DOI:10. 3969/j. issn. 1674-1951. 2020. 08. 007

基于区块链技术的能源电力特色数据库管理

Database management with energy and power characteristics based on blockchain technology

杨琳[a],龚钢军[b],林红[a],王宝清[a],魏沛芳[b]
YANG Lin[a],GONG Gangjun[b],LIN Hong[a],WANG Baoqing[a],WEI Peifang[b]

(华北电力大学a.图书馆;b.电气与电子工程学院,北京 102206)
(a.Library;b.School of Electrical and Electronic Engineering,North China Electric Power University,Beijing 102206, China)

摘 要:如果能源电力数据被非法导出或篡改,国家安全将受到严重威胁。以华北电力大学能源电力特色数据库为例,分析了数据库管理现状与存在的问题,针对这些问题,基于区块链技术中的联盟链技术,提出了数据库与用户身份信息双重鉴权的技术方案,该方案能够强化信息安全认证,提高数据库的安全系数,保护数据贡献者的权利。根据区块链技术防篡改和可追溯的特点,提出能源电力数据库可溯源管理模型和管理流程,利用哈希算法得到文献防伪标签并记录于区块,为数据库文献的安全监管和溯源提供可信证据,能够有效防止能源电力数据被恶意访问者篡改。为能源电力数据库的高效监管和安全共享贡献了方案与思路。

关键词:区块链;数据库;双重鉴权;溯源;哈希算法
中图分类号:TP 311.13:TM 73:TK 01 **文献标志码**:A **文章编号**:1674-1951(2020)08 - 0048 - 06

Abstract: If the energy and power data are illegally exported or tampered with, national security will be seriously threatened. Taking the database with energy and power characteristic from North China Electric Power University for example, the current situation and existing problems of database management are analyzed. Based on the consortium blockchain technology, a technical solution with dual authentication for the database and users' identity information is proposed. This solution can strengthen information security certification, improve the security factor of the database, and protect the rights of data contributors. Based on the anti-tampering and traceability of the blockchain technology, the traceability management model and procedure for the energy and power database are put forward.Taking Hash algorithm to obtain anti-counterfeit labels for documents and recording them in the block can provide credible evidence for the safety supervision and traceability of the document, and can effectively prevent energy and power data from being tampered with by malicious visitors. Solutions and ideas for efficient supervision and secured sharing of energy and power databases are provided.

Keywords:blockchain; database; dual authentication; traceability; Hash algorithm

0 引言

互联网诞生初期主要是为了方便收发电子邮件(Email),但如今互联网已经渗透到人们工作、学习、生活的方方面面,收发E-mail仅仅是互联网的一个小小的应用。与之类似,区块链(blockchain)最初是作为比特币的底层技术进入人们的视线,但现在区块链技术已经在数据库管理、版权保护、电商供应链管理、物联网、智能制造、数字金融、数字资产交易、教育、医疗等领域广泛应用[1-4]。

谷俊、许鑫[5]基于Hyperledger Fabric项目的区块链框架上设计了人文社科数据共享联盟平台,促进了数据共享的发展。罗孟儒等[6]认为区块链技术在图书馆资源建设方面具有广阔的应用前景,研究了将区块链技术应用于图书馆资源采购、用户个性化资源推荐、馆藏资源共建共享等方面的技术框架。谢朝颖[7]分析了当前高校图书馆数字资源管理中存在的问题,提出了基于区块链技术的数据资源管理技术架构。邓国家等[8]将区块链技术应用于高校图书馆特色数据库管理,有助于图书馆数据库覆盖到更大的范围,并提高了数据库共享的安全性。上述研究对于提高数据资源的管理水平起到了积极的推动作用。

能源电力行业关乎国家的繁荣发展与社会稳

收稿日期:2020-06-22;**修回日期**:2020-07-14
基金项目:国家能源局科技项目(2017BJ0166)

定，如果能源电力数据被非法导出或篡改，国家安全将受到严重威胁。本文以华北电力大学能源电力特色数据库为例，分析数据库管理现状与存在的问题，基于区块链技术提出数据库与用户身份信息双重鉴权的技术方案和数据库可溯源管理模式，能够有效防止能源电力数据的泄漏和篡改。

1　数据库管理现状与存在的问题

在长期的办学实践中，华北电力大学在能源电力领域形成了独特的学科基础和鲜明的办学特色。目前，华北电力大学已购买与能源电力相关的国内外数据库 80 多个，例如：中国电力科技成果数据库、IEEE/IET Electronic Library 等。目前，师生使用能源电力特色数据库的途径有 2 种：校内通过校园网进入图书馆页面（这种途径不需要输入账号、密码），点击相关数据库的链接进入数据库，查询、下载数据；校外通过登录华北电力大学虚拟专用网络（VPN）（这种途径需要输入账号、密码），进入图书馆页面，点击相关数据库的链接进入数据库，查询、下载数据。

目前面向全校开放的能源电力特色数据库在管理方面存在着数据库容易被未授权用户伪装入侵、备份数据暴露、数据库关键文献数据被窃取或篡改等潜在的安全风险。其中，如果数据库文献数据被用户恶意修改，破坏了数据的完整性和有效性，那么使用该数据库的师生会接收到错误的资源，带来难以预知的后果。因此，能源电力特色数据库需进一步强化身份验证方案，拒绝非法入侵。但在实际情况中，加强版的身份验证只能有效地拒绝大多数外来攻击，依然可能存在被入侵的风险，因此如何应对入侵者，保护数据不被篡改，仍需深入研究。

2　区块链技术相关概念简介

2.1　哈希算法

哈希算法广泛应用于区块链技术中，哈希（或散列）算法能够将任意长度的输入值映射为较短固定长度的二进制值，这个二进制值称为哈希值（或散列值），区块链通常不保存原始数据的值，而是保存该数据的哈希值[9]。

2.2　非对称加密

为了保护隐私，可以通过签名和验签完成权属证明过程。在非对称加密技术中，密钥成对出现，即公钥和私钥成对出现[9]。公钥是公开的，私钥是保密的。私钥加密的信息只有对应的公钥才能解开；反之亦然，公钥加密的信息也只有对应的私钥才能解开。在加密、解密过程中，发送者用私钥加密（即：签名），接收者用公钥解密（即：验签）；在签名、验签过程中，常用私钥签名，公钥验签[10-11]。

2.3　公有链、私有链和联盟链

公有链是指任何个人或者团体都可以共用的区块链，只要接入该链就可以在上面发送交易，而且交易能够获得该区块链的有效确认，任何个人或团体都可以自由加入公有链。

私有链指仅仅使用区块链这一技术进行记账操作，不对外公开。私有链的数据写入权限完全归一个组织所有，该组织单独拥有数据改写的权限，或许会对外开放，但是有高度限制的读取权限[9]。私有链更适用于机构的内部。

联盟链是一种介于公有链和私有链之间的区块链，对于成员加盟有严格的准入机制，节点之间的信任强度大而且相互制约，所以联盟链的数据存储效率与公有链相比有很大的提升，同时其基于联盟节点的共识机制还能确保数据不会被其他机构非法修改[5]。

2.4　智能合约

智能合约是以数字形式定义的承诺，是合约参与方可以在其上执行这些承诺的协议，是传统合约的数字化版本，在区块链上是一种可执行程序[10]。区块链智能合约与传统程序一样拥有接口，接口可以接收和响应外部消息，也可以处理和储存外部消息。智能合约能够存储个人的身份信息或保存现有的身份状态，如果身份信息被非法修改，就会触发一定的条款，身份信息的所有者就会知晓[9]。

3　数据库与用户身份信息双重鉴权

本文涉及的应用场景为多个机构共同参与管理的分布式能源电力数据库，每个组织或机构管理一个或多个节点，数据只允许联盟内不同的机构进行读写和发送，所以联盟链更适合本文的应用场景。为了强化信息安全认证，提高数据库的安全系数，保护数据贡献者的权利，本节基于联盟链技术提出数据库与用户身份信息双重鉴权的技术方案，其整体系统架构如图 1 所示。

图 1 中，用户鉴权功能的实体分为：系统级 CA 节点（归属单一节点）和网络级 CA 节点（归属联盟链）。华北电力大学的能源电力数据库仅向特定的用户（本校师生）开放，作为一个机构，华北电力大学已经具有自己独立的用户管理系统（本文称之为原用户管理系统），用户可以从原用户管理系统发起数据服务请求，在原来系统内完成数据服务的接入鉴权流程。用户数据由原用户管理系统管理，用

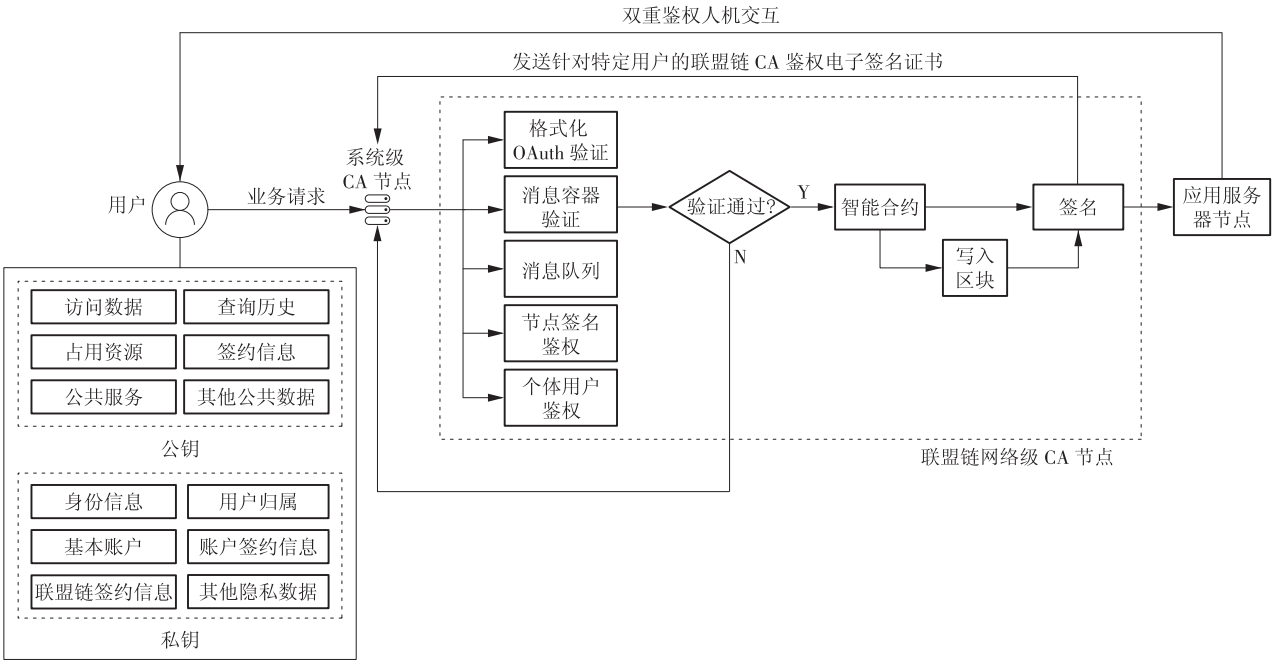

图 1 数据库与用户身份信息双重鉴权的整体系统架构

Fig. 1 Overall system architecture of dual authentication for the database and users´ identity information

户不直接和联盟链 CA 节点之间实施联盟链接入鉴权流程。下面从数据结构分析和信息系统双重鉴权机制 2 个方面介绍数据库与用户身份信息双重鉴权的技术方案。

3.1 数据结构分析[12]

本架构模型设计了符合数据共享要求的区块链体系架构用户数据结构，如图 1 左下部分。整合原用户管理系统中与用户相关的数据结构，按照数据属性分为 2 大类。

(1)可共享的公共数据。包含访问数据、查询历史、占用资源、节点签约信息、公共服务和其他公共数据信息。该类数据安全性要求较低，在联盟链中一般用电子签名中的公钥来认证。

注意这里节点主体是“原用户管理系统”数据所有者，并局限于特定的用户。这样设计的好处是，最大程度保护了原系统和数据所有者的利益，鼓励他们积极共享数据。

(2)不可共享的私有数据。包含身份信息、用户归属、基本账户信息、账户签约信息、联盟链签约信息和其他隐私数据。该类数据安全性要求较高，在联盟链中一般用电子签名中的私钥来认证。

3.2 信息系统双重鉴权机制

双重鉴权主要借助消息容器技术解决信息系统 CA 节点作为独立的分散个体共享用户数据的积极性不高的问题。消息容器是一种在消息的传输过程中处理消息的中间件技术。消息容器对于用户透明，在消息源(用户)、消息目标(联盟链 CA 集群)之间充当中间人的作用。为了提升联盟链 CA 节点的处理容量，联盟链 CA 节点不直接处理来自用户的鉴权请求，而是处理由系统级 CA 节点通过消息容器批量导入用户鉴权消息。从系统级 CA 节点一侧看，消息容器封装了系统签约用户数据；从联盟链网络级 CA 节点集群一侧看，消息容器是一种软件消息队列，队列的主要目的是保证消息的传递并提供回程路由索引。当系统级 CA 节点向联盟链 CA 节点发送消息时，如果联盟链 CA 节点接收者不可用，消息队列就会保留消息，直到成功送达为止。

在本文提出的设计中，不需要再重复创建独立的数据库与用户身份信息双向验证体系，而是采用基于 OAuth 2.0 开源协议的连接不同系统级 CA 节点主体的信息系统，将每个机构的系统级 CA 节点与联盟链网络级 CA 节点进行对接。双重鉴权的具体步骤如下。

(1)用户向原用户管理系统 CA 节点发起业务请求，经过认证过程后，原系统用户被赋予鉴权证书。用户可以在原系统 CA 节点覆盖的作用域内服务节点获取签约服务。

(2)原系统 CA 节点与联盟链网络级 CA 节点签约后，如用户希望在联盟链数据共享区域内获取共享数据服务，则原系统 CA 节点与联盟链网络级 CA 节点交互，完成用户身份信息双重鉴权。

(3)原系统 CA 节点利用消息容器技术将原系统用户鉴权证书打包，将消息容器数据包发送给联

盟链CA鉴权节点。

(4)联盟链CA鉴权节点实施系列化验证操作,包含OAuth协议栈处理、消息容器验证、消息队列完整性保护与加密处理、节点签名鉴权、个体用户鉴权。

(5)联盟链网络级CA节点实施系列化验证操作;如果都验证通过,执行步骤(6);如果有某一个条件不通过,向原系统CA节点反馈。

(6)执行该用户申请的签约服务,对应智能合约。

(7)颁发联盟链CA鉴权电子签名证书,同步写入联盟链区块。

(8)联盟链网络级CA节点向应用服务器发送特定用户授权服务范围和签约数据范围,并同步向用户发送联盟链CA鉴权电子签名证书。

3.3　技术方案的优势

3.3.1　容量增益方面的优势

消息发送者(由系统级CA节点通过消息容器转发)向联盟链网络级CA节点发送鉴权请求消息,无须等待响应。通过消息容器技术,消息发送者将消息发送到一条虚拟的通道上,联盟链网络级CA节点作为消息接收者监听该通道。一条消息可能最终转发给联盟链网络内的一个或多个网络级CA节点。这些联盟链网络级CA节点都无需对消息发送者做出同步回应,整个过程是异步的。采用异步处理模式可以提升联盟链网络级CA节点接入容量,同时保障用户感知。

3.3.2　信息安全增益方面的优势

应用程序和应用程序调用关系为松耦合关系,发送者和接受者不必了解对方,只需要确认消息。分布式联盟链网络级CA节点不必同时在线,分布式CA节点形成鉴权消息处理池,个别CA节点宕机不会影响联盟链整体对外提供接入鉴权的处理能力。

4　基于区块链的能源电力特色数据库可溯源管理模式

4.1　管理模型

图书馆中能源电力特色数据库种类多,容量大,为全校师生提供丰富的文献资源,因此其安全隐患不可忽视。除了要保证访问者身份的合法可信,还面临着被恶意访问者篡改等风险。而区块链技术中防篡改和可追溯的特性,正好为数据库安全存储提供很好的思路。本文提出基于区块链的能源电力特色数据库安全存储可追溯模型如图2所示。

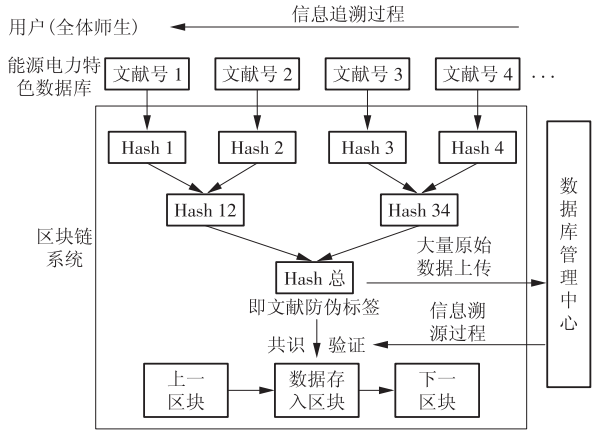

图2　基于区块链的能源电力特色数据库安全存储可追溯管理模型

Fig. 2　Secured storage and traceability management model of the energy and power database based on blockchain

在模型中,数据库管理中心和用户都是维护数据库数据安全运行的参与者,因此仍采用联盟链,因角色功能不同而设置不同权限的区块链节点。其中,赋予数据库管理中心全节点,主要有打包上链,查询验证等全部功能,而赋予用户轻节点,主要是查询和验证的功能,两者协作实现对庞大数据库数据真实性和完整性的高效监管,提高数据库的安全系数。

同时在图2中,不同类型的数据库针对自己包含的所有文献内容采用区块链中的哈希算法最终得到一个摘要值作为文献防伪标签,并记录于区块。其中,区块中加密的数据因修改成本高、难度大而具备难篡改性,所以区块链可以为数据库文献的安全监管和溯源提供有效可信的证据;在Merkle树中,通过两两哈希计算得到文献防伪标签,一旦有任一原始数据改动,其文献防伪标签就会发生改变,因此数据库可依照制定好的哈希算法溯源到被篡改的数据。综合两者优势,数据库采用区块链的管理模型,不仅可以保障记录数据准确无误,还可以通过定期核查哈希值实现及时识别数据库的坏数据,动态地保证数据真实有效。

4.2　管理流程及可行性验证

基于区块链的能源电力特色数据库可追溯管理模型中,能源电力特色数据库管理中心主要承担原始数据处理、打包成块以及定期核验的功能,并且提供给用户文献防伪标签核对服务,同时赋予用户可自行对文献核查的权限,弥补定期核查的缺陷[13]。这样,数据库和用户协同对海量文献数据实现高效可行的监管与溯源,保证数据库安全稳定的运行。具体管理流程如图3所示。

能源电力特色数据库和用户双方协同管理流

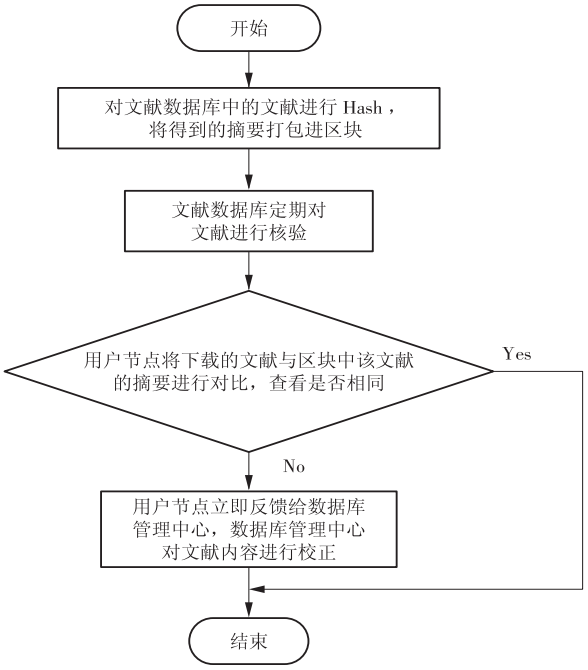

图3 基于区块链的能源电力特色数据库可追溯管理流程

Fig. 3 Traceability management process of the energy and power database based on blockchain

程如下。

(1)数据库针对所有文献内容采用区块链中的哈希算法最终得到一个摘要值作为文献防伪标签。

(2)数据库定期核验文献是否真实完整,通过采用同样的哈希算法对文献现在的内容数据进行运算,得到的值与区块中的文献防伪标签进行核对。

(3)若对比结果一致,则证明数据库里的文献正确可靠;若对比结果不一致,则表明数据库里的文献可能被篡改,可以查询区块,依照哈希算法中Merkle树层层溯源找到被篡改的具体文献号,进行修正。

(4)当用户访问能源电力特色数据库时,需要先通过第3部分所述的数据库与用户身份信息双重鉴权体系,完成身份验证并获得相应授权和电子签名证书后,可以进入数据库主页,在下载文档前,可以选择文献防伪标签核对服务。

(5)用户节点将下载的文献与区块中该文献的摘要进行对比,查看是否相同,如果是相同的则说明要下载的文献是原始真实的,可以安全下载;如果不相同则说明文献可能被篡改,此时应上报数据库管理中心,数据库管理中心对文献内容进行校正。

综上所述,能源电力特色数据库通过区块链赋予数据库管理中心和用户不同的权限,共同维护数据库的数据安全管理,凸显弱中心化优势;同时利用哈希算法实现数据可追溯的管理模式,有效地保障数据的真实性、完整性和保密性。

5 结束语

本文基于区块链中的联盟链技术,提出了数据库与用户身份信息双重鉴权的技术方案,先将用户身份信息按属性分成2类,然后借助消息容器技术实现双重鉴权,该方案能够强化信息安全认证,提高数据库的安全系数,保护数据贡献者的权利。

根据区块链技术防篡改和可追溯的特点,提出了能源电力数据库可溯源管理模型和管理流程,利用哈希算法得到文献防伪标签,并记录于区块,为数据库文献的安全监管和溯源提供可信的证据,能够有效防止能源电力数据被恶意访问者篡改。本文为能源电力数据库的高效监管和安全共享贡献了方案与思路。

参考文献:

[1]吴竞鸿. 基于区块链技术的自治型生鲜电商供应链管理研究[J]. 大理大学学报, 2020, 5(1): 123-128.
WU Jinghong. Research on supply chain management of autonomous fresh food e-commerce based on blockchain[J]. Journal of Dali University, 2020, 5(1): 123-128.

[2]陈诗鹏,陈彬,代明军,等. 一种基于区块链的物联网架构[J]. 物联网学报, 2020, 5(2): 1-6.
CHEN Shipeng, CHEN Bin, DAI Mingjun, et al. Blockchain-based IoT architecture[J]. Chinese Journal on Internet of Things, 2020, 5(2): 1-6.

[3]李健. 区块链在公共事业领域的应用与发展[J]. 人民论坛·学术前沿, 2020 (3): 57-65.
LI Jian. The application and development of blockchain in the public industries[J]. Frontiers, 2020(3): 57-65.

[4]余其凤, 陈振标, 刘敏榕. 区块链技术在图书馆数字资产管理中的应用探讨[J]. 数字图书馆论坛, 2018(7): 30-36.
YU Qifeng, CHEN Zhenbiao, LIU Minrong. A study on library digital assets management using blockchain technology[J]. Digital Library Forum, 2018(7): 30-36.

[5]谷俊, 许鑫. 人文社科数据共享模型的设计与实现——以联盟链技术为例[J]. 情报学报,2019,38(4): 354-367.
GU Jun, XU Xin. Design and implementation of a humanities and social sciences data sharing model: A case study of consortium blockchain[J]. Journal of the China Society for Scientific and Technical Information, 2019, 38(4): 354-367.

[6]罗孟儒,袁小一,熊拥军,等. 基于区块链的高校图书馆馆藏资源建设探析[J]. 图书馆工作与研究,2020(4):

90-97.
LUO Mengru, YUAN Xiaoyi, XIONG Yongjun, et al. Analysis of the construction of university library collection resources based on the block chain[J]. Library Work and Study, 2020(4): 90-97.
[7]谢朝颖. 基于区块链技术的高校图书馆资源管理应用研究[J]. 晋图学刊, 2020(1): 21-26.
XIE Zhaoying. Application research on academic library resource management based on blockchain technology[J]. Shanxi Library Journal, 2020(1): 21-26.
[8]邓国家, 袁西鹏, 郭新武. 基于"区块链"技术的高校图书馆特色数据库管理[J]. 管理观察, 2020 (4): 76-77.
DENG Guojia, YUAN Xipeng, GUO Xinwu. Characteristic database management of university library based on 'blockchain' technology[J]. Management Observer, 2020 (4): 76-77.
[9]何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1-7,15.
HE Pu, YU Ge, ZHANG Yanfeng, et al. Survey on blockchain technology and its application prospect[J]. Computer Science, 2017, 44(4): 1-7,15.
[10]张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG Liang, LIU Baixiang, ZHANG Ruyi, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12.
[11]丁腾波,刘宏波,吴聘. 智慧能源体系信息通信技术构架及实施方案[J]. 发电技术,2020,41(2):150-159.
DING Tengbo, LIU Hongbo, WU Pin. Information communications technology architecture and implementation scheme of smart energy system[J]. Power Generation Technology,2020,41(2):150-159.
[12]邵媛. 火电企业碳排放数据管理研究[J]. 华电技术, 2018,40(3):62-65,69.
SHAO Yuan. Research on carbon emission data management of thermal power enterprises[J]. Huadian Technology,2018,40(3):62-65,69.
[13]田甜. 基于实时数据库的状态监视系统实现[J]. 华电技术,2018,40(6):47-48.
TIAN Tian, Implementation of status monitoring system based on real-time database[J]. Huadian Technology,2018, 40(6):47-48.

(本文责编:齐琳)

作者简介:

杨琳(1978—),女,河南新乡人,讲师,工学博士,从事智慧图书馆、区块链技术在图书馆的应用等方面的工作(E-mail: yanglin@ncepu.edu.cn)。

龚钢军(1974—),男,河南济源人,副教授,工学博士,从事电力工控系统安全、能源互联网和区块链等方面的工作(E-mail: gong@ncepu.edu.cn)。

****

广　告　索　引