开题报告

1. 选题依据

1.1. 选题理由

计算机科学技术的迅猛发展，令互联网经历了“只读”的 Web 1.0 时代和可读可写的 Web 2.0 时代。Web 1.0 时代是专家织网的时代，只有精通计算机技术的专家们才有能力编写网页源代码并架设到服务器上，普通用户只能被动地浏览网页而没有参与网页建设的能力。即使是这样功能受限的互联网，也激起了众多开发者和网名的热情。紧接着，随着 Web 2.0 时代的到来，即使是未掌握任何计算机高级知识的普通用户不仅能轻松地浏览互联网上的海量信息，亦能轻松地修改这些信息。例如，用户可以制作自己的博客，分享自己的所见所想；在影片和音乐下进行评论，抒发自己的所思所感。这种发展趋势也深刻地影响了当时主流操作系统的开发路线图，纷纷将网络功能加入到了各自的内核中。例如，原本未装载网络功能的 Unix 操作系统在 Unix v1 版本中正式加入了网络功能支持；12 年后，DOS 操作系统在其 3.1 版本中增加了网络网络功能支持。这一划时代的革命将开发者从繁重的重复工作中解放了出来，他们不必再为自己的应用程序实现完整的网络栈，更能专注于业务逻辑上，从而大大解放了生产力。

然而，直至 Web 2.0 时代，数据大多仍存放于各大技术公司的中心服务器中，这种集中式、非透明公开的存储方式在越来越强调隐私保护和过程透明的当下受到了越来越多的质疑和批评。Web 3.0 时代正是为此而来，它旨在创造一个去中心化的互联网，将数据存储在网络中的众多计算机（称之为节点）中而非中心化的服务器中。人们可以在没有第三方机构参与的前提下安心地进行点对点的数据甚至资金交换，而不用担心抵赖、数据意外泄露等问题。Web 3.0 时代的技术基础正是区块链技术。作为一种革命性的分布式账本技术，区块链技术采用链式数据结构保存数据，它采用密码学方法对链上数据加以保护、应用共识算法使得存储分布式账本的计算机能就链上状态达成共识，从而提供了去中心化、极难篡改、极难抵赖等优秀特性。若将互联网称为 Web 1.0 和 Web 2.0 时代的基石，那么区块链技术就是 Web 3.0 的基石。

然而，市面上流行的绝大多数操作系统并未在内核层面迎接 Web 3.0 时代的到来。与复杂的网络协议栈类似，从零开发区块链实现也可能为开发者带来沉重的心智负担。经过一定程度的抽象，区块链可认为由数据存储模块、点对点网络支持模块、共识算法模块、交易排序处理模块和加密算法模块构成，它们一般是紧密耦合的子系统，并且很难解耦。倘若其中的某几个子系统存在缺陷，这些难以发现的耦合可能严重破坏区块链系统本身。因此，目前主流的做法是从成熟的区块链方案，例如比特币和以太坊的源代码出发，定制不同的区块链。然而，受制于它们的母本特性，这种定制的能力较为有限，可拓展性一般，也不符合操作系统需要在硬件性能差异很大，并根据需要提供不同服务的特点。因此，设计一种方法，将可高度定制的模块化区块链融入操作系统的系统调用中，让上层应用开发者可以像调用操作系统网络功能一样调用区块链相关的各项功能，成为了操作系统迈向 Web 3.0 时代的一项严峻挑战。

本研究旨在探索如何将区块链技术深度融入操作系统，构建一个支持区块链技术栈的操作系统内核。这种新型内核旨在为运行该操作系统的设备带来较为完整的区块链功能，从而全面提升上层应用开发者开的分布式应用开发体验；同时，内核自身也能利用区块链功能提供的优良特性保护自身，例如利用不可篡改性保护重要文件不受修改，利用不可抵赖性记录应用程序调用系统调用的记录等，为互联网与操作系统行业的健康、可持续发展提供技术保障。

1.2. 研究意义

- 理论意义
  - 当前，区块链技术的应用主要集中在数字货币、金融交易、供应链管理等领域。本研究将区块链技术引入到操作系统内核层面，这种全新的应用尝试和理论探索有助于深入发掘区块链技术在系统底层的安全防护机制，从而丰富和发展区块链技术的应用理论。

- 相比起传统物联网系统的安全措施，本研究旨在利用区块链技术解决物联网设备的安全问题，该方案的建立和完善，不仅可以为物联网安全提供一种新的理论框架，也为其他相关领域的安全性研究提供了参考和借鉴。
- 本研究涉及到物联网、操作系统、区块链等多个学科领域，是对这些领域交叉研究的重要尝试。通过这项研究，我们可以深化对这些领域之间相互作用和影响的理解，推动相关学科理论的发展和融合。

- 应用意义
  - 区块链的去中心化提高了系统鲁棒性，使其在部分设备不能正常工作时仍然保持稳定可用；不可篡改性则极大程度上避免了数据被损坏或恶意篡改，保证了物联网设备采集和存储之数据的可信度。因此，将区块链技术融入物联网操作系统内核，有利于改善物联网系统的整体安全性。
  - 内核态程序可以直接访问硬件资源和执行特权指令，无需通过系统调用进行上下文切换。因此，将用户程序改写移植为内核程序，有利于降低性能开销，为提高高负载任务的执行效率提供除针对任务本身进行优化的新途径。

1.3. 国内外研究现状与发展趋势

1.3.1. 现阶段区块链技术的应用场景

多项研究表明，区块链技术在诸如城市管理 [1]，能源系统 [2] 等领域有相当大的潜力。雄安新区区块链实验室于 2020 年发布的雄安区块链底层系统（1.0）是我国首个城市级区块链底层操作系统。该自主可控的底层平台采用分层多链结构，将网络系统划分为核心链和应用链，旨在构建城市级的可信基础设施。为避免资金在使用过程中的截留或者挪用风险，实验室开发上线了政府投资项目资金管理区块链系统，用区块链上的信息流驱动资金流，从而将数字人民币和区块链技术深度融合，以实现资金的精准拨付、及时拨付和透明拨付。该底层操作系统对智能合约亦提供了支持，可以在满足条件时自动触发一些逻辑，例如在每月月末自动结算水电费等，以方便自动管理居民日常起居开支。

1.3.2. 区块链技术在消费级设备上的应用

目前大多数区块链节点是专门设计用于挖矿的计算机，然而诸如手机和可穿戴设备的消费级设备也可能也应当成为区块链网络中的一部分，尤其是在充电时 [3] 。截至 2017 年，全球一共有 7 亿台正在运转的移动设备，其中 44% 的设备都是智能手机 [4] 。

1.3.3. 区块链操作系统 LibertyOS

LibertyOS 是世界上第一个区块链操作系统。LibertyOS 结合了区块链技术和加密货币技术，为操作系统用户创造了新的用户体验。LibertyOS 的创始团队认为，现代操作系统将客户视为商品，可以出售给广告商和其他非政府组织或政府组织。像 Windows 和 macOS 这样的现代操作系统正在客户不知情的前提下从他们那里收集信息，甚至访问和操作用户的所有文件和数据。而 LibertyOS 为这种情况提供了一个解决方案。LibertyOS 由操作系统的用户 100% 拥有。没有必要连接到任何公司，所有的数据都是 100% 你的。另一方面，LibertyOS 也为广告客户提供了接触他们客户的途径。这是通过一个点对点令牌模型完成的，该模型直接向广告的观众支付费用。LibertyOS 的本地令牌是 LIB 令牌。广告商必须支付 LIB 令牌和用户收到观看广告的 LIB 令牌。然后，用户可以使用这些 LIB 令牌向他们喜欢的项目捐款，这样就可以激励创建一个开放自由的开发者社区。然而，LibertyOS 对现代操作系统的改良尚且停留在用户程序层面，它注重保护用户数据隐私安全性和提升用户体验，而并未使用区块链的优良特性对操作系统内核加以保护。

1.3.4. NEAR 区块链操作系统

NEAR 在诞生之初只是一组普通的区块链协议。NEAR 团队将他们的协议设计得简洁而灵活，并以三大特点博得了超 10 亿用户的青睐：易懂的账户表示法，Nightshade 分片法和开发者友好的 JavaScript 开发套件。在日益风靡的 Web 3.0 浪潮下，NEAR 团队与时俱进地将他们的协议升级为操作系统。

1.3.5. 系统调用

Linux 内核建议的增添系统调用的场合：https://www.kernel.org/doc/html/latest/process/adding-syscalls.html?highlight=syscall_define

> 思路：syscall，密码学

2. 研究内容

工作分为三阶段展开。

第一阶段针对 Substrate Node Template 项目（下称节点模板项目）展开。官方模板，具备所有基本机能。同时对项目代码和依赖软件包进行分析。

第二阶段针对 rCore 进行完善工作。（rCore 的简要介绍）。将必要的依赖引入 rCore，为后续区块链机能的引入打好基础。完成后，节点模板项目应当可以作为用户程序在 rCore 中运行。

第三阶段，将节点模板项目放入内核并为 rCore 增添新的系统调用。哪些系统调用？

3. 研究方案

文献研究法：知网、arXiv 和导师推荐的文献资料进行学习，了解操作系统和区块链有关的基础知识，确保研究工作在一定的理论基础上设计而成，具备研究价值和借鉴意义。

实验研究法：对用户态和内核态的节点模板进行测试，对比它们实现同样的功能所需的代码量、运行性能等

4. 研究工作进度安排

5. 预期研究成果

rCore-Blockchain 实现。增添新的系统调用，用户程序可以直接调用这些系统调用实现：

- 账户创建、交易
- 智能合约部署和运行
- 对等节点通信

6. 本课题创新之处

7. 研究基础

7.1. 与本项目有关的研究工作积累和已取得的研究工作成绩

rCore 教学版实验。

本科毕设，Substrate 初步使用。

7.2. 已具备的实验条件，尚缺少的实验条件和解决的途径（包括利用国家重点实验室和部门开放实验室的计划与落实情况）

7.3. 研究经费预算计划和落实情况

参考文献

[1] S. A. Bagloee, M. Heshmati, H. Dia, H. Ghaderi, C. Pettit, and M. Asadi, “Blockchain: The operating system of smart cities”, *Cities*, vol. 112, p. 103104, 2021, doi: 10.1016/J.CITIES.2021.103104.

[2] D. K. Fyaritovich and M. C. Vasilyevich, “The role of blockchain technology in improving the efficiency of fuel & energy companies”, *International Review*, 2022, doi: 10.5937/intrev2202101k.

[3] A. Ometov *et al.*, “An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends”, *IEEE Access*, vol. 8, pp. 103994–104015, 2020, doi: 10.1109/ACCESS.2020.2998951.

[4] Cisco, “Global mobile data traffic forecast 2017–2022”, 2019.