

开题报告：基于rCore的区块链操作系统设计与实现

汇报人：傅泽

系统架构

1. 课题概述

Web 3.0时代旨在创建一个去中心化的互联网，数据将被存储在网络中的众多节点中，并以区块链技术提供极难篡改、极难抵赖等安全保障，是大势所趋的未来网络发展方向。然而,市面上流行的绝大多数操作系统内核并未做好迎接 Web 3.0 时代到来的准备。它们并未内置开发分布式应用dapp所需的技术栈，使得开发dapp的流程十分繁琐。

2. 课题工作

- 基于rCore操作系统内核作为基底
- 采用Substrate区块链作为dapp技术栈实现
- 构建一套在内核中运行区块链节点，并以系统调用形式提供服务的区块链操作系统内核rCore-Blockchain

关键问题

1. 国内外研究现状

- 区块链技术被广泛应用于城市管理等领域。
- 区块链技术在一般算力设备上的应用正在逐步突破。
- RISC-V正在积极拥抱区块链技术，两者相辅相成，在构造区块链虚拟机以及实现我国软硬件完全自主可控等方面形成诸多成就。
- 区块链技术与操作系统的融合尚起步不久，目前有两种技术途径实现两者的融合：
 - 用户的特定操作需云端区块链辅助完成，操作系统本身不参与区块链网络，如 NYNJA 虚拟操作系统。
 - 操作系统也充当区块链网络节点，如 LibertyOS、ethOS。

2. 课题研究内容

本研究工作对区块链技术在以操作系统为代表的计算机行业内应用情况进行调研。在基于 Rust 的开源操作系统内核项目 rCore的基础上,以系统调用的形式引入开源区块链 Substrate 的基于 Rust 的节点实现 SubstrateNode Template 及其客户端 Substrate api client的部分功能,令 rCore 具备原生的区块链交互开发能力,减轻上层应用开发者开发 dapp 的心智负担。

技术方案

1. 研究工作三步走

本课题的研究工作分为三部分展开。

- 第一阶段针对 Substrate 项目展开。该阶段的主要目标为:对项目代码进行分析以确定其依赖项,确认 rCore 内核提供的服务是否能满足这些依赖项的要求。若不满足,则需确定需要进一步实现的系统调用。
- 第二阶段针对 rCore 进行完善工作。按照第一阶段的依赖分析,逐一将依赖引入 rCore 中。对于 rCore 缺少的系统调用,参考已有的系统调用和 Linux 等开源项目的实现进行补充。预期该阶段完成后,Substrate 应当可以以用户程序的形态在 rCore 中运行。
- 第三阶段,将 Substrate 从用户态迁移向内核态,并将区块链开发的关键操作以新系统调用的形式向用户程序开放。具体而言,这将包含账号管理、余额管理和智能合约三大类功能,每一类功能下设数个系统调用,供上层应用开发者使用。该阶段完成后,可编写简单的用户态测试程序,验证区块链操作系统的功能完备性和正确性。

技术方案

2. Substrate的C/S架构

Substrate区块链采用了服务器-客户端架构。它提供了名为Substrate Node Template的节点实现。作为官方基于 Rust 的精简版节点实现,Substrate Node Template 具备管理账号、转储余额等基本机能,同时也支持通过引入“pallet”的形式提供诸如智能合约等功能,完全可以满足本课题区块链部分的所有需求。在计算机上启动节点,即可连接到基于Substrate开发的区块链网络并与链上的其他账号与智能合约互动。

要对节点发送命令,或从节点取得链上数据,则需要 Substrate api client 等客户端与之通信来实现。Substrate api client 是 Substrate 官方的客户端项目 subtx 的轻量级替代。它以部分功能性作为代价,换取了与 no-std 环境的良好兼容性。它包含了一组较为用户友好的接口和一个通信模块,以 JSON-RPC格式向节点发送请求并取得返回值。

本课题预期实现的效果为:令 SubstrateNode Template 运行在内核中,而 Substrateapi client 被封装为数个系统调用提供给上层用户应用程序开发者。上层用户应用程序开发者仅需使用这些系统调用,即可方便地实现账户管理、链上区块查询等功能,从而简化 DApp 的开发流程,减轻心智负担。

预期结果

实现融合区块链功能的 rCore 改进版rCore-Blockchain。相比 rCore,rCore-Blockchain 增添了新的系统调用,用户程序可以直接调用它们,用于其App的业务逻辑。

区块链客户端支持的操作多种多样,为所有这些操作提供系统调用显然是不现实的。因此,必须确定 rCore-Blockchain 将支持哪些区块链操作。开发者的以太坊之旅是一系列指引入门学习者上手以太坊区块链的博客文章,其中清晰地展示并使用了以下以太坊区块链客户端的功能特性:

- 网络连接
- 区块管理
- 账号管理
- 交易支持
- 智能合约支持

综合以上功能特性的重要程度及实现难度,本课题计划优先支持四三个功能特性,即网络连接、区块管理、账号管理和交易支持功能。在此基础上,尝试实现有关智能合约的支持功能。

请各位老师批评指正