DOI:10.12158/j.2096-3203.2020.06.002

基于侧链技术的电力物联网跨域认证研究

李大伟[1,2]，霍瑛[1,2]
（1. 南京工程学院计算机工程学院，江苏 南京 211167；
2. 南京工程学院能源研究院，江苏 南京 211167）

摘　要：能源互联网和 5G 通信技术的发展使电力物联网规模不断增大，对于跨域数据交换的业务需求缺少有效的认证手段。文中分析了电力物联网终端跨域认证需求和面临的问题，介绍了区块链跨链技术中的侧链技术及实现机理，并将其引入到电力物联网跨域认证方案中，提出一种基于侧链技术的电力物联网跨域认证方案。首先建立基于侧链技术的跨链认证架构，设计区块数据结构和双向锚定认证信息传递模型，通过公钥证书和数字签名生成认证凭据，通过时间戳确保认证信息的时效性。然后提出基于侧链技术的电力物联网终端跨域认证流程，实现认证凭证从申请域到认证域的可信传递。认证方案通过主链和侧链进行数据交互和共享，具有认证信息跨域有效、不可篡改以及分布式共识的特点。最后，在配电自动化应用场景中进行仿真，验证了该方案的可行性。

关键词：电力物联网；区块链；侧链技术；双向锚定；接入认证
中图分类号：TM71；TP391.44　　**文献标志码**：A　　**文章编号**：2096-3203(2020)06-0008-05

0　引言

随着 5G 和能源互联网的发展以及电力物联网部署范围的增大，终端可信接入对电力系统整体安全性的影响越来越大[1—2]。传统电力物联网接入安全主要依靠集中式的密钥管理机制，其缺点是认证效率低、易出现单点失效的风险。随着分布式电源、可控负荷、增量配电网、物资服务等需要跨域数据共享的综合性业务的不断涌现，集中化的接入认证手段已无法满足电力物联网源网荷储互动、物资精准供应等由多方参与的跨域业务系统的信任需求，因此需要探索跨域认证方案[3]。

区块链技术作为一种去中心化场景中信任传递的有效方法，得到了物联网安全领域的广泛研究[4—6]。文献[7]提出一个基于区块链的物联网访问控制框架，为物联网目标、模型、架构和机制规范提供了参考模型。接入认证方面，文献[8—9]提出基于区块链的分布式公钥基础设施(public key infrastructure，PKI)系统，通过公共总账来记录用户证书，解决传统 PKI 系统单点故障问题。文献[10]提出一种基于区块链的安全认证协议，确保物联网结点整个生命周期中认证数据的有效性。跨域认证方面，文献[11]使用区块链技术设计了分布式用户认证框架，通过智能合约向每个站点授予不同的权限。文献[12]提出一种基于区块链的有效跨域认证方案，该方案包括区块链证书颁发机构的信任模型和体系结构、区块链证书格式和用户跨域认证。

目前的研究主要集中在利用单一区块链来提高认证服务的分布性和可信度[13—15]。但单链结构在运行效率、维护成本和隐私保护等方面难以满足能源互联网业务的需求。文中针对电力物联网环境下认证证书安全存储和共享、跨域信任传递机制、认证参数易被篡改等问题，构建分布式共识的接入认证策略，将传统的中心化认证策略下放到边缘侧，通过不可篡改的认证凭据实现灵活有效的跨域认证，对电力物联网的安全运行具有重要意义。

文中介绍了跨链技术中的侧链技术并将其引入到电力物联网跨域认证中；提出了基于双向锚定的电力物联网跨域认证方案；开发了原型系统并在配电自动化业务场景中进行试点，验证了该方案的可行性。

1　基于侧链的认证技术

侧链协议是一种链链互动的跨区块链数据交互方案，是多区块链跨链数据交换的重要形式[16—19]。通过这种技术，可以实现数字资产从第 1 个区块链到第 2 个区块链的转移，又可以在稍后的时间点从第 2 个区块链安全返回到第 1 个区块链。其中第 1 个区块链称为主链，第 2 个区块链称为侧链。

侧链技术通过将不同区块链相互连接在一起，扩展了单条区块链的技术，实现了账本之间的互操作，在减缓主链处理压力的同时确保了本地域中信息的可控共享。侧链架构的好处是代码和数据独

收稿日期：2020-06-05；修回日期：2020-07-11
基金项目：国家自然科学青年基金项目(61802174)

立,不增加主链的负担,避免数据过度膨胀,是一种天然的分片机制。

侧链技术的核心是实现主链和从链的协同与数据交互,这种协同机制称为“双向锚定”。双向锚定实现了同一数据资产在主链和侧链上的流动,当主链上的资产锁定时,侧链上可以释放等价的固定侧链资产;当侧链上的资产被锁定之后,主链上等价的资产被释放。实现双向锚定的方法主要如下:

(1) 对称式双向锚定。数据在侧链和主链之间的转移机制相同,2 个方向进行对等的简单支付验证(simplified payment verification,SPV),确保数据在一个链中的真实性。数据交换时,主链和侧链的地位是对等的。

(2) 非对称式双向锚定。侧链和主链的信息不对称,侧链上的用户对主链能完全验证,而主链上的数据向侧链转移的时候需要进行 SPV 验证。该模式下,侧链的验证者需要跟主链进行同步。

(3) 单一托管模式。在主链上指定一个托管方,实现主链侧链同步时的信息锁定、资产同步和解锁功能。

(4) 联合托管模式。部署多个托管中心以联盟的方式对主链和侧链的数据交换进行确认,联盟成员之间通过多重签名机制确保数据的安全性。

(5) SPV 模式。用户将数据发送到主链上,经过主链上 6 个区块的确认之后,交易以主链区块的形式存储到账本中,主链通过创建 SPV 验证的形式启动侧链数据更新。

(6) 驱动链模式。用户驱动主链和侧链之间的数据互动,并监测侧链的状态,通过共识算法确保数据的一致性。

电力物联网跨域认证中,每个认证域都有各自的认证策略和凭证,存储在本地链的分布式账本,即侧链中。由多个认证域组成的电力物联网系统维护一个认证链,作为系统的主链。

终端需要跟远程域进行数据交互时,发起跨域认证请求。首先将本地的认证凭证通过双向锚定的方式传递到主链,主链对凭证进行确认后用同样的方式传递到远程域,远程域的侧链就具有了对本地域终端进行认证的能力。具体过程如图 1 所示。

双链互动的电力物联网跨域认证中区块链结构如图 2 所示。其中侧链包含的认证信息通过 hash 处理后以元数据的形式,通过双向锚定发布到主链中,作为主链区块体的一次记账,通过另一次双向锚定,这些信息以一种安全的方式传递到远程认证域的侧链中,从而实现认证信息的跨域交互。

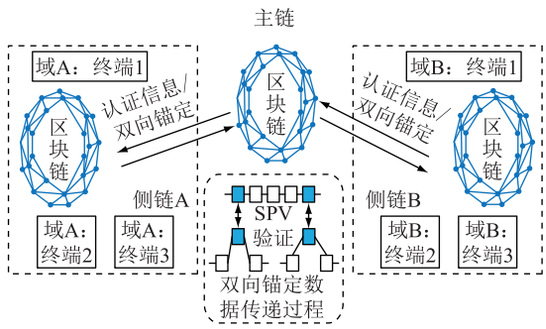

图 1　基于侧链技术的认证架构

Fig.1　Authentication architecture based on side chain technology

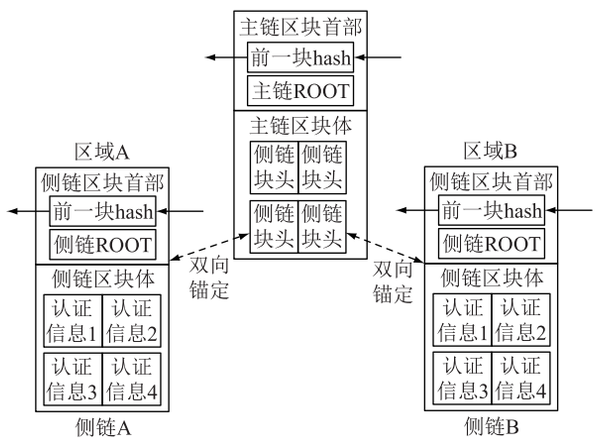

图 2　区块链结构

Fig.2　Blockchain structure

2　跨域认证方案

电力物联网环境具有一定复杂性,大范围的组网和海量并发接入方式带来了接入鉴权、隐私保护、传感节点认证等方面的安全风险。随着能源互联网的发展,电力物联网承载的电力生产自动化、输电线路检测、变电配电调度自动化、电力负荷控制、电力市场交易、电力用户信息管理、分布式绿色能源等业务都有跨域认证需求。电力物联网跨域认证中,认证信息保存在各自域的侧链中,认证信息包括系终端标识、公钥证书、时间戳、权限标识等。在侧链中,所有结点的认证信息都是共识的,并通过数字签名的方式进行鉴权。区块链中数据的一致性保证了恶意结点很容易被发现,因此侧链中的认证信息具有权威性,可以进行域间传递。

假设认证参与者为 A 和 B,认证请求方为 A,验证方为 B。A 负责提供认证数据和对应的数据索引,通过侧链 A 和主链的双向锚定将记录上传到主链,B 所在区域的侧链 B 与主链交互信息,得到认证数据,实现对 A 的认证。其认证协议的流程如图 3 所示。

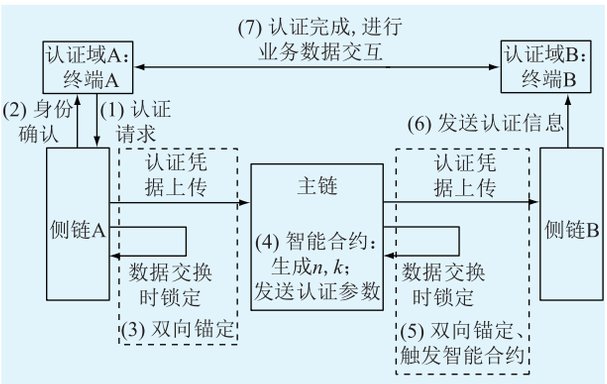

图 3　认证协议流程

Fig.3　Authentication protocol process

（1）本地域内节点 A 发起跨域认证请求。对唯一身份标识 I_A，远程域节点标识 I_B，时间戳 t 和持有的证书信息 c_A 进行数字签名，$\mathrm{En}_{s_A}(I_A \| t \| c_A \| I_B)$，其中 En( ) 为公钥加密算法，推荐使用标识基加密体制（identity-based cryptograph，IBC），s_A 为 A 的私钥，作为签名的密钥。节点 A 触发侧链 A 上的智能合约，将带有数字签名的跨域认证请求信息上链。

（2）侧链 A 上的验证逻辑结合侧链 A 中存储的公钥信息进行查询和验证。具体如下：首先用 A 的公钥 p_A 进行解密，然后验证证书。如果能正确解密获得请求方的身份标识、时间戳和数字证书，则本地认证通过，可发起对主链的认证信息交换，否则返回错误信息。

（3）侧链 A 与主链进行双向锚定，将请求信息的 hash 值传递至主链存储。具体包含 2 个步骤，步骤一：生成认证请求，包含请求方和接受方的唯一身份标识，并用哈希函数进行打包：$\mathrm{Hash}(I_A \| c_A \| I_B)$，Hash( ) 为哈希函数；步骤二：锁定侧链 A 中对应区块，以保持认证信息的一致性，将认证信息转移到公链中。

（4）双向锚定完成后，触发公链中的智能合约，生成随机数 n 和临时会话密钥 k，并通过 P2P 信道发送给请求节点 A，格式为 $\mathrm{En}_{p_A}(t \| n \| k)$。

（5）发起对认证域 B 中侧链 B 的双向锚定，将认证信息写入侧链 B。

（6）公链与侧链 B 的双向锚定完成后，触发侧链 B 中智能合约，验证认证信息，并将临时会话密钥发送给 B，格式为 $\mathrm{En}_{p_B}(I_A \| t \| n \| k \| c_A)$，其中 p_B 为 B 的公钥。

（7）本地域节点 A 和远程域节点 B 之间完成接入认证，双方可进行业务数据交互。

基于侧链技术的电力物联网接入认证具有以下优势：（1）数据真实不可篡改，更可靠。利用区块链不可篡改特性，保证数据不会被篡改。（2）数据链链传递过程中进行了加密处理，即使认证请求数据被窃取，也无法破解和非法使用。（3）认证服务器部署在边缘侧，通过边缘物联代理进行数据转发，系统运行效率和安全性都可以保证。（4）使用智能合约完成交互，更开放。使用智能合约进行业务访问时，根据定义好的规则，只返回业务结果，保证平台的数据更安全，更开放。

3　仿真分析

文中采用基于 HyperLedger Fabric 联盟链搭建实验环境，认证场景为配电监控终端装置的跨域认证。实验环境分为 2 个认证域，每个认证域部署 1 台边缘认证服务器，配置为 Intel i7-7700HQ CPU，主频 2.80 GHz，16 GB DDRIII 内存，256 GB SSD 硬盘，操作系统为 CentOS 7，系统运行 Docker 容器级虚拟化系统模拟 P2P 区块链网络，容器编排工具为 kubernetes 1.9。认证网关为嵌入式系统，配置为博通 BCM2837B0 SOC，集成 4 核 ARM Cortex-A53 64 位 CPU，主频 1.4 GHz，1GB LPDDR2 SDRAM。

仿真基于国网某公司配电自动化系统。请求节点位于区域 A，被请求节点位于区域 B，每个区域运行侧链，主站所在区域运行主链。拓扑关系如图 4 所示。

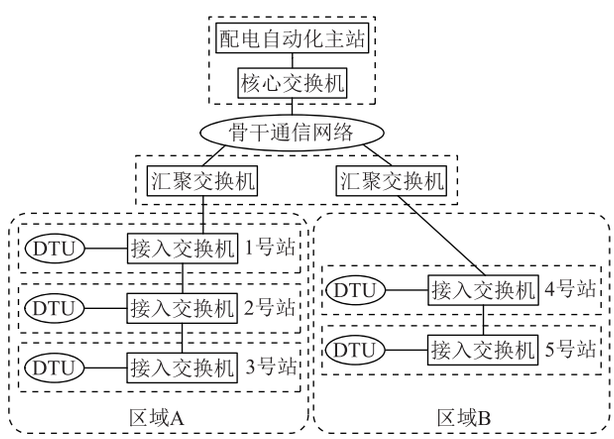

图 4　仿真试验拓扑

Fig.4　Simulation topology

在每个站点配电终端单元（distribution terminal unit，DTU）上安装部署认证网关，使其成为区块链中的节点，具有运行智能合约、访问分布式账本和进行分布式认证投票的功能。实验共选取 14 个 DTU 进行验证，采集了不同并发数量下的系统性能，所有数据为 10 次实验的平均值。

图 5 为电力物联网终端跨域接入从申请到接入

完成所需要的时间开销,对比曲线是传统集中式管理中的时间开销。可以看出,在传统的集中式接入认证方案下,认证中心计算和网络开销随物联网终端数量的增加而增大,导致认证效率降低,直接反应为认证时间的迅速增长。而在基于区块链的分布式认证方案下,当物联网终端节点数量较少时,认证效率较集中式认证低,这是因为区块链方案中运行分布式认证协议开销在网络规模较小时占比较大,当物联网规模增大时,认证效率有明显提高。

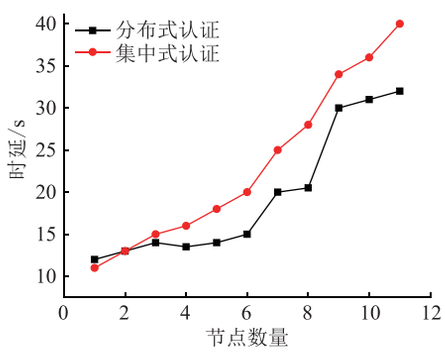

图 5 认证时间曲线

Fig.5 Certification time curve

图 6 为并发接入时认证服务器 CPU 负载随节点数量增加的情况,由于采用了 kubernetes 的弹性调度算法,CPU 增加情况在可接受范围内。分析仿真数据可知,随着区块链长度的增加,新区块生成时间相应增加。当并发数量从 7 个增加到 14 个时,CPU 负载从 20%增加到 60%,系统性能在可接受范围内。在实际应用环境部署中,可通过增加服务器系统资源以支持更大范围的并发业务。

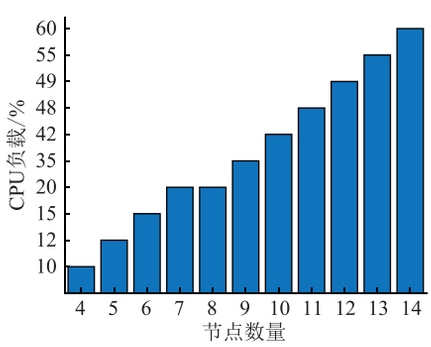

图 6 认证性能

Fig.6 Certified performance

4 结语

按照规划,预计到 2025 年接入电力物联网终端的设备将超过 10 亿台,到 2030 年将超过 20 亿台。电力物联网规模的扩大使得跨域数据交互需求显著增加。区块链是一种分布式数字账本技术,具有主体对等、公开透明、安全通信、难以篡改和多方共识等特性,是继大数据、云计算、人工智能、虚拟现实等技术后又一项将对未来产生重大影响的新兴技术,在电力物联网中的应用日益广泛。

文中针对物联网跨域认证中的安全问题,基于侧链技术,研究双链协同机制并应用到电力物联网跨域认证场景中,将认证信息存储在多级分布式账本中进行安全传递,通过本地链和联盟链数据可信互动共享,实现认证策略的漫游,达到提高边缘侧接入认证能力,避免传统认证中心计算、存储和时间开销以及单点失败问题。仿真结果显示,文中方案在可行性和执行效率等方面较传统集中式认证方案具有显著优势。下一步研究将在具体的电力物联网场景中进行试点和验证。

本文得到江苏省高校自然科学基金项目(19KJB520036),南京工程学院人才引进项目(YKJ201721),南京工程学院校级科研基金项目(CXY201922)资助,谨此致谢!

参考文献:

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

[2] 吕继伟. 基于泛在电力物联网的换流站在线监测系统优化综述[J]. 电力工程技术,2019,38(6):9-15.
LYU Jiwei. Optimization survey of online monitoring system for converter station based on ubiquitous power IoT[J]. Electric Power Engineering Technology,2019,38(6):9-15.

[3] 丁永善,李立新,李作辉. 基于证书的匿名跨域认证方案[J]. 网络与信息安全学报,2018,4(5):32-38.
DING Yongshan, LI Lixin, LI Zuohui. Certificate-based cross-domain authentication scheme with anonymity[J]. Chinese Journal of Network and Information Security,2018,4(5):32-38.

[4] ABDULKADER O,BAMHDI A M,THAYANANTHAN V,et al. A lightweight blockchain based cybersecurity for IoT environments[C]//The 6th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2019). IEEE, 2019.

[5] WU M, WANG K, CAI X, et al. A comprehensive survey of blockchain:from theory to IoT applications and beyond[J]. IEEE Internet of Things Journal,2019,6(5):8114-8154.

[6] ALI M S,VECCHIO M,PINCHEIRA M,et al. Applications of blockchains in the Internet of things:a comprehensive survey [J]. IEEE Communications Surveys & Tutorials,2019,21(2): 1676-1717.

[7] OUADDAH A,ELKALAM 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.

[8] FROMKNECHT C, VELICANU D. Cert coin: a namecoin based decentralized authentication system [EB/OL]. [2020-06-05]. http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf, 2014.

[9] FROMKNECHT C, VELICANU D. A decentralized public key infrastructure with identity retention [EB/OL]. [2020-06-05]. https://eprint.iacr.org/2014/803.pdf, 2014.

[10] MOINET A, DARTIES B, BARIL J. Blockchain based trust authentication for decentralized sensor networks [EB/OL]. [2020-06-05]. https://arxiv.org/pdf/1706.01730.pdf, 2017.

[11] ZHANG L, LI H, SUN L, et al. Poster: towards fully distributed user authentication with blockchain [C]//Privacy-Aware Computing (PAC), 2017 IEEE Symposium on IEEE. 2017: 202-203.

[12] 周致成,李立新,李作辉. 基于区块链技术的高效跨域认证方案[J]. 计算机应用,2018,38(2):316-320,326.
ZHOU Zhicheng, LI Lixin, LI Zuohui. Efficient cross-domain authentication scheme based on blockchain technology [J]. Journal of Computer Applications, 2018, 38(2): 316-320, 326.

[13] JIA Xudong, HU Ning, SU Shen, et al. IRBA: an identity-based cross-domain authentication scheme for the internet of things [J]. MDPI, 2020, 9(634): 1-21.

[14] 马晓婷,马文平,刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报,2018,46(11):2571-2579.
MA Xiaoting, MA Wenping, LIU Xiaoxue. Across domain authentication scheme based on blockchain technology [J]. ACTA Electronica Sinica, 2018, 46(11): 2571-2579.

[15] YANG Yanyan, HU Mingsheng, KONG Shan, et al. Scheme on cross-domain identity authentication based on group signature for cloud computing [J]. Wuhan University Journal of Natural Sciences, 2019, 24(2): 134-140.

[16] 李芳,李卓然,赵赫. 区块链跨链技术进展研究[J]. 软件学报,2019,30(6):1649-1660.
LI Fang, LI Zhuoran, ZHAO He. Research on the progress in cross-chain technology of blockchains [J]. Journal of Software, 2019, 30(6): 1649-1660.

[17] 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(2):35-48.
GUO Zhao, GUO Shuaiyin, ZHANG Shengli, et al. Analysis of cross-chain technology of blockchain [J]. Chinese Journal on Internet of Things, 2020, 4(2): 35-48.

[18] 叶少杰,汪小益,徐才巢,等. BitXHub:基于侧链中继的异构区块链互操作平台[J]. 计算机科学,2020,47(6):294-302.
YE Shaojie, WANG Xiaoyi, XU Caichao, et al. BitXHub: side-relay chain based heterogeneous blockchain interoperable platform [J]. Computer Science, 2020, 47(6): 294-302.

[19] 张诗童,秦波,郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全,2018,9(11):57-62,67.
ZHANG Shitong, QIN Bo, ZHENG Haibin. Research on the protocol of multiple cross-chains based on the hash lock [J]. Cyberspace Security, 2018, 9(11): 57-62, 67.

作者简介:

李大伟

李大伟(1981),男,博士,高级工程师,从事区块链技术、信息安全、电力物联网技术等领域研究工作(E-mail:lidw@njit.edu.cn);

霍琰(1988),女,博士,副教授,研究方向为区块链技术、智能计算等。

Cross domain authentication of power IoT based on side chain

LI Dawei[1,2], HUO Ying[1,2]

(1. School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China;
2. Energy Research Institute, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: With the development of energy Internet and 5G communication technology, the scale of power IoT is increasing, and there is a lack of effective authentication means for cross domain data exchange. The requirements of power IoT terminal cross domain authentication are analyzed and the side chain technology and its implementation mechanism in the cross chain technology of blockchain are discussed. Then, a cross domain authentication scheme of power IoT based on side chain technology is proposed. Firstly, the cross chain authentication architecture based on side chain technology is established, and the block data structure and two-way peg authentication information transfer model are designed. The authentication credentials are generated by public key certificate and digital signature, and the timeliness of authentication information is ensured by time stamp. Then, the cross domain authentication process of power IoT terminal based on side chain technology is proposed, which realizes the authentication certificate from application domain to authentication trusted delivery of the domain. Through the interaction and sharing of main chain and side chain data, the authentication scheme has the characteristics of cross domain effective, tamper proof and distributed consensus. Finally, simulation experiments are carried out in the application scenarios of distribution automation system to verify the feasibility of the scheme.

Keywords: power internet of things; blockchain; side chain technology; two-way peg; access authentication

(编辑　方晶)