基于区块链的分布式电能量数据可信存储机制

李瑾[1,2]，仵松颀[1,2]，张森林[1,2]，陆月明[1,2]
（1. 北京邮电大学网络空间安全学院，北京 100876；
2. 北京邮电大学可信分布式计算与服务教育部重点实验室，北京 100876）

摘　要：针对电能量数据中心化存储面临中心单点故障、恶意篡改等问题，利用区块链的去中心化、防篡改、高度可拓展特点，通过构建电能量数据星际存储联盟链（ISCB），提出一种包括身份认证、传感数据上传、IPFS(星际文件系统)存储、区块链上传、访问验证 5 个部分的可信存储机制。针对电能量数据来源广、容量大等特点，将区块链技术与星际文件系统相结合，链上保存 IPFS 返回的数据哈希及查询属性，有效地解决了电能量数据区块链存储扩容及数据篡改识别问题。

关键词：联盟区块链；电能量数据；星际文件系统；安全存储
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−109x.2020029

Trusted storage mechanism of distributed electric energy data based on blockchain

LI Jin[1,2], WU Songqi[1,2], ZHANG Senlin[1,2], LU Yueming[1,2]
1. School of Cyber Science and Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Facing the problems of central single point failure and malicious tampering in the centralized storage of electric energy data, a trusted storage mechanism including identity authentication, sensor data upload, IPFS storage, blockchain upload and access verification was proposed by building the inter satellite storage consortium blockchain (ISCB) of electric energy data based on the decentralized, tamper proof and highly expandable characteristics of blockchain. In view of the characteristics of electric energy data, such as wide source and large capacity, the blockchain technology was combined with the inter planetary file system (IPFS), and the data hash and query attributes returned by IPFS were saved on the chain, so as to effectively solve the problems of storage expansion and data tampering identification of electric energy data blockchain.

Key words: consortium blockchain, electric energy data, IPFS, secure storage

收稿日期：2020−01−15；**修回日期**：2020−02−17

通信作者：陆月明，ymlu@bupt.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2019YFB2102403）
Foundation Item: The National Key R&D Program of China (No.2019YFB2102403)

论文引用格式：李瑾, 仵松颀, 张森林, 等. 基于区块链的分布式电能量数据可信存储机制[J]. 网络与信息安全学报, 2020, 6(2): 87-95.
LI J, WU S Q, ZHANG S L, et al. Trusted storage mechanism of distributed electric energy data based on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 6(2): 87-95.

1 引言

电能量计量是影响电能生产技术评估和电力交易结算的重要因素。随着智能电网、新型电力设备与电网信息系统的更新换代，分布式计量方式已成为电力系统中准确计量的重要手段。为使电能量数据安全、可靠、高效地存储及共享，智能电网需要广泛部署无线传感网络来监控电网状态，以便及时处理电网的异常情况。目前在智能电网中，利用可信中心节点集中采集无线传感数据进行存储和共享，这种集中存储方式面临数据恶意篡改、单点故障攻击等风险。针对这些信息安全问题，利用区块链分布式存储技术的去中心化、防篡改、高度可拓展等特征为电能量数据的高效可信存储提供有效的解决方案。

区块链[1]是一种按照时间顺序生成区块并顺序组合的链式数据结构，采用共识算法生成和更新数据，使用加密技术保证数据不被篡改或伪造。针对利用区块链结合实际场景完成数据存储和共享的研究，文献[2]建立基于区块链技术的医疗数据安全存储模型，通过分布式存储和传播机制，实现大规模可靠的端对端信息交互模式存储；文献[3]将传统区块链技术和数字签名相结合，完成对电能量的安全交易和交易数据的安全验证及存储；文献[4]基于电能量分布式采集提出一种基于区块链技术的电能计量数据分布式采集模式及安全机制，通过将设备信息与公钥证书上链以及设备间数据交互采用签名验签机制，保证了数据安全及设备不受非法攻击。由于智能电网中的节点类型多样，部分节点计算能力有限，将无线传感节点直接部署于传统区块链会使传感网络的能耗开销剧增甚至影响正常工作，不适用于传统区块链全体节点参与共识过程，且智能电网产生的电能量数据具有数据来源广、数据量巨大的特点，传统区块链体系中不可容纳全部数据。为此，本文结合星际文件系统（IPFS，inter planetary file system）及联盟区块链技术构建一种基于区块链的电能量数据可信存储机制，设计针对电能量数据的可信存储系统，命名为电能量数据星际存储联盟链（ISCB，energy interplanetary storage consortium blockchain）。星际文件系统[5]的基本原理是将信息保存到 IPFS 分布式节点中，系统会返回基于该信息计算得出的唯一哈希值，并可根据哈希值进行文件访问。联盟区块链[6]可建立在特定预选认证节点上实现共识记录，ISCB 将智能电网数据采集基站作为预选节点[7]。通过构建电能量数据星际存储联盟链，完成数据从采集节点到数据采集基站的传输、数据采集基站到 IPFS 的数据交互，及数据采集基站与区块链的数据交互过程，有效地解决了针对电能量数据的区块链容量扩展及数据篡改问题。

2 背景技术

2.1 联盟链

在不同的应用场景或设计体系中，区块链技术根据准入机制一般被分为公有链、私有链和联盟链[8]。公有链节点可以自由地进入或退出区块链网络，并且读取或写入链上的数据。私有链节点的准入与写入操作受内部权限控制，读操作可选择性地对外开放，仍具有区块链分布式存储架构。联盟链不同于公有链、私有链，它采用多中心的方式，通过预先设置参与节点和权限控制，成为介于公有链和私有链之间的“中间态”产品。联盟链因节点数量相对有限且有组织构成，具有弱中心化、强可控性、强拓展性、交易速度较快等特性，主要适用于特定组织或公司进行搭建。电能量数据一般应用于电网公司内部，电网技术人员可通过设置权限控制数据访问，且电能量数据并不需要全网节点共识，具有弱中心化特点，联盟链符合电能量数据存储所需的访问可控、高效存储及可信存储等数据存储需求。

2.2 智能合约

智能合约是 1994 由尼克萨博提出，在 2009 年区块链技术开始提供可信执行环境后，逐渐在以太坊、Hyperledger 技术框架上高效运行的一段可自发运行的计算机程序[9]。智能合约的出现赋予了区块链的可编程特性。与传统的程序代码相比，智能合约具有区块链的不可篡改、分布式存储、强制执行等特性。在电能量数据存储系统的搭建初期，电网技术人员可根据实际需求编写触发执行合约条件及合约内容，以脚本的形式部署至搭建的电能量数据存储系统中，在系统处于运行阶

段时，合约一旦满足触发条件便可执行合约内容，完成对数据的上传、访问等处理。

在基于区块链的电能量数据存储系统中，智能合约一方面，可以通过上述特点保证数据的隔离性、不可篡改性；另一方面，可以在智能合约中实现更小粒度的权限控制。此外，在服务调用的过程中，保证了数据的有效存储及访问可控。

2.3　IPFS

星际文件系统最初是由 2014 年 Protocol Labs（协议实验室）Juan Benet 设计并发展[10]的一种点对点连接、基于内容寻址的超媒体分布式协议。相对传统 HTTP 中心化服务器而言，它是一种点对点的分布式文件系统，服务器文件定位采用基于内容寻址而非多层目录寻址，大文件数据将被分割成小文件块存储在多个服务器中，能够创建持久且可用于高吞吐量的大量文件存储和共享。信息保存到 IPFS 系统成功后，将返回基于该文件内容计算的哈希值作为唯一标识。根据唯一标识请求文件时，它使用分布式哈希表查找文件所在的节点，检索文件并验证文件数据。

电能量数据具有数据来源广泛、数据容量大等特点，为解决集中存储数据面临的数据恶意篡改、单点故障攻击等问题，提出利用区块链技术去中心化、防篡改、高度可拓展的特点完成数据高效、可信的存储，但区块链存储容量有限，若在链中存储完整电能量数据，区块链系统将消耗大量算力达成共识。IPFS 作为一种非固定、细粒度、分布式的通用基础设施，没有存储限制且提供高吞吐量的基于内容寻址的块存储模型，可实现跨组织跨地域的大规模数据集链接存储，满足电能量数据来源广泛、容量大的存储需求，同时为利用区块链技术解决电能量数据防篡改存储的扩容问题提供了解决方案。

2.4　电能量数据

智能电网系统主要包括数据采集监视控制系统、电网调度管理系统、智能电表系统、能量管理系统等多套智能电网管理系统，这些智能数控系统被用来采集处理不同类型的电网数据，由此决定了电网数据的多源性。此外，智能电网由多个部分组成，包括电网传输线路、电子设备元件、终端传感器，智能电网中的数据采集终端对电网企业的输电、变电、配电、售电等各个环节产生的数据进行实时采集，这些电网数据包含信息种类较多，智能电网数据本质属性的不同导致了电网数据的异构性。通过利用电网采集终端与区块链技术相结合，利用共同维护的账本结构解决电网中多源异构数据存储问题，实现电能量数据的安全、可靠的分布式存储，具有较强的可拓展性；还可以通过设置系统访问权限，有效地控制电网数据平台的开放性。本文实验主要利用表码表[11]的数据存储证明存储方案的有效性，表码表记录了终端电能表每小时的表码读数，包括正相有功表码、无功表码等。

表 1　表码表数据样例

Table 1　Sample of code table data

数据库字段名	中文名称	示例数据	
POINTID	计量点编码	146 009	4 349
DATALINE	数据时间	2015/4/3 0:00	2015/4/3 0:00
PHASETYPE	分相类别	0	0
TARRIFTYPEID	费率类型	0	0
ZYBM	正向有功表码	96 679	2 171 912

3　方案设计

电能量数据星际存储联盟链结构如图 1 所示，ISCB 系统由数据采集节点、无限传感网络、数据采集基站、星际文件系统及区块链系统构成，数据采集节点通过无线传感网络，将采集的数据经过加密后发送到附近的数据采集基站，再由这些数据采集基站将数据传输到 IPFS，并返回数据的哈希值，作为文件的唯一索引，电能量数据星际存储联盟链选取数据采集基站节点作为预选节点，数据采集基站节点将文件哈希值、查询属性（如客户端节点 ID、查询目标数据采集节点 ID、查询数据类型、查询时间等）上传至区块链，联合运行共识算法，通过审计检验将数据录入电能量数据星际存储联盟链形成账本结构，实现去中心化的电能量数据安全可靠存储[7]。这个公共的账本可通过智能合约的方式设置查询条件参数，自动执行数据在节点间共享、授权的区块链节点进行安全访问。

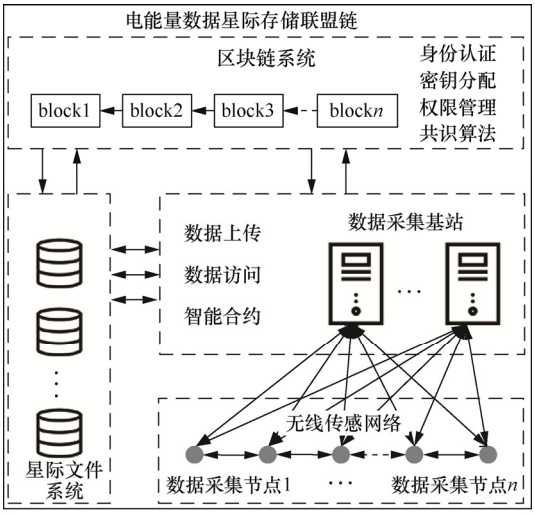


图 1 电能量数据星际存储联盟链结构

Figure 1 Electric energy data interstellar storage alliance chain structure

电能量数据星际存储联盟链运行主要包括以下 5 方面。

3.1 身份认证机制

Hyperledger Fabric 的成员身份认证基于标准的 X.509 证书，采用 PKI（public key infrastructure）体系为每个成员生成数字证书以标识用户身份。MSP（membership service provider）是 Hyperledger Fabric 的一个组件，它将证书发布、用户认证、后台加密机制和协议进行抽象，提供身份到组织的映射，利用 PKI 体系发布数据证书，结合 MSP 进行身份认证和权限控制。通过信任背书签发证书，从根 CA 证书的私钥签名生成的证书还可以签发新证书，中间 CA 证书可由其他 CA 证书签发，也可利用自身私钥签发新证书由此可形成一个证书信任链；Fabric CA 是超级账本的数字证书认证中心模块，Fabric CA 服务端提供用户登录和注册的数字证书管理功能，提供了 RESTful 接口供客户端访问，数据存储在 MySQL 中。通过 MSP 标识检查身份证书有效性、证书路径检查是否存在用户证书到根 CA 证书的有效路径及 CRL 检查证书是否被吊销完成身份认证。

3.2 传感数据上传

电能量数据采集节点先发送数据给附近数据采集基站，第 i 个数据采集节点 N_i 向数据采集基站中第 j 个数据采集基站 DC_j 传输的数据格式为

$$Record_{N_i \to DC_j} = E_{PK_{DC_j}}(Data_{E_{N_i}} \| Cert_{N_i} \| Sig_{sign_{N_i}} \| timestamp) \tag{1}$$

$$Data_{E_{N_i}} = E_{PK_{N_i}}(Data_{N_i} \| timestamp) \tag{2}$$

$$Sig_{sign_{N_i}} = Sign_{SK_{N_i}}(Data_{E_{N_i}}) \tag{3}$$

其中，PK_{DC_j} 为实体 DC_j 的公钥，$E_{PK_{DC_j}}$ 为利用 PK_{DC_j} 加密信息，PK_{N_i} 为实体 N_i 的公钥，$E_{PK_{N_i}}$ 为利用 PK_{N_i} 加密信息，$Data_{N_i}$ 为利用数据采集节点 N_i 采集到的原始数据，$timestamp$ 为时间戳，SK_{N_i} 为实体 N_i 的私钥，$Sign_{SK_{Ni}}$ 为利用实体 N_i 的私钥对 $Data_{E_{N_i}}$ 哈希运算后进行的签名数据。

3.3 数据 IPFS 存储

数据采集基站收集上传数据后对上传 $Record$ 进行验证，如利用自身私钥解密 SK_{DC_i} 得到字段如式(4)所示。

$$D_{SK_{DC_j}}(Record_{N_i \to DC_j}) = (Data \| Cert \| Sig \| timestamp) \tag{4}$$

提取其中的 $Cert$ 字段，对其进行身份验证确定数据来源为 N_i，并计算出 N_i 的公钥 PK_{N_i}，对提取出的 Sig 字段进行解密，得到 $D_{PK_{N_i}}(Sig)$，再对 $Data$ 进行哈希加密得到哈希数值，与发送节点发送来的数字签名解密得到的哈希数值 $D_{PK_{N_i}}(Sig)$ 进行校验，若相同则通过校验，验证数据正确。

如果数据来源安全且完整有效，数据收集节点客户端向 IPFS 请求将信息存储到 IPFS 中，IPFS 作为基于内容寻址的分布式存储网络，采用分布式哈希表（DHT）索引结构及 Merkle 有向无环图数据结构，服务器位置及文件存储名称或路径都不被作为索引条件。客户端提交数据存储请求至 IPFS 节点，IPFS 将会根据文件内容计算得到的哈希值返回给数据采集基站客户端。

3.4 数据区块链上传

数据采集基站节点向区块链网络发送上传请求，调用智能合约 stub.PutState 并将哈希值和信息类型等参数传入区块链网络；区块链节点收到请求首先验证用户身份，通过后执行智能合约将

哈希值、客户端 ID、数据采集节点 ID、查询数据类型（表码表）、数据收集时间绑定并广播该请求给其他节点执行相同的操作；然后在节点间达成共识后将智能合约执行结果写入区块链账本，反馈给收集节点客户端信息保存情况。电能量数据上传流程如图 2 所示。

3.5　数据访问验证

若客户端节点 DC_m 提交访问请求 DC_n 数据采集器所采集的 N_j 数据采集节点数据。

首先，客户端节点 DC_m 应向数据采集器节点 DC_n 提出感知数据共享请求，DC_n 节点查验身份后，将请求转发给数据采集节点 N_j；采集节点 N_j 制定访问约束条件（如数据共享范围、时效、访问次数等）授权访问，并将访问约束条件及访问数据的加密私钥 SK_j 发送给数据采集器节点 DC_n，数据采集器节点 DC_n 将访问条件、加密私钥 SK_j 等用客户端节点 DC_m 公钥 PK_{DC_m} 加密发送给客户端节点 DC_m。

其次，数据采集器节点 DC_m 通过自身私钥解密数据，并向智能合约提出访问请求，访问过程如图 3 所示，根据访问条件及访问身份调用智能合约解锁脚本，智能合约分析访问请求，提取信息类别后向区块链节点请求调用 stub.GetState 将查询条件作为参数传入，区块链节点执行智能合约，从区块链账本中检索出查询信息对应的哈希记录并反馈给客户端节点 DC_m；客户端 DC_m 根据哈希记录向 IPFS 节点发起请求查询出对应的加密信息，若根据哈希记录在 IPFS 中检索不出文件或检索出文件不符合访问条件，则证明数据被篡改。

最后，客户端节点 DC_m 利用从区块链上访问数据及 DC_n 发送的加密私钥 SK_j 后，利用加密私钥 SK_j 解密访问数据，完成数据访问过程。

4　系统实现

本文构建的基于区块链的分布式电能量数据安全存储方案，底层区块链采用 Hyperledger Fabric 构建联盟链，部署 3 台装有 Fabric 官方客户端的服务器为区块链节点，并将 Hyperledger 客户端节点上部署智能合约，将中国南方电网有限责任公司 2014 年—2015 年的表码表记录作为实验数据，完成基于区块链的分布式电能量数据安全存储方案的模拟实验，开发环境为 Centos 操作系统、Inter Core i5 处理器、内存 16 GB、硬盘空间 460 GB。为验证电能量数据安全存储方案的真实有效性，实验选取存储方案中 3 个关键环节进行测试，分别为电能量数据存储至 IPFS、电能量数据上传至区块链及电能量数据访问，并针对电能量数据存储至 IPFS 及电能量数据上传至区块链的吞吐量进行实验测试。

4.1　电能量数据存储至 IPFS 实验测试

客户端节点发布上传电能量数据至 IPFS 请求，IPFS 将返回数据哈希值作为 IPFS 唯一标识，其关键代码及功能展示如图 4 所示。

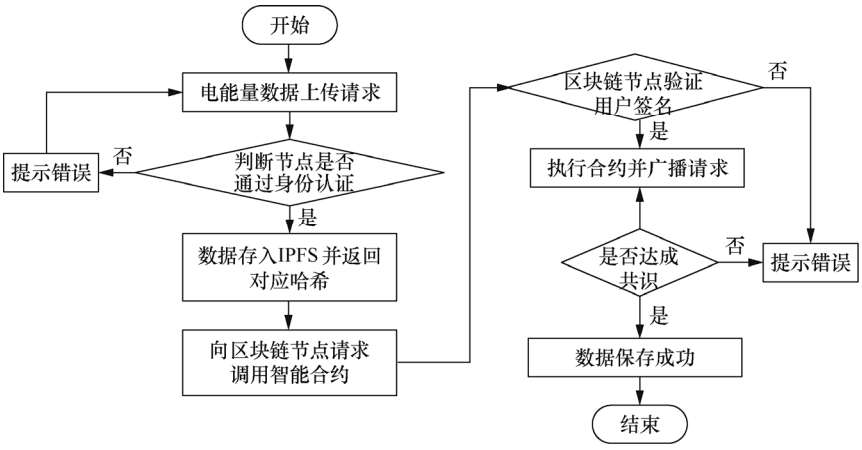


图 2　电能量数据上传流程

Figure 2　Electric energy data upload process

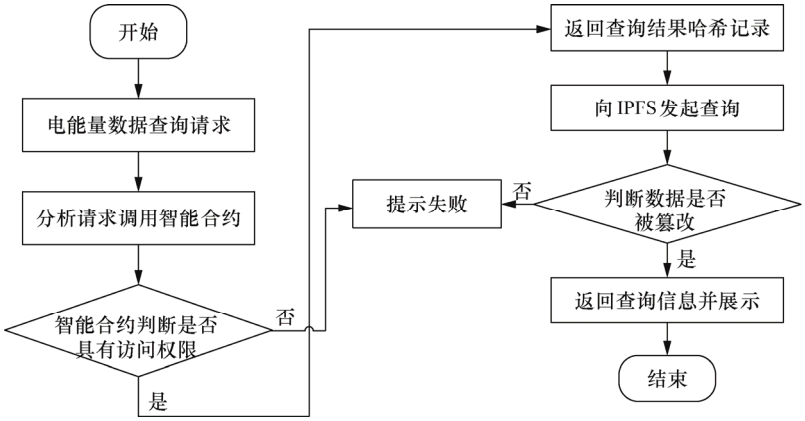


图 3　电能量数据访问流程

Figure 3　Electric energy data access process

4.2　电能量数据上传至区块链实验测试

客户端节点发布电能量数据上传至区块链请求，区块链节点请求调用 stub.PutState 并将电能量数据哈希值和信息类型等作为参数传入，在节点间达成共识后将智能合约执行结果写入区块链账本，反馈给收集节点客户端信息保存情况。其关键代码及功能展示分别如图 5、图 6 所示。

4.3　电能量数据访问实验测试

客户端节点提交电能量数据访问请求，调用智能合约分析访问请求，提取信息类别，将查询条件作为参数传入，智能合约根据查询信息从区块链账本中检索出对应的哈希记录并反馈给客户端；客户端节点根据哈希记录向 IPFS 节点发起请求查询出对应的加密信息，并利用查询信息解密出请求信息完成数据访问。其关键代码、功能展示、结果展示分别如图 7~图 9 所示。

4.4　实验数据

在仿真实验中，数据上传至 IPFS 的吞吐量测

```
[root@localhost test]# ipfs add -r updateFiles
added QmUy9NhLj4ei6AbqAvN4qGMjGkoiwtjsKcqq7S851QT4UQ updateFiles/ZDT_FREEZE_1401.dmp
added QmTcRcRnVQQLVzWzZizb1DxmSXLJHHrmHugSKGXZSSZpcR updateFiles/ZDT_FREEZE_1402.dmp
added Qmbt8gdzRaFybtpxxwW8aTSEB7D66VS2tNjUbTMnMTrJ1S updateFiles/ZDT_FREEZE_1403.dmp
added QmXZiQpAeponJvWBtDLXY8dWq5gnaKKhGbJEfAX2FNRHPG updateFiles/ZDT_FREEZE_1404.dmp
added QmUrz6aN7VgbNfkcfYpUNF64jWUZ4DL3v9fCDrnnjeacdS updateFiles/ZDT_FREEZE_1405.dmp
added QmbpRCcQNJK66zCTqSN1xn2NNxWJrQ3FEVB7iAqAniYTF7 updateFiles/ZDT_FREEZE_1406.dmp
added QmardJyXerBYjLGkzjL8MM3QpmFom8KN4qzrwgsh83sarR updateFiles/ZDT_FREEZE_1407.dmp
added QmbVP8WgWSo4ns3orH7YrKEsmDtKE57EUiX7pPiXLXHS6W updateFiles/ZDT_FREEZE_1408.dmp
added QmZBTeCqsg7Lmi7MKAc8qzWbv779hivR5UUVcSHWxVEoEE updateFiles/ZDT_FREEZE_1409.dmp
added QmWAbnysFUz94y25Z4cS178HpsoHCUtWWvqKsitxZnEX9r updateFiles/ZDT_FREEZE_1410.dmp
added QmSxeK2FrdVH3p9HEDSDYktvpKaY4S98uy4vwwcaoNcDF6 updateFiles/ZDT_FREEZE_1411.dmp
added QmdHbe6xeefzLKtTm6tzZgfCeQVeAd13EQwhR5Qpd2Wnyr updateFiles/ZDT_FREEZE_1412.dmp
added QmPgGRdenFneoFrkXBFeSjuSvj1gq4NyYPgXdVJhpGbJJk updateFiles
 125.18 MiB / 125.18 MiB [=============================================================================] 100.00%
```

图 4　电能量数据存储至 IPFS 关键代码及功能展示

Figure 4　Key codes and function display of electric energy data storage to IPFS

```
func (t * ElectricityBusiness) Init(stub shim.ChaincodeStubInterface) peer.Response{

    args := stub.GetStringArgs()
    err0 := stub.PutState("A",[]byte(args[0]))
    if err0 != nil {
        shim.Error(err0.Error())
    }
    var err error
    for i:=0 ; i<len(allFileNameArr); i++ {
        err = stub.PutState(allFileNameArr[i],[]byte(allFileHashIDArr[i]))
    }

    fmt.Printf("初始化成功! \n")
    return shim.Success(nil)
}
```

图 5　电能量数据上传至区块链关键代码展示

Figure 5　Key codes for uploading electric energy data to the blockchain

图 6　电能量数据上传至区块链功能展示

Figure 6　Function of uploading electric energy data to the blockchain

```
//查询方法
func (t *ElectricityBusiness) query(stub shim.ChaincodeStubInterface , fileName []string) peer.Response{
    fmt.Printf("开始查询\n")
    searchEArrUint8, _ := stub.GetState(fileName[0])//searchEArrUint8[]uint8 类型
    searchES := arrUint8ToString(searchEArrUint8)//[]uint8 -> string
    fmt.Printf("文件名:%s\n", fileName[0])
    fmt.Printf("HashID:%s", searchES)
    return shim.Success(nil)
}
```

图 7　电能量数据访问关键代码展示

Figure 7　Key codes for electric energy data access

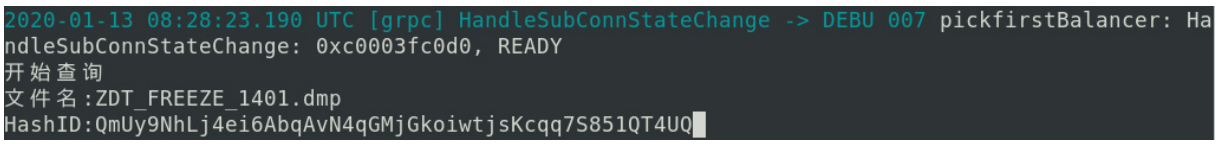


图 8　电能量数据访问功能展示

Figure 8　Electric energy data access function display

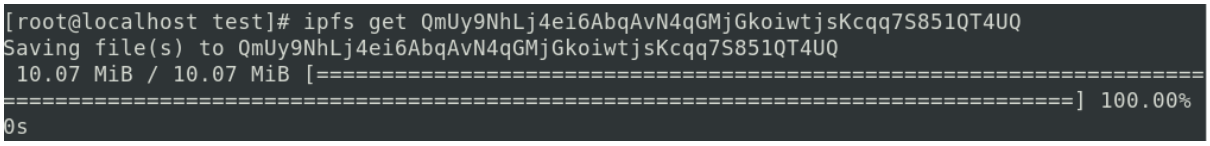


图 9　电能量数据访问结果展示

Figure 9　Electric energy data access result display

试结果如图 10 所示，数据容量选取以电能量数据中表码表数据容量为例，数据采集节点产生表码表数据为每 15 min 采集一次，记录 508 条数据产生的数据容量约为 110 kB，因此一个数据采集点 1 h 观测到 4 条数据，一个小区大概涵盖 3 000 到 5 000 数据采集节点，单位小时内产生的数据容量为 2 MB 到 4 MB，按照每 1 h, 2 h, …, 11 h 上传至 IPFS 为数据容量作为实验数据，得到完成上传及认证的时间分别为 0.353 39 ms、0.727 32～4.059 94 ms。针对电能量数据上传至区块链的吞吐量测试结果如图 11 所示，假设同一时间段内有 100～1 000 条电能量数据哈希记录值被加入区块链矿池中等待记录，测试上链只要耗时达成共识的时间约为 57.935～513.277 ms。

5　结束语

针对智能电网应用场景中心化存储所存在的中心单点攻击、数据被故意篡改等信息安全问题，利用区块链技术响应去中心化的分布式存储，IPFS 解决了区块链技术存在的数据存储容量问

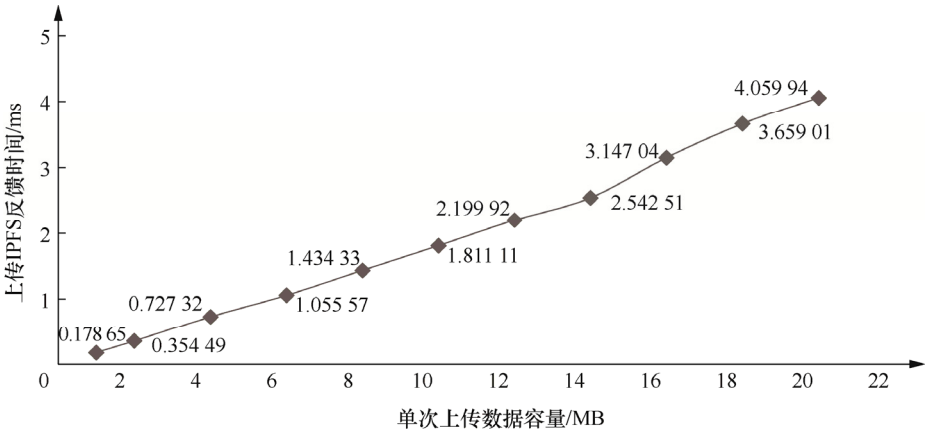


图 10　电能量数据上传至 IPFS 系统反馈时间

Figure 10　Feedback time of uploading electric energy data to IPFS system

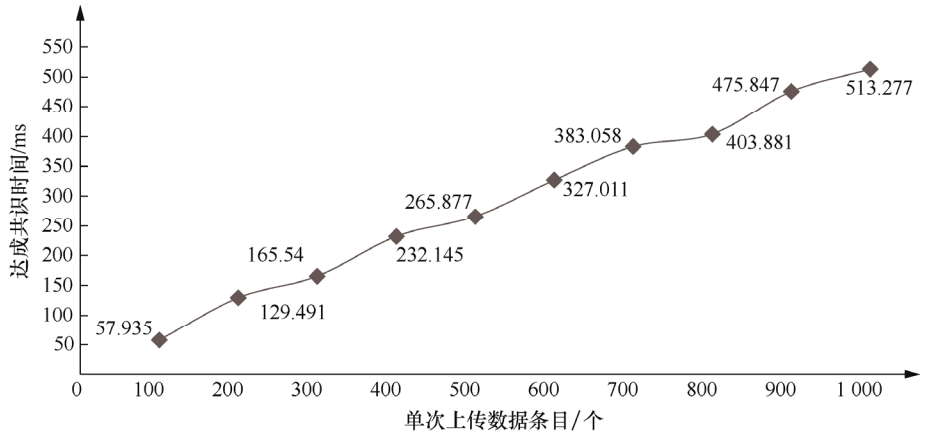


图 11　电能量数据上传至区块链达成共识时间

Figure 11　Consensus time for uploading electric energy data to the blockchain

题，区块链技术与 IPFS 的结合实现了针对电能量数据可识别篡改的安全存储。

本文结合电能量数据存储场景，将区块链技术和 IPFS 技术应用于解决电能量数据安全防篡改存储问题，从身份认证机制、感知节点数据上传、数据 IPFS 存储、数据区块链上传、数据访问验证 5 个部分全面描述了实现细节，并针对数据的吞吐量做了初步实验。但目前处于实验阶段，能否推广应用仍需进一步测试与验证，未来可尝试将方法与认证共享等需求相结合应用到电能量数据可信共享应用场景中。

参考文献：

[1] LIEBEHERR J, DONG G. An overlay approach to data security in ad-hoc networks[J]. Ad Hoc Networks, 2007, 5(7): 1055-1072.

[2] CHO J H, SWAMI A, CHEN I R. A survey on trust management for mobile ad hoc networks[J]. IEEE Communications Surveys & Tutorials, 2011, 13(4): 562-583.

[3] AITZHAN N Z, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. IEEE Transactions on Dependable and Secure Computing, 2016(10): 840-852.

[4] 卢继哲, 阿辽沙·叶, 刘宣, 等.基于区块链技术的分布式电能计量数据采集及安全机制研究[J]. 电测与仪表, 2020(1): 1-8.
LU J Z, ALIAOSHA Y, LIU X, et al. Research on distributed energy metering data collection and security mechanism based on blockchain technology[J]. Electrical Measurement & Instrumentation, 2020(1): 1-8.

[5] 陈杰, 张再跃, 张晓如. 融合 IPFS 与以太坊的爬虫智能合约研究[J]. 软件导刊, 2020(1): 1-4.
CHEN J, ZHANG Z Y, ZHANG X R. Research on identifier data

management strategy of industrial internet based on blockchain[J]. Software guide, 2020(1): 1-4.

[6] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.
SHEN X, PEI Q Q, LIU X F. Survey of block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.

[7] 章峰, 史博轩, 蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报, 2018, 4(4): 22-29.
ZHANG F, SHI B X, JIANG W B. Review of key technology and its application of blockchain[J]. Chinese Journal of Network and Information Security, 2018, 4(4): 22-29.

[8] 吴皓敏, 付绍静, 徐明, 等. 微型电网中基于联盟链的需求侧竞价方案[J]. 郑州大学学报(理学版), 2020(1): 1-7.
WU H M, FU S J, XU M, et al. Consortium blockchain based demand response in microgrids[J]. Journal of Zhengzhou University (Science Edition), 2020(1): 1-7.

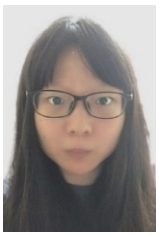
[9] 汪允敏, 李挥, 王菡, 等. 区块链在工业互联网标识数据管理策略研究[J]. 计算机工程与应用, 2020(1): 1-8.
WANG Y M, LI H, WANG H, et al. Research on identifier data management strategy of industrial internet based on blockchain[J]. Computer Engineering and Applications, 2020(1): 1-8.

[10] NIZAMUDDIN N, SALAH K, AJMAL AZAD M, et al. Decentralized document version control using Ethereum blockchain and IPFS[J]. Computers and Electrical Engineering, 2019(3): 183-197.

[11] 陈航. 基于数据挖掘的电力计量自动化系统异常分析[D]. 北京: 北京邮电大学, 2017.
CHEN H. Anomaly analysis of power measurement automation system based on data mining[D]. Beijing: Beijing University of Posts and Telecommunications, 2017.

[作者简介]

李瑾（1996− ），女，黑龙江齐齐哈尔人，北京邮电大学硕士生，主要研究方向为网络空间安全。



仵松颀（1998− ），女，陕西省西安人，北京邮电大学硕士生，主要研究方向为网络空间安全。

张森林（1996− ），男，河南商丘人，北京邮电大学硕士生，主要研究方向为网络空间安全。

陆月明（1969− ），男，江苏苏州人，北京邮电大学教授、博士生导师，主要研究方向为分布式计算、网络空间安全。