

基于Rust的简易区块链项目产品方案

项目背景

在数字化浪潮下，数据安全、可信存储与传输需求迫切。区块链以去中心化、不可篡改、可追溯特性，为金融、供应链、医疗等行业痛点提供创新解法，潜力巨大。Rust 作为运行快、内存安全的系统语言，用其实现区块链，既能深化对区块链的理解，又能提升 Rust 语言运用熟练度，在此背景下，我们开发了这款简易区块链项目。

产品概述

产品定位

区块链是一个极为复杂且庞大的概念，难以凭借一个简单的演示项目（demo）就将其全貌完整呈现。然而，区块链的概念及实现原理却清晰可循。借助 Rust 语言，我们能够打造一个简易区块链系统。在这个构建过程中，参与者不仅能深入洞悉区块链的实现原理，还能大幅加深对 Rust 语言的理解。随着持续对该演示项目进行完善，它将对后续新涉足 Rust 语言编程领域或区块链领域的人员，发挥极为重要的辅助作用，成为他们学习探索路上的得力帮手。

目标用户

- 新人：作为一个基于Rust完成的简易区块链，对想要入门Rust或者入门区块链的人来说是一个很好的参考。
- 开发者：基于这个简易的系统，可以通过重构、增加功能等方式扩展该demo，使得该demo逐渐完善，成为一个更好更易用更有教学意义的项目。

产品功能

区块生成

- 实现区块结构的编写、区块的创建，增加。创世区块的生成等
- 区块链添加区块逻辑实现

Hash计算

- 提供基于SHA-256实现的hash算法，将区块最终生成256位的hash值

工作量证明

- 工作量证明本质是重复hash直到获得一个认可的hash值，生成的hash值作为该区块的hash
- 产品实现了工作量证明的代码，使用简单的方式计算出正确的hash以及增加验证代码

区块链持久化

- 创建好的区块，通过使用数据库的方式，将区块存入磁盘中，保证数据持久化
- 防止每次运行都会重新生成创世区块，检测到数据库有数据就进行反序列化，检测到数据库没有数据就会生成创世区块，等待交易。

产品设计

架构设计

- 采用模块分离的方式，将区块逻辑存放在core中、将工具型代码存放在utils中，将cli或者界面话程序存放在main中。

技术选型

- 数据库选用rocksdb，该数据库是一个嵌入式数据库，rust操作友好。