RustChain_RustCamp_ProjectProposal

1. 产品概述

“RustChain”是一款基于 Rust 语言开发的轻量级区块链平台，是一个以学习为目的的安全、透明、易于定制和扩展的分布式账本系统开发实践。

平台实现了核心区块链功能，包括区块构造与验证、交易处理、UTXO 模型、钱包管理以及 P2P 网络通讯等，既适合用于技术学习与开发实践，也可作为构建定制化区块链解决方案的基础产品。

2. 核心功能与特点

- **区块链核心：**
  - 实现了区块链数据结构、区块链迭代、区块验证与 Proof-of-Work 共识机制（基于 SHA256 算法和 Merkle 树）
  - 支持创世区块生成、区块挖矿以及链上数据存储（采用 sled 数据库）
- **交易与 UTXO 模型：**
  - 完成了 UTXO 模型的交易构造，包括普通交易与 coinbase 交易
  - 实现了交易签名与验证（基于 ed25519 算法），保证交易的不可篡改性和安全性
  - 提供查找未花费输出、重建 UTXO 集合及更新机制，确保账本数据一致性
- **钱包管理：**
  - 提供钱包创建、地址生成、密钥管理功能
  - 基于 bitcoincash_addr 生成地址，结合公私钥机制实现用户身份验证与资产安全
- **P2P 网络与节点通信：**
  - 内置节点服务器，支持 TCP 网络通信，消息类型涵盖版本信息、区块数据、交易数据、地址同步等
  - 支持节点发现、区块和交易的广播与请求，确保多节点间数据同步和共识达成
- **CLI 命令行接口：**
  - 提供丰富的命令行工具，包括创建区块链、钱包管理、查询余额、发送交易、启动节点/矿工等功能
  - 方便开发者和运维人员通过命令行快速上手和调试系统

3. 技术架构

- **语言与开发框架：**
  - 核心代码采用 Rust 编写，充分利用 Rust 的高性能、安全性和并发处理优势
- **数据存储：**
  - 采用 sled 作为内嵌式数据库，实现区块、UTXO 数据持久化存储与高效检索

- **网络通信：**
  - 基于 TCP Socket 实现点对点通信，采用自定义消息格式（包括命令码与数据载荷）保证节点间的信息互通
- **加密与安全：**
  - 使用 SHA256 和 Merkle 树实现区块哈希计算与数据完整性校验
  - 基于 ed25519 及 Ripemd160 实现交易签名与公钥哈希，确保交易的不可伪造性
- **模块化设计：**
  - 代码分为 block、blockchain、transaction、utxoset、server、CLI 等多个模块，各模块职责清晰，方便后续扩展和维护
- **安全机制：**
  - 严格的加密算法（SHA256、ed25519、Ripemd160）确保数据和交易安全
  - 交易签名与验证机制防止恶意篡改
  - 定期代码审计和安全测试，及时修复潜在漏洞

4. 总结

“RustChain”区块链平台以其轻量高效、模块化设计和强大的安全特性，适合作为学习实践及定制化区块链应用的基础框架。实现了简单的核心区块链功能、钱包与交易模块，供 CLI 工具及基础的 P2P 节点网络。未来如有需求，可根据市场需求和技术发展趋势，逐步扩展功能、提升性能，为 Rust 语言的学习和开发实践提供一定程度的支持。