刘卓娴. 融合 IPFS+区块链技术的执法办案数据访问控制方案[J]. 智能计算机与应用,2025,15(1):103-109. DOI:10.20169/j.issn.2095-2163.24081502

融合 IPFS+区块链技术的执法办案数据访问控制方案

刘卓娴

(中国人民公安大学 信息网络安全学院, 北京 100038)

摘 要: 针对执法办案数据电子化存储可能出现的被篡改、被伪造以及泄露问题,提出了一种融合 IPFS+区块链技术的数据访问控制方案。该方案以 DPOS 共识机制为基础,结合 hash 算法和非对称加密算法,在半分布式网络使用 Merkle 树,验证数据传输的完整性;激励层使用 Token 和智能合约奖惩机制,提升了公安传送档案的准确性。应用结果表明,该方案可以保证档案内容的保密性及不可篡改性,对于防止徇私枉法、档案泄露具有重大意义。

关键词: 执法办案数据; 区块链; Token 机制; 共识机制; 访问控制

中图分类号: TP311.13;D631 **文献标志码**: A **文章编号**: 2095-2163(2025)01-0103-07

A data access control scheme for law enforcement and handling cases integrating IPFS+ blockchain technology

LIU Zhuoxian

(Information Network Security Academy, People's Public Security University of China, Beijing 100038, China)

Abstract: In response to the potential issues of tampering, forgery, and leakage in the electronic storage of law enforcement case data, this article proposes a data access control scheme that integrates IPFS+blockchain technology. The scheme is based on the DPOS consensus mechanism, combined with hash algorithm and asymmetric encryption algorithm, and uses Merkle tree to verify the integrity of data transmission in a semi distributed network. The incentive layer uses Token and smart contract reward and punishment mechanism to improve the accuracy of public security file transmission. The application results show that this scheme can ensure the confidentiality and immutability of archive content, which is of great significance in preventing favoritism, bending the law, and archive leakage.

Key words: law enforcement and case handling data; blockchain; Token mechanism; consensus mechanism; access control

0 引 言

近年来,随着信息技术的飞速发展与普及,数字档案的应用已经深入到社会生活的各个领域,成为信息时代不可或缺的重要组成部分。无论是政府机构、企事业单位还是学术研究、文化传承等领域,数字档案都以其高效、便捷、易于保存与检索的特性,逐渐取代了传统的纸质档案,成为信息记录与传承的主流方式。

20 世纪 90 年代以来,美国最早开始研究数字档案,此后一些国家也逐步开始了数字档案的探索。20 世纪 90 年代末,国家档案局首次提出了建立数字档案的构想,并尝试将纸质档案、音频档案、视频等材料进行数字化,从而可以永久地查询及共享数据。随着数字档案技术的发展和相关建设原则的提出,数字档案在中国逐渐发展起来。肖敏[1]引用大数据技术进行数字档案建设,从中进一步挖掘出档案的内在价值,对于帮助管理者决策、提高档案管理系统的价值和服务质量具有积极意义。游姗姗[2]将云计算技术应用到福建数字档案馆信息平台的建设,实现了档案信息的云共享、高效处理和海量存储。刘悦[3]提出一种 NAS 加持下的数字档案存储和管理系统,为档案的便捷化、数字化管理提供了一种有效方案。

随着数字档案长时间的建设和发展,相关标准和规则在逐步完善,同时更多前沿技术也被不断引入以强化数字档案的建设与管理。然而,尽管取得了显著进步,数据库技术的集中性特征以及电子文

作者简介: 刘卓娴(2000—),女,硕士研究生,主要研究方向:区块链,数据隐私保护。Email:1240875185@qq.com。

收稿日期: 2024-08-15

件在安全性、真实性方面面临的挑战依然严峻,文件伪造、盗窃、篡改等风险事件时有发生,这对数字档案的长期保存与价值实现构成了威胁。在此背景下,区块链技术以其独特的分散性、无真相性和防篡改能力,为数据保护和共享提供了新的解决方案,开辟了数据安全管理的新纪元。近年来,国内外众多专家与机构积极投身于区块链技术在数据保护领域的研究与实践,旨在利用这一技术强化电子文件的真实性与安全性。

区块链[4]起源于比特币白皮书,是一种分散的、无真相的、防篡改的分布式记账技术,其综合运用了密码学、共识机制、分布式网络等多种技术,开辟了数据篡改和安全的新途径。近年来,国内外许多专家和相关机构不断探索和实践区块链技术在数据保护和共享方面的应用。为了保护电子文件的真实性,Proof of Existence[5]方案将对应文件的哈希值存储于区块链的交易记录中,并可以证明文件的存在。该方案在电子文件数据保护方面进行了实践,但数据保护功能相对单一,成本较高。国内蚂蚁金服公司采用区块链技术,记录支付宝捐赠的具体流程,从而保证资金使用的透明性、可追溯性和不可篡改性[6]。在公安领域,李康震等[7]进行了区块链在公安情报中的应用探究;陈学凡[8]提出了区块链技术应用于公安工作的思考与探讨;熊建英[9]以设计一种公民信息管理模型为例,进行了区块链在公安信息管理领域的探索;陈潮[10]提出了一种公检法证据的区块链储存方案,有效提升了电子证据的可信度。

执法办案档案是记录案件处理过程、证据材料以及执法活动的重要载体,对于确保司法公正、维护社会稳定具有不可替代的作用。不同于具有唯一性和较强的防篡改性的传统纸质档案,基于中心化的数字档案管理系统已广泛应用于执法办案档案管理工作中,其管理、维护及控制权的掌握全部由单一机构执行,因此面临更多网络攻击的风险。本文借鉴上述基于数字档案和区块链的相关研究的基础上,针对中国执法办案档案管理系统中普遍存在的数据安全性和真实性问题,将星际文件系统(Inter Planetary File System,IPFS)[11]融入区块链技术,应用于电子档案的真实性保护,提出一种基于 IPFS+区块链技术的执法办案数据访问控制方案。

1 方案设计

1.1 执法办案档案数据存储设计

公安执法办案档案主要包括行政案件和刑事案件两种。行政案件由于绝大多数是公安机关做出的裁决和决定,因此案卷档案都由公安机关内部保管。刑事案件则分为两种情况,对于案件已经破获,犯罪嫌疑人已经抓获的案件,其卷宗先在公安组卷,随着刑事诉讼的程序,经过公检法,最终在法院归档;对于未破案件,或者嫌疑人尚未抓获的刑事案件,卷宗档案一直在公安机关保管。行政和刑事案件卷宗档案的内容,根据案件的性质、类别、复杂程度的不同,内容条目的繁简程度亦有所不同。以某类刑事案件为例,其执法办案档案见表 1。本文的数据访问控制方案仅以普遍情况为例进行阐述。

表 1 刑事案件办案内容

Table 1 Contents of criminal cases

序号	办案内容	序号	办案内容
1	换押证	17	拘留证
2	移送起诉告知书	18	呈请拘留报告书
3	起诉意见书	19	变更羁押期限通知书
4	呈请侦查终结报告书	20	呈请变更羁押期限报告书
5	逮捕通知书	21	扣押决定书
6	逮捕证	22	扣押物品清单
7	批准逮捕决定书	23	扣押物品报告书
8	提请批准逮捕书	24	呈请延长传唤报告书
9	呈请提请逮捕报告书	25	呈请破案报告书
10	变更羁押期限通知书	26	立案决定书
11	呈请变更羁押期限报告书	27	立案告知书
12	扣押决定书	28	呈请立案报告书
13	扣押物品清单	29	案件特征信息
14	扣押物品报告书	30	受案回执
15	提讯提解证	31	受案登记表
16	拘留通知书	32	接警出警登记表

1.2　数据访问控制架构设计

区块链架构设计如图 1 所示。

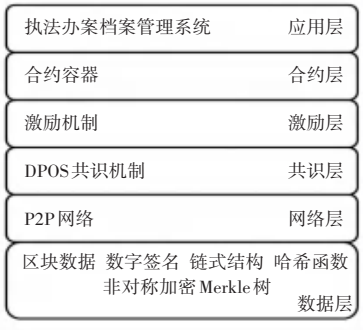

图 1　区块链架构设计图

Fig. 1　Blockchain architecture design

区块链平台整体可划分为网络层、共识层、数据层、激励层、合约层和应用层 6 个层[12]。基于公安内部信息的涉密性和不可泄露性，本方案应用了区块链中的私有链架构形式，具体原理及实现方案将在以下章节中展开阐述。

2　数据访问控制方案实现

2.1　网络层

网络层采用 P2P 半分布式网络。超级节点对普通节点具有很好的管理职能。普通节点为基层公安机关的档案写入部门，超级节点为上层公安机关及监察机构。

如图 2 所示，在应用 P2P[13] 技术来实现分布式网络机制时，结合中心化和分布式模型各自的优点，将节点分类成普通节点和超级节点，从而构成了半分布网络结构。其中，普通节点可以由基层公安机关注册而来，而超级节点即为上级公安机关或有关监察部门注册的节点。每个超级节点维护部分网络节点地址、文件索引等工作，共同实现中心服务器功能。超级节点本身分布式的，可以自由扩展退出，具备分布式网络优点，kazza[14] 是其代表性的成功应用。

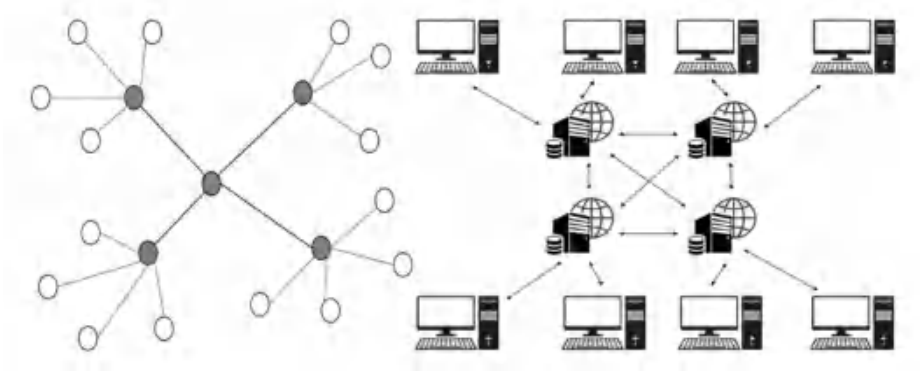

图 2　半分布式网络中的 P2P 传输模式

Fig. 2　P2P transmission mode in a semi-distributed network

2.2　共识层

共识层采用股份授权共识机制（DPOS）[15]，DPOS 是一种基于投票选举的共识算法。如：民主大会，持币人选出几个代表节点来运营网络，用专业运行的网络服务器来保证区块链网络的安全和性能。DPOS 机制中，不需要算力解决数学难题，而是由持币者选出谁是生产者，如果生产者不称职，随时有可能被投票出局，因此解决了 POS 的性能问题。本方案应用 DPOS 共识机制，首先认定每个超级节点为一般节点，即一般节点是从所有的超级节点中选取而来。一般节点类似于有投票权的股东，其既可以参与投票选举董事会成员，同时可以竞争成为董事会成员。这些被大家选举出来的社区中，对方案发展和运行最有利的成员可以被叫做记录节点。记录节点具有一般节点没有的校验和更新区块的功能，既可以高效维护系统的运转，也会贡献自己的能力促进区块链方案的发展。本文在模型中采取 DPOS 共识机制，既达到了去中心化的选举共识，保证了整个系统的运行效率又减少了能源浪费。共识机制部分伪代码如下：

```
// 超级节点结构体
结构体 Trustee：
    字符串 name
    整数 votes
// 选举超级节点
函数 selectTrustee：
    初始化 _trusteeList 为 m 个 Trustee，随机生成票数
    排序 _trusteeList
    result = 取前 n 个元素
    移动 result[0] 到 result 末尾
    返回 _trusteeList
```

2.3 数据层

为了实现数据的不可篡改性,区块链引入了以区块为单位的链式结构,本方案中的比特币区块链中,每个区块由区块头和区块体两部分组成。区块体中以 Merkle 树[16]的形式存放了自前一区块之后发生的多笔交易;区块头中存放了前块哈希(PreBlockHash)、随机数(Nonce)、Merkle 根(Merkle Root)[17]等信息。基于块内交易数据哈希生成的 Merkle 根,实现了块内交易数据的不可篡改性与简单支付验证;基于前一区块内容生成的前块哈希将孤立的区块链接在一起,形成了区块链;时间戳表明了该区块的生成时间。

本方案中,对于底层架构的设计,首先要建立的是一个“创世区块”(该区块链的第一个区块)。在此基础上,每一个区块都存储了前一个区块的 Hash,根据链状结构的性质,可以在创世区块上不断增加新区块。当一个区块中的内容发生篡改时,将引起所有之后区块中内容的改变。

Merkle 树中存储了交易的相关信息,由于本系统是基于比特币区块链的设计,因此 Merkle 树采用二叉树的形式,树上的每个节点都是哈希值,每个叶子节点都对应块内一笔交易数据的 SHA-256 哈希。系统中,“交易”即为普通节点向超级节点中的记录节点发送数字摘要与签名的过程。其中,数字摘要是将档案用 SHA-256 算法求得。在普通节点向记录节点发送信息时,被发送文件先用 SHA 编码加密,产生 128 bit 的数字摘要,然后发送方即普通节点用自己的私用密钥对摘要再加密,由此形成数字签名。普通节点应当将原文和加密的摘要同时传给对方。记录节点在得到信息时,首先需要将该信息广播给全部超级节点,其中包括一般节点。一般节点用发送方的公共密钥对数字签名解密,同时对收到的文件用 SHA 编码加密产生又一摘要,并将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比,如两者一致,则说明传送过程中信息没有被破坏或篡改,否则不然。如此,保证了普通节点和超级节点之间传输信息的准确性。当记录节点收到的一般节点的肯定反馈超过 2/3 时,就可以将信息写入区块。这时,为了验证这个传输过程的完整性,类似简单支付认证(SPV)[18],应用 Merkle 树的原理,不需要验证全部数据,当数据从 A 端传到 B 端时,只需要验证 A、B 端上所构造的 Merkle 树的根节点是否一致即可。若一致,表示数据在传输过程中没有发生改变;反之,说明数据在传输过程中被修改。而且通过 Merkle 树很容易定位找到被篡改的节点。定位的时间复杂度为 $O(\log(n))$。通过该方法,可以得知想要写入的信息是否写入了区块。

```
// Merkle 树结点结构体
结构体 MerkleNode:
    指针 Left
    指针 Right
    字节数组 Data
// 创建 Merkle 树结点
函数 NewMerkleNode(left, right 指针 MerkleNode, data 字节数组) 返回指针 MerkleNode:
    创建空的 MerkleNode mNode
    如果 left 和 right 都是空:
        对 data 进行 sha256 哈希,赋值给 mNode.Data
    否则:
        合并 left.Data 和 right.Data,进行 sha256 哈希,赋值给 mNode.Data
    设置 mNode 的 Left 和 Right
    返回 mNode 的指针
// 构建 Merkle 树
函数 NewMerkleTree(data 二维字节数组) 返回指针 MerkleTree:
    初始化空的节点列表 nodes
如果 data 长度为奇数,复制最后一个元素以确保偶数
    对于每个 dataitem:
        创建新的 MerkleNode,添加到 nodes 列表
    循环 len(data)/2 次:
        初始化 newNodes 列表
        每次循环步长为 2,创建新的 MerkleNode 并添加到 newNodes
        更新 nodes 为 newNodes
    创建 MerkleTree,根节点为 nodes 的第一个元素
    返回 MerkleTree 的指针
```

2.4 激励层

为提高公安人员传送档案的准确性,增加公安工作积极性和协同性,更大程度上减少档案录入错误,本课题提出在公安系统增设代币发放和奖励机制的构想。通过制定相应的奖惩办法,系统将向公安档案人员发放 Token[19]。Token 可以作为公安人员绩效考核的依据。代币的发放和奖惩通过智能合约自动完成,保证公安内部奖惩公开、公正、透明。

为了提高公安人员的工作效率，采用智能合约设置任务完成要求、档案录入要求、完成期限以及相应的令牌奖惩措施。对提前完成工作给予相应的象征性奖励，对不按时完成工作或不符合任务要求的，扣减相应的象征性处罚，激发公安人员的工作活力。智能合约作为区块链的激活器，保证了系统自动执行代币奖惩，大大提高了公平正义的原则。本方案的区块链系统作为一条私有链，没有挖矿需求，Token 的产生可以直接通过智能合约赋予公安账户。公安部门视公安人员工作情况奖惩相应 Token，用作绩效评估、薪资发放的参考依据。

```
// 定义智能合约执行逻辑
函数 executeSmartContract(结构体 contract):
    对于 contract.conditions 中的每个 condition:
        如果 condition 被满足:
            执行 contract.actions // 执行与条件相关的动作
// 定义任务完成处理流程
函数 completeTask(结构体 officer, 结构体 task, 字符串 current_time):
    如果 task.completion_status 是 "已完成":
返回
    如果 current_time 小于等于 task.deadline:
        officer.token_balance 增加 task.reward_tokens // 增加 Token 余额
        记录交易 officer.officer_id, task.task_id, task.reward_tokens // 记录奖励过程
    否则:
        officer.token_balance 减少 task.penalty_tokens // 扣减 Token 余额
        记录交易 officer.officer_id, task.task_id, -task.penalty_tokens // 记录扣减过程
    task.completion_status 设为 "已完成" // 更新任务状态为 "已完成"
// 记录过程
函数 recordTransaction(字符串 officer_id, 字符串 task_id, 整数 amount):
    定义 transaction 为一个新的 TokenTransaction 实例:
        transaction_id 设为 generateUniqueTransactionID()
        officer_id 设为 officer_id
        task_id 设为 task_id
        amount 设为 amount
        timestamp 设为 getCurrentTimestamp()
    保存 transaction // 保存过程记录
函数 generateUniqueTransactionID():
    返回 唯一 ID
函数 getCurrentTimestamp():
    返回 当前时间戳
函数 saveTransaction(结构体 transaction):
    将 transaction 保存到数据库或区块链中
```

2.5　应用层

在应用层中，本方案是基于区块链的执法办案档案管理系统，基层人员记录的电子档案完成后，系统会自动应用 SHA-256 求出数字摘要和数字签名等，然后发送给超级节点进行审核。具体而言，系统提供如下功能应用：

1）基层民警对于档案的自主上传：基层人员根据办案流程，详细上传包含案件的各项信息的档案。

2）档案的自动加密与签名生成：通过 SHA-256 算法计算电子档案的数字摘要（哈希值）确保档案的内容在存储和传输过程中未被篡改。之后，利用公安人员的私钥对生成的数字摘要进行签名，生成该电子档案的数字签名，保证档案的真实性和不可否认性。最后，使用非对称加密算法（如 RSA）进行加密传输。

3）档案的审核与归档：档案加密与签名完成后，系统将加密后的档案发送至超级节点进行审核，如果档案审核通过，超级节点将档案标记为已审核，并将其归档至区块链中。

4）档案的共享与调用：不同执法部门（如刑侦、交警、禁毒等）需要协同处理某些案件时，系统允许相关部门在权限范围内共享档案。相关人员可以通过区块链查询到档案的摘要信息及其签名，确保信息的真实性和一致性。共享时，系统会根据权限控制，对档案的某些敏感内容进行部分遮蔽或加密处理。

私密档案的角色访问权限控制。执法办案档案中，存在一些涉密性极强的档案，只能对公安内部部分人员进行公开，此类档案的数目相对少，因此采取自主访问控制的方法对部分公安人员进行授权：

1）公安人员请求查看机密信息，向上级管理人员发送带证书签名的请求；

2）管理人员验证签名并同意请求，生成一个临时对称密钥对机密信息加密；

3）管理人员用员工的公钥加密对称密钥，并发送给员工；

4)员工用自己的私钥解密出对称密钥;

5)员工用对称密钥解密出机密信息。

3 方案测试

本文不改变现有的较为完善的公安机关执法办案档案系统管理界面,在此基础上实现本文提出的基于区块链的数据访问控制方案,并实现对于档案内容的存储、调用,以及整个过程的留痕记录。实验环境设置见表 2。

由于执法办案档案的涉密性,本文将利用大模型生成虚拟档案进行实验,并模拟在真实办案过程中公安人员上传存储档案的过程。

表 2 实验环境设置

Table 2 Experimental environment setup

名称	版本
操作系统	Win11
pandas	1.5.3
cryptography	3.4.7
bitcoinlib	0.9.0
python	3.10.0
SQLAlchemy	1.4.0
PyNaCl	1.5.0

档案的上传和存储测试结果如图 3 所示。在创世区块基础上,存储两个加密档案 Hash1 和 Hash2 的内容。

图 3 档案上传与存储测试结果图

Fig. 3 File upload and storage test results

共享调用档案及过程留痕。如图 4 所示,模拟了公安人员 admin 给小王传送文件的过程,区块上记录了该传递过程,并以哈希的方式存储。

图 4 档案调用与过程留痕测试结果图

Fig. 4 Diagram of file invocation and process trace test results

4　结束语

互联网技术已经颠覆了整个世界，而如今区块链即将颠覆互联网。区块链技术在各个领域都开始了突破，对于公安领域而言，执法办案档案系统，作为记录案情、警情的重要载体，与区块链的结合将成为必然，并会更快的推进公安信息化、执法公正化的建设。基于比特币区块链执法办案档案系统存在一定的局限性，随着档案数目的增加，会影响该系统的性能，应用“IPFS+区块链”[20]的手段解决这个问题，将执法办案档案存储在同样去中心化的星际文件系统（IPFS）中，在链上只需要保存这些数据的ID[21]，是一种实现节省空间效果的方案。

未来，随着区块链、IPFS 等技术的不断成熟与应用的深入拓展可以预见，将会有更多高效、安全的数据访问控制方案和去中心化存储系统被应用于公安执法办案档案管理中。这些新技术将进一步提升公安机关的执法效能，加强数据的安全性和隐私保护，为构建更加公正、透明、高效的执法环境提供有力支持。

参考文献

[1] 肖敏. 大数据环境下档案利用服务体系建设研究[D]. 湘潭：湘潭大学，2015.

[2] 游姗姗. 基于云计算的福建省数字档案馆信息服务研究[D]. 福州：福建农林大学，2016.

[3] 刘悦，张翔宇，张月. 基于 NAS 的数字档案存储管理与实践研究[J]. 中国口岸科学技术，2021，463(2)：58-63.

[4] 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.

[5] 林雅榕，侯整风. 对哈希算法 SHA-1 的分析和改进[J]. 计算机技术与发展，2006(3)：124-126.

[6] 李晓光，石丹. 蚂蚁金服的区块链野望[J]. 商学院，2020，178(1)：65-67.

[7] 李康震，张翔. 区块链技术在公安情报工作中的应用研究[J]. 贵州警官职业学院学报，2018，30(5)：42-51.

[8] 陈学凡. 区块链技术应用于公安工作的思考与探讨[J]. 警察技术，2018(3)：53-56.

[9] 熊建英. 区块链技术在公安信息管理中的应用探索——以设计一种公民信息管理模型为例[J]. 江西警察学院学报，2018，213(6)：120-124.

[10] 陈潮. 基于区块链的公检法电子证据存证模型研究[J]. 智能计算机与应用，2023，13(6)：103-107.

[11] 孙知信，张鑫，相峰，等. 区块链存储可扩展性研究进展[J]. 软件学报，2021，32(1)：1-20.

[12] 林知微，张嵩川，王成吉，等. 区块链技术综述：在下一代智能制造中的应用[J]. 智能科学与技术学报，2023，5(2)：200-211.

[13] 岳昆，王晓玲，周傲英. Web 服务核心支撑技术：研究综述[J]. 软件学报，2004(3)：428-442.

[14] 徐伟荣. P2P 网络中的著作权问题探讨[D]. 南京：南京师范大学，2008.

[15] 刘艺华，陈康. 区块链共识机制新进展[J]. 计算机应用研究，2020，37(S2)：6-11.

[16] 吴梦宇，朱国胜，吴善超. 基于 Merkle 树的区块链数据修改方法研究[J]. 信息通信，2020，214(10)：10-12.

[17] 黄根，邹一波，徐云. 区块链中 Merkle 树性能研究[J]. 计算机系统应用，2020，29(9)：237-243.

[18] 刘燕，楼建波. 企业并购中的资管计划——以 SPV 为中心的法律分析框架[J]. 清华法学，2016，10(6)：63-83.

[19] 李传艺，葛季栋，胡海洋，等. 一种基于 Token Log 的符合性检查方法[J]. 软件学报，2015，26(3)：509-532.

[20] 崔家旺. 基于区块链与 IPFS 的隐私访问应用研究[D]. 武汉：武汉轻工大学，2023.

[21] 朱亚丽，许鸣睿，丰茂智，等. 基于区块链和 IPFS 的存储机制设计[J]. 无线互联科技，2024，21(1)：82-87.