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相较在用户模式下可能发挥的更多价值，从而丰富和发展区块链技术的应用理论。

- 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。进行这项研究，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
  - 本研究旨在将区块链服务引入操作系统内核。该方案的建立和完善，可以极大改善上层应用程序开发者的开发体验。他们无需自行实现底层协议、点对点网络、数据存储等区块链协议栈，而是可以让操作系统内核为之代劳，从而将更多的精力投放在分布式应用程序的业务逻辑上，减轻重复且不必要的心智负担。
  - 内核态程序可以直接访问硬件资源和执行特权指令，无需额外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，有利于减少上下文切换成本，进而降低性能开销，为提高高负载任务的执行效率提供除优化任务本身以外的新途径。

1.3. 国内外研究现状

1.3.1. 区块链技术现阶段应用场景

多项研究表明，区块链技术在诸如城市管理 [1] 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用、划拨工人工资等，实现了居民日常收入开支的自动化管理，在免去冗杂人工操作的同时也避免了拖欠费用的情况 [2] 。

1.3.2. 区块链技术在一般算力设备上的应用

目前，大多数区块链节点是专门设计用于挖矿的计算机。然而截至 2017 年，全球一共有 7 亿台活跃运行的移动设备，其中 44% 都是智能手机 [3] 。这些设备因为单体算力和续航力有限，无法参与到未经优化的区块链网络中，从而导致这种单体性能一般但保有量巨大的算力资源大量浪费。为此，文献 [4] 提出了一种综合了 PoW、PoS 和 PoA 的共识算法，并在全球范围内的 2000 余台设备上进行运行测试。在测试中，该新型综合共识算法对电池的消耗量仅为基于工作量证明算法的$\frac{1}{8}$，证明了利用移动设备进行区块链网络加速方案的可行性。

此外，物联网技术尤其是工业物联网技术的迅速发展带来的异构设备问题和高可用性要求也阻碍了区块链技术在这些行业中的应用。异构设备问题，是指物联网系统中设备种类繁多，性能参差不齐的问题，这将导致在所有设备上部署相同的区块链节点变为不可能。高可用性要求是工业物联网的特点之一，它要求物联网系统始终可用，在系统状态发生变化时立即做出反应。而区块链上各个节点繁重的哈希计算和共识过程将大大延长系统对突发事件的反应时间。

文献 [5] 创新型地提出了一种区块链系统架构。该架构将整个系统划分为多个单元，每个单元中有一个性能较好的代表节点，它负责收集该单元中所有物联网设备的数据，并代表单元中的所有设备参与到区块链的运行中来。并且，该文献也提出了一种轻量级哈希密码学方法，根据链上积压的交易数量判断链上负载情况，以此动态地调整当前使用的哈希算法。实验数据显示，当交易体积达到 7MB 时，其耗时仅为三种哈希函数中安全性最高的 SPONGENT 算法的$\frac{1}{5}$；而当交易体积较小时，该算法又能从 QUARK 和 PHOTON 哈希函数中选择最适应链上压力的一种进行计算，在安全性和高效性中取得了较好的平衡。

1.3.3. RISC-V 与区块链技术

RISC-V 是开源的指令集架构，其目标是创建一个开放的、平价、高性能的芯片架构，以替代繁冗的 x86 指令集和闭源的 ARM 指令集。

RISC-V 指令集与区块链技术的结合点之一是开发区块链虚拟机。区块链系统可以视为一台巨大的状态机，其支持的区块链虚拟机则提供这台状态机的运行环境，并于其上制定状态机的状态转换函数。

目前，区块链虚拟机有两条主流的技术路径：以太坊虚拟机和 WebAssembly。EVM 为以太坊及其衍生产品所支持，它首创了区块链虚拟机技术，使得开发链上自动执行的业务逻辑（即智能合约）成为现实，但面领着严峻的性能问题和设计安全问题。WebAssembly 技术的本意是用浏览器可执行的二进制字节码编写程序，辅助 JavaScript 实现更高性能的浏览器环境下的程序执行效率，后由 Polkadot、Near 和 Cosmos 等区块链项目提供支持，成为了区块链虚拟机实现方案的一部分，它也同样面领着加载速度慢，无法满足区块链虚拟机性能要求的困扰。

针对这种情况，Nervos 利用 RISC-V 指令集开发了 CKB-VM 虚拟机。使用真实存在的 CPU 指令集，而非某种中间语言开发虚拟机的优势在于：任何支持 RISC-V 架构的编程语言，例如 C、Rust 和 JavaScript 都可以原生用于 Nervos 开发，区块链中的复杂操作，比如推出新的密码学原语，将变得就像添加一个新库一样简单。此外，由于指令无需中间代码即可转换为 CPU 能高效执行的汇编代码，使用 RISC-V 开发虚拟机还能规避中间代码带来的限制，使得语义更加灵活精准。

得益于 RISC-V 的开源性，构建完全自主可控的区块链软硬件系统成为了可能。2021 年 1 月 27 日，国内首个自主可控区块链软硬件技术体系长安链正式发布。硬件上，长安链节点采用基于 RISC-V 架构设计的 96 核专用加速板卡，令数字签名及其验证的速度提升了 20 倍，智能合约处理效率更是达到了原先的 50 倍之高。软件上，长安链通过协作网络建设了信息通信链、食品安全链等一系列数字化可信基础设施，实现了冷链溯源、物资采购管理、漫游跨境运营商数据追溯等功能，为我国数字化转型增添了一份坚实的力量。

1.3.4. 区块链与操作系统的融合领域发展现状

现阶段的主流区块链大多以用户程序的形式运行在 Linux 和 Windows 操作系统下。由于用户程序并不一定随系统启动且可以被用户随意启动关闭，这种区块链形式不一定能保证节点的在线时长，从而与区块链社区需要尽可能吸引新用户（即新的节点）加入网络建设，并留住已有的节点贡献者的宗旨相违背[1]。基于区块链的操作系统能够保证节点在系统工作时始终在线，从而为区块链网络的稳定运行提供保障。

再者，无论区块链网络本身的去中心化程度如何，用户始终需要某种“前端”（分布式应用程序，dApps）来和区块链“后端”（通常包含区块链网络及其上运行的智能合约等基础设施）交互，而前端的代码来源仍然是中心化的，例如从代码托管网站或软件下载站上获取。这造成了一个尴尬的情况：想访问去中心化网络，用户必须先通过中心化网络下载软件。这种需要额外前置步骤的实践会带来一定的风险。例如信任中介问题。区块链操作系统打破了这一局面，用户可以直接从操作系统中访问或开发 dApps 而无需额外从中心化网络中获得任何软件。所有 dApps 的代码和存储均位于链上，从而彻底将中心化网络排除在去中心化网络之外。

区块链操作系统的概念定义尚有争议，一种较为流行的观点认为，区块链系统是一种网络操作系统，用户在设备上发出的指令被传送到云端的区块链网络上，进行身份验证、程序执行等操作后，结果数据将被返回给用户。NYNJA 公司与 Amgoo 智能手机制造商建立了战略合作关系，以支持其基于区块链的 NYNJA 虚拟操作系统 (vOS)。这两家公司将与拉丁美洲的电信运营商合作，在设备激活时为 NYNJA vOS 用户提供初始数据块。vOS 支持提供文本、语音、视频会议和项目管理工具的通信层，用于商业交易的安全支付层，以及支持比特币、以太坊和所有 ERC-20 兼容代币的多币种钱包。在这种架构中，诸如挖矿等计算量大的任务在云端完成，移动设备仅负责发出操作请求和接收计算结果。

区块链操作系统的另一种定义是在操作系统内核中提供区块链的功能。LibertyOS 即是如此，它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，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，再出售给广告商和其他非政府组织或政府组织。而 LibertyOS 为此提供了

[1] https://medium.com/nearprotocol/introducing-the-blockchain-operating-system-bos-8004345d02ba

一个解决方案：系统中的所有东西都由操作系统的用户 100% 掌控。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，称为 LIB 令牌。广告商必须支付 LIB 令牌用于广告投送，而用户可以使用 LIB 令牌向他们喜欢的项目捐款，以此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上层应用的开发提供任何帮助。

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] 新华社, “‘云’上的未来之城——‘智能雄安’成长记”. [Online]. Available: https://www.gov.cn/xinwen/2022-06/30/content_5698579.htm

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

[4] 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.

[5] B. Seok, J. Park, and J. H. Park, “A Lightweight Hash-Based Blockchain Architecture for Industrial IoT”, *Applied Sciences*, vol. 9, p. 3740, 2019, doi: 10.3390/app9183740.