引用本文：王剑，杜亮，陈甜妹，等. 基于区块链的供应商信息库去中心化的解决方案[J]. 光通信技术，2022，46(2)：56–61.

基于区块链的供应商信息库去中心化的解决方案

王 剑，杜 亮，陈甜妹，陈 冰，傅天奕
（浙江省电力物资供应公司，杭州 310000）

摘要：针对传统供应商信息库集中式的部署模式难以保证数据真伪性和系统安全性问题，构建区块链的异构供应商电子文件存储系统。首先，根据区块链和星际文件系统（IPFS）进行异构数据的分布式存储，由区块链保存小文件，IPFS 网络进行异构大文件拆分和分布式存储，提升文件的存储速度；然后，采用区块链智能合约的文件访问控制策略，保证供应商文件管理的安全性和透明度，满足多场景下的文件安全访问。仿真结果表明：系统在保证高效的吞吐性能的同时，又能有效保障链上信息安全性和隐私性。

关键词：区块链；去中心化；智能合约；星际文件系统存储
中图分类号：TM734　**文献标志码**：B　**文章编号**：1002-5561(2022)02-0056-06
DOI：10.13921/j.cnki.issn1002–5561.2022.02.011　**开放科学（资源服务）标识码（OSID）**：

Decentralized solution of supplier information base based on block chain

WANG Jian, DU Liang, CHEN Tianmei, CHEN Bing, FU Tianyi
(Zhejiang Electric Power Supplies Co., td., Hangzhou 310000, China)

Abstract: Aiming at the problem that the centralized deployment mode of traditional supplier information base is difficult to ensure the authenticity of data and system security, a heterogeneous supplier electronic file storage system of blockchain is constructed. Firstly, the distributed storage of heterogeneous data is carried out according to the blockchain and interPlanetary file system(IPFS), the blockchain saves small files, and the IPFS network splits and stores heterogeneous large files, so as to improve the storage speed of files. Then, the file access control strategy of blockchain smart contract is adopted to ensure the security and transparency of supplier file management and meet the file security access in multiple scenarios. The simulation results show that the system can not only ensure efficient throughput performance, but also effectively ensure the information security and privacy on the chain.

Key words: blockchain, decentralization, smart contracts, interPlanetary file system storage

0 引言

随着我国国民经济持续快速增长，电力工程建设项目越来越多，项目供应商的数量和相关的资质信息也成倍增长。然而，信息类别、信息种类的差异和信息的真伪性等因素给后期项目评标工作带来了较大困难[1–3]；此外，基于采用传统信息库的集中式部署模式的系统存在可扩展相对较弱、中心节点抗峰值压力大和安全性受制于中心服务器的缺点，难以满足系统高抗峰能力和安全可靠的要求[4–7]。

近年来，区块链技术具有去中心化、不可篡改和高可靠的特性，突破了共识机制、隐私保护以及智能合约等方面的技术，使其在金融、医疗、供应链和物联网等行业的应用前景十分广泛[8]。区块链采用分布式部署结构，可有效破解集中式部署模式下中心节点抗峰值压力大的技术难题，且信息公开透明防篡改、数据可快速回溯，有效提升系统整体性能和吞吐量[9–11]。如基于区块链技术建立供应商信息库，既能保证其开放性，又能保证内部数据的安全[12]。交易数据写入区块

收稿日期：2021–10–30。
基金项目：国网浙江省电力有限公司科技项目（编号：5211WF200003）资助。

作者简介：王剑（1984—），男，硕士，高级经济师，浙江省电力学会会员，主要研究方向为物资管理、智慧供应链和区块链技术应用。负责完成省部级项目 6 项，获得省级管理创新一等奖 1 项、二等奖 2 项，研究课题获省级数据挖掘类一等奖 1 项。

链中能实现持久化存储，仅对单个节点数据的修改无法被全网通过，单个节点的数据丢失也不会对系统造成影响，保证了供应商相关数据的稳定性和可靠性[13-14]。通过建立区块链供应商信息库，可以获取当前数据库中的所有信息，自动生成标书，提高工作效率；对于已审核通过的供应商信息也可以实现所有节点共享，减轻了工作量[15]。

本文基于区块链技术对电力工程项目供应商信息库管理的积极作用，提出构建区块链的异构供应商电子文件存储系统，结合星际文件系统(IPFS)提升该存储系统对异构信息的存储速度和吞吐量，并提出基于区块链的智能合约访问控制策略，保证系统信息安全性，建立可靠的去中心化供应商信息库。

1 区块链技术

区块链是由区块有序链接形成的一种数据结构。其中，区块作为区块链的基本单元，由保证区块链接完整性的区块头和记录网络更新数据的区块主体构成，如图 1 所示。区块链技术通过其数据存储方式[16]、共识机制和智能合约技术[17]实现去中心化、实时共享和安全可靠等性能[18]。

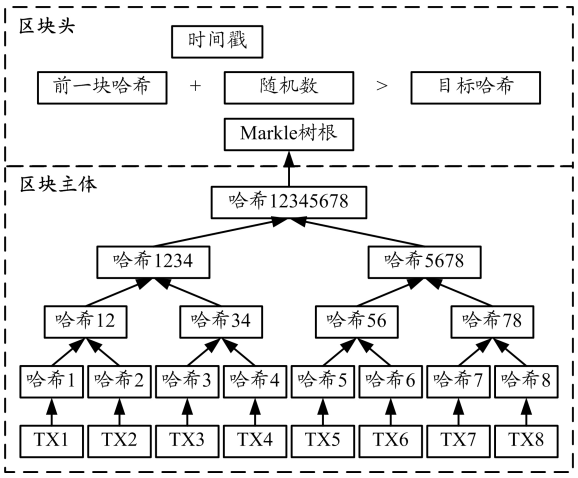

图 1 区块链数据区块结构

在区块链网络中采用点到点的组网方式，整个网络不设置中心服务器和中心路由器，网络中的各节点地位相等，可同时作为客户端和服务器端。各节点保存了整个区块链中所有数据信息，使所有诚实节点保存一致的区块链视图。当某一节点需要写入时，首先打包最小的数据存储结构“区块”，并向全网广播。全网节点接收到区块数据并对其合法性进行验证，若该区块链合法，则将该区块接入当前区块链中，进行数据遍历更新。一旦数据被写入区块链中，任何人都不能进行篡改；同时，在区块链中引入非对称加密来保证安全性需求。基于公开密钥和私有密钥进行数据加密和解密操作，保证数据来源的真实性和一致性。区块链的去中心化特征、强大的安全性以及可扩展性被广泛应用于不可信环境下的数据管理，适用于对安全性和保密性要求极高的招投标流程。

2 基于区块链的供应商信息库去中心化的解决方案

2.1 供应商信息库的分布式建设

传统的工程项目供应商信息库采用集中式存储方式将用户信息、数据、各类图片和音频进行中心化存储。由于受中心数据库和数据类型的制约，传统的供应商信息库存在事物不一致、数据不安全的问题[19]。区块链技术所具有的去中心化、中立、开放以及安全可信的优点，更有利于建立高度安全的系统。但在处理大型数据和异构文件时，区块链容易出现中央集权、数据不可信的缺陷。因此，本文将区块链与 IPFS 相结合，针对异构化供应商数据进行分布式存储[20]。

2.1.1 IPFS

IPFS 作为一类开源的、点对点分布式超媒体协议，通过结合分布式哈希表、区块链技术，可实现安全、自由的文件存储服务[21]。IPFS 中将大文件划分成多个固定大小数据库，使用默克有向无环图(Merkle DAG)组织数据库，无需护树的平衡，各中间节点也允许包含数据。IPFS 文件存储的简单流程如图 2 所示。

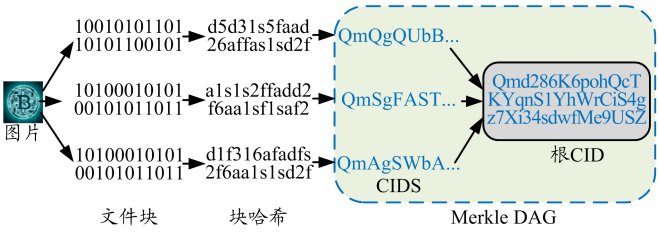

图 2 IPFS 文件存储的简单流程

由图 2 可知，IPFS 中默认图片的存储容量为 256 kb。首先，通过哈希计算获得各文件块的哈希值，并采用 Multihash 转化为相应的内容标识符(CID)，由 Merkle DAG 构建各文件数据块确定最终生成根 CID，实现基于文件内容的寻址方式；然后，使用数据块的唯一数字摘要代替传统访问路径识别指定块内容，通过检查树数据库摘要验证数据信息真伪性；最终，获得文件存储在 IPFS 的数据对象结构，如图 3 所示。

基于上述数据结构形式，对于存储容量大于 256 kb

```
type IPFSObject struct {
      links []IPFSLink      // 链接IPFS对象的一个数组
      data []byte           //一个二进制对象，最高存储256 kb的数据
}
Type IPFSLink struct {
      Name string           //链接的名称
      Hash Multihash        //链接对象的哈希值
      Size int              //连接对象的累计大小
}
```

图 3 IPFS 的数据对象结构

的文件,可细分为多个 IPFS 存储子对象,每个对象均包括数据 Data 和相连接的下个对象数组 Links，存储包括链接名称、链接对象的哈希值。图 4 为 IPFS 存储一个 678 kb 文件流程图。

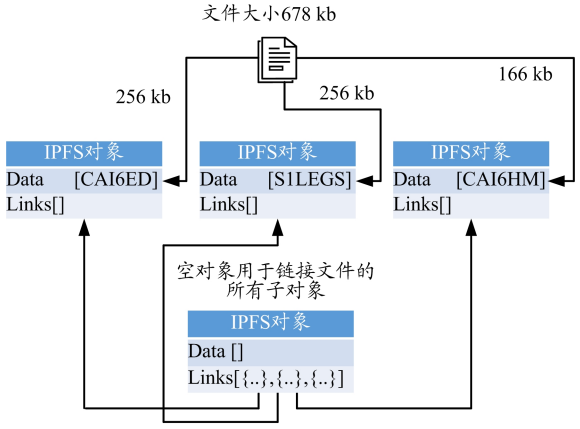

图 4 IPFS 文件分片存储

2.1.2 文件的分布式安全存储

为安全有效地管理和共享供应商文档信息,本文采用区块链系统构建供应商联盟链,使用智能合约存储和管理系统中相关的供应商电子文件信息进行存储。区块链和 IPFS 存储供应商联盟链上各节点供应商相关文件信息,某一供应商节点发布信息时,联盟内各节点通过访问网络上供应商文件实现文件共享,由联盟节点创建智能合约实现对供应商文件的存储和管理。

IPFS 文件主要用来解决区块链系统中大文件的存储,对于大量小文件,由于 IPFS 存储边际效应,使其绝对存储速度较慢。因此,本文设定 64 kb 为界,将小于 64 kb 文件定义为小尺寸文件,采用 Solidity 编写智能合约建立的使用流程如图 5 所示。

一个典型的智能合约包括合约编写、合约部署和合约调用 3 个主要步骤。合约中设置数据存储模块,通过 saveFileInfo()接口读写文件信息;同时,定义 fileInfo 结构体记录供应商文件信息,如表 1 所示。

对供应商联盟中用户所有者和文件访问者创建

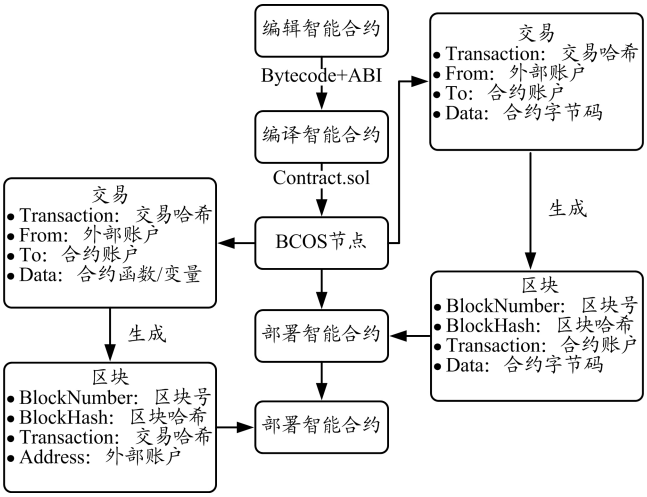

图 5 智能合约使用流程

表 1 智能合约文件数据结构

数据类型	参数	说明
uint	fileid	文件标识 ID
uint	logscn	关联数据库标识 scn
string	filedata	小文件的具体内容,大文件 IPFS 地址
string	filename	文件名
string	filesize	文件大小
string	creattime	文件存储时间
string	filelevel	文件密级

用户公钥和私钥;同时,创建节点的数据管理智能合约保存供应商文件信息,存储算法[22]如图 6 所示,具体执行步骤如下:

①解析日志信息,抽取供应商文件。从操作记录中抽取表 1 终端描述参数,根据文件存储路径抽取文件 F。

②计算文件大小。当文件 F 的字节存储容量大于 64 kb 时,转为 IPFS 中,为配备对应的哈希地址,记为 filedata;对字节小于 64 kb 的文件内容标记为 Filedata。

③根据解析事物日志判定供应商文件的密级决定是否公开。若为公开文件,则将产生的 filedata 和相关参数打包成待上链的文件数据;若为内部文件,则利用秘钥 K 加密 filedata 后,与相关参数融合打包。

④各供应商节点拥有自己的数据管理智能合约存储待上链的文件数据,由节点智能合约分配地址调用数据接口 saveFileInfo(),将待上链的文件数据存储在区块链上。

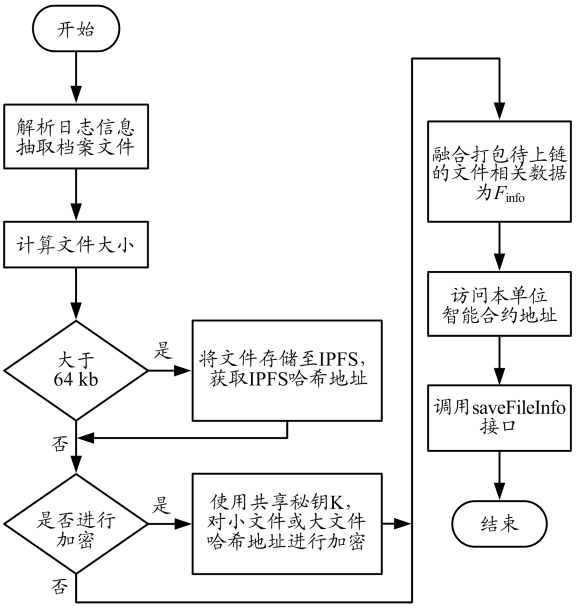

图 6 不同文件类型的存储算法

2.2 基于智能合约的文档控制

对于建立的基于区块链的供应商分布式数据存储模型中，基于 IPFS 寻址访问方式在访问文件时仅由文件哈希地址就可实现。由于供应商文件包含多种密级，直接将地址存储至区块链的方式尽管在一定程度上提升了数据的安全性，但基于区块链所存在的数据透明和数据访问控制的缺失，容易引发隐私问题。因此，本文针对不同角色访问不同密级文件权限，建立智能合约的分级动态访问控制模型进行访问权限管理。

2.2.1 分级动态访问

分级动态访问控制是一种基于智能合约技术的访问控制模型。在控制模型中，整个访问控制包括合约内和合约外。智能合约内主要用来实现合约内文件访问控制和读取，包括访问控制管理函数、文件管理函数；智能合约外设有文件信息的管理模块，包括文件名称、编号和合约地等信息。整个智能合约访问控制执行框架如图 7 所示。

首先，文件拥有者通过合约管理模块部署合约内接口函数，获得访问结果。当文件访问者发送授权请求后，拥有者通过合约模块调用权限管理函数为该用户分配角色和权限，并写入权限集，并将授权结果反馈给访问者。然后，当访问者要选定供应商信息范围时，由链外文件管理模块得到供应商文件编号地址和智能合约访问地址，调用合约内访问文件接口函数。智能合约根据一定规则访问合约内权限集，查询 Policy Map 和 TempPolicyMap 中是否记录用户权限信息，

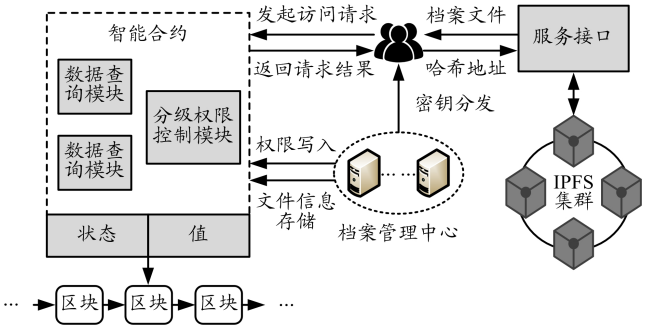

图 7 智能合约访问控制执行框架

若当前权限集包含该用户权限，则获取用户角色和权限记录，否则直接访问结果；若用户权限高于文件密级，根据文件密级访问相应的文件，获得供应商信息后，访问获得的文件数据。当文件中找到相应地质信息，返回空值。

2.2.2 访问控制策略

根据文件描述，本文将供应商信息分为公开、内部和秘密 3 个等级，采用 addPubFile、addInterFile 和 addSecretFile 等文件密级接口函数。文档信息包括供应商文件密级和文件编号和详细信息，通过该节点智能合约地址访问和调用信息存储接口。文件信息的分级存储写入代码如图 8 所示。

```
Input: Si, SCAddr, idfile, FInfo
Output: void

Procedure addFileInfo (Si, SCAddr, idfile, FInfo)
        // 根据合约地址获取智能合约
1:    DMSC←access(SCAddr)
        // 访问合约时确认是否为智能合约管理账户
2:    if DMSC.msgsender = = DMSC.ownerAddr then
            // 判断当前要存入的档案文件属于哪个密级
3:        if Si == public then
4:            publicFileMap ← DMSC.addPub File(idfile, FInfo)
5:        else if Si == internal then
6:            interFileMap ← DMSC.addInterFile(idfile, FInfo)
7:        else
8:            secretFileMap ← DMSC.addSecretFile(idfile, FInfo)
9:        end if
10:   else if
End procedure
```

图 8 文件信息分级存储

智能合约内访问控制模块分为访问权限授予和判断。访问权限授予包括流程准备和授权节点。流程准备阶段包括各供应商文件节点创建档案文件的智能合约、访问用户的账号和公钥、私钥，以及对账户进行授权。对于项目供应商，管理员在创建用户和分配秘钥时，根据用户角色在智能合约内进行分级授权；对于项目外用户，则需要用户根据所在节点为账户发起权限请求。当用户向智能合约申请访问密级供应商文件时，首先判定用户永久访问权限是否大于设定权限，若不符合，则查询用户临时动态权限是否大于设

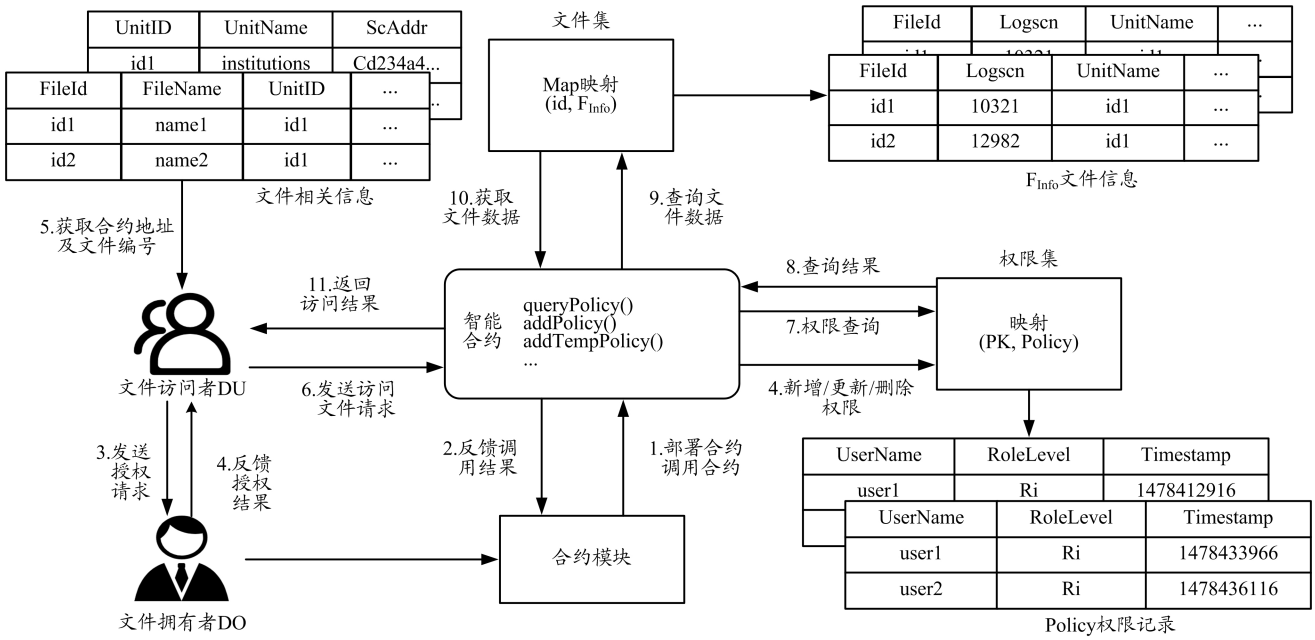

图 9 访问控制智能合约流程

定权限;若符合,则根据相应权限访问供应商文件信息。供应方分级存储至智能合约控制流程如图 9 所示。

3 仿真实验结果分析

为验证所提方案的可行性,本文对其进行性能测试,评估区块链的交易吞吐量和存储性能。实验环境为搭建在 4 个节点的区块链网络。系统运行 CPU 采用 Inter Xeon CPU E5-2630 v4@2.20 GHzx40, 系统的缓存读取速率为 8239.98 Mb/s,硬盘读写速度为 400.97 Mb/s,带宽为 941 Mb/s。

3.1 系统的数据交易吞吐量

数据交易吞吐量即每秒区块链网络接收交易的数量。采用 16 个进程向 4 个节点发送 20 万条记录,每条记录约 500 字节。图 10 为区块交易吞吐量点状图。可以看出,区块链在 952 s 时接受了 20 万个交易,最终网络吞吐量中位数为 213 tx/s,平均数为 210 tx/s。

为测试在超负荷环境下的系统性能,将交易进程数由 4 个增加到 48 个,每组交易吞吐量仍为 20 万条记录。多进程下数据吞吐量及延时情况如图 11 所示。可以看出, 系统的吞吐量随进程数量增加不断上升。进程数达到 16 个时的交易吞吐量在 215 tx/s 左右,并趋于稳定, 交易延迟也由最初的 0.036 s 上升到了 0.295 s,可见高并发使得每笔交易延迟有所增加,但整体依然处于低延迟状态。

3.2 文件存储性能测试

本文选择 4 种典型小文件场景进行文件存储性

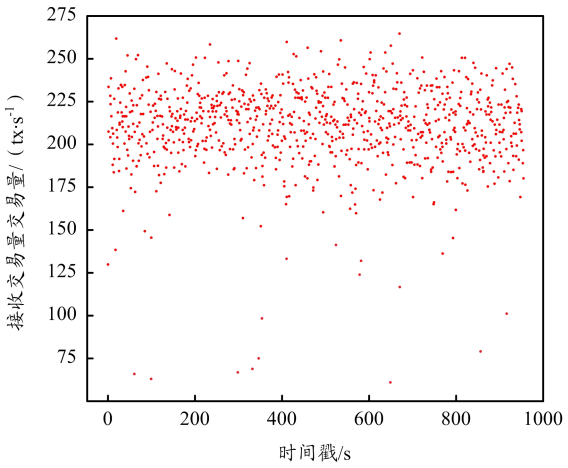

图 10 区块链数据交易吞吐量点状图

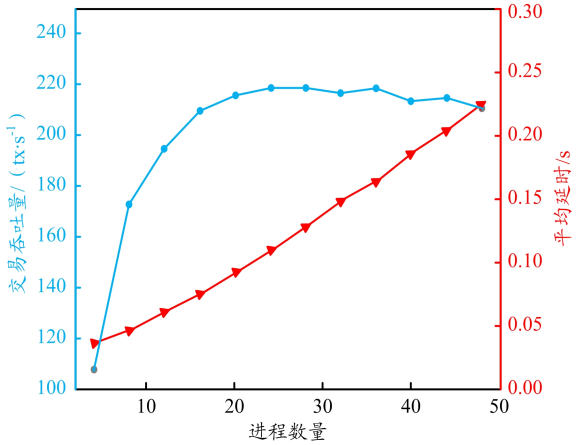

图 11 多进程下数据吞吐量及延时

能测试，典型的案例数据如表 2 所示。本文以 64 kb 划分文件大小，形成不同小尺寸文件占比。4 组测试中，每组数据集设定大小为 20 Mb，每组进行 10 次试验，以平均值作为结果，分别计算传统 Oracle 中心存储和本文存储方法的文件上传时间。

表 2 测试应用案例

场景	文件大小/kb	小尺寸文件比例	数据来源
1	1~128	80%	邮件
2	4~1024	60%	日志
3	10~2048	40%	图片
4	32~5120	20%	音频

4 种场景中存储测试性能情况如表 3 所示。与中心存储法和 IPFS 方案相比，本文方案的存储效率分别提升了 20.86%和 13.49%。随着小尺寸文件占比下降，本文方案的提升效果逐渐下降，在场景 4 中，本文方案相较于 IPFS 方案的存储效率提升了 8.33%。此外，随着大尺寸文件比例的上升，存储用时也不断减小，主要是由于数据集文件的减少，降低了区块链与 IPFS 交互作用。因此，本文方案在小尺寸文件存储方面效果明显，且通过区块链、IPFS 实现了数据存储的中心化、防恶意串改，保证了数据的安全性。

表 3 存储测试性能情况

类型	存储用时/s			
	场景 1	场景 2	场景 3	场景 4
中心存储法	463	392	238	187
IPFS 方案	426	372	241	132
本文方案	348	326	218	121

4 结束语

区块链技术的去中心化、共识机制、隐私保护和智能合约等方面的技术突破，给传统供应商系统带来了巨大变革。本文将区块链和 IPFS 存储技术进行融合，构建了异构供应商电子文件存储系统。在文件存储方面，提出区块链上存储小文件、IPFS 网络存储大文件的方式，从而提升区块链对大量小文件场景下的存储速度；同时，为保证供应商文件管理的安全性和透明度，提出基于区块链智能合约的文件访问控制策略，通过对供应商文件进行密集分类、智能合约的访问权限授予与判定，实现多种需求场景下对供应商文件的安全访问。通过对建立的异构文件存储系统进行仿真，结果表明：结合区块链和 IPFS 网络的存储方法具有高效的吞吐性能，能有效保障链上信息安全性和隐私性。

参考文献：

[1] 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.
[2] 程华，杨云志. 区块链发展趋势与商业银行应对策略研究[J]. 金融监管研究，2016(6)：73–91.
[3] 张宁，王毅，康重庆. 能源互联网中的区块链技术：研究框架与典型应用初探[J]. 中国电机工程学报，2016，36(15)：4011–4023.
[4] 钱卫宁，邵奇峰，朱燕超. 区块链与可信数据管理：问题与方法[J]. 软件学报，2018，29(1)：150–159.
[5] 邵奇峰，金澈清，张召. 区块链技术：架构及进展[J]. 计算机学报，2018，41(5)：969–988.
[6] 刘敖迪，杜学绘. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报，2018，29(7)：2092–2115.
[7] 蔡维德，郁莲，王荣. 基于区块链的应用系统开发方法研究[J]. 软件学报，2017，28(6)：1474–1487.
[8] 杨德昌，赵肖余，徐梓潇. 区块链在能源互联网中应用现状分析和前景展望[J]. 中国电机工程学报，2017，37(13)：3664–3671.
[9] 曾鸣，程俊，王雨晴，等. 区块链框架下能源互联网多模块协同自治模式初探[J]. 中国电机工程学报，2017，37(13)：3672–3681.
[10] 欧阳旭，朱向前，叶伦，等. 区块链技术在大用户直购电中的应用初探[J]. 中国电机工程学报，2017，37(13)：3737–3745.
[11] 汪传雷，万一荻，秦琴. 基于区块链的供应链物流信息生态圈模型[J]. 情报理论与实践，2017，40(7)：115–121.
[12] 韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望[J]. 自动化学报，2019，45(1)：206–225.
[13] 何蒲，于戈，张岩峰. 区块链技术与应用前瞻综述[J]. 计算机科学，2017，44(4)：1–7，15.
[14] 王继业，高灵超. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展，2017，54(4)：742–749.
[15] 赵阔，邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全，2017(5)：1–6.
[16] 李彬，卢超，曹望璋，等. 基于区块链技术的自动需求响应系统应用初探[J]. 中国电机工程学报，2017，37(13)：3691–3702.
[17] 武赓，曾博，李冉. 区块链技术在综合需求侧响应资源交易中的应用模式研究[J]. 中国电机工程学报，2017，37(13)：3717–3728.
[18] 杨慧琴，孙磊，赵西超. 基于区块链技术的互信共赢型供应链信息平台构建[J]. 科技进步与对策，2018，35(5)：21–31.
[19] 陈何清. 基于区块链的 IMIX 传输系统的设计与实现 [D]. 南京：南京大学，2016：66–72.
[20] 王发明，朱美娟. 国内区块链研究热点的文献计量分析[J]. 情报杂志，2017，36(12)：69–74，28.
[21] 李彬，曹望璋，张洁. 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.
[22] 余维，胡跃. 基于能源区块链网络的虚拟电厂运行与调度模型[J]. 中国电机工程学报，2017，37(13)：3729–3736.