹(1974−),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为区块链,访问控制,物联网,下一代互联网.