计算机科学
COMPUTER SCIENCE

基于区块链技术的身份认证研究综述

张淑娥，田成伟，李保罡

引用本文

张淑娥，田成伟，李保罡.基于区块链技术的身份认证研究综述[J]．计算机科学, 2023, 50(5): 329-347.

ZHANG Shue, TIAN Chengwei, LI Baogang. Review of Identity Authentication Research Based on Blockchain Technology [J]. Computer Science, 2023, 50(5): 329-347.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220400169

基于区块链技术的身份认证研究综述

张淑娥　田成伟　李保罡
华北电力大学电子与通信工程系　河北 保定 071003
河北省电力物联网技术重点实验室　河北 保定 071003
(zhangshue@ncepu.edu.cn)

摘　要　区块链技术由中本聪于2008年的白皮书中提出。作为点对点网络中的一种去中心化和分布式公共账本技术,区块链应用链接块结构来验证和存储数据,用可信共识机制来同步数据变化,为身份认证的实现提供了一种可信的技术方案。与传统集中式认证方式相比,基于区块链技术的身份认证可以在保护数据真实可靠、节点隐私安全的同时实现数据共享。文中概述了基于区块链技术的身份认证研究现状及进展。首先,从区块链的技术架构、分类以及共识算法系统地介绍了区块链的一些基本理论;然后重点介绍了口令认证技术、生物识别技术、PKI技术以及其结合区块链应用的身份认证目前的研究现状;接着从物联网、车联网、智能电网、金融、医疗等应用方面介绍了基于区块链的身份认证技术的研究进展;最后分析了区块链身份认证技术目前存在的问题,并展望了未来的发展趋势。

关键词:区块链;身份认证;隐私安全;数据保护;访问控制
中图法分类号　TP309

Review of Identity Authentication Research Based on Blockchain Technology

ZHANG Shue,TIAN Chengwei and LI Baogang
Department of Electronic and Communication Engineering,North China Electric Power University,Baoding,Hebei 071003,China
Hebei Key Laboratory of Power Internet of Things Technology,Baoding,Hebei 071003,China

Abstract　Blockchain technology was proposed by Nakamoto in his 2008 white paper. As a decentralized and distributed public ledger technology in point-to-point networks,blockchain verifies and stores data by applying link block structure,and synchronizes data changes by applying trusted consensus mechanism,providing a trusted technical solution for the realization of identity authentication. Compared with traditional centralized authentication,identity authentication based on blockchain technology can realize data sharing while protecting the authenticity and reliability of data and the privacy and security of nodes. This paper summarizes the status and progress of identity authentication based on blockchain technology. Firstly,it systematically introduces some basic theories of blockchain from the technical architecture,classification and consensus algorithm of blockchain. Next,it focuses on password authentication technology,biometric technology,PKI technology and the current research status of identity authentication combined with blockchain application. Then it introduces the research progress of identity authentication technology based on blockchain from the application fields of Internet of things,Internet of vehicles,smart grid,finance,medical treatment and so on. Finally,it analyzes the current problems of blockchain identity authentication technology,and puts forward the future development trend.

Keywords　Blockchain,Identity authentication,Security of privacy,Data protection,Access control

1　引言

随着信息通信技术的快速发展,万物互联、6G、隐私计算等的不断研究与应用,云计算、物联网、大数据给社会带来了巨大的好处,同时,其中的安全性、隐私却逐渐成为目前网络发展中最关键和最具挑战性的问题。近年来,关于数据隐私

到稿日期:2022-04-17　返修日期:2022-09-03
基金项目:国家自然科学基金(61971190);河北省自然科学基金(F2022502020);中央高校基本科研业务费专项资金(2019MS089);河北省高等学校科学技术研究重点项目(ZD2021406);河北省省级科技计划(SZX2020034)
This work was supported by the National Natural Science Foundation of China(61971190),Natural Science Foundation of Hebei Province,China(F2022502020),Fundamental Research Funds for the Central Universities(2019MS089),Technology Research in Colleges and Universities of Hebei Province(ZD2021406) and S&T Program of Hebei(SZX2020034).
通信作者:李保罡(baogangli@ncepu.edu.cn)

泄露的例子屡见不鲜，表1列出了一些隐私泄露的案例。

为了安全地传递敏感数据，身份认证是关键。身份认证可帮助网络过滤非法用户并有效防止用户被欺骗，因为身份认证过程会识别他或她声称的用户身份。随着移动边缘设备的疯狂增长，无论是移动边缘设备之间的信息交互，还是移动边缘设备和人的协作体系，都迫切需要构建身份认证体系，以达到保护隐私安全的目的。因此，设计新颖的身份认证方案非常重要[1]。

表1 隐私泄露案例

Table 1 Privacy disclosure cases

序号	时间	事件	影响	原因
1	2018年10月	Facebook严重漏洞	2900万用户数据失窃	黑客入侵
2	2018年12月	美国问答网站Quora遭攻击	约1亿用户信息被泄露	恶意第三方访问了该公司计算机系统
3	2019年5月	Canva数据泄露	1.39亿用户数据被窃取	黑客窃取
4	2019年10月	Zynga数据泄露	2.18亿游戏玩家数据被泄露	黑客入侵
5	2020年2月	雅诗兰黛记录泄露	超4.4亿内部记录曝光	数据库未加密，中间件故障
6	2020年3月	CAM4泄露	7TB数据被泄露，近110亿条记录被公开	服务器未受保护
7	2021年1月	MeetMindful遭受攻击	228万会员身份信息被公开	黑客入侵
8	2021年5月	Android遭受攻击	超1亿用户的个人信息被泄露	黑客入侵，服务器配置出错

区块链诞生于2008年中本聪发表的一篇名为《比特币：一种点对点式的电子现金系统》的论文中，经过十几年的发展，其以分布式存储、数据不易篡改、可追溯性和匿名性等优势，提供分布、透明和安全的系统，在众多领域均有突出贡献。区块链是一种分布式账本技术，其使用加密技术，将交易记录存放在由哈希相互连接的区块之中，可维护交易账本并保护它[2]。

区块链的安全与信任机制，使得区块链与隐私保护可以完美结合，能够有效管理数据透明度和访问权限。加密货币是区块链系统在安全交易过程中为增加匿名性的激励，且能够防止攻击，如拒绝服务(Denial of Service，DoS)和女巫攻击。分布式散列算法用于加密数据，并通过智能合约确保可用性和可扩展性。区块链解决了在没有第三方干预的情况下控制个人和敏感数据的问题，以及基于原始数据的计算和分析，但不披露它。将区块链应用于身份认证系统，可以有效解决身份认证和操作授权问题。利用区块链来确认用户的合法身份信息，可以达到保护信息安全、防止隐私泄露的目的。

在区块链系统中，任何参与者都可以记账，同样也可以对账本进行检查，每一个参与者都严格按照规则和共识来共同维护账本的更新。由于区块链具有去中心化、不可篡改、可追溯性等优点，因此研究者们将它应用于身份认证领域。然而目前，对这些研究缺乏系统性的梳理工作。Makhdoom综述了区块链技术在信息安全领域的研究进展，包括认证技术、访问控制技术、数据保护技术，但对身份认证并未进行过多系统性的描述。Makhdoom等[4]的工作也只是针对区块链在物联网方面的应用及关键问题进行了介绍。Liu等[5]的工作是对基于区块链的身份管理系统进行介绍，但未对身份认证进行说明。与身份认证最相关的一篇综述是由Li等[6]发表的，该文章从区块链系统节点认证机制、用户身份认证机制、用户权限管理机制3个方面，系统地阐述了区块链系统认证机制的研究现状与发展趋势，但是该文所涉及的区块链应用场景较少，没有对这些应用研究进行分类总结，也未提及未来的研究方向。本文对近几年基于区块链的身份认证关键技术进行了梳理，从生物识别、口令认证、密钥认证3方面介绍了基于区块链的身份认证的最新研究进展，同时针对多个应用领域进行了详细介绍，并系统性地分析了当前基于区块链技术的身份认证面临的问题及未来的研究方向。

本文第2节对区块链背景知识进行介绍；第3、第4、第5节分别从口令认证、公钥基础设施(Public Key Infrastructure，PKI)认证以及生物识别方面介绍了基于区块链的身份认证研究的最新进展；第6节对其应用领域进行了具体介绍；第7节对未来研究方向进行了展望；最后总结全文。

2 区块链技术概述

本节从区块链的架构、分类和共识算法3个方面介绍区块链的有关知识。

2.1 区块链架构

区块链系统是一个分布式系统，主要由6层组成，分别为数据层、网络层、共识层、合同层、服务层和应用层。数据层和网络层主要用于数据收集、验证和操作。共识层和合约层主要包括共识协议、智能合约、脚本代码和激励机制。服务层和应用层主要是将基于区块链的活动付诸实践[7]。图1为区块链系统架构图，简要展示了与6层相关的组件或技术。

根据架构，区块链包括3个核心元素：基于时间戳的链块结构、基于点对点(Peer To Peer，P2P)网络的分布式存储机制以及基于去中心化节点的共识机制。

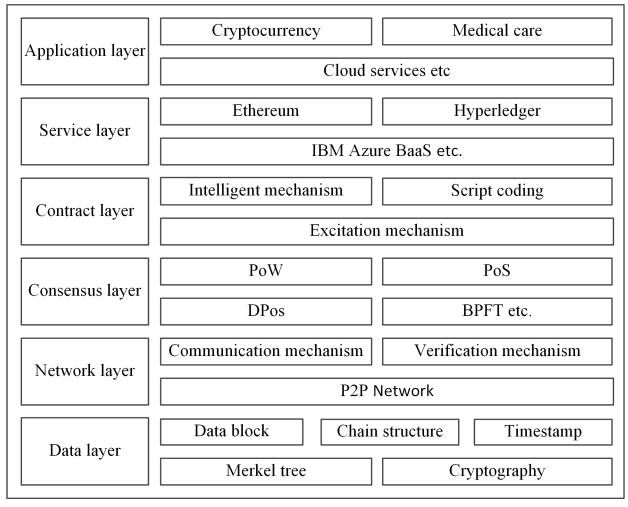

图1 区块链系统架构图

Fig. 1 Blockchain system architecture

2.2 区块链分类

目前,区块链主要分为3类:公有区块链、私有区块链和联盟区块链。表2根据去中心化程度、参与者、记账者、优缺点、使用场景总结了3种区块链模式的对比情况。

公共区块链对任何用户、任何网络节点都授予访问权限,所有人都可以在上面进行交易、读写等操作。公有区块链是完全分布式的,数据公开,用户参与度高,便于推广,但是系统运行依赖奖励机制,如比特币、以太坊。

私有区块链只对特定的用户授予访问权限,应用场景一般是企业或公司内部,如银行业、政府部门等。他们正在寻求将私有区块链作为自己的数据交换平台。

联盟区块链会限制外部用户,只允许经过审核的联盟内部成员参与。联盟区块链上的读写权限、参与记账权限按联盟规则来制定。整个网络由成员机构共同维护,网络接入一般通过成员机构的网关节点接入,共识过程由预先选好的节点控制。

表2 区块链模式对比

Table 2 Comparison of blockchain modes

	去中心化程度	参与者	记账者	优点	不足	使用场景
公有区块链	去中心化	任何人	所有参与者	安全性极强,参与难度低	吞吐量低,算力大	节点之间互相不信任
私有区块链	相对中心化	指定的可参与成员	内部拟定	吞吐量高	系统封闭,安全性低	节点之间高度信任
联盟区块链	多中心化	经过审核准入的成员	成员选举	易于权限控制,扩展性高	节点数量受限	公司或者组织

2.3 共识算法

在区块链中,如何在不可信节点之间达成共识是拜占庭将军问题的关键。拜占庭将军问题,指一群指挥拜占庭军队的将军环绕着这座城市,一些将军更喜欢进攻,而其他将军更喜欢撤退。然而,如果只有部分将军攻击城市,攻击就会失败。因此,他们必须达成攻击或撤退的协议[8]。同样,如何在分布式环境中达成共识也是一项挑战。

共识算法是一种技术,区块链的所有对等体都通过这种技术网络就分布式账本的当前状态达成了共同的协议。因此,共识算法在未知对等体之间提供信任和可靠性。分布式环境、共识机制确保每个新区块都被添加到区块链是所有区块链节点都同意的唯一真理[9]。常见的共识算法有工作量证明算法、权重证明算法、股份授权证明算法、权益证明算法以及拜占庭容错算法等。

3 基于区块链技术的口令认证研究

口令认证一般分为两种,静态口令和动态口令。口令的运用方式是:通常需要先注册一个用户账号,且认证者在数据库中必须是唯一的,认证的口令就是根据用户设置的字符串组合或者计算机自动生成的不可预测的随机数字组合。口令认证相对于其他的认证方式而言更方便,只需要一个名称和口令,就可以从任何地方进行连接,而不需要附加的硬件和软件知识[10]。

3.1 口令认证技术现状

(1)静态口令

静态口令是过去常用的方式,它的原理为系统有一个认证服务器。服务器提前保存每一个用户的一组信息,即用户名和密码。当用户要求访问系统时,用户在客户机或终端上输入用户名和密码,系统将用户输入的用户名和密码与认证服务器内保存的合法用户的用户名和密码信息对进行匹配,若匹配成功,则证明该用户为合法用户,允许用户访问系统资源,反之用户身份没有通过验证,系统拒绝用户登录和访问。静态口令的优点是使用方便,操作简单,成本低,运行速度快,但也有诸多安全隐患,例如未经授权的入侵者可以轻易访问静态密码,被破解、被遗忘、被窃听的可能性很高。

(2)动态口令

动态口令是为处理静态口令可能出现的安全隐患而产生的。动态口令亦被称为一次性口令,采用一次性使用口令的方法,用户每次使用动态口令牌生成动态密码,因为只有合法用户才能使用动态令牌,所以认证服务器可以通过验证密码来认证用户,保证了用户身份的安全。

动态口令不但兼顾了静态口令成本低廉、认证便捷、响应迅速等优点,更重要的是增强了口令的安全性。动态口令因其简单、不易破解、不可复用、高效、低廉等特点而被广泛应用于各种认证机制中。

虽然目前动态口令已经被广泛应用在各行各业,也受到广大用户的喜爱,但这并不意味着现有的动态口令认证方式是无懈可击的。目前所提出的动态口令方案虽然已经避免了口令重复使用的缺陷,但仍有不足之处需要改进。因此,发展和完善动态口令方案,给予用户安全性能更高的动态口令认证方式刻不容缓。通过分析可以发现,目前存在的动态口令方案大多是在由Lamport[11]提出的一次性口令(One-Time Password,OTP)方案的基础上进行改进的。OTP是一种仅使用一次有效的密码类型(使用一次并扔掉它们),用于对用户进行身份认证,主要作为进行在线交易的确认。此类密码在注册账户时生成一次。虽然它不能取代传统的密码身份认证,但它为静态身份认证增加了一层安全性和随机性[12]。

目前存在的动态口令方案大多忽略了一个严重的安全性问题:动态口令的有效时间问题。现有的动态口令虽然一次一变,具有不可重复利用的优点,但是在用户使用下一个动态口令之前,该动态口令一直有效。正常情况下,用户两次登录会有一定的时间间隔,假设攻击者在偷窥到若干个动态口令的基础上推测或者利用其他的方式知道了下一次登录的动态口令,那么攻击者只要在用户下一次登录之前假扮用户,就可以攻击成功。因此,限制每个动态口令的有效时间也是非常有必要的。目前,如何在满足认证次数不受限制的基础上,同时支持离线认证,保持口令具有时效性,从而进一步提高口令的安全性还没有一个行之有效的解决方案[13]。

3.2 基于区块链的口令身份认证研究

动态口令认证凭借其安全、低成本的优点,逐渐成为口令认证的主流技术,被广泛应用于信息安全领域。区块链通过

数据加密、时间戳和共识机制，在没有可信权限的情况下，在一组互不信任的节点之间实现了分布的信任机制。将 OPT 应用于区块链身份认证，可在两个不熟悉的实体之间建立信任，满足新兴技术对认证的更高安全要求。

Zhang 等[14]提出了一种基于区块链的 OTP 身份认证方法，其中区块链充当 OTP 验证器和身份提供者，避免了集中式身份认证方法存在的问题，并确保 OTP 承诺值（用于验证 OTP 令牌）不能被篡改。在整个身份认证协议中，区块链充当 OTP 验证器，并代表多个服务提供商对用户进行身份认证。服务提供商不需要参与注册阶段，只需要将 OTP 令牌（即客户端发送的一次性密码）转发到区块链，并在身份认证阶段接受区块链的身份认证结果即可。这无疑减轻了服务提供商部署身份认证解决方案的负担，并使用户能够访问具有相同身份的多个服务。

Zhang 等提出的架构如图 2 所示，包含 3 个组件。

（1）服务提供者：主要负责向用户提供服务。服务提供商不需要参与注册阶段，只需要将 OTP 令牌从客户端转发到区块链，并在身份认证阶段接收来自区块链的身份认证结果。

（2）客户端：主要负责生成 OTP 令牌并为用户提供接口，以访问服务提供商提供的服务。

（3）区块链网络：主要负责用户身份的注册和验证，部署 4 个智能合约进行注册、认证、同步和审计。

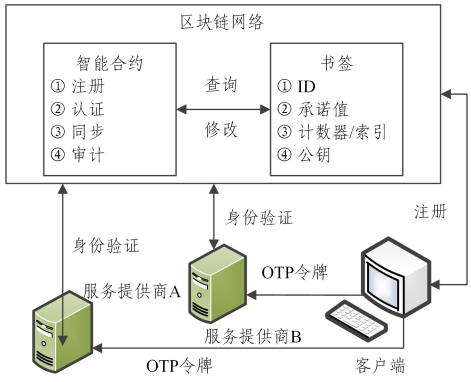

图 2 基于区块链的 OTP 身份认证系统架构图

Fig. 2 Architecture of OTP identity authentication system based on blockchain

注册时，客户端调用区块链上的智能合约进行注册，将客户端发送的 OTP 承诺值写入账本。当用户想要访问服务提供商 A 提供的服务时，客户端生成一个 OTP 令牌（包括用于验证的一次性密码和用于下一次身份认证的新承诺值）发送给服务提供商 A；服务提供商 A 与区块链网络交互，并通过调用智能合约中的认证对用户进行身份认证。若身份认证成功，则原始承诺值将被替换为新承诺值，这意味着客户端始终为每个身份认证发送不同的 OTP 令牌。此时，如果客户端想要访问服务提供商 B，它将重新生成新的 OTP 令牌以完成身份认证过程。用户可以通过调用智能合约中的审计来查询自己的登录日志，快速检测异常登录行为。

基于区块链的 OTP 身份认证系统使用哈希算法以及签名算法完成密钥的加密与解密。首先进行用户注册，注册时，用户提交自己的注册信息，系统根据用户注册信息通过哈希迭代将注册信息中的静态口令生成 OTP 令牌，OTP 令牌可分为用于验证的一次性密码和用于下一次验证的新承诺值，无论身份验证是否成功，索引的值都将增加，因为一旦生成 OTP 令牌并将其发送到服务器，它就已经在区块链网络中生成了记录。然后通过密码散列函数和生成算法在给定安全参数的情况下生成私钥及其对应的公钥，并使用签名算法将私钥生成消息的签名。签名可确保 OTP 令牌的真实性和完整性，从而防止恶意服务提供商篡改 OTP 令牌。随后，服务器将签名转发到区块链网络，区块链各个节点检查与其通信的服务器是否与 OTP 令牌中的服务器一致，然后，将签名通过公钥以及哈希变换进行解密以及身份验证，如果身份验证成功，智能合约将会更新下一次验证的索引值，并返回给服务器。

消息队列遥测传输（Message Queuing Telemetry Transport，MQTT）协议是设备间通信广泛采用的协议之一，其需要使用消息代理来实现发布-订阅模式。代理互连一组客户端，扮演发布者和/或订阅者的角色。在物联网领域，根据（International Organization for Standardization，ISO）参考架构，发布者通常是传感设备，而订阅者是执行器。由于 MQTT 不包含安全功能，因此在 MQTT 规范中，对开发人员的安全性要求很高，这就增加了实施不善的风险。Buccafurri 等[15]提出了一种新颖的 OTP 认证模式，用于消息队列遥测传输协议。此协议可以实现开发人员要求的本机安全身份认证机制。该模式使用以太坊区块链来实现第二因素带外通道，允许对本地和远程设备进行身份认证，从而保护用户隐私，并通过以太坊智能合约保证信任和问责制。类似的，Jayan 等[16]提出了一种使用 OTP 进行 MQTT 的认证方案，他们建议对交换的消息进行加密。但这种方法仍需要额外的工作，类似于采用 TLS 协议。

Erdem 等[17]提出了一次性密码即服务（One-time Password as a Service，OTPaaS），这是一种基于云的 OTP 架构，用于可靠的用户身份认证。OTPaaS 在对云服务进行身份认证的过程中建立 OTP 提供商，并执行云用户注册、服务提供商激活和身份认证。OTPaaS 可以防御外部人员的攻击，用户可断开连接属性以及指定环境中 OTP 验证器的攻击。Elbooz 等[18]提出了一种云存储系统，该系统结合了基于时间的一次性密码（Time-based One-Time Password，TOTP）和自动拦截器协议（Automatic Blocker Protocol，ABP）。该系统由以下 3 部分组成：1）完全控制云的组织经理；2）第三方审计员（Third-Party Auditor，TPA），其可以应管理员的请求审计云中存储的数据；3）存储数据的云服务提供商（Cloud Service Provider，CSP）。TOTP 对用户进行身份认证，数据通信过程由用户和云存储之间的 TPA 审核。如果出现问题，将通过 ABP 阻止访问。

Lai 等[19]采用聚合消息身份认证代码和 OPT，提出了一种基于区块链的安全组移动性管理方案，该方案支持一组车辆的安全切换。该计划可分为 3 个阶段：注册阶段、初始化阶段和移交阶段。在注册阶段和初始化阶段，每辆车和车队都与防御恶意移动锚点和访问路由器相互认证；此外，双方还就会议钥匙进行了谈判。在移交阶段，采用区块链和 OTP

技术，以确保顺利移交，满足了相互认证、会话密钥保密、重放攻击、女巫攻击等重要安全要求，降低了身份认证期间的切换延迟和信令成本。

4 基于区块链的 PKI 身份认证研究

在当今网络时代，数字身份分布于各个网络设备及终端设备之中，用于在网络中对各个软硬件进行身份认证。基于公钥密码学的 PKI 技术是一种常见的用于数字身份认证的解决方案。其以公开密钥理论为基础，使用公钥加密、数字签名以及数字证书等技术，以实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能，以及验证证书持有者的身份和确保网络信息传输的安全性。PKI 技术主要用于身份认证、数字签名、密钥协商等安全问题，现有研究将其与区块链结合，对网络节点进行数字身份认证，防止交易数据被篡改。

4.1 PKI 身份认证现状

公钥基础设施是许多应用程序依赖的安全可靠的身份认证，如数字电子邮件、智能卡和网络连接。传统的 PKI 身份认证体系主要由 6 个部分组成，即用户、公钥加密技术、数字证书、证书颁发机构(Certificate Authority，CA)、注册机构(Registration Authority，RA)以及验证机构(Verification Authority，VA)。其中用户是 PKI 的使用者，指向认证中心申请数字证书的客户，可以是个人，也可以是团体机构等；公钥机密技术用于实现网络通信安全；数字证书主要用于验证用户的身份；CA 是一个权威、可信且公正的第三方机构，主要负责验证用户申请信息的可信性，包括创建、颁布、撤销证书以及更新证书撤销清单等证书的管理工作；RA 主要用于接受用户的请求。RA 提供用户和 CA 之间的一个接口，主要用来获取并认证用户的身份，向 CA 提出证书请求，收集用户信息和确认用户身份；VA 用于管理证书撤销清单(Certificate Revocation List，CRL)并提供查询下载 CRL 的服务。

如图 3 所示，传统 PKI 身份认证的主要流程如下：1)PKI 用户首先创建私钥、公钥密钥对，然后再创建证书签名请求并提交给 RA，RA 对申请人身份进行验证；2)申请人身份认证通过后，RA 向 CA 请求颁发证书；3)CA 创建数字证书，并将数字证书发送给 PKI 用户；4)CA 定期向 VA 发送更新后的 CRL；5)PKI 用户用数字证书对传送的信息进行数字签名，并将数字证书和签名后的文件一起发送给接收方；6)信息接收方从 VA 下载 CRL，然后对接收到的数字证书进行验证；7)数字证书验证通过后，文件接收方用数字证书对数字签名进行验证。

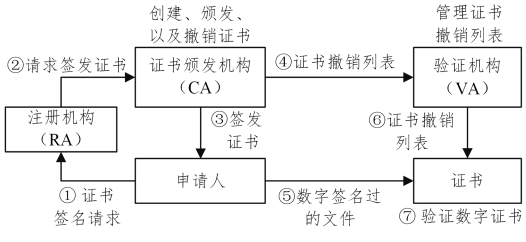

图 3 传统 PKI 身份认证流程

Fig. 3 Traditional PKI identity authentication process

但是，传统的 PKI 有诸多弊端，主要体现在以下 4 个方面：

(1)证书批量配置效率低。PKI 用户在配置和使用证书时，需要将证书颁发机构 CA 签发的证书配置到目标设备或者服务器中，在传统互联网应用中，一般采用人工的方式来配置，而在移动通信网、物联网等场景中，证书来源可能不同，数量巨大，导致证书配置效率低下。因此，如何快速、高效地实现证书批量配置成为了关键问题。

(2)多 CA 互信复杂。PKI 用户的证书只能由所属 CA 的根证书进行验证，不同 CA 之间的证书不能相互验证。

(3)内网设备无法使用证书撤销列表/在线证书状态协议(Certificate Revocation List / Online Certificate Status Protocol，CRL/OCSP)。CRL 和 OCSP 是发布撤销最常见的机制，在一些运营商网络和企业内网中，部分内网设备需要支持数字证书验证，需要连接互联网使用 CRL/OCSP 协议查询证书状态，由于这些内网设备不具备连接互联网的能力，故无法使用 CRL/OCSP。

(4)CRL/OCSP 单点故障。传统的 PKI 数字证书采用中心化结构，难以避免 CRL/OCSP 单点故障问题。一旦 CA 机构由于自身原因或遭受安全攻击等不能提供该服务，将影响使用相应 CA 机构数字证书的用户。

基于 PKI 的身份认证是目前较为成熟并得到普遍应用的传统云中心身份认证技术。但是此技术存在认证路径复杂、签名验证次数较多、证书管理困难等问题，不仅成本过高，而且还存在单点故障问题。区块链技术具有去中心化、透明度高、结构扁平等优点，将区块链技术应用在 PKI 体系中，有望从根本上解决上述问题，提高整个互联网建立信任关系的能力和效率[20]。

4.2 基于区块链 PKI 身份认证研究

4.2.1 基于区块链 PKI 身份认证研究概述

鉴于上述 PKI 的传统设计存在的安全漏洞，区块链技术及其衍生物的特性为 PKI 的传统设计问题提供了某些方面的解决方案，特别是证书的透明度和消除单点故障方面。如文献[21]和文献[22]中所述，区块链 3.0 中的许多功能可用于实现许多互联网用途的分布式应用程序。至于身份管理，其主要思想是生成一个系统，该系统可以存储和管理具有分布式分类账的所有优点的身份。为了实现这一目标，区块链相关的身份管理实现和信任网络(Web of Trust，WoT)共同享有共识协议。矿工或验证者(取决于所使用的区块链类型)和 WoT 上的老用户在创建区块时，验证并保护访问分类账的每个用户的身份存储。但是，在 WoT 中，所谓的共识是由用户执行的，而不是由网络本身执行的。因此，一组恶意用户可以通过充当伪 CA 来劫持网络并破坏网络的整个有效性[23-24]。相反，在区块链网络中，如果交易(创建或修改用户证书)是有效的，那么矿工或验证者就将区块添加到账本中，而无须修改交易的内部信息或与定义的共识算法之外的新区块进行交互。这意味着区块链不仅充当了分布的分类账，还充当了中立的分类账，用户可以不依赖于其他人的验证来创建或使用他们的证书。

此外，与 PKI 实现相比，区块链的安全功能还有一些额外的考虑，例如，透明度属性公开存储于区块链中的每笔

交易，为用户增加信任。换言之，每个证书都是公开的，可以在没有任何特殊访问或授权的情况下进行搜索和查看。此外，区块链的不可变性使得用户无法更改或修改已经存储的任何证书，这使基于区块链的 PKI 完全公开且完全不可变，即使是证书所有者也不例外。事实上，此属性可能会给传统公钥基础结构带来一些问题，导致需要吊销证书。在基于区块链的 PKI 中，每个存储的证书都是不可变的，这意味着每个存储的证书都不能被卸载、丢弃，所有者不能失去对它的访问权限。虽然证书不能从区块链中修改或删除，但智能合约的功能允许用户“替换”自己的证书或存储的信息，而不会影响以前存储的数据[25]。这意味着，当证书过时后，所有者可以通过创建具有与原始证书相同的信息的新证书来声明原始证书无效，该证书将存储在新块中，并且自创建之日起被视为唯一有效的证书。以前的证书永远不会被删除或更改，但新证书说明它是当前和未来事务的唯一有效证书。对于分布的 PKI，此功能消除了对 CRL 或者另一个相关系统的需求，这些系统可能被劫持或成为恶意用户[26]。事实上，区块链的不变性也提供了一种透明且始终可用的方式来记录 PKI 中进行的每笔交易。对于任何 PKI 来说，可审计性和问责制都是重要的考虑因素，区块链技术提供了一种自然的解决方案，它允许将所有功能从集中和不安全的环境迁移到新的分布环境中，其中整个系统的可靠性不依赖于一个权限或用户组，而是依赖于网络本身及其所有功能。

4.2.2 基于区块链 PKI 系统架构

图 4 是基于区块链的 PKI 身份认证总体架构图，主要可分为四大模块：基础层、核心层、接口层以及跨层功能。

(1)基础层：包括区块链节点和 P2P 网络。区块链节点提供系统所需的计算和存储资源，以及共识算法和智能合约所需的处理和执行环境；P2P 网络提供点到点之间的高效通信。

(2)核心层：主要包括证书管理以及查询。证书管理包括证书验证、证书更新、证书记录、证书变更；查询包括证书查询以及状态查询。

(3)接口层：主要包括证书管理和证书查询接口，提供证书发布及变更和证书状态查询等功能服务。

(4)跨层功能：主要提供与系统相关的运行管理、身份认证、授权管理以及日志审计等功能。运行管理包括对系统运行状态的检测、异常问题的处理及系统策略的管理等；身份认证是对用户身份进行验证的过程；授权管理是授权用户访问和使用资源的权限；日志审计通过收集和维护系统运行的相关日志，并对系统进行审计管理。

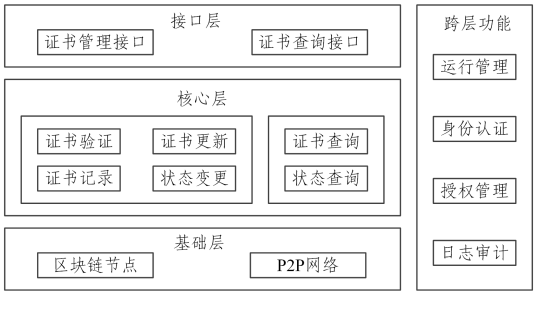

图 4 基于区块链的 PKI 身份认证总体架构图

Fig. 4 Overall architecture of PKI identity authentication based on blockchain

图 5 给出了基于区块链的 PKI 的证书管理系统，包含证书申请、证书发布、证书更新、证书撤销、证书使用以及证书查询，具体流程如下：

(1)证书申请：证书用户首先生成自签名证书，并向提交节点提交证书发布申请，然后提交节点对未发布的证书进行验证，包括证书内容验证和用户身份验证，验证通过后会向区块链系统发布证书发布申请，并在提交区块链系统时对发布申请进行签名保护。

(2)证书发布：基于区块链的 PKI 系统在收到证书发布申请后，验证节点会验证证书、内容格式、发布节点签名信息，通过验证后会在区块链记录下新提交的证书以及证书状态。

(3)证书更新：证书用户需要在证书到期之前通过提交节点发起证书更新申请，实时更新证书，以确保证书能连续使用，更新后的证书以及证书状态信息将被记录到区块链中。

(4)证书撤销：如若在认证过程中存在私钥等隐私泄露或其他不安全问题，则需证书用户或提交节点发起申请，向基于区块链的 PKI 系统发送证书撤销请求，立即撤销证书，并将区块链账本中的证书状态更新为撤销。

(5)证书使用：证书用户将证书摘要或完整的证书提交给依赖方，依赖方收到证书摘要或完整的证书后，向区块链证书查询节点查询证书以及证书的状态，保证其合法性。

(6)证书查询：任何能够访问基于区块链的 PKI 系统的设备都可以提供证书查询服务，查询节点收到查询请求后提供证书完整信息查询或证书状态查询。

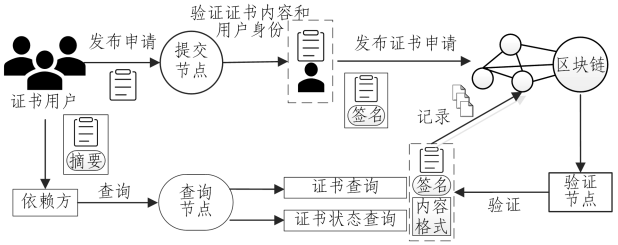

图 5 基于区块链的 PKI 的证书管理系统

Fig. 5 Certificate management system of PKI based on blockchain

4.2.3 基于区块链 PKI 身份认证研究内容

与传统 PKI 身份认证相比，基于区块链的 PKI 具有以下优势：首先，证书及其 CA 证书链的验证简单快捷；其次，基于区块链的 PKI 解决了传统 PKI 长期存在的问题，由于网络节点之间的区块链同步，不需要使用发布证书撤销列表的服务，其中对证书状态的任何修改都将立即通知给所有节点。下文将针对传统 PKI 弊端，介绍区块链应用于 PKI 的身份验证研究。

(1)证书批量配置效率低。针对此问题，可以利用区块链的智能合约及共识机制，实现数字身份的在线审核。证书用户可以先产生数字证书，由多个参与方共同对这些数字用户进行审核验证，验证通过之后才能记录到区块链中。将传统的先申请证书再配置证书的应用逻辑，改为先产生配置证书再发布证书。设备商在生产过程中制证，经区块链节点多方验证并达成共识之后发布，可有效提升证书批量配置的效率。

Shohei 等[27]提出的 Meta-PKI 通过建立证书颁发机构之间的信任关系，并根据对公钥证书的信任来计算分区，以统一

的方式在区块链之外构建认证路径,由区块链来保证认证路径的有效性,加快了证书配置的速度。但是该方法仅使用边缘连接状态来构建认证路径。由于交叉认证的限制和政策原因,一些公钥证书可能是无效的,同时,PKI 客户端的处理负载会很高,并且 PKI 客户端的约束和策略的管理可能很复杂。

同样地,为了提高证书配置效率,Yan 等[28]提出了一种基于区块链的 PKI 证书管理系统,在简化了证书提供和证书管理过程的同时,降低了部署和维护 CA 的成本。在此管理系统中,提交节点可以是 CA 的代表,并认可自签名证书的可信度。如果提交节点是供应商、服务提供商和运营商的代表,那么它们只能为自己组织的设备或实体提交证书。按照传统方式,供应商的委托向 RA 发送证书申请请求,请求包含公钥和设备的标识。RA 验证委托的身份,然后颁发证书。使用区块链解决方案,提交节点的是供应商、运营商或 CA 的代表,他们将认可设备的身份。自签名证书的主题归档中的组织信息应与提交节点的组织信息一致,一致性由验证程序节点进行验证。如果证书包含域名,则应验证域的所有者。按照传统方式,供应商的委托向 RA 发送证书注册请求,该请求包含证书中的公钥和域。RA 验证代理的身份,并验证域的所有者。仅当域由供应商拥有,或由所有者授权时,CA 才会颁发证书。通常,受信任的一方用于验证域的所有者。使用区块链解决方案,将引入相同的受信任方来验证域的所有者。证书中的组织信息、提交节点的组织以及域所有者的组织将由验证程序节点进行验证。

将基于区块链的 PKI 系统与传统解决方案进行实验对比,结果表明基于区块链的 PKI 证书管理系统能够有效提高证书配置和管理的效率。

(2)多 CA 互信复杂。区块链具有去中心化的特性,多个可信参与方共同形成联盟链,多个参与方共同对数字证书进行验证,将通过参与方验证的数字证书记录到区块链中,这些数字证书就可以被区块链中的所有参与方认可。在多 CA 之间建立联盟链,打通多信任域,通过对多 CA 证书全生命周期的记录管理,可实现跨域证书的快速查验,解决多 CA 互信复杂的问题。

Yakubov 等[29]提出了在车辆边缘计算和网络中安全高效地共享数据的区块链,用于解决多 CA 互信复杂。但为了保护车辆用户的身份隐私,需要经常与 CA 进行交互,以更新定期更新的假名的公钥证书。因此,繁重的计算成本和通信带宽要求不仅会损害高效内容交付,还会偏离资源受限车辆的轻量级特性。通过分析与特定区块链地址相关联的一系列可公开访问的历史交易数据,有极大可能可以成功地推断出区块链用户的真实 IP 地址。此外,由于采用伪随机字符串作为区块链用户地址,缺乏与其真实身份之间的关联性,因此无法在不知道其真实身份的情况下有效追踪不当行为来实现问责。

为了解决上述问题,Shen 等[30]在此基础上提出了一种用于联盟区块链的轻量级阈值 CA 和区块链强制车联网中的高效隐私保护基于位置的服务协议。在此方法中,通过设计阈值代理签名,只需为每个合法用户生成一次代理签名密钥,就可以每次在在线阶段生成更新的区块链地址自行进行身份认证,而无须涉及在线 CA。

Beckwith 等[31]提出了一种基于区块链的物联网认证机制来替代 PKI。随后,Saha 等[32]在物联网环境中介绍了一种基于联盟区块链的访问控制方案。在该方案中,终端客户端之间可以实现相互认证。为了解决证书透明度低的问题,Wang 等[33]在 PKI 系统中提出了一种基于区块链的解决方案,将全局证书区块链作为本地副本存放到浏览器中,并用于 web 服务器的证书验证。虽然该解决方案实现了证书透明性,但需要依赖于可信 CA 层次结构。

上述基于区块链的跨域认证虽然在一定程度上实现了不同信任域之间的可靠认证,然而,它们大多是针对分布式应用场景提出的,没有考虑特定的认证协议和认证效率。总而言之,缺乏安全有效的跨域身份验证协议。于是,Zhao 等[34]分析了跨域身份认证协议的设计要求,考虑了跨域节点的注册场景和跨域身份认证场景两种应用场景,提出了一种双层跨域身份认证模型,通过构建由认证服务器节点和部分内部区块链组成的联盟区块链,可以在不改变内部体系结构的情况下极大地提高 PKI 系统的可扩展性;通过将区块链证书的生成过程及其哈希的存储过程放在身份注册过程中,在保证安全性的前提下,解决了 CA 互信复杂的问题。

(3)内网设备无法使用 CRL/OCSP。由于区块链中节点可以访问所有区块数据,通过在网络边界部署区块链节点,可以获取区块链中的证书信息,提供证书状态查询服务,从而解决内网设备无法访问互联网 CRL/OCSP 服务器的问题。

在过去的几年中,一些研究者针对上述问题进行了研究。文献[35]给出了物联网和 PKI 区块链的框架,该框架适用于物联网的基于区块链的 PKI,其中的验证者必须在验证步骤中检查映射表。Simplicio 等[36]介绍了解决 CRL 扩展问题的步骤。旧的假名证书变得无用,以防止旧的被吊销车辆获得激活码,并从 CRL 中删除。但是,假名证书 ACPC 的激活码仍然需要使用集中式 SCMS 管理器来检查证书的有效性。

Cho 等[37]基于文献[35-36]的研究,通过对流程采用激活码来改进基于区块链的假名证书。基于 ACPC 以及通过区块链进行的假名管理,同时考虑了 PKI 初始化或更新证书的环境,并存储系统初始化数据/更新和撤销数据。与其他区块链应用程序类似,CRL 对所有隐私管理员可见。此外,PKI 保留了证书撤销列表。

之后,Yan 等[28]提出了基于区块链的移动网络 PKI 框架,通过分析基于区块链的 PKI 的系统与传统解决方式,解决了 CRL/OCSP 不可用、预置信任锚不可用、通信负载高等问题,证明了证书的可信度。

另外,传统 PKI 中的 CRL 存在列表发布时间长、存储开销大、交易并发量大导致效率降低的问题。针对以上问题,传统的解决方案有以下两种。1)将大 CRL 划分为多个可控片段,通过多个 CRL 发布一个 CA 的证书注销信息。在证书的扩展中,设置 CRL 分发点子项,标记 CRL 分发点的位置,引导用户根据参数访问对应的 CRL。2)通过设置 LDAP(Lightweight Directory Access Protocol)镜像服务器来降低并发访问的压力。

而基于区块链的 PKI 身份认证系统将 CRL 保存在区块

链中，检索效率并不会因为区块链的递增而降低，相反会大大提高证书验证和检索的效率。这是由于区块链账本只储存了证书的哈希值，而没有储存明文信息，因此相比传统的 CRL 更节省空间。在查询证书是否被撤销时，区块链账本不会返回特定的明文，而是返回有效或无效的信息。发起者只需要构造已撤销证书的数据结构，通过区块链任意节点查询证书的有效性，以获得构造信息是否有效的返回值。由于基于区块链的 PKI 的 CRL 发布周期短、规模小，优于传统 CRL，没有过多的列表空间，同时其使用原始的 OCSP 协议补偿证书的实时明文状态，因此更能提高证书的检索及身份认证效率。

(4)单点故障。由于区块链不依赖中心化第三方，区块链中的数据以分布式的方式存储于多个节点之中，破坏任意节点均不会导致区块链数据丢失，因此，在区块链基础上构建 PKI 系统，将数字证书及其状态信息记录到区块链中，通过自身分布式节点进行数字证书的存储、验证、传递和使用，可以有效避免传统 PKI 体系的 CRL/OCSP 单点故障问题。

在 PKI 系统中，核心 CA 容易受到攻击。一旦被控制，CA 根证书和 CA 颁发的证书不再受信任。Matsumoto 等[38]使用以太坊智能合约作为谷歌透明证书的替代品来监控和处理 CA 的不当行为。Leiding 等[39]提出用 Authcoin 作为基于 CA 的 PKI 和信任网络的替代方案，Authcoin 结合了针对域、证书、电子邮件账户和公钥的基于质询-响应的验证和身份验证过程。然而，这些方法没有考虑物联网设备环境中的区块链技术，也没有提供与 SSL/TLS 库集成的具体实现。

Won 等[40]建议使用 Emercoin NVS 来代替传统的基于 CA 的 PKI 系统。但将区块链用于键值对存储，当需要将更复杂的属性(如访问控制策略或设备功能)存储在区块链上时，就会受到限制。Singla 等[41]的工作是对部署在物联网设备上的不同区块链技术的证书验证时间进行基准测试，并利用以太坊区块链提供的智能合约功能解决了这一限制。

Qin 等[42]提出了一种分布式证书方案，将证书视作货币，并记录到区块链上，从而消除了单点故障问题。矿工们可以验证有效的证书，遵循一系列的规则，以确保所有权的一致性，并允许身份绑定多个公共密钥证书。为了有效地检索和验证证书并快速操作，引入了修改后的梅克尔树，并用它来实现分布式证书库。

Huang 等[43]设计了一种基于区块链的 PKI 系统，将数字证书及证书操作记录在区块链上存储，使得查询变得简单高效，同时解决了传统 PKI 体系高度中心化带来的单点故障问题，提高了 PKI 体系的鲁棒性。

与此相似的是 Chiu 等[44]的工作，他们也是针对集中式 PKI 架构带来的单点故障问题进行研究，不仅解决了单点故障问题，而且为了防止 PKI 系统中 CA 的恶意治理导致的隐私泄露，他们通过改进原有系统，提出了一种基于隐私感知区块链的 PKI 系统，在缓存中删除和添加属性，尽可能地减少可访问的信息，进而防止隐私泄露。

4.3 小结

基于区块链的 PKI 身份认证方法弥补了传统 PKI 的几点不足，同时提升了验证过程的性能。Yan 等[28]提出了一种用于移动设备的系统，此系统基于 X.509v3 证书，具有多种类型的节点，因此可以兼容传统的 PKI 系统。其中系统中每个设备的身份由制造商预定义或由设备基于某些身份特征从 CA 获取。即使设备的识别号(ID)由国际移动设备标识固定，也需要 CA 来验证设备标识。虽然该提案保留了经典的基础结构，但它在设计中省略了用于吊销证书的 CRL。Shen 等[30]提出了一种使用区块链的认证机制，用于在车联网中实现有效的隐私保护和基于位置的服务，此机制虽提供了强大的安全性和隐私保护功能，但无法分析其可扩展性。

公钥用于识别区块链中的所有用户，从而间接防止匿名。由于节点执行的交易是共享的，因此第三方可以解释此类交易，并且可能发现参与者(节点)的真实身份。为了解决匿名性以及单点故障问题，Qin 等[42]提出的方法允许在投票、支付进行和盲目拍卖期间进行私人交易和匿名。虽然该系统不需要受信任的第三方，但它将全节点(即在区块链上管理数据的实体)视为 CA，而不提供任何认证方法。身份管理也是其中的一个非常严重的问题。此问题可以用许可区块链来解决，该区块链可以轻松管理多个物联网节点。这种类型的区块链轮换非对称密钥以防止攻击，并为身份管理提供分布式方法。这些密钥在参与节点上生成。要成功轮换密钥，系统必须验证用户的身份。

Chiu 等[44]提出的 ChainPKI 系统存在一些问题。例如，系统使用网络地址作为中继节点的 ID。虽然用户可以更改网络地址，但仍可能显示与用户相关的一些信息，如位置。此外，耗尽的网际协议版本 4(Internet Protocol version 4，IPv4)地址池和电信公司应用的网址转换器可能会使系统难以识别全球部署的个人。因此，需要设计一个合适的 ID 编码系统，该系统可以为分布式 PKI 下的每个节点提供唯一、匿名和安全的 ID。

综上所述，本节介绍了传统 PKI 目前研究及存在的问题，以及对应的解决方案；并阐述了基于区块链 PKI 身份认证的研究现状，如表 3 所列。

表 3 基于区块链 PKI 身份认证研究总结

Table 3 Summary of research on PKI identity authentication based on blockchain

传统 PKI 存在的问题	区块链优势	相关文献	解决思路
证书批量配置效率低	智能合约及共识机制	Yan 等[28] Shen 等[30]	简化证书提供和证书管理过程，降低部署和维护 CA 的成本 设计阈值代理签名
内网设备无法使用 CRL/OCSP	区块链中节点可以访问所有区块数据	Yan 等[28]	移动网络 PKI 框架
单点故障	分布式节点	Qin 等[42] Huang 等[43] Chiu 等[44]	将数字证书及证书操作记录在区块链上存储 将证书视作货币，记录到区块链上 在缓存中删除和添加属性，尽可能减少可访问的信息

5 基于区块链和生物识别的身份认证研究

作为网络安全的核心，身份认证是系统安全的第一道也是最重要的防线。然而，传统的基于身份的身份认证携带不方便，容易被伪造或受到假冒攻击。长密码这种基于算法的身份认证很难记忆，并且也容易受到推测攻击和欺骗攻击。与传统的识别方式相比，生物识别认证技术不易被遗忘和丢失，不易被伪造或被盗，可以随时随地使用。借助强大的计算机和网络技术，图像处理和模式识别可以使生物识别具有更好的安全性、可靠性和有效性。

5.1 生物识别技术研究

5.1.1 生物识别技术简介

生物识别技术指利用生物特征进行身份认证的一种技术，通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性和行为特征来进行个人身份的认证。人类的生物特征通常具有唯一性、可测量或可自动识别和验证、遗传性或终身不变等特点，因此生物识别认证技术较传统认证技术而言有较大的优势。

生物识别技术通过提取个人独特的身体和行为来保证身份认证系统的安全。目前已被用于生物识别的生物特征有手形、指纹、脸形、虹膜、视网膜、脉搏、耳廓等，行为特征有签字、声音、按键力度等。图 6 给出了生物识别认证过程中使用的部分物理标识符。在日常生活中，我们可以发现指纹识别、人脸识别、虹膜识别、发音识别的应用越来越多，生物特征识别技术已经在过去的几年中取得了长足的发展。

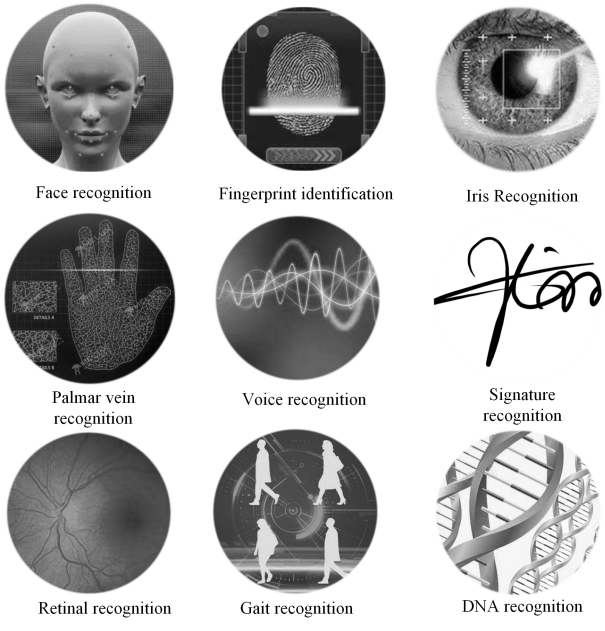

图 6 生物识别特征

Fig. 6 Biometric features

5.1.2 生物识别现状

生物识别身份认证系统可能面临各种安全威胁，例如生物识别信息的复制、盗窃和操纵已注册的模板。由于生物特征信息的不变性，生物特征信息的泄漏可能会导致连续的安全威胁。此外，生物识别信息通常由中央模块管理，这妨碍了认证系统的安全性和可靠性。现有研究主要集中在使用模板的加密、转换和分发来对生物识别信息进行安全管理。除此之外，它们还可能被错误地或出于恶意目的共享或提供给未经授权的人员。而且，尽管生物识别技术可能被认为是身份认证领域的最先进技术，但其传统的解决方案有非常大的局限性：获得访问权限比较困难，但一旦进入，又无法控制。因此，在允许用户使用资源后，访问可能会被入侵者转移或劫持。

5.1.3 生物识别系统

生物识别系统一般有 5 个不同的模块：传感器模块、用于特征提取的模块、模板数据库模块、匹配器模块和用于做出最终决策的模块。图 7 是一个经典的生物识别身份认证系统。用户和生物识别系统之间的认证边界由传感器形成。扫描的生物特征信息由特定的特征提取模块进行处理，提取的生物特征数据集以模板的形式存储在系统数据库中，该数据库由用户的识别特征标记。此过程为注册阶段，如图 8 所示。此模板数据库包含数百万条信息，并按地理位置分布。由于数据库很大，保护模板数据库免受各种安全攻击，确保此信息的安全成为一项至关重要的任务。匹配器模块的任务是在身份认证期间将两个生物识别功能集作为输入。一个是存储模板，另一个是查询模板。在比较两个匹配器模块后，生成一个分数，表示它们之间的相似程度。决策模块是最后一个模块，决定接受或拒绝并回答初始查询。此过程为验证阶段，如图 9 所示[45]。

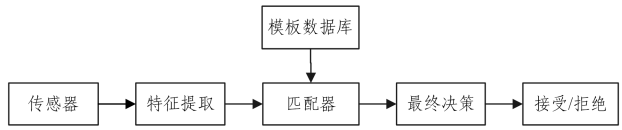

图 7 生物识别身份认证系统

Fig. 7 Biometric identity authentication system

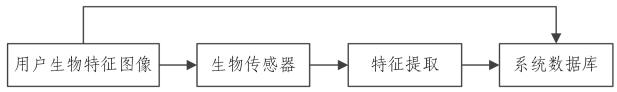

图 8 生物识别认证系统注册阶段

Fig. 8 Biometric authentication system registration stage

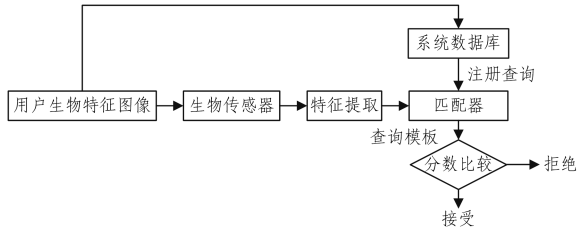

图 9 生物识别认证系统验证阶段

Fig. 9 Biometric authentication system verification stage

5.2 应用于区块链的生物识别的身份认证研究

生物识别技术保护了用户的安全，提升了用户身份认证的准确度，缺陷是存储方式中心化会导致用户信息被恶意篡改。将区块链技术与生物识别技术结合，并将采集到的用户生物信息存储到区块上，可以解决此问题，大幅度提升身份认证的准确度，以达到保护用户信息安全的目的。

图 10 给出了基于区块链的生物识别系统架构，架构主要包括 4 层，即应用层、网络层、事务层和物理层。

(1)应用层：应用层允许用户通过网络应用程序或者手机应用程序与系统进行通信，通过连接到基于区块链的网络，将

用户需求通过移动端应用程序或网页应用程序发送到系统。当用户直接与系统通信时，应用层为最终用户提供直接服务。

(2)网络层：网络层负责系统和用户之间的交互，由通信技术组成，可帮助用户、服务提供商和物联网设备(如传感器和安全摄像头)之间相互连接。该层提供物理层安全性的保证。

(3)事务层：负责整个区块链网络的所有共识机制，也负责系统中节点之间的操作。用户使用智能合约和共识机制以安全的方式交换数据，交易层与区块链网络交互并验证新交易，区块链接受用户信息交互作为交易并通过智能合约进行身份验证。生物特征信息公共分类账也通过该层进行更新。

(4)物理层：该层主要是不同类型的执行器和传感器、无线传感器网络(Wireless Sensor Networks，WSN)设备。其使用加密设备驱动程序来进行身份验证，然后将信息在公共分类账中更新。

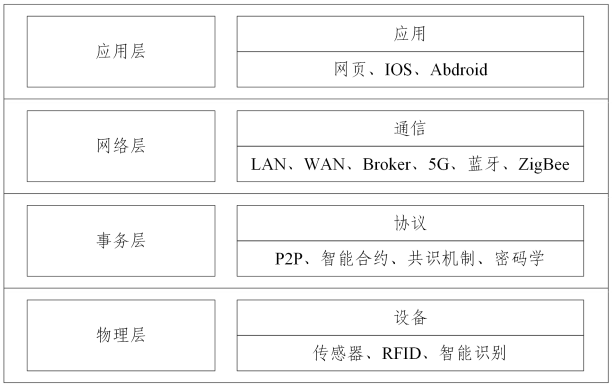

图 10 基于区块链的生物识别系统架构

Fig. 10 Biometric system architecture based on blockchain

区块链技术是一种新兴技术，它使用加密技术存储大数据并防止数据受到任何攻击。近年来，许多研究学者将其应用于区块链的系统研究。一些早期的研究工作试图将生物识别认证与区块链相结合，所提出的方案或没有很好的记录，或不够完善，无法应用于实际场景。Toutara 等[46]提出了一种分布式生物特征认证方案，成为首批实际实现者之一。该方案是基于以太坊区块链平台和星际文件系统(InterPlanetary File System，IPFS)的分布式文件系统，同时使用同态加密算法来加密用户的生物识别模板。当用户模板从其设备发送出去时，都会进行转换和加密，而加密算法的同态属性可以计算出此类向量对之间的距离。因此，第三方可以在进行身份认证尝试时做出决定，而无须访问用户的实际生物特征数据。

Lee 等[47]等设计了一种基于区块链的分布式生物识别认证系统(Blockchain-based Distributed biometric Authentication System，BDAS)。区块链是一种新兴技术，它支持加密操作，并使应用系统能够在没有中央机构的情况下实现弹性安全机制。通过结合区块链技术，BDAS 提供了用于处理生物识别身份认证的分布式机制，以及用于处理生物识别信息的可审计机制。此系统通过将每个生物识别模板拆分为片段并将其存储到区块链上的不同客户端，从而实现了对生物识别信息的安全管理。BDAS 采用区块链机制来提供可靠的身份认证，允许区块链上的每个客户端在没有中央机构的情况下执行交易。由于区块链上的每个交易都经过了验证并记录有时间戳，因此 BDAS 中的每个身份认证活动都记录在交易中，并且可以永久跟踪。

BDAS 与以往生物识别认证系统不同，这是因为：1)它通过基于区块链的分布式管理增强了生物识别信息的安全性；2)它通过基于区块链的去中心化认证提高了认证操作的可靠性；3)它通过基于区块链的审计机制保证了生物识别信息流的透明度。本文通过真实场景的比较分析来评估 BDAS 的可靠性，并通过比较 BDAS 与现有系统的身份认证时间来评估其性能。与现有方法相比，BDAS 提供了可靠的身份认证，同时在实际场景中引入的性能开销可以忽略不计。

Zhou 等[48]提出了一种基于区块链技术的生物识别和密码双因素跨域认证。基于区块链的不可篡改和分布式存储作为底层数据存储结构，用户能够使用模糊提取技术恢复出生物特征随机密钥。从根本上来说，用户在注册和身份认证阶段输入的静态密码将转换为动态密码作为密码因素。生物特征和密码的双因素认证是通过对称加密解密和生物特征随机密钥的识别匹配来实现的，但其算法计算复杂、效率低。为了在保证安全的前提下简化算法、提高效率，针对传统跨域认证方案少而复杂的问题，Xu 等[49]提出了一种基于区块链技术的跨域双卸载生物识别认证方案。该方案通过模糊提取技术来提取生物特征认证的随机密钥，从而解决了永久不可用导致的生物特征泄漏问题；其次，使用区块链来存储生物识别公共信息，消除了容易被主动攻击的模糊提取技术的威胁；最后，基于分布式存储功能和联盟区块链架构，实现了用户在本地和远程环境中的生物识别跨域认证。此外，对于双重卸载，一个是当方案卸载用户注册域的服务器时，在帮助用户注册并向区块链服务节点提交信息后不再需要。另一个卸载是，当另一个域服务器获取并存储客户端的身份认证信息时，区块链服务节点可以被卸载。

Bao 等[50]基于模糊提取器和区块链的去中心化和匿名性优势，提出了一种新的生物特征身份认证方案。首先，使用生物特征信息的模糊提取器参与认证过程，解决了生物特征模板泄漏导致的永久不可用的问题。然后，利用 Fabric 架构构建区块链，存储通过模糊提取器获得的随机密钥的哈希值，解决传统身份认证机制中存在的集中存储问题。基于区块链和模糊提取器，实现双因素身份认证方案。

图 11 给出了模糊提取技术的过程，形式如下：

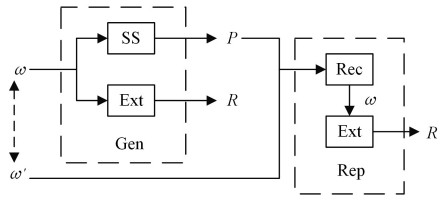

图 11 模糊提取技术过程

Fig. 11 Fuzzy extraction process

(1)随机字符生成算法 $Gen(\omega)\rightarrow(P,R)$：输入用户的生物特征信息 ω，并输出一个字符串 R 和公共信息 P，通过随机字符生成算法，其中 R 对应用户的生物特征的随机密钥。

(2)随机字符恢复算法 $Rep(\omega',P)\rightarrow R$：输入用户的生物特征 ω' 以及对应用户的公开信息 P，若两个输入生物特征的误差在给定的允许范围 ε 内，$dis(\omega,\omega')\leqslant\varepsilon$，则输出 R。

基于区块链和模糊提取的双因素认证模型如图 12 所示。

用户通过客户端访问服务提供者的服务，第一次发起服务请求时，需要完成注册操作，注册成功后服务提供者返回服务和公钥；当用户再次请求服务时，需要完成验证操作，服务提供者验证成功后返回服务和新的公钥。其中模糊提取器接收用户输入的生物特征信息，使用随机字符生成算法生成随机字符串 R。每个服务提供者都是区块链中的节点之一。客户端向具有注册权限的服务节点输入生物特征模板和证书信息，服务节点在注册、验证等操作中进行写入和验证等不同的计算。

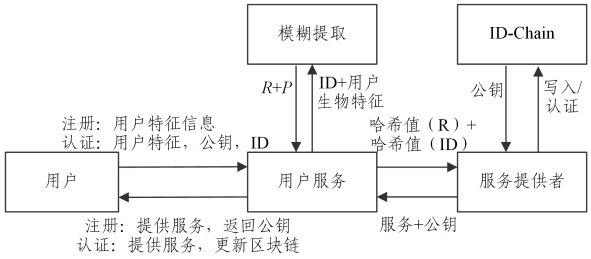

图 12 基于区块链和模糊提取器的双因素认证模型框架

Fig. 12 Two factor authentication model framework based on blockchain and fuzzy extractor

基于生物特征的模糊签名是一种基于生物信息的数字签名技术，其特点是每次都会从用户的生物特征信息中生成一个密钥，因此不需要将密钥存储在服务器或密钥管理设备上，用户没有丢失密钥管理设备的风险，并且可以防止来自窃取密钥的恶意软件的攻击。基于生物特征的模糊签名在双因素认证模型中利用区块链完成认证操作，具体流程如下。

(1)用户注册：在注册时，用户将用户名、证书信息、生物特征信息输入传感器，并从生物特征信息中提取特征值。接下来，使用特征值作为输入进行单向转换，用相关生物特征处理算法生成生物特征模板 ω。

(2)模糊提取：使用模糊提取器进行模糊提取 ω 获得 R 和 P，将随机密钥 R 进行哈希运算得到 HR_i，并将生物特征模板存储在认证设备中。用户的模板数据是公开信息，即使该信息被泄露给攻击者，也很难重构用户的密钥或生物特征信息。

(3)生成数字签名：使用密钥恢复算法和本地公共帮助信息 P 恢复认证用户的随机密钥 R' 并对其进行哈希处理以获得 HR'，当生成数字签名时，用户将生物特征信息输入到认证传感器设备并提取特征值。接着，根据模板和特征值重构密钥。只有当注册时的特征值和认证时的特征值足够接近时，才能重建正确的密钥。生成密钥后，用户生成用于交易的数字签名，并立即从内存中删除密钥。生成的签名可用公钥进行验证。

(4)认证：服务节点调用智能合约中的函数，读取用户的身份信息，并在区块链网络中搜索用户名引用。对比身份信息(证书信息和密钥)，对比成功则返回服务，否则认证失败。

多生物识别系统由于能够消除单峰系统的局限性而在各种应用中被广泛接受。将生物识别模板直接存储到集中式服务器中会导致隐私泄露问题。在过去几年中，学者们研究了许多基于同态加密的生物识别身份认证系统，以便为模板提供安全性。现有的大多数解决方案都依赖于服务器是“诚实但好奇”的假设的含义。因此，服务器造成的危害会导致整个系统产生漏洞，并且无法提供完整性。为了解决这个问题，Kumar 等[51]提出了一种多实例虹膜认证系统来处理通过传输通道和不受信任的服务器实施的恶意攻击，使用 ElGamal 加密对虹膜模板进行加密，以保证机密性，在区块链上运行的智能合约有助于实现模板的完整性和匹配结果，打破了将区块链用于隐私和昂贵存储等生物识别技术的局限性。

5.3 小结

将区块链应用于生物识别技术，是身份认证的一种手段，它允许以分布式的方式验证用户的身份，而无须建立存储敏感数据的中央实体。此外，它还可以防止恶意活动，迫使用户使用其个人生物识别信息签署交易。对于身份认证过程，系统必须获得区块链中所有节点的许可，当发生任何攻击，未经所有节点许可，任何人都无法更改数据，这就保证了区块链技术的防篡改。

Toutara 等[46]提出的方案虽使用户能够进行安全和私密的生物识别认证，但还需进一步研究加密算法，以更好地评估所提出协议的安全参数。Lee 等[47]通过将生物识别模板拆分为片段并基于区块链机制对其进行管理，提高了现有生物识别认证系统的安全性和可靠性。Xu 等[49]的工作与相关研究相比虽然效率更高，且可以防止重放攻击，达到了验证接收的目的，但其安全性还需进一步研究。

本节将区块链应用于生物识别的身份认证研究总结如表 4 所列。

表 4 基于区块链和生物识别的身份认证研究总结

Table 4 Summary of identity authentication research based on blockchain and biometrics

相关文献	问题	解决思路	优势
Toutara 等[46]	生物识别认证与区块链相结合无法应用于实际	基于以太坊区块链平台和 IPFS 分布式文件系统，同时使用同态加密算法来加密用户的生物识别模板	第三方可以在进行身份认证尝试时做出决定，而无须访问用户的实际生物特征数据
Lee 等[47]	生物识别信息安全管理	基于区块链的分布式生物识别认证系统	1)基于区块链的分布式管理增强了生物识别信息的安全性；2)通过基于区块链的去中心化认证提高了认证操作的可靠性；3)通过基于区块链的审计机制保证了生物识别信息流的透明度
Xu 等[49]	算法复杂，效率低，传统跨域认证方案少	基于区块链技术的跨域双卸载生物识别认证方案	采用模糊提取技术提取生物特征认证的随机密钥，从而解决永久不可用导致的生物特征泄漏问题。其次，使用区块链来存储生物识别公共信息，解决容易被主动攻击的模糊提取技术的威胁
Bao 等[50]	生物特征模板泄漏导致永久不可用	基于模糊提取器和区块链的的生物特征身份认证方案	基于区块链和模糊提取器，实现双因素身份认证方案
Kumar 等[51]	集中式服务器中可能会泄露隐私	多实例虹膜认证系统	ElGamal 加密对虹膜模板进行加密，以保证机密性，在区块链上运行的智能合约实现模板的完整性

6 基于区块链的身份认证应用领域研究

6.1 物联网

物联网是基于互联网连接事物的网络系统，是连接的设备和传感器的集合，目的是实现便捷、高效、智能的连接。物联网不同于传统 IT 网络，它们之间的显著区别在于终端设备的可用资源水平不同。物联网通常包括资源受限的嵌入式设备，如传感器。物联网设备的特征为内存小、计算能力低、电池寿命短。然而，传统的网络是由功能强大的计算机、服务器和智能手机组成，它们拥有充足的资源。因此，传统的网络可用复杂的、多因素的安全协议而不考虑任何资源限制。与此相反，物联网系统需要轻量级的安全算法，要在安全性和资源消耗之间保持平衡。

据估计，到 2023 年，全球 330 亿台联网设备中将有近 220 亿台成为物联网设备。随着连接到物联网系统的设备数量的增加，潜在的漏洞也会增加。例如，物联网设备容易受到网络攻击而产生数据盗窃、数据伪造等问题。物联网网络可以连接数百万台具有各种存储和计算能力的设备。由于数据和资源的这种异构性质，它们大多部署在未受保护的环境中，容易受到物理攻击，出现许多隐私和安全问题。一旦攻击者进入设备，它们就能看到启动序列，修改启动参数，获得对设备的底层访问权，还可能暴力强制根密码，并发起网络层攻击。区块链技术是一种有前途的解决方案，也是一种用于记录通过物联网技术获得的数据的可验证、安全和不可变的方法。

现有的物联网解决方案工作效率较低，中央云和大型服务器的维护成本也非常昂贵。区块链技术可以借助其优势和技术特性来降低高成本，提供更安全、更动态的解决方案。Dorri 等[52]利用比特币底层区块链技术构建了一个物联网轻量级架构。Ouaddah 等[53]通过引入 FairAcess 构建了一个物联网管理授权框架，使用户可以控制其数据。但区块链与物联网的集成仍处于起步阶段，问题仍有待解决。由于物联网设备的功能低下，计算开销是面临的挑战之一，但这个问题已经通过消除工作量证明策略和硬币的概念得到解决。同样，物联网设备的轻量级特性致使其存储容量有限，因此，数据无法长时间存储。这个问题与可扩展性问题密切相关，因为物联网设备存储越来越多的事务，存储成本很快就会变得昂贵。这也引发了人们对交易延迟的担忧。

区块链与物联网的结合被广泛应用于智能电网、智能家居、智能交通系统等领域。下面将从车联网、智能电网、金融、医疗等方面进行详细介绍。

6.2 车联网

中国通信学会发布的《蜂窝车联网(C-V2X)技术与产业发展态势前沿报告》中提到关于基于区块链的车联网安全技术。报告显示，区块链技术所倡导的问题场景和优势与车联网特征不谋而合。因此，借鉴区块链技术的优势，并将其应用于车联网的访问控制、通信安全、数据安全等方面，对提升车联网的安全性具有重要意义。

传统的车联网有集中管理权限，这种设计有许多弊端。一方面，如果某一个节点出现故障，会给攻击者提供一个机会；另一方面，用户隐私性较小。另外，集中式车联网模式及其对第三方信任机构的依赖，导致车联网存在一些安全问题。首先，如果集中式权限出现故障，整个系统可能无法正常工作，这对系统可用性构成了威胁。此外，为了保证网络安全，传统的车联网模型应该具有访问控制机制和消息验证操作。Sharma 等[54]考虑了稳健性的两个主要方面，即身份认证和隐私保护，通过区块链提供的分布式和可扩展的平台来进行授权访问和车辆身份验证。授权访问的真实性是通过将有效交易上传到区块链来实现的，其中有 4 个主要实体，即注册服务器，服务提供商，区块链和车辆，它们构成了拟议的三阶段系统，即注册阶段、身份认证阶段和授权阶段。这些步骤与其自身的功能协同工作，以保持所建议系统的鲁棒性。在认证阶段，使用区块链来确保系统的安全性和隐私性，并在 Remix 平台中实现智能合约。

考虑到安全性，我们假设第三方机构可以绝对信任。但是，由于网络不稳定或网络内部攻击，该假设不能始终被满足，因此需要提出一种无信任架构来解决上述问题，其中网络中每辆车的信任值由其他车辆保持。然后，可以在车辆信任的帮助下评估每辆车的行为。Li 等[55]提出了 CreditCoin 来解决物联网中消息转发的两个主要问题。具体而言，一是如何在不暴露用户隐私的情况下转发可靠的公告；二是如何激励车辆节点转发公告。针对第一个问题，提出了车辆公告协议 Echo-Notice，该协议可以在转发公告的同时实现效率和隐私保护。针对第二个问题，提出了一种基于区块链的激励机制。每个用户都可以管理其声誉点，同时赚取或花费硬币作为奖励。Luo 等[56]侧重于研究位置隐私泄露问题，提出了一种基于区块链和分布式机制的位置隐私保护分布式管理机制。首先，基于不同参与者的特征，设计了一种基于狄利克雷分布的信任管理方法；然后，区块链充当分布式数据库，记录该机制中的信任值，以便发起车辆和合作车辆仅在匿名隐身区域中与它们信任的车辆合作。

Liu 等[57]旨在解决网络中的两个问题，即消息是否可靠以及车辆的隐私是否受到保护。对于第一个问题，提出了一种用于安全车辆通信的条件隐私保护公告协议。在此协议中，消息聚合可以有效地实现身份认证并降低网络开销。消息公告的可靠性可以通过车辆的阈值数量来提高。对于第二个问题，提出了基于区块链的信任管理模型。该模型包含两个部分：声誉更新算法和分布式共识算法。信誉数据存储在块中，其值将按直接信任值和间接信任值进行评估。

颁发给每辆车的证书是车联网中每辆车的通信身份。在传统物联网中，证书管理的工作由公钥基础设施完成，包括证书颁发和吊销。但是，这种架构存在单点故障问题，会降低网络的可靠性。

为解决上述问题，Lu 等[58]假设可信机构是半可信的，在发生争议时不会恶意跟踪或揭示公钥与目标车辆真实身份之间的联系。此外，半可信机构是透明和可验证的，因为所有证书和交易都永久且不变地记录在区块链中。最后，BPPA 采用 Chronological Merkle Tree(CMT)和 Merkle Patricia Tree(MPT)来扩展传统的区块链结构，从而提高效率和可扩展性。为了解决证书管理问题，Ma 等[59]提出了一种分布式密钥管理机制，其中集成了轻量级身份认证和基于区块链的

密钥协议,通过区块链和智能合约实现。基于该机制,可以防御一些典型的攻击,如抵御内外攻击、公钥篡改、DoS 攻击和串通攻击。

Lu 等[60]提出了一种基于区块链的匿名信誉系统,以解决车联网中的 3 个问题,即声誉管理、证书管理以及证书与车辆身份之间的隐私保护。在基于区块链的匿名信誉系统中,他们还提出了 3 个区块链,包括用于消息的区块链、用于证书的区块链和用于吊销公钥的区块链,以管理证书初始化、更新、撤销和身份认证的过程。其次,提出了一种信誉评估算法,用于在车联网中构建信任模型。该算法利用奖励机制来激励诚实和活跃的节点,同时利用惩罚机制来抑制诸如分发伪造消息等不当行为。然后,使用第三方执法机构来保持车辆身份的隐私。第三方机构取代了证书颁发机构的某些职能,证书颁发机构不了解车辆身份与其相关证书之间的联系,而相关证书仅由执法机构控制。但是,还有些问题并没有得到完全解决。首先,在网络中传输的所有消息都记录在区块链上,使得消耗了过多的带宽。特别是在车联网中,消息分布频繁,并非所有消息都可以及时记录在区块链上。其次,使用了第三方执法机构来保护证书颁发机构不暴露车辆身份,但是,这种方式与仅使用证书颁发机构的原始机制没有太大区别。

Cheng 等[61]在半集中式交通信号控制系统中构建了基于密文策略属性的加密区块链,以支持车辆对交通数据的访问控制。结构从 3 个方面进行描述。首先,在开始通信之前,认证中心和跟踪管理器对用户的身份进行身份认证,并根据车辆的属性(如动态位置和方向)将其划分为组。其次,车辆通过与他人交互达成临时信号控制协议,而不会泄露隐私。最后,在建立通信后,所有用户都可以验证最终决定。Singh 等[62]提出了用于安全、智能车辆通信的区块链技术,可用于跟踪车辆生成的数据并使用区块链进行验证。Yang 等[63]在基于 PKI 认证基础上设计了基于区块链的交通事件验证框架,可以两次通过阈值的事件验证机制帮助验证事件。

基于区块链的车联网安全技术在展现生命力的同时,仍然面临诸多挑战,包括低效的区块生成机制导致交易数据处理时延过高,海量车联网数据给区块链节点存储空间带来压力,区块链自身面临安全隐患,不同区块链底层技术限制了多链之间的互联互通,用户身份隐匿性阻碍了网络安全事件的追踪溯源,防篡改特性增加了内容管理等[64]。

6.3 智能电网

电网是国家的关键基础设施,可提供可靠的电力供应,电网的安全对国家安全至关重要。随着移动网络的快速发展和应用,智能电网中电力移动终端的种类和数量也不断增多。在这种情况下,电力人员需要使用移动终端随时连接到所需的电力服务系统。在使用移动终端进行身份认证时,电力人员需要保留一些关键的认证信息,但在认证过程中存在容易丢失和易受攻击等安全问题。因此,如何将电力移动终端安全地连接到电力系统已成为一个亟需解决的问题。

目前对身份认证安全性的研究已成为研究重点,可分为提高移动终端安全性和数据操作,以及研究新的去中心化架构,或改进和简化现有的身份认证架构。

(1)在提高移动终端自身安全性方面:为了解决移动终端身份信息容易被攻击的问题,Li 等[65]将几种对称密钥算法结合到移动终端的身份认证中,提高了移动终端的身份安全。Ma 等[66]将生物识别技术应用于实时身份认证,提高了身份认证技术的效率和安全性。Fan 等[67]对用户的身份进行电子化处理,并提出了电子身份认证机制,提高了移动身份认证系统的便利性和效率。

(2)在提高数据运行安全性方面:为防止用户身份信息受到攻击,保证高级用户的数据安全,Chen 等[68]应用量子密钥技术为业务数据保护提供动力,有效提高了用户身份数据的安全性。针对异构环境中的用户身份信息安全问题,Dong 等[69]将区块链技术应用于用户身份的认证机制,通过去中心化架构来提高用户身份认证机制的安全性。针对移动终端认证效率低、安全性低的问题,Ma 等[70]采用区块链技术来完善认证机制的架构,实现了跨域认证的技术方案,有效解决了跨域环境中用户身份易受攻击的问题。

(3)在研究新的去中心化架构方面,Ma 等[70]将区块链技术应用于跨域认证,并提出了一种基于区块链的跨域认证方法。Dong 等[71]为了解决低安全级别终端未经授权就访问高安全级别域的问题,结合联盟区块链、风险评估机制和主观信任加权算法,提出了一种基于区块链的跨域认证可信机制。

(4)在改进和简化现有的身份认证架构方面,为了简化域代理部署,Guo 等[72]提出了一种基于信任的跨域认证机制,将身份密码与信任度相结合,有效降低了跨域认证的计算和通信开销。Wang 等[73]将现有服务器充当区块链节点,支持基于联盟区块链的跨域身份认证,以简化计算、存储和通信开销。为了解决跨域认证中身份吊销缓慢的问题,Xie 等[74]在跨域认证模型中加入了安全仲裁,以存储终端的私钥。现有的研究大多集中在改进和简化现有的身份认证框架上,然而,如何实现智能电网中电力终端的跨领域认证仍是一大问题。为此,Huang 等[75]通过分析电力通信网络的组网特性,提出了一种基于区块链的电力终端认证机制,并且取得了良好的效果。

通过对现有研究的分析可以看到,针对电力终端设备的身份认证取得了良好的研究成果。

6.4 金融

对于金融行业来说,2008 年以来,监管加剧和经济增长乏力以及随之而来的金融危机,迫使金融部门不断采用先进技术来提高透明度和增强安全性,从而节省成本和提高效率。近年来,区块链引起了人们的关注,它可以促进流程的自动化和简化,消除手动后台劳动,减少时间,提高透明度和安全性。

金融业的问题具体体现在:1)金融机构之间的对账和结算成本非常高,存在许多复杂的过程;2)在证券市场,交易过程耗时长,成本高;3)资产管理主要由中介机构管理,这增加了交易成本和假冒风险;4)用户识别问题,不同金融机构之间的用户数据很难有效交互;5)在跨境交易的情况下,双方往往信任不足,需要中介担保。区块链是解决金融业问题的有效工具,它能够建立精确、及时、多方面的监管。例如,点对点价值转移、分布式技术和数字资产、通过智能合约建立机制以确保遵守合同,以及数字身份识别。

目前,信任问题仍然是建立数字支付的主要挑战。关于移动支付的特别研究表明,需要受信任的服务经理参与处理身份认证、授权和账户结算,以及直接和间接网络的影响。基于 P2P 网络,分布式交易平台在去中心化的帮助下,为这一挑战提供了解决方案。新的数字支付系统正在推出,专门用于满足银行服务的需求,但新系统目前无法处理以前不存在的需求。使用区块链技术的新支付系统不仅意味着减少现金支付,而且银行也将这种设置视为处理消费者支付的安全可靠的方法。此外,移动运营商希望使用 SIM 卡进行付款人识别来从增加的收入中受益。平台战略的定价、开放性等谈判直接受到相互冲突的目标的影响。因此,在监管严格的金融领域,使用区块链技术的新数字支付平台正面临着一场极具挑战性的战斗[76]。

除了数字支付,区块链技术还被用于供应链金融。每天,数十亿件产品被制造并运往世界各地的最终客户手中。在交付之前,产品通过构成供应链的零售商、分销商、运输商、存储设施和供应商网络进行运输。供应链中的故障可能会中断运营,导致财务和声誉损失以及环境破坏。供应链管理的复杂性要求透明度和可追溯性,以便通过提高对因果关系的认识来降低风险。在当前实践中,可信信息的存储由第三方组织集中维护,这增加了与数据存储的技术可靠性和互操作性、安全性和隐私性相关的风险。区块链解决方案的集成有可能改善买家和供应商之间的流程和问责制[77]。

Abeyratne 等[78]提出了一个私有区块链框架,旨在提供一个共享的透明系统,供货方可以通过智能合约访问。每一方都可以通过验证身份和资格的注册服务加入网络。在此之后,注册方有权使用其私钥访问、写入和读取区块链。在供应过程中,记录了 5 类数据:时间戳、产品信息、时间顺序位置、时间顺序所有权和对产品的环境影响。与原始验证过程不同,任何新的供应记录都将在产品运送到客户并且双方签署智能合约以验证交换时进行验证。

易腐产品通常对温度和储存条件很敏感。Tian[79]提出了一种区块链解决方案,通过共享记录、智能合约和传感器来确保生命周期信息的透明度。通过注册服务,用户可以获取公钥和私钥,用于访问网络并维护其隐私。存储的数据分为两类:用户配置文件(存储有关用户、位置、认证以及与产品的关联的信息)和产品配置文件(存储产品规格和处理更新)。该方案研究了生产、加工、仓储、冷链配送、零售、权威组织 6 个节点的应用场景。在食品供应链中,使用分布系统的优势是可以通过提供透明度、可靠性和安全性来防止信息欺诈和勒索。

除了基于区块链的供应系统提供的记录的可追溯性和防篡改性外,对环境影响的适应性也是一个重要问题。OriginChain 是一个私有区块链系统,旨在适应不断变化的环境和法规[80]。OriginChain 中的数据来自 4 种类型的节点:供应商或零售商、测试实验室、可追溯性服务提供商、工厂或货场检验员。为了允许各方使用区块链,管理人员验证各方的请求并颁发准入证书,工厂审查员检查工厂的资格,货运堆场检查员检查产品并监督产品的装载和密封。所有信息都通过智能合约和供应链各方之间的法律协议进行注册和验证。

供应链中对产品的透明度和可追溯性的需求是区块链利用的主要驱动因素,这是因为该技术的可分配性有助于向授权方提供交易的可见性。分布式解决方案对于易腐货物供应链有重要价值,原因在于它通过提供数据透明度、可靠性和安全性来防止欺诈和勒索。

尽管有这些好处,但区块链技术在供应链系统中的应用仍然需要在各方的站点上具有一定的技术基础设施,以保持系统更新。克服保持最新记录和互操作性的困难的一个解决方案是利用传感器等技术有效地增强信息的连续性。区块链解决方案中最具挑战性的问题是:随着网络的扩展,所需的计算能力和存储容量会不断增加,为了克服这一困难,Lu 等[80]使用链上记录(可追溯性证书和可追溯性法规信息的哈希)和链下记录(可追溯性证书和智能合约的地址)来管理性能和隐私之间的平衡。其他挑战源于传统供应链系统的性质,包括技术的不成熟,需要更新当前的供应技术以及当前系统中的培训实践[81]。

6.5 医疗

在医疗行业,由于有保护患者医疗信息的额外法律要求,因此对安全性和隐私性有独特的要求。在互联网时代,随着云存储和移动健康设备的采用,记录和数据的共享变得更加普遍,恶意攻击的风险以及共享时私人信息受到损害的风险也会增加。随着健康信息越来越容易通过智能设备获取,这些信息的共享和隐私成为一个重要问题。医疗行业的独特要求包括身份认证、互操作性、数据共享、医疗记录传输以及移动医疗注意事项[82]。

传统的集中式身份管理系统,限制了患者和医疗保健提供者身份识别的互操作性,这就导致无法在电子健康应用程序域之外对自己进行身份认证。将基于区块链的身份技术应用于医疗行业,使用加密算法、密钥机制或生物识别方案来保护敏感或关键信息,主要有以下几点好处:

(1)分布式医疗。区块链可以成为去中心化的健康数据管理骨干网,所有利益相关者都可以从中控制访问权限相同的健康记录,没有人扮演中央权威的角色来控制全球卫生数据。

(2)安全和隐私。数据一旦被保存到区块链上就不能被破坏、更改,其不变性大大提高了医疗数据的安全性。此外,医疗数据使用加密密钥,有助于保护患者的身份或隐私。

(3)医疗数据所有权。患者需要拥有自己的数据,并控制其数据的使用方式。患者需要保证自身的医疗数据不被其他利益相关者滥用,并且可以检测何时发生这种滥用。区块链可以通过强大的加密协议和定义明确的智能合约来满足这些需求。

(4)稳健性。系统是健壮且有弹性的,区块链上的记录可以在多个节点中复制,因此可以防止存储在区块链上的医疗数据丢失、数据损坏和对数据可用性的一些安全攻击。

(5)透明性和可信性。区块链利用其开放和透明的性质,创造了一种可信任的氛围,这有利于用户接受与其相关的应用程序。

(6)数据可验证性。用户无须访问存储在区块链上的记录的明文,并且可以验证这些记录的有效性。此功能在需要

验证记录的医疗领域有重要作用，例如药品供应连锁管理和保险索赔处理。

总之，区块链技术在医疗行业具有潜在的应用价值。但由于区块链技术在医疗行业中的应用仍然是一个新兴领域，因此需要为研究人员开发更多的原型和概念验证，以加深理解以及掌握该技术在医疗中的应用的成熟度。医疗行业正面临着适应不断发展的技术基础设施的问题，这些基础设施专注于支持互联网的设备、物联网、智能设备和传感设备，可以使医疗行业在不断增长的互联世界中更好地为患者提供服务。但恶意行为者可以利用这些技术中的漏洞来访问和复制数据，使医院之间共享记录变得更加困难，也可能导致数据过时，从而导致健康问题或误诊，出现验证患者身份的问题。现有应用程序应专注于身份认证、完整性、记录共享、互操作性、安全性、边缘主机安全性和患者授权等问题，将着重点放在患者能够事先授权访问患者记录，在紧急情况下，可以使用哪些备份计划或紧急协议来允许医生在未经授权的情况下访问记录，让患者控制医疗数据并有拥有医疗数据共享的权利，让被允许查看数据的人在安全的环境中查看数据，以提高对技术的信心，并促进其在医疗行业中的广泛应用。

6.6 小结

区块链与物联网结合被广泛应用于智能电网、智能家居、智能交通系统等领域。本节从物联网开始，详细介绍了目前基于区块链的身份认证在车联网、智能电网、金融、医疗等领域的研究现状。

基于区块链的身份认证的总结如表5所列。

表5 基于区块链的身份认证的应用领域

Table 5 Application fields of identity authentication based on blockchain

应用领域		文献	描述
物联网		Dorri 等[52]	利用比特币底层区块链技术的物联网轻量级架构
		Ouaddah 等[53]	基于区块链技术的物联网访问控制框架
车联网		Sharma 等[54]	利用区块链技术维护分布式服务提供商之间共识的车辆信息系统的新型架构
		Li 等[55]	车辆公告协议 Echo-Notice，在不暴露用户隐私的情况下转发可靠的公告；基于区块链的激励机制，激励车辆节点转发公告
		Luo 等[56]	基于区块链和分布式机制的位置隐私保护分布式管理机制，侧重于位置隐私泄露问题
		Liu 等[57]	用于安全车辆通信的条件隐私保护公告协议，判断消息是否可靠；基于区块链的信任管理模型
		Lu 等[58]	基于区块链的隐私保护身份认证方案，假设可信机构是半可信的，在发生争议时不会恶意跟踪或揭示公钥与目标车辆真实身份之间的联系
		Ma 等[59]	分布式密钥管理机制，集成了轻量级身份认证和基于区块链的密钥协议，通过区块链和智能合约实现
		Lu 等[60]	基于区块链的匿名信誉系统，提出3个区块链，包括用于消息的区块链、用于证书的区块链、用于吊销公钥的区块链，用以解决声誉管理、证书管理以及证书与车辆身份之间的隐私保护问题
		Cheng 等[61]	在半集中式交通信号控制系统中构建基于密文策略属性的加密区块链，以支持车辆对交通数据的访问控制
		Singh 等[62]	本地动态区块链和主区块链，智能车辆信任点
		Yang 等[63]	基于区块链的交通事件验证框架，两次通过阈值的事件验证机制可以帮助验证事件
智能电网	提高移动终端自身安全性	Li 等[65]	将几种对称密钥算法结合到移动终端的身份认证
		Ma 等[66]	将生物识别技术应用于实时身份认证
		Fan 等[67]	对用户的身份进行电子化处理，提出电子身份认证机制
	提高数据运行安全性	Chen 等[68]	应用量子密钥技术为业务数据保护提供动力
		Dong 等[69]	将区块链技术应用于用户身份的认证机制，通过去中心化架构提高用户身份认证机制的安全性
		Ma 等[70]	采用区块链技术，完善认证机制的架构，实现跨域认证的技术方案
	研究新的去中心化架构	Ma 等[70]	将区块链技术应用于跨域认证，提出了一种基于区块链的跨域认证方法
		Dong 等[71]	结合联盟区块链，结合风险评估机制和主观信任加权算法，提出了一种基于区块链的跨域认证可信机制
	改进和简化现有的身份认证架构	Guo 等[72]	将身份密码与信任度相结合，有效降低了跨域认证的计算和通信开销
		Xie 等[74]	在跨域认证模型中加入了安全仲裁，以存储终端的私钥
		Huang 等[75]	通过分析电力通信网络的组网特性，提出了一种基于区块链的电力终端认证机制
金融		Abeyratne 等[78]	提出了一个私有区块链框架，旨在提供一个共享的透明系统，供货方可以通过智能合约访问
		Tian[79]	通过共享记录，智能合约和传感器确保生命周期信息的透明度
		Lu 等[80]	私有区块链系统
医疗		Javed 等[83]	提出了一个基于区块链的分布式身份管理系统，该系统允许患者和医疗保健提供者在不同的电子医疗领域透明安全地识别和验证自己
		Wang 等[84]	基于双区块链的隐私保护远程医疗诊断方案，通过构建一个公链用户链和一个联盟医疗链，实现用户、医生和医院之间的有效交互
		Mamun 等[85]	提出了个人控制系统，以使用密码技术增强患者数据的安全性和隐私性
		Kumar 等[86]	无证书聚合签名方法，用于智能医疗系统中的安全通信
		Sharma 等[87]	WSN 隐私保护方法，使用多路径路由、秘密散列和共享的规则来实现数据隐私
		Ray 等[88]	基于隐私保护属性的敏感信息访问控制方法，具有以用户为中心的信息、策略管理、隐私保护和权限撤销等特点
		Shrestha 等[89]	提出了一个改进的安全框架，用于授权和身份认证

7 未来研究展望

基于区块链技术的身份认证呈现出了良好的发展态势，未来发展空间也会更加广阔，展现了其独特的价值。基于区块链的统一身份认证的价值在于：

(1)区块链的去中心化功能可以缓解认证平台数据共享的安全问题。一旦身份认证平台通过区块链共享数据，构建和维护这些平台的成本就会降低。

(2)可以提高使用身份属性信息的便利性。将存储在不同认证平台中的用户身份信息整合在一起，便于验证用户身份信息。

针对现有研究，未来的发展可能呈现出以下趋势。

(1)可扩展且经济。复杂的加密原语通常会带来繁重的计算和通信开销，随着区块链系统中参与者数量的增加，存储和通信成本也会增加，这些高成本限制了匿名集的可扩展性。因此，一个可能的方向是解决现有或新型加密原语及其可能配置之间的组合优化问题。

(2)共识机制。区块链共识协议会消耗大量的计算资源和功率，导致系统吞吐量低，延迟变长。区块链需要更好的平台操作性和更兼容的功能来支持其发展。为此，设计一种能够聚合和利用分布式共识节点的群智能交互机制是区块链目前的重中之重。虽然区块链技术的基础相对比较成熟，但在协议改进方面还有很多问题需要解决，现如今的问题是如何构建共识机制以提高系统吞吐量。目前，有许多特定于不同区块链平台的标准和功能的协议。对共识机制的研究可以从不同角度进行比较和分析，目标是寻求更好的协议，以实现更高水平的能源和成本的节约，从而提高系统的可扩展性、安全性和隐私性等。

(3)可扩展性和容量。区块链要求系统中的每个节点都要维护数据的备份，这对于不断增长的海量数据存储来说是不现实的。虽然轻量级验证节点可以在一定程度上解决问题，但仍然需要研究和设计更有效的工业解决方案。在区块链系统中，每个网络节点都可以存储所有历史交易数据。这虽然保证了数据的开放性、透明度和高可用性，但也带来了数据隐私和性能问题，而单个节点不能无限期地存储数据。交易量和数据量的快速增长带来了两种解决可扩展性问题的方案：通过扩展区块链存储或重组区块链。

(4)法规和法律。虽然基于区块链的身份认证在许多方面改变了社会生活，但它也挑战了法律和法律体系。特别是在发展初期，由于区块链技术的独特性和法律监管的滞后性，引发了一系列法律问题。全面了解区块链的特征有助于建立和完善与区块链活动相关的法律法规。许多国家正在积极部署区块链技术，并改进监管措施，如权力下放和法律适用以及管辖权问题、匿名化和互联网实名问题、可靠性和删除权问题，以及透明度和个人数据隐私问题。此外，在国家治理和社会治理领域，技术和法律是相互替代的，如何吸收技术带来的制度创新，同时规避技术决定一切、保护法律价值的社会物理立场，将成为决定区块链技术良性循环的重要因素。

结束语 本文阐述了区块链技术应用于身份认证研究的意义，介绍了关于区块链在身份认证方面有关的基础理论知识，广泛调研了基于区块链技术在身份认证领域相关的国内外文献，详细论述并总结了基于区块链技术的身份认证研究在口令认证方面、PKI、生物识别方面的相关研究，给出了基于区块链技术的身份认证在一些应用领域的研究现状，包括车联网、智能电网、金融、医疗。最后，针对现今区块链认证技术存在的问题，对未来进行展望。

参 考 文 献

[1] HUSSAIN M, MEHMOOD A, KHAN S, et al. Authentication techniques and methodologies used in wireless body area networks[J]. Journal of Systems Architecture, 2019, 101(5): 1-28.

[2] NAKAMOTO S. Bitcoin: A peer to peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[3] WENG J, WENG J, ZHANG J, et al. DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 18(5): 2438-2455.

[4] MAKHDOOM I, ABOLHASAN M, ABBAS H, et al. Blockchain's adoption in IoT: The challenges, and a way forward[J]. Journal of Network and Computer Applications, 2019, 125(2): 251-279.

[5] LIU Y, HE D, OBAIDAT M S, et al. Blockchain-based identity management systems: A review[J]. Journal of Network and Computer Applications, 2020, 166(15): 245-255.

[6] LI Q, SHU Z X, YU X, et al. Authentication Mechanism in Blockchain Systems[J]. Journal of Command and Control, 2019, 5(1): 1-17.

[7] YANG L. The blockchain: State-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15(4): 80-90.

[8] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4: 382-401.

[9] DURRANI A. Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey[J]. Applied Sciences, 2021, 11(14): 245-258.

[10] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.

[11] LAMPORT L. LAMPORT, Password Authentication with Insecure Communication[J]. Communications of the ACM, 1981, 24(11): 770-772.

[12] SHANKAR T N, RAKESH P, BHARGAWA R T, et al. Providing Security to Land Record with the computation of Iris, Blockchain, and One Time Password[C]// Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). Greater Noida, India, 2021: 226-231.

[13] KANG J, RONG Y, HUANG X, et al. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains[J]. IEEE Transactions on Industrial Informatics, 2017, 15(5): 840-852.

[14] ZHANG M, WANG L, YANG J. A Blockchain-Based Authentication Method with One-Time Password[C]// Proceedings of

the 2019 IEEE 38th International Performance Computing and Communications Conference(IPCCC). London,UK,2019:1-9.

[15] BUCCAFURRI F,ANGELIS V D,NARDONE R. Securing MQTT by Blockchain-Based OTP Authentication[J]. Sensors,2020,20(7):261-269.

[16] JAYAN A P,BALASUBRAMANI A,KAIKOTTIL A,et al. An enhanced scheme for authentication using OTP and QR code for MQTT protocol[J]. International Journal of Recent Technology and Engineering,Blue Eyes Intelligence Engineering and Sciences Publication,2019,7:70-75.

[17] ERDEM E,SANDKKAYA M T. OTPaaS—One Time Password as a Service[J]. IEEE Transactions on Information Forensics and Security,2019,14(3):743-756.

[18] EL-BOOZ S A,ATTIYA G,EL-FISHAWY N. A secure cloud storage system combining time-based one-time password and automatic blocker protocol[J]. EURASIP Journal on Information Security,2016,37(1):1-13.

[19] LAI C,DING Y. A Secure Blockchain-Based Group Mobility Management Scheme in VANETs[C]// Proceedings of the 2019 IEEE/CIC International Conference on Communications in China(ICCC). Changchun,China,2019:340-345.

[20] ZHANG Z,XIAO Y,MA Z,et al. 6G Wireless Networks:Vision,Requirements,Architecture,and Key Technologies[J]. IEEE Vehicular Technology Magazine,2019,14(3):28-41.

[21] ZHANG R,XUE R,LIU L. Security and privacy on blockchain [J]. ACM Computing Surveys,2020,52(3):1-34.

[22] LIN I C,LIAO T C. A Survey of Blockchain Security Issues and Challenges[J]. International Journal of Network Security,2017,19(5):653-659.

[23] WANG C,CHEN S,CHEN S,et al. Trust Management for Reliable Cross-Platform Cooperation Based on Blockchain[C]// 2021 IEEE International Conference on Web Services (ICWS). Chicago:IEEE,2021:629-634.

[24] LI X,JIANG P,CHEN T,et al. A Survey on the Security of Blockchain Systems[J]. Future Generation Computer Systems,2018,16(8):258-268.

[25] MOHANTA B K,PAN S S,JENA D. An Overview of Smart Contract and Use Cases in Blockchain Technology[C]// Proceedings of the 2018 9th International Conference on Computing,Communication and Networking Technologies(ICCCNT). Bengaluru,India,2018:1-4.

[26] BLACK P,LAYTON R. Be Careful Who You Trust:Issues with the Public Key Infrastructure[C]// Proceedings of the 2014 Fifth Cybercrime and Trustworthy Computing Conference. Auckland,New Zealand,2015:12-21.

[27] SHPHEI K,YOSHIAKI S,MASAMI M,et al. Cross-Certification Towards Distributed Authentication Infrastructure:A Case of Hyperledger Fabric[J]. IEEE Access,2020,8:135742-135757.

[28] YAN J,HANG X,YANG B,et al. Blockchain Based PKI and Certificates Management in Mobile Networks[C]// Proceedings of the 2020 IEEE 19th International Conference on Trust,Security and Privacy in Computing and Communications(TrustCom). Guangzhou,China,2020:1764-1770.

[29] YAKUBOV A,SHBAIR W,WALLBOM A,et al. A Blockchain-Based PKI Management Framework[C]// 2018 IEEE/IFIP Network Operations and Management Symposium. Taipei:IEEE,2018:1-6.

[30] SHEN H,ZHOU J,CAO Z,et al. Blockchain-Based Lightweight Certificate Authority for Efficient Privacy-Preserving Location-Based Service in Vehicular Social Networks[J]. IEEE Internet of Things Journal,2020,7(7):6610-6622.

[31] BECKWITH E,THAMILARASU G. BA-TLS:Blockchain Authentication for Transport Layer Security in Internet of Things [C]// 2020 7th International Conference on Internet of Things:Systems,Management and Security(IOTSMS). 2020:268-275.

[32] SAHA S,CHATTARAJ D,BERA B,et al. Consortium blockchain-enabled access control mechanism in edge computing based generic Internet of Things environment[J]. Transactions on Emerging Telecommunications Technologies,2021,32(6):1-34.

[33] WANG Z,LIN J,CAI Q,et al. Blockchain-based Certificate Transparency and Revocation Transparency[J]. IEEE Transactions on Dependable and Secure Computing,2020,19(1):681-697.

[34] ZHAO G,DI B,HE H. A novel decentralized cross-domain identity authentication protocol based on blockchain[J]. Transactions on Emerging Telecommunications Technologies,2022,33(1):4377-4393.

[35] BAO S,LEI A,CRUICKSHANK H,et al. A Pseudonym Certificate Management Scheme Based on Blockchain for Internet of Vehicles[C]// 2019 IEEE International Conference on Dependable,Autonomic and Secure Computing,International Conference on Pervasive Intelligence and Computing,International Confe-rence on Cloud and Big Data Computing,International Conference on Cyber Science and Technology Congress(DASC/PiCom/CBDCom/CyberSciTech). Fukuoka:IEEE,2019:28-35.

[36] SIMPLICIO M A,COMINETTI E L,PATIL H K,et al. ACPC:Efficient revocation of pseudonym certificates using activation codes[J]. Ad hoc networks,2019,7(90):1-14.

[37] CHO E,PERERA M. Efficient Certificate Management in Blockchain based Internet of Vehicles[C]// 2020 20th IEEE/ACM International Symposium on Cluster,Cloud and Internet Computing(CCGRID). Melbourne,VIC,Australia:IEEE,2020:794-797.

[38] MATSUMOTO S,REISCHUK R. IKP:Turning a PKI Around with Decentralized Automated Incentives[C]// 2017 IEEE Symposium on Security and Privacy(SP). San Jose:IEEE,2017:410-426.

[39] LEIDING B,CAP C H,MUNDT T,et al. Authcoin:Validation and Authentication in Decentralized Networks[J]. Cryptography and Security,2016,5:121-134.

[40] WON J,SINGLA A,BERTINO E,et al. Decentralized Public Key Infrastructure for Internet-of-Things[C]// 2018 IEEE Military Communications Conference(MILCOM). Los Angeles:IEEE,2018:907-913.

[41] SINGLA A,BERTINO E. Blockchain-Based PKI Solutions for IoT[C]// 2018 IEEE 4th International Conference on Collaboration and Internet Computing(CIC). Philadelphia:IEEE,2018:9-15.

[42] QIN B, HUANG J K, WANG Q, et al. Cecoin: A decentralized PKI mitigating MitM attacks[J]. Future Generation Computer Systems, 2020, 107: 805-815.

[43] HUANG Y X, WANG Y W, CHEN W X, et al. PKI cross-domain authentication model based on alliance chain[J]. Computer Engineering and Design, 2021, 42(11): 3043-3051.

[44] CHIU W Y, MENG W, JENSEN C D. Chain PKI-Towards Ethash-based Decentralized PKI with Privacy Enhancement [C]// Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC). Aizuwakamatsu, Fukushima, Japan, 2021: 1-8.

[45] SARKAR A, SINGH B K. A review on performance, security and various biometric template protection schemes for biometric authentication systems[J]. Multimedia Tools and Applications, 2020, 79(3): 27721-27776.

[46] TOUTARA F, SPATHOULAS G. A distributed biometric authentication scheme based on blockchain [C] // Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain). Rhodes, Greece, 2020: 470-475.

[47] LEE Y K, JEONG J. Securing biometric authentication system using blockchain[J]. ICT Express, 2021, 7(3): 322-326.

[48] ZHOU Z, LI L X, GUO S, et al. Biometric and password two-factor cross domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, 38(6): 1620-1627.

[49] XU, Y, MENG, Y, ZHU H. An Efficient Double-Offloading Biometric Authentication Scheme Based on Blockchain for Cross Domain Environment [J]. Wireless Personal Communications, 2022, 125: 599-618.

[50] BAO D, YOU L. Two-factor identity authentication scheme based on blockchain and fuzzy extractor[J]. Soft Computing, 2021, 27: 1091-1103.

[51] KUMAR M, PRASAD M, RAJU U. BMIAE: Blockchain-based Multi-instance Iris Authentication using Additive ElGamal Homomorphic Encryption [J]. IET Biometrics, 2020, 9(4): 165-177.

[52] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home [C]// Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Kona, HI, USA, 2017: 618-623.

[53] OUADDAH A, ELKALAM A A, OUAHMAN A A. FairAccess: a new Blockchain-based access control framework for the Internet of Things[J]. Security and Communication Networks, 2016, 9(18): 5943-5964.

[54] SHARMA R, CHAKRABORTY S. BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV[C]// Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps). Abu Dhabi, United Arab Emirates, 2018: 1-6.

[55] LI L, LIU J, CHENG L, et al. Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(7): 2204-2220.

[56] LUO B, LI X, WENG J, et al. Blockchain enabled trust-based location privacy protection scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2020, 69(2): 2034-2048.

[57] LIU X, HUANG H, XIAO F, et al. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs[J]. IEEE Internet of Things Journal, 2020, 7(5): 4101-4112.

[58] LU Z, WANG Q, QU G, et al. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs[J]. Very Large Scale Integration (VLSI) Systems, 2019, 27(2): 2792-2801.

[59] MA Z, ZHANG J, GUO Y, et al. An Efficient Decentralized Key Management Mechanism for VANET with Blockchain[J]. Vehicular Technology, 2020, 69(6): 5836-5849.

[60] LU Z, LIU W, WANG Q, et al. A Privacy-Preserving Trust Model Based on Blockchain for VANETs[J]. IEEE Access, 2018, 6: 45655-45664.

[61] CHENG L, LIU J, XU G, et al. SCTSC: A Semicentralized Traffic Signal Control Mode With Attribute-Based Blockchain in IoVs[J]. IEEE Transactions on Computational Social Systems, 2019, 6(6): 1373-1385.

[62] SINGH M, KIM S. Branch Based Blockchain Technology in Intelligent Vehicle[J]. Computer Networks, 2018, 145(9): 219-231.

[63] YANG Y T, CHOU L D, TSENG C W, et al. Blockchain-based traffic event validation and trust verification for vanets[J]. IEEE Access, 2019, 7: 30868-30877.

[64] TRIPATHI G, ABDUL A M, SATHIYANARAYANAN M. The Role of Blockchain in Internet of Vehicles (IoV): Issues, Challenges and Opportunities[C]// Proceedings of the 2019 International Conference on contemporary Computing and Informatics (IC3I). Singapore, 2019: 26-31.

[65] LI Y, GUO J W, DU L P, et al. Research on mobile terminal identity authentication scheme based on combined symmetric key algorithm [J]. Network Security Technology & Application, 2016, 1: 94-95.

[66] MA X, ZHAO F G. Mobile terminal multi source biometric real-time identity authentication system for mobile Intemet[J]. Video Engineering, 2017, 41(11): 162-166.

[67] FAN Y, XU J, GAO Y. Research and Implementation of eID-based Identity Authentication System [J]. Netinfo Security, 2015, 3: 48-53.

[68] CHEN Z, GAO D, WANG D, et al. Quantum Key Based Optimal Data Protection Model for Power Business[J]. Automation of Electric Power System, 2018, 42(11): 113-121.

[69] 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.

[70] MA X, MA W, LIU X. A Cross Domain Authentication Scheme Based on Blockchain Technology[J]. Acta Electronica Sinica, 2018, 46(11): 2571-2579.

[71] DONG G S, CHEN Y X, LI H W, et al. Cross-domain Authentication Credibility based on Blockchain in Heterogeneous Environment[J]. Communications Technology, 2019, 52(6): 1450-1460.

[72] GUO Y, MA W, LI X. Cross-domain authentication scheme based on tmst for server entity Systems[J]. Engineering and

Electronics,2019,41(2):438-443.

[73] WANG X,GAO F,ZHANG J,et al. Cross-domain Authentication Mechanism for Power Terminals Based on Blockchain and Credibility Evaluation[C]// Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS). Shanghai,China,2020:936-940.

[74] XIE Y R,MA W P,LUO W. New Cross-domain Authentication-Model for Information Servers Entity[J]. Computer Science, 2018,45(9):177-182.

[75] HUANG H,CHEN X. Power Mobile Terminal Identity Authentication Mechanism Based on Blockchain[C]// Proceedings of the 2020 International Wireless Communications and Mobile Computing(IWCMC). Limassol,Cyprus,2020:195-198.

[76] OMAR A,MUSTAFA A,CLUTTERBUCK,et al. The state of play of blockchain technology in the financial services sector:A systematic literature review[J]. International Journal of Information Management,2020,54:1-19.

[77] ASHARAF S,ADARSH S. Decentralized Computing using Blockchain Technologies and Smart Contracts[C]// Pennsylvania. USA:IGI Globa,2017.

[78] ABEYRATNE S A,MONFARED R. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger[J]. International Journal of Research in Engineering and Technology,2016,5(9): 1-10.

[79] TIAN F. An agri-food supply chain traceability system for China based on RFID & blockchain technology[C]// Proceedings of the 2016 13th International Conference on Service Systems and Service Management(ICSSSM). Kunming,China,2016:1-6.

[80] LU Q H,XU X W. Adaptable Blockchain-Based Systems:712-72 A Case Study for Product Traceability[J]. IEEE Software, 2017,34(6):21-27.

[81] AL-MEGREN S,ALSALAMAH S,ALTOAIMY,et al. Blockchain Use Cases in Digital Sectors:A Review of the Literature [C]// Proceedings of the 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,2018:1417-1424.

[82] MCGHIN T,CHOO K,LIU C Z,et al. Blockchain in healthcare applications:Research challenges and opportunities[J]. Journal of Network and Computer Applications,2019,135:62-75.

[83] JAVED I T,ALHARBI F,BELLAJ B,et al. Health-ID:A Blockchain-Based Decentralized Identity Management for Remote Healthcare[J]. Healthcare,2021,9(6):712-724.

[84] WANG W,WANG L,ZHANG P,et al. A privacy protection scheme for telemedicine diagnosis based on double blockchain [J]. Journal of Information Security and Applications,2021, 61(2):2214-2126.

[85] MAMUN Q,RANA M. A robust authentication model using multi-channel communication for eHealth systems to enhance privacy and security[C]// Proceedings of the 2017 8th IEEE Annual Information Technology,Electronics and Mobile Communication Conference(IEMCON). Vancouver, BC, Canada, 2017:255-260.

[86] KUMAR P,KUMARI S,SHARMA V,et al. A Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Network[J]. Sustainable Computing:Informatics and Systems, 2017,18(6):80-89.

[87] SHARMA N,BHATT R. Privacy Preservation in WSN for Healthcare Application[J]. Procedia Computer Science,2018, 132:1243-1252.

[88] RAY I,ALANGOT B,NAIR S,et al. Using Attribute-Based Access Control for Remote Healthcare Monitoring[C]// Proceedings of the 2017 Fourth International Conference on Software Defined Systems(SDS). Valencia,Spain,2017:137-142

[89] SHRESTHA N M,ALSADOON A,PRASAD P,et al. Enhanced e-health framework for security and privacy in healthcare system[C]// Proceedings of the 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC). Beirut,Lebanon,2016:75-79.

ZHANG Shue,born in 1964,master,associate professor. Her main research interests include data security and microwave technology and application.

LI Baogang,born in 1980,Ph.D,professor. His main research interests include wireless communication,blockchain,industrial Internet of Things,energy Internet and big data analysis.

(责任编辑:何杨)