大连理工大学软件学院毕业设计（论文）开题报告

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **姓名** | **赵焓超** | **学号** | **201992183** | **题目类型** | □校内工程 ☑校内研究  □校外工程 □校外研究 | | | |
| **班级** | **1901班** | **专业** | **软件工程** | **开题日期** | **2023年 2月5日** | | | |
| **联系电话** | | **15132201741** | | **E-mail** | **1664637635@qq.com** | | | |
| **中文题目** | | **一种区块链系统中数据存储模块的研究与实现** | | | | | | |
| **英文题目** | | **Research and implementation of a data storage module in blockchain system** | | | | | | |
| **外文翻译题目** | | **LBFT: An Asynchronous Committee-Based Blockchain Storage Strategy on Zero Trust Model** | | | | | | |
| **外文翻译期刊名称、出版年月** | | **Electronics 2022年12月** | | | | | **是否近五年期刊论文** | ☑是  □否 |
| **校内导师姓名** | | **姜国海** | | **职称** | **工程师** | | | |
| **题目来源** | | ☑科研项目 □工程模拟 □实际应用 □自拟课题 □其他 | | | | | | |
| **校外导师信息（校外题目填写，校内题目以下三行不必填写）** | | | | | | | | |
| **校外导师姓名** | |  | | **职务/职称** | |  | | |
| **所在单位** | |  | | | | | | |
| **联系电话** | |  | | **Email** | |  | | |

**一、选题的依据（**不少于1000字**）**

|  |
| --- |
| **1.1 选题背景与应用价值（**题目来源、理论意义或工程背景、应用价值等**）**  当今时代是信息化时代，电子数据这个时代的产物。电子数据具有易创建、易存储、易传输和高利用率等特点，比如我们可以很容易的通过网络给任何地方的友人发送信息，我们可以云盘进行备份一些重要的信息，我们还可以和公司签署电子合同等等，但是如今常用的数据存储模式还存在容易受到攻击、存储成本较高、中心化系统带来的泄密风险、不信任实体间难以达成共识等问题。  区块链由于其去中心化、不可篡改性的特点，能安全有效的降低新任成本且安全的存储数据，它将数据关键信息锚定在主链上，同时控制了不同用户对电子数据的访问权限，有效解决了电子数据存证存在的安全问题[5]；同时密码学的基础，保证了攻击者在现有计算能力的前提下几乎不可能攻击成功[2]。在某些特定的场景比现有的存储结构更加优秀，比如品质溯源，随着我国居民消费水平的全面提升，对农产品、婴幼儿奶粉、生鲜、保健品等食品及其它重要产品的安全性、信息透明性、查询便捷性提出了更高的要求，传统的溯源系统需要一个中心化机构存储(源头企业或品牌方)，但因为利益相关无法保证溯源信息不被篡改，并且传输过程也需要特别保护，这就无法得到人员的完全信任，而区块链就可以通过上述特点很好解决这个问题；再比如数字存证，也就是我们提到的电子合同、版权保护、商业机密保护、电子发票等；除此以外，还有数字金融、政务协同、信用网络、保险科技等诸多应用场景。  因此，研究区块链系统中的数据存储模块的实现是很有现实意义的。 |
| **1.2 国内外研究现状分析（**通过文献综述，分析国内外相关研究进展、存在的问题、技术方案选择依据等**）**  当前的区块链应用存储数据有五种：  第一种：把一切都存在区块链里。目前，大多数简单的去中心化应用程序都以这种方式工作。这是实现数据存储最简单粗暴的方式，但存在确认缓慢、信息不可变以及容量问题，这种数据存储方式虽然实现简单，但并不是一个好的选择  第二种：P2P文件系统：如IPFS[1]，IPFS允许在客户端计算机上共享文件，并把它们整合到全局文件系统中。这个技术整合了分布式哈希表、BitTorrent、Git和自验证文件系统4种技术的优点。用DHT实现内容检索；借鉴BitTorrent，实行分块存储、分块传输和奖励机制；Git中应用的默克尔DAG使得大文件分享、修改变得简单高效；而自验证文件系统确保了数据发布的真实性。比如由Juan Benet建立的协议实验室（Protocol labs）开发的FileCoin，致力于实现一个存储人类社会最重要信息的分布式网络  第三种：去中心化的云文件存储，还有一些去中心化云文件存储，它们去掉了 IPFS 的一些限制。区别在于内容是托管在用户的计算机上，而不是在数据中心里，这些用户出租硬盘空间而已。例如，Sia，Storj，Ethereum Swarm。但是它们只提供静态文件，也没有内容搜索，还因为它们都是建立在租用的硬件上，所以不是免费的  第四种：巨链数据库：它声称可以解决数据存储和交易速度问题。它也是区块链，拥有巨大的数据容量和非常快的交易。巨链数据库建立于RethinkDB集群之上，并用它来存储所有的区块和交易。它是基础no SQL数据库中的其中一个。所有的巨链数据库节点（用BDB 表示）连接到集群，拥有对数据库的完全写访问权限。但是有一个很严重的问题：整个巨链数据库不是拜占庭证明的！任何恶意的BDB都可以破坏RethinkDB集群。但是无论如何，它对私有区块链很有用。  第五种：Ties DB：这是目前好的公共数据库的可选项。最接近理想的是no SQL数据库。它们唯一缺乏的是拜占庭容错（Byzantine fault tolerance）。Ties.Network数据库：Ties.network 是对 Cassandra 数据库的深度修改，提供了一个更好的解决方案：TiesDB 继承了基础 noSQL 数据库的大部分功能，并增加了拜占庭容错和激励。有了这些功能，它可以成为公共数据库，并通过智能合约在 Ethereum 和其他区块链上启用功能丰富的应用程序。任何用户都有数据库写入权限。但是，用户由他们的公钥识别，同时，所有的请求有签名。创建之后，记录记住它的创建者，创建者则成为记录的所有者。之后，记录只能被记录所有者修改。每个人都可以阅读所有的记录，因为数据库是公开的。根据请求和复制检查所有的权限。额外的权限可以通过智能合约管理。  上述五种存储方式各有利弊，并且研究成果都很有参考意义，本系统会在上述研究的基础上开展，选择一种合适的数据存储方式。 |
| 1.3 参考文献（不少于8篇参考文献，格式参照论文模板中参考文献要求）   1. 董天一,戴嘉乐,黄禹铭.IPFS原理与实践[M].北京:机械工业出版社,2019:2-15. 2. 梁保陈,张兴兰. 基于改进区块存储结构的高效数据检索模型[J]. 计算机科学与应用, 2021, 11(4), 803-813. 3. 李兆森,李彩虹. 基于区块链的电子数据存证应用研究[J].软件, 2017, 38(8): 63-67. 4. 马舒婕. 基于区块链的存储结构的设计与实现[D].天津大学,2018. 5. 冒小乐,陈鼎洁,孙国梓.基于区块链的电子数据存证的设计与实现[J].中兴通讯技术,2018,24(06):28-34. 6. 张晓蝶. 基于区块链的农产品溯源数据存储技术研究[D].河北地质大学,2022. 7. JD Chain开发文档[EB/OL]. https://ledger.jd.com/doc/ 8. Du Zhengyi and Gong Junqing and Qian Haifeng. LBFT: An Asynchronous Committee-Based Blockchain Storage Strategy on Zero Trust Model[J]. Applied Sciences, 2022, 12(22): 11790-11790. 9. Feng Hangwei and Wang Jinlin and Li Yang. A Blockchain Storage Architecture Based on Information-Centric Networking[J]. Electronics, 2022, 11(17): 2661-2661. |

**二、研究内容和方法（**不少于1000字**）**

|  |
| --- |
| **2.1 研究内容与目标（**研究内容、研究目标、技术指标等**）**  本系统旨在实现非信任实体间的数据交换，要保证数据的一致性，重难点在于非信任实体间数据一致性的问题，也就是拜占庭将军问题。  基于研究目标，涉及的研究内容有：区块链、默克尔树、区块结构、智能合约、分布式存储，JD Chain的搭建与部属。 |
| **2.2 拟采取的研究方案（**需求分析、理论与技术方法、软硬件开发平台参数、技术路线等**）**  系统使用JD Chain，计划实现一个能让非信任实体间达成共识的系统。  重点需求在于，利用区块链系统的去中心化，不可篡改的特性，通过合适的共识机制，编写合适的智能合约，保证电子数据传输过程的透明，也就是非信任实体发出电子数据的真实可信。  预计在VMware中搭建一个CentOS 7的虚拟机环境，然后在此环境下完成JD Chain的部署，并以此为学习平台，参考JD Chain的开发文档，学习JD Chain的使用方法、设计理念，然后以此为基础，实现一个符合需求的系统。 |
| **2.3 预期成果与创新性（**成果形式、代码量、创新性**）**  预期成果将以系统及其核心代码进行展示。在区块链中实现特定情况下数据的存储，比如品质溯源、电子合同、数字金融等等。  此外，在加密算法，共识机制以及智能合约方面进行不断尝试，试图寻找一个较好的组合，让整个系统的可用性更高，实用性更好  本系统能够用于特定信息的存储，具有以下创新意义：  1）通过区块链的去中心化，不可篡改性特性，建立一个去中心化的数据存储平台。  2）利用恰当的共识机制和智能合约使系统更加合理。  3）充分考虑各方需求，让不同需求的用户能够各取所需。 |
| **2.4 进度计划（**按照“周”展开工作计划，不少于18周**）**  **第一阶段：需求分析**  第 1 周：查阅相关资料；理解系统需求，参考相关算法及研究内容，按模块记录笔记。  第 2 周：查阅文献，完成外文资料的翻译。  第 3、4 周：根据JD Chain文档，在虚拟机环境下学习与搭建JD Chain，并计划整体系统架构。  **第二阶段：系统设计**  第 5、6 、7周：学习智能合约以及共识机制相关知识，寻求一个适合系统的解决方案。  第 8、9 周：完成系统的概要设计：系统结构设计和用户接口设计；完成结构设计文档和用户接口设计文档；同步学习相关技术。  第 10 周：完成系统的详细设计，包括共识机制，智能合约相关内容。  **第三阶段：系统实现**  第 11、12、13 周：完成代码编写。初步搭建系统  第 14、15 周：单元测试、模块测试、集成测试与修改；修改 Bug；进一步完善系统。  **第四阶段：成果总结**  第 16 周：对整体系统进行总结；完成毕业论文初稿。  第 17 周：修改毕业论文与其他要求文档；总结成果，制作答辩 PPT 初稿。  第 18 周：完成毕业论文终稿；完善各种文档资料；完成答辩所需 PPT。  第 19 周：准备答辩稿、排练。 |

|  |  |
| --- | --- |
| 指导教师意见：  签字： 年 月 日 | |
| 考核成绩 | **□**通过  **□**不通过 |

备注：1、考核组织：由各个系自行组织安排，成绩由指导教师或考核小组给出。

2、考核结论：考核成绩分为通过与不通过两种。

（1）对于不通过者需指出主要问题，导师帮助其分析原因，提出相应的改进措施，待修改完成后再次进行开题。

（2）未提交开题报告及二次考核不合格者，将延期答辩。

3、各个系将开题考核结果及开题报告统一汇总到教务员处。