面向 6G 的分布式可信技术研究*

梁亚从[1],夏 旭[2],包施晗[1],徐 晖[1]
(1.大唐移动通信设备有限公司,北京 100083;2.中国电信研究院,北京 102209)

摘 要:随着移动通信技术的发展,6G 网络将通过网络分布式下沉缓解承载网络压力,通过分布式协同优化资源配置,但是如何保障分布式可信,助力多方协同体系是即将面临的安全挑战。区块链作为一种分布式账本技术,将区块链运用到跨域认证与跨域资源协调中,可以保障交易的透明和数据的可信,建立起多方参与者之间的信任关系,成为解决分布式可信的关键技术。

关键词:分布式可信;6G;区块链;跨域认证;网络切片
中图分类号:TN918.91 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.223510

中文引用格式:梁亚从,夏旭,包施晗,等. 面向 6G 的分布式可信技术研究[J].电子技术应用,2022,48(12):5-10.
英文引用格式:Liang Yacong,Xia Xu,Bao Shihan,et al. Research on distributed trust in 6G[J]. Application of Electronic Technique,2022,48(12):5-10.

Research on distributed trust in 6G

Liang Yacong[1],Xia Xu[2],Bao Shihan[1],Xu Hui[1]
(1.Datang Mobile Communication Equipment Co.,Ltd.,Beijing 100083,China;
2.China Telecom Research Institute,Beijing 102209,China)

Abstract:With the development of mobile communication technology, the 6th Generation mobile networks(6G) network will ease the pressure on the bearer network through distributed network sinking, and optimize resource allocation through distributed coordination. However, how to ensure distributed trustworthiness and help the multi-party collaborative system is an upcoming security challenge. As a distributed ledger technology, blockchain can be applied to cross-domain authentication and cross-domain resource coordination. Blockchain can ensure the transparency of transactions and the credibility of data, and establish a trust relationship between multiple participants, which become the key technology to solve distributed trust.

Key words:distributed trust;6G;blockchain;cross-domain authentication;network slice

0 引言

第六代移动通信网络(6th Generation Mobile Networks,6G)具有“万物互联、全球覆盖、泛在智能”等多重需求,这些需求使得 6G 网络需要成为异构融合的全连接网络。同时,6G 网络需要部署灵活扩展的分布式架构,随着新技术的不断成熟以及设备能力的提高,6G 网络将不仅承载着 5G(5th Generation Mobile Networks)网络既有的业务,还需要面对新兴的业务需求,如全息通信、扩展现实(Extended Reality,XR)、虚拟现实(Virtual Reality,VR)等。这些新兴的业务以及既有业务的进一步发展,对网络的吞吐量、时延、可靠性以及连接密度数提出了更高的要求。网络的去中心化——分布式网络架构有望缓解中心网络的压力,提升业务体验。同时 6G 网络将从地面扩展到空天地海融合,空天地海一体的泛在接入需求需要分布式网络架构的支持,子网与子网之间、不同运营体系之间需要具备多方运营协作治理体系,支持多方资源共享。网络架构的分布式、产业界参与方的丰富化,使得提供多方、跨域的分布式可信体系成为 6G 安全需要考虑的问题。

1 分布式可信与区块链技术

区块链技术作为一种对等网络的分布式账本技术,具有去中心化、不可篡改、可追溯、匿名性和透明性的特征,成为了目前分布式信任的研究热点。区块链网络结构自带的分布式账本技术能够在实现去中心化数据管理的同时保证数据可追溯、不可篡改。同时,采用分布式共识算法,保证数据的快速同步与及时更新,实现信息共享。6G 分布式网络中每个子网将作为一个单独的管理域都拥有大量的设备、独立的域内通信协议与管理方式。但是不同网络域间的设备存在着合作、交互与资源

*基金项目:2022 年度国家重点研发计划“6G 移动通信安全内生及隐私保护技术”专项(2022YFB2902200)

调度的需求，需要信息共享，跨域协作的前提是需要在域间建立信任机制。基于区块链的分布网络设计能够提供可信的网络服务和弹性伸缩，以及跨域信息共享。

2 基于区块链的可信跨域认证

6G 网络中一个任务的完成往往需要多个域进行协作，不同域间的设备需要相互通信，但是不同域之间不一定相互信任，因此需要进行跨域认证。但是，6G 去中心化开放式的网络架构使得身份的认证和管理越发复杂和耗时。现有的大多数认证机制建立在公钥基础设施(Public Key Infrastructure，PKI)上，需要可信第三方的参与，例如证书授权机构(Certificate Authority，CA)。CA 为所有 PKI 数字证书提供信任根，数字证书被用来验证用户、设备和其他实体的身份。在分布式网络环境中，一个域内会设置一个 CA，形成一个相对独立的信任域，以防止未经授权的用户访问内部资源。而用户需要跨域认证时，不同域间的 CA 要经过多次数字证书的传递、签名的加密和解密，频繁的跨域访问还会增加网络延迟，提高网络成本。同时，可信第三方的参与也有可能受到单点故障等威胁，并且会产生昂贵的管理成本。

目前研究多将区块链引入跨域认证中，使认证信息上链，用区块链存储更新已经发放和激活的认证参数，基于区块链的不可篡改性，区块链为认证结果进行信任背书，保证认证参数的真实性，为跨域认证提供了保障。链上存储的数据由多个域进行维护，相当于进行了冗余备份，具有容错性，从而避免了中心化认证导致的单点故障和效率低下的问题。同时，多个域内的认证服务器均从区块链下载认证鉴权信息，避免了频繁的跨域访问。目前关于区块链与认证结合的研究主要是基于数字证书上链、基于主从链以及基于公钥上链的 3 种认证方法，接下来的内容将介绍这 3 种基于区块链的跨域认证架构。

2.1 基于数字证书上链的跨域认证

基于数字证书的跨域认证方法主要思想如图 1 所示，是将不同域内设备数字证书或数字证书的哈希值上传至区块链，并持续更新，当设备进行跨域通信时，不必进行域间 CA 的相互认证，用户 A 向域 B 内的认证服务器提供认证请求，认证服务器负责检查用户提交的数字证书，即将区块链中存储的数字证书或数字证书的哈希值与用户提交的进行对比，若一致则认证成功，实现跨域认证[1-2]。

2.2 基于主从链的跨域认证

基于主从链进行跨域认证是通过使用主链和从链两个区块链实现跨域认证[3]。如图 2 所示，从链相当于域内认证服务器的作用，为该域内设备生成数字证书，并将数字证书的哈希值存储在主链上，域内设备也可用该证书与其他域进行通信。主链作为可信共享平台，主要用于解析跨链认证请求，保证设备的跨域可信认证，区块链相当于认证服务器进行域内认证信息的生成与存储。Feng 等人[4]利用私有链和联盟链，建立起无人机之间的跨域身份认证。

2.3 基于公钥上链的跨域认证

密钥生成中心(Key Generation Center，KGC)为负责管理该域内设备私钥的控制设备，如图 3 所示，KGC 根据设备提交的身份信息生成非对称密钥，然后将私钥发送回请求设备。不同域内的区块链代理服务器(Blockchain Agent Server，BAS)作为 KGC 的代理参与区块链网络，BAS 从 KGC 接收公钥信息并将其写入区块链。身份认证服务器(Authentication Agent Server，AAS)通过从 BAS 处查询区块链上存储的公钥认证信息，并基于下载的公钥及认证信息对请求的设备进行认证，收到的认证信息与区块链上的一致则认证成功。基于 KGC 的跨域认证

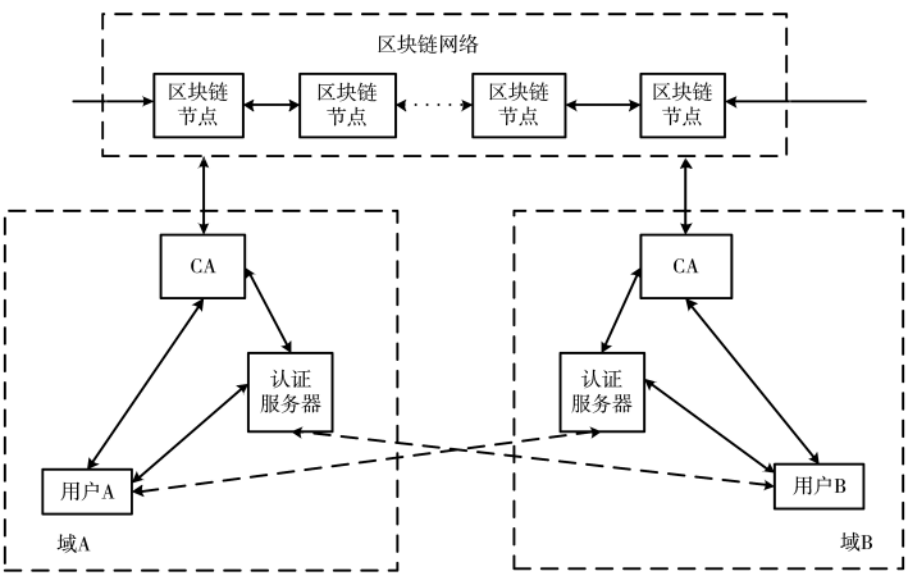

图 1 基于数字证书的可信跨域认证

《电子技术应用》http://www.chinaaet.com

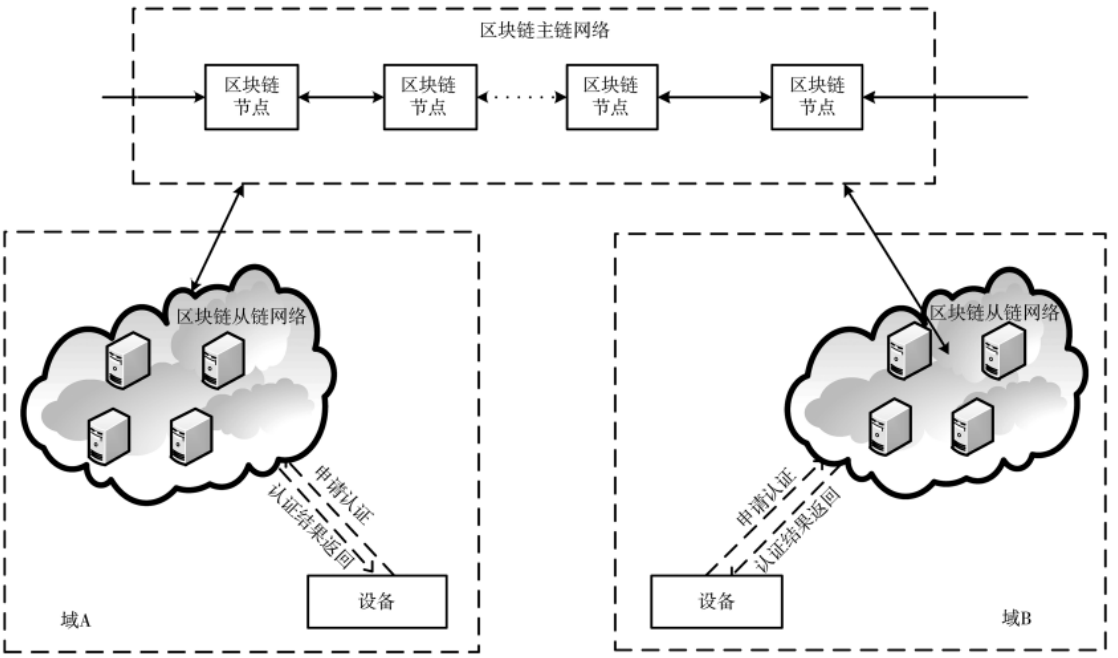

图 2 基于主从链的可信跨域认证

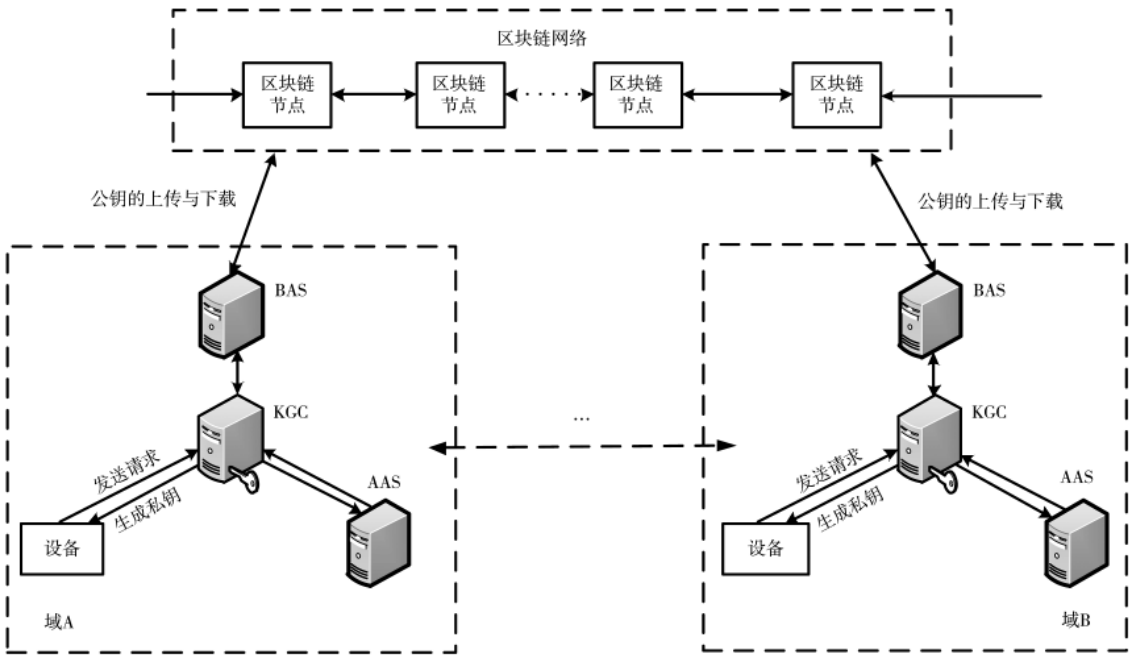

图 3 基于公钥上链的可信跨域认证

通常需要引入假名机制，利用假名机制的身份信息使攻击者在域外不能够溯源到设备的真实身份[5]。

在基于区块链进行认证的方案中，区块链只是作为一个存储平台负责权限信息的存储、更新、删除等，保障数据的不可篡改以及真实共享，而真正的认证工作仍然需要域内的服务器进行操作。

3 基于区块链的可信跨域认证

3.1 构建多方信任，实现资源共享

在未来 6G 时代，会出现来自更多参与方的网络基础设施共建共享，特别是各种移动边缘设备和基站的共建部署。在过去，网络的共建共享主要发生在若干传统电信运营商之间，他们可以在同一地理区域内共享网络资源，也可以跨不同地理区域进行共享。随着 6G 网络参与者的增多，垂直行业参与者和普通企业家庭用户有望也参与进来。在网络共建共享的场景中，每个参与者既是网络资源服务的贡献者，也同时是消费者。当多个参与方一同参与网络基础设施的共建共享时，应考虑何种分布式架构可以准确、高效、实时、可信地结算每个参

与者的资源服务贡献量和消费量，将关键参数、运维信息等存储以便于事后追溯或审计，避免产生争端。

在网络切片部署方面，运营商存在着跨域协作的需求。网络切片利用虚拟化技术在物理网络上虚拟化出多个虚拟网络，通过网络切片可以根据客户需求定制跨运营商/运营商内部的虚拟网络，减少物理网络投资成本。但是运营商之间存在着竞合关系，如果需要高效实现网络切片的部署以实现网络资源的充分共享，避免不必要的沟通成本，前提是在运营商网络之间创建信任关系。

在垂直行业应用中同样也需要实现运营商与行业客户之间的跨域。例如能源互联网中，往往包括能源供应方(如大型发电企业)、能源消费方(如能源局域网等)，以及通信系统、配电网络等，其中能源互联网与电信运营商网络进行了深度融合，运营商网络与这些复杂系统在业务运行时存在一定的交互，由于各个参与者隶属于不同的利益方，不同利益方追求自我利益的本性使得需要构建起多方信任的关系。

3.2 基于区块链的网络切片资源共享架构

网络运营商通过多个基础设施网络间协作及资源共享的方式扩充网络容量，进而降低部署成本并且提升投资收益。为了给用户提供差异化定制化的服务，网络切片的概念被提出，其本质是依据服务需求将基础设施网络切分成多个相互独立且彼此隔离的逻辑网络。

目前，在一个运营商内部，切片管理基于切片管理域进行资源编排，如图 4 所示，切片资源横跨无线网、承载网以及核心网，完成端到端网络切片实例化。具体地，网络资源共享主要指的是在底层基础设施上进行共享(如无线网或承载网)，再将接入其他运营商的共享资源利用到自己内部网络切片的端到端建设中去。像这样需要创建跨多个参与者构建端到端网络切片实例时，运营商需要分解端到端网络切片的服务请求，并将其管理数据提供给其他参与者。创建该网络服务的先决条件是参与者之间存在信任关系。然而，大多数参与者还是会担心暴露敏感数据，或者其他参与者可能不遵守网络切片的协议。

考虑到上述信任问题，Gorla[6]等人认为可以部署区块链来确保不同电信运营商间的信任，以实现网络切片中的多参与者协调管理。Rathi[7]提出了一种包含多域边缘编排的架构，以通过智能合约实现服务水平协议(Service Level Agreement，SLA)自治管理。文献[8]介绍了 5G 网络切片代理的概念，它可以促进按需资源分配和基于流量监控和预测的准入控制。Nour[9]和 Zanzi[10]提出使用区块链通过智能合约部署代理机制，使得移动虚拟网络运营商(Mobile Virtual Network Operator，MVNO)、Over The-Top(OTT)提供商和基础设施提供商(Infrastructure Providers，InP)都参与到区块链网络中，切片代理机制将在切片部署中协调多个参与者。可见，利用区块链保持跨域资源可信已经成为研究的热点。本文基于云化的无线网络架构[11]提出一种基于区块链的跨域资源协作方法，如图 5 所示，图中虚线为逻辑连接。

无线基础设施在多基础设施供应商之间进行共享。图 5 中列举了分属于不同基础设施供应商(InP1 和 InP2)的无线网络，分别是 5G 网络与无线保真(Wireless Fidelity，Wi-Fi)网络。InP1 为 5G 网络的基础设施供应商，下一代基站(the next Generation Node B，gNB)与核心网建立连接，进而接入互联网。InP2 为 WiFi 网络的基础设施供应商，无线接入点(Access Point，AP)与 WiFi 无线网网关(WiFi Access Gateways，WAG)建立连接，进而接入互联网。为了便于无线资源在不同基础设施供应商之间共享，在 gNB 与 AP 引入网络功能虚拟化(Network Function Virtualization，NFV)技术，使部分 gNB 或部分 AP 具有虚拟化能力，其中，使用 Hypervisor 创建软件实例——virtual gNB(VgNB)和 virtual AP(VAP)，VgNB 或 VAP 仿真模拟其他基础设施供应商的基础功能[11]。

InP1 和 InP2 中的 SDN controller 为逻辑模块，编排管理软件实例 VgNB 及 VAP，该控制器外界服务器连接进入区块链网络。其中，InP1 域内的管理模块为逻辑功能模块，与 InP1 中的 SDN controller 建立逻辑连接，负责向 SDN controller 发送网络性能以及资源信息以便于 SDN

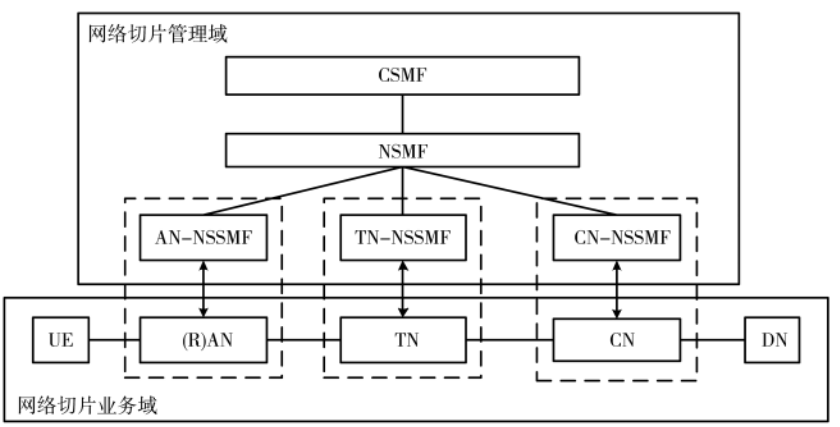

图 4 5G 端到端网络切片框架示意

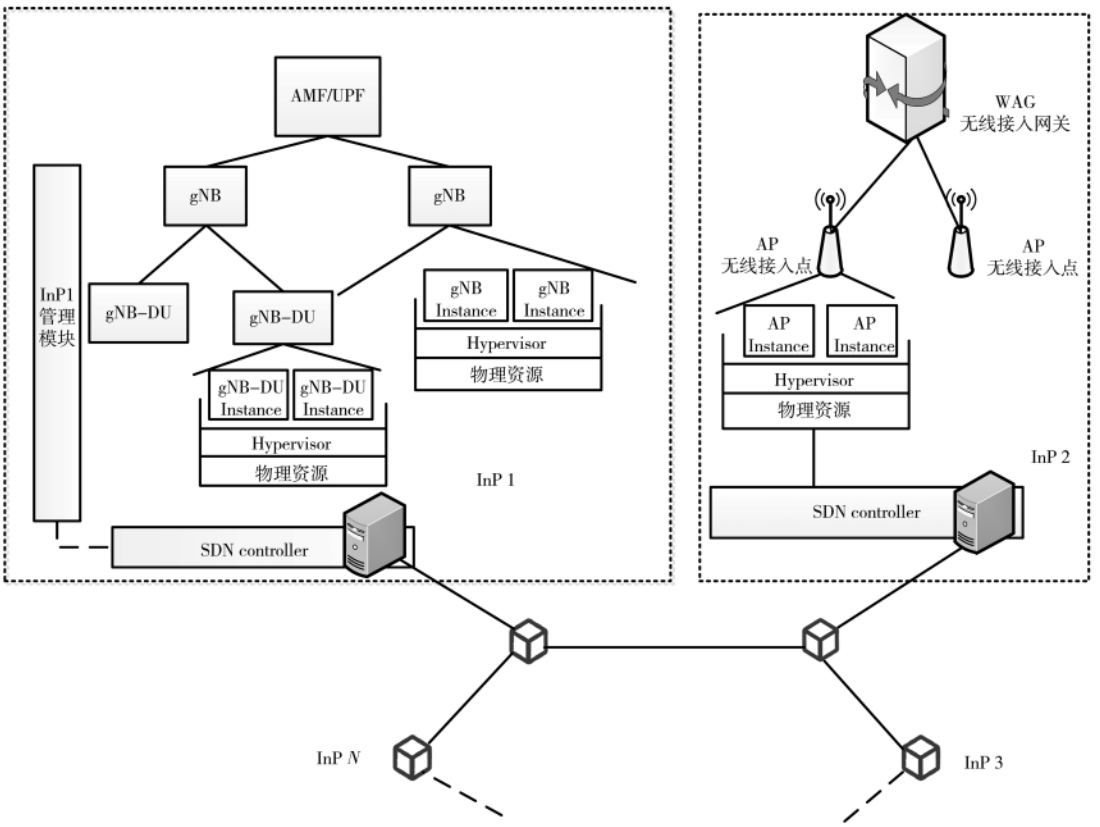

图 5 基于区块链的跨域资源协作方法示意

controller 具有对网络的全面掌握，进而 InP1 可以依据这些信息通过区块链网络分享其未被充分利用的资源。而 InP2 域内的 WiFi 无线网关负责聚合来自多个 WiFi AP 的流量并处理整个 WiFi 网络的互联网连接。在该架构中，WAG 发挥着与 InP1 管理模块相同的作用，与 InP2 中的 SDN controller 建立逻辑连接，负责向 SDN controller 发送网络性能以及资源信息，以便于 SDN controller 具有对网络的全面掌握，进而 InP2 可以同样通过区块链网络依据这些信息分享其未被充分利用的资源。

所有基础设施供应商通过 SDN controller 服务器连接到区块链网络上，广播资源需求，或发布共享资源所需的资源参数，其他参与者根据资源请求利用 Hypervisor 虚拟化其需求的物理无线资源(如 Hypervisor 可以让 gNB 虚拟化物理无线资源，并使运行在物理层之上的多个软件实例之间共享)，以便进行资源共享。

为了实现认证安全，区块链网络上存储了各个基础设施供应商上传的认证信息，使得域与域之间能够实现身份认证。同时，交易记录存储在分布式账本中，不可抵赖，保证了透明可信，使各个参与者一起公平地参与到网络共建共享和规划运营中。

4 结论

本文总结了分布式可信技术在 6G 中的研究，主要从跨域认证和跨域资源协作的角度切入，总结了 3 类基于区块链的跨域认证模型，同时以网络切片为例，阐述了分布式可信在跨域资源协调的应用场景，并提出一种基于区块链的跨域资源协作方法，展示了区块链如何应用在可信的跨域资源协调中。

关于分布式可信在 6G 中的应用和研究，目前业界仍然处于研究阶段，而区块链有望成为信任分布式的潜在技术之一。同时，区块链与人工智能进行结合从而提供安全策略、安全检测等也成为安全方面研究的热点。

参考文献

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

[2] Gu Pengpeng, Chen Liquan. An efficient blockchain-based cross-domain authentication and secure certificate revocation scheme[C]//2022 IEEE 6th International Conferenct on Computer and Communications, 2020.

[3] Guo Shaoyong, Wang Fengning, Zhang Neng, et al. Master-slave chain based trusted cross-domain authentication mechanism in IoT[J]. Journal of Network and Computer Applications, 2020, 172: 102812.

[4] FENG C, LIU B, GUO Z, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones[J]. IEEE Internet of Things Journal, 2022, 9(8): 6224-6238.

[5] SHEN M, LIU H, ZHU L, et al. Blockchain-assisted secure

device authentication for cross-domain industrial IoT[J].IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.
[6] GORLA P, CHAMOLA V, HASSIJA V, et al.Network slicing for 5G with UE state based allocation and blockchain approach[J].IEEE Network, 2021, 35(3): 184-190.
[7] RATHI V K, CHAUDHARY V, RAJPUT N K, et al.A Blockchain-enabled multi domain edge computing orchestrator[J].IEEE Internet of Things Magazine, 2020, 3(2): 30-36.
[8] SAMDANIS K, COSTA-PEREZ X, SCIANCALEPORE V. From network sharing to multi-tenancy: the 5G network slice broker[J].IEEE Communications Magazine, 2016, 54(7): 32-39.
[9] NOUR B, KSENTINI A, HERBAUT N, et al.A Blockchain-based network slice broker for 5G services[J].IEEE Networking Letters, 2019, 1(3): 99-102.
[10] ZANZI L, ALBANESE A, SCIANCALEPORE V, et al. NSBchain: a secure blockchain framework for network slicing brokerage[C]//ICC 2020-2020 IEEE International Conference on Communications(ICC).Dublin, Ireland: IEEE, 2020: 1-7.
[11] JIANG M, XENAKIS D, COSTANZO S, et al.Radio resource sharing as a service in 5G: a software-defined networking approach[J].Computer Communications, 2017, 107: 13-29.

(收稿日期: 2022-11-04)

作者简介:

梁亚从(1994-),通信作者,女,硕士研究生,主要研究方向:6G 安全、分布式信任,E-mail:liangyacong@cictmobile.com。

夏旭(1980-),男,硕士研究生,高级工程师,主要研究方向:5G/6G 核心网架构、空天一体技术等。

包施晗(1992-),男,博士研究生,主要研究方向:后 5G 内生安全、隐私保护。

扫码下载电子文档

(上接第 4 页)

[7] 林奕琳.6G 网络潜在关键技术研究综述[J].移动通信, 2021, 45(4): 120-127.
[8] Liu Yang, Wei Yifei, YU F, et al.Joint routing and scheduling optimization in time-sensitive networks using graph convolutional network-based deep reinforcement learning[J].IEEE Internet of Things Journal(Early Access), 2022.
[9] Wu Zonghan, Pan Shirui, Chen Fengwen, et al.A comprehensive survey on graph neural networks[J].IEEE Transactions on Neural Networks and Learning Systems, 2020, 32(1): 4-24.
[10] VAN HASSELT H, GUEZ A, SILVER D.Deep reinforcement learning with double q-learning[C]//Proceedings of the AAAI Conference on Artificial Intelligence, 2016: 2094-2100.
[11] GAVRILUT V.Scheduling in time sensitive networks(TSN) for mixed-criticality industrial applications[C]//Proceedings of IEEE International Workshop on Factory Communication Systems, 2018.

(收稿日期: 2022-09-16)

作者简介:

邢燕霞(1972-),女,硕士,高级工程师,主要研究方向:移动通信网络架构和关键技术、网络运营和管理。

胡兴洪(2000-),男,硕士,主要研究方向:移动通信网络架构和关键技术、人工智能技术应用。

扫码下载电子文档

版权声明