项目编号：2020YFB1005500 密级：公开

**国家重点研发计划项目** 2021 **年度**

**课题技术进展报告**

课题名称 “以链治链”的跨链协同监管体系与方法

项目名称： “以链治链”的监管架构与关键技术研究

所属专项： 云计算和大数据

项目管理专业机构：科学技术部高技术研究发展中心

执行期限：  2020年11月 至 2023年 10月

2021年10月18日

[科技报告编号] 公开范围[延迟期限]

科 技 报 告

报 告 名 称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

支 持 渠 道：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 单 位：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 时 间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编写说明

一、课题负责人负责组织研究人员编写科技报告，并按相关计划管理的要求审核和提交。

二、科技报告一般包括封面、基本信息表、目录、插图清单、附表清单、正文、附录和参考文献等部分。

三、报告内容应客观真实、准确完整、层次清晰。本领域的专业读者依据这些描述能重复调查研究过程、评议研究结果。

科技报告基本信息表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.报告名称 | | 中文：“以链治链”的跨链协同监管体系与方法课题年度报告（2021年） | | | | | | |
| 英文：Annual Technology Report on Cross-Chain Collaborative Supervision System and Methods of “Chain Governing Chain”（2021） | | | | | | |
| 2.报告作者及单位 | | 中文： | | | | | | |
| 英文： | | | | | | |
| 3.使用范围（公开和延期公开，延期公开需明确延期时间）  原因： | | | | | | 4.编制时间（YYYY-MM-DD）  2021-10-18 | | |
| 5.报告编号（单位机构代码+课题编号+/顺序号，XXXXXXXXX -- NNNNUUNNNNNN/NN） | | | | | | | | |
| 6.备注（须注明的特殊事项，如延期公开报告的查询权限、免责声明、报告与其它工作或成果的联系等） | | | | | | | | |
| 7. 摘 要 | 中文（600字左右）：  本课题的主要研究目标是提出“以链治链”架构下跨链分布式监管的协同体系和“以链治链”架构下的新型数据加密审计方法。首先，根据不同密码原语、中继链接、哈希锁定、投票机制、动态优化理论、大数据挖掘和机器学习等理论技术，提出节点分级权限动态迁移机制、跨链监管边云协同技术、安全计算协议自适应生成等关键技术；在此基础上，研发典型应用场景下“以链治链”的跨链协同原型验证程序，并制定适用于该系统的权限分级机制和内容审计方案。  本年度课题的研究内容主要包括以下2个方面。1）针对不同的区块链业务场景下用户区块链类型具有差异性的问题，完成动态迁移的跨链节点权限分级技术研究，设计高效的多级权限管理及监督方案。提出一种多链场景下数据跨链访问控制方法，能够满足面向多链场景下的数据跨链访问控制需求； 2）针对分布式跨链情形下密态内容难于审计的问题，研究链上加密数据的搜索与查询技术。提出一种可检索证明和复制证明的去中心化方法，利用时间限制证明、激励机制、隐私增强等技术，提供安全的密文数据检索服务。并研究了区块链网络安全保障相关的攻击与防御方法，调研关于区块链安全漏洞的最新进展，详细介绍了目前最先进的防御方法，系统调研了区块链系统的安全性问题。最后，针对对于区块链潜在的安全问题，提出了对应的安全策略。 | | | | | | | |
| 英文（不超过2500个字符）： | | | | | | | |
| 8. 关 键 词 | 中文（3-8个，以分号隔开）： | | | | | | | |
| 英文（3-8个，以分号隔开）： | | | | | | | |
| 9.支持渠道 | 项目名称 | | |  | | | | |
| 主管部门 | | |  | | | 计划名称 |  |
| 项目编号 | | |  | | | 应用领域 |  |
| 承担单位 | | |  | | | | |
| 合作单位（不超过5家） | | |  | | | | |
| 总经费（万元） | | |  | | | 国拨经费（万元） |  |
| 项目负责人 | | |  | | | | |
| 起始日期 | | |  | | | 截止日期 |  |
| 10.联系人 | 姓名 | |  | 单位 |  | | | |
| 电话 | |  | E-Mail |  | | | |

**目 录**

[引言 1](#_Toc85398726)

[1 研究概述 3](#_Toc85398727)

[1.1 研究背景及意义 3](#_Toc85398728)

[1.2 课题二与其它课题的关系 3](#_Toc85398729)

[1.3 课题二研究内容 4](#_Toc85398730)

[1.3.1拟解决的关键科学与技术问题 4](#_Toc85398731)

[1.3.2拟开展的主要研究内容 5](#_Toc85398732)

[1.4 研究技术路线 6](#_Toc85398733)

[2 多链场景下数据跨链访问控制方法 8](#_Toc85398734)

[2.1 现有多链场景下数据跨链访问控制系统存在的问题 8](#_Toc85398735)

[2.2 多链场景下数据跨链访问控制及系统详细技术方案 10](#_Toc85398736)

[2.3 本方法的优点 17](#_Toc85398737)

[3 BOSSA：一种可检索证明和复制证明的去中心化系统 18](#_Toc85398738)

[3.1 现有系统存在的问题 18](#_Toc85398739)

[3.2 BOSSA方法及系统详细技术方案 18](#_Toc85398740)

[3.3 本方法的优点 19](#_Toc85398741)

[4 区块链网络安全保障：攻击与防御 20](#_Toc85398742)

[4.1 问题现状 20](#_Toc85398743)

[4.2 研究内容 20](#_Toc85398744)

[4.3 研究优势 21](#_Toc85398745)

[5 结论 22](#_Toc85398746)

[参考文献 23](#_Toc85398747)

# 插图清单

[图 1 课题二与其他课题关系 4](#_Toc85396698)

[图 2 课题二拟开展的主要研究内容 6](#_Toc85396699)

[图 3 课题二技术路线 7](#_Toc85396700)

[图 4 密态内容审计方法研究技术路线 8](#_Toc85396701)

[图 5 多链场景下数据跨链访问控制方法流程图 11](#_Toc85396702)

[图 6 数据跨链访问控制方法的跨链访问流程图 12](#_Toc85396703)

[图 7 多链场景下数据跨链访问控制系统结构框图 14](#_Toc85396704)

[图 8 多链场景下数据跨链访问控制系统结构原理图 15](#_Toc85396705)

[图 9 数据跨链访问控制方法的跨域属性映射示意图 15](#_Toc85396706)

[图 10 数据跨链访问控制方法的跨链调用流程图 15](#_Toc85396707)

[图 11 数据跨链访问控制方法的CP-ABE原理示意图 16](#_Toc85396708)

[图 12 BOSSA系统模型 18](#_Toc85396709)

# 附表清单

[表 1 区块链安全威胁和防御方法 20](#_Toc85354339)

# 引言

课题“以链治链”的跨链协同监管体系与方法总的研究目标是提出“以链治链”架构下跨链分布式监管的协同体系和“以链治链”架构下的新型数据加密审计方法。首先，根据不同密码原语、中继链接、哈希锁定、投票机制、动态优化理论、大数据挖掘和机器学习等理论技术，提出节点分级权限动态迁移机制、跨链监管边云协同技术、安全计算协议自适应生成等关键技术；在此基础上，研发典型应用场景下“以链治链”的跨链协同原型验证程序，并制定适用于该系统的权限分级机制和内容审计方案。

本年度，项目和课题启动，明确各自目标，全面开展相关研究。课题的研究内容主要包括以下2个方面：1）针对不同的区块链业务场景下用户区块链类型具有差异性的问题，完成动态迁移的跨链节点权限分级技术研究，设计高效的多级权限管理及监督方案； 2）针对分布式跨链情形下密态内容难于审计的问题，研究链上加密数据的搜索与查询技术。

具体研究包括以下内容：

1. 提出一种多链场景下数据跨链访问控制方法，能够满足面向多链场景下的数据跨链访问控制需求，针对区块链技术在单链架构下存在着性能、容量不足问题和传统技术无法满足或者实现复杂的跨区块链业务的资产交换和信息交换需求提出了跨链访问控制方案。
2. 提出一种可检索证明和复制证明的去中心化方法及系统，利用Block以近似固定的速率上链的特性，提出了一个时间限制证明，迫使云服务商和农民提供数据可用性的证明。并设计了一个激励机制来激励农民为用户在任何时候提供数据检索服务。为防止隐私泄露，结合了隐私增强技术来生成证明，并确保证明的正确性。
3. 研究区块链网络安全保障相关的攻击与防御方法，调研关于区块链安全漏洞的最新进展，详细介绍了目前最先进的防御方法，系统地调研了区块链系统的安全性问题。针对对于区块链潜在的安全问题，提出了对应的安全策略。

# 研究概述

## 研究背景及意义

目前区块链应用面临数据孤岛、信息价值无法共享等问题，无法有效满足实际业务需求。跨链技术的诞生有效解决了以上问题，但在权限分级、跨链监管、跨链协同方面仍存在不足。英国金融行为监管局(FCA)提出了区块链监管沙盒技术，国际清算银行提出区块链金融监管架构及其区块链产品，中国央行票据交易所提出数金链用于数字票据区块链监管。当前大部分的跨链方案在实现对节点权限的分级监管时，依赖于自身的实现及相关的共识算法，而这种权限分级并不灵活，为每个用户或节点的权限监管带来了重大挑战。此外，当前的跨链协同机制大多通过权威证明（POA）共识算法来进行多方信息协同，但该方法需要多方共同信任一个可信的第三方，这种机制给跨链协同带来了新的安全威胁。

本课题的总体目标是通过技术研究突破，构建“以链治链”架构下跨链分布式监管的协同体系和“以链治链”架构下的新型数据加密审计方法。利用投票机制、中继机制、哈希锁定、同态加密、动态优化理论、机器学习等理论与方法，解决现有监管方法跨链交互能力弱、协同性差、效率低等问题。提出节点分级权限动态迁移机制、跨链监管边云协同技术、安全计算协议自适应生成等关键技术；在此基础上，研发典型应用场景下“以链治链”的跨链协同原型验证程序，并制定适用于该系统的权限分级机制和内容审计方案。通过项目实施，期望能实现新兴信息通信技术在服务业全要素、全领域、全产业链的深度融合与集成应用，对推动和促进我国物流行业转型及产业升级、提升国际竞争力具有重要意义。

## 课题二与其它课题的关系

在课题一“以链治链”监管结构和安全模型的基础之上，本课题重点讨论跨链协同机制，从监管者的视角，纵向涉及节点、交易、管理的权限等级设置，横向考虑不同区域的异构跨域协同，继而做到从微观到宏观的分级多域、从物理结构上的端边云结合，以实现全方位、自动化、协同式监管；另外考虑到监管者不一定是绝对可信的，从系统设计的角度，既要考虑对用户隐私行为——密态内容的监督，也要考虑对监督行为的密态内容进行审计。课题二各任务与其他课题的关系如图1所示。

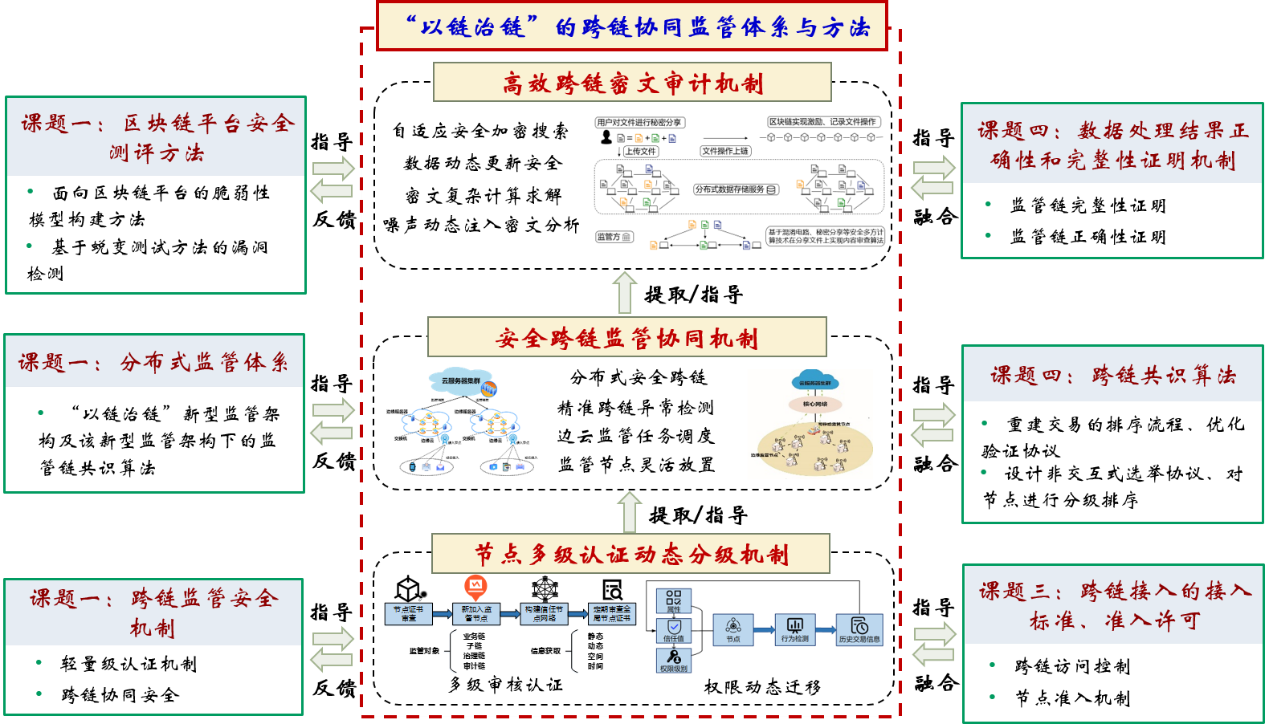


图 1 课题二与其他课题关系

## 课题二研究内容

### 拟解决的关键科学与技术问题

(1) 跨链自动化监管的协同机制问题

跨链自动化监管的协同机制问题监管任务分解和协调机制是通信资源和计算资源高效协同的重要纽带。为满足分布式、多模态、复杂区块链业务的监管协同需求，如何将一个具有多监管目标的复杂监管任务进行细粒度划分，如何设计合理的子监管任务分配方案以及子任务协调机制，是本项目要解决的关键技术之一。

(2) 分布式跨链情形下密态内容难于审计问题

基于分布式监管架构，面向大规模区块链业务用户数量庞大、交易模式多态、等特点，分布式监管难以审计跨链的密态内容。链上数据持续增加对访问模式和搜索模式提出了更高的要求。本研究旨在不侵犯数据隐私内容的前提下完成数据的精准审计，设计支持链码的数据加密方案，转化目标问题，在加密数据上完成复杂计算任务的求解。

### 拟开展的主要研究内容

(1) 动态迁移的跨链节点权限分级机制

针对不同领域下区块链业务场景复杂、角色繁多、可信度存疑等特点，开展区块链用户节点权限动态分级机制研究。基于信誉计算和多人投票机制研究节点权限动态调整技术，探索链间权限迁移对安全强度的影响，研究同构/异构链不同模态下权限可控迁移机制。

(2) 异构多态的分布式跨链监管技术

深入研究安全可控的分布式跨链监管技术，具体包含以下两个部分：面向节点参与度、链上链下、中继与否等监管模态差异，从跨链路由、中继桥接等角度研究不同场景下的分布式跨链技术，基于同态加密等技术研究不可信场景下的链间隔离方案，在跨链交互的同时，实现链间安全隔离和隐私。

(3) 边云结合的跨链监管协同机制

在分布式跨链监管架构和安全机制下，考虑到移动设备应用场景的增多和计算能力的增加，研究边云结合的多模态监管协同机制，实现监管任务的高效执行。面向不同粒度的监管需求，基于最优化技术研究边云结合监管节点放置和协同机制，以及不同场景下的分布式监管协同技术。

(4) 精准高效的密态内容审计方法

设计支持链码的同态加密、差分隐私等数据加密方案，抽取数据审计的共性计算操作，构建合规属性集，在加密数据上完成复杂计算任务的近似求解，完成具有自适应安全等级或多关键字的密文搜索与查询等技术研究，并开展加密数据统计分析研究。针对基于差分隐私的数据保护方案，设计链上数据的前期去隐私化处理机制，实现支持噪声动态注入的链上数据统计分析；基于混淆电路的隐私保护方案，完成安全计算协议自适应生成方案。

课题二拟开展的主要研究内容如图2所示。



图 2 课题二拟开展的主要研究内容

## 研究技术路线

通过项目实施，预期实现跨链监管协同原型验证系统。为此，课题的总体研究思路按照“以链治链”的关键技术突破、系统平台构建和行业应用示范三个层次展开：首先，攻克节点权限分级、监管协同、密态审计三大核心关键技术；基于此，设计新型“以链治链”协同监管架构，并构建权限灵活、权限灵活、协同性强、内容易审计的协同仿真系统；最后，在该平台上进行典型行业的应用示范。

针对不同的区块链业务场景下用户区块链类型具有差异性的问题，研究面向不同模态下的跨链交互方案。一方面，面对多模态区块链交易场景下，部分不可信节点恶意操作导致存在异常交易的情况，分析用户敏感数据的类型以及敏感程度，结合同态加密或者保序加密等安全防护机制，研究可定制的授权安全交互和链间安全隔离方案；另一方面，基于机器学习技术，构建跨链异常行为模型，同时对比部分已知恶意节点信息，并考虑采用联邦学习机制或改进机器学习解释流程，对学习后的异常行为模型在安全性方面和效率方面进行优化，提高跨链异常行为识别的准确率和隐私性。

针对“以链治链”架构下跨链自动化监管的协同机制问题，对面向不同业务跨链需求以及同构/异构链的监管差异，采用中继和哈希锁定等技术，实现多模态的跨链交互授权；在不同业务场景下，分析交易对象、交易模式、交易数据之间内在关联和差异，使用同态加密和匿名支付等技术，研究面向不可信场景的链间安全隔离技术，实现跨链交互的安全性和隐私性保护；针对分布式区块链场景复杂、节点众多的特点，面向不同粒度的监管需求，使用最优化技术研究边云结合监管节点放置和协同机制，实现监管任务执行的低延迟和高吞吐量。

针对分布式跨链情形下密态内容难于审计的问题，拟研究链上加密数据的搜索与查询技术，实现丰富的语义搜索、自适应安全等级的加密搜索、支持数据动态更新、前向和后向安全，为快速准确的海量敏感数据密文搜索创造理论基础；拟研究链上加密数据的统计与分析技术，实现复杂计算问题的求解和支持噪声动态注入的链上数据统计分析。进一步研究多种隐私保护机制下安全性、效率和分析结果精确性之间的内联关系，以满足监管方对不同审计任务的需求。

课题二具体的技术路线如图3所示。



图 3 课题二技术路线

课题参与方武汉大学具体研究的目标是结合智能合约的底层特点，设计支持链码的同态加密、差分隐私等数据加密方案，抽取数据审计的共性计算操作，构建合规属性集，对目标问题进行相应转化，在加密数据上完成复杂计算任务的近似求解；利用混淆电路自动化生成安全计算协议，在不侵犯数据隐私内容的前提下完成数据的精准审计。

如图4是密态内容审计方法研究技术路线图，研究成果包括数据加密方案，加密数据近似求解，去隐私化机制和密文搜索、分析与查询。数据加密方案通过同态加密和差分隐私实现，支持链码。基于差分隐私的数据保护方案是链上数据去隐私化处理机制的基础，这种处理机制支持噪声动态注入的链上数据统计分析。提取链上数据审计的共性计算操作，构建合规属性集，进行加密数据的复杂计算任务的近似求解。

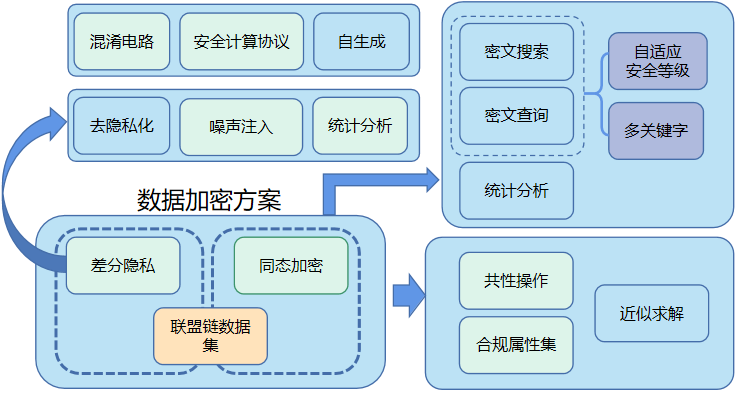


图 4 密态内容审计方法研究技术路线

# 多链场景下数据跨链访问控制方法

## 现有多链场景下数据跨链访问控制系统存在的问题

目前，当前的区块链应用和底层技术平台呈现出百花齐放的状态，但主流区块链应用中的每条链大多仍是一个独立的、垂直的封闭体系。在业务形式日益复杂的商业应用场景下，链与链之间缺乏统一的互联互通机制，这极大限制了区块链上数字资产价值的流动性，跨链需求由此而来。

跨链指的是通过连接相对独立的区块链系统，实现不同账本的可信互操作。跨链依据其交换内容的不同可以大体分为数字资产交换和信息交换。在数字资产交换方面，当前资产交换主要依靠中心化的交易所来完成，中心化的交换方式既不安全、规则也不透明，业界也出现了去中心化的资产交换方式如Uniswap、Curve、SushiSwap等，但是当前的去中心化资产交易多数只能实现同一个区块链上不同合约资产的交换，对跨链数字资产去中心化交换仍不完善，事实上仍处于互相隔离的状态，信息交换由于涉及链与链之间的数据同步和相应的跨链调用，实现更为复杂，因此每个区块链应用之间互通壁垒极高，无法有效地进行链上信息共享。

另一方面，区块链技术在单链架构下本身存在着性能差、容量不足等问题。单链受限于去中心化、可扩展性和安全性的权衡，难以支撑高交易吞吐量低延迟的商业场景应用。此外，随着区块链运行时间的增长，其存储容量也将逐渐增长，且这种数据增长的速度甚至会超过单链存储介质的容量上限，故通过跨链技术实现多链协作的多层多链体系架构是解决区块链性能瓶颈的可取之道。因此，亟需一种多链场景下数据跨链访问控制方法、系统、设备及终端。

通过上述分析，现有技术存在的问题及缺陷为：

（1）中心化的交换方式既不安全、规则也不透明。

（2）当前去中心化资产交易多数只能实现同一个区块链上不同合约资产的交换，对跨链数字资产去中心化交换仍不完善，事实上仍处于互相隔离的状态。

（3）信息交换由于涉及链与链之间的数据同步和相应的跨链调用，实现更为复杂，故每个区块链应用之间互通壁垒极高，无法有效地进行链上信息共享。

（4）区块链技术在单链架构下本身存在着性能差、容量不足等问题，单链受限于去中心化、可扩展性和安全性的权衡，难以支撑高交易吞吐量低延迟的商业场景应用。

（5）随着区块链运行时间的增长，其存储容量也将逐渐增长，且数据增长速度甚至会超过单链存储介质的容量上限，极大限制了区块链技术的健康发展。

解决以上问题及缺陷的难度为：

（1）跨链交易的验证问题，如何确认记录交易发生的区块得到了足够的确认，即交易事务中各分布式网络间的数据一致性问题；

（2）跨链事务的原子性问题，如何管理跨链事务中的各子交易确保跨链事务整体完整的原子性，即跨链事务的发生只存在两中状态完成或失败；

（3）不同区块链之间的协议适配问题，如何对采用不同架构与协议的区块链之间进行适配，需要跨链协议中设计可以兼容多种异构区块链的数据结构、命名规范以及通信方式等。

解决以上问题及缺陷的意义为：通过解决上述问题，一种多链场景下数据跨链访问控制方案，结合区块链去中心化、可追溯、不可篡改等技术特点，构建一个高可扩展、强鲁棒性、易升级的区块链跨链平台，为去中心化应用提供通信枢纽，支撑链上可信数据资产高效流动，服务区块链业务安全治理，为区块链互联网的形成提供可靠的底层技术支撑。保证跨链交易的安全性、灵活性与可靠性。

## 多链场景下数据跨链访问控制及系统详细技术方案

针对现有技术存在的问题，本方案提供了一种多链场景下数据跨链访问控制方法。图5是本方案提出的的多链场景下数据跨链访问控制方法流程图，多链场景下数据跨链访问控制方法包括以下步骤：



图 5 多链场景下数据跨链访问控制方法流程图

注册阶段：每个域中用户或物联网设备在其各自归属域中进行身份注册与认证，获取身份属性信息，使得每个用户或物联网的数据分类存放，方便进行访问控制。

数据上传：将加密过的数据上传至服务端存储，数据所有者DO生成随机文件密钥k，使用密钥k执行对称加密算法AES加密明文数据M生成密文C上传至服务端存储，同时记录数据M元数据信息。数据M元数据信息，包括哈希值、上传域、文件大小、上传时间和所有者。数据跨链调用，包括：

（1）进行跨链访问时，应用链A在所在域D1向自治域D2的应用链B发出跨链访问请求时；

（2）应用链A通过调用中继链进行跨链访问，中继链对访问链进行身份认证与合法性确认，通过属性映射将域D1属性映射为域D2属性，使得请求者获取域D2属性；

（3）中继链根据映射后的D2属性集生成D2颁发的公私钥对分发至数据请求者，并将调用请求转发至应用链B；

（4）应用链B传输密文数据信息至数据请求者。

数据上链：方便用户查找服务端的现有数据，数据所有者DO设定该数据访问结构策略树T，结合访问策略执行CP-ABE算法加密密钥k生成文件对称加密密钥的密文ET(k)，将数据上传阶段中元数据信息、访问策略及ET(k)生成区块，更新至数据信息链。

数据访问：通过中继链实现访问控制，数据请求者DU在所在域D1发起数据访问请求；若涉及跨域数据，则D1跨链通过调用中继链对数据所在域D2申请访问；D2对申请者进行判决，若判决成功，则D1传输密文数据给DU。

访问记录上链：记录数据的访问情况，数据访问阶段中访问控制判定结束后，数据所在域将此次访问请求及结果的相关信息上链记录，以供后续查询与审计。

数据获取：用户解密获得数据，DU使用CP-ABE算法解密数据信息链中的ET(k)获取文件密钥k，然后使用k通过AES算法解密密文C获取明文数据M 。

数据上传和获取阶段中，其中CP-ABE算法，包括：

（1）系统初始化算法（1τ）→（PK，MK）：输入一个安全参数τ，输出系统公钥PK和主密钥MK；

（2）密钥生成算法（PK，MK，S）→（SK）：输入一个属性集合S、主密钥MK和公钥PK，输出用户私钥SK；

（3）加密算法（PK，M，AS）→（CT）：输入一个需要加密的明文M、公钥PK和访问结构AS，输出包含访问策略的密文CT；

（4）解密算法（PK，SK，CT）→（M）：输入包含访问策略AS的密文CT、由属性集合所生成的公钥PK和私钥SK，如果属性集合S满足访问策略时，用户即可成功解密出明文M。



图 6 数据跨链访问控制方法的跨链访问流程图

图6是数据跨链访问控制方法的跨链访问流程图。多链场景下数据跨链访问控制方法还包括数据跨域访问，具体包括以下步骤：

（1）完成区块链网络内各个云组织之间属性映射，由跨链服务管理平台维护属性映射表；

（2）用户进行身份注册，自动化生成用户公私钥对和用户属性；

（3）数据所有者DO生成随机文件密钥k，使用密钥k执行对称加密算法加密明文数据M生成密文C上传至自治域，并记录数据M元数据信息；其中，所述数据M元数据信息包括：数据所在域FileAddr、数据关键词集合Keywords和加密文件的散列值hash；

（4）DO设定该数据访问结构策略树T，调用跨链服务管理平台属性映射接口完成各域间属性映射扩展；

（5）DO执行CP-ABE算法加密密钥k生成ET(k)，将元数据信息、访问策略及ET(k)生成区块，将生成的文件信息经过共识算法上链；

（6）数据使用者DU可通过文件信息链FIC检索多域下所有数据信息，调用跨链接口发起数据访问请求；

（7）跨链服务管理平台通过文件信息链FIC和中继链自动查询数据访问策略和用户属性，进行访问判决，若DU属性匹配策略，转步骤（9）；否则拒绝访问，流程结束；

（8）目标链所在域传输数据密文C给DU；

（9）DU首先通过解密数据信息链中的ET(k)获取文件密钥k，然后使用k通过解密密文C获取明文数据。

此外，多链场景下数据跨链访问控制方法，还包括基于多云共识的共识机制Raft更新区块，当系统中有用户发起的新提案时，由于当前区块链的记账权由领导者节点掌握，跟随者节点具体工作；其中，区块更新具体包括以下步骤：

（1）跟随者将提案行为发送给领导者节点；

（2）领导者节点验证证书的数字签名，校验通过后将收到的数字证书和操作类型打包成区块，并把该区块向所有跟随者节点广播；

（3）跟随者节点验证区块内容后向领导者节点返回响应；

（4）领导者节点在收获超过一半的节点响应后，通知所有跟随者节点确认写入该区块，跟随者节点再通知各自域内节点更新区块链，完成账本更新。

本方案的另一目的在于提供一种应用所述的多链场景下数据跨链访问控制方法的多链场景下数据跨链访问控制系统，图7是其多链场景下数据跨链访问控制系统结构框图，图8是多链场景下数据跨链访问控制系统结构原理图，图 9为数据跨链访问控制方法的跨域属性映射示意图，图10为数据跨链访问控制方法的跨链调用流程图。具体系统包括以下模块：



图 7 多链场景下数据跨链访问控制系统结构框图

用户模块，由用户实体组成，是数据调用的实际参与者，用于用户身份注册、访问数据和上传数据；

多链自治模块，由多个服务自治域D组成，用于负责用户身份注册与属性颁发，以及用于属性加密的密钥生成与分发，同时记录数据信息，每个域拥有其独立维护的数据信息链与访问记录链；

数据存储模块，由具有强大计算能力和大存储容量的云服务提供商CSP和其他物联网设备组成，用于负责数据的存储及下载服务。

用户模块具体包括用于用户身份注册、属性分配的认证单元，用于根据用户操作要求对数据进行上传、下载、修改等动作的操作单元，用于记录用户的访问请求与对应结果的访问记录链ARC。

访问记录链ARC包括数据访问用户DU、访问用户所在域D、数据访问时间FileTime、数据所在域FileAddr及访问结果AccessResult。

多链自治模块包括采用Raft协议使域内各节点达成共识的共识机制，用于进行跨链调用和域间差异化属性映射的中继链，用于维护数据所有者DO上传数据的元信息的文件信息链FIC。

文件信息链FIC包括数据所在域FileAddr、数据关键词集合Keywords、加密文件的散列值hash及经过属性基CP-ABE加密后，用户加密文件所使用的文件对称加密密钥的密文ET(k)。

数据存储模块，用于存储经过数据所有者DO加密上传后的数据，接受数据访问者DU的请求并提供密文下载服务。



图 8 多链场景下数据跨链访问控制系统结构原理图



图 9 数据跨链访问控制方法的跨域属性映射示意图



图 10 数据跨链访问控制方法的跨链调用流程图

本方案的另一目的在于提供一种计算机设备，计算机设备包括存储器和处理器，存储器存储有计算机程序，计算机程序被所述处理器执行时，图11为数据跨链访问控制方法的CP-ABE原理示意图，处理器执行如下步骤：

（1）注册阶段：每个域中用户或物联网设备在其各自归属域中进行身份注册与认证，获取身份属性信息；

（2）数据上传：数据所有者DO生成随机文件密钥k，使用密钥k执行对称加密算法AES加密明文数据M生成密文C上传至服务端存储，同时记录数据M元数据信息；

（3）数据上链：数据所有者DO设定该数据访问结构策略树T，结合访问策略执行CP-ABE算法加密密钥k生成ET(k)，将步骤二中元数据信息、访问策略及ET(k)生成区块，更新至数据信息链；

（4）数据访问：数据请求者DU在所在域D1发起数据访问请求；若涉及跨域数据，则D1跨链通过调用中继链对数据所在域D2申请访问；D2对申请者进行判决，若判决成功，则D1传输密文数据给DU；

（5）访问记录上链：数据访问阶段中访问控制判定结束后，数据所在域将此次访问请求及结果的相关信息上链记录，以供后续查询与审计；

（6）数据获取：DU使用CP-ABE算法解密数据信息链中的ET(k)获取文件密钥k，然后使用k通过AES算法解密密文C获取明文数据M。



图 11 数据跨链访问控制方法的CP-ABE原理示意图

## 本方法的优点

结合上述的所有技术方案，本方案所具备的优点及积极效果为：本方案提供的多链场景下数据跨链访问控制方法，能够满足面向多链场景下的数据跨链访问控制需求，针对区块链技术在单链架构下存在着性能、容量不足问题和传统技术无法满足或者实现复杂的跨区块链业务的资产交换和信息交换需求提出了跨链访问控制方案。本方案允许多链场景下异构链间的资产交换、数据共享及合约调用。依据场景导向可灵活组织部署架构，具有通用跨链传输协议、异构交易验证引擎核心功能特性，保证跨链交易的安全性、灵活性与可靠性。该方案为去中心化应用提供通信枢纽，支撑了链上可信数据资产高效流动，为服务区块链业务安全治理、区块链互联网的形成提供了可靠的底层技术支撑。

# BOSSA：一种可检索证明和复制证明的去中心化系统

## 现有系统存在的问题

云计算作为一种新的计算范式，为普通用户提供了一种便捷的途径使用强大的计算资源和存储资源。用户可以将其数据外包给云服务提供商，以摆脱复杂的本地数据管理。虽然前景看好，但将数据外包给远程服务器会引起严重的安全问题。这种行为剥夺了数据所有者的物理控制权。关键问题之一是确保数据的正确性。恶意服务器可能为了节省存储资源而丢弃很少访问的数据，或者为了维护声誉而故意掩盖数据丢失事故。此外，云服务商通常将数据与几个副本存储在一起，以确保高可靠性，如果发送数据丢失，它在其服务级别协议(SLA)中承担有限责任。最近腾讯云发生了数据安全的事故，其他的云服务也表示云服务是不能完全可信的。

可检索证明以及复制证明是两种典型的加密方法，允许服务器证明原始文件以及所有副本都正确存储在服务器上。可检索证明和复制证明的解决方案可以让用户不必时刻在线进行数据完整性和可检索的审计，但是这些方案在很大程度上依赖于半可信的第三方审计(Third Party Audit，TPA)来执行公共验证。但是这种方法有以下两个缺点:

（1）合谋攻击（Collusion Attack）：一般文献设定TPA不会和云服务商S合谋。但是在实际中，这种强假设会轻易被利益驱动所破坏，一旦云服务商和TPA合谋后可以轻易地给出假的数据证明。而且，从用户的角度看，这种合谋是不可感知的。

（2）腐化攻击（Corruption Attack）：持续在线的TPA容易受到未知意外的单点故障攻击，如地区停电、DDoS黑客攻击等。

我们将这些安全问题归因于TPA过于中心化的控制。构建一个分布式的审计框架可以从根本上解决上述问题。区块链由于其不可篡改和不可否认的特性，在电子投票、拍卖和公平交易等领域被广泛用于取代第三方。用区块链取代TPA使得用户可以跟踪整个审计过程。因此，用户能够验证证据检索和备份的每一步。此外，区块链的去中心化提高了单点故障的容忍度。区块链是抵御共谋攻击和腐化攻击有前景的解决方案。此外，对于旨在保证数据可靠性的数据副本服务，云服务商可以故意删除副本以节省存储资源，而无需担心被监控到。受分布式存储网络(Distributed Storage Network，DSN)的启发，分布式存储网络试图构建一个点到点网络，允许单点买卖空闲存储资源，分布式数据备份使攻击者更难做出恶意行为，因为数据传输、存储和删除的每一步都是记录和可跟踪的。

## BOSSA方法及系统详细技术方案

我们提出了基于区块链的外包存储和审计(BOSSA)方案，这是一个可检索证明和复制证明的通用框架。BOSSA 将原始数据单独存储在服务器上，并将相应的副本存储在位于区块链的分布式网络的节点(也称为BOSSA中的农民)上，并通过智能合约检查它们的完整性。BOSSA可以自然地防御共谋攻击和腐化攻击，同时提供可视化的数据复制。BOSSA并不深度依赖像这样的特定共识机制，这使得BOSSA可以部署在图灵完备的区块链的离线网络上。BOSSA解决了以下三个挑战：

（1）时间限制证明：简单地将现有的可检索证明方案与区块链相结合无法实现我们的预期目标，区块链只支持简单的功能。区块链不能主动提出审计，只能根据收到的交易被动做出反应。该属性允许对手逃避审计。为了防止这种消极行为，我们利用区块以近似固定的速率上链的特性，提出了一个时间限制证明，迫使云服务商和农民节点提供数据可用性证明。

（2）激励机制：BOSSA组织农民节点存储用户数据的副本。但是农民节点并不完全可信，可能会随意离开网络，导致副本丢失，破坏副本的可靠性。为了解决这个问题，我们设计了一个激励机制来激励在必要时刻提供数据副本的节点。我们定义了一种奖励机制，在这种机制下，如果农民能够定期提供备份数据的有效证据，他们就会得到定期奖励。同时，部分奖励被暂时冻结，直到农民承诺的服务期满，这一设计在动机上阻碍了农民离开网络。为了进一步激励农民节点共享数据副本，我们定义了一个称为贡献率的度量，并将农民节点冻结的奖励与贡献率联系起来，只有贡献率为100%的农民才能得到所有的冻结奖励。

（3）隐私保护：像Ethereum这样的区块链平台大多以明文存储交易，任何参与者都能够检索交易的信息，包括智能合约的输入、中间计算结果等。对于一个建立在原生区块链网络的审计系统，区块链的开放性使对手能够记录证据并恢复原始数据。为了防止这种隐私泄露，我们结合了隐私增强技术来生成证明，同时确保它们的正确性。

### 2.2.1系统模型

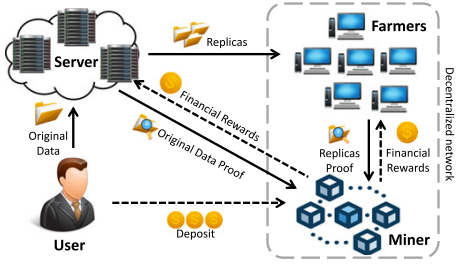


图2.1 BOSSA系统模型

如图2.1是BOSSA的系统模型。系统中包含以下实体：云服务商S，云服务用户U，分布式网络的两类节点：矿工M和农民F。矿工维护整个区块链网络，并执行智能合约。农民是加入到区块链网络中出租空闲存储资源的节点。在本系统中，服务商从用户中获得原始数据，用于数据分析，比如预测和推荐。为了节省服务商的存储资源，服务商将数据副本外包给农民，利用农民的空闲存储资源存储数据备份。用户委托矿工分别审计服务商的原始数据和矿工的备份数据。

BOSSA的核心功能流程如图2.2所示。

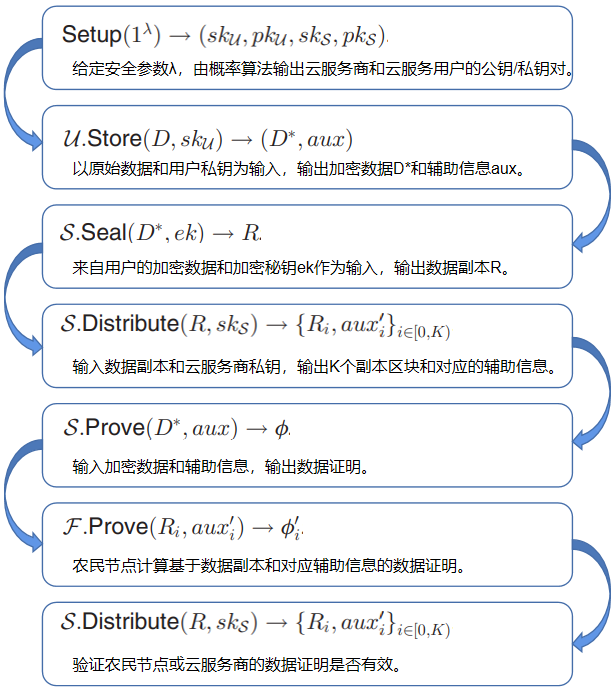


图2.2 BOSSA系统核心功能流程

### 2.2.2威胁模型

根据以前的工作我们以理性的云服务商为研究对象，其行为大多数时候遵守规则，除非恶意行为能带来更多的收益，例如删除很少访问的数据块以节省存储资源。区块链网络可以视为一个可信的公共实体。区块链的大部分算力由诚实的矿工掌握，他们会如实地执行智能合约。区块链网络中的任何节点都可以了解网络内部状态和区块链收到的消息。

来自分布式网络的农民节点出租他们的空闲磁盘空间来存储云服务用户的数据副本。我们假设有大量的农民节点，他们的数量足以存储所有用户的副本。如果农民失去了储存数据副本的兴趣，他们可能会不负责任地离开网络。因此，有必要保证副本的可用性，激励农民诚实地保存用户数据副本直到服务器满。

### 2.2.3 系统构建

BOSSA系统为数据完整性审计和数据备份提供了一个新的范例，它使用区块链网络定期审计服务器并存储数据副本。具体来说，为了确保服务器正确存储数据，BOSSA采用了传统的PoR方案，但用区块链代替了TPA。由于区块链只能被动地接收事务，不能向服务器发出质询，因此限时证明用于强制服务器主动提供证明。此外，BOSSA的另一个重要组成部分是在区块链网络中的节点(农民)之间存储副本。向农民节点发送数据备份会产生数据隐私、可靠性和可检索性安全担忧。在BOSSA中，服务器对数据副本进行编码和加密，以保证隐私和可靠性，激励证明鼓励农民节点保持了副本的完整性。此外，农民因提供有效数据证据(诚实地存储数据副本)，他们的回报取决于他们是否能在用户需要的时提供数据副本，这是通过贡献率来衡量的。100%贡献率的农民，可以取回自己所有的报酬。

### 2.2.4 审计算法

审计算法的设计和实现使用了一些密码学工具。如图2.2是BOSSA的功能流程。

（1）在Setup阶段，用户使用椭圆曲线加密算法，初始化秘钥对，并生成云服务商的密钥对。云服务商密钥对将随外包数据发送给云服务商。

（2）用户预处理数据后，再发送给云服务商。用户使用纠删码对原始数据编码，得到处理后的数据D\*。

（3）为保证数据副本的可用性，并保护用户隐私。需要对数据副本进行密封。如图2.3是对数据的密封示例。我们密封了22个区块中的22个（黄色区块和深灰色区块）。浅灰色区块为带有两个零填充的原始数据区块，暗灰色的区块由密封算法（Seal Algorithm）第一阶段生成，黄色区块由密封算法的第二阶段生成。我们省略了加密过程。这些数据的每一列都会外包给不同的农民节点。

（3）云服务商将过程（3）中的数据分为K块，生成不同的块副本和对应的辅助信息。并分发给不同的农民节点。

（5）云服务商和农民节点提供数据的可用性证明。

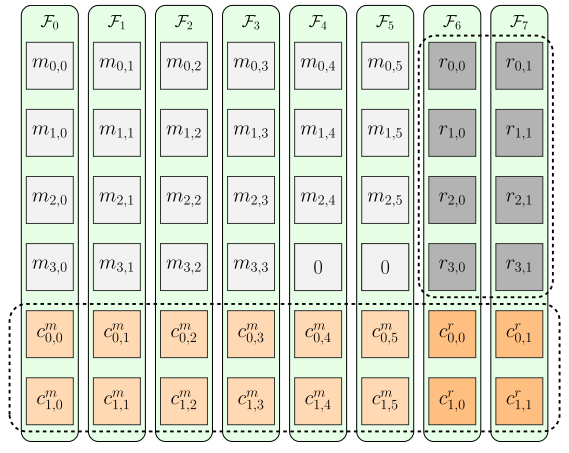


图2.3 数据密封示例

## 本方法的优点

首先，本研究利用Block以近似固定的速率上链的特性，提出了一个时间限制证明，迫使云服务商和农民提供数据可用性的证明。以此解决恶意节点逃避审计的问题。

其次，设计了一个激励机制来激励农民为用户在任何时候提供数据检索服务。在这种机制下，如果农民能够定期提供数据备份的有效证据，就会得到定期奖励。同时，部分奖励被暂时冻结，直到农民服务期满。为了进一步激励农民共享数据副本，我们定义了一个称为贡献率的度量，并将农民的冻结奖励与贡献率联系起来，这样只有贡献率为 100%的农民才能取得所有的冻结奖励。

第三，Ethereum等区块链平台以明文存储交易数据，任何参与者都能够检索交易的信息，包括智能合约的输入、中间结果等。对于建立在原生区块链上的审计系统，区块链的开放性使攻击者能够记录证据并恢复原始数据。为了防止这种隐私泄露，我们结合了隐私增强技术来生成证明，并确保证明的正确性。

# 区块链网络安全保障：攻击与防御

## 问题现状

随着区块链的快速发展与普及，其潜在的安全漏洞逐渐暴露出来。2020 年 7 月底，西班牙加密货币交易平台 2gether 遭攻击，损失约140万美元[1]。最近，在以太经典（ETC, Ethereum classic）平台上爆发的一起51%攻击导致大约价值 560 万美元的加密货币被双倍消费[2]。由此可见，区块链技术的漏洞可能导致无法挽回的财产损失和隐私泄露。目前，国内研究者针对区块链安全问 题进行了系统的综述[3-6]，但这些工作与本文的侧 重点和覆盖面有所差别。例如，文献[3]侧重于宏观 层面的区块链技术发展；文献[5-6]侧重于介绍区 块链威胁和漏洞相关研究，没有详细调研针对区块 链威胁的具体防御措施。

## 研究内容

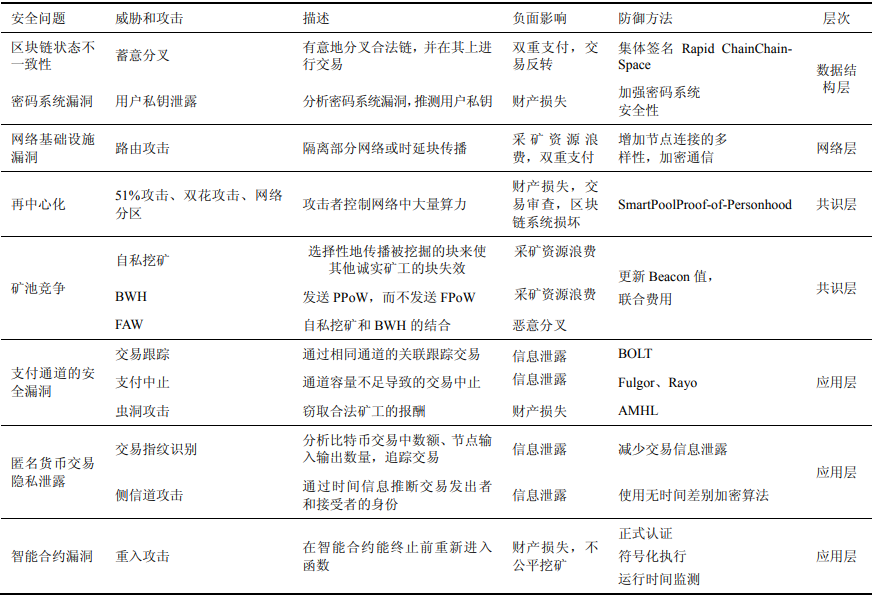
如表1，是区块链数据结构层、网络层、共识层、应用层面临的安全威胁。区块链的基本组成部分为区块。在交易过程中，不断有新的区块链接到区块链中，而链接过程存在区块链状态不一致和分叉的威胁。另外，区块链底层高度依赖密码算法，攻击者可以利用密码系统的漏洞造成用户私钥泄露，从而引发财产损失等安全问题。

在网络层，区块链网络的基础网络基础设施漏洞和自身 P2P 网络结构是引发安全问题的主要原因。

区块链的实现很大程度上得益于共识层的设计。在这一层中，区块链在一个分布式去中心化的账本上运行，链中的所有节点通过共识机制保持统一运行状态。目前，共识层中的大多数安全威胁都是随着矿池的出现而产生的。

在应用层，近期研究主要集中在提高性能和拓宽区块链系统的应用潜力上[7,8]，与之密切相关的安全问题包括支付通道的隐私和安全问题，匿名货币交易隐私泄露，智能合约漏洞等。

表 1 区块链安全威胁和防御方法



本研究针对对于区块链潜在的安全问题，提出了对应的安全策略。

在数据层面，区块的不一致性会引起区块链结构分叉等问题，而保证一致性会影响到区块链系统的运行效率，从而削弱可伸缩性。然而，为提高性能而设计的新方案可能会面临更严重的不一致性问题。为了提高交易的一致性同时保证高吞吐量，Syta等[9]提出了一种可扩展的集体签名协议Cosi来提高交易的确认效率。另一个提高区块链吞吐量的解决方案是分片[10,11] 机制，它将处理交易的开销分割为多个较小的节点组。

在网络层，为了防止路由攻击，从部署的角度划分，可以实行短期和长期对策[12]。短期对策更容易部署，不需要对协议进行任何更改。如果节点所有者能增加节点连接的多样性，攻击将变得极其困难。从长远来看，对比特币通信进行加密可以防止信息泄露。

在共识层，为了解决共识协议（例如工作量证明或权益证明）的再集中化问题，Borge等[13]提出了全新的个人身份证明机制（PoP, proof-of-personhood）并设计了一种名为 PoPCoin 的加密货币。

在应用层，近年来，大量工作致力于分析和提升链下支付通道的安全性。但是如何在保证效率的情况下设计出匿名性好的加密货币系统是目前学术界和工业界的一大挑战。智能合约的安全从多个方面加强，包括自动形式化验证、字节码级别验证、时检测重入攻击等。

## 研究优势

本文调研关于区块链安全漏洞的最新进展外，并详细介绍了目前最先进的防御方法，系统地调研了区块链系统的安全性问题。作为一个集成框架，区块链系统可分为4层：数据结构层、网络层、共识层和应用层。本文从区块链系统结构角度出发，深入分析数据结构层、网络层、共识层和应用层的安全漏洞、攻击原理以及对应的防御措施。

# 结论

本年度技术进展主要在2方面，包括跨链节点权限分级机制研究、链上加密数据的搜索与查询技术研究。分别提出了多链场景下数据跨链访问控制方法、一种可检索证明和复制证明的去中心化方法及系统，并研究了区块链网络安全保障相关的攻击与防御方法。此外，在跨链安全交互方面进行了详细的调查研究，初步设计了通用的跨链交互路由模型，为课题的后续研究提供基础。

## 参考文献

[1] GOGO J. European Bitcoin exchange hacked for $1.4 million, claims it cannot afford to repay users [EB/OL]. Bitcoin.com, 2020-08-04.

[2] HAIG S. 51% attack bleeds more than $5M from Ethereum classic [EB/OL]. Cointelegraph, 2020-08-06.

[3] 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.

[4] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.

[5] 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.

[6] 斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述[J]. 密码学报, 2018, 5(5): 8-19.

[7] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]//Symposium on Self-Stabilizing Systems. Berlin: Springer, 2015: 3-18.

[8] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 17-30.

[9] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities “honest or bust” with decentralized witness cosigning[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 526-545.

[10] GAO S, LI Z, PENG Z, et al. Power adjusting and bribery racing: Novel mining attacks in the bitcoin system[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 833-850.

[11] CORBETT J C, DEAN J, EPSTEIN M, et al. Spanner: Google’s globally distributed database[J]. ACM Transactions on Computer Systems, 2013, 31(3): 1-22.

[12] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: routing attacks on cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 375-392.

[13] BORGE M, KOKORIS-KOGIAS E, JOVANOVIC P, et al. Proof-of-personhood: redemocratizing permissionless cryptocurrencies[C]//2017 IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE Press, 2017: 23-26.