计算机科学与探索
Journal of Frontiers of Computer Science and Technology doi: 10.3778/j.issn.1673-9418.2304003

基于 DID 的跨链身份认证研究综述

白伊瑞[1], 田宁[2,3], 雷虹[1,4+], 刘雪峰[5], 芦翔[6], 周勇[1]

1. 海南大学 网络空间安全学院（密码学院）, 海口 570228
2. 海南大学 计算机科学与技术学院, 海口 570228
3. 华威大学 制造学院, 英国 考文垂 CV4 8UW
4. 云海链控股股份有限公司, 海南 澄迈 571924
5. 西安电子科技大学 网络与信息安全学院，西安 710126
6. 中国科学院信息工程研究所，北京 100864

+ 通信作者 E-mail: leiluono1@163.com

摘 要：随着元宇宙和 Web3.0 等概念的出现，区块链在很多领域中发挥了非常重要的作用，区块链跨链技术是实现链间互联互通和价值转移的重要技术手段。在现阶段，公证人和侧链等传统的跨链技术存在信任问题，在一定程度上已经不适应数字经济的要求，同时，跨链身份认证领域中存在各链身份不统一以及身份不掌握在用户自己手中的问题。分布式数字身份（Decentralized Identity, DID）不依赖于集中式身份管理系统，在分布式场景下赋予每个用户独立控制和使用数字身份的能力，能有效解决跨链交易效率低的问题，还能够让身份完全掌握在用户自己手中，同时也打破了区块链之间的障碍，避免身份的重复认证。首先系统地总结了数字身份和跨链技术的发展历程、技术方案，并对主流项目进行分析比较，然后重点研究了跨链身份认证实现方案，通过对现有的身份认证实现方案进行分析和比较，总结了三种基于 DID 的跨链身份认证模型，并分析其优点、局限性和效率，最后对跨链在身份认证领域未来的研究方向进行展望。

关键词：分布式数字身份；区块链；跨链；身份认证

文献标志码：A **中图分类号：**TP309.2; TP39

Overview of Cross-chain Identity Authentication Based on DID

BAI Yirui[1], TIAN Ning[2,3], LEI Hong[1,4+], LIU Xuefeng[5], LU Xiang[6], ZHOU Yong[1]

1. School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China
2. School of Computer Science and Technology, Hainan University, Haikou 57228, China
3. School of Manufacturing, Warwick University, Coventry CV4 8UW, United Kingdom
4. SSC Holding Company Ltd., Chengmai 571924, China
5. School of Network and Information Security, Xidian University, Xi'an 710126, China
6. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100864, China

基金项目：国家重点研发计划项目（2021YFB2700600）；海南省重大科技计划项目（ZDKJ2020009）；国家自然科学基金（62163011）；海南大学科研启动基金项目（KYQD(ZR)-21071）。

This work was supported in part by the National Key R&D Program of China (2021YFB2700600); in part by the Finance Science and Technology Project of Hainan Province (ZDKJ2020009); in part by the National Natural Science Foundation of China (62163011); in part by the Research Startup Fund of Hainan University (KYQD(ZR)-21071).

Abstract: With the emergence of concepts such as Metaverse and Web3.0, blockchain plays a very important role in many fields. Cross-chain technology is an important technical means to realize interconnection and value transfer between chains. At this stage, traditional cross-chain technologies such as notary and sidechain have trust issues, and to a certain extent are not suitable for the requirements of the digital economy. At the same time, in the field of cross-chain identity authentication, there are problems that the identities of each chain are not unified and the identities are not in the hands of users themselves. Decentralized Identity (DID) does not relay on centralized identity management system, and gives each user the ability to control and use digital identity independently in a distributed scenario, which can effectively solves the problem of low efficiency of cross-chain transactions. It can also enable the identity to be completely in the hands of the user, and also breaks the barriers between blockchains and avoids repeated authentication of identities. Firstly, it systematically summarizes the development process and technical solutions of digital identity and cross-chain technology, and analyzes and compares mainstream projects. Then it focuses on the cross-chain identity authentication implementation scheme, and summarizes three DID-based cross-chain identity models by analyzing and comparing the existing identity implementation schemes, and analyzes their advantages, limitations and efficiency. Finally, the future research direction of cross-chain in the field of identity authentication is prospected.

Key words: Decentralized identity; Blockchain; Cross-chain; Identity authentication

随着区块链应用场景不断丰富和复杂化，区块链之间的数据流通、应用协同需求日益显现，区块链之间互通性的问题一直限制着区块链的应用空间，而跨链机制可以通过技术手段，将原本不同的、独立的区块链上的信息、价值进行交换和流通[1]。但跨链技术并不只是跨链数据转移，在联盟链以及私有链中，更关键的技术是处理在多链场景下对不同区块链系统的信任与身份验证问题。

通常情况下，每个用户在不同的区块链系统中都需要进行一次身份的注册，由于多场景下的业务需求往来，用户在多个区块链系统中会有多个注册账号，且各账号互不相连，身份并不互通，形成身份信息管理“孤岛”[2]。用户在跨链访问时需要进行交叉认证，在这种情况下存在用户身份隐私泄露的风险，并且带来了重复认证的额外运行开销[3]。现有的基于区块链的跨链身份认证方案大多将区块链与传统公钥基础设施（Public Key Infrastructure, PKI）技术结合，难以适应不同类型接入链的差异化身份认证需求。因此，对多种不同的区块链平台的互联互通提出了新的要求。

当前使用最广泛的跨链身份验证方法包括密码验证[4]和可信第三方验证[5]。这些传统的中心化的身份管理系统的优势在于实现简单，但存在如下问题：单点故障、安全性低、异构链用户身份认证难、系统间消息封闭互通难以及用户信息在各系统交互时隐私保护难等问题。因此，对跨链身份管理以及跨链隐私保护也提出了新的需求。

针对跨链账户体系中各链身份不统一以及身份不掌握在用户自己手中的问题，可以考虑使用分布式数字身份（Decentralized Identity, DID）作为统一身份标识符来实现跨链身份认证，使得用户身份可以完全掌握在用户自己手中，同时也打破了区块链之间的障碍，适应多个区块链的场景，在不同的区块链上实现 DID 的验证，避免了身份的重复认证。

此文的主要贡献如下：

(1)首先，按时间顺序总结了数字身份和跨链技术的发展历程，分析了不同数字身份模型的优缺点，并对 9 个具有代表性的跨链项目进行分析比较。

(2)其次，为确保只有授权的用户才能进行跨链互操作，需要验证用户身份，详细解释了目前跨链身份认证模型架构的组件以及通信流程，并对目前所提出的方案进行对比分析，最后总结了现有跨链身份认证方案存在的不足之处。

(3)最后，对 6 个具有代表性的基于 DID 的跨链身份认证方案进行对比分析，总结其优势与不足，在此基础上总结了三种基于 DID 的跨链身份认证

模型，并分析其效率和优缺点。最后从 5 个方面对跨链在身份认证领域中的研究方向进行展望。

1 DID 与跨链技术

1.1 DID

数字身份的发展经历了集中式身份[6]、联盟身份[7]、以用户为中心的身份[8]和自主主权身份（Self-Sovereign Identity, SSI）[9]的四个阶段，并逐渐从集中式向分布式发展[10]。表 1 总结了数字身份发展经历的四个阶段所产生的四个模型优缺点。中心化身份时代的标志是使用用户名和密码登录的所有网站，账户背后代表了一个真实存在的个体；联盟身份可以类比为 Facebook（Meta）、Instagram、Twitter、微信、支付宝的跨平台登录；以用户为中心的身份使得用户可以控制自己的身份；在 SSI 模型中，用户不仅可以控制身份还可以控制与之相关的数据。

图 1 按时间顺序对数字化身份发展做了梳理。

为了避免集中化带来的问题，数字身份正在向去中心化发展。基于身份提供者（Identity Provider, IdP）[11]的身份是一种集中式身份的优化方案。该方案在本质上是弱中心化的，仍然存在身份泄露和滥用的风险。为了使身份真正具有自主主权，其基础设施需要驻留在分散信任的环境中，而不是由任何单一组织拥有或控制[12]。区块链技术是实现这一目标的突破口。基于区块链技术的 SSI 允许用户真正拥有和控制自己的个人数据和资产，形成一个分布式的网络，具有保证数据真实性和有效性的特点。

SSI 与 DID 和可验证声明（Verifiable claim, VC）交互结合可以实现创建不可抵赖、且不可篡改的身份记录。DID 可提供全局唯一的分布式实体身份标识、可信数据交换协议，摆脱对传统模式下单一中心 ID 注册的依赖，这种去中心化的特性意味着用户的身份数据掌握在其自己手中，对于 DID 具有完全的控制权[13]。DID 通常与加密相关的内容（如公钥、服务端点）相关联，以建立安全通信通道。

表 1　四种数字身份模型比较

Table 1　Comparison of the characteristics of four models

模型	用户可以生成自己的标识符	用户可以控制自己的身份凭证	信息孤岛	密钥恢复	可选择性披露	支持假名	中心化存储
集中式身份[9]	×	×	×	√	×	×	√
联盟身份[10]	×	×	√	√	×	×	√
以用户为中心的身份[11]	×	√	×	×	×	×	×
SSI[12]	√	√	×	√	√	√	×

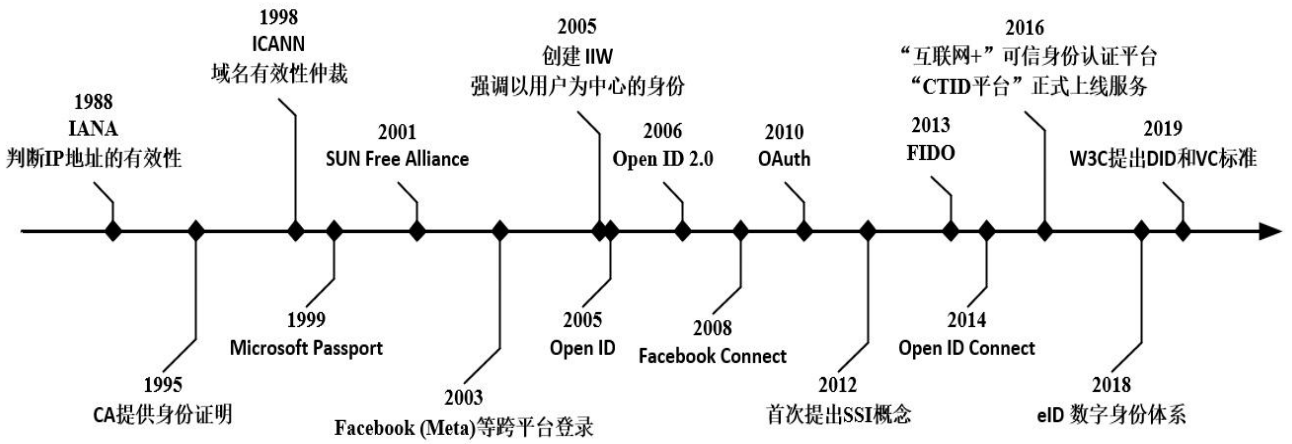

图 1　数字身份发展历程时间轴

Fig.1　Timeline of the development of digital identity

DID 通过使用生成具有足够熵的 128 位值的算法，使得碰撞的几率极小，也就是说产生两个相同的 DID 几乎是不可能的，因此可以实现唯一性的特点。Bryce Wilcox-O'Hearn[14]提出了 Zooko 三角形理论表明没有任何标识符能够同时实现人类可读、安全和去中心化，W3C 的 DID 选取了后两者，所以 DID 通常表现为“did: method: 123456abc”的形式。

如图 2 为 DID 标准示意图，DID 文档用于描述公钥、身份验证协议、服务端点等与身份实体进行密码验证交互所需的信息。DID 和 DID 文档本身不携带任何用户的个人身份信息，比如真实姓名、地址、手机号等，因此只靠 DID 是无法验证一个人的身份的，必须要靠 DID 应用层中的 VC。VC 提供了一种规范来描述实体所具有的某些属性，实现基于证据的信任[15]。同时，结合数字签名和零知识证明等密码学技术[16]，可以进一步保障用户隐私不被侵犯。数字签名通常使用 DID 的私钥对消息进行签名，并使用 DID 文档中存储的公钥进行验证。使用零知识证明可以在不泄露任何个人信息的情况下验证身份，用户的证据（witness）需要与特定的 DID 相关联[17]，例如用户的私钥或姓名等其它用户身份相关信息，以确保证明者可以验证用户的身份。

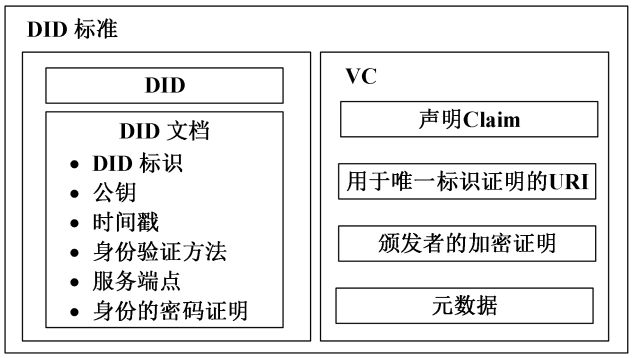

图 2 DID 标准示意图

Fig.2 DID standard diagram

在更深的层次上，DID 是去中心化公钥基础设施（Decentralized Public Key Infrastructure, DPKI）的核心组件。DID 基础设施可以被视为一个全球化的 Key Value 数据库，Key 是 DID，Value 是 DID 文档。它可以是一个区块链、分布式账本或与所有 DID 兼容的分布式网络[18]。Alexander Mühle 等人[19]提出了典型 DID 基础设施中 VC 应用层的不同组件之间的关系，不同参与者之间的关系如图 3 所示。Issuer 是拥有用户数据并能开具 VC 的实体，与 IdP 不同的是 Issuer 不代替用户管理证书。Verifier 是需要验证服务提供者（Service Provider，SP）。Holder 一般为用户或用户的身份代理，可以向 Issuer 请求、收到、持有 VC 的实体，Holder 将开具的 VC 放在其个人存储库里，方便以后再次使用。Identifier Registry 主要用于维护 DIDs 的数据库，如某条区块链、分布式账本。

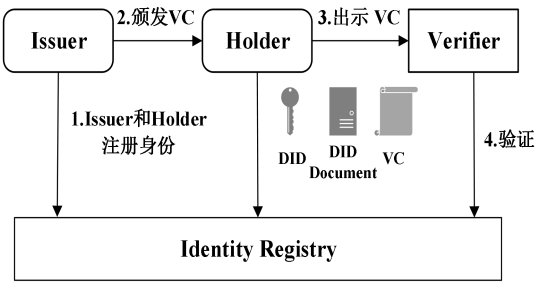

图 3 DID 基础设施交互图

Fig.3 DID infrastructure interaction

在整个 Web 3.0 的图景中，DID 是非常重要的实践，可以契合非同质化代币（Non-Fungible Token, NFT）、元宇宙、去中心化金融（Decentralized Finance, DeFi）、集中式去中心化金融（Centralized Decentralized Finance, CeDeFi）等新兴产业模式[20]，可以解决一些当前 Web 3.0 的痛点。例如，采用 DID 和 VC 来确定 NFT[21]的归属权能有效解决困扰艺术家和创作者的欺诈和抄袭问题，将 NFT 的所有权限制在社区成员手中来限制黄牛的投机行为，同时买家和卖家也能够验证数字艺术品的来源。

1.2 主流跨链技术及项目

两条链是相互独立的系统，发起跨链交易的时候，需要一个“中间人”的角色，承担两条链的信息交互，才能完成对双方的交易确认[22]。按时间顺序总结的跨链技术的发展过程如图 4 所示。当前一些主流的跨链技术有：公证人机制、哈希锁定、侧链、中继和分布式私钥控制。

(1) 公证人机制。该机制引入了一个或多个受信任的实体，即公证人来做信用背书，负责监听链

上的事件并在另一个链上采取相应的操作，实现原理简单且无需复杂工作量证明，但有中心化风险，需要对公证人有足够的信任。根据实施过程中签名方式的不同，公证人机制主要包括三种类型：单签名公证人、多签名公证人、分布式签名公证人[23]。

(2) 哈希时间锁机制。该机制通过资产锁定并设置相应的时间和解锁条件来实现资产交换，可以在没有第三方参与的情况下保证不同链之间资产交易的安全性和原子性[24]。该机制安全性高，缺点是使用场景有限，只支持资产或者信息交换而不支持资产或者信息转移。

(3) 侧链机制。Adam 等人[25]提出了侧链，其原理是将数字货币在主链中锁定，同时将等价的数字资产在侧链中释放[26]。Plasma[27]作为一种以太坊扩容方案，通过将大量交易和计算下放到侧链来提高以太坊主链可扩展性。RSK（Rootstock）[28]将一个图灵完备虚拟机合并到比特币中，提高了网络的性能。每条侧链都有实现自己的身份管理和加密算法的主权[29]。

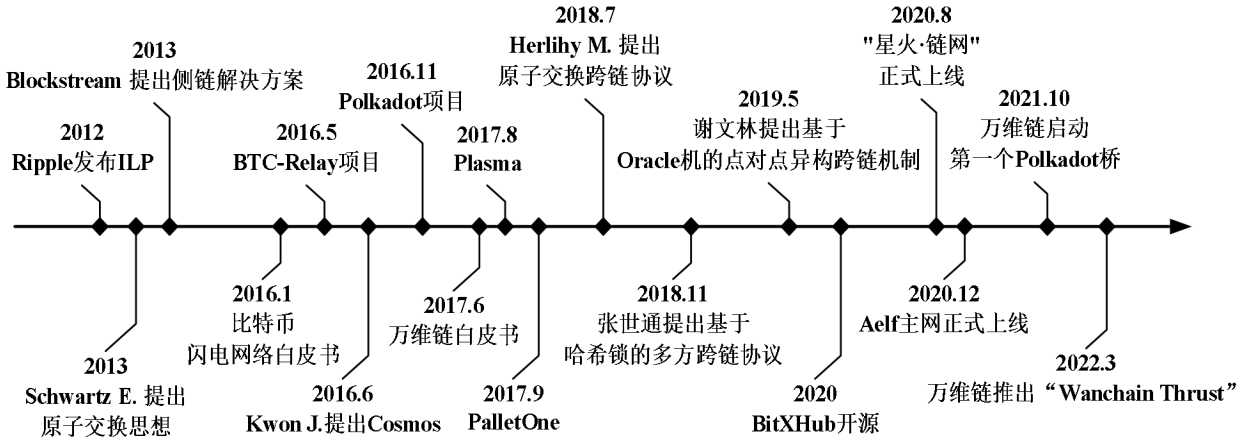

图 4　跨链技术发展历程

Fig.4　Development history of cross-chain technology

(4) 中继机制。中继机制不完全依赖于可信第三方的验证判断，仅通过中间人收集不同链的数据状态进行自我验证并完成交易确认[30]。目前最活跃的跨链项目是 Kwon 等提出的网络架构 Cosmos[31] 和 Wood G.等提出的 Polkadot[32]，采用的都是基于中继链的多链多层架构，其中 Cosmos 目前支持的是跨链资产交互，而 Polkadot 则宣称支持不同共识系统之间去中心化和无信任的跨链交互。中继机制具有很高的扩展性，是当前最被广泛应用的跨链方案，但仍需要考虑接入链授权的安全性问题[33]。

(5) 分布式私钥控制机制。该机制使用分布式私钥的生成与控制来实现将多种不同区块链的数字资产映射到一条新的区块链上，并在这条新的区块链上实现不同链之间的数字资产交换[34]。此机制使用场景有限，目前只应用于数字资产领域。

从跨链技术、共识机制、安全性和局限性 4 个方面对 9 个具有代表性的跨链项目进行分析比较，如表 2 所示。这些跨链项目采用的跨链机制不同，所以每个跨链项目的特点也不同。从比较结果中可以知道，单个跨链项目可能涉及到本节提到的多个跨链机制的综合应用。例如，ILP（Interledger Protocal）采用公证人和哈希锁机制[35]。此外，一些项目使用通信协议套件作为跨链机制。例如 Cosmos 在跨链过程中会通过 IBC（Inter-Blockchain Communication）协议将资产锁定在区块链上，然后将证书发送给目标区块链，因此目标区块链会相应地创建一个与被锁定资产等价的资产，但也增加了实现的难度。

在安全性方面，目前主流跨链技术的安全性有待进一步加强；在应用场景方面，哈希锁定机制的应用场景比较有限，仅支持实现资产的跨链交换。总之，目前同一应用场景下可采用多种跨链技术，此时需要将跨链技术的技术原理与应用背景结合，选择最合适的跨链技术去解决实际应用问题[37]。

表 2 跨链项目对比

Table 2 Cross-chain project comparison

项目	跨链技术	共识机制	安全性	局限性
ILP[35]	公证人和哈希锁定	托管机制	公证人互信机制	依赖第三方公证人
Lighting Network[36]	哈希锁定	哈希算法	哈希算法	应用场景单一；不支持多链互连
Plasma[27]	侧链	PoS	Merkle 证明	交易速度慢
RSK[28]	侧链	PoW	基于 SHA256 工作证明保护	依赖名为“联邦”的公证性质的组织
Cosmos[31]	中继	改进的 PoS 方法	链间安全性	实现难度大
Polkadot[32]	中继	NPOS, BABE, GRANDPA 混合共识	多个有效性检查	中心化挖矿的风险
WeCross[38]	中继	Merkle 证明	Merkle 证明	新攻击媒介产生
Fusion[39]	分布式私钥控制	分布式私钥与门限签名	多签名算法	智能合约功能有待完善
Wanchain[14]	分布式私钥控制	星系共识—PoS 机制	门限签名	应用场景单一；面向金融市场

2 跨链身份认证方案

2.1 研究现状

传统的身份认证协议大多以集中式认证为主，需要可信第三方，数字身份通常是由集中的机构颁发的，会存在身份数据分散和冗余认证[40]、用户对个人身份数据没有控制权、中心化基础设施维护成本高等问题。由此可见传统集中式认证方案已不再适合当今的应用需求。区块链作为一种以密码学为基础的分布式账本，具有去中心化、可溯源、不可篡改的特性，可提供分布式的可信服务，为解决传统方案的安全问题提供了新的途径[41]。

基于区块链的去中心化用户身份识别是当前研究的新方向，一些研究学者提出了可能的解决思路。董贵山等人[42]提出了一种基于区块链的异构身份联盟与监管体系方案，但该方案并未实现跨区块链的身份管理。邓小鸿等人[43]提出一种基于区块链的身份认证模型采用椭圆曲线签名算法进行登录验证，但此模型不能很好地应对实际应用可能会有高并发的请求问题。Yoon 等人[44]提出一种基于区块链证书方案的跨域身份认证模型，通过用户授权证书授权机构（Certificate Authority, CA）的哈希值与区块链中存储的哈希值的一致性进行跨域认证。Wang[45]等人提出一种基于区块链的跨域身份认证机制，可以在不同的域中进行身份认证和信任建立。

从上述研究内容可以看出，目前研究内容主要是采用单个区块链解决传统中心化的用户身份管理问题，对跨链用户身份管理的研究较少。

针对当前在不同独立的区块链之间进行身份认证的问题，一些研究人员[46-51]也提出了一些跨链身份认证的解决方案，方案对比见表 3，包括杨淳等[46]提出的异构身份联盟统一身份信息标识模型、陈武阳等[47]提出的可添加身份属性的高效跨链认证方案、Shao 等[48]提出的基于身份的物联网区块链跨链通信机制、王洒洒等人[49]提出的面向跨链系统的用户身份标识认证模型、Li 等[50]提出的改进的 MACT（Multi-channel Anonymous Consensus based on Tor）分布式账本和雷志伟等[51]提出的基于中继链的跨链平台等。这些方案采用了不同的技术手段，如全局统一身份标识、PKI 认证服务、IBE（Identity-Based Encryption）机制、椭圆曲线加密算法和零知识证明等，来处理不同方面的跨链身份认证问题。

2.2 跨链身份认证模型架构

目前实现的跨链身份认证方案主要使用基于 OAuth2 和 OpenID Connect 的身份认证协议以实现跨链身份认证。例如，在 Cosmos、Polkadot 中使用此身份认证协议，用户可以通过身份认证中心注册和管理身份标识，并使用身份认证证书进行跨链身份认证。

表 3　跨链身份认证方案对比

Table 3　Cross-chain identity authentication comparison

文献	方法描述	优点	局限性
杨淳等[46]	通过全局统一身份标识 UID 实现与各个接入联盟链的身份关联。	互操作性强，可以结合用户的操作记录，得出可信评价值。	依赖于全局统一身份标识 UID，没有考虑 UID 的安全性和管理问题。
陈武阳等[47]	用户仅需证书以及服务授权票据即可实现同第三方服务提供商之间的安全认证。	减少了身份的重复认证带来的资源浪费，提高了身份利用率。	服务授权票据需要得到保护，避免被非法使用。
Shao 等[48]	跨链公证人通过 IBE 机制计算出相应的私钥，并以安全的方式返回给代理节点。	通过选择代理节点，提高了跨链通信的效率和安全性。	选择代理节点的过程需要考虑节点的可信度和分布情况
王洒洒等[49]	引入椭圆曲线加密算法和零知识证明，实现跨链身份标识注册、更新以及认证。	零知识证明可保护用户隐私信息不被泄露	没有解决跨链身份标识的管理和维护问题
Li 等[50]	基于改进的 Keberos 协议设计了一套身份认证机制，完全独立于第三方公钥基础设施。	一定程度上降低了拜占庭节点的出现概率	对于拜占庭节点的处理仍然需要进一步研究
雷志伟等[51]	基于中继链跨链平台的基础上引入监管链，并将监管链分为账户信息链和交易信息链。	安全性强，提高了交易的监管性和隐私保护。	跨链事务管理需要解决跨链一致性和可靠性问题

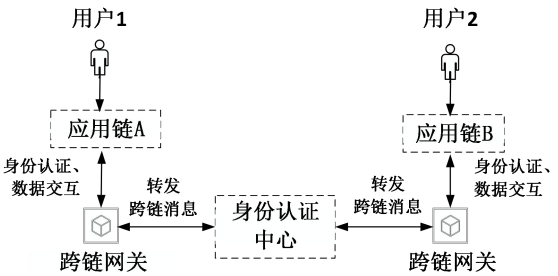

图 5　跨链通信流程

Fig.5　Cross-chain communication flow

目前主流跨链身份认证通用模型如图 5 所示，该跨链网络模型主要角色组成有三个：身份认证中心、应用链与跨链网关。

(1) 身份认证中心。负责处理跨链身份认证请求，提供身份认证服务，包括身份标识的注册、管理和验证等。身份认证中心还需要提供身份认证证书的颁发和管理服务。身份认证证书是用于验证用户身份的数字证书，包括用户身份标识信息、身份认证中心的签名和有效期等信息。

(2) 应用链。应用链是目前市面上已经投入使用的，需要参与跨链交互的区块链平台，在满足身份认证的基础上，应用链可以和跨链网络中其他应用链进行跨链交互。

(3) 跨链网关。跨链网关是连接不同区块链系统的桥梁，可以将不同区块链系统之间的数据进行转换和交换，需要支持身份认证协议，以实现用户身份的跨链认证。

图 5 所示的跨链通信流程如下：

(1) 用户 1 发起跨链身份认证请求，提供自己的身份标识和其他必要的认证信息，调用应用链 A 的合约方法，合约方法被执行后抛出跨链事件 Ta；

(2) 应用链 A 的跨链网关 A 监听到 Ta，将其转换成跨链消息，提交到身份注册中心；

(3) 身份注册中心依据相关规则对 Ta 进行验证，验证成功后，颁发身份认证证书给用户，并进行路由转发将消息发给跨链网关 B；

(4) 跨链网关 B 接收到事件 Ta 并根据跨链消息进行解析，转换成应用链 B 可识别的交易 Tb，并将 Tb 提交到应用链 B 上进行执行。

2.3　存在的问题

现有的跨链身份认证方案存在以下缺点：

首先，现有的身份认证方案大多将区块链与传统 PKI 技术结合，难以适应不同类型接入链的差异化身份认证需求；

第二，基于中继链的 IBE 的跨链身份认证方案虽解决了数据孤岛问题，但 IBE 认证机制存在硬件投入大，并且认证运算复杂、效率低的问题，不适用于海量用户链安全接入；

第三，安全性问题。现有的跨链身份认证方案中存在一些安全风险，如身份信息泄露、身份伪造等问题。例如，一些跨链身份认证方案中使用基于 OAuth2 和 OpenID Connect 的身份认证协议，但这些协议本身也存在一些安全问题，如中间人攻击和

令牌劫持等。

第四，不同的应用链安全性有差异，会涉及到不同接入链的跨链授权问题，确保授权操作的可靠性和安全性，以保护整个跨链网络的安全。

第五，跨链身份认证方案需要管理跨链身份信息，包括身份注册、更新、认证和撤销等操作。在不同的应用链中，需要确保跨链身份信息的一致性和完整性，以避免身份信息的冲突和错误。

3 基于 DID 的跨链身份认证

3.1 基于 DID 的跨链身份认证方案

DID 可以解决跨链账户体系中各链身份不统一以及身份不掌握在用户自己手中的问题。DID 通过区块链技术提供可信的身份，并提供基于 VC 的完整身份验证方法，解决了传统集中式身份的问题，使得用户身份可以完全掌握在用户自己手中。

现有的 DID 验证方法是成熟可行的，但模型存在一定的局限性。目前实现的方法可以在单个区块链上工作，但在区块链网络中工作效果不好，因为不同的 DID 及其身份信息存储在不同的区块链上，而区块链之间的通信和连接是孤立的，这导致了区块链网络中互操作性的局限性和 DID 验证的困难。因此，迫切需要打破区块链之间网络隔离造成的障碍，实现对不同区块链上的 DID 的验证。一些研究者提出了基于 DID 的跨链验证模型[52-56]。

王姝爽等人[52]提出一种基于中继链的 IBE 的跨链身份认证方案，使用 DID 作为跨链身份认证的统一标识符，并使用智能合约来验证跨链身份认证的有效性和安全性。同时采用安全密钥协商策略，对进行跨链交易的两条链进行交易信息加密传输，保障跨链交易的隐私安全性。该方案解决了现有跨链模型中的安全性和数据孤岛问题，更适用于复杂动态的跨链网络环境，但该方案没有考虑到跨链通信的权限问题，并且 IBE 存在效率低的问题，不适合大量用户接入。

Chao 等人[53]设计了账本数据代理层，利用 DID 和星际文件系统（InterPlanetary File System，IPFS）实现了不同链上用户之间的数据访问和通信，以解决现有通信技术高度集中导致的单点故障和安全管理与控制问题。该方案有效地打破了信息壁垒，增强了数据流。从实验结果来看，该系统的在稳定性方面表现较好，在访问增加的情况下，可以保持较于其他系统更优越的稳定性。

表 4 基于 DID 的跨链身份认证方案对比

Table 4 Comparison of cross-chain identity authentication schemes based on DID

文献	特点	优势	不足	效率
王姝爽等[52]	提出基于中继链的 IBE 的跨链身份认证方案，通过安全密钥协商保障跨链交易的隐私安全性。	可行性高、安全性高，更适用于复杂动态的跨链网络环境。	没有考虑权限控制问题，并且不适合海量用户接入。	$O(n)$
Chao 等[53]	利用 DID 和 IPFS 实现了不同链上用户之间的数据访问和通信。	TCP/IP 协议与 BNS 融合，可以抵抗消耗服务器资源的攻击。	不能保证资产交换的安全可靠。	$O(n\log(n))$
Wang 等[54]	提出基于 DID 的跨链统一数字身份系统，并在后续节点自动多重签名的基础上实现了资产的安全交换方法。	跨链身份验证效率高；同时保证资产交换的安全可靠。	可扩展性低	$O(n)$
Xie 等[55]	基于跨链通道的 DID（C3-DID）模型，实现 DID 的分布式存储，并允许基于中继的跨链数据交换。	建立了权限链通道以实现跨链数据交换，安全性高。	应用场景受限	$O(n)$
Zhong 等[56]	构建信用评估体系统一描述 DID 的可信度，并部署智能合约实现 DID 的跨链验证。	跨链 DID 验证延迟低；性能高。	安全性低，跨链交互依赖智能合约。	$O(n)$
Zhao 等[57]	使用智能合约实现动态访问控制策略，IPFS 中的电子病例哈希地址与患者 DID 一起存储在区块链中。	跨链身份和信息的隐私保护；链上存储开销小。	性能受读写操作的数量影响较大	$O(n^2)$

Wang 等人[54]结合 DID 和 VC，提出了一种基于 DID 的跨链统一数字身份系统以及基于中继链中中继节点自动保管的多签名资产管理方法，实现了用户链的跨链身份认证，保证了跨链过程中身份的可控共享和相互认证。该模型实现了跨链资产交换证书的规范化，提高整个跨链资产交换的去中心化，保证资产交换的安全可靠，但应用链接入成本较大，有可扩展性不高的问题。

针对金融贷款中抵押物的身份认证问题，Xie 等人[55]提出基于跨链通道的 DID 模型，实现 DID 的分布式存储，并允许基于中继的跨链数据交换。这种机制可以帮助贷款机构更快地验证借款人的身份信息，从而提高抵押贷款的效率。该模型在两个 Tendermint 开发的联盟链上分别部署贷款流程和身份验证流程。此外，还建立了权限链通道，称为点对点匹配通道（Match Channel, MC），以实现跨链数据交换。该模型的安全性较高，但是应用场景有限，仅适用于金融贷款中抵押物的身份认证。

Zhong 等人[56]提出了一种对 DID 进行跨链验证的模型，可以对不同区块链上的 DID 信息进行相互验证。该模型构建信用评估体系，统一描述可验证声明的可信度，并部署智能合约实现 DID 的跨链验证。与单链相比，跨链机制可以增强区块链的联动，提供足够的互操作性，且性能损失很小。

Zhao 等人[57]提出了一种医疗数据共享的跨链访问控制模型，设计了基于身份和角色的访问控制算法，使用 QR（Quick Response）码来获取 DID，通过智能合约的权限控制分离读写权限，保证了医疗数据源的真实性。同时，采用 IPFS 为医疗数据的存储系统，减少了链上的存储开销。

将 6 个具有代表性的基于 DID 的跨链身份认证方案进行对比分析，如表 4 所示。这些方案采用的方法不同，因此每个方案的特点也不同。从比较结果中可以得出的结论：多数跨链身份认证方案采用中继跨链机制，相比于其他跨链技术，中继方案更加灵活且易于扩展。虽然使用区块链作为跨链认证的中继会增加一定的时间复杂度和交互成本，但是，文献[52]使用基于 IBE 的高效身份认证策略，文献[55]设计的 DID 生成算法的每个过程都是在一个常数时间内完成的，可以减少身份认证的时间和成本，因此，其时间复杂度均为 O(n)。利用 IPFS 可以实现链外可信存储，但 IPFS 进行 DID 文档的存储和传输时，其带宽和存储能力会直接影响方案的效率和时间复杂度，文献[53]提出的身份验证算法中的 call 操作会调用另一个合约，受此影响其时间复杂度为 $O(n\log(n))$，文献[57]设计的身份识别访问控制算法，包括角色权限的授权和撤销，时间复杂度为 $O(n^2)$。文献[54]的方案确保了资产交换的安全性和可靠性，但存在应用链接入成本高，可扩展性低的问题。Zhong 等人[56]创建了可验证 claim 的统一数据结构，而不是由不同 DID 原型生成的异构 VC，提出的算法时间复杂度为 O(n)，因为算法中的 for 循环操作会遍历 SIGNERS 中的所有签名者，每个签名者会执行一次 if 操作。该方案的验证延迟较低，有更好的互操作性，但跨链交互完全依赖智能合约，容易受到攻击，所以其安全性较低。

3.2 基于 DID 的跨链身份认证模型

在 3.1 节提出基于 DID 的跨链身份认证方案之后，对其身份认证模型进行了总结。本节介绍 3 种基于 DID 的跨链身份认证模型，分别是基于中继链和 DID 的跨链身份认证模型，基于 IPFS 和 DID 的跨链身份认证模型以及基于智能合约和 DID 的跨链身份认证模型，并对 3 种模型进行对比，如表 5 所示。

3.2.1 基于中继链和 DID 的跨链身份认证模型

目前实现的基于 DID 的跨链身份认证方案大多采用以中继链为中心的交互模型架构[52, 54-55]，该模型通过引入中继链来实现不同区块链之间的信息传递和身份认证，如图 6 所示，具体实现步骤如下。

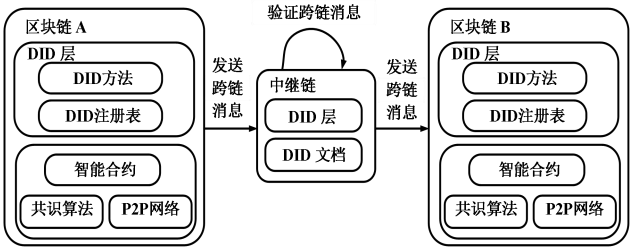

图 6　基于中继链和 DID 的跨链模型

Fig.6　Cross-chain identity authentication model based on relay chain and DID

首先，用户在区块链 A 上创建自己的 DID 标识，并在中继链上注册对应的 DID 标识。

然后，当实体需要进行跨链身份认证时，它会向目标区块链发送一个身份认证请求，请求被转发到中继链。中继链维护需要跨链的所有数字身份 DID 元数据和完整描述信息 DID 文档，是跨链系统的核心，统筹管理跨链事务。

接着，中继链使用 DID 标识和身份信息，采用 IBC 技术[52]、多重签名验证[54]以及数字签名[55]进行身份认证。这些身份认证方法可以保障跨链请求的身份信息的真实性和可信度，提高跨链身份认证的安全性和可靠性。

最后，如果身份认证通过，中继链再将结果和跨链消息发送给目标区块链 B。

用户有唯一的标识符 DID，但 DID 文档里可以包含多个公钥信息，这些公钥信息可以是用户在不同的区块链中的公钥信息，提高了 DID 的可扩展性。例如，用户可以在 DID 文档中包含多个公钥，以便在不同的场景和应用中使用不同的加密算法和密钥对。

整个模型设计运用“以链治链”思想，整个跨链网络可以保证去中心化或者弱中心化，具有较高的安全性和可扩展性，但是引入中继链会增加系统的复杂性，由于不同的区块链之间可能采用不同的协议和技术标准，中继链需要对这些不同的协议进行兼容，才能够实现跨链通信和资产转移。例如，在此模型方案中，中继链需要同时兼容不同区块链上的 DID 标识和身份验证机制，以便能够实现跨链身份认证。中继链还需要兼容不同区块链之间的数字签名和交易验证协议，以确保跨链交易的安全性和可靠性。

3.2.2 基于 IPFS 和 DID 的跨链身份认证模型

该模型利用 IPFS 提供的分布式文件存储和传输能力，结合 DID 提供的去中心化身份标识机制，实现了跨链身份认证[53]，如图 7 所示，具体实现步骤如下。

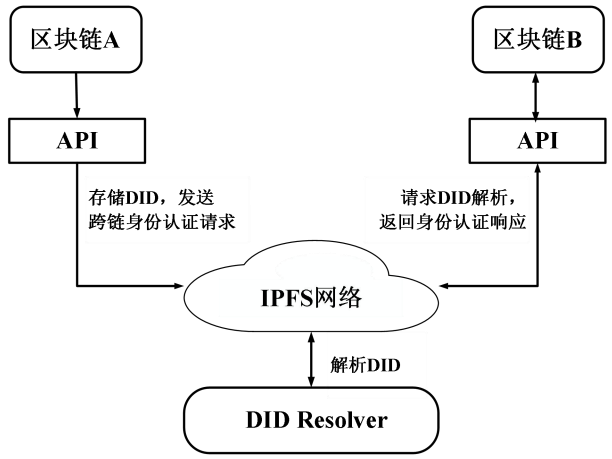

图 7 基于 IPFS 和 DID 的跨链模型

Fig.7 Cross-chain identity authentication model based on IPFS and DID

首先，创建 DID 标识。区块链 A 上的用户在区块链 A 上创建自己的 DID 标识，并将其存储在 IPFS 网络中[57]。

然后，发起跨链身份认证请求。当用户需要进行跨链身份认证时，向目标区块链 B 发送一个跨链身份认证请求，并提供自己的 DID 标识和相应的证明信息。跨链身份认证请求被转换为一个 IPFS 对象，并存储在 IPFS 网络中。

接着，解析和验证 DID。区块链 B 使用 DID Resolver 从 IPFS 网络中获取用户的 DID 文档，并验证其真实性和有效性。DID Resolver 是一个用于解析和验证 DID 标识的工具，它可以从 IPFS 网络中获取 DID 文档，并验证其中包含的公钥和其他身份信息。

最后，验证身份信息。区块链 B 使用 DID 文档中包含的公钥对用户提供的证明信息进行验证，以确认用户的身份信息是否真实有效。如果验证成功，则目标区块链会向用户发出跨链身份认证成功的响应。用户收到跨链身份认证成功的响应后，即可在目标区块链上进行相应的操作和交易。跨链身份认证完成后，IPFS 对象会被删除，以保护用户的隐私和安全。

总体来说，该模型的主要优势在于为多个区块链之间的身份认证提供支持的同时，还可以保护用户的身份隐私和安全性，具有很高的实用性和可行

性。但由于跨链身份认证请求需要通过 IPFS 网络进行传输和存储，存在无法实现即时跨链身份认证、性能依赖 IPFS 网络的稳定性等问题，如果 IPFS 网络出现故障或不稳定，可能会导致跨链身份认证失败或延迟。

3.2.3 基于智能合约和 DID 的跨链身份认证模型

通过智能合约的管理[56]，该模型可以确保身份认证信息的安全性和可靠性，实现不同区块链之间身份认证信息共享和互通的模型，如图 8 所示，具体实现步骤如下。

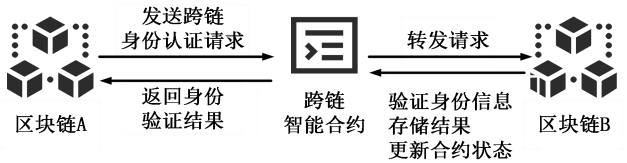

图 8　基于智能合约和 DID 的跨链模型

Fig.8　Cross-chain identity authentication model based on smart contracts and DID

表 5　基于 DID 的跨链身份认证模型对比

Table 5　Comparison of cross-chain identity authentication models based on DID

相关文献	模型类别	优势	局限性
[52，54，55]	基于中继链和 DID 的跨链身份认证模型	可扩展性较强；可确保跨链交互的稳定性和安全性；支持多种跨链交互功能。	中继链需主动兼容；依赖于中继链的稳定性和安全性。
[53，57]	基于 IPFS 和 DID 的跨链身份认证模型	实现简单；支持多种不同的数据类型交互，满足不同类型应用的需求。	依赖 IPFS 网络的稳定性；需要使用 DID resolver；无法实现即时跨链身份认证。
[56]	基于智能合约和 DID 的跨链身份认证模型	可扩展性强；灵活性高。	存储限制；智能合约执行影响网络性能。

首先，用户在区块链上创建自己的 DID 标识，并将其存储在该区块链上。

然后，用户通过将跨链身份认证请求信息存储到智能合约中，并触发智能合约的执行，发送到目标区块链 B。智能合约会根据预设的规则和逻辑，将身份认证信息发送到区块链 B，并等待响应。区块链 B 收到信息后，开始验证 DID 和身份信息，并将验证结果通过智能合约的状态变量或事件来存储到智能合约中。验证包括检查 DID 是否合法、DID 是否存在、DID 是否被篡改等，检查身份信息的正确性和真实性等。

最后，如果身份认证通过，触发跨链智能合约根据预设的规则和逻辑将身份验证结果返回给源区块链 A。如果用户在多个区块链上进行身份认证，每个区块链都会记录该用户的 DID 标识和身份认证状态，这些信息可以通过智能合约进行共享和互通。

在此模型中，智能合约的状态变量可以用来存储用户的身份信息和验证结果。例如，可以定义一个名为"identityInfo"的状态变量，存储用户的 DID 标识信息，或者定义一个名为"authenticationResult"的状态变量，存储身份验证结果。除了状态变量，智能合约还可以使用事件来记录身份认证信息的变化和验证结果。事件是智能合约中的一种特殊数据类型，可以用来记录某个事件的发生。在此模型中，可以定义一个名为"IdentityVerified"的事件，用来记录身份验证结果。例如，当一个用户的身份验证通过时，智能合约可以触发"IdentityVerified"事件，并将验证结果作为事件参数来记录。

基于智能合约和 DID 的跨链身份认证模型可以通过智能合约的编写和部署来扩展功能，易于扩展，可以根据不同的业务需求和应用场景进行定制。并且，该模型不依赖于中继链、IPFS 等工具，可以在不同的区块链平台上实现，灵活性与前两种模型相比有很大的提升。但由于智能合约的执行需要消耗一定的计算资源，可能会对网络性能和响应时间产生一定的影响。该模型需要用户将 DID 相关信息存储在区块链上，随着用户大量的增加，存储的数

据量也会越来越大，可能会超出某些区块链的存储限制，从而导致存储限制问题。

4 讨论

4.1 发展难点

目前已经实现的基于 DID 的跨链身份认证模型尽管解决了异构链互联互通和信任的问题，但仍在监管、发行者颁发数字证书方面存在安全性漏洞，还需考虑跨链中间件的兼容难度和适配性。下面将解释在构建可行且有效的基于 DID 跨链身份认证模型过程中面临的一些挑战。

(1) 监管

区块链由于其本身的设计机制以及针对智能合约和共识算法等的恶意攻击，存在很多安全漏洞，可能会引发双花攻击、密钥泄漏、拒绝服务（Denial-of-Service，DoS）攻击等问题[58]。此外，监管机构需要制定相应的法律和政策来规范数字身份的使用和管理，例如，在身份验证时可能涉及个人身份隐私信息，需要建立相应的数据隐私保护机制，采取措施确保个人身份信息不受到非法访问、篡改、泄露和滥用。

为解决区块链系统的安全问题，设置监管系统对智能合约进行安全性检测；采取数据加密、访问控制等隐私保护措施对个人身份信息进行隐私保护；采用模拟攻击、压力测试等方式，检测共识算法的安全性和可靠性；对密钥管理进行监测，采用加密存储、密钥轮换、密钥备份等方式，确保密钥的安全和不被泄露；系统漏洞监测可以采用安全漏洞扫描、漏洞分析、代码审计等方式，及时发现系统中的漏洞和隐患[59]。在多链互联的状况下，监管系统在智能合约、共识算法、数据隐私保护、密钥管理和系统漏洞监测多方面为不同区块链系统提供监管检测服务。

(2) 证书管理

传统的可验证凭证为 DID 提供了一种可信任的验证模式。但是，不同的组织为不同的 DID 颁发不同的凭据，由于凭证是异构的，不利于跨组织协作[60]。所以，需要为不同区块链的 DID 采用统一的数据结构，以标准化的方式描述不同发行人的 DID。此外，证书需要及时验证和撤销，以保证数字身份的安全和可靠性，避免证书被滥用和泄露。

(3) 兼容难度和适配度

基于 DID 的跨链身份认证模型的兼容难度和适配度主要受到区块链系统的兼容性和跨链交互中间件主动兼容性的影响。不同区块链系统之间的协议可能不同，这可能导致它们之间的数据交换和交互存在一定的兼容难度。中继链作为一个中间层，需要主动兼容不同的区块链系统，考虑不同区块链系统的特点和差异性，从而设计出符合不同区块链系统需求的兼容性协议[61]。中继链主动兼容的难度与兼容性协议的设计复杂度相关，此外，实现协议转换和数据格式转换也是中继链主动兼容的难点。

4.2 展望

针对当前基于 DID 的跨链身份认证模型的不足，提出以下四点未来研究方向：

(1) 可以考虑引入智能合约来完成更复杂的跨链身份访问控制，使得中继节点可以提供身份认证、权限分配、访问控制等功能，给不同的用户组授予不同的权限，帮助用户安全地控制资源的访问。

将同一个智能合约的代码部署到多条区块链上还是会存在一系列特殊的挑战及问题。由于智能合约的代码每部署到一个新的区块链上，都需要创建一份原应用的副本，导致不同链上的用户体验不能保证完全一样。所以，为了安全地跨链传输数据，也就是在各个链上环境之间传输任意数据、通证和指令，需要采用一种全新的思路来设计智能合约的基础架构，让信息和数据以可信、可验证的方式在多个区块链上流通。同时，通过对接入链身份进行分级，保证跨链操作的安全性。

(2) 如何在跨链身份认证过程中更好地验证彼此身份的合法性和有效性，可以作为未来的研究方向之一。

身份认证对系统安全性有着极为重要的影响。每个链内可能都存在一套本链身份管理机制，在这种情况下，用户在不同链交互时需要进行交叉认证，

实现跨链互联。因此，设计不同链间合理高效的用户身份管理和认证机制是未来研究的重点。

此方向主要解决的问题是跨链信息的真实性证明和有效性证明，即该信息是否确实是 A 链用户发送给 B 链的，保证消息的时效性和完整性。此目的主要是确认用户是否是本人在传递消息或此用户身份是否过期，防止伪造和假冒等情况发生。

(3) 跨链技术存在安全漏洞，在信任模型上还有较大的提升空间。

在进行跨链操作的过程中会面临很多安全问题，跨链技术本身存在的安全漏洞，包括跨链的技术原理与实现机制本身存在的安全性缺陷，都会对跨链系统带来不安全影响。

在跨链过程中会存在非授权使用、跨链重放等安全问题。在跨链的过程中，A 链发送加密保护的隐私信息给 B 链时，可能会由于网关权限设置的原因出现加密信息未经授权而直接被 B 链所使用。跨链重放攻击主要涉及跨链过程中的智能合约。由于目前区块链技术并不成熟，各区块链都可能面临系统升级或重大故障而需要进行硬分叉，跨链重放攻击会让用户的资产严重损失。因此在对未来研究的过程中需要考虑这样的攻击问题。

在跨链安全方面，可以考虑设置监管系统对智能合约等进行安全性检测，来提高系统的安全性和健壮性。

(4) 基于跨链机制，利用区块链与云计算相融合，通过网络中数据的加密和共识，解决数据和价值交换的安全性和可信性问题。

区块链技术的核心是共识算法，其资源开销大小和安全性将直接影响区块链系统的效率和稳定性。而区块链的计算和存储能力是有限的，现阶段的共识机制存在着资源消耗大的问题[62]。云计算服务作为一种将计算资源以服务的方式提供给用户的重要服务模式，可以降低传统共识算法的资源消耗，同时也可以保障工作的稳定性和安全性。下一步的研究应尝试将云计算与区块链融合，实现安全、真实、完整和高效的数据交换，构建一个双方信任的公平交易环境。

(5) 通过优化验证算法、网络传输、智能合约，以及增加缓存机制等方式，提高跨链身份认证的效率。

跨链身份认证的实现效率对于区块链系统的整体性能和用户体验非常重要，直接影响到系统的运行速度和可扩展性。在跨链身份认证中，需要频繁的查询和验证身份信息，这样会对系统的性能产生很大影响。为了减轻这种影响，可以采用缓存机制来缓存已经验证过的身份信息，从而减少重复查询和验证。身份验证是整个跨链身份认证系统中最核心的环节，可以采用零知识证明等更高效的验证算法来提高身份验证的效率，基于零知识证明的实现方式可以通过减少计算量来提高身份认证的效率，时间复杂度主要取决于零知识证明的计算复杂度，通常为 $O(\log n)$。在优化网络传输方面，采用更高效的网络传输协议和技术来提高传输效率，如 Wecross 使用 HIP(Heterogeneous Interchain Protocol) 跨链互联协议来传输数据等。同时，可以采用数据压缩和加密等技术，进一步提高网络传输效率和安全性。

5 结束语

文中面向跨链身份认证领域，重点研究了基于 DID 的跨链身份认证模型，并对这些模型进行了分析对比，总结了现有模型存在的问题，最后针对研究现状中的不足与挑战，展望了未来的研究方向。需要注意的是，在开发完整的 DID 的跨链身份认证解决方案时，必须关注国际标准和协议以保证可扩展性和互操作性。目前 DID 用于跨链互联互通模型的实施仍处在的早期阶段，但发展速度非常快，围绕基于 DID 的跨链身份认证模型产生的方案迅速增长。

参考文献：

[1] 何帅,黄襄念,陈晓亮.区块链跨链技术发展及应用研究综述[J].西华大学学报(自然科学版),2021,40(3):1-14.
He S, Huang X N, Chen X L. The Research Summary of the Development and Application of Blockchain Cross-chain Technology [J]. Journal of Xihua University

(Natural Sci-ence Edition), 2021,40 (3): 1-14.

[2] BAI Y R, LEI H, LI S Z, et al. Decentralized and self-sovereign identity in the era of blockchain: a sur-vey[C]//2022 IEEE International Conference on Blockchain (Blockchain 2022), Espoo, Aug 22-25, 2022. Piscataway: IEEE, 2022: 500-507.

[3] 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(6):1637-1641.

ZHANG Y B, XING K. Cross-domain authentication scheme based on multi-layer blockchain [J]. Application Research of Computers, 2021,38 (6): 1637-1641.

[4] KESZTHELYI A. About passwords[J]. Acta Polytechnica Hungarica, 2013,10(6): 99-118.

[5] CELESTI A, TUSA F, VILLARI M, et al. Three-phase cross-cloud federation model: The cloud SSO authentica-tion[C]//In 2010 Second International Conference on Ad-vances in Future Internet, Venice, July 18-25, 2010. Pisca-taway: IEEE, 2010: 94-101.

[6] A brief history of digital identity in time from 1995 to 2018 [EB/OL]. (2018-09-13) [2023-03-02]. http://www.lianmenhu.com/blockchain-6328-1.

[7] Microsoft and Oracle create open standard for Covid 'passports'[J]. Biometric Technology Today, 2021, 2021(2): 1-2.

[8] 中钞区块链技术研究院.四大分布式数字身份架构的对比及研究. [EB/OL]. (2020-05-19) [2023-03-12]. https://www.ccvalue.cn/article/221958.html.

[9] PREUKSCHAT A, DRUMMOND R. Self-sovereign iden-tity: decentralized digital identity and verifiable creden-tials[M]. Shelter Island: Manning, 2021: 21-37.

[10] LENNART A, CONSTANTIN F. A bibliometric review of research on digital identity: Research streams, influential works and future research paths[J]. Journal of Manufac-turing Systems, 2022,62: 523-538.

[11] MICHAEL S, ANNA Z J. An identity provider as a service platform for the edugain research and education communi-ty[C]//In 2019 IFIP/IEEE Symposium on Integrated Net-work and Service Management (IM), Arlington, VA, USA, April 08-12,2019. Piscataway: IEEE, 2019:739-740.

[12] MÜHLE A, GRÜNER A, GAYVORONSKAYA T, et al. A survey on essential components of a self-sovereign identi-ty[J]. Computer Science Review, 2018(30): 80-86.

[13] MUKTA R, PAIK H Y, LU Q, et al. CredTrust: Credential Based Issuer Management for Trust in Self-Sovereign Identity[C]. 2022 IEEE International Conference on Blockchain (Blockchain 2022), Espoo, Aug 22-25, 2022. Piscataway: IEEE, 2022: 334-339.

[14] YUAN Y, WANG F. Parallel blockchain: concept, methods and issues. Acta Autom[J]. Acta Automatica Sinica, 2017, 43 (10):1703–1712.

[15] LIM S, RHIE M, HWANG D, et al. A Subject-centric cre-dential management method based on the verifiable cre-dentials[C]//2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea (South), January 13-16, 2021. Piscataway: IEEE, 2021: 508-510.

[16] NAIK N, JENKINS P. A secure mobile cloud identity: Criteria for effective identity and access management standards[C]//2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mo-bileCloud 2016), Oxford, UK, March 29-April 01, 2016. Piscataway: IEEE, 2016: 89-90.

[17] DIEYE M, VALIORGUE P, GELAS J P, et al. A self-sovereign identity based on zero-knowledge proof and blockchain[J]. IEEE Access, 2023(11): 49445-49455.

[18] LUX Z A, BEIERLE F, ZICKAU S, et al. Full-text search for verifiable credential metadata on distributed ledg-ers[C].//2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, October 22-25,2019. Piscataway: IEEE, 2019: 519-528.

[19] ALEXANDER M, ANDREAS G, TATIANA G, et al. A survey on essential components of a self-sovereign identity[J]. Com-puter Science Review, 2018,30:80-86.

[20] Decentralized Identity (DID) Research Report: Important Practices of Web 3.0 Development [EB/OL]. (2022-10-03) [2023-03-11]. https://www.ccvalue.cn/article.html.

[21] LEE Y E, KIM H W, LEE M J. NextAuction: A DID-based robust auction service for digital contents[J]. Journal of the Korea Society of Computer and Information, 2022, 27(2): 115-124.

[22] VITALIK B. Chain Interoperability[EB/OL]. (2016-07-08) [2023-03-01].https://docslib.org/doc/5895634/chain-interoperability-vitalik-buterin.

[23] 郭朝,郭帅印,张胜利,等.区块链跨链技术分析[J].物联网学报,2020,4(02):35-48.

GUO C, GUO S Y, ZHANG S L, et al. Analysis of cross-chain technology of blockchain [J]. Chinese Journal on Internet of Things, 2020, 4 (02): 35-48.

[24] 孙浩,毛瀚宇,张岩峰,等.区块链跨链技术发展及应用[J].计算机科学,2022,49(5):287-295.

SUN H, MAO H Y, ZHANG Y F, et al. Development and application of blockchain cross-chain technology [J]. Computer Science, 2022, 49 (5): 287-295.

[25] BACK A, CORALLO M, DASHJR L, et al. Enabling Blockchain Innovations with Pegged Sidechains. [EB/OL]. (2014-05-13) [2023-03-09]. http://www.opensciencereview.com/papers/123/enabling blockchain-innovations-with-pegged-sidechains.

[26] 陈畅.区块链安全跨链技术研究[D].广州:广州大学,2022。

CHEN C. Research on blockchain security cross-chain

technology[D]. Guangzhou: Guangzhou University, 2022.

[27] 李芳,李卓然,赵赫.区块链跨链技术进展研究[J/OL].软件学报,2019,30(6):1649-1660.

LI F, Li Z, ZHAO H. Research on the progress in cross-chain technology of blockchains[J/OL]. Journal of Software, 2019,30(6):1649−1660. http://www.jos.org.cn/1000-9825/5741.htm

[28] GUO Z, LIU L, LIANG Z, et al. Blockchain cross-chain technology research[C].//2022 IEEE 5th Advanced Infor-mation Management, Communicates, Electronic and Au-tomation Control Conference (IMCEC), Chongqing, China, December 16-18,2022. Piscataway:IEEE, 2022: 1064-1070.

[29] CHANDRA G B, RAMAKRISHNA V, GOVINDARAJ AN C, et al. Decentralized cross-network identity management for blockchain interoperation.[EB/OL]. (2021-07-07) [2023-03-07]. http://arxiv.org/abs/2104.03277.

[30] 孟博,王乙丙,赵璨,等.区块链跨链协议综述[J].计算机科学与探索, 2022,16(10):2177-2192.

MENG B, WANG Y B, ZHAO C, et al. Survey on cross-chain protocols of blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2022, 16(10):2177-2192.

[31] GIACOBINO A, GRIERSON D, SINGH H P, et al. Cosmos Cash: Public permissionless approach towards ssi and use cases[C].// 2022 IEEE International Conference on Block-chain (Blockchain 2022), Espoo, Aug 22-25, 2022. Pisca-taway: IEEE, 2022: 462-467.

[32] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework[J]. White Paper 21, 2016: 2327–4662.

[33] BAO Z, WANG Q, ZHANG Y, et al. TPRou: A priva-cy-preserving routing for payment channel net-works[C].//the 26th European Symposium on Research in Computer Security (ESORICS 2021), September 13-17, 2021, Darmstadt, Germany. Cham, Switzerland: Springer, 2021: 630-648.

[34] OU W, HUANG S Y, ZHENG J J, et al. An overview on cross-chain: Mechanism, platforms, challenges and ad-vances[J]. Computer Networks, 2022: 1389-1286.

[35] ADRIAN H B, STEFAN T. Interledger: creating a standard for payments[C]. Proceedings of the 25th International Conference Companion on World Wide Web, April 11, 2016. New York: ACM, 2016: 281–282.

[36] POON J, DRYJA T. The Bitcoin lightning network: scalable off-chain instant payments [EB/OL]. (2016-12-19) [2023-03-11]. https://lightningnetwork/lightning-network-paper.pdf, 2016.

[37] QASSE I A, ABU T M, NASIR Q, Inter blockchain communication: a survey[C]//Proceedings of the ArabWIC 6th Annual International Conference Research Track, New York, USA,2019. New York: Association for Computing Machinery,2019: 1–6.

[38] LIN S, KONG Y, NIE S, et al. Research on cross-chain technology of blockchain[C].//2021 6th International Con-ference on Smart Grid and Electrical Automation (ICSGEA), Kunming, China, May 29-30, 2021. Piscat-away: IEEE, 2021: 405-408.

[39]王皓,宋祥福,柯俊明,等.数字货币中的区块链及其隐私保护机制[J].信息网络安全,2017(07):32-39.

WANG H, SONG X, KE J M, et al. Blockchain and privacy preserving mechanisms in cryptocurrency[J]. Netinfo Se-curity,2017(7):32-39.

[40] WANG W, NING H, XIN L. BlockCAM: A Block-chain-Based Cross-Domain Authentication Model[C]//2018 IEEE Third International Conference on Data Science in Cyberspace(DSC), Guangzhou, China, 2018. Piscataway: IEEE, 2018: 896-901.

[41] 火链科技研究院.区块链数字身份：数字经济时代基础设施[EB/OL]. (2022-09-19) [2023-03-09]. https://img3.gelonghui.com/pdf/e7923-13813235-c970-4513-a64e-f35448ce5849.pdf.

FireChain Technology Research Institute. blockchain digital identity: infrastructure in the digital economy era[EB/OL]. (2022-09-19) [2023-03-09]. https://img3.gelonghui.com/pdf/e7923-13813235-c970-4513-a64e-f35448ce5849.pdf.

[42] 董贵山,张兆雷,李洪伟,等.基于区块链的异构身份联盟与监管体系架构和关键机制[J].通信技术,2020,53(2):401-413.

DONG G S, ZHANG Z L, LI H W, et al. Regulatory system architecture and key mechanisms of blockchain-based het-erogeneous identity alliance[J]. Communications Technol-ogy,2020,53(02):401-413.

[43] 邓小鸿,朱年红,黄磊,等.基于区块链的身份托管模型研究[J].计算机工程与应用,2020,56(04):24-30.

DENG X H, ZHU N H, HUANG L, et al. Research on identity trusteeship model based on blockchain[J]. Com-puter Engineering and Application, 2020, 56(04): 24-30.

[44] YOON D, MOON S, PARK K, et al. Blockchain-based personal data trading system using decentralized identifiers and verifiable credentials[C]//2021 International Confer-ence on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, Oct 20-22,2021.Piscataway:IEEE,2021: 150-154.

[45] Liu Y Z, Liu A D, XIA Y, et al. A blockchain-based cross-domain authentication management system for iot devices[J]. IEEE Transactions on Network Science and Engineering, 2023:1-13.

[46] 杨淳,李经纬,李洪伟,等.异构身份联盟统一身份标识模型研究[J].信息安全与通信保密,2019(06):27-35.
YANG C, LI J W, LI H W, et al. A Research on Heteroge-neous Identity Alliance Unified Identity Model[J]. Infor-mation Security and Communication Security, 2019(06): 27-35.

[47] 陈武阳. 基于区块链的 PKI 身份认证的研究[D].兰州：兰州理工大学,2020.
CHEN W. Research on PKI identity authentication based on blockchain[D]. Lanzhou: Lanzhou University of Technol-ogy,2020.

[48] SHAO S S, CHEN F, XIAO X Y, et al. IBE-BCIOT: an IBE based cross-chain communication mechanism of blockchain in IoT[J]. Wold Wide Web-Internet and Web Information Systems, 2021,24: 1665-1690.

[49] 王洒洒,戴炳荣,朱孟禄,等.面向跨链系统的用户身份标识认证模型[J].计算机工程与应用,2022,58(19):135-141.
WANG S S, DAI B R, ZHU M L, et al. User identity au-thentication model for cross-chain system[J]. Computer Engineering and Applications, 2022, 58(19): 135-141.

[50] LI X Y, ZHENG Z Y, CHENG P Y, et al. A multi-channel anonymous consensus based on Tor[J]. World Wide Web-Inernet and Web Information Systems, 2022, 26(3): 1005-1029.

[51] 雷志伟,朱义,张健,等.一种可监管的区块链跨链平台设计[J].计算机与数字工程,2021,49(12):2544-2550+2572.
LEI Z W, ZHU Y, ZHANG J, et al. Design of a Supervised Blockchain Cross Chain Platform[J]. Computer & Digital Engineering, 2021, 49 (12): 2544-2550+2572.

[52] 王姝爽,马兆丰,刘嘉微,等.区块链跨链安全接入与身份认证方案研究与实现[J].信息网络安全, 2022, 22(06): 61-72.
WANG S S, MA Z F, LIU J W, et al. Research and Imple-mentation of Cross-Chain Security Access and Identity Authentication Scheme of Blockchain [J]. Netinfo Security, 2022, 22(6): 61-72.

[53] CHAO P. Research on cross-chain communication based on decentralized identifier[C]//2021 4th International Con-ference on Hot Information-Centric Networking (HotICN), Nanjing, China, November 25-27,2021. Piscataway: IEEE, 2021: 7-12.

[54] WANG X. A credible transfer method of cross-chain assets based on DID and VC[C]//IEEE 4th International Con-ference on Information Systems and Computer Aided Ed-ucation (ICISCAE), Dalian, China, September 24-26,2021. Piscataway: IEEE,2021: 238-242.

[55] XIE T X, ZHANG Y, GAI K K, et al. Cross-Chain-Based decentralized identity for mortgage loans[C]//14th Inter-national Conference on Knowledge Science, Engi-neering, and Management (KSEM), Tokyo, Japan, August 14-16, 2021.Cham: Springer Nature Switzerland, 2021 (12817): 619-633.

[56] ZHONG T, SHI P C, CHANG J S. JointCloud cross-chain verification model of decentralized identifiers[C]//2021 IEEE International Performance, Computing, and Commu-nications Conference (IPCCC), Austin, TX, USA, October 29-31, 2021. Piscataway: IEEE, 2021:1-8.

[57] ZHAO F X, YU J G, YAN B W. Towards cross-chain access control model for medical data sharing[J]. Procedia Com-puter Science, 2022(202): 330-335.

[58] REN Q, LIU H, LI Y, et al. Cloak: A framework for de-velopment of confidential blockchain smart contracts[C]// 2021 International Conference on Distributed Computing Systems (ICDCS), DC, USA, July 07-10, 2021. Piscat-away: IEEE, 2021:1102-1105.

[59] LI D, LIU J, TANG Z, et al. Agentchain: a decentralized cross-chain exchange system[C]//In 2019 18th IEEE In-ternational Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE Inter-national Conference on Big Data Science and Engineering (Trust-com/BigdataSE), Rotorua, New Zealand, August 5-8, 2019.Piscataway: IEEE, 2019, 1: 491–498.

[60] WANG Q, ZHANG Y, BAO Z, et al. SorTEE: Ser-vice-oriented routing for payment channel networks with scalability and privacy protection[J]. IEEE Transactions on Network and Service Management, 2022, 19(4): 3764-3780.

[61] QASSE I A, ABU T M, NASIR Q, Inter blockchain communication: a survey[C]//Proceedings of the Arab WIC 6th Annual International Conference Research Track, New York, USA,2019. New York: Association for Computing Machinery,2019: 1–6.

[62] 颜阳,王斌,邹均.区块链+赋能数字经济[M].北京:机械工业出版社-区块链书系, 2018:157-211.
YAN Y,WANG B,ZOU J. Blockchain + empowering digital economy[M]. Beijing: China Machine Press-Blockchain Book Department, 2018:157-211.

白伊瑞（1999—），女，山西临汾人，硕士研究生，主要研究方向为区块链、可信数字身份、可信计算等。

BAI Yirui, born in 1999, M.S. candidate. Her research interests include blockchain, Trusted digital identity, trusted computing, etc.

田宁（1994—），女，安徽宿州人，博士研究生，主要研究方向为数字身份，区块链等。

TIAN Ning, born in 1994, Ph.D. candidate. Her research interests include digital identity, blockchain, etc.

雷虹（1984—），男，湖南常德人，博士，教授，博士生导师，主要研究方向为区块链，可信执行环境，隐私计算等。

LEI Hong, born in 1984, Ph.D., professor, Ph.D. supervisor. His research interests include blockchain, trusted execution environment, privacy computing, etc.

刘雪峰（1985-），男，安徽亳州人，博士，副教授，博士生导师，主要研究方向安全计算、区块链隐私。

LIU Xuefeng, born in 1985, Ph.D., associate professor, Ph.D. supervisor. His research interests include secure computing, blockchain privacy, etc.

芦翔（1982—），男，山东烟台人，博士，副研究员，硕士生导师，主要研究方向为区块链安全监管，物联网密码工程与应用等。

LU Xiang, born in 1982, Ph.D., associate researcher, M.S. supervisor. His research interests include blockchain security supervision, Internet of Things cryptography engineering and application, etc.

周勇（1999—），女，重庆人，硕士研究生，主要研究方向为区块链等。

ZHOU Yong, born in 1999, M.S. candidate. Her research interests include blockchain, etc.