计算机科学与探索
Journal of Frontiers of Computer Science and Technology doi: 10.3778/j.issn.1673-9418.2211004

面向区块链的物联网终端跨域认证方法综述

霍炜[1+]，张琼露[2]，欧蔚[3]，韩文报[2,3]

1.清华大学 计算机科学与技术系，北京 100084
2. 中国科学院信息工程研究所 信息安全国家重点实验室，北京 100093
3. 海南大学 网络空间安全学院（密码学院），海南 海口 570228
+ 通信作者 E-mail: huow20@mails.tsinghua.edu.cn

摘 要:物联网终端设备分布广、数量多、层次复杂并且涉及多个管理域，常处于不可控的环境中，相比于传统互联网终端，更容易受到攻击，其安全管控面临着更为巨大的风险与挑战。身份认证作为物联网终端安全防护的“第一道防线”，对物联网安全发展起着不可替代的重要作用。然而，基于传统技术的身份认证机制和方案已经不能有效适用于物联网终端跨域认证业务场景。区块链具有去中心化、分布式、不易篡改、可追溯等特点优势，能够有效实现物联网终端跨域认证需求，解决物联网身份认证中存在的可信第三方单点信任失效、多域异构性难以满足最小授权原则等安全问题，使用区块链技术是物联网终端跨域认证未来发展的重要趋势。鉴于此，对近年来基于区块链的物联网终端跨域认证主要研究成果进行了总结，对每个成果和方案进行了技术特点及方案优缺点的分析。在此基础上，总结归纳了目前物联网终端跨域认证领域存在的问题，并给出了物联网终端跨域认证未来的研究方向和发展建议，实现对基于区块链的物联网终端跨域认证方案研究进展和发展趋势的总体把握。同时，也希望这些总结成果能够帮助从业者和研究人员快速掌握相关领域的研究进展，获取相关应用方法和知识，为后续开展更为深入的研究做好铺垫和储备。

关键词:物联网；跨域认证；区块链；身份认证

文献标志码：A **中图分类号：**TP309

Survey on Blockchain-based Cross-domain Authentication for Internet of Things(IoT) Terminals

HUO Wei[1+], ZHANG Qionglu[2], OU Wei[3], HAN Wenbao[2,3]

1. China Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
3. School of Cyberspace Security (School of Cryptology), Hainan University, Haikou, Hainan 570228, China

Abstract: IoT devices are widely distributed, numerous and complex, which are involved in multiple management domains. They are often in uncontrollable environments and are more vulnerable to attacks than traditional Internet terminals, security management and protection of which face greater risks and challenges. As the "first line of defense" for the security protection of IoT devices, authentication plays an irreplaceable and important role in the development of IoT security. However, authentication mechanisms and solutions based on traditional technologies are no longer effectively applicable to the cross-domain authentication business scenarios of IoT devices. The blockchain technology has the characteristics and advantages of decentralization, distribution, immutability, and traceability. And thus, it can effectively realize the cross-domain authentication requirements of IoT devices, solve the single-point trust

failure of trusted third parties and satisfy the principle of least authorization for multi-domain heterogeneity in IoT authentication. Using the blockchain technology is an important trend in the future development of the IoT device cross-domain authentication. In view of this, this paper summarizes the main research achievements of IoT device cross-domain authentication based on blockchain technology in recent years, and then analyzes the technical characteristics, advantages and disadvantages of each output and scheme. On this basis, the current problems and issues in the field of cross-domain authentication of IoT devices are summarized, and the future research directions and development suggestions for the cross-domain authentication of IoT devices are given, so as to achieve a general and overall grasp of the research progress and development trend of the IoT device cross-domain authentication schemes based on blockchain technology. At the same time, it is also hoped that these summary results can help practitioners and researchers quickly grasp the research progress in related fields, acquire relevant application methods and knowledge, and lay the groundwork and reserve for conducting in-depth research in the future.
Key words: Internet of things; cross-domain authentication; block chain; authentication

随着物联网（Internet of Things，IoT）应用的日益普及，传感器、智能终端等海量设备呈指数级接入网络，广泛应用于消费物联网、智慧城市、智能医疗和工业物联网等关系人们日常生产生活的各种场景。据全球移动通信系统协会（Global System for Mobile communications Association，GSMA）《移动经济 2022》报告[1]显示，2021 年全球物联网设备连接数量达到 151 亿；预计到 2025 年，全球物联网连接数将增长到 233 亿，我国物联网连接规模将达到 80 亿。物联网终端数量众多、种类多样、层次复杂，大多终端设备计算能力相对较弱、资源受限、常处于不可控环境中，相比于传统互联网终端，其受攻击面更大，更容易遭到攻击和威胁。2016 年，Mirai 僵尸网络控制了数以百万计的物联网设备发起分布式拒绝服务（Distributed Denial of Service，DDoS）攻击，致使若干重要互联网网站无法访问[2]。SAM Seamless Network《2021 物联网安全形势》报告指出，针对物联网设备的攻击占据 2021 年发生的 10 亿次与安全相关的攻击中的九成，10 亿级物联网设备遭到攻击[3]，安全已成为制约物联网发展的重要因素。身份认证作为安全防护的“首要防线”，被视为物联网安全发展的关键要求，身份认证的不健全或是安全漏洞都会直接导致整个物联网陷入安全危机。目前物联网终端身份认证方面已有大量成熟的研究成果，不同物联网终端设备会根据应用场景、接入位置等情况，采用基于公钥基础设施（Public Key Infrastructure, PKI）、基于身份的签名（Identity-based signature, IBS）、多因素认证、代理等机制的身份认证方案或方法接入相应的管理域/信任域，在域内进行资源共享与信息交互。例如，Yu 等人[4]提出一种云环境下的物联网安全轻量级多因素认证方案，该方案利用秘密参数和生物特征提供安全的互认性和匿名性，且参与交互过程的云服务器在控制服务器进行注册后提供物联网服务，能够抵抗会话密钥泄露、重放和中间人等攻击，与同类型方案相比，具有更好的安全性和效率，适用于实际物联网云计算环境。Lin 等人[5]提出基于代理的云边联合认证方案，引入可信第三方作为联合认证中心协助完成对各设备的认证，解决终端设备既要与云认证又要与边缘服务器认证的问题，减轻用户频繁认证负担。但是这些方案都需要引入控制服务器和可信第三方，增加了额外的硬件或部署开销，成本较高。并且，仅能解决域内身份认证的物联网终端认证方案也间接导致了物联网应用和系统逐渐呈现烟囱式状态，封闭式系统建设模式形成了一个个信息孤岛。不同系统之间认证模式各不相同，证书形式、区块链应用模式、密钥管理方式等均存在差异，造成了十分显著的应用隔离，形成了安全需求不同、信任模式迥异的多个信任域。

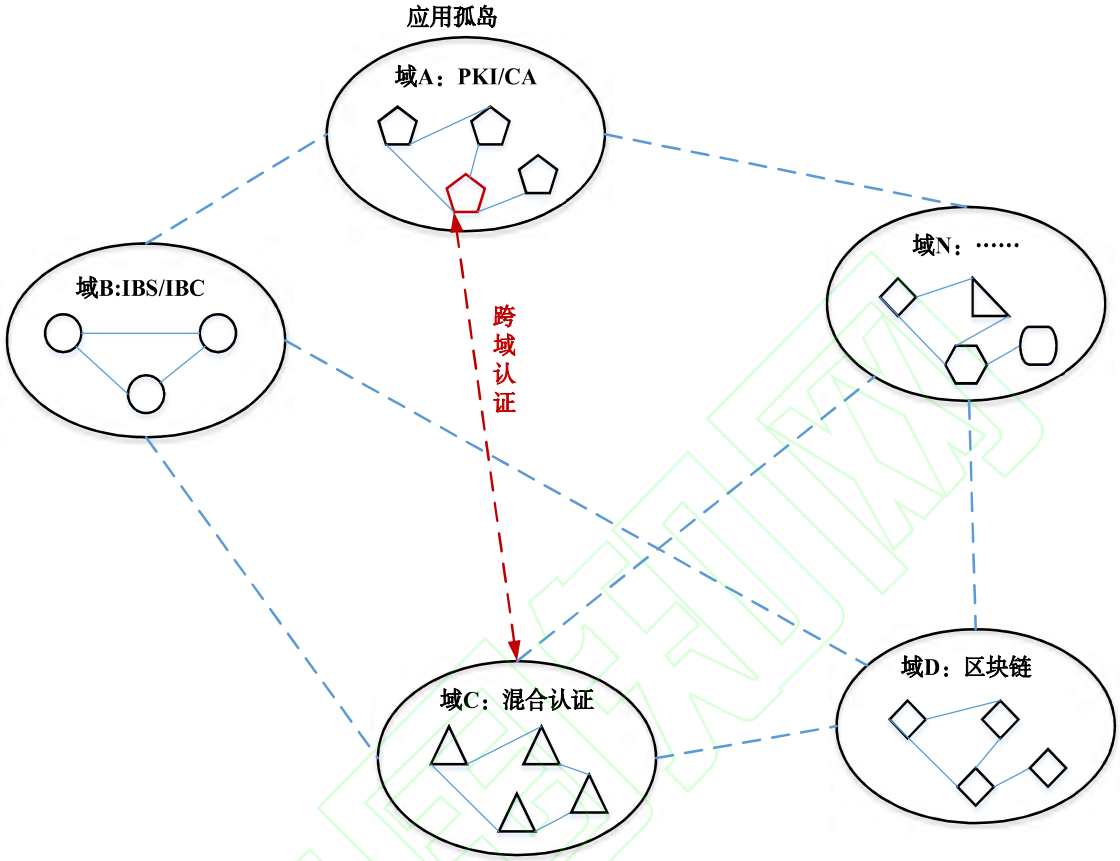

图 1　多信任域间的跨域身份认证需求

Fig.1　Requirements of cross-domain authentication between multiple trust domains

随着物联网应用场景持续丰富，不同应用之间不可避免会迸发出价值交换、协同控制、信息交互以及多域访问等业务需求，如图 1 所示，终端跨域访问也成为时下备受关注的研究热点问题之一。为此，学术界和产业界针对物联网终端跨域身份认证问题，开展了大量方案设计和研究工作，以期打通物联网垂直应用，打破信息孤岛，构建互联互通的物联网应用访问环境。丁等人[6]利用 PKI 和 IBS 认证的相关特性，提出一种基于证书的签名(certificate based signature, CBS)方案，有效避免了 PKI 证书管理复杂性和 IBS 密钥托管与分发等问题，实现了安全、高效、匿名的物联网跨域认证，具有更小的计算和通信开销，适用于资源受限的移动设备。万等人[7]提出了基于身份密码体制和无证书加密体制的不同系统参数的跨域签密方案，优化了跨域环境下的签密算法，并根据无线传感模型构建了一种物联网跨域认证机制。该方案能保证会话临时密钥的安全性，相比于已有方案计算量和能量消耗更少，成本更低。吴等人[8]提出一种适用于边缘计算环境下基于 PKI 和 SM9 标识的认证体系，设计基于标识的“云-边-端”认证方案和基于 K 匿名思想的位置隐私保护方案，物联网终端在边缘进行跨域认证，降低了复杂度，实现了高效安全接入、跨域认证及位置隐私保护，适用于低性能物联网终端设备。毛等人[9]针对物联网跨域认证和可信度量中的安全问题，提出了一种基于证书的物联网身份联盟跨域认证方案，通过组建身份联盟及其可信第三方密钥中心，为实体签发跨域证书，实现异构系统之间的实体身份管理和跨域认证；通过分析联盟中不同身份管理系统的身份认证方式、安全级别以及实体跨域访问记录等信息，对跨域实体的可信度进行计算评价，减少身份管理系统和认证机制对跨域认证结果的影响。季等人[10]面向物联网环境提出了一种分层身份加密（Hierarchical Identity-Based Encryption,

HIBE）的多私钥生成机构（Private Key Generator, PKG）联合跨域认证方案。该方案使用不同 PKG 作为信任网关，通过密钥共享解决密钥托管问题，并建立安全的通信密钥协商机制，实现不同系统参数的信任域用户节点间的互相认证，方案安全可行，且提高了通信效率。

以上仅采用 PKI 等传统技术的认证方案存在证书管理体系复杂、跨域认证效率低、工作量大等诸多问题，不能有效解决物联网环境异构性和跨域安全等级差异化大、终端设备计算能力有限带来的身份认证及其安全问题，尤其是在面向低延时、实时性高的物联网场景时，不能有效满足物联网跨域身份认证和通信业务需求。并且，这类集中式物联网终端认证方式严重依赖受信任的服务器，无法防止单点故障和针对集中存储的攻击，存在明显缺点。此外，部分方案还增加了额外的硬件、数据维护等成本和开销。

区块链可用于建立物联网环境下的分布式信任机制，其去中心化、不可篡改等特性，能够有效解决集中式证书管理体系带来的低效、重负载以及认证服务系统单点信任失效等安全问题，实现分布式验证，缓解中央机构性能瓶颈问题，满足物联网终端设备跨域身份认证需求，提高跨域通信效率。例如，文献[11-33]给出了融合区块链技术同时采用传统认证机制（PKI 机制、IBS/IBC 体系、令牌等）的物联网终端跨域认证机制，Wang[11]等人提出了 BlockCAM 模型、马晓婷等人[14]设计了 ISE-CBCM 模型、Kim 等人[15]提出了分布式 ID 管理系统、黄穗等人[16]提出了 IABC 等等，相比于仅采用传统认证的跨域认证方式，在性能、安全或成本等方面均有不同的改善和影响，但在带来技术便利性和优势的同时，也不可避免地引入了新的问题。因此，研究现有基于区块链的物联网终端跨域认证方案，分析其中存在的问题和不足，提出相应建议并找到未来物联网终端认证发展的方向，对于促进物联网跨域认证技术发展，确保物联网终端设备安全接入和整体规模有序健康扩展具有重要意义。本文的主要贡献如下：

1）研究总结了近年来基于区块链的物联网终端跨域认证的主要研究成果，并在此基础上分析了目前物联网跨域认证领域存在的问题。针对这些问题，提出未来的研究方向和发展建议，实现对基于区块链技术解决物联网跨域身份认证问题研究进展的总体把握。

2）研究总结基于区块链的物联网终端跨域认证方法和机制，有助于相关领域研究人员和从业者快速掌握区块链和物联网技术的交叉应用及研究进展，帮助其快速获取相关的应用方法与知识，以便后续开展更为深入的研究工作。

本文首先介绍了成文的背景和意义，第 1 节描述了物联网终端认证中使用的相关关键技术，第 2 节分析了基于区块链的分布式跨域认证方案及其特点，第 3 节总结了现存问题，第 4 节展望了未来研究方向和发展趋势，最后第 5 节对本文进行了总结。

1 关键技术

1.1PKI 体系

PKI 是指通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种信任体系，是完成用户身份鉴别、保护网络数据传输的常用方法，能够确保通信可信、安全。PKI 体系主要由密钥管理中心（Key Management Center, KMC）、证书颁发机构（Certification Authority, CA）、证书注册机构（Register Authority, RA）和发布中心组成，包括两种重要技术，即证书和密钥。PKI 证书是指授予实体参与 PKI 密钥交换的权限文件。证书包括公钥、来自双方都信任的来源的官方证明。CA 负责证书的颁发、更新以及维护证书废除列表（Certificate Revocation List, CRL）。RA 用于接收证书的申请请求，负责用户身份信息收集、用户身份审查和确认，向 CA 发出证书请求，是用户和 CA 之间的接口。

PKI 通过采用对称加密算法、非对称加密算

法、杂凑算法、数字签名等技术，提供公钥加密和数字签名服务，从而自动管理密钥和证书，验证用户身份的真实性，确保数据传输的保密性、完整性以及行为的不可否认性，最终实现数据安全和身份确认等安全功能。例如，PKI 能够使用公钥对传输中的数据流进行加密操作，防止通信过程中被非法恶意窃取或监听，并且借助私钥唯一性这一特点，有效保证只有接收方才能正确成功解密相应数据流信息。

1.2 基于身份的密码体系

基于身份的密码体系（Identity-Based Cryptograph, IBC）最早由 Shamir 于 1984 年提出[34]，是在 PKI 基础上发展而来，包括基于身份的签名 IBS 算法组、基于身份的加解密（Identity-Based Encrypted, IBE）算法组、基于身份的密钥协商（Identity-Based Key Agreement, IBKA）身份认证协议。用户的身份作为公钥，对应私钥由可信密钥生成中心（Key Generate Center, KGC）发布，且该私钥从 KGC 的主密钥导出，并且 KGC 能够以带外（Out-of-band）方法验证用户的身份，简化了 PKI 要求，消除了 PKI 体系和证书管理的成本，用户使用更方便，安全策略控制更灵活，安全应用更易部署和使用。例如，我国的商用密码算法 SM9 就是基于 IBC 体系设计的。

IBC 体系保有了 PKI 的技术优点，具有数据加密、数字签名、数据完整性、数字信封、用户识别和用户认证等安全机制与功能，其安全性模型已经获得国际密码学界的证明。IBC 作为 PKI 体系的发展和补充，尤其是 IBC 与 PKI 体系的融合，既保证了强签名的安全特性，又满足了各种应用更灵活的安全需求。当然，IBC 体系也有技术缺点，例如固有的密钥托管特性会导致安全问题，因为 KGC 可以导出系统中所有用户的私钥，必须确保其不会滥用这一能力和权限。这一点与 PKI 体系不同，PKI 体系中的 CA 仅发布公钥证书，并不会获悉对应的私钥信息。

1.3 基于令牌的身份认证机制

基于令牌（Token）的身份验证是一种协议，它允许用户验证身份，并作为回报接收一个唯一的访问令牌，能够有效减少对密码系统的依赖，并增加第二层安全性，主要用于验证用户的身份、保证用户身份的真实性，从而实现对网站、安全系统或应用程序等的正常访问。身份认证令牌存储在用户浏览器中，在其生命周期内，用户可以访问已为其颁发令牌的网站或应用程序，如图 2 所示，而不必在每次返回相同的网页、应用程序或受相同令牌保护的任何资源时重新输入身份凭据，再次进行身份认证。只要令牌保持有效，用户就保留访问权限。一旦用户注销、退出应用程序/服务或者超出令牌有效期，令牌就会失效。不同于传统的基于口令或基于服务器的身份验证技术，基于令牌的身份认证提供第二层安全性，用于表明用户的登录状态，管理员可以详细控制每个操作和交易，对令牌设置限制，比如在指定时间段结束后令牌自毁等。令牌提供了一种更难窃取和安全的访问方式，并且会话记录不占用服务器空间。

身份认证令牌主要有三种类型：已连接式（Connected）、非接触式（Contactless）和断开连接式（Disconnected）。已连接令牌主要指密钥、驱动器等物理介质插入系统后进行访问。非接触式令牌指身份认证设备与服务器在一定距离范围内可与其进行非接触式通信，无需直接插入设备或系统。断开连接式令牌是指身份认证设备与服务器之间进行远距离通信，不受距离等因素的限制，服务端会生成一串字符作为令牌。当然，在以上三种类型令牌应用场景中，用户必须首先输入口令或通过回答问题等方式启动认证流程，但是即使完成第一次身份认证过程后，在没有令牌的帮助下后续依旧无法正常访问相应服务、应用程序等。

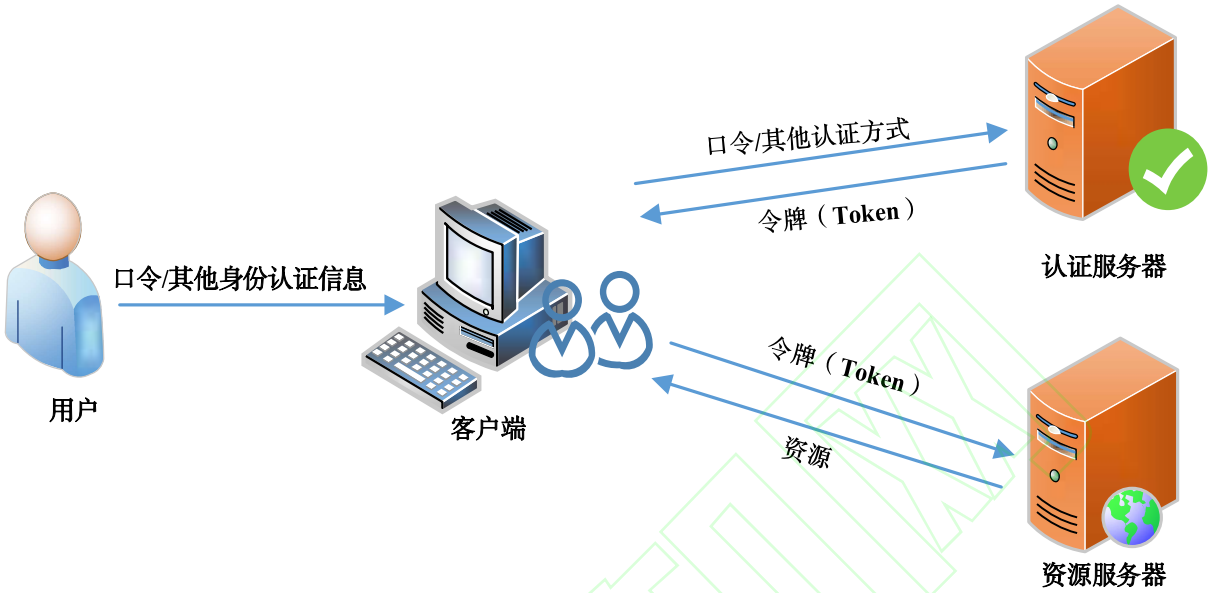

图 2　基于令牌的身份认证过程

Fig.2　Token-based authentication process

1.4 区块链技术

区块链（Blockchain）技术解决了传统网络安全的一些安全缺陷，例如通过分布式节点消除了单点故障隐患，密码学的密集应用可保证数据传输和访问安全，特有数据结构可验证存储数据，同时能够提供端到端的加密保护，因其可编程性、分布式、不可变、一致性和安全性等多种特性而备受关注。并且，区块链具有较强的可拓展性，可以与其他安全技术相互融合应用，从而促进安全机制的完善与融合，构建更加安全的网络环境，其出现与应用发展对信息安全保护工作产生了极其重要的影响。

具体而言，区块链以分布式方式实现的防篡改数字分类账本，是在计算机网络节点之间共享的分布式数据库，由多方共同维护、共享且不可变，也称为分布式账本技术（Distributed Ledger Technology, DLT），用于记录交易、跟踪资产和建立信任。该技术利用共享账本记录交易，在区块链网络正常运行的情况下，一旦发布，任何交易都不能被更改，关键要素包括分布式账本技术、不可变记录以及智能合约，通过使用密码技术保证数据的一致存储、以及难以被篡改和防止抵赖。区块链具有防篡改、去中心化、多方维护、内置合约、匿名性、透明度等多种特征。目前，区块链结构主要有公共区块链架构、联盟区块链架构、私有区块链架构等三种类型。

链参与方按照约定规则存储信息，达成共识。为了防止共识信息被篡改，区块链以组的形式收集和存储信息，称为区块（Block），其中包含信息集。块具有一定的存储容量，在填充时会关闭并通过包含一个基于前一个块数据的唯一标识符来链接到先前填充的块，形成称为区块链的数据链（Chain）。因此，区块链的数据结构包括两个主要元素，即指针和链表，如图 3 所示。指针是指向另一个变量位置的变量，链表是链表块的列表，其中每个块都有数据和指向前一个块的指针。区块链通过共识机制选取记录节点，其他节点参与区块的验证、存储和维护。块一旦上链，难以删除更改，仅能进行授权查询等操作。

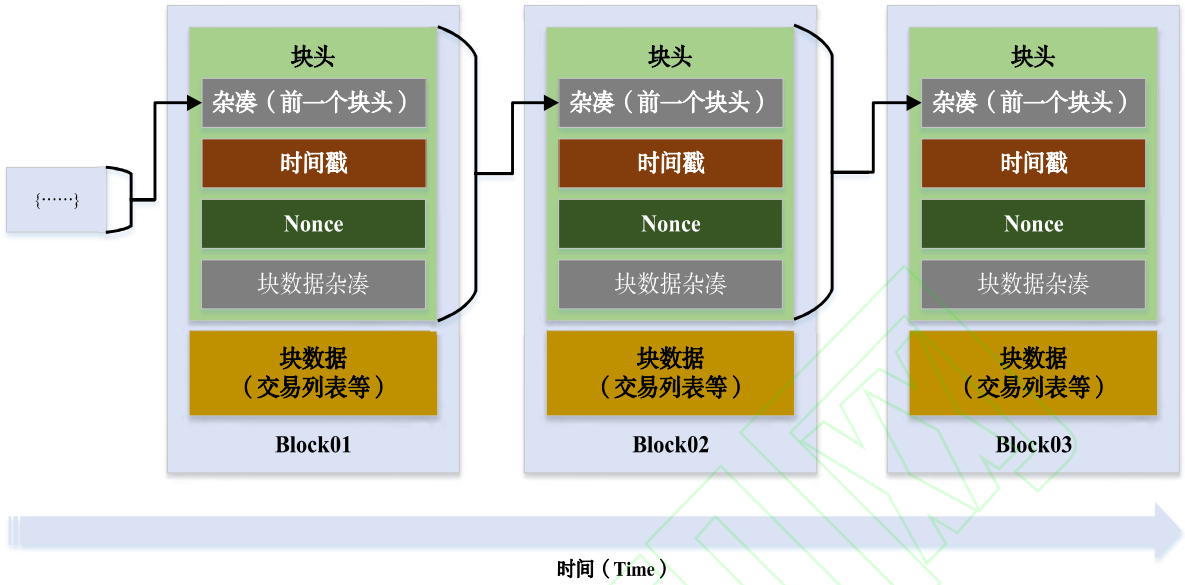

图 3　区块链通用链结构

Fig.3　General bockchain structure

区块链技术框架如图 4 所示，密码机制为区　　块链各层提供相应的密码服务，保障系统安全。

图 4　区块链技术框架

Fig.4　Technical framework of block chain

硬件和基础设施层包括虚拟机、容器、服务、消息等，涵盖数据中心服务器以及对等网络　　（peer-to-peer，P2P）中的每台计算机（节点）。区块链的内容托管在数据中心的服务器中，区块

链网络中的计算机（节点）能够彼此共享这些数据，数据既能够存储在数据中心的服务器中也能够存储在节点上，节点是这一层的核心[35][36][37]。这也进而导致了 P2P 网络的形成，网络上的节点进行信息的验证。在达成共识的同时，节点将区块提交到区块链网络并更新其本地账本副本。由于区块链是 P2P 网络，它计算交易、验证交易并将其以有序的形式存储在共享账本中，形成一个分布式数据库。

数据层的区块链数据结构表现为交易排序的区块链表。默克尔树（Merkle Tree）、密码学和共识算法是区块链技术的基础，Merkle 树为区块链技术提供安全性、完整性和无可辩驳性。每个区块都包含 Merkle 根的哈希值（区块中所有交易的哈希值组合）以及前一个区块的哈希值、时间戳、随机数、区块版本号和当前难度目标等信息，具体可分为块头和块数据两个主要部分[38]，如图 3 所示。块头信息包括块号、前一个区块的哈希值、时间戳、块大小、随机数等，块数据则包括块中的交易与分类账事件的列表，以及其他可能存在的数据。交易使用私钥签名，以确保存储其中的数据安全完整。拥有公钥的人可以验证签名信息、检查信息是否被篡改。签名在法律上与所有者相关联，不能被拒绝。

网络层（亦称 P2P 层或传播层）负责分布式节点间的通信，确保节点可以相互发现并能够通信、传播和同步，共同分担网络负载，节点分为全节点和轻节点两种类型。全节点保证交易的验证和确认、共识规则的挖掘和执行，包含节点的完整信息。轻节点只保留区块链的头部，可以发送交易，节点同步速度更快，所占存储空间更少。

共识层是区块链平台的核心和关键层，主要负责验证区块，对区块排序并确保每个人都同意。共识层是节点遵循的规则，在分布式 P2P 网络的节点之间创建一组明确的协议，确保权力保持分布式和去中心化，确保交易在这些规则的边界内得到验证。

应用层/表达层由智能合约、链码、分布式应用程序（Decentralized Application，DApp）和用户接口组成，分为应用层和执行层两个子层。应用层由用户应用组成，包括脚本、应用程序接口（Application Programming Interface，API）、用户界面和框架，应用程序通过 API 与区块链网络连接。执行层包括智能合约、底层规则和链码。应用程序向执行层发出指令，交易从应用层传输到执行层，在执行层得到验证与执行。

2 现有方案

经过对现有物联网终端设备跨域认证方案进行分析，可以发现：域内物联网终端认证设备可通过有中心的方式（如 PKI、令牌、IBC）实现身份认证，或通过无中心方式（如边缘计算、区块链）等方式实现域内身份认证；在域内认证的基础上采用区块链、第三方可信中心（身份联盟）等方式进行终端设备的域间认证机制设计，从而实现终端设备的跨域认证，如图 5 所示。

第三方可信中心存在单点失效、易受攻击等安全风险，且建立成本消耗相对较高，而区块链具有无中心、分布式、不可篡改等独特技术优势，是实现物联网终端跨域认证可选择的优势技术，因此本文主要针对基于区块链技术的物联网终端跨域认证方法和成果进行调研分析。

本文对 52 篇相关文献进行了研究分析与总结，将基于区块链的物联网终端跨域认证方案大致分为三种类型，即融合了传统身份认证机制的区块链跨域认证方案、采用跨链技术的跨域认证方案以及其他基于区块链的物联网终端跨域认证方案，具体分类如图 6 所示。其中，融合了传统身份认证机制的区块链跨域认证方案主要解决了跨域认证过程中引入可信第三方和有中心等导致的问题，跨链技术则解决了跨区块链信任建立、实现物联网跨域访问等问题，其他基于区

块链的物联网终端跨域认证方案则采用了定制设备或满足特殊功能需求的机制等解决了物联网终端设备的跨域访问问题。

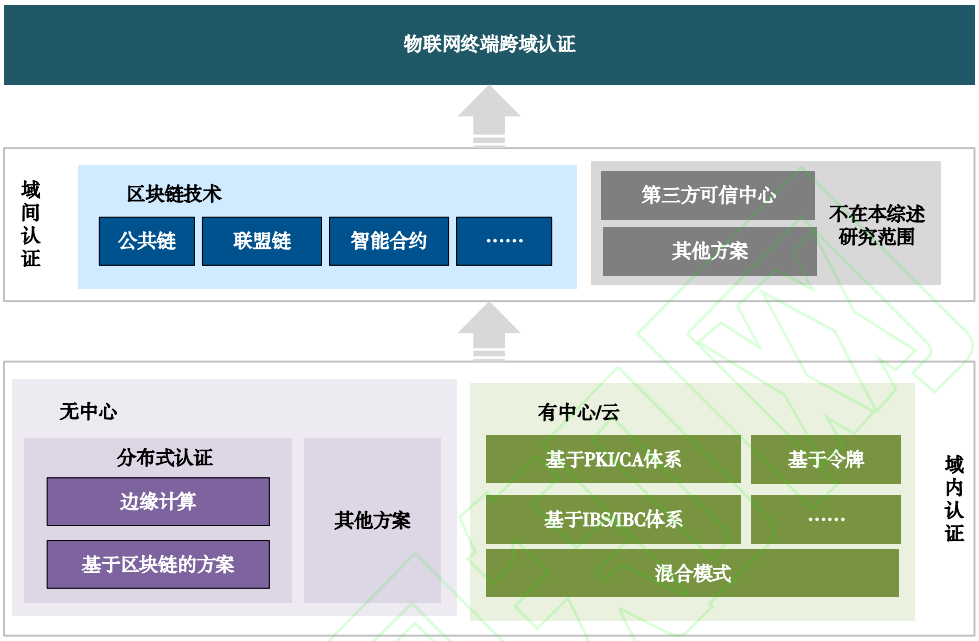

图 5　现有典型跨域认证方案分类

Fig.5　Classification of existing typical cross-domain authentication schemes

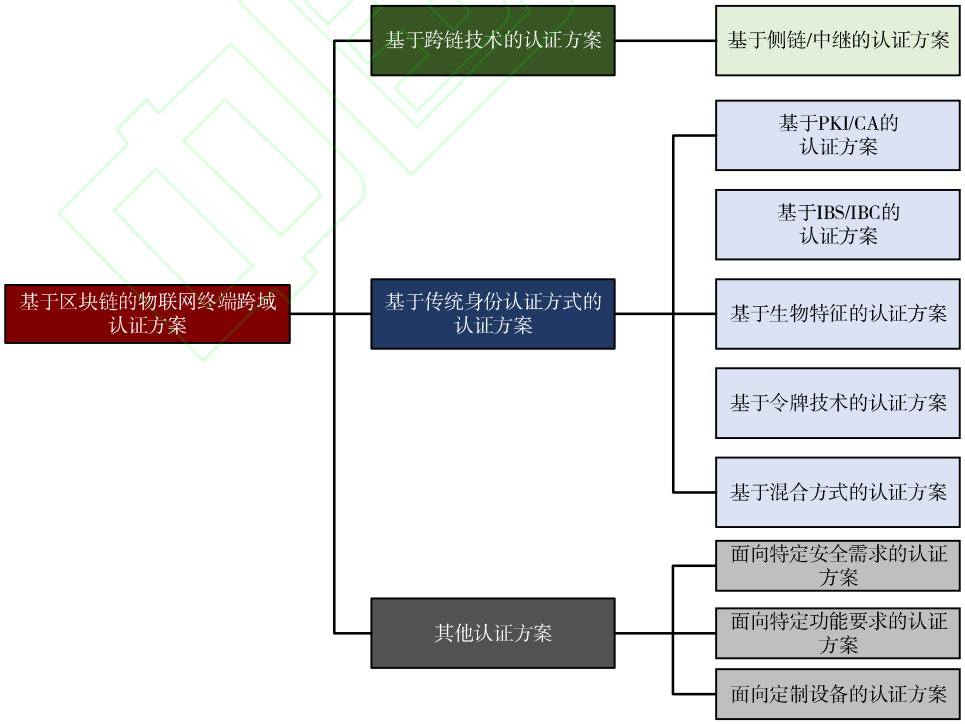

图 6　现有基于区块链的跨域认证方案分类

Fig.6　Classification of existing blockchain-based cross-domain authentication schemes

2.1 基于传统身份认证方法的跨域认证

2.1.1　基于 PKI/CA 的认证方案

为了确保安全高效地访问不同领域的资源，2018 年，Wang 等人[11]提出了一种基于区块链的跨域认证模型 BlockCAM，采用联盟链构建了一个以根证书授权机构为验证节点的去中心化网

络，并设计了跨域认证协议。授权证书的哈希值存储在每个区块中，身份验证过程省略了密钥加密和解密的开销，只需比较用户提供的证书哈希值是否与区块链中存储的哈希值一致。BlockCAM 具有去中心化、匿名性和抗干扰性等特点，在效率上比现有的公钥基础设施（PKI）跨域认证方案更具优势。

2018 年，周致成等人[12]在不改变域内 PKI 认证体系结构的基础上，提出了一种基于联盟链的高效跨域认证方案，将认证服务器和根 CA 证书服务器设置为区块链的节点，通过代理认证服务器查询并验证对方域根 CA 证书服务器在区块链上的无签名证书哈希值，实现跨域认证。相比于已有方案，减少了签名验签的次数，提升了跨域认证的效率，具有较强的可扩展性。

2019 年，面向电子政务应用，Chen 等人[13]提出了一种利用区块链共识代替传统可信第三方的信任转移模式。作者探讨了如何通过共识解决国家层面的 PKI 的统一信任服务问题，即将一些 CA 管理功能转移到区块链上，从工程角度证明了该方案的可行性。与传统方案相比，方案能够满足多个 PKI 系统的信任转移要求，可扩展性强，同时也能够保证安全性和效率。

2019 年，马晓婷等人[14]设计了基于区块链的 PKI 域联盟模型 ISE-CBCM，设计了 PKI 域证书管理机制，简化了证书使用过程，降低了证书维护成本，实现了异构 PKI 域间高效快速的跨域认证交流。该方案存在三方面的不足：一是设计的证书结构未与 X.509 证书进行仿真比较；二是未量化分析链上存储的证书在查询接口时产生的通信量、计算量以及时间开销；三是跨域方案未解决区块链存储数据造成的开销浪费固有问题，信息服务实体（Information Services Entity, ISE）端的计算量待优化。

为了克服传统 ID 管理系统跨多个域的局限性，2020 年，Kim 等人[15]提出了一个使用区块链的分布式 ID 管理系统，为工业物联网（Industrial Internet of Things, IIoT）应用程序提供跨域联邦 ID。该系统将在互联网规模的实体之间（即使它们第一次见面）产生更大的信任。Kim 认为：使用区块链的去中心化联邦 ID 管理（Federated ID management, FIM）方案将是物联网世界一个很有前途的替代方案。

2020 年，黄穗等人[16]在不改变原有认证架构的前提下，提出一种基于区块链和布谷鸟过滤器的跨域认证方案（IABC）。通过智能合约构造布谷鸟过滤器，实现证书的注册、查询和撤销，提高了跨域用户身份认证效率；设计区块链跨域数字证书（Blockchain Cross-domain Digital Certificate, BCDC）组成结构，证书由区块链多个域的根 CA 节点生成，唯一性通过添加证书生成时间戳等信息进行保证，并将证书映射为二进制指纹信息插入过滤器，直接将证书存储成本降低了一个数量级。此外，方案的有效性和可行性通过在联盟链平台 Hyperledger Fabric 上搭建测试模型得到了验证。

2021 年，张金花等人[17]设计了边缘计算环境下基于区块链的跨域认证与密钥协商协议，减轻了云中心的压力。该方案由物联网终端设备（Devices，D）、边缘认证服务器（Edge Servers，ES）、区块链认证中心（Blockchain Certificate Authority，BCCA）组成。BCCA 负责颁发证书，将终端设备的证书 Hash 值存储在区块链上，减少了证书签名验签次数。基于联盟链的跨域属性也使得不同域间的设备能够顺利完成认证和密钥协商。与已有方案相比，该方案能够抵抗重放攻击，具有前向安全性，且计算开销较少、效率较高，适用于低性能的物联网设备。

为了解决电力终端跨域认证中复杂的认证过程和隐私泄漏问题，2020 年，Wang 等人[18]提出了一种基于区块链的身份认证机制。通过对电力通信网络的分析，详细设计了三种流程，包括

身份认证、域内认证和终端的跨域认证。此外，为了解决交叉认证中不同安全级别的领域之间的安全问题，作者对身份安全进行了评估，然后建立了一个跨领域的认证可信度矩阵。通过优化可信度矩阵，能够更准确地计算出功率终端的识别级别。最后，从场景、算法科学、可扩展性和鲁棒性等方面对所提出的跨域认证机制进行了评估和分析。下一步，Wang 等人将研究深度学习和机器学习等智能算法，并将其应用到提出的认证机制中，实现可信度评估的动态性和自适应性。

针对智能电网 V2G（vehicle-to-grid）网络中的攻击威胁，2020 年，Liu 等人[19]基于联盟区块链和 SM9 密码算法，提出了一种跨域认证方案，能够在不改变 PKI 认证模式的前提下，将授权域加入区块链中实现高效跨域认证。该方案在自适应选择消息攻击下具有生存性和不可遗忘的安全性，可以抵抗重放攻击和拒绝服务攻击，具有可扩展性。

2020 年，Li 等人[20]提出了一种基于区块链智能合约的跨域认证和密钥协商系统，设计了一个跨域的认证和密钥协商协议，使用智能合约管理节点的公钥，系统参数通过合约查询确认。在该协议中，漫游用户可以根据漫游域的系统参数选择临时认证参数来完成认证和密钥协商，用户在此过程中是匿名的。协议安全性通过 CanettiKrawczyk（CK）模型、形式化分析工具得到了证明和进一步的分析。由于该协议没有复杂的加密操作和证书验证，它的计算和通信开销较低。但是该系统存在不足，系统只测试了其计算消耗，没有对整个系统进行仿真实验来测试通信等其他性能。

2020 年，郭炜立等人[21]提出了一种基于区块链的跨域认证改进方案。该方案以区块链为基础，在系统内设置签名算法和加密算法，节点之间互相监督，从而在一定程度上保证去中心化区块链内存储的数据具有较高的可信度。该方案假定各个加入区块链的根 CA 是可信的，作为验证节点自生成区块链根 CA 证书，在区块链内进行登记，以便其他节点查验区块链内的节点是否可进行有效的查询和读写操作，同时借助区块链的工作量证明（Proof of Work, PoW）共识算法，共同维护区块链。但是，该方案存在两个方面的不足，一是采用和比特币一样的 PoW 共识机制，会导致大量计算资源的浪费，且耗时较长；二是当跨域规模变大后，随着加入系统的节点数越来越多，系统的灵活性会降低。

为了克服 IBE 不适合大规模跨域架构的缺点，2021 年，Liu 等人[22]提出了一种可以实现跨域认证的区块链模型。该方法在不改变现有 PKI 认证模型的情况下引入了区块链，提出了一种将 PKI 环境和区块链相结合的认证协议。它允许跨不同的 IBE 和 PKI 域进行通信，同时确保在分布式多域网络环境中的资源或服务共享的安全性。此外，它还提供了匿名性，因为在区块链中只存储用户的证书哈希就可以保护私有信息。该模型具有良好的安全性、实用性和较高的可伸缩性，避免了传统 PKI 模型和复杂的认证传输存在的瓶颈问题。与其他方法相比，该方法具有良好的计算能力和吞吐量，并且通用、简单。

考虑到车辆制造的复杂性和智能传输终端的异构性，在消息交换过程中进行车辆身份验证至关重要，而现有的方案不能适应多域场景、满足安全性、匿名性和条件隐私保护。2021 年，Yang 等人[23]提出了一种基于区块链的分层多域车辆认证方案，感知层采用基于假名的认证方法保证匿名性和可追溯性，管理层采用 PKI 体系，设置 CA、假名 CA（Pseudonym Certificate Authority, PCA）和可信管理机构（Trust Authority, TA），并在管理层上架构区块链层实现域联通。其中，假名的生成和分发由多个实体监督和执行，提高了可靠性，能够适应动态和不可预测的假名请求。安全性分析和实验结果表明，分层多域车辆认证

方案可行且开销较低。

2021 年，魏欣等人[24]设计了适应于物联网跨域认证的架构。该架构通过引入边缘网关，实现对物联网设备的接入及管理，提高物联网的管理效率，屏蔽底层异构性问题。在不同 CA 之间部署联盟链，利用多 CA 共识简化域间认证流程，构建物联网可信跨域信息交互环境。通过边缘网关实现物的描述及接口上链，访问者可通过调用智能合约对物进行操作，增强了物联网的连通性。通过设计基于网关的跨域认证流程，增强了认证中的隐私保护。该方案存在四个方面的不足：一是多中心备份的服务方式能够促进可信合作，但是需要作为完整节点对链上的全部信息进行存储，存储成本明显增加；二是区块链不断增量且不可删除，会导致数据持续增长，规模化实施后，难以保证查询效率；三是匿名化与可信之间存在平衡，实际部署中需要按照相关法律法规要求进行具体操作；四是物联网环境错综复杂，完整节点难以保证数据可信发布，设备常以微弱的计算及安全性能暴露在大量攻击下，也难以保证上链数据真实可信。

2021 年，Chen 等人[25]提出了一个高效的隐私保护的跨域认证方案（XAuth），它能够兼容现有的 PKI 和证书透明度（Certificate Transparency, CT）系统。通过采用星际文件系统（Inter Planetary File System, IPFS）和区块链技术解耦存储和控制层，从而提高 XAuth 的性能和安全性；设计了一种基于多默克尔哈希树（Multiple Merkle Hash Tree, MMHT）结构的轻量级正确性验证协议，处理大量身份数据，满足快速响应的需求；利用零知识证明算法，提出了一种保护隐私的跨域认证方法，满足用户隐私保护需求。安全分析和实验结果表明，XAuth 在实践中是高效且适用的。

表 1 对基于 PKI/CA 认证方案从应用场景、技术特点和方案优缺点等方面进行了对比分析。除了适用场景不同外，上述方案整体而言在安全性、认证效率、通信和计算开销或有不同程度的改良。部分方案如文献[11][12][17][22]等在技术上的一大革新就是通过区块链存储证书的哈希值，以此达到提升效率、增强安全性等目的。当然有些方案如文献[21][24]也存在计算资源浪费、存储成本增加等问题。

表 1　基于 PKI/CA 的认证方案的对比分析

Table 1　Comparative analysis of authentication schemes based on PKI/CA technology

文献	特定场景	技术特点	方案优点/缺陷
[11]	-	以根证书授权机构为验证节点，区块存储授权证书的哈希值	具有匿名性、抗干扰性，效率更有优势
[12]	-	设置认证服务器和根 CA 证书服务器为区块链的节点,代理认证服务器,无签名证书哈希值	签名验签次数减少，认证效率提升，具有较强的可扩展性
[13]	电子政务	共识，将一些 CA 管理功能转移到区块链上	可扩展性强，安全性和效率可以得到保证
[14]	-	PKI 域证书管理机制	证书使用过程简化，证书维护成本降低；未量化计算、通信和时间开销
[15]	工业物联网	去中心化联邦 ID 管理	信任提升
[16]	-	布谷鸟过滤器，区块链跨域数字证书	证书存储成本降低一个数量级，方案有效可行
[17]	边缘计算	边缘认证服务器、区块链认证中心、区块链存储证书 Hash 值	抗重放攻击，具有前向安全性，且计算开销较少、效率较高
[18]	智能电网	认证可信度矩阵	算法科学性验证、具有可扩展性和鲁棒性
[19]	智能电网	SM9 算法，授权域加入区块链	抗重放等攻击，具有可扩展性
[20]	-	智能合约管理节	计算和通信开销

		点的公钥和查询系统参数	较低，缺少通信性能测试
[21]	-	自生成区块链根 CA 证书	计算资源的浪费，耗时较长，灵活性低
[22]	-	区块链存储证书哈希	良好的安全性、实用性和较高的可伸缩性，通用、简单
[23]	车联网	假名，PKI 体系	可行且开销较低，匿名可追溯
[24]	-	边缘网关，智能合约	物联网管理效率提升，屏蔽底层异构性问题；存储成本增加
[25]	-	IPFS、多默克尔哈希树、零知识证明算法	轻量级快速响应，保护用户隐私

2.1.2 基于 IBS/IBC 的认证方案

2020 年，Shen 等人[26]提出了一种高效的区块链辅助的安全设备认证机制 BASA（Blockchain-Assisted Secure Authentication mechanism），引入联盟链构建不同领域之间的信任，用于工业物联网跨域身份认证。通过区块链外存储减少链上数据的写入，消除吞吐瓶颈。在认证过程中利用基于身份的签名，设计了身份管理机制，通过调用实体的公钥弥补 IBC 机制身份暴露的缺点，从而保护设备隐私，实现实体跨域匿名访问。为了保证后续通信的安全性，双方会协商会话密钥。安全分析和模拟实验结果证明了 BASA 认证机制的有效性和效率。

2020 年，Jia 等人[27]提出了一种基于身份的物联网跨域认证方案 IBRA（Identity, Recognize, Blockchain, Algorithm），对传统的认证方案进行了创新，包括基于 IBC 的跨域认证方法、基于阈值加密和智能合约的多域联合授权机制，避免了物联网终端需要维护不同应用域多个证书的问题。并基于 Hyperledger Fabric 和 YH-RADIUS 开源项目实现了 IRBA 的原型系统，对其核心机制进行了性能评估。实验结果表明，IRBA 具有良好的处理性能和灵活性，适用于多种物联网场景。

2021 年，王弘洁等人[28]通过研究传统的 PKI 和 IBC 模型，对比分析两者的特点、适用场景及差异，指出了 PKI 体系中证书库庞大导致的维护问题、IBC 体系中主密钥泄露即密钥托管问题等不足之处。鉴于这些情况，针对智慧医疗场景资源受限医疗设备缺少轻量级跨域认证方案的问题，提出了基于区块链的跨域认证模型 BASA，通过引入区块链来构建不可信域之间的信任，并利用联盟区块链账本和链码，将公钥调用过程转化为一个区块链账本编写操作，使得 IBS 系统中的公钥调用过程简单易行。但是 BASA 仍有局限性：①KGC、区块链代理服务器（Blockchain Agent Server, BAS）和身份验证代理服务器（Authentication Agent Server, AAS）之间频繁的数据交换，导致通信开销增加；②由于区块链的使用，需要额外的链码写入和查询延迟；③对于 IBC 密钥托管问题，BASA 也还不能完全解决，主密钥泄露问题在单个域内仍然存在，在密钥托管问题仍有待进一步优化；④该远程医疗系统只完成了核心的跨域问诊功能，距离完整的远程医疗系统仍有很多功能需要完善，如域内信息的管理、新域拓展、区块链相关功能的可视化。

2021 年，魏松杰等人[29]针对异构网络环境中用户访问不同信任域网络服务时的跨域身份认证问题，提出了联盟链上基于身份密码体制的跨信任域身份认证方案。该方案利用联盟链架构来设计跨域身份认证模型，采用基于身份的方式来认证分属于不同 IBC 信任域的用户实体和信息服务实体，有效地减轻了用户端的计算压力。通过真实机器上的算法性能测试，与现有同类方案在统一测试标准下比较，该方案在运行效率上也体现出了明显的优势：计算量和通信量较低，实现了系统性能和安全性的有效均衡。

表 2 给出了基于 IBS/IBC 的物联网终端跨域

认证方案的对比分析。相较基于 PKI/CA 的身份认证方案而言，基于 IBS/IBC 的方案在数量上有所减少，但也都关注了工业互联网、智慧医疗等典型应用场景。整体而言，方案能够在充分利用区块链智能合约等技术特点的基础上，很好地应用会话密钥协商等安全机制，借此获得隐私保护、良好的性能或较好安全性等目标。

表 2　基于 IBS/IBC 的认证方案的对比分析

Table 2　Comparative analysis of authentication schemes based on IBS/IBC technology

文献	特定场景	技术特点	方案优点/缺陷
[26]	工业互联网	实体公钥调用，会话密钥协商	匿名访问、隐私保护
[27]	-	基于阈值加密、智能合约	处理性能和灵活性良好
[28]	智慧医疗	账本编写操作，链码	通信开销增加，查询延迟，主密钥泄露
[29]	-	异构网络基于身份的认证	计算量和通信量较低

2.1.3　基于令牌的认证方案

物联网面临的安全挑战复杂多变，访问授权对于其中的资源共享和信息保护至关重要。为了保护访问授权的安全性，2018 年，Xu 等人[30]提出了一种基于区块链去中心化能力的访问授权方案（BlendCAC），实现了面向物联网系统的去中心化、可扩展、轻量级和细粒度的访问授权机制；基于区块链提出了一种基于身份的令牌管理策略，利用智能合约进行访问授权的注册、传播和撤销。在该方案中，物联网设备是它们自己的主人，来控制它们的资源，而不是由中央机构监督。通过在 Raspberry Pi 设备和本地私有区块链网络上实施和测试，实验结果证明了 BlendCAC 方法的可行性。

2021 年，王思源等人[31]针对多域物联网下的设备协作场景，提出了一种融合区块链和权能令牌的访问控制机制。采用基于分布式的基于权能的访问控制（capability-based access control, CapAC）模型，将访问控制决策的工作由中心化服务器下放到被请求客体处进行分布式执行，每个设备仅负责处理与自身相关的访问请求，解决了物联网海量节点可能带来的中心化访问控制决策服务器单点故障问题。设计并实现了比简单支付验证（simplified payment verification, SPV）节点硬件需求更低的超轻节点。超轻节点不存储区块信息，只维护一个本地权能令牌列表，该列表是访问控制矩阵中对应的访问控制列表，它包含了所有其他实体持有的对该设备的访问权限。同时，超轻节点对权能令牌的验证是基于其本地令牌列表实现的。目前，该方案存在的不足：①在部分特殊场景中，权能令牌可能会暴露用户的一些隐私信息，不适合直接公开透明地存储在区块链中；②区块链上存储的数据随时间的推移必然会逐渐增加。加入区块链系统的物联网节点越多，权能令牌的数量随之越多，产生的访问控制日志记录也越多，使得跨域访问系统需要解决区块链互操作性、访问控制策略冲突、智能合约兼容性等一系列问题；③无法满足访问控制的实时性要求。

2021 年，Li 等人[32]提出了一种基于区块链的物联网跨域授权访问控制方法（CDDAC），设计了一种适用于轻量级设备的能力令牌结构。Li 提出的授权-轨迹上链策略增强了跨域委托系统的可扩展性，多域授权轨迹聚合方案支持域内/跨域委托系统的取证分析。采用的区块链轨迹策略，极大地提高了系统的可伸缩性，并具有更简单的策略变化过程。在以太坊官方公链测试网络 Ropsten 上的实验评估结果表明，CDDAC 具有良好的可扩展性，比现有方案 CapBAC 和 BlendCAC 具有更快的令牌验证速度和更高的决策效率。目前，虽然该方案具有许多优势，但仍存在隐私泄露问题。

2022 年，Zhang 等人[33]提出了一种基于联

盟区块链的轻量级身份验证方案，设计了一种类似加密货币的数字令牌来建立信任，并且信任生命周期管理是通过操作令牌的数量来执行的。综合分析和评估表明：该方案能够抵抗各种常见的攻击，并且在存储、通信和认证成本方面比竞争对手的方案更有效。下一步，作者等人希望在现实世界的物联网应用程序上进行广泛实验，并将该方案扩展到更多的跨域身份验证场景，如教育漫游，同时考虑隐私的增强和细粒度的信任管理。

基于令牌的认证方案对比分析情况见表 3，在方案数量上也不如基于 PKI/CA 的身份认证方案丰富，且均是针对通用场景下设计的身份认证方案，充分融合了区块链智能合约、策略上链以及基于令牌的身份认证机制等具有的技术特色，实现了更好的扩展性、效率和抗攻击性等目标，且多表现出了轻量级的特点。

表 3　基于令牌的认证方案的对比分析

Table 3　Comparative analysis of authentication schemes based on Token technology

文献	特定场景	技术特点	方案优点/缺陷
[30]	-	基于身份的令牌管理、智能合约	可扩展、轻量级和细粒度访问控制，自管理资源
[31]	-	委任权益证明、智能合约、引入轻量化节点	适配异构设备，系统可扩展性强；隐私泄露、实时性差
[32]	-	授权-轨迹上链策略，轻量级	可扩展性好，速度更快、效率更高；隐私泄露
[33]	-	类似加密货币的数字令牌，轻量级	抵抗常见攻击，存储、计算、通信成本消耗更少

2.2 基于跨链技术的认证方案

在物联网接入认证领域，当认证需求跨越异构区块链系统的多个域时，跨链认证数据和远程认证互操作性显得尤为重要。跨链技术主要分为公证人方案、侧链/中继和散列锁定等三种机制，不同的跨链技术适用于不同的应用场景。相比于基于传统方案的跨域认证方案，基于跨链技术的跨信任域的认证方案相对较少，物联网终端设备跨域认证方案和机制设计中推荐并大多采用的是基于侧链/中继的跨链技术。

2.2.1　通用场景认证方案

2019 年，Tong 等人[39]设计了一个分片协议 MDIoTSP，解决海量数据认证需求，相应联盟区块链系统由一个 Trust Authority、一个 Main Shard 和多个 Shard 组成。该协议将整个区块链划分为多个小碎片，每个小碎片是一个微区块链（即 Shard），通过合并多域物联网区块链生态系统中碎片生成的子块的哈希摘要来达成最终共识。开发了 MicrothingsChains，在多域物联网区块链中运行 MDIoTSP，经证明：MDIoTSP 随着碎片数量近似线性地扩大交易吞吐量。

2020 年，Li 等人[40]针对物联网多域认证要求，提出了一种基于跨链技术的物联网跨域认证方案。通过设计块数据结构实现增强访问认证功能，认证过程通过智能合约实现，认证信息通过密钥共享方法进行加密和分发，以确保认证数据的安全性。该系统安全性高、稳定性好，实现了跨域终端的互操作性，可以直接部署在现有的系统中，并与本地系统兼容。但是该方案在效率、场景适用性以及灵活性方面有待提升。

2020 年，Zhang 等人[41]针对公有链共识耗时长以及私有链不能统一认证的问题，提出了基于混合区块链模型的异构节点跨域认证方案。基于信任模型，选择能力节点作为代理节点实现与区块链网络的交互，完成认证操作，方案具有较好的安全性和效率。

2020 年，Jia 等人[42]提出了一种结合边缘计算和侧链技术的分布式物联网认证方案 A2 Chain，包括应用域区块链和联盟区块链。该方案利用边缘计算去中心化处理认证请求，消除认证服务和网络的负担；其次，利用侧链技术安全共享物联网设备的身份验证信息，实现物联网设备的跨域

身份验证。此外，A2 Chain 将公钥基础设施（PKI）算法替换为基于身份的密码算法（IBC），以消除中心化认证模型带来的管理开销，实现去中心化认证。

2020 年，Li 等人[43]针对物联网多域认证需求，将跨链技术应用于跨域认证证书传输，建立了物联网认证系统中的链数据通道，提出了一种基于改进实用拜占庭容错（Practical Byzantine Fault Tolerance, PBFT）算法的物联网跨域认证方案。首先，提出了一种基于区块链的跨域认证体系结构，设计了块数据结构，以增强访问认证功能；认证过程通过智能合约实现，认证信息通过密钥共享方式进行加密和分发，以确保认证数据的安全性。仿真结果表明，方案在安全性和可用性方面具有显著优势。

2020 年，Gauhar Ali 等人[44]提出了一个基于分布式区块链（BC）的跨域授权和访问控制轻量级框架 xDBAuth，提出了本地和全球智能合约的层次结构，本地 BC 和本地智能合约管理内部资源，全球智能合约对外部用户\物联网设备执行跨域授权和访问控制。该框架通过允许外部用户在其父物联网域中获得身份验证来保护外部用户的隐私。在身份验证期间，使用身份验证/完整性证明（PoAI）机制查找和检索存储在本地 BC 上的用户/物联网设备平台杂凑。认证成功后，全球智能合约将根据 BC 上存储的授权策略对用户/IoT 设备进行授权。在该框架中，全局 BC 用于验证和存储授权策略，“授权策略”的创建、撤销和实施对所有用户都是透明的。该框架使用 Node.js 进行实现，实验结果表明，xDBAuth 计算开销较小，具有高吞吐量。但是 xDBAuth 的授权策略保存在区块链上，策略变更存在困难。

总体来说，将策略上传至区块链的设计会带来巨大的同步负担，且策略不易更改，难以实现灵活和可扩展的访问控制。

2021 年，张亚兵等人[45]针对现有集中式身份认证方式在物联网应用场景下管理成本高、异构信任域之间证书管理困难以及多信任域难以互信等问题，提出了一种基于多层区块链的跨域认证方案。即使用本地区块链进行分布式节点管理，使用公共区块链实现区块链之间的跨链身份认证。并且，针对跨域访问多信任域难以互信的问题，提出了基于信任度评价的委托权益证明，用以评估节点的可信度。安全和效率分析表明在保证较好安全性和有效性的基础上，方案跨域认证效率得到了提升。

2022 年，Alsaeed 等人[46]基于区块链和雾计算提出了一种跨域物联网认证框架，用以增强物联网系统的安全性和可扩展性。该框架采用多级区块链平台，采用雾节点、设置私有链支持计算和存储资源紧密的物联网设备，设置全球 CA 和公有链支持物联网系统之间的跨域认证。但该方案未提供框架技术细节，未进行性能评估和安全性分析。

2022 年，赵平等人[47]针对异构信任域之间的跨域认证问题，设计了一种主从区块链身份认证结构和匹配使用的分层拜占庭容错算法，实现了 PKI 体制与 CL-PKC 体制异构信任域间的双向跨域身份认证，解决了集中攻击和整链共识效率低等问题。通过主从链分层、分阶段共识，减少了共识参与节点数量，提高了认证效率；在不改变信任域节点功能的前提下，将信任域的特有功能节点与主从链节点对应，链下存储元数据，链上存储数据杂凑值，使用区块链证书的哈希值高效传递信任，优化了认证流程。仿真实验结果表明，与已有方案对比，该方案能够实现安全通信，提高了共识效率和容错性，降低了认证过程的计算和通信开销。

表 4 从方案的技术特点、优缺点等角度对上述方案进行了对比。可以看出，通用场景下的跨域身份认证方案总体来讲在安全性、效率上或开销等方面有不同程度的提升和改善，能够充分有

效利用区块链本身所具备的技术特点，如智能合约、公私链等，针对海量数据认证、效率提升、成本节约、异构互信等不同应用需求，设计符合要求的物联网终端跨域认证方案。但是部分方案也存在明显不足，如文献[46]未进行性能评估和安全性分析，这导致所提方案的正确性与可行性论证十分欠缺。

表 4　通用场景下基于跨链技术认证方案的对比分析

Table 4　Comparative analysis of authentication schemes based on cross-chain technology in common scenarios

文献	技术特点	方案优点/缺陷
[39]	区块链分块	吞吐量线性增加
[40]	智能合约、密钥共享	安全性高、兼容性好
[41]	信任模型、能力节点	安全性和效率较好
[42]	边缘计算、IBC	开销和负担较小
[43]	改进 PBFT 算法、块数据结构、智能合约、密钥共享	安全性、可用性优势显著
[44]	轻量级、本地与全球智能合约层次结构	开销较小、高吞吐量，但授权策略变更困难
[45]	本地链、公共链、基于信任度评价的委托权益证明	安全性和有效性较好，效率得到提升
[46]	雾节点、私有链，全球 CA 和公共链	未进行性能评估和安全性分析
[47]	主从链、分层拜占庭容错算法	安全通信、提高共识、认证效率和容错性

2.2.2　典型场景认证方案

2019 年，Zhang 等人[48]针对电力多业务集成后业务交互可能出现不可靠等安全问题，设计提出了一种基于区块链的电力服务跨域可信认证的主从链体系结构。通过引入主从链，实现了多种服务的隔离和服务交互的可信身份验证，及时检测异常服务节点的异常情况。实践证明，该方案能有效解决电力多服务集成不可信和提供可信服务。

2020 年，Cui 等人[49]提出了一种基于区块链的物联网多无线传感器网络（Wireless Sensor Network, WSN）认证方案。根据物联网节点的能力差异，将这些节点分为基站、集群头节点和普通节点，形成一个分层网络。在不同类型的节点之间构建一个区块链网络，形成一个混合的区块链模型，包括局部链和公共链，实现各种通信场景中节点身份的相互认证。其中，本地区块链完成普通节点的身份认证操作，集群头节点的身份认证在公共区块链中实现。实验结果表明，方案具有较为全面的安全性和较良好的性能。

2020 年，Dong 等人[50]提出了一种基于区块链的跨域认证策略。该策略使用 cosmos 网络模型，使移动设备在跨域移动时能够可靠地访问外部域网络。该方案中，由多个区块链组成的区块链网络可以使区块链通过区块链间通信协议（IBC）相互通信，从而实现移动设备在网络间移动时，可通过区块链间的通信访问外部域网络，而无需新一轮的身份认证。测试结果表明该策略具有可行性，且相比于其他跨域认证方案具有更好的性能。

2020 年，李大伟等人[51]分析了电力物联网终端跨域认证需求和面临的问题，提出了一种基于侧链技术的电力物联网跨域认证方案。包括：设计了区块数据结构和双向锚定认证信息传递模型，通过公钥证书和数字签名生成认证凭据，利用时间戳确保认证信息的时效性；设计了基于侧链技术的物联网终端跨域认证流程，实现了认证凭证跨域可信传递。

2021 年，为了解决无人机部署中的身份安全限制，Liu 等人[52]提出了一种基于区块链和 5G 技术的无人机跨域认证方案。无人机的身份通过应用多签名智能合约来动态管理，该合约包含用于动态身份管理和身份验证的访问控制表，来自不同域的实体可以在不知道真实身份的情况下相互进行身份验证。应用本地私有链用于管理域内资源，联盟链面向授权节点进行数据共享，主要用于跨域认证。性能评估结果表明，该方案效率优于其他方案。但是，该方案存在两个局限性，

即当事务失败率较高时，无人机可能必须启动多个事务来完成身份验证；而且，在区块链上基于智能合约写入和读取数据会引入延迟。

针对工业物联网(IIoT)中现有的用户认证机制存在单因素认证和适应性差的问题，2021 年，Wang 等人[53]构建了一个边缘智能授权的 IIoT 架构，提出了一种基于转移学习的区块链认证机制 ATLB。通过引入基于转移学习的认证机制，构建了可信智能区块链，从而进一步增强了工业应用的隐私保护。实验结果表明，ATLB 能够在 IIoT 中对本地用户和外部用户进行准确的认证，且在各种 IIoT 场景中实现了高吞吐量和低延迟。

2022 年，Xue 等人[54]提出了一种适用于区域医疗联盟系统的基于两个协作区块链(BC)的安全高效跨域认证方案。域内 BC 记录任何合法用户的注册和认证信息，域间 BC 负责记录用户的跨域认证信息。在每个领域中，综合医院作为可信第三方服务提供商实现跨链交互。在整个跨域认证过程中，利用匿名机制增强安全性；在跟踪恶意用户时，域内 BC 使用改进的变色龙杂凑算法对用户状态进行编组；在跨域 BC 中扩展黑名单默克尔树，保护不同域的服务不被非法访问。方案安全性和性能优于其他方案。

表 5 从方案适用的特定场景、技术特点以及方案优点等角度对上述方案进行了对比。典型场景包括电力、工业互联网、无线网络、移动网络、无人机、医疗系统等具有代表性的行业，这些行业由于各自的行业特殊性，其产生的安全问题和对物联网终端跨域认证的需求也相对更具有特色，如电力存在交互不可靠、无线网络存在节点能力差、IIoT 存在单因素认证和适应性差等问题。因此基于这些不同需求和问题提出的物联网终端跨域认证方案也更有需求针对性和场景局限性。整体而言，典型场景下基于跨链技术的物联网终端跨域认证方案都在解决应用需求的同时更好地兼顾了安全性或性能，可行性、安全性和性能有所提升。

表 5 典型场景下基于跨链技术认证方案的对比分析

Table 5 Comparative analysis of authentication schemes based on cross-chain technology in typical scenarios

文献	特定场景	技术特点	方案优点/缺陷
[48]	电力	主从链	可信身份验证、检测异常
[49]	WSN	节点分层网络、局部链、公共链	全面安全性和较好性能
[50]	移动场景	cosmos 网络模型、IBC	可行且性能较好
[51]	电力	证书、时间戳、双向锚定认证信息传递模型	不可篡改、分布式共识
[52]	无人机	多签名智能合约	效率优于其他方案，但有两个局限性
[53]	工业物联网	转移学习、边缘智能授权	认证准确、高吞吐量和低延迟
[54]	医疗联盟系统	可信第三方、匿名机制、改进的变色龙杂凑算法、协作区块链	安全性和性能优于其他方案

2.3 其他认证方案

基于区块链的其他跨域认证方案主要涉及面向特定全需求、特定功能要求以及基于定制设备等多种类别，重点结合特定场景和特定业务需求、已有资源设备或解决特定问题而被研究提出。

2.3.1 面向特定安全需求的跨域身份认证

特定安全需求主要包括匿名化、用户隐私保护等，基于区块链的物联网终端跨域认证方案着重考虑在满足安全需求和指标的前提前进行方案设计和考量。

2019 年，Yao 等人[55]提出了一种区块链辅助的分布式车辆雾服务（Vehiclar Fog Service, VFS）轻量级匿名认证机制（BLA），用于驾驶车辆。BLA 具有以下优点：1）车辆本身在进入新数据中心时可以决定是否重新认证；2）车辆可以匿名访问 VFS 并随时更改假名；3）BLA 是非交互式的，

显著减少了通信延迟；4）采用区块链技术可以有效抵御对中央权威管理数据库的攻击，能通过消除认证过程中与服务管理器（service managers, SMs）之间的通信来减少用户认证时间。但是，作者只对 BLA 的安全特性进行了非正式的安全证明，且身份验证和共识阶段的开销有待进一步降低。

2022 年，Huang 等人[56]提出了一个统一的区块链辅助安全跨域授权认证（authorization and authentication, AA）框架，可以保证跨域资源访问的透明，同时保护用户隐私。在该框架中，应用服务提供商（application service providers, ASPs）可以灵活地将认证能力委托给区块链，由不同 ASPs 授权的用户可以通过区块链进行认证，对认证事件进行公开审计和跟踪。由于区块链是公开访问的，用户的敏感身份属性可能会在身份验证过程中暴露。为了解决认证事件导致的隐私泄漏问题，利用基于阈值的同态加密、零知识证明和随机排列等隐私保护技术，在区块链上隐藏用户的敏感信息。此外，将一个加密累加器和安全哈希函数集成到允许 ASPs 通过全局撤销合同撤销其用户的框架中，从而提高用户撤销效率。安全分析表明，所提出的框架可以实现所有理想的安全和隐私特性，并开发了一个概念验证原型来证明所提出框架的正确性和有效性。

2.3.2 面向特定功能要求的跨域身份认证

特定功能需求主要包括合法用户区分、认证日志存储、可信认证、可信度量、异构资源认证、轻量级认证等。针对这些特定功能需求，研究人员基于区块链技术设计了大量的物联网终端新型跨域认证机制。

2018 年，Fu 等人[57]提出了一种在物联网环境下进行跨域通信的新认证机制，能够有效地区分合法用户和竞争对手。该机制具有“挑战-响应”架构，利用物联网设备拍摄的照片进行身份验证。通过使用带外信息而不是加密原语，该机制实现了较高的可用性和高效率。

为了提高认证效率，2019 年，Guo 等人[58]提出了一种基于区块链和边缘计算的分布式可信认证系统，包括物理网络层、区块链边缘层和区块链网络层。通过区块链网络，设计优化实用的拜占庭容错共识算法，构建存储认证数据和日志的联盟区块链，保证可信认证，实现终端活动可追溯。此外，边缘计算应用于区块链边缘节点，提供基于智能合约的名称解析和边缘认证服务。同时，设计了一种非对称密码机制，防止节点和终端之间的连接受到攻击。并提出了一种基于边缘计算的缓存策略来提高命中率，仿真结果表明，缓存策略在平均延迟方面优于现有边缘计算策略 6%－12%，在命中率方面优于现有方案 8%－14%。但是未在基于区块链的数据共享平台上进行试点验证。

针对异构资源集成需求增长和复杂工业网络下边缘服务安全挑战问题，2019 年，Zhang 等人[59]提出了一种边缘智能和区块链授权的工业物联网框架，以高效安全的方式整合调度工业应用的分布式异构边缘资源，实现了灵活和安全的边缘服务管理；提出了一种基于跨域共享的边缘资源调度方案，以最小化边缘节点的运行成本，提高服务容量；设计了一种信用差异化的边缘交易审批机制，高效达成边缘资源交易共识。实验结果表明，该方案在边缘服务成本和服务容量方面都有显著的改善。但是为考虑前期知识学习在动态变化环境中对后期理解学习的影响，并且未考虑不同区块链技术间的互操作和集成问题。

2019 年，董贵山等人[60]针对跨域认证中存在的身份可信度量机制缺乏问题，提出基于区块链的异构身份联盟基础架构，包括异构身份联盟链（联盟区块链）、身份管理系统（如 eID、电信等）、基础身份信息库等。通过联盟链管理联盟统一身份信息（包括可信评价）和相应的跨域验证密钥，通过智能合约实现异构系统间信任传递、

跨域访问。设计了身份可信度初始化方法和基于熵的概率加权的主观信任度与风险评价方法，动态描述跨域认证用户的可信度，具有良好的可扩展性、准确性和健壮性，能够提高跨域认证的安全性和自适应性，促进统一信任服务的普及。

2020 年，Xiao 等人[61]针对跨域物联网设备轻量级身份验证问题，首次提出基于 IOTA 区块链技术和移动边缘计算（mobile edge computing, MEC）的轻量级跨域近距离身份验证方案，包括定制的事务定义和实现基于临近性认证的关键操作流程，减少了繁重的后端参与，并对方案进行了内部原型系统实现，可行性得到验证，但未开展性能增益评估。

2021 年，面向物联网终端的异构性给跨域认证带来的巨大困难，Tan 等人[62]针对分布式绿色智能设备（green smart device, GSD）管理模型带来的异构 GSD 用户访问和控制复杂性增加和 GSD 应用程序可伸缩性降低问题，提出了一个由区块链授权的通用 GSD 访问控制框架，基于 W3C 的分布式标识符（Decentralized Identifier, DID）标准构建统一的 GSD 管理平台，为用户分发虚拟 ID（visual ID, VID），实现分布式、轻量级、细粒度的访问控制，降低了访问控制的复杂性，提高了应用程序的可伸缩性，并保证了访问过程中权限数据和身份数据的可信度和不变性，但是带来了用户隐私泄露的风险。

2021 年，Xuan 等人[63]针对跨域访问过程中认证协议授权认证速度较慢的问题，在不考虑实际跨域的情况下，对跨域环境中的所有通信节点都采用相同的加密系统参数，基于无证书公钥加密 (Certificate-less Cross-domain Signature Algorithm with Different System Parameters, DSP-CCSA) 和智能合约技术，设计并实现了一种支持参数区分的无证书异构物联网数据跨域访问认证方案，该方法提高了跨域身份授权认证能力，支持在不同物联网应用之间使用不同的密码系统参数，但是通信成本较高，且不支持不同密码系统间的异构域跨域身份验证。

2021 年，Zhao Hongmei[64]提出了一种结合区块链技术和密码学的非对称加密技术，实现了高效跨境数据共享。首先，基于区块链和非对称加密技术，设计了文件同步合约和授权合约，利用区块链分布式存储优势确保用户跨境电子商务信息的隐私性。其次，设计跨域采集合约验证数据共享双方的身份，安全过滤非法用户。实验结果表明，该方案具有有效的存储服务器、较低的交易延迟与功耗以及可追溯性。但是，存在传播过程中人为泄露密钥等概率性安全问题。

2021 年，Wang 等人[65]从物联网中智能设备之间的认证关系中抽象出一个通用的无向图，结合累加器知识和标准数字签名方案，提出了一种不存在边顶点间的跨域数字认证框架 CroDA，将认证问题转化为签名传递性问题。CroDA 将用户的访问认证信息记录在区块链的公共账本上，被访问用户对交易进行验证，以决定是否接受访问；通过计算签名者到验证者的认证信息，并证明其合法性，实现跨域认证。分析和比较结果表明，与现有方案相比，CroDA 能够很好地解决实际的认证问题，实现了所有安全目标，并且具有更低的计算成本。

2.3.3 面向定制设备的跨域身份认证

定制设备主要包括路由及其协议修改定制、角色服务器设定等，需要对硬件设备及其相应软件支撑进行调整优化以支持物联网终端的跨域身份认证工作，具有一定的特色，但改造成本相对较高。

2019 年，Jordi Paillisse 等人[66]通过对基于组的策略进行扩展，提出、实现和评估了一种支持跨域通信中的访问控制体系结构。利用 Hyperledger Fabric 许可区块链，以安全且可审核的方式，分发访问控制策略，帮助克服传统 PKI 解决方案的缺点，同时保持每个组织的独立性。

为了减轻网络管理员的负担，前端构建在基于组的策略(Group-Based Policy, GBP)之上，这是一种著名的意图驱动语言，网络管理员指定区块链交易中的策略。LISP（Locator/ID Separation Protocol, RFC 6830）控制平面允许执行访问控制的路由器向区块链查询授权。作者实现了一个端到端实验原型系统，从可伸缩性和网络延迟方面对方案进行了评估。实验评估表明，这种设计可以用适中的存储介质来存储数千个访问策略，并在许可的区块链上实现线性更新时间。

2020 年，Sun 等人[67]通过集成区块链和角色映射访问控制技术，构建了一个基于区块链的可信、高效的跨域访问控制系统，主要由三部分组成：域组织、域管理服务器和区块链。使用区块链来记录用户角色、角色映射规则、访问策略和审计记录，从而防止单个服务器欺诈性地拒绝授权用户或允许非法用户访问资源。考虑到区块链的低吞吐量，设计了一个高效的智能合约，根据用户的访问历史做出访问决策，所有请求和决定都会上链，从而实现访问的不可否认性。作者通过仿真实验对方案的可行性和性能进行了评估，还对方案的抗攻击性进行了分析，但未进行形式化证明。

3 现存问题

在物联网总体框架中，身份认证是支撑物联网设备正常运行的重要组成部分。由上述现有方案可以看到，大多方案为通用方案，且多数在联盟链、测试链上进行了性能测评，安全性和效率针对传统方案更具优势，但是一般不针对具体应用场景进行更为有针对性的适用性分析。而针对特定场景的方案会更考虑场景特质和特殊性进行方案设计，更具有场景适用性。但是就目前而言，这些物联网环境中的身份认证机制仍存在许多问题，主要表现在以下方面：

3.1 系统安全问题

区块链安全存疑：用户存储在区块链中的数据是公开透明的，即使用户的地址假名关联不到真实用户，但是通过分析这些公开数据，可以跟踪用户活动或分析用户个人习惯，尤其是随着链上数据往来的增多，其关联性将或多或少地泄露个人隐私，一旦交易信息被恶意挖掘与利用，将会严重威胁用户隐私。因此，匿名性的不完善和不健全是区块链面临的严重潜在安全威胁之一。

集中式身份管理安全风险：部分已有身份认证模型和方案往往采用集中式管理的方式对用户凭证和身份进行管理，存在单点失效与故障，以及极大的隐私泄露风险。例如，用户身份凭证，如口令、生物特征因子等通常存储在服务端，一旦服务端遭受攻击，可能导致系统无法使用，且所有用户凭证面临被泄露的风险。

认证机制设计潜在隐患：一些身份认证机制只采用了单向身份认证，并且用户的身份信息与认证信息是相互分离的，这会导致非法用户能够冒充合法用户发送信息，盗取系统使用权限。同时，大部分身份认证机制只适用于特定的身份数据结构，导致在异构身份管理系统之间对实体的身份信息进行管理仍存在比较大的安全可靠融合互通问题。此外，物联网规模持续扩大的需求与日俱增，如何保证认证机制具备安全可扩展的能力也是必须关注与考量的重要问题。

认证协议脆弱性问题：目前的认证协议多关注可用性、效率及身份认证过程中的安全性，但是对于抗攻击性的研究相对薄弱。现有方案一般会考虑部分面向部分攻击的鲁棒性，有些仅是简单描述分析，未进行形式化安全证明。有些认证方案甚至没有考虑应对潜在攻击时的鲁棒性问题，例如 sybil、节点捕获、中间人攻击和侧信道攻击等。

3.2 隐私保护问题

现有部分基于区块链的物联网跨域身份认证模型和方案存在用户隐私信息泄露的风险。用户的秘密信息，如用户身份、交易数据、位置等信息可能会被身份服务提供方或应用服务方滥用。第三方平台自身也存在隐私泄露的风险，如应用服务方自身的业务运营数据可能会被身份服务提供方滥用。特别是在特定的物联网应用，如智能电网、车联网等场景中，需要考虑位置和身份隐私保护问题。

3.3 传输与认证效率问题

现有物联网跨域身份认证方案在实际应用，随着用户和接入设备的增加，证书开销不断扩大，导致证书撤销列表过大、发证方批量维护列表周期较长、验证者下载更新列表不及时。同时，由于区块链的追加特性，各类数据的频繁交互、撤销等操作，会造成持续增长的数据存储量，将对身份认证系统造成巨大的存储和计算负担，影响系统的可用性、适用性以及运行性能。

4 发展趋势与建议

4.1 区块链性能亟待提高

尽管可以通过区块链的加密和数字签名提高物联网的安全性，但由于物联网系统和区块链系统的脆弱性，区块链网络缺乏有效管理和管控，安全性和隐私性仍然是基于区块链物联网方案的研究重点。同时现有区块链的可扩展性限制了区块链在大规模物联网中的广泛应用，区块链将事务数据记账到区块中，通过多级杂凑操作获得默克尔树保证数据的完整性性，极大降低了事务处理的速度。因此，提升区块链性能、增加区块链可监管特性是未来跨链认证研究的方向之一。

4.2 认证场景持续丰富多样化

随着 5G、智慧城市等技术的不断发展，物联网终端跨域认证场景不断丰富多样化，终端设备节点种类持续复杂化，互操作、互通性需求快速增长，应用孤岛将被持续打破，新的安全需求、隐私保护需求不断增加。物联网终端认证方案将在考虑多样化物联网终端节点特性兼容的情况下，满足跨多域环境下的动态、自适应身份验证，解决异构、多应用之间的身份互联互通等问题。

4.3 认证方案具有更好可扩展性

基于区块链的物联网终端跨域认证发展将具有较好的可扩展性，在管理大量物联网终端节点的同时，能够在没有任何设置、配置和额外附加冗余功能的前提下，更为快速、轻量级地添加新的物联网终端节点。并且，认证方案能够更好地考虑和满足设备的异构性问题，在保证终端节点认证安全性、抗攻击鲁棒性的同时，均衡考虑安全、效率和计算成本等多方面的问题。

4.4 统一身份认证广泛应用

随着跨域、跨境、跨层级身份认证需求的不断增加，统一身份认证的应用以及优化将成为一种必然且重要的选择。该认证模式，既能提升用户体验，又能规范系统管理、方便后续推广；不仅能够提升管理的安全性，还能提升用户管理、开发人员以及管理人员的协调性，便于业务系统的升级与更替，推动更为规范管理体系的建设。

4.5 新型身份认证技术赋能未来

量子密码学可以提供无条件的安全性，因此在过去的三十年中，陆续出现了一些使用量子资源的身份认证方案，即量子身份认证（Quantum identity authentication, QIA）协议。QIA 旨在设计具有由物理定律（量子力学）产生安全性的协议，是一种结合了量子力学和密码学的新型身份认证技术，通过将身份信息量子化，借助量子传输通道传递用户身份密钥。量子力学保证，即使窃听者能够完全访问量子通道也无法完美地区分非正交或部分可访问的量子态，并且窃听行为引入的干扰可以被检测到。基于量子力学最基础的海森堡测不准原理，量子密码身份认证具有不可复制和不可破译等高安全特性，对于身份认证技

术发展具有不可替代的颠覆意义。

4.6 深度学习与身份认证加速融合

基于深度学习的智能风险控制是未来跨域身份认证的重要安全保障和研究方向。移动互联网业务多因子身份认证虽然大大提升了身份认证的灵活性和安全性，但由于无法保证绝对身份认证安全并无法防止身份认证凭证复制，故此引入风险控制机制的智能风险控制成为确保身份安全的有效手段。

5 结束语

本文主要研究总结了国内外基于区块链技术的物联网终端跨域认证方案，详细分析了每个方案的主要工作及其解决的问题。在此基础上进一步归纳提炼出目前技术方案中存在的问题以及尚未解决的安全问题，为未来物联网终端跨域身份认证指明方向。也希望借此综述，能够帮助业内相关领域研究人员和工作者更好把握目前的物联网跨域身份认证研究进展和技术发展情况，为后续在物联网身份认证领域开展更为深入的研究奠定有力、坚实基础。

参考文献：

[1] GSMA. The Mobile Economy 2022[EB/OL]. 2022 [2022.05.10]. https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf.

[2] 深信服安全产品研发 . Mirai 物联网僵尸网络攻击事件深度剖析[EB/OL]. 2016 [2022.04.11]. https://bbs.sangfor.com.cn/forum.php?mod=viewthread&tid=22148.
Sangfor security product development. In-depth analysis of Mirai IoT botnet attack incident [EB/OL]. 2016 [2022.04.11]. https://bbs.sangfor.com.cn/forum.php?mod=viewthread&tid= 22148.

[3] cnBeta. 2021 物联网安全形势报告：去年有十亿级智能电子设备遭到攻击[EB/OL]. 2022[2022.05.10]. https://netsecurity.51cto.com/article/707523.html.
cnBeta. 2021 IoT Security Situation Report: One billion smart electronic devices were attacked last year[EB/OL]. 2022 [2022.05.10]. https://netsecurity.51cto.com/article/707523.html.

[4] Yu S J, Park K S, Park Y H. A secure lightweight three-factor authentication scheme for IoT in cloud computing environment[J]. Sensors, 2019, 19(16): 3598.

[5] Lin Y D, Truong D T, Ali A, et al. Proxy-based federated authentication: A transparent third-party solution for cloud-edge federation[J]. IEEE Network, 2020, 34(6): 220-227.

[6] 丁永善,李立新,李作辉.基于证书的匿名跨域认证方案[J].网络与信息安全学报,2018,4(05):32-38.
Ding Y, Li L, Li Z. Certificate-based cross-domain authentication scheme with anonymity[J]. Chinese Journal of Network and Information Security, 2018, 4(05):32-38.

[7] 万雨薇. 物联网环境下的跨域认证机制研究[D]. 南昌大学, 2018.
Wan Y. Research on the cross-domain authentication under the environment of the Internet of things[D]. Nanchang University, 2018.

[8] 吴卫. 边缘计算环境下物联网身份认证与隐私保护技术研究[D]. 西安电子科技大学, 2019.
Wu W. Research on Identity Authentication and Privacy Protection Technology of Internet of Things in Edge Computing Environment. Xidian University, 2019.

[9] 毛浥龙. 物联网跨域身份认证研究[D]. 重庆邮电大学, 2020.
Mao Y. Research on Cross Domain Authentication of Internet of Things[D]. Chongqing University of Posts and Telecommunications, 2020.

[10] 季一木, 陆毅成, 刘尚东, 等. HIBE-MPJ: 一种基于 HIBE 的物联网环境下跨域通信机制研究[J]. 南京邮电大学学报: 自然科学版, 2020, 40(4): 1-10.
Ji Y, Lu Y, Liu S, et al. HIBE-MPJ: cross-domain communication mechanism based on HIBE in Internet of Things environment[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2020, 40(4): 1-10.

[11] Wang W, Hu N, Liu X. BlockCAM: a blockchain-based cross-domain authentication model[C]//2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018: 896-901.

[12] 周致成. 基于区块链的大数据安全应用跨域认证关键技术研究[D]. 战略支援部队信息工程大学, 2018.
Zhou Z. Research on Key Technology of Cross Domain Authentication for Big Data Security Application based on Blockchain[D]. PLA Strategic Support Force Information Engineering University, 2018.

[13] Chen Y, Dong G, Bai J, et al. Trust enhancement scheme

for cross domain authentication of PKI system[C]//2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, Oct 17-19, 2019. Piscataway, NJ: IEEE, 2019: 103-110.

[14] 马晓婷. 基于区块链技术的证书管理与跨域认证方案[D]. 西安电子科技大学, 2019.
Ma X. Certificate Management and Cross-Domain Authentication Scheme Based on Blockchain[D]. Xidian University, 2019.

[15] Kim E, Cho Y S, Kim B, et al. Can we create a cross-domain federated identity for the industrial Internet of Things without Google?[J]. IEEE Internet of Things Magazine, 2020, 3(4): 82-87.

[16] 黄穗,李健,范冰冰. IABC:一种基于区块链和布谷鸟过滤器的跨域认证方法[J]. 小型微型计算机系统, 2020, 41(12):2620-2625.
Huang H, Li J, Fan B, et al. IABC: a Cross-domain Authentication Method Based on Blockchain and Cuckoo Filter[J]. Journal of Chinese Computer Systems, 2020, 41(12):2620-2625.

[17] 张金花, 李晓伟, 曾新, 等. 边缘计算环境下基于区块链的跨域认证与密钥协商协议[J]. 信息安全学报, 2021, 6(1): 54-61.
Zhang J, Li X, Zeng X, et al. Cross domain authentication and key agreement protocol based on blockchain in edge computing environment[J]. Journal of Cyber Security, 2021, 6(1): 54-61.

[18] Wang X, Gao F, Zhang J, et al. Cross-domain Authentication Mechanism for Power Terminals Based on Blockchain and Credibility Evaluation[C]//2020 5th International Conference on Computer and Commu- nication Systems (ICCCS). IEEE, 2020: 936-940.

[19] Liu D, Li D, Liu X, et al. Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid[C]//2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2018: 1-5.

[20] Li G, Wang Y, Zhang B, et al. Smart contract-based cross-domain authentication and key agreement system for heterogeneous wireless networks[J]. Mobile Information Systems, 2020, 2020.

[21] 郭炜立. 基于区块链的异构物联网跨域认证研究[D]. 北京工业大学, 2020.
Guo L. Research on heterogeneous IOT cross-domain authentication based on blockchain[D]. Beijing University of Technology, 2020.

[22] Liu J, Liu Y, Lai Y, et al. Cross-heterogeneous Domain Authentication Scheme Based on Blockchain[J]. Journal of Artificial Intelligence and Technology, 2021, 1(2): 92-100.

[23] Yang Y, Wu J, Long C, et al. A Blockchain-based Cross-domain Authentication for Conditional Privacy Preserving in Vehicular Ad-hoc Network[C]//2021 The 3rd International Conference on Blockchain Technology. 2021: 183-188.

[24] 魏欣, 王心妍, 于卓, 等. 基于联盟链的物联网跨域认证[J]. 软件学报, 2021, 32(8): 2613-2628.
Wei X, Wang X, Yu Z, et al. Cross Domain Authentication for IoT Based on Consortium Blockchain. Journal of Software, 2021, 32(8): 2613-2628.

[25] Chen J, Zhan Z, He K, et al. XAuth: Efficient Privacy-preserving Cross-domain Authentication[J]. IEEE Transactions on Dependable and Secure Computing, 2021.

[26] Shen M, Liu H, Zhu L, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.

[27] Jia X, Hu N, Su S, et al. IRBA: an identity-based cross-domain authentication scheme for the internet of things[J]. Electronics, 2020, 9(4): 634.

[28] 王弘洁. 智慧医疗场景下基于联盟区块链的跨域身份认证[D]. 南京邮电大学, 2021.
Wang H. Research on Cross-domain Identity Authen- tication Scheme Based on the Consortium Blockchain in the Wise Medical Scenario[D]. Nanjing University of Posts and Telecommunications, 2021.

[29] 魏松杰,李莎莎,王佳贺.基于身份密码系统和区块链的跨域认证协议[J].计算机学报,2021,44(05):908-920.
Wei S, Li S, Wang J. A Cross-Domain Authentication Protocol by Identity-Based Cryptography on Consortium Blockchain. Chinese Journal of Computers, 2021, 44(05): 908-920.

[30] Xu R, Chen Y, Blasch E, et al. Blendcac: A blockchain-enabled decentralized capability-based access control for iots[C]//2018 IEEE International Conference on Internet of

Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, Jul 30 – Aug 03, 2018. Piscataway, NJ: IEEE, 2018: 1027-1034.

[31] 王思源. 融合区块链和权能的物联网跨域访问控制机制研究与实现[D].北京邮电大学,2021.
Wang S. Research and implementation of a cross-domain access control mechanism of Internet of Things with blockchain and capabilities[D]. Beijing University of Posts and Teleconmmunications, 2021.

[32] Li C, Li F, Yin L, et al. A Blockchain-Based IoT Cross-Domain Delegation Access Control Method[J]. Security and Communication Networks, 2021, 2021.

[33] Zhang Y, Luo Y, Chen X, et al. A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT[J]. Security and Communication Networks, 2022, 2022.

[34] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology: Proceedings of CRYPTO 84, California, USA, Aug 19-22, 1984. Berlin, Heidelberg: Springer, 1985: 47-53.

[35] Tara M.. What Are Layers Of Blockchain? Full Guide To Blockchain Architecture[EB/OL]. 2022[2022.10.11]. https://www.cryptologi.st/news/blockchain-layers-the-layered-structure-of-the-blockchain-architecture.

[36] Kamya Pandey. Understanding the basics of a blockchain is the building “block” of success in the crypto space.[EB/OL]. 2022[2022.10.11]. https://www.jumpstartmag.com/what-are-the-different-layers-of-blockchain-technology/.

[37] Shardeum Content Team. What are Blockchain Layers and How Do They Work?[EB/OL]. 2022[2022.12.11]. https://shardeum.org/blog/what-are-blockchain-layers/.

[38] Yaga D, Mell P, Roby N, et al. Blockchain technology overview[J]. arXiv preprint arXiv:1906.11078, 2019.

[39] Tong W, Dong X, Shen Y, et al. A hierarchical sharding protocol for multi-domain iot blockchains[C]//ICC 2019-2019 IEEE International Conference on Communi- cations (ICC), Shanghai, China, May 20-24, 2019. Piscataway, NJ: IEEE, 2019: 1-6.

[40] Li D, Yu J, Gao X, et al. Research on Multidomain Authentication of IoT Based on Cross-Chain Technology[J]. Security and Communication Networks, 2020, 2020(10):1-12.

[41] Zhang S, Cao Y, Ning Z, et al. A heterogeneous IOT node authentication scheme based on hybrid blockchain and trust value[J]. KSII Transactions on Internet and Information Systems (TIIS), 2020, 14(9): 3615-3638.

[42] Jia X, Hu N, Yin S, et al. A2 chain: a blockchain-based decentralized authentication scheme for 5G-enabled IoT[J]. Mobile Information Systems, 2020, 2020.

[43] Li D, Yu J, Gao X, et al. Research on multidomain authentication of IoT based on cross-chain technology[J]. Security and Communication Networks, 2020, 2020.

[44] Ali G, Ahmad N, Cao Y, et al. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things[J]. IEEE Access, 2020, 8: 58800-58816.

[45] 张亚兵,邢镔.基于多层区块链的跨域认证方案[J].计算机应用研究,2021,38(06):1637-1641.
Zhang Y, Xing B. Cross domain authentication scheme based on multi layer blockchain[J]. Application Research of Computers, 2021,38(06):1637-1641.

[46] Alsaeed N, Nadeem F. A Framework for Blockchain and Fogging-based Efficient Authentication in Internet of Things[C]//2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, Jan 25-27, 2022. Piscataway, NJ: IEEE, 2022: 409-417.

[47] 赵平,王赜,李芳, 等.主从区块链容错异构跨域身份认证方案[J/OL].计算机工程与应用:1-12[2022-04-12].
Zhao P, Wang Z, Li F, et al. Master-slave Blockchain Fault-tolerant Heterogeneous Cross-domain Identity Au-thentication Scheme[J/OL]. Computer Engineering and Application:1-12[2022-04-12].

[48] Zhang Z, Zhong C, Guo S, et al. A Master-Slave Chain Architecture Model for Cross-Domain Trusted and Authentication of Power Services[C]//Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, Shanghai, China, Dec 20-23, 2019. New York: ACM, 2019: 483-487.

[49] Cui Z, Fei X U E, Zhang S, et al. A hybrid block-chain-based identity authentication scheme for mul-ti-WSN[J]. IEEE Transactions on Services Com- puting, 2020, 13(2): 241-251.

[50] Dong S, Yang H, Yuan J, et al. Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT[C]//2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, Jun 15-19, 2020. Piscataway, NJ: IEEE, 2020: 1610-1612.

[51] 李大伟,霍瑛.基于侧链技术的电力物联网跨域认证研究[J].电力工程技术,2020,39(06):8-12.
Li D, Huo Y. Cross domain authentication of power IoT based on side chain[J]. Electric Power Engineering Technology, 2020,39(06):8-12.

[52] Liu B, Yu K, Feng C, et al. Cross-domain authentication for 5G-enabled UAVs: a blockchain approach[C]// Proceedings of the 4th ACM MobiCom Work-shop on Drone Assisted Wireless Communications for 5G and Beyond, New Orleans, US, Oct 25-29 ,2021. New York: ACM, 2021: 25-30.

[53] Wang X, Garg S, Lin H, et al. Enabling secure authentication in industrial iot with transfer learning empowered blockchain[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7725-7733.

[54] Xue L, Huang H, Xiao F, et al. A Cross-domain Authentication Scheme Based on Cooperative Block- chains Functioning with Revocation for Medical Consortiums[J]. IEEE Transactions on Network and Service Management, 2022.

[55] Yao Y, Chang X, Mišić J, et al. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.

[56] Huang C, Xue L, Liu D, et al. Blockchain-assisted Transparent Cross-domain Authorization and Authentication for Smart City[J]. IEEE Internet of Things Journal, 2022.

[57] Fu C, Kezmane T, Du X, et al. An location-aware authentication scheme for cross-domain internet of thing systems[C]//2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, Mar 05-08, 2018. Piscataway, NJ: IEEE, 2018: 452-456.

[58] Guo S, Hu X, Guo S, et al. Blockchain meets edge computing: A distributed and trusted authentication system[J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 1972-1983.

[59] Zhang K, Zhu Y, Maharjan S, et al. Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things[J]. IEEE network, 2019, 33(5): 12-19.

[60] 董贵山, 陈宇翔, 李洪伟, 等. 异构环境中基于区块链的跨域认证可信度研究[J]. 通信技术, 2019, 52(6): 1450-1460.
DONG G, CHEN Y, LI H, et al. Cross-domain Authentication Credibility based on Blockchain in Heterogeneous Environment[J]. Communications Technology, 2019, 52(6):1450-1460.

[61] Xiao X, Guo F, Hecker A. A Lightweight Cross-Domain Proximity-Based Authentication Method for IoT Based on IOTA[C]//2020 IEEE Globecom Workshops (GC Wkshps. IEEE, 2020: 1-6.

[62] Tan L, Shi N, Yu K, et al. A blockchain-empowered access control framework for smart devices in green Internet of things[J]. ACM Transactions on Internet Technology (TOIT), 2021, 21(3): 1-20.

[63] Xuan S, Xiao H, Man D, et al. A Cross-Domain Authentication Optimization Scheme between Heterogeneous IoT Applications[J]. Wireless Commu- nications and Mobile Computing, 2021, 2021.

[64] Hongmei Z. A cross-border E-commerce approach based on blockchain technology[J]. Mobile Information Systems, 2021, 2021.

[65] Wang L, Tian Y, Zhang D. Toward Cross-Domain Dynamic Accumulator Authentication Based on Block- chain in Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2858-2867.

[66] Jordi P. Distributed access control with blockchain[J]. CoRR, abs/1901.03568, 2019.

[67] Sun S, Chen S, Du R. Trusted and efficient cross-domain access control system based on blockchain[J]. Scientific Programming, 2020, 2020.

霍炜（1971—），男，河南省,博士研究生，主要研究方向为密码安全、物联网安全等。

HUO Wei, born in 1971, Ph.D.. His research interests include cryptographic security, IoT security, etc.

张琼露（1987—），女，河南省,博士研究生，高级工程师，主要研究方向为物联网安全、区块链等。

ZHANG Qionglu, born in 1987, Ph.D., associate professor. Her research interests include IoT security, blockchain, etc.

欧崴（1978—），男，湖南省,博士研究生，副教授，主要研究方向为物联网安全、类脑计算应用等。

OU Wei, born in 1978, Ph.D., associate professor. His research interests include IoT security, brain-like computing, etc.

韩文报（1963—），男，河北省,博士研究生，教授，主要研究方向为密码学、类脑计算等。

HAN Wenbao, born in 1963, Ph.D., professor, Ph.D. supervisor. His research interests include cryptography, brain-like computing, etc.