**使用联盟区块链实现安全高效的科研项目管理文献综述**

# 一、研究意义

随着知识经济的发展，科学技术在社会发展中发挥着越来越重要的作用。政府和企业对科研的投入明显增加，高校、科研院所、企业的科研项目数量逐渐增加。但目前科研项目管理的观念比较落后，缺乏科学的和规范的科研项目管理制度，并且科研管理的信息化水平不高，容易出现以下问题：科研项目逾期甚至终止失败、科研项目资金违规使用、科研项目外泄、科研项目转化率低。因此，建立完整、科学、规范、保密的科研项目管理制度具有十分重要的意义。

# 二、**研究相关技术**

一个高效的科研项目管理体系首先应该是规范的，将项目管理划分为多个流程，并严格按照流程开展科研，以防止出现延迟甚至失败的科研项目。项目管理起源于美国，其中以关键路径法(CPM)和项目评估与评审技术(P ERT)为代表。随着时间的推移，出现了越来越多的标准化项目管理方法，例如 PMBOK、PRICNCE2和WWPMM，其中PMBOK和PRINCE2是高度兼容和互补的。基于此，本研究将这两个项目管理标准结合起来，将项目管理流程概括为：项目启动、项目申报、项目执行、阶段控制、项目收尾。此外，还涉及到项目时间管理、项目成本管理和项目质量管理。

其次，需要有一套完整的量化体系，对科研项目的各项指标和预期完成目标进行量化，从而更科学地解释项目在阶段检查和最终结果验收中是否达到预期，值得注意的是，保密性也非常重要，这便需要相关技术加以实现。

随着区块链技术的不断发展和应用，越来越多的领域开始尝试利用区块链技术实现信息的安全和高效管理。科研项目管理作为一个需要高度机密性和精密性的领域，也受到了区块链技术的关注。

根据访问机制的不同，区块链可以分为三类：公有区块链、联盟区块链和私有区块链，其中联盟区块链非常适合两家或数量有限的机构参与科研项目的活动，联盟区块链的访问机制和去中心化可以在很大程度上增加科研项目过程中的机密性，为科研项目管理提供了一种安全、高效、去中心化的解决方案。

联盟区块链是指由多个组织或实体共同参与维护的区块链网络。在科研项目管理中，这些组织可以包括研究机构、学术期刊、资助机构等。联盟区块链通过去中心化的方式，实现了数据和交易的安全和透明，避免了数据篡改和单点故障等问题。此外，联盟区块链还可以实现智能合约，使得科研项目管理的过程更加高效。

在联盟区块链的框架下，科研项目管理可以实现以下功能：

1. 数据安全：联盟区块链通过分布式存储和加密技术，保证了科研项目的数据安全。所有参与者都可以共享数据，但只有授权的人才能查看和修改数据。
2. 资金管理：科研项目通常需要大量的资金支持，而联盟区块链可以实现资金的透明和高效管理。通过智能合约，可以自动执行资金的分配和使用，避免了传统项目管理中的繁琐流程。
3. 项目评估：联盟区块链可以实现科研项目的评估和审查，保证项目的公正和透明。参与者可以通过区块链上的智能合约，自动完成项目评估和审查，减少人力和时间成本。

目前，一些学术期刊和研究机构已经开始尝试使用联盟区块链来管理科研项目。例如，英国伦敦大学学院的“MIRRA”项目就是一个基于联盟区块链的科研项目管理平台。该平台可以实现研究人员之间的数据共享和合作，同时保证了数据的安全和隐私。

其次，IPFS技术可以实现科研项目的数据存储和共享，它是一种去中心化的点对点数据分发协议，其节点形成分布式文件系统，为每个文件生成一个唯一的哈希值，构建哈希值到文件的映射。此外，IPFS能够快速、高效地实现文件的传输和共享，同时保证数据的安全性，将IPFS技术应用于科研项目管理中，可以更好地对科研项目产生的文件进行管理，在降低成本的同时保证数据的安全，促进科研合作的发展。

最后，智能合约技术可以自动化执行科研项目管理中的各种操作和流程。智能合约是一种基于区块链技术的智能化合约，可以自动化执行合同中的各种操作和流程，从而实现合同的自动化和规范化管理。具有以下优点：（1）执行准确，（2）人为干预风险低，（3）去中心化，（4）运行成本低。在科研项目管理中，智能合约技术可以帮助科研人员自动化管理项目的流程和任务，从而提高项目的效率和管理的规范性。

# 三、具体系统概述

孟庆峰，孙润耕的文章设计了符合联盟区块链和IPFS的科研项目管理系统，采用基于联盟链的智能合约技术和IPFS系统结合非对称加密技术，利用智能合约规范科研项目管理流程，利用IPFS系统解决科研项目管理中的数据存储和隐私保护问题，实现了从项目启动到项目结束的全过程管理。

安全性体现在有权访问该系统的人必须是授权的组织或机构，可以作为区块链节点加入联盟区块链。授予人可在系统内发起或申报他人发起的项目，建立合作关系后再启动科研合作。在合作过程中，所有资金转账、进度检查提示等工作，都将由智能合约自动执行。

该系统由两个功能模块组成：数据文件加密模块和联盟链模块。

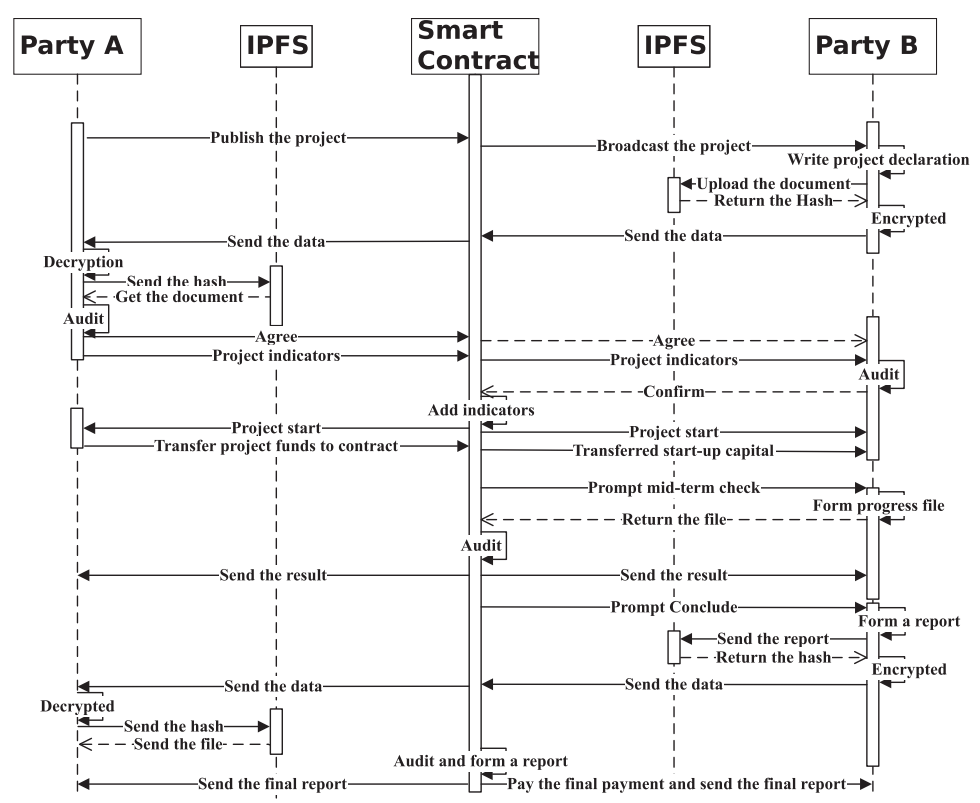
①数据文件加密模块利用星际文件系统(IPFS)和非对称密码技术，当A想要通过区块链将文件发送给B时，A首先获取B的公钥，然后用它对文件进行加密。然后，A 使用IPFS将加密后的文件添加到IPFS中，获取文件的哈希值。该哈希值通过区块链发送给B后，B会接收到该哈希值，并通过IPFS获取该文件。然后，用B自己的私钥对哈希值进行解密，获得完整的文件。

②联盟链模块负责系统运行和项目参与者之间的数据交互。智能合约部署在区块链上后将自动执行，并且合约不能再变化，这可以有效防止项目参与者违约，其中智能合约上的项目数据结构如表1所示：

**表1** 智能合约上的项目数据结构

|  |  |  |
| --- | --- | --- |
| 属性名 | 类型 | 描述 |
| Name | string | 项目名称 |
| partyA | address | 甲方地址，甲方余额可从中获取 |
| partyB | address | 乙方地址，乙方余额可从中获取 |
| startTime | uint | 项目开始时间 |
| endTime | uint | 项目结束时间 |
| totalFund | uint | 项目总资金 |
| startFund | uint | 启动项目资金 |
| timeNodes | TimeNode[] | 项目的一些时间节点 |
| Indicators | Indicator[] | 项目部分进度指标 |
| Datas | Data[] | 项目的数据 |

系统工作流程图如图1所示，



**图1** 系统序列图

在绩效评估方面，孟庆峰，孙润耕的文章使用PC机模拟一个参与项目的组织，测试其对系统请求的响应时间。在实验中重点评估了文件上传时间，因为它是项目管理系统的一个重要性能指标。实验后得出结论：文件上传时间几乎与文件大小无关。这是因为IPFS网络返回的哈希值不大，影响上传时间的主要因素是上传请求的数量，即文件上传时间与文件数量成正比。以10MB文件为例，上传1次、5次、25次、125次的时间分别为0.62s、3.12s、15.63s、79.6s。与传统科研项目管理中手工传输文件的方式相比，该系统在保证其安全性的前提下，大大节省了人力、物力和时间。

# 四、总结

总的来说，联盟区块链、IPFS和智能合约等技术的应用，为科研项目管理提供了更加安全、高效、透明和可追溯的合作与管理方式。但也需要注意到联盟区块链在科研项目管理中仍存在一些挑战和限制。例如，联盟区块链的实现需要各个参与者的共同努力和合作，而这可能会受到利益和政策等方面的影响。此外，区块链技术的普及和应用仍需要时间和资源的投入，需要逐步推广和完善。我们有理由相信，随着技术的不断发展和完善，这些技术将在科研项目管理领域发挥越来越重要的作用，促进科研合作和管理的发展。