第46卷 第8期 2022年4月25日
DOI：10.7500/AEPS20210127006
电力系统自动化
Automation of Electric Power Systems
Vol. 46 No. 8 Apr. 25，2022

基于区块链的联盟信任分布式认证在电力行业的应用探索

王 栋[1,2]，杨 珂[1,3]，王 瑜[4]，玄佳兴[1,2]，陈 亚[4,5]，许洪华[6]
（1. 国网电子商务有限公司，北京市 100053；2. 国网区块链科技(北京)有限公司，北京市 100053；
3. 国家电网有限公司区块链技术实验室，北京市 100053；4. 中国科学院信息工程研究所，北京市 100093；
5. 中国科学院大学网络空间安全学院，北京市 100093；
6. 国网江苏省电力有限公司南京供电分公司，江苏省南京市 210019）

摘要：电力业务快速发展使其网络安全边界不断扩大，而电力业务系统大多停留在中心化身份或联盟身份阶段，难以应对海量接入、异构认证、频繁交互等新需求。首先，文中提出适用于电力行业的基于区块链的联盟信任分布式认证体系。然后，从网络架构、用户身份控制和隐私保护3个角度分析该体系的适用性，阐述其体系架构及运行机制。该体系设计了联盟数字身份，并按照共识和隐私保护策略将身份信息存储在分布式身份账本中，提供数字身份的全生命周期管理，实现身份数据的跨域安全共享和自主控制以及用户的跨域身份认证。最后，针对充电桩充电生态圈、电网人员安全管理、电力供应链金融3个行业场景面临的身份认证瓶颈，提出了基于该体系的解决思路。

关键词：电力业务；区块链；分布式身份认证；身份认证

0 引言

电力业务融合5G、边缘计算、物联网、人工智能等前沿技术，推动了充电桩、智能家居、电费金融等众多新电力业务的快速发展。各新业务系统终端与用户量持续增加，出现海量接入、异构认证、频繁交互[1]等新的需求。数字身份认证体系作为防护电力行业网络安全的第一道关口，既要满足新业务跨域统一身份认证需求，又要应对前沿技术带来的问题和挑战[2]。

面对中国电力行业新业务规模越来越大、分布越来越广的情景，现有电力业务身份认证系统大多停留在中心化身份或联盟式身份阶段，运用分布式认证技术建立统一、适应新业务的安全身份认证体系的探索刚刚开始[3-4]，仍存在诸多问题。一是传统基于中心式的数字证书认证体系中[5-7]用户身份难以可信高效互通，分布式业务系统上架设单一身份认证服务器使得数据完全被中心机构管理控制，无法实现用户身份主权自我控制。二是随着电力物联网建设过程中微服务、微应用的发展，身份管理不只是考虑人的认证，设备和服务同样需要身份认证[8-10]。因此，需要将人、设备、服务等建立统一身份标识库进行管理。三是实际应用中使用频次较高的电力应用通常安全风险低，重便携性，而安全风险高的通常使用频次低，重安全性[11-12]，各应用间的认证交互较差。

针对电力新型业务提出的更高需求，基于区块链的新型分布式数字身份引起了电力行业高度关注。目前，分布式数字身份已取得了一些成果，如MicrosoftDID[13]、HyperLedger Indy[14]、uPort[15]、Civic[16]、SelfKey[17]等分布式数字认证验证原型。此外，万维网联盟(World Wide Web Consortium，W3C)、全球去中心化身份联盟(Decentralized Identity Foundation，DIF)以及结构化信息标准促进组织(Organization for the Advancement of Structured Information Standards，OASIS)[18-19]等国际组织也正加紧制定相关标准规范。这些方案实现了用户完全自主控制身份信息，但缺乏对用户身份的严格审核和监管，存在恶意用户注册为合法身份的重大隐患，并且危害服务系统后，因用户完全自主控制身份生成的特点造成难以追踪。新型电力系统的新业态、新服务模式具有大规模分布式能源主体接入、设备种类繁多、交互频繁等特点，需要严格管控接入电力业务实体，最大限度地保证电力业务系统的安全，上述基于区块链的身份认证技术难以满足电力行业可监管自主控制和安全可移植的身份认

收稿日期：2021-01-27；修回日期：2021-11-16。
上网日期：2022-03-04。
国家电网公司科技项目(面向电网应用场景的电力区块链智能合约关键技术研究，5700-202072372A-0-0-00)。

证要求。此外,区块链在支撑能源电力行业新业态、新服务模式上成为重要的创新方向[20-22]。针对能源区块链业务,该体系可以采用双链模式或与原有能源区块链集成等方式[23-25]部署,在不影响原有业务的情况下提供更为安全、灵活可靠的身份认证服务。

本文构建了基于区块链的电力行业联盟信任分布式数字身份认证体系,建立了电力行业数字身份,根据业务模式详细阐述了系统架构与运行机制,同时设计了涵盖联盟数字身份注册、验证、更新、撤销等环节的全生命周期弹性管控机制。最后,设计和实现了该认证系统,并对联盟分布式身份认证的3个典型应用场景提出实施思路。

1　联盟分布式身份认证体系在电力行业的适用性分析

电力行业业务系统身份认证体系由中心化身份、联盟式身份、以用户为中心数字身份逐渐向联盟去中心化身份体系演进。以下从网络架构、用户身份控制、隐私保护角度分析区块链联盟分布式身份认证在电力系统的适用性。

1)网络架构

目前,电力行业中不少业务系统采用微服务架构[26-27],将单体结构系统转换为分布式系统,大多使用中心化统一身份认证体系[3,5]。然而,中心化身份认证服务器易遭受恶意攻击[28],比如分布式拒绝服务(distributed denial of service,DDoS)攻击、单点故障等。区块链技术的分布式架构[29-30]契合身份认证需求,多个组织构建可信联盟网络[31],去中心化节点在多个服务器上运行,消除了对集中化服务器的依赖。该技术可为电力行业实体建立身份标识库,实现身份跨域统一安全管理。

2)用户身份控制

用户对身份信息的控制要求愈加细化[32],但中心化数字身份的第三方机构和联盟数字身份的超级中心使用户无法实现身份控制。区块链将信息上链存储过程记录进分布式账本,根据智能合约自动执行策略,实现用户身份的注册管理[33],身份控制权由第三方机构或组织转移到用户手中,并保证记录的可追溯、防篡改,安全性较高。根据电力业务场景的需求,本文设计了用户身份监管机制,可促进跨部门、跨地域的身份认证和数据协同。

3)隐私保护

异构分布式网络中任意系统的暴露都会泄露其他系统用户隐私,区块链分布式身份认证利用隐私保护策略改变用户数字身份数据的所有权,采用零知识证明和同态加密[34]技术有选择地共享用户身份信息,以实现隐私保护。

综上所述,联盟分布式身份认证技术依托区块链实现电力行业实体的数字身份全生命周期管理、安全交互以及弹性管控,保障身份信息的可信存储、可追溯和防篡改[35],并确保电力业务系统的安全。此外,身份认证的去中心化特点可以避免服务器因受到攻击而造成全网瘫痪。

2　联盟分布式数字身份关键概念

电力行业数字身份的标准化是电力行业实现统一身份认证的基础。本文采用联盟分布式数字身份作为电力行业数字身份,其由联盟分布式数字身份标识符(以下简称联盟ID)和联盟数字身份凭证(以下简称凭证)组成。前者为联盟内实体的唯一标识,后者本质上是与实体相关联的身份属性声明集合,以证明实体身份真实性。数字身份相关信息由联盟分布式身份账本存储。

2.1　联盟ID

联盟ID用来代表电力系统中实体的一个数字身份,由标识符以及与之关联的公私钥对[18]组成,其中,公私钥用于控制身份和签署身份证明。联盟ID具有联盟内公开唯一、分布式与自主可控等特点。电力服务系统或设备、业务或监管部门、安全管理人员、上下游单位、外部第三方(如银行金融机构)等各类实体可以自主完成联盟ID的注册、解析、更新或撤销操作。

单个电力系统中的实体可拥有多个数字身份,结合电力行业标识规范可以分配多个联盟ID,在不同场景下拥有与之对应的身份凭证,如图1所示。联盟ID及其公钥存储在账本上,同一实体的不同身份标识符之间没有关联信息,攻击者难以分析联盟ID和实体之间的联系,有效避免信息归集造成隐私泄露。联盟ID虽然对全局公开,但是不包括和实体真实身份相关的信息,需依赖实体的凭证[19]验证身份。

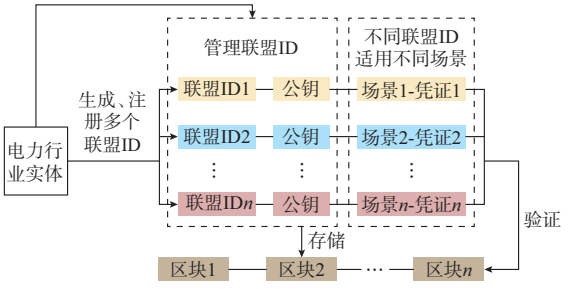

图1　用户的多个数字身份示意图

Fig. 1　Schematic diagram of multiple digital identities of a user

2.2　凭证

凭证是电力系统中实体身份信息真实性的证明，也是电力行业联盟信任分布式数字身份认证体系架构对接入电力系统实体进行监管的手段。该凭证核心是一组实体身份属性的集合，并附上了颁发者的签名及凭证元数据。凭证用于描述实体的某些身份属性，联盟ID持有者通过凭证向其他实体证明自己的属性可信。凭证由用户保存，数据结构由账本存储。

1）凭证数据结构

凭证的数据结构包括3个部分：元数据、属性定义集合和颁发者相关签名信息。元数据包括凭证名称、颁发者、颁发日期等；属性定义集合包含用户具体身份属性信息，内容可包括人员姓名、性别、编号、所属部门、职称等；签名信息包括颁发者使用的签名算法、凭证创建时间、创建者、数字签名信息等。

2）业务交互流程

凭证的业务交互流程如图2所示，包括凭证颁发者、持有者和验证者3类角色，三者在业务交互前根据场景需求注册联盟ID并将其上链存储。业务交互双方须完成对双方联盟ID的解析和验证，建立可信连接进行业务交互，实现一种以身份持有者为主导，凭证颁发者和验证者不需要直接通信的凭证流转与验证方式。

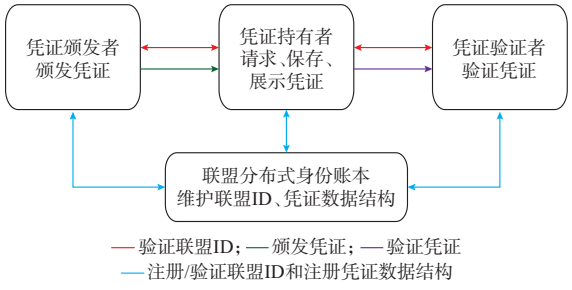

图2　基于凭证的业务交互示意图

Fig. 2　Schematic diagram of certificate-based business interaction

颁发者是指审核电力系统中实体身份信息真实性并能开具凭证的实体，如电力业务管理或监管部门；持有者即实体用户，如电力系统或设备、安全管理人员、上下游单位、外部第三方机构等。电力系统中实体用户向颁发者请求颁发身份凭证，接受颁发者对其身份信息的审核，向验证者出示凭证，身份凭证由用户保存，便于“一次颁发、多次使用”。验证者接受凭证并进行匿名或最小化披露验证，若通过则为该用户提供后续服务。该用户在联盟ID的基础上完成凭证的认证从而进行跨域业务应用。

2.3　联盟分布式身份账本

联盟链作为底层技术[29]符合电力行业可信交互、无缝对接需求，具有性能较优、监管友好等特性。各电力业务组织机构都有记账权，维护同一份账本实现身份互认。智能合约作为区块链的跨域服务协议[36]，完成不同应用间高效认证交互。认证体系编写智能合约实现联盟ID和凭证的业务逻辑处理，包括联盟ID的注册、查询、更新和撤销操作，以及身份凭证数据结构的定义、查询、更新和撤销操作。

联盟分布式身份账本用于维护存储联盟ID的数据库及各凭证的数据结构，在联盟内公开可见。凭证中包含用户身份属性信息，由用户自身保存，若存到账本中联盟内全局可见，易产生隐私泄露问题。

3　身份认证机制

3.1　体系架构

基于区块链的电力行业联盟信任分布式认证体系架构如图3所示。架构分为基础层、服务层及应用层。基础层主要由不同的电力业务组织机构共同搭建底层联盟分布式身份网络，各区块链节点通过共识机制维护同一份账本。服务层的中间代理程序作为身份层协议接收上层用户接口请求，进行业务逻辑处理，根据隐私保护策略为用户提供存储方案。凭证协议提供数字身份凭证的颁发、更新、验证以及撤销过程的处理逻辑。应用层面向电力业务系统构建应用程序，支持用户进行联盟分布式数字身份的全生命周期管理，提供必要的应用程序管理服务，其中，身份钱包存储用户的联盟ID和身份凭证。

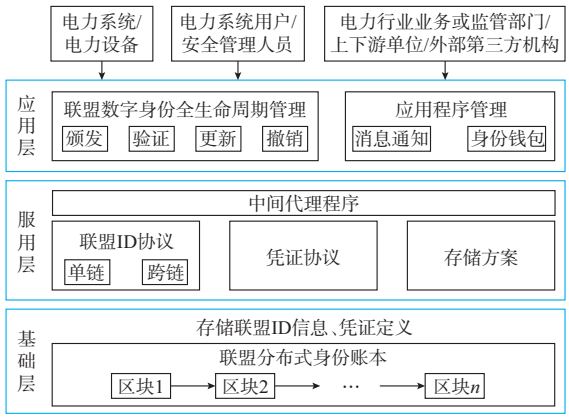

图3　基于区块链的电力行业联盟信任分布式认证的体系架构

Fig. 3　Architecture of blockchain-based distributed authentication with alliance trust in power industry

3.2　运行机制

基于区块链的电力行业联盟信任分布式认证体系运行机制如图4所示。运行机制包括4个部分。

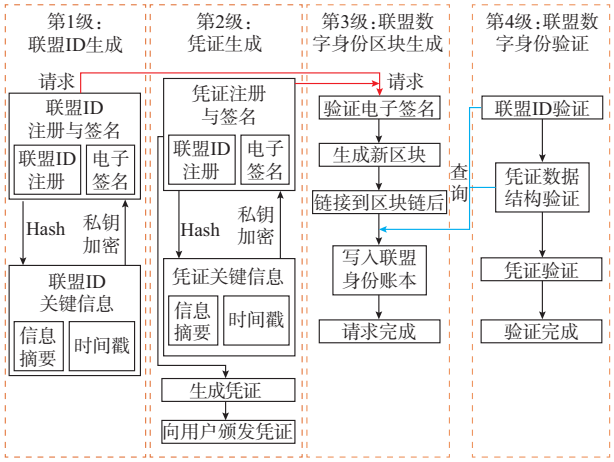

图4　基于区块链的电力行业联盟信任分布式认证体系运行机制

Fig. 4　Operation mechanism of blockchain-based distributed authentication with alliance trust in power industry

1)联盟ID生成：电力业务用户注册联盟ID及其公私钥对，进行Hash计算与数字签名后发送到账本。

2)联盟身份凭证生成：凭证颁发者将凭证的数据结构进行签名后发送到账本。颁发者在自身数据库中创建身份注册表，检索身份注册表后关联凭证与申请者线下角色。颁发者基于该凭证的数据结构、身份注册表与申请者基本信息为用户颁发凭证。

3)联盟数字身份区块生成：接收用户联盟ID以及凭证数据结构，验证电子签名，通过后生成新区块并广播至全网，达成共识后写入账本。

4)联盟数字身份验证：查询账本上的用户联盟ID和凭证数据结构，如果用户联盟ID和凭证都通过验证，则用户身份验证通过，否则验证不通过。

3.3　区块链身份认证的优势

目前，电力信息系统认证体系多采用由独立认证服务器来处理系统认证请求的方案，存在依赖于中心服务器以及隐私泄露、难以应对DDoS攻击等安全风险。基于区块链的联盟信任分布式身份认证系统在电力行业场景下的优势如表1所示。

表1　电力系统联盟信任分布式认证体系和传统身份认证体系的对比

Table 1　Comparison of blockchain-based distributed authentication system with alliance trust and traditional identity authentication system for power system

认证体系	身份控制	系统管理	信息共享	安全保障
传统身份认证体系	第三方机构完全控制用户身份	完全依赖于中心化身份认证服务器管理	数据不能针对性共享	服务器易遭受恶意攻击，系统中其他信息易泄露或破坏
区块链联盟信任分布式身份认证体系	用户身份自主控制	身份账本存储身份信息，各节点共同维护管理	在不暴露身份隐私的情况下实现跨域身份认证	底层区块链防篡改、可追溯

4　身份认证系统设计与实现

4.1　电力行业联盟分布式身份认证系统

电力行业联盟分布式身份认证系统示意图如图5所示，主要由联盟分布式数字身份账本、联盟分布式身份协议节点和分布式身份客户端3个部分组成。底层构建联盟链账本，存储联盟ID和凭证数据结构信息。此外，联盟链网络支持各组织节点动态进入与退出。联盟分布式身份协议节点连接账本和客户端，与下层用户相关联，接收用户客户端请求。各节点运行同一组智能合约，通过联盟ID协议和凭证协议提供业务逻辑处理。客户端为用户提供联盟ID及凭证管理、消息通知等服务。用户在客户端自主生成联盟ID，经协议节点在对应的账本上链存储。用户通过客户端可向相关权威机构申请凭证，实现凭证与联盟ID的绑定，以适应不同应用场景的跨域身份认证需求。

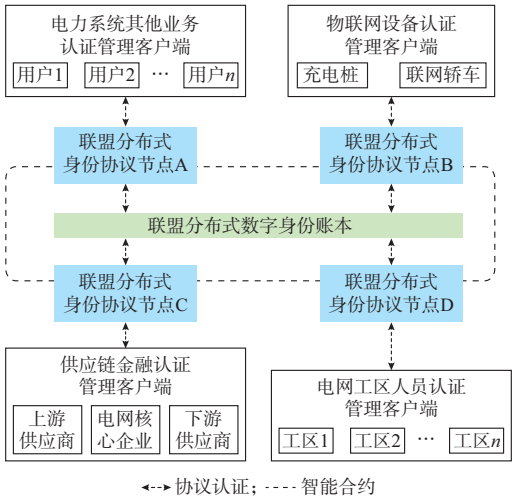

图5　分布式身份认证系统示意图

Fig. 5　Schematic diagram of distributed identity authentication system

4.2　全生命周期管理设计

全生命周期管理包括联盟ID全生命周期管理

和凭证管理2个部分。

4.2.1　联盟ID全生命周期管理

联盟ID全生命周期管理如附录A图A1(a)所示，包括联盟ID的注册、验证、更新与撤销流程。

首先，根据联盟ID的数据结构定义，各类电力业务系统用户根据自身类型进行注册。联盟ID的头部信息固定，用户选择对应的类型绑定相应公私钥对。用户将信息发送给账本上链存储，并存储在本地身份钱包中。其次，用户利用联盟ID及私钥，附以时间戳与数字签名后发送验证请求，接收方查询发送方联盟ID及公钥，利用该公钥信息进行验证。

当用户需要更新时，将变更请求发送至服务节点，经查询账本审核通过后在账本上更新联盟ID，标识旧联盟ID不可用，同步更新身份钱包。最后，用户可以提交撤销请求，审核后将联盟ID标识为已撤销。钱包中已撤销联盟ID相应变为用户不可用状态。

4.2.2　凭证全生命周期管理

1)凭证颁发

凭证颁发流程如附录A图A1(b)所示。颁发者向电力业务系统合法用户颁发凭证，该用户能够在系统中取得信任。第1阶段：用户与颁发者相互验证。以颁发者验证用户的联盟ID为例，颁发者收到用户消息后，查询账本中用户的联盟ID及其对应公钥，验证消息的签名，通过后颁发者与用户建立起初步可信连接。第2阶段：用户向颁发者请求获取凭证，并向账本发出请求，颁发者验证请求消息的签名。通过后颁发者识别参与实体角色，设置特定权限，为用户颁发数字身份凭证，用户接受凭证并存储在本地身份钱包中。

2)凭证验证

凭证验证流程如附录A图A1(c)所示。首先，拥有者与验证者进行联盟ID与公钥的验证，具体过程类似凭证颁发的第1阶段。验证通过则拥有者从钱包中取出凭证，向账本请求凭证的数据结构。拥有者创建证明消息，将消息发送给验证者。验证者接收证明消息，向账本请求得到凭证数据结构，对拥有者的凭证进行验证，通过则提供后续服务。

为实现隐私保护，凭证拥有者利用隐私保护策略有选择地暴露部分身份属性信息。隐私保护策略结合同态加密与零知识证明技术保证数据的安全性和隐私性。凭证验证协议采用Feige-Fiat-Shamir零知识身份认证协议，参与方为凭证拥有者和验证者，联盟链为可信第三方。凭证拥有者计算自己某些身份属性的零知识证明值用以验证，验证者通过验证后将自身联盟ID写入Merkle树中，并广播到整个联盟链所有节点。同时，零知识证明中的zk-SNARK密码技术包含同态加密思想，使用zk-SNARK加密身份数据，仅有通过认证的机构或组织，即拥有解密密钥者，才能够查看数据，实现数据安全共享。

3)凭证更新与撤销

凭证更新与撤销流程如附录A图A1(d)所示。首先，凭证拥有者与颁发者进行联盟ID与公钥的验证，过程类似凭证颁发的第1阶段。颁发者更新账本上的凭证数据结构，向拥有者发出通知。拥有者向账本请求数据结构，请求更新凭证。颁发者接收请求对用户进行验证，通过则颁发者更新凭证发送给用户，用户接受更新凭证并存储在身份钱包中。撤销操作中，当凭证到达有效期即视为撤销。

4.3　系统仿真验证

为验证本文提出的基于区块链的电力行业联盟信任分布式数字身份认证体系的有效性，本节将身份认证系统部署在联盟链上，针对分布式电力交易场景开展仿真验证。

联盟链中服务器的操作系统均为Linux 6.8，内存容量为32 GB，CPU核心个数为16，智能合约采用Solidity语言编写，在HyperEVM上执行。该仿真场景包括1个电力交易中心节点、6个电力用户节点(购电方或售电方)和2个电网企业节点，1组认证合约，并选取权威电力机构的节点作为5个鲁棒拜占庭容错(robust Byzantine fault tolerance，RBFT)共识节点，包括1个电力交易中心节点、2个电网企业节点与2个信用强的电力用户节点。其中，RBFT共识算法是本文对实用拜占庭容错(practical Byzantine fault tolerance，PBFT)的改进算法，具有通信开销小、吞吐量高、可扩展性强、容错性强等优点[37-40]，更适用于大规模分布式电力节点网络。分布式电力交易流程如下：首先，电力用户在电力交易中心节点通过身份认证后在区块链上发布售电信息或购电信息，按照符合交易条件就近匹配机制完成匹配；然后，与电网企业节点经过身份认证后签订三方供用电电子合同；最后，再次通过身份认证完成付款。

设计一组售电和购电数据如表2所示，在电力交易平台上通过主流性能测试工具Loadrunner 11(该客户端运行在性能测试机上，测试机的操作系统为Windows7，内存容量为16 GB，CPU型号为Intel Core i5)，运行完成1 000次身份认证测试过程。仿真测试在2种情形下分别执行一次。情形1：全部采

用基于证书颁发机构(certification authority,CA)颁发证书的身份认证;情形2:全部采用基于区块链的分布式身份认证。分别计算2种情形下1 000次验证的平均值,身份认证验证耗时结果如表3所示。联盟分布式身份认证平均验证耗时为86 ms/次,比一般系统的CA证书认证时间效率提高约13.1%,能够满足电力行业各参与主体之间的认证需求。

表2　电力用户购售电信息
Table 2　Information on purchase and sale of electricity by electricity users

报价者	角色	报价/(元·kW·h)$^{-1}$)	电量/(kW·h)
用户1	售电者	0.55	100
用户2	售电者	0.57	55
用户3	购电者	0.58	35
用户4	购电者	0.60	20
用户5	购电者	0.61	60
用户6	购电者	0.59	40

表3　身份认证验证耗时对比
Table 3　Time-consumption comparison of identity authentication verification

认证方式	验证次数	验证耗时/(ms·次$^{-1}$)
CA证书身份认证	1 000	99
联盟分布式身份认证	1 000	86

此外,进一步测试了该分布式电力交易仿真场景中基于区块链的身份认证系统的性能。如表4所示,针对不同并发用户数,基于区块链的身份认证平均响应时间随并发用户数的增加而逐渐增加,认证吞吐量先增加后降低,其中认证平均响应时间不超过93 ms,认证吞吐量约为500笔/s。而应用服务器CPU利用率不高于9%,内存利用率稳定在35.6%左右,事务通过率均为100%。可见,基于区块链的身份认证能够满足分布式电力交易下的业务需求。

表4　基于区块链的身份认证系统性能分析
Table 4　Performance analysis of blockchain-based identity authentication system

并发用户数	认证平均响应时间/ms	认证吞吐量/(笔·s^{-1})	CPU利用率/%	内存利用率/%	事务通过率/%
30	87	417.616	6.837	35.664	100
40	89	500.238	6.958	35.672	100
50	93	497.672	8.970	35.732	100

4.4　系统可行性论证

从法律可行性角度分析,文献[41]明确指出当事人提交的证据通过区块链技术存证,并经技术核验推定该证据材料上链后未经篡改,人民法院可确认该证据的真实性,为区块链证据的法律效力提供了依据。

从技术可行性角度分析,区块链具有不可篡改、多方共识、集体维护、防抵赖等特性,基于区块链的联盟信任分布式身份认证体系由高可信区块链生成身份凭证,共同背书其身份和公钥的绑定关系,能够代替CA证书,与基于CA证书的身份认证体系具有同等级别的保密性、认证性、完整性、防篡改性和安全性,同时节约CA机构高额的第三方服务费,成本更低,使用也更加便捷。

从可扩展性分析,区块链身份认证体系可以通过标准接口提供服务,在监管前提下支持自由扩展节点和自定义智能合约,集成开发工作量小,具有优秀的可扩展性。

5　应用场景探索

5.1　充电桩业务

充电桩运营商多采用中心化身份认证管理方式,充电桩和用户身份数据难以在生态圈内全局公开易形成孤岛,导致充电桩接入认证难,抵御单点攻击能力弱[42]。而联盟分布式身份认证可构建起统一、安全、互信的充电桩身份认证生态圈。

充电桩业务的应用结构示意图如附录B图B1所示。管理部门作为身份凭证颁发者,通过凭证全生命周期管理实现对各类充电桩有效管理。充电桩作为凭证持有者,出示凭证提供充电服务。充电用户作为验证者,也是电力最终消费者。认证过程的4个阶段如下:

身份初始化:参与主体通过客户端调用联盟ID协议生成联盟ID,将其存储在身份钱包中。

身份注册:参与主体将联盟ID通过共识和身份隐私保护存储在账本中,保证其身份安全共享互通。

凭证颁发:管理部门根据客户端接入请求及各运营商的申请资料,统一对接入电网的充电桩做联盟ID验签和可信性审核,颁发用电服务的凭证。客户端将凭证以加密方式保存于本地身份钱包中。凭证中包含颁发日期、参考电价信息、颁发者签名信息等,管理部门借助凭证颁发管理防止不可信充电桩接入。

数字身份验证:电动汽车在不同运营商的充电桩充电时,充电桩客户端出示凭证给电动汽车用户客户端进行验证。通过后电动汽车充电结算,监督

企业定价合理性，反馈给管理部门。

5.2　电网人员安全管理

电力调度业务中各部门子业务需要跨部门、跨工区协同完成。各部门工作人员身份认证系统根据自身业务需求独立建设而无法共享，造成身份盗用和冒用、行为难以追溯。联盟分布式身份认证采用身份标识跨链复用，具有可扩展、安全性高等特点。

电网人员安全管理结构示意图如附录B图B2所示。同一部门身份数据注册保存于同一份身份账本，与其他部门的身份数据安全隔离。如人员A要跨部门进入工区2操作设备，其认证管理的3个阶段如下：

跨链身份注册：首先，人员A通过客户端携带自身联盟ID向协议节点1发送请求，A在身份账本1验证后，转发认证请求给公证人模块；然后，该模块采用多重签名机制对请求校验并签名，公证人可由各工区及上级管理部门组成，都拥有一对公私密钥。当该认证请求获得2/3以上公证人签名后，该签名结果转发给节点2；最后，人员A通过节点2完成在账本2中跨链联盟ID的注册。

数字身份凭证颁发：节点2申请颁发人员A凭证。工区2管理部门根据账本2中凭证数据结构给A颁发凭证，凭证认证可细粒度到具体门禁和某一设备。该凭证发送到人员A分布式身份客户端。

数字身份验证：人员A进入工区2或操作工区2的设备时，验证通过，获得该设备的访问权限，否则拒绝访问。

5.3　电网供应链金融

不同地域多业务主体参与、身份认证不统一和信用机制不完善等问题给电网供应链安全增加风险。金融机构不能有效获取上下游供应商的商业信用情况[43]。

电网供应链金融结构示意图如附录B图B3所示。数据上链实现数字身份联盟内全局公开、分布式和自主可控的互联互通。认证响应过程分为如下5个阶段。1）申请凭证：上下游供应商向电网核心企业申请贷款许可相关凭证；2）颁发凭证：企业查询供应商的债权交易信息颁发凭证；3）申请贷款：供应商向金融机构申请贷款出示凭证；4）验证凭证：金融机构查询账本，验证联盟ID和凭证；5）授权放贷：验证通过后金融机构为供应商发放贷款，不通过则拒绝贷款。

5.4　应用场景对比

应用场景对比如表5所示。在技术可行性方面，不改变原有电力业务，仅将身份认证平滑移植到基于区块链的联盟分布式身份认证系统，可增强系统安全性。在经济可行性方面，由于该身份认证系统的扩展性良好，部署一套基于区块链的身份认证体系，可应用于多个业务场景，解决了一个业务系统需要建设一套身份认证系统以及各个企业需要独立建设和维护自身的身份认证体系的难题，可节约百万甚至千万级的系统建设和维护成本。此外，相较于CA机构的第三方服务费与用户规模成正比的情况，即用户数量越多，成本越高，而基于区块链的身份认证系统具有规模效应，用户数量越大，人均成本越低。

表5　应用场景对比

Table 5　Comparison of application scenarios

应用场景	存在问题	作用对象	具体内容
充电桩业务	充电桩和用户身份互通性差，跨运营商结算难；身份数据无法自主控制，隐私泄露风险高	电网公司充电桩管理部门、充电桩设备、电动汽车充电用户	管理部门设置统一规则为充电桩颁发凭证，用户验证凭证享受公平合理用电服务
电网人员安全管理	各部门系统独立，隐私身份数据难以共享，不满足跨部门协同数字身份“可用不可见”需求	各工区管理部门、跨部门和跨工区工作人员、调度设备	采用跨链公证人机制，跨区人员在被访问工区进行身份注册和凭证申请，保证跨域统一身份认证和授权管理
电力供应链金融业务	用户身份数据公开难，信用无法有效传递，身份认证不统一，信用机制不完善，融资难	电网核心企业、上下游供应商、金融机构	绑定联盟身份凭证和供应商商业信用，实现数字身份互通互联和商业信用可靠传递，促进供应商融资

6　结语

基于区块链的联盟分布式认证体系包括联盟ID协议、凭证协议以及上层应用程序。相比传统身份认证体系，能够实现用户身份数据的安全共享与自主控制，但是仍存在向原有电力业务系统快速迁移实施难的问题。下一步，将研究电力行业基于区块链的联盟信任分布式认证所涉及的隐私保护方案改进与认证机制的效率优化等方向，推动分布式认证技术在更多场景的应用落地。

本文在研究过程中得到中国科学院信息

工程研究所科研人员的支持，尤其是王雅哲副研究员、吕朋辉博士研究生和刘超硕士研究生对本研究的方案设计提出了宝贵的意见，特此感谢！

附录见本刊网络版（http://www.aeps-info.com/aeps/ch/index.aspx），扫英文摘要后二维码可以阅读网络全文。

参 考 文 献

[1] 郭建，顾志强.电力企业信息安全现状分析及管理对策[J].信息技术，2013，37(1)：180-183.
GUO Jian, GU Zhiqiang. Analyzing current situation and management solution of the information security of the power enterprise[J]. Information Technology, 2013, 37(1): 180-183.

[2] 谢宗晓，马春旺.GB/T 36633—2018《信息安全技术　网络用户身份鉴别技术指南》解析[J].中国质量与标准导报，2019(5)：16-19.
XIE Zongxiao, MA Chunwang. Analysis of GB/T 36633—2018 "information security technology network user identity authentication technical guide"[J]. China Quality and Standards Review, 2019(5): 16-19.

[3] 王静.统一身份认证和用户管理平台在集团型电力企业的应用[J].信息网络安全，2016(12)：81-85.
WANG Jing. Application of the unified identity authentication and user management platform in electric group enterprise[J]. Netinfo Security, 2016(12): 81-85.

[4] 夏同飞，秦浩，李志，等.可信身份认证云服务在泛在电力物联网中的研究与应用[J].电力信息与通信技术，2019，17(7)：11-15.
XIA Tongfei, QIN Hao, LI Zhi, et al. Application and research of trusted identity authentication cloud service in ubiquitous power Internet of Things[J]. Electric Power Information and Communication Technology, 2019, 17(7): 11-15.

[5] 汤阳，张翼英，何业慎，等.一种基于PKI的能源信息系统多渠道统一身份认证方法[J].电信科学，2019，35(6)：41-49.
TANG Yang, ZHANG Yiying, HE Yeshen, et al. A PKI-based multi-channel unified identity authentication method for energy information system[J]. Telecommunications Science, 2019, 35(6): 41-49.

[6] 李静，来风刚，李祖建.国家电网公司PKI/CA认证体系的建设思路[J].电力信息化，2011，9(3)：8-11.
LI Jing, LAI Fenggang, LI Zujian. Construction approach of state grid PKI/CA system of State Grid Corporation of China[J]. Electric Power Information Technology, 2011, 9(3): 8-11.

[7] 孙树才，朱陈鹏.基于第三方验证的变电站命令交互方法的研究[J].电气技术，2018，19(11)：115-118.
SUN Shucai, ZHU Chenpeng. Research on the method of substation command interaction based on third party verification[J]. Electrical Engineering, 2018, 19(11): 115-118.

[8] 肖勇，钱斌，蔡梓文，等.电力物联网终端非法无线通信链路检测方法[J].电工技术学报，2020，35(11)：2319-2327.
XIAO Yong, QIAN Bin, CAI Ziwen, et al. Malicious wireless communication link detection of power Internet of Thing devices[J]. Transactions of China Electrotechnical Society, 2020, 35(11): 2319-2327.

[9] 马靖，许勇刚，刘增明，等.基于零信任框架的泛在电力物联网安全防护研究[J].网络安全技术与应用，2020(1)：117-119.
MA Jing, XU Yonggang, LIU Zengming, et al. Research on ubiquitous power Internet of Things security protection based on zero trust framework[J]. Network Security Technology & Application, 2020(1): 117-119.

[10] 郜盼盼.智能电网系统中面向用电信息安全防护的认证加密系统研究[D].北京：北京邮电大学，2013.
GAO Panpan. Research on authentication encryption system for the security protection of smart grid electric data[D]. Beijing: Beijing University of Posts and Telecommunications, 2013.

[11] 吴桐.电力行业统一权限平台设计与实现[D].大连：大连理工大学，2016.
WU Tong. Design and implementation of electric power industry unified permissions platform[D]. Dalian: Dalian University of Technology, 2016.

[12] 王萍，胡聪，李彦生.如何推进统一权限平台身份授权单轨使用[J].中国管理信息化，2015，18(8)：103.
WANG Ping, HU Cong, LI Yansheng. How to promote the single-track use of unified authority platform identity authorization[J]. China Management Informationization, 2015, 18(8): 103.

[13] Toward scalable decentralized identifier system [EB/OL]. [2021-01-15]. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/toward-scalable-decentralized-identifier-systems/ba-p/560168.

[14] BHATTACHARYA M P, ZAVARSKY P, BUTAKOV S. Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain [C]// 2020 International Symposium on Networks, Computers and Communications (ISNCC), October 20-22, 2020, Montreal, Canada.

[15] NAIK N, JENKINS P. uPort open-source identity management system: an assessment of self-sovereign identity and user-centric data platform built on blockchain[C]// 2020 IEEE International Symposium on Systems Engineering, October 12-November 12, 2020, Vienna, Austria.

[16] KUPERBERG M. Blockchain-based identity management: a survey from the enterprise and ecosystem perspective[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1008-1027.

[17] STOKKINK Q, POUWELSE J. Deployment of a blockchain-based self-sovereign identity[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data, July 30-August 3, 2018, Halifax, Canada: 1336-1342.

[18] LUX Z A, THATMANN D, ZICKAU S, et al. Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials [C]// 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), September 28-30, 2020, Paris,

France: 71-78.

[19] MANU S, DAVE L, DAVID C. Verifiable credentials data model 1.1 [EB/OL]. [2021-01-15]. https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential.

[20] 赵曰浩，彭克，徐丙垠，等.能源区块链应用工程现状与展望[J].电力系统自动化，2019，43(7)：14-22.
ZHAO Yuehao, PENG Ke, XU Bingyin, et al. Status and prospect of pilot project of energy blockchain[J]. Automation of Electric Power Systems, 2019, 43(7): 14-22.

[21] 徐嘉辉，马立新.区块链技术在分布式能源交易中的应用[J].电力自动化设备，2020，40(8)：17-22.
XU Jiahui, MA Lixin. Application of blockchain technology in distributed energy transaction [J]. Electric Power Automation Equipment, 2020, 40(8): 17-22.

[22] 曾隽芳，刘禹.能耗监测中的区块链终端信任管理[J].电力自动化设备，2020，40(8)：31-37.
ZENG Junfang, LIU Yu. Trust management of blockchain terminals in energy consumption monitoring[J]. Electric Power Automation Equipment, 2020, 40(8): 31-37.

[23] 杨洪明，阳泽峰，漆敏，等.双链式区块链架构设计及其点对点交易优化决策实现[J].电力系统自动化，2021，45(9)：19-27.
YANG Hongming, YANG Zefeng, QI Min, et al. Design of double-chain blockchain architecture and its implementation of peer-to-peer transaction optimization decision[J]. Automation of Electric Power Systems, 2021, 45(9): 19-27.

[24] 韩冬，张程正浩，孙伟卿，等.基于区块链技术的智能配售电交易平台架构设计[J].电力系统自动化，2019，43(7)：89-96.
HAN Dong, ZHANG Chengzhenghao, SUN Weiqing, et al. Framework design of smart distribution trading platform based on blockchain technology [J]. Automation of Electric Power Systems, 2019, 43(7): 89-96.

[25] 李彬，曹望璋，张洁，等.基于异构区块链的多能系统交易体系及关键技术[J].电力系统自动化，2018，42(4)：183-193.
LI Bin, CAO Wangzhang, ZHANG Jie, et al. Transaction system and key technologies of multi-energy system based on heterogeneous blockchain [J]. Automation of Electric Power Systems, 2018, 42(4): 183-193.

[26] 万书鹏，易强，张凯，等.基于微服务架构的新一代调控系统服务编排技术[J].电力系统自动化，2019，43(22)：116-121.
WAN Shupeng, YI Qiang, ZHANG Kai, et al. Microservice architecture based service choreography technology for new generation dispatching and control system [J]. Automation of Electric Power Systems, 2019, 43(22): 116-121.

[27] 承林，王海宁，高春成.微服务在电力交易系统中的应用研究[J].电网技术，2018，42(2)：441-446.
CHENG Lin, WANG Haining, GAO Chuncheng. Research on application of micro service in power transaction system [J]. Power System Technology, 2018, 42(2): 441-446.

[28] ELLISON C, SCHNEIER B. Ten risks of PKI: what you are not being told about public key infrastructure [J]. Computer Security Journal, 2000, 16(1): 1-7.

[29] 袁勇，王飞跃.区块链技术发展现状与展望[J].自动化学报，2016，42(4)：481-494.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[30] 王胜寒，郭创新，冯斌，等.区块链技术在电力系统中的应用：前景与思路[J].电力系统自动化，2020，44(11)：10-24.
WANG Shenghan, GUO Chuangxin, FENG Bin, et al. Application of blockchain technology in power systems: prospects and ideas[J]. Automation of Electric Power Systems, 2020, 44(11): 10-24.

[31] FOUNDATION T L. Hyperledger fabric [EB/OL]. [2020-02-16]. https://www.hyperledger.org/use/fabric.

[32] 姜文博，李洪伟，郝尧，等.网络空间身份管理研究综述[J].信息安全与通信保密，2019，17(9)：46-57.
JIANG Wenbo, LI Hongwei, HAO Yao, et al. A survey on cyberspace identity management [J]. Information Security and Communications Privacy, 2019, 17(9): 46-57.

[33] 蔡元纪，顾宇轩，罗钢，等.基于区块链的绿色证书交易平台：概念与实践[J].电力系统自动化，2020，44(15)：1-9.
CAI Yuanji, GU Yuxuan, LUO Gang, et al. Blockchain based trading platform of green power certificate: concept and practice [J]. Automation of Electric Power Systems, 2020, 44(15): 1-9.

[34] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]// 2015 IEEE Security and Privacy Workshops, May 21-22, 2015, San Jose, USA: 180-184.

[35] 刘懿中，刘建伟，张宗洋，等.区块链共识机制研究综述[J].密码学报，2019，6(4)：395-432.
LIU Yizhong, LIU Jianwei, ZHANG Zongyang, et al. Overview on blockchain consensus mechanisms[J]. Journal of Cryptologic Research, 2019, 6(4): 395-432.

[36] 智能合约[EB/OL].[2021-01-27].https://github.com/EthFans/wiki/wiki/% E6%99%BA% E8%83%BD% E5%90%88%E7%BA%A6.
Smart contract[EB/OL]. [2021-01-27]. https://github.com/EthFans/wiki/wiki/% E6%99%BA% E8%83%BD% E5%90%88%E7%BA%A6.

[37] 黄冬艳，李浪，陈斌，等.RBFT：基于Raft集群的拜占庭容错共识机制[J].通信学报，2021，42(3)：209-219.
HUANG Dongyan, LI Lang, CHEN Bin, et al. RBFT: a new Byzantine fault-tolerant consensus mechanism based on Raft cluster[J]. Journal on Communications, 2021, 42(3): 209-219.

[38] DISTLER T, KAPITZA R. Increasing performance in Byzantine fault-tolerant systems with on-demand replica consistency[C]// Proceedings of 6th Conference on Computer systems, April 10-13, 2011, Salzburg, Austria: 91-106.

[39] GOLAN-GUETA G, ABRAHAM I, GROSSMAN S, et al. SBFT: a scalable decentralized trust infrastructure for blockchains [EB/OL]. [2021-01-27]. https://arxiv.org/pdf/1804.01626.pdf.

[40] SELLAPPAN. A robust Byzantine fault-tolerant replication technique for peer-to-peer content distribution [J]. Journal of Computer Science, 2011, 7(2): 159-166.

[41] 最高人民法院关于互联网法院审理案件若干问题的规定[EB/OL].[2021-01-27].http://www.hncourt.gov.cn/public/detail.php? id=175169.
Regulations of the Supreme People's Court on several issues

concerning the hearing of cases in Internet courts [EB/OL]. [2021-01-27]. http://www.hncourt.gov.cn/public/detail.php?id=175169.

[42] 徐江珮,王晋,刘畅,等.电动汽车充电桩CAN总线协议的安全检测[J].山东大学学报(理学版),2020,55(5):95-104.
XU Jiangpei, WANG Jin, LIU Chang, et al. Security detection of CAN bus protocol for electric vehicle and charging pile [J]. Journal of Shandong University (Natural Science), 2020, 55(5): 95-104.

[43] 朱兴雄,何清素,郭善琪.区块链技术在供应链金融中的应用[J].中国流通经济,2018,32(3):111-119.
ZHU Xingxiong, HE Qingsu, GUO Shanqi. On the role of blockchain technology in supply chain finance [J]. China Business and Market, 2018, 32(3): 111-119.

王　栋(1985—),男,硕士,高级工程师,主要研究方向:区块链、信息安全。E-mail:wangdong@sgec.sgcc.com.cn

杨　珂(1990—),男,通信作者,博士,工程师,主要研究方向:网络安全、区块链。E-mail:yangke@sgec.sgcc.com.cn

王　瑜(1985—),男,硕士,助理研究员,主要研究方向:区块链安全、信息安全、身份认证。E-mail:wangyu@iie.ac.cn

(编辑　杨松迎)

Application Exploration of Blockchain-based Distributed Authentication wtih Alliance Trust in Power Industry

WANG Dong[1,2], *YANG Ke*[1,3], *WANG Yu*[4], *XUAN Jiaxing*[1,2], *CHEN Ya*[4,5], *XU Honghua*[6]

(1. State Grid Electronic Commerce Co., Ltd., Beijing 100053, China;
2. State Grid Blockchain Technology (Beijing) Co., Ltd., Beijing 100053, China;
3. Blockchain Technology Laboratory of State Grid Co., Ltd., Beijing 100053, China;
4. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
5. School of Cyberspace Security, University of Chinese Academy of Sciences, Beijing 100093, China;
6. Nanjing Power Supply Company of State Grid Jiangsu Electric Power Co., Ltd., Nanjing 210019, China)

Abstract: The rapid development of electric power business has led to the expansion of its network security boundary. However, while most of electric power business systems stay at the stage of centralized identity or federated identity, which is difficult to meet new demands such as massive access, heterogeneous authentication, and frequent interaction. First, this paper proposes a blockchain-based distributed authentication system with alliance trust applicable to the power industry. Then, this paper analyzes the applicability of the system from three perspectives: network architecture, user identity control, and privacy protection. Its system architecture and operation mechanism are elaborated. The alliance digital identity is designed, and the identity information is stored in the distributed identity ledger according to the consensus and privacy protection policies. The full lifecycle management of digital identity is provided, and the cross-domain secure sharing and autonomous control of identity data as well as the cross-domain identity authentication of users are realized. Finally, the solution ideas based on this system are proposed to address the identity authentication bottlenecks faced by three industry scenarios: charging ecosystem of charging piles, safety management of power grid personnel, and power supply chain finance.

This work is supported by State Grid Corporation of China (No. 5700-202072372A-0-0-00).

Key words: power business; blockchain; distributed identity authentication; identity authentication