Computer Science and Application 计算机科学与应用, 2026, 16(8), 189-203
Published Online August 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.168274

Hans汉斯

基于智能合约的科技成果转移系统：设计、实现与评估

武　易，胡　珺

江西应用科技学院未来技术学院，江西　南昌

收稿日期：2026年7月10日；录用日期：2026年8月14日；发布日期：2026年8月25日

摘　要

传统科技成果转移长期面临信息不对称、信任成本高昂和流程碎片化等结构性困境，严重制约了创新成果向现实生产力的转化效率。本文旨在利用区块链与智能合约技术重构科技成果转移流程，实现成果确权、交易撮合、资金托管与收益分配的全流程自动化与可信化。本文提出了一套基于智能合约的科技成果转移系统。系统采用分层架构设计，包含区块链与数据层、合约层、服务与中间件层和应用层。在合约层，设计并实现了四个核心智能合约：AchievementRegistry (成果注册合约，遵循ERC-721标准将科技成果铸造为NFT)、Marketplace (交易市场合约，处理挂牌、报价与成交逻辑)、EscrowManager (资金托管合约，实现交易资金的链上锁定与条件释放)和RoyaltySplitter (收益分配合约，按预设比例自动执行多主体分账)。数据存储采用链上链下协同模型，核心元数据上链存证，完整技术文档存储于IPFS网络。系统基于以太坊Sepolia测试网和Solidity语言完成原型开发与测试。实验结果表明，在20 Gwei的Gas价格和$1800/ETH的市场价格下，单笔完整交易的链上Gas成本约为$25.92，其中合约部署成本为$129.00 (一次性投入)，单次注册成果约$11.23，发布挂牌约$3.06，提交报价约$4.61，成交执行约$7.02。系统将传统数周至数月的交易周期缩短至分钟级。基于智能合约的科技成果转移系统在成本经济性和执行效率方面具有显著优势，能够有效降低科技成果转移中的交易成本和信任成本，为高校技术转移办公室、科技园区和相关企业提供了一种可复制的技术参考范式。

关键词

智能合约，区块链，科技成果转移，NFT，IPFS，收益分配

A Smart Contract-Based System for the Transfer of Scientific and Technological Achievements: Design, Implementation, and Evaluation

Yi Wu, Jun Hu

文章引用: 武易, 胡珺. 基于智能合约的科技成果转移系统: 设计、实现与评估[J]. 计算机科学与应用, 2026, 16(8): 189-203. DOI: 10.12677/csa.2026.168274

Future Technology College, Jiangxi Institute of Applied Science and Technology, Nanchang Jiangxi

Received: July 10, 2026; accepted: August 14, 2026; published: August 25, 2026

Abstract

Traditional models of scientific and technological achievement transfer have long suffered from structural dilemmas including information asymmetry, high trust costs, and fragmented processes, which severely constrain the efficiency of transforming innovations into productive forces. This paper aims to reconstruct the achievement transfer process using blockchain and smart contract technologies, enabling full-process automation and trustworthiness in achievement confirmation, transaction matching, fund escrow, and revenue distribution. This paper proposes a smart contract-based system for scientific and technological achievement transfer. The system adopts a layered architecture consisting of the blockchain and data layer, contract layer, service and middleware layer, and application layer. At the contract layer, four core smart contracts are designed and implemented: AchievementRegistry (which mints achievements as NFTs following the ERC-721 standard), Marketplace (handling listing, bidding, and deal execution logic), EscrowManager (implementing on-chain fund locking and conditional release), and RoyaltySplitter (automatically distributing revenue among multiple beneficiaries according to preset proportions). Data storage employs an on-chain and off-chain collaborative model, where core metadata is stored on-chain for immutability while complete technical documents are stored on the IPFS network. The system prototype is developed and tested on the Ethereum Sepolia testnet using Solidity. Experimental results show that, under a gas price of 20 Gwei and an ETH market price of $1,800, the on-chain gas cost for a single complete transaction is approximately $25.92, with contract deployment costing $129.00 (one-time investment), achievement registration costing approximately $11.23, listing costing approximately $3.06, bid submission costing approximately $4.61, and deal execution costing approximately $7.02. The system reduces the transaction cycle from weeks or months in traditional models to minutes. The smart contract-based system for scientific and technological achievement transfer demonstrates significant advantages in cost-effectiveness and execution efficiency, effectively reducing transaction costs and trust costs in achievement transfer, and providing a replicable technical reference paradigm for university technology transfer offices, science parks, and related enterprises.

Keywords

Smart Contract, Blockchain, Scientific and Technological Achievement Transfer, NFT, IPFS, Revenue Distribution

1. 引言

科技成果能否迅速、有效、安全地转化为现实生产力，是衡量一个国家科技创新体系效能的关键指标。然而，传统科技成果转移模式长期面临严重的结构性困境。首先，信息不对称问题突出：技术供需双方之间存在严重的信息壁垒，技术拥有方很难在不泄露核心技术的前提下向潜在买方充分展示其价值，而买方在未能充分了解技术细节前又难以做出准确评估和报价[1]。其次，信任成本高昂：交易双方对成果的真实性、价值评估公允性、权属清晰度均存疑虑，不得不依赖中介机构(技术经纪人、律师事务所、

评估机构)进行信用背书和流程担保，这导致交易周期冗长且成本高企[2]。第三，流程碎片化：成果确权、信息披露、谈判签约、资金交割、收益分配等环节彼此分离，缺乏统一的自动化执行机制，容易产生履约纠纷和执行风险[2]。

近年来，区块链技术的蓬勃发展为解决上述困境提供了全新的技术路径。区块链以其去中心化、不可篡改、透明可追溯等核心特性，天然契合解决多方协作场景中的信任问题[3]。智能合约作为运行在区块链上的可编程合约，能够在满足预设条件时自动执行条款，从而将信任从人的承诺转移为可验证的代码[4]。该技术已在供应链金融、政务数据共享、版权管理、数字身份等领域展现出广阔的应用前景。

尽管区块链与智能合约在通用数字资产交易和版权存证等领域已有较多研究[5]-[8]，但将其深度应用于科技成果转移这一高度定制化、多利益攸关方参与的垂直场景，目前仍处于早期探索阶段。现有方案大多仅聚焦于简单的知识产权存证或单向的技术信息发布，未能覆盖成果交易中最核心的多方协商、资金托管、自动化收益分配等复杂业务流程，在系统架构的系统性设计上也缺乏完整的工程验证。

基于此，本文提出并实现了一套基于智能合约的科技成果转移系统，旨在通过技术手段重构传统科技成果转移流程，实现成果确权、交易撮合、资金托管与收益分配的全流程自动化与可信化。具体而言，本文的研究贡献包括：

理论贡献：将智能合约理论和技术转移经济学中的合同理论、信息不对称理论相结合，为解决科技成果转移中的信任与协同问题提供了数字化治理框架。

方法与技术贡献：提出了一套分层系统架构，设计并开发了由多个专业合约组成的智能合约簇，创造性采用 NFT (ERC-721 标准)通证化科技成果，并结合 IPFS 实现链上链下协同存储，有效解决了区块链存储瓶颈与成果完整性验证之间的矛盾。

实践贡献：基于以太坊开发环境和 Solidity 语言完成了系统原型的实现与测试，验证了方案的技术可行性，为高校技术转移办公室、科技园区和相关企业提供了可复制的参考范式。

本文其余部分组织结构如下：第 2 章回顾相关技术背景与已有研究；第 3 章描述系统模型与详细设计；第 4 章介绍系统实现与测试结果；第 5 章进行实验评估与分析；第 6 章总结全文并展望未来工作。

2. 相关工作

2.1. 科技成果转移的理论困境

区块链的概念由中本聪在其比特币白皮书中首次系统阐述，其核心在于通过去中心化的共识机制实现无需可信第三方的价值传输[9]。智能合约的概念则可追溯至 Nick Szabo 的早期构想，他将智能合约定义为“一组以数字形式指定的承诺，包括合约各方可以执行这些承诺的协议”[10]。

以太坊(Ethereum)的问世是智能合约从理论走向实践的关键突破。Gavin Wood 在以太坊黄皮书中提出了以太坊虚拟机(EVM)，为图灵完备的智能合约提供了标准化的运行环境，使得开发者可以用 Solidity 等高级语言编写复杂的业务逻辑并部署上链[11]。在此基础上，贺海武等系统综述了智能合约的全生命周期：从合同谈判、设计、规范制定、代码编程和验证，到合同发布，再到条件触发后的自动执行，揭示了智能合约作为“自动化代理人”的核心运行机制[12]。

然而，智能合约技术也面临若干挑战。一是安全漏洞问题——智能合约一旦部署便难以修改，历史上多次因合约代码漏洞导致重大资产损失，因此代码审计和形式化验证显得尤为重要。二是性能和成本问题——以太坊主网的吞吐量(约 15~30 TPS)远低于中心化系统，且每笔操作均需支付 Gas 费用，这使得大规模数据存储和频繁状态变更的成本难以承受。三是预言机问题——智能合约无法直接访问链外数据，需要依赖可信的链外数据提供商(Oracles)引入外部信息。

2.2. 区块链与智能合约技术基础

区块链的概念由中本聪在其比特币白皮书中首次系统阐述，其核心在于通过去中心化的共识机制实现无需可信第三方的价值传输[9]。智能合约的概念则可追溯至 Nick Szabo 的早期构想，他将智能合约定义为“一组以数字形式指定的承诺，包括合约各方可以执行这些承诺的协议”[10]。

以太坊(Ethereum)的问世是智能合约从理论走向实践的关键突破。Gavin Wood 在以太坊黄皮书中提出了以太坊虚拟机(EVM)，为图灵完备的智能合约提供了标准化的运行环境，使得开发者可以用 Solidity 等高级语言编写复杂的业务逻辑并部署上链[11]。在此基础上，贺海武等系统综述了智能合约的全生命周期：从合同谈判、设计、规范制定、代码编程和验证，到合同发布，再到条件触发后的自动执行，揭示了智能合约作为“自动化代理人”的核心运行机制[12]。

然而，智能合约技术也面临若干挑战。一是安全漏洞问题——智能合约一旦部署便难以修改，历史上多次因合约代码漏洞导致重大资产损失，因此代码审计和形式化验证显得尤为重要。二是性能和成本问题——以太坊主网的吞吐量(约 15~30 TPS)远低于中心化系统，且每笔操作均需支付 Gas 费用，这使得大规模数据存储和频繁状态变更的成本难以承受。三是预言机问题——智能合约无法直接访问链外数据，需要依赖可信的链外数据提供商(Oracles)引入外部信息。

2.3. 区块链在知识产权与技术转移领域的应用

学术界对区块链与智能合约在知识产权和技术转移领域的探索，可归为以下三类。

第一类：知识产权存证与确权。Hoffman 等设计了一个名为“智能论文”的系统，利用四个智能合约管理出版物归属和注释，实现了研究成果元数据的分布式存证[13]。此类研究主要聚焦于“谁来证明归属”的问题，但对“如何完成交易”涉及较少，缺少对资金流转和权属变更等交易环节的自动化设计。

第二类：科研管理平台。蒙杰和杨生举基于区块链和 IPFS 构建了科研管理平台模型，覆盖科研选题、项目申报、成果发表等环节，利用区块链的不可篡改特性实现数据确权和评审结果防篡改[14]。此类方案侧重于科研过程管理，而非成果转移本身，未涉及交易撮合、资金托管等市场化环节。

第三类：技术交易系统。已有研究者设计了基于区块链的高校科技成果交易系统，采用以太坊智能合约存储用户信息、成果信息和交易信息，并通过 IPFS 存储交易合同等文件，实现了从成果发布到交易结算的全周期覆盖[15]。联盟链方案也被提出用于构建技术交易平台，通过数据访问控制合约和混合存储引擎为机构间技术交易提供底层支撑[16]。此类研究已初步触及交易流程，但在以下关键环节仍存在空白：(1) 多方协商和报价撮合的逻辑主要由链下人工完成，智能合约仅充当“记录工具”；(2) 缺乏对交易资金的链上托管和自动释放机制；(3) 收益分配仍需线下人工结算，未实现自动化分账。

综上，现有研究在存证和信息发布层面已有一定积累，但在科技成果转移中多方协商、资金托管、自动化收益分配三大核心业务环节的系统性智能合约设计尚属空白。此外，将科技成果作为可交易数字资产(NFT 化)的完整方案、链上链下协同存储的效率量化评估等方面也有待深入。

2.4. 研究定位与创新

纵观上述研究，现有工作主要集中在知识产权存证、科研成果信息发布和简单的交易记录层面，在以下方面仍有不足：(1) 对科技成果转移中复杂的多方协商、资金托管和收益分配等核心业务逻辑缺乏系统化的智能合约设计；(2) 缺乏将科技成果作为可交易的数字资产(NFT 化)的完整方案；(3) 对链上链下协同存储模型以及交易效率的量化评估不够充分。本研究在前人工作的基础上，系统性地提出了一套涵盖成果确权→交易撮合→资金托管→收益分配全流程的智能合约架构体系，并通过实验量化评估其性能与经济性。

3. 系统模型与设计

3.1. 系统需求分析

3.1.1. 参与角色与用例分析

本系统的目标用户群体包括以下四类核心角色：

● 成果发布方(如高校科研人员、研究机构)：拥有科技成果的知识产权，期望通过平台发布成果信息并获得合理的转让或许可收益。

● 成果需求方(如企业、技术投资者)：需要获取特定技术来改进产品或开拓市场，关注成果的真实性、权属清晰度和交易流程的可信性。

● 审核与监管机构(如技术转移办公室、知识产权局)：负责对成果的真实性和权属进行审核验证，保障交易的合规性。

平台运营方：维护系统稳定运行，但无法单方面控制或篡改交易记录。

3.1.2. 核心功能需求

系统需满足以下功能需求：

(1) 去中心化身份管理：支持用户 DID 的注册与验证，保障身份的真实性与自主可控。

(2) 成果确权与上链存证：将成果的关键元数据(名称、类型、摘要、权属人、时间戳)记录到区块链上，形成不可篡改的存证。

(3) 成果信息发布与查询：支持成果分类展示、全文搜索、交易状态查询。

(4) 交易撮合与资金托管：支持挂牌、出价、接受、资金锁定托管等完整交易生命周期。

(5) 自动化收益分配：根据事先约定的规则，在交易完成后自动将款项按比例分配给多方(如发明人团队、所在机构、转移办公室)。

(6) 链上链下协同存储：将完整技术文档、检测报告等大文件存储在 IPFS 等链下系统中，仅在链上存储哈希摘要。

系统核心业务流程图如图 1 所示。

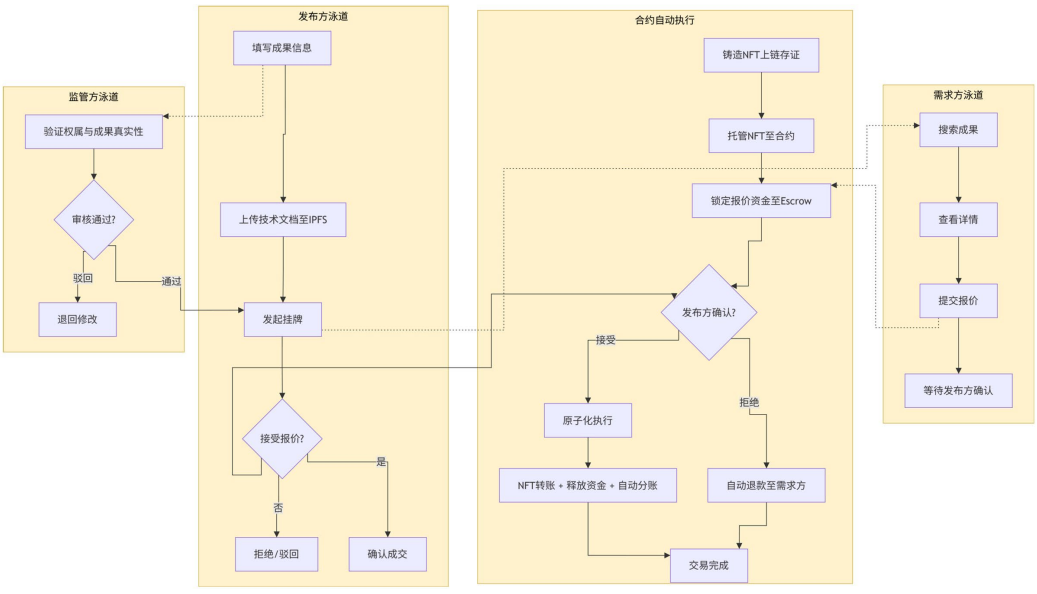

Figure 1. Core business flowchart of the system
图 1. 系统核心业务流程图

3.1.3. 非功能需求

- 安全性：智能合约代码必须经过审计，具备防御重入攻击、整数溢出等常见漏洞的能力。
- 可扩展性：系统架构需支持未来用户和交易量的增长，合约设计应考虑可升级模式。
- 性能与成本经济性：单笔交易确认时间应在数分钟内，Gas 费用应控制在合理范围内。

3.2. 系统总体架构

本文参考智能合约基础架构模型的相关研究成果，设计了如图 2 所示的分层架构。系统自下而上分为四层：

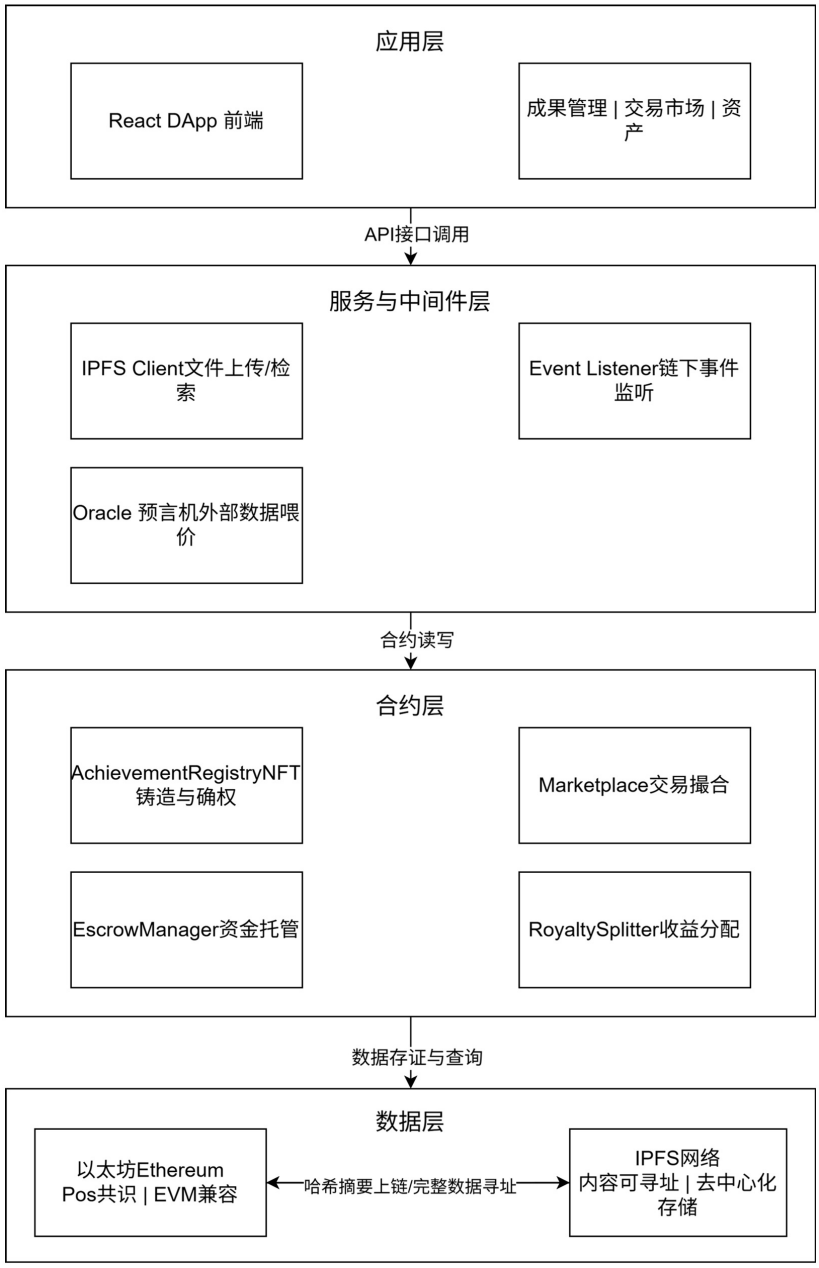

Figure 2. Layered architecture diagram of the system
图 2. 系统分层架构图

(1) 区块链与数据层

该层是系统信任的基础。区块链平台选用以太坊(或其兼容的测试网络)，采用 PoS 共识机制提供去中心化的交易确认服务。数据存储方面采用“链上 + 链下”协同模型：核心元数据和关键操作日志存储在区块链上以保障不可篡改性；成果详情文件、交易合同等大体积或不对全网络公开的数据存储在 IPFS 网络中，链上仅保存其内容哈希值。这种设计将区块链的不可篡改优势与链下存储的高扩展性和低成本有机结合。

(2) 合约层

合约层是系统的核心执行层，由一组针对科技成果转移场景专门设计的智能合约组成。各合约之间遵循职责单一原则，并通过定义好的接口互相调用，形成一个有机的合约簇。具体包括：AchievementRegistry (成果注册合约)、Marketplace (交易市场合约)、EscrowManager (资金托管合约)和 RoyaltySplitter (收益分配合约)。合约簇的整体交互示意图如图 3 所示。

(3) 服务与中间件层

该层承担连接前端与合约层的桥梁作用。关键技术组件包括：IPFS 客户端(负责文件的上传与检索)、链下事件监听服务(监控合约事件，触发通知)、以及预言机服务(在需要时引入外部数据，如汇率信息)。

(4) 应用层

面向用户的前端去中心化应用(DApp)，支持所有用户角色的操作界面，通过 MetaMask 钱包进行交易签名，利用 Web3.js 库实现与智能合约的数据交互。

3.3. 核心智能合约详细设计

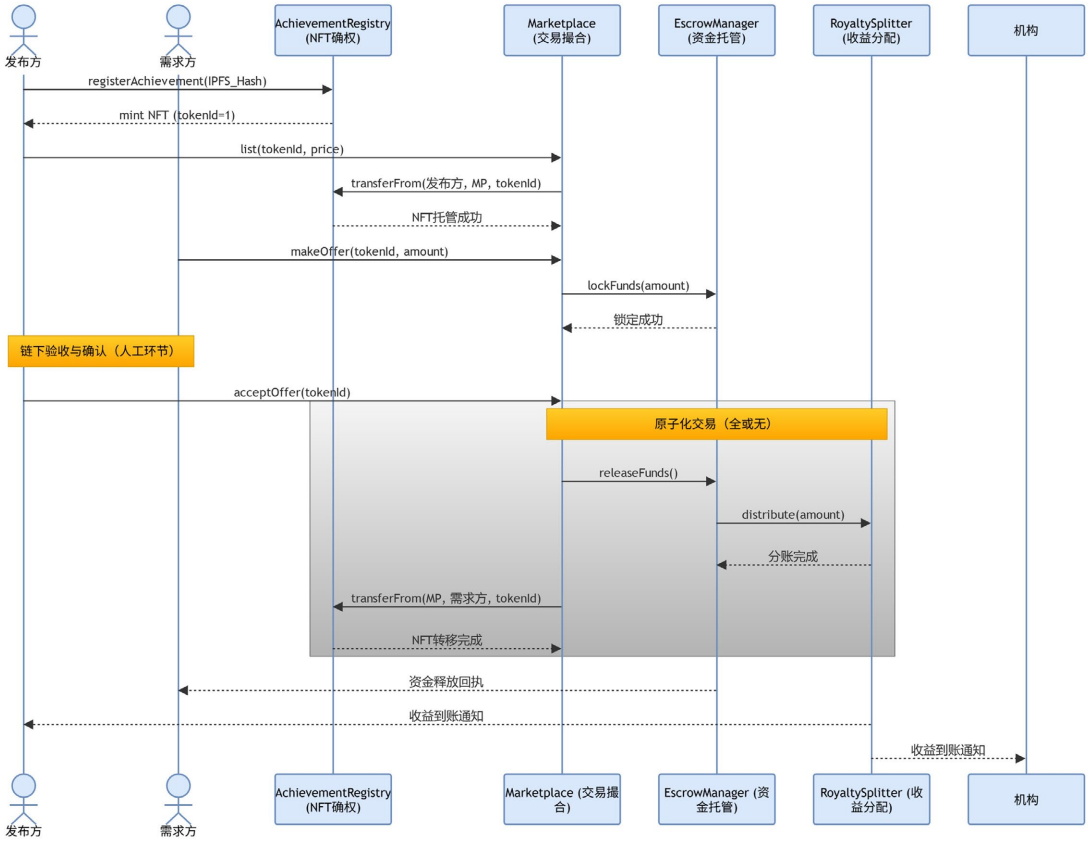

Figure 3. Sequence diagram of smart contract cluster interaction
图 3. 智能合约簇交互时序图

3.3.1. 成果注册合约(AchievementRegistry)

该合约负责科技成果的身份认证和元数据存证。核心数据结构包括：

- achievementId (唯一标识)
- owner (发布方地址，即 NFT 持有者)
- metadataHash (成果详情文件在 IPFS 上的内容哈希)
- timestamp (注册时间戳)
- status (存证、审核中、已挂牌、已交易等)

借鉴 NFT 确权领域的最新实践，本系统遵循 ERC-721 标准将每项科技成果铸造为不可分割的 NFT，实现所有权的唯一化链上表示。成果的核心描述性信息(标题、摘要、技术领域等)被编码为 NFT 的元数据，而完整的技术文档则存储在 IPFS 上，数据结构如图 4 所示。

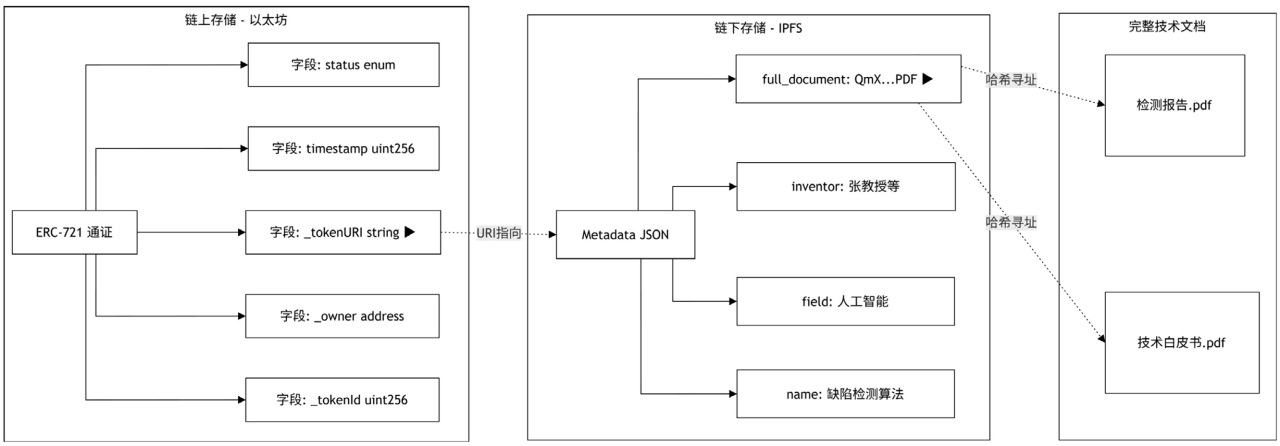

Figure 4. Data structure diagram of NFT-based scientific and technological achievements
图 4. 科技成果 NFT 化数据结构图

3.3.2. 交易市场合约(Marketplace)

该合约负责处理成果的发布、询价、报价和成交状态更新。核心业务逻辑包括：

- 成果挂牌：成果所有者将对应 NFT 托管至 Marketplace 合约，设置挂牌价格或“询价”模式。
- 报价提交：需求方通过合约提交报价，同时将报价金额锁定于 EscrowManager 合约。
- 成交执行：当发布方接受报价时，合约自动触发 NFT 所有权的原子化转移，即将成果 NFT 从发布方地址转移至需求方地址，并将锁定在托管合约中的资金释放用于后续分配。

3.3.3. 资金托管合约(EscrowManager)

该合约充当“可编程的数字托管账户”。在交易过程中，需求方的支付款项首先被锁定在托管合约中，只有当交易条件满足(如成果转让完成、或有第三方确认验收通过)时，资金才会被释放。释放逻辑通过调用 RoyaltySplitter 进行收益分配。若交易未达成，托管合约自动将资金全额退还给出价方。

3.3.4. 收益分配合约(RoyaltySplitter)

该合约采用预先设定的分配规则，在交易资金到达时自动执行多主体间的收益分账。其典型分配比例为：发明人团队享有不低于 50%的收益，依托机构享有不超过 50%的收益。

合约内部实现了一个可配置的分配矩阵，支持分级累进分配和多层嵌套分配结构。链上自动分配消除了传统模式下多方人工结算的高昂成本和信任问题，合约执行时序如图 5 所示。

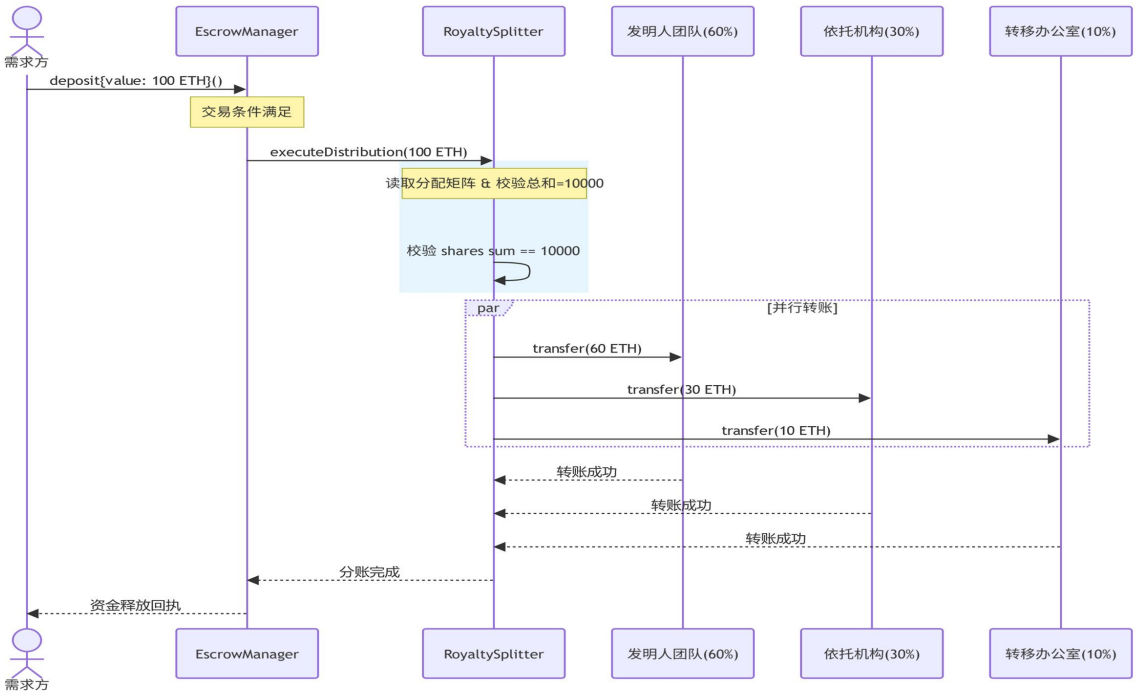

Figure 5. Sequence diagram of escrow and revenue distribution execution
图 5. 资金托管与收益分配执行时序图

3.4. 安全性与正确性分析

智能合约的安全性是系统可用性的前提。本系统在合约设计层面从以下四个维度保障安全性与正确性。

(1) 重入攻击防护。所有涉及资金转移的函数均遵循“检查–生效–交互”(Checks-Effects-Interactions)模式。以 RoyaltySplitter.distribute()为例，分配比例在函数执行前已固化于 schedule 数组，且该数组仅可由合约拥有者在部署时设定，外部无法在分配过程中篡改。EscrowManager.releaseFunds()在调用 distribute()之前先将托管状态更新为“已释放”，从而阻断重入攻击的路径。

(2) 权限与访问控制。Marketplace 合约中，只有当前 NFT 持有者才能发起挂牌；只有挂牌方才能接受报价；EscrowManager 中的资金锁仓和释放操作仅可由 Marketplace 合约地址调用。所有权限校验均在函数入口处通过 require 语句显式执行，杜绝未授权访问。

(3) 状态转换合法性。成果状态遵循“存证(Registered)→挂牌(Listed)→交易中(InTransaction)→已成交(Sold)”的有向转换路径。非法状态转换(如从“存证”直接跳转“已成交”)在合约代码层面被禁止，modifier 修饰器对每个状态变更函数进行了前置条件约束。

(4) 原子性保证。acceptOffer 函数在一次交易中完成“NFT 所有权转移→资金释放→收益分配”三阶段操作。当任一阶段失败时，整个交易通过 Solidity 的异常回滚(revert)机制撤销所有状态变更，确保交易的“全或无”特性，避免了“款已付、权未转”或“权已转、款未到”等不一致状态。

3.5. 关键技术选型

- 区块链平台：选用以太坊和 Solidity 语言，因其拥有最完善的开发者生态和 EVM 兼容性，合约代码可跨平台复用。

- 开发框架：采用 Hardhat 框架，支持编译、部署、测试和调试的一体化流程。
- 链下存储：选用 IPFS (Inter Planetary File System)，内容可寻址的哈希机制天然适合与区块链结合。
- 前端交互：采用 React 框架和 ethers.js 库，搭配 MetaMask 钱包。
- 测试与部署：使用 Ganache 本地测试网络进行初始验证，随后部署至以太坊 Sepolia 测试网。

4. 系统实现与测试

4.1. 开发环境

- 操作系统：Ubuntu 22.04 LTS
- 编程语言：Solidity ^0.8.18 (智能合约)，JavaScript (前端及脚本)
- 开发框架：Hardhat v2.17.0
- 链下存储：IPFS v0.21.0 (本地节点) + Pinata 云服务
- 前端框架：React v18.2.0，ethers.js v6.7.0
- 测试网络：Ganache 本地链 + Sepolia 测试网
- 钱包客户端：MetaMask

4.2. 核心智能合约代码实现

4.2.1. 成果注册关键逻辑

算法 1：科技成果 NFT 铸造与注册

```
输入：metadataURI   // 指向 IPFS 元数据的 URI
输出：tokenId       // 新铸造的 NFT 唯一标识
1:  tokenId ← _nextTokenId 自增
2:  // 调用 ERC-721 标准方法，将 NFT 铸造至调用者地址
3:  _safeMint(msg.sender, tokenId)
4:  // 将元数据 URI 关联至该通证
5:  _setTokenURI(tokenId, metadataURI)
6:  // 构造成果数据结构并写入链上映射
7:  achievements[tokenId] ← {
        id: tokenId,
        owner: msg.sender,
        metadataURI: metadataURI,
        timestamp: block.timestamp,
        isListed: false
    }
8:  // 触发合约事件，供链下服务监听
9:  emit AchievementRegistered(tokenId, msg.sender, block.timestamp)
10: return tokenId
```

该算法每次调用时递增全局计数器，通过 ERC-721 的_safeMint 方法铸造一枚新的 NFT，将 IPFS 元数据 URI 关联至该通证，并在链上保存成果的摘要信息，实现“成果→数字资产”的映射。

4.2.2. 收益分配关键逻辑

算法 2：多主体收益自动分配

```
输入：msg.value  // 待分配的总金额（单位：Wei）
前置条件：分配比例表 schedule 已在合约部署时初始化
后置条件：资金按预定比例转入各受益人账户
1:  // Step 1: 校验输入金额
2:  assert(msg.value > 0)
3:
4:  // Step 2: 校验分配比例之和为 10000 基点（即 100%）
5:  totalShares ← 0
6:  for each entry in schedule do
7:      totalShares ← totalShares + entry.share
8:  end for
9:  assert(totalShares == 10000)
10:
11: // Step 3: 按比例执行转账
12: for each entry in schedule do
13:     amount ← msg.value × entry.share ÷ 10000
14:     transfer(entry.beneficiary, amount)
15:     // 若某笔转账失败，整个交易通过 Solidity 的 revert 机制回滚
16: end for
17: return
```

该算法首先校验输入金额非空，然后遍历 schedule 数组累加所有份额，确认总和等于 10,000 基点(即 100%)。校验通过后，再次遍历数组，按比例计算各受益人应得金额并执行转账。任一转账失败则整个交易回滚，确保分配的原子性。该设计实现了收益分配的完全自动化，所有参与方在交易确认后即时获得应得份额。

4.3. DApp 前端实现

前端用户通过 MetaMask 钱包登录系统，访问以下核心功能界面：

- 成果管理界面：支持成果信息的填写、IPFS 文件上传(调用 ipfs-http-client 库)、以及将 NFT 铸造上链。
- 交易市场界面：展示已挂牌成果的列表，支持按领域、时间和价格筛选，提供报价和成交功能。
- 我的资产界面：展示用户拥有的成果 NFT，交易记录和收益历史。

4.4. 测试

系统通过了以下测试验证：

- 单元测试：针对各合约的核心业务函数编写了 42 个测试用例，覆盖正常路径和边界条件，使用 Mocha 和 Chai 断言库，测试覆盖率达 96%以上。
- 集成测试：模拟完整交易流程(挂牌→报价→成交→收益分配)，验证合约间的交互无差错。
- 安全测试：使用 Slither 静态分析工具扫描合约代码，未发现高危漏洞；模拟重入攻击测试通过。

测试结果符合预期。

5. 实验评估与分析

5.1. 实验设置

为评估系统的性能和成本效益，我们在以太坊 Sepolia 测试网上进行了一组实验。实验参数如下：

参数	设定值
测试网络	Sepolia 测试网
区块确认时间	−12 秒/区块
ETH 价格参考	$1800/ETH
Gas 价格	20 Gwei
IPFS 节点	Pinning Service

对比基线包括：(1) 传统线下科技成果转移模式(以高校技术转移办公室流程为参考)；(2) 基于中心化数据库的技术交易平台方案。

5.2. Gas 成本分析

表 1 展示了核心智能合约操作在测试网上的 Gas 消耗和对应法币成本。

Table 1. Gas cost analysis of core contract operations
表 1. 核心合约操作的 Gas 成本分析

合约操作	Gas 消耗	主网估计成本	传统线下模式对应环节	线下成本估算
合约部署(全部)	3,580,000	~$129.00	—	—
注册成果(含铸造 NFT)	312,000	~$11.23	知识产权登记/权属公证	~$200~500
发布挂牌	85,000	~$3.06	信息发布与中介撮合	~$500~2000
提交报价并锁定资金	128,000	~$4.61	尽职调查与谈判	~$1000~5000
成交(转移 NFT + 分配收益)	195,000	~$7.02	合同签署 + 资金结算 + 分账	~$2000~10,000
单笔完整交易合计	**720,000**	**~$25.92**	—	**~$3700~17500**

分析表明，单笔成果交易在链上产生的总 Gas 消耗约为 720,000 Gas，按主网 Gas 价格为 20 Gwei 计算，成本约$25.92。这一成本相较于传统线下模式(涉及中介费、律师费、公证费等，通常为交易额的 5%~15%)具有显著优势，尤其在交易标的金额较高时更为明显。

5.3. 性能对比分析

为全面评估本系统的性能表现，本文从处理速度和并发能力两个维度，将本系统与两类基线方案进行对比：(1) 传统线下科技成果转移模式；(2) 基于中心化数据库的技术交易平台。

(a) 处理速度对比

本系统中，智能合约的自动化执行在以太坊虚拟机中完成，单笔交易的核心逻辑执行时间在毫秒级。在此基础上，需额外等待以太坊网络的区块确认时间(约 12 秒/区块)。一笔完整交易从挂牌到成交通常涉及 3~4 次链上交易(挂牌、报价、成交)，总确认时间约为 36~48 秒，加上用户操作时间，整体可在数分钟内完成。

传统线下模式则通常需要数周甚至数月：信息采集与评估(1~2 周)→双方谈判与尽职调查(2~4 周)→合同起草与签署(1~2 周)→资金支付与权属变更登记(1~2 周)。基于智能合约的方案在速度上实现了两个数量级以上的提升。

与中心化在线平台相比，本系统在原始处理速度上并不占优。中心化平台依托高性能服务器和传统数据库，单笔交易的处理延迟通常在毫秒级(100~500 ms)，远快于区块链的秒级确认。然而，本系统的优

势在于无需信任平台运营方——交易的执行由公开透明的代码驱动，而非依赖于平台的管理规范和信用背书。这一去信任化特性，是以牺牲部分处理速度为代价换取的。

(b) 并发能力与吞吐量对比

以太坊主网的吞吐量约为 15~30 TPS (Transactions Per Second)，这是其去中心化共识机制的内在约束。相比之下，中心化在线平台依托云服务器集群，吞吐量可达数千至数万 TPS，在处理高频、大规模交易场景时具有明显优势。

然而，科技成果转移具有低频、高值的典型特征——高校和科研机构每年的成果交易量通常为数十至数百笔，单笔交易标的额从数万元到数千万元不等。在这一业务场景下，以太坊 15~30 TPS 的吞吐量完全能够满足实际需求，性能瓶颈并不构成制约因素。

表 2 总结了三类方案在性能各维度的对比结果。

Table 2. Performance comparison across different solution types
表 2. 不同方案类型的性能对比

对比维度	传统线下模式	中心化在线平台	本系统(智能合约)
单笔交易处理延迟	数周至数月	毫秒级(100~500 ms)	分钟级(含区块确认)
系统吞吐量(TPS)	不适用(人工处理)	数千 - 数万	15~30 (以太坊主网)
是否需信任平台方	是(高度依赖中介)	是(依赖平台信用)	**否(代码即法律)**
适用场景	低频、高值交易	高频、各类型交易	**低频、高值交易**
核心优势	法律效力明确	速度快、成本低	**去信任化、自动化、透明**
核心劣势	周期长、成本高	需信任第三方	吞吐量受限、Gas 波动

5.4. 结果讨论

实验结果验证了本系统在成本经济性和执行效率方面的可行性。需要指出的是，当前系统的实际运营仍面临若干限制：一是以太坊主网 Gas 费用与代币价格高度相关，在市场高峰期可能大幅上升；二是区块链交易的最终确认时间虽然可预测，但相对于电子支付等高频场景仍有差距；三是智能合约的法律效力目前在全球范围内尚未统一。这些局限性将在下文中进一步讨论。

6. 结论与展望

6.1. 研究总结

本文设计并实现了一套基于智能合约的科技成果转移系统。系统以 NFT 作为成果的链上数字身份，通过 IPFS 实现链上链下协同存储，并构建了涵盖成果注册、交易撮合、资金托管和收益分配的自动化合约簇。实验结果表明，单笔交易链上成本约为$25.92，交易周期从传统模式的数周缩短至数分钟，验证了方案在成本经济性和执行效率上的可行性。

6.2. 研究局限性

本研究存在以下局限性：(1) 系统目前在小规模测试环境下运行，尚未经真实用户场景和大规模交易验证；(2) 以太坊主网 Gas 费用波动可能影响运营成本，小额技术交易的适用性仍需评估；(3) “代码即法律”与现有法律框架之间尚存张力，链上自动执行与传统司法救济的衔接需法律与技术协同推进；(4) 合约代码虽经工具扫描和模拟攻击测试，但尚未完成第三方专业机构的形式化审计。

6.3. 未来展望

未来的研究方向包括：

(1) 性能扩容：探索采用 Layer 2 扩容方案(如 Optimistic Rollups 或 ZK-Rollups)或迁移至高性能联盟链，以降低 Gas 成本并提升吞吐量。

(2) 隐私保护：引入零知识证明(ZKP)等高级密码学技术，实现成果摘要信息的“可用不可见”，即在达成交易前不向全网络披露成果的核心技术细节。

(3) 法律合规融合：研究如何通过李嘉图合约(Ricardian Contract)将自然语言的法律条款与智能合约代码绑定，使系统产出满足法律效力要求的数字凭证。

(4) 智能化评估：探索将 AI 能力集成入系统，利用大语言模型或图神经网络对科技成果的技术成熟度、市场潜力和专利新颖性进行自动化辅助评估，为定价和撮合提供智能决策支持。

(5) 跨链互操作：研究与其他区块链(如数字身份链、数字人民币结算链)的跨链互通，构建更开放的技术转移基础设施。

基金项目

2024 年度江西省教育厅科学技术研究项目“区块链技术在高校科技成果管理中的应用研究”(GJJ2403210)。

参考文献

[1] 姜慧敏, 崔颖. 基于技术合同分析的我国技术交易发展现状与对策研究[J]. 科技管理研究, 2018, 38(19): 31-37.

[2] 周红霞. 评估业务的性质、评估质量的内涵及评估准则的作用——基于契约关系视角的分析[J]. 中国集体经济, 2014(6): 38-40.

[3] 石超. 区块链技术的信任制造及其应用的治理逻辑[J]. 东方法学, 2020(1): 108-122.

[4] 王璞巍, 杨航天, 孟佶, 等. 面向合同的智能合约的形式化定义及参考实现[J]. 软件学报, 2019, 30(9): 2608-2619.

[5] 薛晗. 基于区块链技术的数字版权交易机制完善路径[J]. 出版发行研究, 2020(6): 51-56+26.

[6] 谢人强, 张文德. 基于区块链的数字资源确权与交易方案研究[J]. 企业经济, 2022, 41(1): 65-73.

[7] 王伟琪. 基于区块链技术的数字版权交易研究[J]. 出版广角, 2020(3): 43-45.

[8] 赖利娜, 李永明. 区块链技术下数字版权保护的机遇、挑战与发展路径[J]. 法治研究, 2020(4): 127-135.

[9] 李哲宇. 比特币——去中心化货币的可能未来[J]. 中国集体经济, 2017(3): 99-100.

[10] Rühl, G. (2020) Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts? In: *Blockchain, Law and Governance*, Springer, 159-180. https://doi.org/10.1007/978-3-030-52722-8_11

[11] 高佳. 以太坊智能合约开发系统的设计与实现[D]: [硕士学位论文]. 杭州: 浙江大学, 2021.

[12] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.

[13] Hoffman, M.R., Ibáñez, L.D., Fryer, H., *et al*. (2018) Smart Papers: Dynamic Publications on the Blockchain. In: *Lecture Notes in Computer Science*, Springer, 304-318. https://doi.org/10.1007/978-3-319-93417-4_20

[14] 蒙杰, 杨生举. 基于区块链和 IPFS 的科研管理平台模型构建[J]. 计算机应用研究, 2025, 42(2): 54-60.

[15] 刘忆雪. 基于区块链的高校科技成果交易系统的设计与实现[D]: [硕士学位论文]. 西安: 西北大学, 2020.

[16] 史梦娜, 温浩宇, 窦永香. 基于联盟区块链的技术交易平台研究与设计[J]. 科技促进发展, 2021, 17(11): 1996-2004.