

基于区块链的电网可信分布式身份认证系统

杨冠群¹, 刘荫¹, 徐浩¹, 邢宏伟², 张建辉², 李恩堂²

(1. 国网山东省电力公司信息通信公司, 山东 济南 250001;

2. 山东鲁软数字科技有限公司, 山东 济南 250001)

摘 要: 基于区块链的身份认证系统大多基于公有区块链平台, 本质上仍是传统的中心式身份管理和验证方式, 难以满足微电网中可信接入、细粒度访问控制等需求。因此, 基于 FISCO BCOS 联盟区块链技术, 设计了一个支持多中心的分布式身份认证系统, 提出了基于 DID 的身份管理协议, 实现了用户身份的自主控制; 研究了微网中终端节点的分布式可信接入技术, 设计了基于零知识证明的隐私保护凭证, 为用户和上层应用构建一个公开透明可信的底层身份架构, 满足了不同的隐私安全场景下用户身份的可信可验证的需求, 实现了实体身份的自主控制、细粒度访问控制和可信数据交换。通过系统实验和性能分析证明了所设计系统的可用性和有效性。

关键词: 微网; 区块链; 零知识证明; 隐私保护凭证; 分布式身份认证; 访问控制

中图分类号: TP399

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021054

Credible distributed identity authentication system of microgrid based on blockchain

YANG Guanqun¹, LIU Yin¹, XU Hao¹, XING Hongwei², ZHANG Jianhui², LI Entang²

1. Information & Telecommunications Company, State Grid Shandong Electric Power Company, Ji'nan 250001, China

2. Shandong Luruan Digital Technology Co., LTD, Ji'nan 250001, China

Abstract: Most of the blockchain-based identity authentication systems are based on public blockchain, which are still essentially traditional centralized identity management and verification methods, making it difficult to meet the needs of trusted access and fine-grained access control in microgrids. Therefore, based on the FISCO BCOS consortium blockchain technology, a distributed identity authentication system supporting multi-center was designed. A DID-based identity management protocol to achieve autonomous control of user identity in a practical scenarios was designed. Distributed trusted access technology for end nodes in microgrids was studied, and privacy-protecting

收稿日期: 2021-06-24; 修回日期: 2021-10-13

通信作者: 李恩堂, ls_liet@163.com

基金项目: 国网山东省电力公司科技项目 (520627200004)

Foundation Item: State Grid Shandong Electric Power Company Science and Technology Project (520627200004)

论文引用格式: 杨冠群, 刘荫, 徐浩, 等. 基于区块链的电网可信分布式身份认证系统[J]. 网络与信息安全学报, 2021, 7(6): 88-98.

YANG G Q, LIU Y, XU H, et al. Credible distributed identity authentication system of microgrid based on blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 88-98.

credentials based on zero-knowledge proof were designed. This scheme meets the requirements of trustworthy and verifiable user identity in different privacy security scenarios, and achieves autonomous control of entity identity, fine-grained access control and trusted data exchange. The usability and effectiveness of the proposed algorithm are demonstrated through system experiments and performance analysis.

Keywords: microgrid, blockchain, zero-knowledge proof, privacy credentials, distributed identity authentication system, access control

1 引言

随着微电网行业的不断变革, 新能源的布局占据着国家重要的战略地位^[1]。2020年4月, 国家能源局综合司发布的《关于做好可再生能源发展“十四五”规划编制工作有关事项的通知》, 通知指出: “优先开发当地分散式和分布式可再生能源资源, 大力推进分布式可再生电力、热力、燃气等在用户侧直接就近利用, 结合储能、氢能等新技术, 提升可再生能源在区域能源供应中的比重。”可再生能源分布式是未来的发展方向, 而在这样的分布式系统中发展充电站乃至充电站无疑是大势所趋, 甚至有可能成为标配^[2]。

随着我国新能源的广泛应用, 风电、太阳能等占比大幅提升。例如, 大力发展光储充一体化的微电网技术, 将清洁能源供电通过光伏发电后存储电能, 光伏、储能和充电设施形成了一个微网, 根据需求与公共电网智能互动, 可实现并网、离网两种不同运行模式^[3]。为了缓解充电桩大电流充电时对区域电网的冲击, 储能系统的传输配送过程通常伴随分布式发电、分布式售电、智能电表、终端智能充电桩等服务需求。

微电网在迅速扩展的同时, 也带来了愈加严重的安全挑战^[4]。以风电、光伏为主的新型供电系统呈现分布式架构, 集中式的用户管理系统已经无法满足分布式各主体之间进行点对点可信交互的需求。此外, 能源物联网的终端节点分布广、范围宽、数量大、环境复杂且计算资源有限, 极易受到冒用、篡改等攻击^[5-6]。

为适应新型的电力发展要求, 2019年, 国网公司提出“开展区块链等新技术应用研究, 有效支撑和促进‘两网’融合发展”, 推动了区块链技术在电力行业的进一步研究和深化应用^[7]。区块

链开放、共享、协同的技术形态与国网公司建设中国特色国际领先的微网战略目标高度契合, 可以有效解决泛在微网建设过程中面临的数据融通、设备安全、个人隐私、架构僵化和多主体协同等问题, 在引领泛在微网建设方面具有不可替代的重要作用^[8-9]。

区块链技术以其去中心化、安全透明、不易篡改等特性与分布式能源交易的需求具有极高的契合度^[10]。为了解决微网中终端节点的身份管理、可信接入和业务访问控制等问题, 本文基于FISCO BCOS联盟区块链技术, 设计了一个多中心的分布式身份认证系统, 支持细粒度的声明描述和基于零知识证明的隐私凭证, 实现了实体身份的自主控制、属性级的细粒度访问控制、用户身份的隐私保护和可信数据交换。具体而言, 本文贡献如下。

1) 用户身份的自主控制: 与传统身份管理不同, 身份不必再掌握在身份提供者手中, 用户的身份由自己建立和保存, 用户自己管理自己的信息, 用户完全拥有、控制和管理自己的身份。

2) 分布式可信接入: 提出了基于联盟区块链的分布式身份管理技术, 支持扁平化的分布式认证, 不依赖于单一企业的认证, 通过分布式的用户社会关系获得全面的身份认证, 真正意义上实现了用户身份自治, 通过KYC (know your customer) 技术实现身份监管, 解决了微网终端节点的分布式可信接入问题。

3) 用户信息身份隐私保护: 提出了适用于微网的基于用户细粒度属性的可验证凭证, 基于零知识证明技术, 系统支持生成匿名凭证, 针对用户的敏感信息, 可以在不披露秘密信息的情况下完成验证, 有效实现了用户身份的隐私保护。

4) 多中心化机构的移植: 基于区块链技术,

支持多个证书颁发机构并对应不同的信任等级,是一个分布式多中心的身份管理平台,支持多平台、跨链、跨应用间身份标识和凭证的移植。

2 相关工作

随着互联网的普及和发展,网络数字身份应运而生,并用于补齐互联网缺失的身份层,解决可信交互的问题。第一代网络身份为应用账户,由中心式的身份提供方分配本地账户并简单地提供用户名和账户密码。

由于不同应用间的本地账户无法联通,人们需要维护大量的应用账户,基于联盟的账户身份产生。SSO 单点登录系统^[11]是比较流行的联盟身份解决方案,可以解决在多个应用系统中的访问联盟所有应用系统和跨系统的信任问题。传统的微电网的认证系统一般也通过 SSO 单点登录系统来解决。Celesti 等^[12]在异构环境中建立联盟的体系结构,提出了一种基于 IdP/SP 模型和 SAML 技术的身份认证解决方案。魏晓菁等^[13]为国家电网公司建设了全网统一索引的身份管理和认证系统,为国网各大业务体系提供了身份认证、账户管理、SSO 单点登录等基础设施服务,节省了各子应用系统之间各自数据保持的存储开销和降低了安全风险,避免了数据孤岛的困境,基本解决了全网互联互通的问题。然而,中心化系统中的用户的身份信息完全由服务商所掌控,可能存在信息超量收集、恶意收集分析、数据泄露和数据买卖等不可控行为。

为了实现用户身份自治,研究人员开始探索基于区块链的数字身份管理方案^[14-15]。公钥基础设施(PKI)^[16]是较为常用的身份和证书管理技术。Yu 等^[17]设计并开发了基于区块链的 PKI 管理框架,用于发布、验证和撤销 X.509 证书,以解决单点故障和实现对 CA 中心缺陷的快速反应。uPort^[18]是基于以太坊和分布式网络设计的开放式身份系统,基于智能合约实现了支持多中心身份数据的自治,支持多中心化应用。Kikitamara 等^[19]将身份管理权限归于个人并在区块链系统上共享,从而支持多个系统和应用程序之间交互和服务。

基于区块链的身份认证系统大多基于公共

区块链平台,没有针对微电网的联盟场景进行有效改造和整合,难以满足微电网中可信接入、细粒度访问控制等需求,因此不适合电网场景。虽然区块链在电网的应用较多,但大多是集中于区块链平台在电网交易场景中的应用,而缺乏从身份管理的角度来解决分布式身份可信的问题。因此,本文基于 FISCO BCOS 联盟区块链技术,提出了一个支持多中心的分布式身份认证系统,实现用户身份的自主控制和可信接入,并通过属性声明技术实现属性级的细粒度访问控制。

3 系统模型

3.1 系统目标

可信身份认证作为身份治理底层基础设施,用以解决跨部门、跨组织、跨机构的可信身份认证问题,确保用户的身份信息由自己掌握,保护隐私与个人信息,同时为监管保留查验通道(如 KYC 认证或与 eID 联通)。其系统目标如下。

(1) 自主控制

DID 可以由用户自己建立,自己管理自己的信息。用户完全拥有、控制和管理自己的身份。

(2) 分布式认证

不依赖于单一企业的认证,通过分布式的用户社会关系获得全面的身份认证。

(3) 建立信任

本文先选取委员会节点作为发证者和记账节点,而区块链技术旨在确保网络中每一个记账节点都参与数据交互及记录管理等工作,再根据 KYC 的真实用户信息记录及审计规则,对用户所提供的信息进行审核,并以委员会节点作为凭证颁发者对用户凭证进行背书,可以实现多中心机构中信任桥梁的建立,由此实现支持多中心的特点及节点间的相互信任。

(4) 隐私保护

用户的数字身份标识符无法推测出用户真实的身份信息,用户的可信身份认证标识符和可验证数字凭证链下存储,链上存证。用户属性可表示为离散对数模型,转换为密码承诺隐藏用户隐私,实现更高级别的隐私需求。

(5) 可撤销性

使用辅链支撑的撤销策略，实现密码凭据的撤销查询，提供未撤销性证明。

(6) 可移植性

支持多平台、跨链、跨应用间身份标识和凭证的移植。

3.2 系统架构

与传统的密钥证书管理 PKI 体系相似，在可信身份认证生态中，系统拥有 4 种角色，分别为发证者 (Issuer)、持有者 (Holder)、验证者 (Verifier) 和标识符注册机构，其中系统可以拥有多个发证中心，如图 1 所示。此外，机构委员会成员、系统管理员也是联盟链角色，分别具有管理发证机构的权限和系统管理权限。系统角色具体描述如下。

发证者：拥有用户数据并能开具可验证声明凭证的实体，如政府、银行、大学等。区块链中的委员会充当发证者。针对用户的身份社会属性多样化与统一身份管理中心之间的矛盾，本文采用多机构颁发代替传统的中心化证书中心。假设已有一个用于选择委员会节点的许可模型，系统中选取委员会作为证书的颁发者。令 Cmt 表示委员会，由 n 个节点 $\{Cmt_i\}_{i=1}^n$ 组成。委员会节点各自存储一个私钥 sk ，用于颁发凭据。相应的公钥 pk 用于验证凭据。任何一方（分布式应用程序或委员会节点）都可以充当凭据发证者，发证者的

主要功能包括发证方注册/注销、发布凭证模板、签发用户凭证等。辅助以 KYC 规则，对用户所提供的信息进行审核，并以委员会节点作为凭证颁发者对用户凭证进行背书，为多中心机构建立信任的桥梁。

验证者：也称应用方，接受可验证声明凭证并进行验证，由此可以提供给出示可验证声明凭证者某种类型的服务。验证者的主要功能包括发布验证规则、通过链上信息验证用户 DID、验证用户凭证等。验证者包括雇主、安全人员和网站等。

持有者：向 Issuer 请求可验证声明凭证的实体。向验证者出示可验证声明凭证。开具的可验证声明凭证可以放在可验证声明凭证钱包里，方便再次使用。持有者的主要功能包括 DID 注册/注销/更新、向发证者申请凭证、向验证者展示凭证等。持有者包括学生、员工和客户等。

标识符注册机构：负责维护 DID 的数据库，如某条区块链、分布式账本 (DID 里的 example 字段)，方便验证者验证可验证声明凭证、Holder、Issuer、可信身份认证数据库。

微网区块链分布式身份认证系统可以拥有多个 CA 发证中心，一般由电网机构或其他机构承担，如图 2 所示。此外，微网中终端节点众多，同一个用户既可以作为持有者，也可以作为验证者。

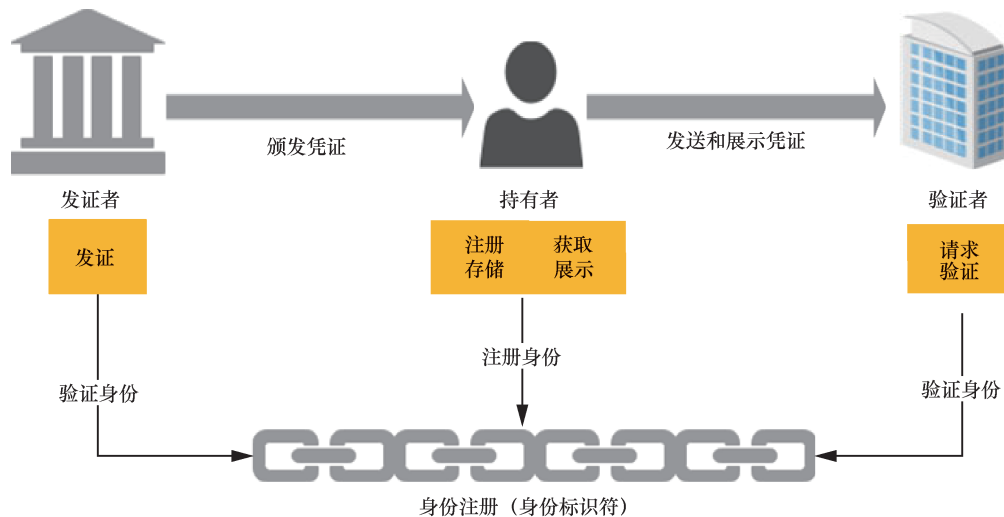


图 1 身份认证系统模型

Figure 1 Identity authentication system model

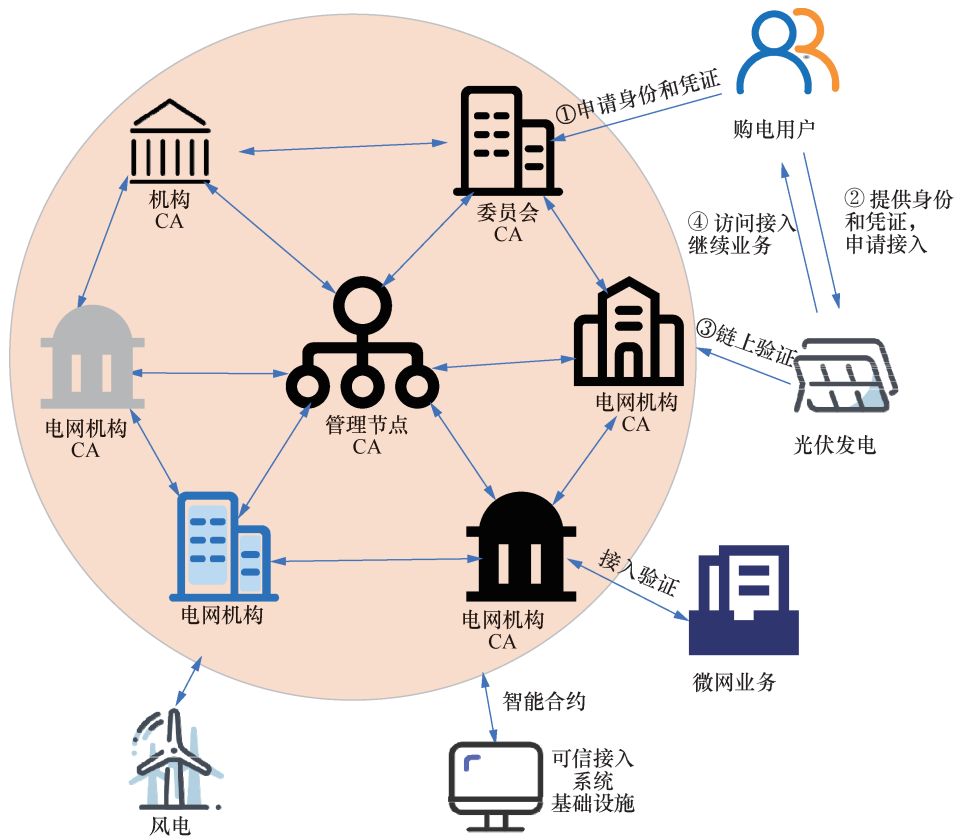


图 2 多授权中心的微网接入架构
Figure 2 Microgrid access architecture with multiple authorization centers

4 基于区块链的分布式身份认证系统

4.1 符号定义

本节的符号定义如表 1 所示。

表 1 符号定义
Table 1 Symbol definition

标识符	释义
DID	分布式身份标识符 ^[9]
DID Document	DID 文档, 包括 DID 的公钥、服务端点、使用方法等相关属性
Subject	表示主体对象, 是声明描述的主体对象。实体示例包括人类、动物和事物等
Claim	声明, 它是对一个实体的陈述。声明使用主体-属性-值关系表示
Verifiable Credential	遵循 W3C Verifiable Credential 规范的电子凭证, 以包含一个或者多个 Claim ^[10]
Presentation	可验证展示来自同一主体的一个或多个可验证凭证的数据

(1) DID

DID 也可以记为 did, 参考比特币的双 hash 方式, DID 标识符的设计可以采用 base58 (ri-

pemd160 (sha256(<Public Key>))) 计算方式, 其中 Public Key 是用户公钥。DID 标识符的具体形式可以表示为 "did:did:1:0x0086eb1f712ebc6f1c276e12ec21"。

(2) Subject

Subject 表示主体对象, 是声明描述的主体对象。实体示例包括人、动物和事物等。

(3) Claim

Claim 指用户凭证中的声明, 是对自己所持有属性、内容等的声明。

(4) Verifiable Credential

Verifiable Credential 指用户向发证方申请和签发的凭证, 由元数据、声明和证明组成。

(5) Presentation

可验证展示来自同一主体的一个或多个可验证凭证的数据。

4.2 算法描述

可信身份认证系统包括数字身份管理体系和凭证管理系统。数字身份管理体系包括身份注册

阶段、身份验证阶段、KYC 过程；凭证管理系统包括凭证创建阶段、存证创建阶段、凭证验证阶段、凭证更新阶段、凭证撤销阶段。

(1) 数字身份管理体系

① 身份注册阶段 $\text{createDid}(\text{addr}) \rightarrow \{\text{pk}, \text{sk}, \text{did}\}$ ：注册是获取身份的过程，需要由链上的机构来承认该所有者的身份，由身份所有者执行。输入用户节点的地址 addr ，系统创建公私钥 (pk , sk) 和链上注册用户身份标识符 did 并返回 (did 可以直接使用公钥地址)。其中系统用户的公私钥记为 (pk_u , sk_u)，发证者公私钥记为 (pk_c , sk_c)，验证者公私钥为 (pk_v , sk_v)。

② 身份验证阶段 $\text{verifyDid}(\text{did}, \text{sign}, \text{pk}_u) \rightarrow \text{result}$ ：验证是校验所提供的身份是否为合法身份的过程。身份所有者提供身份标识符 did 、相关挑战信息的签名 sign 和身份公钥 pk_u ， $\text{sign} = \text{Sign}_{\text{sk}_u}(\text{ch})$ ， ch 为验证者的挑战。验证者在链上查询 did 的存在性，用公钥 pk_u 验证用户签名 sign 的正确性，然后调用智能合约，查询 did 的属性，返回查询结果 result ，其中 $\text{result} = \{\text{TRUE}/\text{FALSE}\}$ ，TRUE 表示身份验证通过，FALSE 表示身份验证失败。

③ KYC 过程：联盟委员会对用户所提供的身份信息进行核验，核验通过后加密存储于数据库中，用于后续监管和用户凭证信息比对核实，以防违法交易发生。

(2) 凭证管理系统

① 凭证创建阶段 $\text{createCredential}(\text{did}, a, v) \rightarrow \text{cred}$ ：凭证创建算法由凭证的发证者执行。DID 持有者提供其身份标识符 did 、用户属性 a 及对应的属性值 v ，发证者核验属性后，首先生成其声明 $\text{claim} = \{a, v\}$ 。然后，计算属性值摘要，并为声明签名生成签名证明 $S = \text{Sign}_{\text{sk}_c}(h)$ ， $h = H(v)$ ，其中 H 为哈希函数；接着，发证者为授权证书添加凭证授权时间、凭证更新时间、用户相关属性、用户 did 的使用方法、验证类型（密钥类型）、使用端口、更新属性和发证者的签名信息等元数据信息，以完成授权证书的创建和签发。

如果用户所持属性为隐私属性，选定群 G 的生成元为 $g \in G$ ，计算 $A = g^a \pmod{q}$ 。选取盲因

子 r ，其承诺值 $c = g^r$ ，于是匿名声明为 $\text{claim} = \{a, A\}$ 并发送给发证者。发证者核验承诺值，验证成功则接受承诺；为声明签名生成签名证明 S ， $S = \text{Sign}_{\text{sk}_c}(c)$ ，并为授权证书添加凭证授权时间、软件相关属性、使用方自身属性和发证者的签名信息，完成授权证书的创建和签发。选取 (ch, rp) 作为结果证明，该证明可被其他用户和验证者验证。普通凭证创建算法和隐私凭证创建算法分别如算法 1、算法 2 所示。

算法 1 普通凭证创建算法

输入 用户身份标识符 did ，属性 a 及对应属性值 v

输出 凭证结果

```
check(did) // 查验 did 的存在性
for  $a_i$  in  $a$ ,  $v_i$  in  $v$ : // 加载用户属性
  setClaim $_i(a_i, v_i)$  // 设置声明值
 $h_i = H(v_i)$  // 计算属性值摘要
end for
 $h = h_1 \parallel \dots \parallel h_n$  // 连接摘要值
 $S = \text{Sign}_{\text{sk}_c}(h)$  // 计算签名值
end
```

算法 2 隐私凭证创建算法

输入 用户身份标识符 did ，属性 a 及对应属性值 v

输出 凭证结果

```
check(did) // 查验 did 的存在性
select  $g \in G$  // 选取群参数
 $A = g^a \pmod{q}$  // 计算  $a$  的承诺
setClaim( $a, A$ ) // 设置声明值
select  $r \in Z_q$  // 选取盲因子  $r$ 
 $c_i = g^r \pmod{q}$  // 计算  $r$  的承诺
 $\text{ch} = H(g, A, t)$  // 计算挑战
 $\text{rp} = v - \text{ch} \cdot a \pmod{q}$  // 计算回应
 $h = H(A)$  // 计算属性值摘要
 $S = \text{Sign}_{\text{sk}_c}(h)$  // 计算签名值
 $\text{cred} = \{\text{claim}, h, S\}$  // 创建凭证
end
```

② 存证创建阶段 $\text{createEvidence}(\text{object}, \text{sk}_c) \rightarrow \text{ev}$ ：输入未上链的对象 object （一般为所颁发的凭证对象）和身份私钥 sk_c ，算法输出存

证 ev 。计算传入的 $object$ 对象的哈希值, 通过身份私钥 sk_c 签名, $S_o = \text{Sign}_{sk_c}(h_o)$, 生成存证 $ev = \{h_o, S_o, ex\}$, ex 为其他辅助消息或备注消息, 并将存证 ev 上链。存证创建算法可以由持有者或发证者调用。

③ 凭证验证阶段 $\text{verifyCredential}(did, cred, pk) \rightarrow \text{result}$: 输入持有者的身份标识 did 、一个或多个待验证凭证 $cred$ 和身份公钥 pk , 验证者首先从凭证 $cred$ 重构凭证摘要 $h_o' = H(cred)$, 然后使用发证方公钥 pk_c 验证凭证的签名 S_o , 并与链上的签名 S_o 和摘要 h_o 进行比对, 比较 h_o' 与 h_o 是否相等。然后返回验证结果 result , 其中 $\text{result} = \{\text{TRUE}/\text{FALSE}\}$, TRUE 表示凭证验证通过, FALSE 表示凭证验证失败。普通凭证验证算法如算法 3 所示。

算法 3 普通凭证验证算法

输入 用户身份标识符 did , 凭证 $cred$, 公钥 pk

输出 $\text{TRUE} / \text{FALSE}$

$\text{check}(did)$ // 查验 did 的存在性

$\text{tag}_1 = \text{verSign}_{pk_c}(S_o)$ // 验证签名值

$h_o' = H(cred)$ // 重构凭证摘要

$\text{tag}_2 = \text{isEqual}(h_o, h_o')$ // 从链上读取摘要 h_o , 并与 h_o' 比较

return $\text{tag}_1 \ \&\& \ \text{tag}_2$

end for

end

零知识凭证验证算法中, 除了常规的输入以外, 还需输入一些零知识辅助参数, 以支撑不披露属性值的零知识验证; 除了常规的凭证验证步骤, 还需进行零知识挑战和回应的验证, 并从链上读取摘要, 并与算法所恢复的摘要数据比较, 具体验证如算法 4 所示。

算法 4 零知识凭证验证算法

输入 用户身份标识符 did , 凭证 $cred$, 公钥 pk , 挑战/回应值 (ch, rp) , 承诺 A

输出 $\text{TRUE} / \text{FALSE}$

$\text{check}(did)$ // 查验 did 的存在性

$\text{tag}_1 = \text{verSign}_{pk_c}(S_o)$ // 验证签名值

$h_o' = H(cred)$ // 重构凭证摘要

$\text{tag}_2 = \text{isEqual}(h_o, h_o')$ // 从链上读取摘要 h_o ,

并与 h_o' 比较

$t' = g^r A^{ch}$ // 重构承诺

$\text{tag}_3 \leftarrow \text{ch} ? H(g, A, t')$ // 比较等式

return $\text{tag}_1 \ \&\& \ \text{tag}_2 \ \&\& \ \text{tag}_3$

end for

end

凭证验证包含两种模式, 分别为链下模式和链上模式。链下模式中验证者只需验证凭证的签名、有效期、是否撤销等属性项来判断授权证书的真伪, 这适用于安全需求较低的场景或者离线/应急场景; 链上模式中, 除上述验证之外, 验证者还需要反向构造存证, 调用智能合约向链上查询和比较存证来证明与所持凭证的一致性。链上模式适用于安全需求较高的场景。

④ 凭证更新阶段 $\text{updateCredential}(did, cred, newClaim) \rightarrow \text{newCred}$: 输入持有者的身份标识 did 、凭证主体 $cred$ 和新声明 newClaim , $\text{newClaim}_i = \{\text{att}'_i, \text{val}'_i\}$ 。发证者核验原证书 $cred$ 和新的属性声明 newClaim 后, 更新授权证书的 update 属性、版本号和声明主体, 并添加签名信息, 完成授权证书的更新。

凭证撤销阶段 $\text{revokeCredential}(did, cid, cred) \rightarrow \text{result}$: 输入持有者的身份标识 did 、凭证主体 $cred$, 发证者核验原证书 $cred$ 后, 更新授权证书的 revoke 属性, 并重新添加签名信息, 将撤销凭证编号 cid 和存证上链。然后返回撤销结果 result , 其中 $\text{result} = \{\text{TRUE}/\text{FALSE}\}$, TRUE 表示凭证撤销成功, FALSE 表示凭证撤销失败。

4.3 系统应用

基于区块链的电网可信分布式身份认证系统应用于微网的分布式交易体系中。通过使用 DID , 用户持有全局唯一的身份标识符, 且该 DID 标识符可以由用户自己建立, 自己管理自己的信息, 因此用户可以完全拥有、控制和管理自己的身份。

由于用户自己掌握身份信息, 用户与验证者(应用)之间缺少信任。通过区块链技术, 可以对每个节点用户所发布的信息进行确认和共识, 以建立链上信息在节点间的信任。

得益于区块链的分布式账本技术, 用户无须在每个电网交易系统(甚至是电网以外系统)都注册账号, 只要用户和验证者在同一个链中, 均

可以通过分布式的用户社会关系获得全面的身份认证；验证者可以通过属性对电网用户执行身份准入，拥有对应属性才能接入访问。

虽然用户的数字身份标识符无法推测出用户真实的身份信息，但凭证中可能包含用户的隐私信息。针对敏感的身份信息，用户可以将用户属性表示为离散对数模型，并加密为承诺来隐藏用户隐私，验证者只需要通过零知识证明技术即可有效验证，实现了隐私的保护。针对过期的或存在问题的凭证，用户和管理者可以撤销密码凭据。另外，基于区块链的电网可信分布式身份认证系统可以实现跨平台的移植，如兼容电网以外的系统身份验证。

5 实验评估

本文通过在 CentOS 主机上部署 FISCO BCOS 和身份认证系统服务器、实验室主机模拟电网客户端来模拟电网的分布式接入验证过程，以验证本文系统的高效性和可用性。服务器主机的参数为：Intel(R) Core i7-7700 CPU @ 3.60 GHz 3.60 GHz, RAM 16.00 GB, CentOS 7 系统。客户端主机的参数为 Intel(R) Core i5-4590 CPU @ 3.30 GHz 3.30 GHz, RAM 8.00 GB, 采用 Apache JMeter 测试工具分别对系统的各接口执行了 Http 请求测试，所有的实验数据为运行 10 次的平均值。区块链部署的节点数为 6 个节点。

5.1 智能合约设计

系统中的智能合约从数据对象上分为 DID 合

约、Credential 合约、CPT（凭证模板合约）；从数据结构的定义和设计维度可以分为 DidData 合约、CredentialData 合约、CptData 合约、IssuerData 合约和其他角色以及对象的权限控制合约，其依赖关系如图 3 所示。

DID 智能合约负责链上 ID 体系建立，包括生成 DID、生成 DID 相关文档、DID 在链上的读取与更新。

Authority 智能合约负责进行联盟链权限管理，包括链上 DID 角色的定义、操作与权限的定义与控制。

5.2 系统性能测试

系统性能测试时，模拟客户端首先发起身份注册请求，即 DID 创建请求。不同用户并发数量下 DID 创建的时间变化趋势如图 4 所示，从图 4 可以看出，身份创建时间随用户并发数量增加而增大。

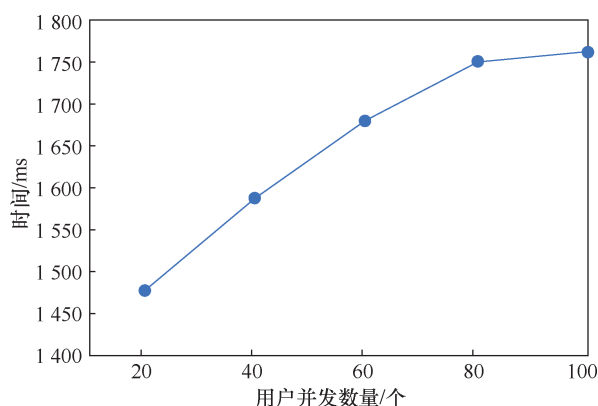


图 4 不同用户并发数量下 DID 创建的时间变化趋势
Figure 4 DID creation time under different concurrent users

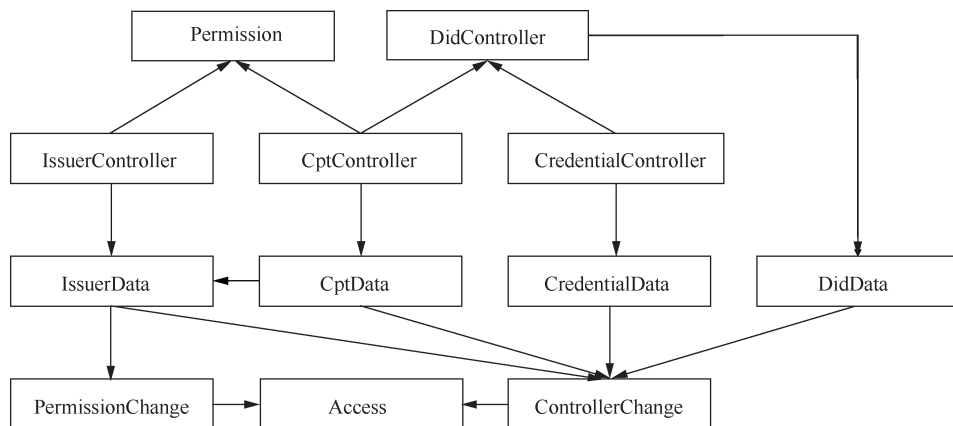


图 3 合约依赖关系
Figure 3 Contract dependencies

声明创建时间随用户属性个数的变化如图 5 所示。可以看出, 声明创建时间随用户属性数量的增加而增大, 基本呈线性趋势, 但增大趋势较弱。实际上分布式的凭证声明中的属性个数是有限的, 不会超过 20 个, 因此该系统完全满足实际运行的需要。

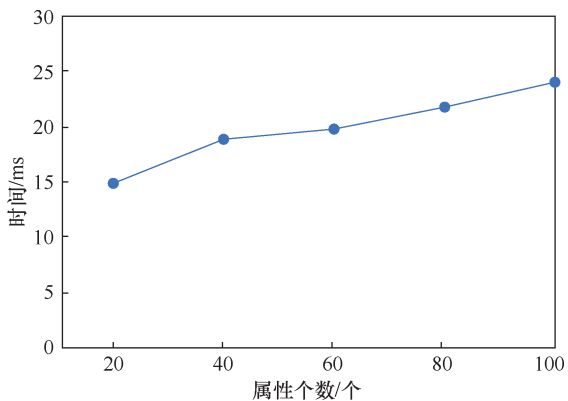


图 5 声明创建时间随用户属性个数的变化

Figure 5 Claim creation time with different number of user attributes

不同用户并发数量下普通凭证创建的时间和零知识凭证创建的时间分别如图 6 和图 7 所示。从图 6 和图 7 可以看出, 凭证创建时间均随用户并发数量的增加而增大, 但增长幅度逐渐减弱。且零知识凭证的性能几乎与普通凭证相近, 使用性能可以满足实际需要。虽然用户并发数量在增加, 但分布式的凭证发放方式降低了系统的总体开销, 相比集中式的凭证发放方式, 效率有所提高。在实际的系统中, 凭证创建分别由不同的委员会节点承担, 实际上是互不干扰的独立和并行运行子模块, 并不会累计于系统总时间中。

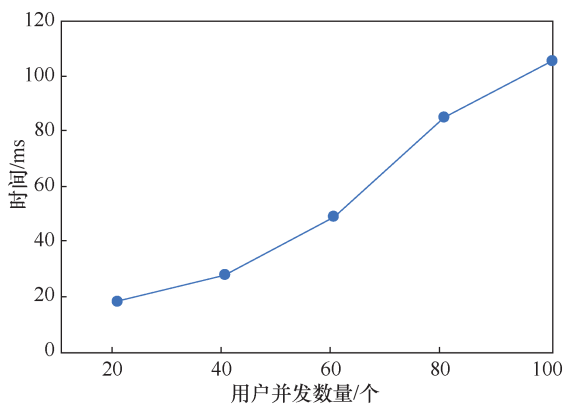


图 6 不同用户并发数量下普通凭证创建的时间

Figure 6 Credential creation time under different concurrent users

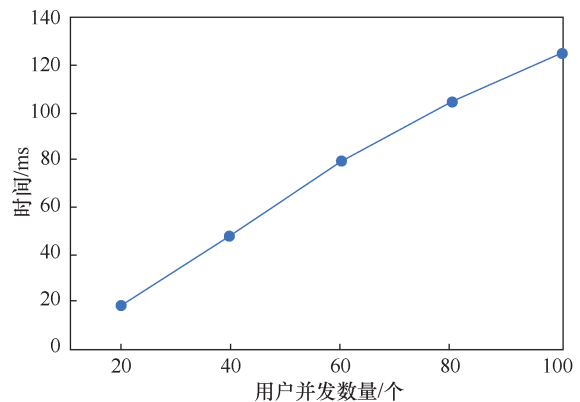


图 7 不同用户并发数量下零知识凭证创建的时间

Figure 7 Zero-knowledge credential creation time under different concurrent users

不同用户并发数量下普通凭证验证的时间和零知识凭证验证的时间分别如图 8、图 9 所示。可以看出, 与凭证创建相似, 凭证验证时间随用户并发数量的增加而增大, 但增长幅度逐渐减弱。因为用户并发数量在增加, 但分布式的凭证验证方式降低了系统的总体开销, 相比集中式的验证方式, 效率有所提高, 总体情况在可接受范围之内。

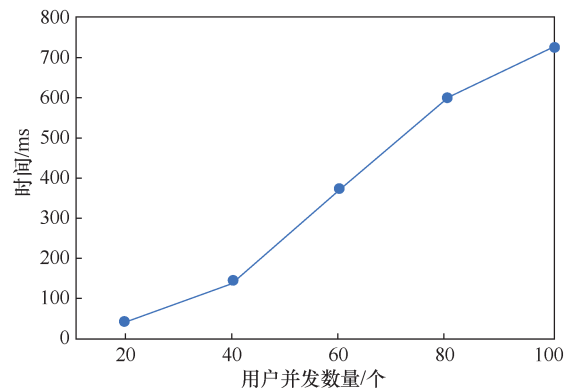


图 8 不同用户并发数量下普通凭证验证的时间

Figure 8 Credential verification time under different concurrent users

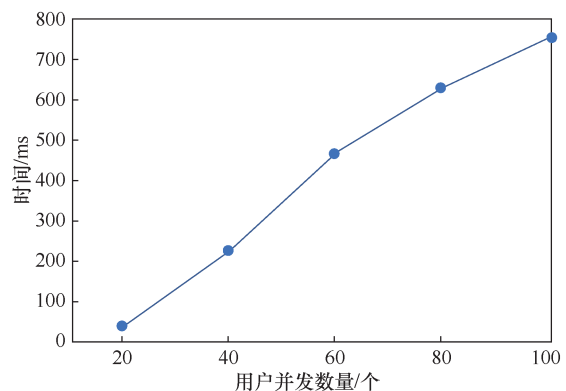


图 9 不同用户并发数量下零知识凭证验证时间

Figure 9 Zero-knowledge credential verification time under different concurrent users

存证创建时间和凭证撤销时间随凭证个数的变化分别如图 10 和图 11 所示, 凭证更新时间随属性个数的变化如图 12 所示。

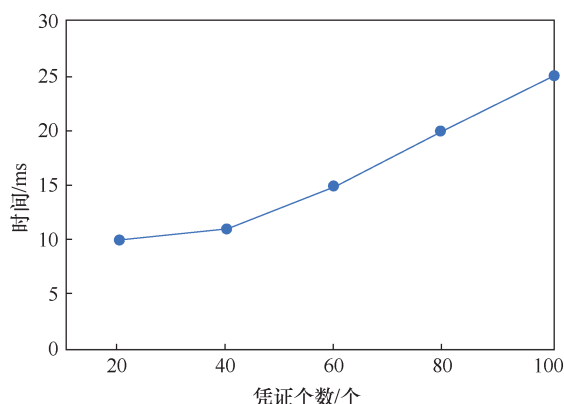


图 10 存证创建时间随凭证个数的变化

Figure 10 Evidence creation time with the number of vouchers

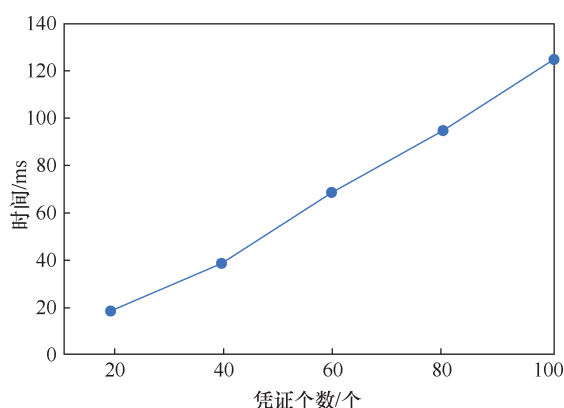


图 11 凭证撤销时间随凭证个数的变化

Figure 11 Credential revocation time with the number of vouchers

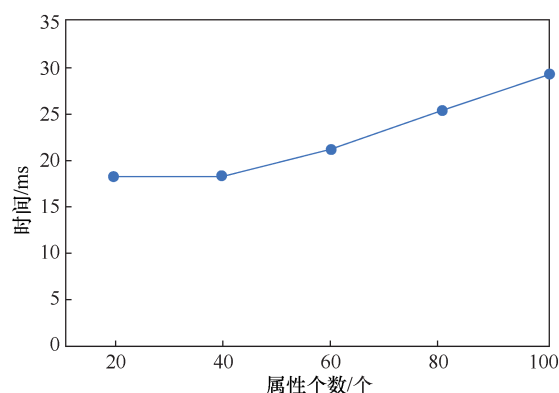


图 12 凭证更新时间随属性个数的变化

Figure 12 Credential update time with the number of vouchers

如图 10 和图 11 所示, 存证创建时和凭证撤销时间, 限制在同一个用户和模块中, 但是系统中的发证者实际上是分布式的而不是集中式的,

分布式的存证生成及撤销方式可以降低系统的总体开销, 相比集中式的验证方式, 效率有所提高。

从图 12 可以看出, 凭证更新时间随用户属性数量的增加而增大, 呈线性趋势, 由于每个属性的量级限制, 增大趋势较弱。在实际应用中, 属性个数是有限的, 一般为个位数, 该时间完全满足实际运行的需要。

6 结束语

为了解决微网中终端节点或应用的可信接入和业务访问控制等问题, 本文基于 FISCO BCOS 区块链提出了一个支持多中心的分布式身份管理平台, 支持用户身份的自主控制和多平台、跨链、跨应用间身份标识和凭证的移植。用户完全拥有、控制和管理自己的身份, 为微网系统和上层应用构建了一个公开透明可信的分布式身份底层框架, 实现了身份的自治和细粒度的访问控制。未来将着重研究认证过程的隐私保护问题。

参考文献:

- [1] 陈柳钦. 安全、稳定、经济、清洁的中国现代能源产业体系构建[J]. 武汉科技大学学报(社会科学版), 2011, 13(5): 497-505.
CHEN L Q. Constructing a safe, reliable, economical and clean modern energy industry system[J]. Journal of Wuhan University of Science and Technology (Social Science Edition), 2011, 13(5): 497-505.
- [2] 洪钟. 电力在我国能源中的战略地位[J]. 中国经贸导刊, 2014(19): 10-16.
HONG Z. The strategic position of electric power in China's energy[J]. China Economic & Trade Herald, 2014(19): 10-16.
- [3] 牛学杰, 李常洪. 中国新能源产业发展战略定位、政策框架与政府角色[J]. 中国行政管理, 2014(3): 100-103.
NIU X J, LI C H. On China's strategic orientation, policy framework and role of government in renewable energy sources[J]. Chinese Public Administration, 2014(3): 100-103.
- [4] 王福润. 智能电网配电技术及其对设备的要求[J]. 电器工业, 2012(1): 34-41.
WANG F R. Smart grid distribution technology and its requirements for equipment[J]. China Electrical Equipment Industry, 2012(1): 34-41.
- [5] 王玮, 李睿, 姜久春. 面向能源互联网的配电系统规划关键问题研究综述与展望[J]. 高电压技术, 2016, 42(7): 2028-2036.
WANG W, LI R, JIANG J C. Key issues and research prospects of distribution system planning orienting to energy Internet[J]. High Voltage Engineering, 2016, 42(7): 2028-2036.
- [6] 龚钢军, 高爽, 陆俊, 等. 地市级区域能源互联网安全可信防护体系研究[J]. 中国电机工程学报, 2018, 38(10): 2861-2873, 3137.

- GONG G J, GAO S, LU J, et al. Study on secure trusted protection architecture for prefecture-level regional energy Internet[J]. Proceedings of the CSEE, 2018, 38(10): 2861-2873, 3137.
- [7] 周洪益, 钱苇航, 柏晶晶, 等. 能源区块链的典型应用场景分析及项目实践[J]. 电力建设, 2020, 41(2): 11-20.
- ZHOU H Y, QIAN W H, BAI J J, et al. Typical application scenarios and project review of energy blockchain[J]. Electric Power Construction, 2020, 41(2): 11-20.
- [8] 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, 58.
- ZHAO Y H, PENG K, XU B Y, et al. Status and prospect of pilot project of energy blockchain[J]. Automation of Electric Power Systems, 2019, 43(7): 14-22, 58.
- [9] 吴斌, 杨超, 唐华. 区块链技术在微电网中的应用初探[J]. 电力大数据, 2018, 21(6): 17-22.
- WU B, YANG C, TANG H. Preliminary applications of blockchain technique in microgrid[J]. Power Systems and Big Data, 2018, 21(6): 17-22.
- [10] 周步祥, 杨明通, 史述青, 等. 基于区块链的微电网市场博弈模型[J]. 电力系统自动化, 2020, 44(7): 15-22.
- ZHOU B X, YANG M T, SHI S Q, et al. Blockchain based potential game model of microgrid market[J]. Automation of Electric Power Systems, 2020, 44(7): 15-22.
- [11] 余幸杰, 高能, 江伟玉. 云计算中的身份认证技术研究[J]. 信息网络安全, 2012(8): 71-74.
- YU X J, GAO N, JIANG W Y. Research on the authentication in cloud computing[J]. Netinfo Security, 2012(8): 71-74.
- [12] CELESTI A, TUSA F, VILLARI M, et al. Three-phase cross-cloud federation model: the cloud SSO authentication[C]//Proceedings of 2010 Second International Conference on Advances in Future Internet. Piscataway: IEEE Press, 2010: 94-101.
- [13] 魏晓菁, 刘冬梅, 温超. 国家电网公司目录服务, 身份管理认证系统的设计与实现[J]. 电力信息化, 2007, 5(10): 43-46.
- WEI X J, LIU D M, WEN C. Design and implementation of identity purpose and authentication system for directory service of State Grid Corporation[J]. Electric Power Information Technology, 2007, 5(10): 43-46.
- [14] DUNPHY P, PETITCOLAS F A P. A first look at identity management schemes on the blockchain[J]. IEEE Security & Privacy, 2018, 16(4): 20-29.
- [15] LIM S Y, TANKAM FOTSING P, ALMASRI A, et al. Blockchain technology the identity management and authentication service disruptor: a survey[J]. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8: 1735.
- [16] NASH A, DUANE W, JOSEPH C, et al. Public key infrastructure (PKI): implementing and managing E-security[M]. McGraw-Hill Education, 2001.
- [17] YU Y, WANG Y, HU Y, et al. Blockchain-based PKI system and its application in internet of things[C]//2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2). 2020: 4210-4215.
- [18] NAIK N, JENKINS P. Puort open-source identity management system: an assessment of self-sovereign identity and user-centric data platform built on blockchain[C]//Proceedings of 2020 IEEE International Symposium on Systems Engineering (ISSE). 2020: 1-7.
- [19] KIKITAMARA S, VAN EEKELEN M, DOOMERNIK D I J P. Digital identity management on blockchain for open model energy system[J]. Unpublished Masters thesis-Information Science, 2017.

[作者简介]



杨冠群 (1989-), 男, 山东济南人, 国网山东省电力公司信息通信公司工程师, 主要研究方向为机器学习、人工智能及区块链技术。

刘荫 (1985-), 男, 山东莱芜人, 国网山东省电力公司信息通信公司工程师, 主要研究方向为大数据分析与应用。

徐浩 (1988-), 男, 山东莱芜人, 国网山东省电力公司信息通信公司工程师, 主要研究方向为大数据分析。

邢宏伟 (1972-), 男, 山东青州人, 山东鲁软数字科技有限公司高级工程师, 主要研究方向为新一代信息通信技术在电网生产和企业管理中的应用。

张建辉 (1971-), 男, 河南洛阳人, 山东鲁软数字科技有限公司高级工程师, 主要研究方向为人工智能、信息安全及区块链技术。

李恩堂 (1977-), 男, 甘肃天水人, 山东鲁软数字科技有限公司工程师, 主要研究方向为人工智能、信息安全及区块链技术。