**北 京 邮 电 大 学**

**本科毕业设计（论文）开题报告**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 计算机学院（国家示范性软件学院） | 专业 | 数据科学与大数据技术 | | | 班级 | 2019211317 |
| 学生姓名 | 胡小蕙 | 学号 | 2019211742 | | | 班内序号 |  |
| 指导教师姓名 | 王祎 | 所在单位 | 北京邮电大学计算机学院（国家示范性软件学院） | | | 职称 | 教授 |
| 设计（论文）题目 | 去中心化金融中跨链安全监控系统设计和实现 | | | | | | |
| The design and implementation of a security monitoring system for cross-chain transactions in decentralized financial services | | | | | | |
| 毕业设计（论文）开题报告内容：（主要包含选题的背景和意义；研究的基本内容和拟解决的主要问题；研究方法及措施；研究工作的步骤与进度；主要参考文献等项目） | | | | | | | |
| 允许进入论文撰写环节：是 □ 否 □ | | | | 指导教师签字 |  | | |
| 日期 | 年 月 日 | | |

注：可根据开题报告的长度加页。

**选题背景与意义**

去中心化金融（DeFi）指的是使用去中心化基础（例如区块链、智能合约）设施构建的借贷和交易等金融服务。在该生态系统下，所有用户对其资产完全控制，通过点对点（P2P）、去中心化应用程序（Decentralized Applications, DApps）进行交互。去中心化金融将区块链技术与金融结合，充分利用区块链的透明性、无许可、分布式计算的特点。区块链上的开源的环境与智能合约能够使用户充分了解金融交易背后所有的清算、结算、撮合机制，掌握交易的底层逻辑，同时区块链的特性也保障了所有交易都可追溯与验证。

但目前，所有区块链都是在独立的环境中发展的，具有不同的规则和共识机制，这意味着他们无法进行原生性通信，代币也无法在区块链之间流动，不可避免地产生了价值孤岛。随着区块链行业的蓬勃发展，多个公有链、私有链、联盟链相继出现，各链的代币都被赋予了不同价值，在去中心化金融生态下产生价值壁垒，阻碍了系统的进一步发展。为了解决不同链的价值交换问题，跨链机制应运而生。跨链主要是指利用某些技术让价值跨越链的障碍，原本具有特定链上价值的代币能够转换为具有另一种链上价值的代币，从而实现价值流通。

然而近两年来，跨链安全事件频发，据统计，在13次单独的跨链桥黑客攻击中，有数十亿美元的加密货币被盗，其中大部分是今年遭受的损失。2022年2月，以太坊和Solana的链桥验证节点签名被伪造，造成损失超3.2亿美元；10月7日，全球最活跃的公链之一BNB Chain被黑客攻击，涉及资产价超5亿美元；10月11日，QANplatform跨链桥项目遭受黑客攻击，疑似因为私钥泄漏导致，共造成约190万美金的损失......截至2022年10月，跨链桥的攻击占被盗资金总额的69%。种种被攻击案例意味着跨链系统的项目繁杂，漏洞较大，机制不完善，黑客群体能够利用跨链漏洞造成巨额损失。

如何能对跨链系统进行实时的监控和预警显得尤为关键。目前的跨链系统亟需检测跨链交易行为，精准匹配出入链信息。只有准确感知可疑交易，才能及时阻止恶意操作并追踪黑客用户，从而降低金融损失。因此跨链系统的监控与预警工作对于提高区块链金融安全、加强生态监管有重要意义。

**研究的基本内容和拟解决的主要问题；**

本项目研究的基本内容包括区块链交易、跨链系统、跨链安全问题、监听系统设计等。

区块链的基础技术主要包括哈希运算、数字签名、P2P网络、共识算法以及智能合约。交易是区块链系统的核心，记录区块链上发生的一切内容，包括转账的完整信息、交易产生的时间以及链上位置信息、完成交易所需要的手续费等。

区块链的互操作性是一个突出的前沿研究领域，其目的是在原本孤立的区块链之间建立桥梁。跨链系统需要完成的工作主要包括代币交易、跨链通信传输、协议认证、可信验证等。跨链协议试图在两个区块链之间移动代币时提供一定的证明机制，例如基于哈希锁、单方或多方签名证明、侧链与中证机制、分布式私钥控制等技术。

若用户以合法流程完成跨链交易，是融合区块链金融的一大激励，有利于区块链生态的良好发展。但实际上当前主流的跨链桥项目机制并不完善 —— 无论在源链存人资金阶段、跨链通信验证阶段、目标链上用户提取资金阶段，都存在不同类型的漏洞。为了尽可能地在监听过程中对可疑跨链交易进行有效预警，需要首先对跨链安全问题进行总结，从而提取出此类交易的特征。

链上监听系统是通过实时收集链上数据，提取出感兴趣的部分。由于本项目以跨链交易作为监听任务对象，需要在不同链上同时提取数据信息，并在后端数据处理中心完成交易匹配与评估，最终实现风险预警。

本项目需要解决的主要问题在于以下5个方面：

1. 如何对跨链项目的源码进行完整语义分析；
2. 如何初步筛查出跨链历史交易中的问题交易
3. 基于大量的跨链项目，如何制定统一的跨链可疑行为认定标准；
4. 如何实时获取多条链上的交易数据；
5. 如何及时有效地提出警示。

**研究方法及措施；**

本项目采用调查与实践相结合的研究方法，基于forta技术框架与PostgreSQL设计并实现跨链监听系统。主要措施以及相关技术包括：

1. 调研跨链交易相关的论文、报告等，对于跨链交易的原理与技术展开理论性学习，从而掌握跨链交易流程与设计机制。
2. 通过阅读主流跨链桥项目的官方文档和项目源代码，对其进行完整的架构分析。以及智能合约的语义解析。进一步梳理所有跨链桥项目的关键信息，包括合约地址、调用方法、触发函数等。
3. 使用开源跨链桥项目的完整体系，在测试链上完成部署与调用，实践跨链桥项目的交易流程。
4. 基于常用区块链浏览器etherscan与chainbase的API，以及geth节点，使用已解析的桥项目逻辑收集多条链上的跨链交易数据，并完成出金-入金交易的匹配，将完整资金流信息存入数据库。
5. 通过计算匹配后的出金-入金额度差值，初步将差值较大的交易定为可疑交易行为，提取该部分交易的特征。
6. 基于可疑交易特征拟定预警逻辑，在历史数据中进行回测，提高预警逻辑的准确率。
7. 学习使用forta技术框架，实现链上监听，实时收集多链数据并完成跨链交易的匹配，随后使用已制定的预警逻辑分析当前交易，及时警报风险交易。

**研究工作的步骤与进度；**

为了建立可信的跨链监控系统，有效解决上文提出的研究问题，本项目将依据以下计划逐步实现：

1. 2022.11 - 2022.12，学习并掌握跨链交易流程；调研主流跨链桥项目并完整解析。
2. 2022.12 - 2023.01，收集多链上的跨链交易入库；精确匹配出入金行为，建立完整资金流；初步筛查出可疑交易。
3. 2023.01 - 2023.02，分析可疑交易的行为特征，进一步制定预警标准；同时实时收集跨链交易信息。
4. 2023.02 - 2023.04，建立完整的跨链监听系统，对跨链交易进行实时分析，完成风险预警。
5. 2023.04 - 2023.05，测试系统，从处理时间、预警准确率等方面提升系统性能；完成毕业设计相关文书等。

**主要参考文献等项目**

1. Herlihy, Maurice, Barbara Liskov, and Liuba Shrira. "Cross-chain deals and adversarial commerce." The VLDB journal 31.6 (2022): 1291-1309.
2. file:///Users/phoenixhu/Downloads/Open\_problems\_in\_cross-chain\_protocols.pdf
3. Shadab, Narges, Farzin Houshmand, and Mohsen Lesani. "Cross-chain transactions." 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.
4. Robinson, Peter, Raghavendra Ramesh, and Sandra Johnson. "Atomic crosschain transactions for ethereum private sidechains." Blockchain: Research and Applications 3.1 (2022): 100030.

**暂定**

扩展而言，跨链也能够传输不同链之间的信息，实现信息交换，最重要的是能够释放不同链的潜力，让更多的用户参与，让更多的链相互流通，最终形成一个和谐发展的大生态，一个具有高度价值的去中心化互联网。

为了及时检测可疑跨链交易，本课题拟提出一种能实时监控跨链安全的系统和方法。通过对跨链安全中关键行为的识别和提炼，能实时感知和发现跨链可疑交易，减少金融损失，完善区块链监管，增强整个生态安全性。

跨链桥作为区块链重要基础设施，发挥着重要作用。首先，跨链桥能转移不同区块链之间的资产和信息；其次，用户群体以及去中心化应用（Decentralized Apps，DApps）通过跨链桥可疑利用各种区块链的优势，降低交易的附加成本，便利去中心化金融的发展；此外，跨链桥的存在使得不同区块链的开发人员实现技术融合，协作发展。

。这些创新性协议在理论上提供了强大的隐私与安全保证，但在实际应用中仍然存在较严重的漏洞。

举例来说，Alice的全部资产均为存储在Ethereum链上的ETH，现在希望购买BSC链上Bob的一部分BNB资产，需要有一个交易中介来完成。跨链桥作为中介，会在不同的链上发布项目本身支持的、不同于ETH和BNB的另一种货币（例如anyETH），但是该货币在链上没有实际价值。Alice需要在Ethereum链上与中介进行货币兑换，按照汇率将自己的ETH兑换为；中介确认Ethereum上的货币兑换流程无误后即向BSC链发起通信，内容包括Alice的账信息以及需求等；BSC链上的中介接收到信息后进行严格验证后，再次按照汇率给Alice发放一定的BNB。Alice于是获得在BSC链上的资产，可以与Bob直接进行交易。

具体地，需要对区块链上智能合约的部署与调用、区块链监听方案、跨链系统项目、跨链可疑行为感知、跨链金额可靠计算等内容展开深入研究。

1. 依据已梳理的项目逻辑，对不同链上的信息进行匹配，即完成同一笔跨链交易出金-入金的精确匹配。
2. 数据收集与筛查、恶意交易行为分析、搭建系统实现链上监听、

采用基于已有的跨链桥进行解析，收集对应的历史跨链交易数据，筛查出可疑的交易记录，从已知本项目需要通过跨链桥项目的深入调研、历史数据的收集与匹配等工作，筛选出