# 基于区块链的身份认证与权限管理系统研究

荆　宇

Bitfish Holdings Pte. Ltd.，新加坡　369551

【摘　要】当前数字化场景中，身份认证与权限管理面临中心化架构的信任依赖、敏感数据集中存储风险以及跨域协作效率低下等挑战。区块链技术凭借其分布式账本、共识机制与密码学保障特性，为构建可信、自主可控的认证管理体系提供了新路径。本文设计模块化的链上身份认证协议与动态权限控制模型，探索去中心化环境下身份数据确权、验证与权限细粒度管理的可行性，以期推动可信数字身份生态的构建。

【关键词】区块链；身份认证；权限管理

## 引言

数字身份作为现代数字社会的核心基础设施，其可信性、安全性与可移植性直接影响用户权益与跨平台协作效率。现有身份认证体系多依赖于封闭式架构，导致身份数据碎片化、用户主权弱化以及跨域互操作性不足。区块链技术通过构建去中心化标识符、可验证凭证与链上策略引擎，为解决身份主权归属、细粒度权限动态适配以及操作存证不可抵赖性提供了技术范式。

## 1　基于区块链的系统总体架构

系统服务层采用Gin框架构建中间件服务，作为连接前端应用与底层区块链网络的协同枢纽。该中间层通过集成Hyperledger Fabric SDK实现与区块链节点的深度交互，其中SDK封装了链码调用、身份证书管理和交易背书等核心功能[2]。前端应用基于React框架与TypeScript语言实现，通过Protobuf库直接解析二进制载荷为结构化对象，消除了JSON文本解析时的冗余类型转换过程，使得业务逻辑层可直接操作类型完备的数据实体[2]。

如图1所示，系统采用分层解耦的模块化架构设计。用户操作请求经React界面封装为Protobuf格式的二进制流，通过HTTPS加密通道传输至服务端。服务端基于Gin框架构建的路由分发模块捕获用户请求后，利用proto3定义的模式文件进行数据重构，生成具有严格类型约束的请求对象。

## 2　基于区块链的身份认证与权限系统设计

### 2.1 模块化架构

本系统基于Hyperledger　Fabric框架构建分布式账本网络，主要用于个人基础信息、职业履历及学术成果等多模态数据的可信存储与管理。区块链底层采用多通道架构实现数据隔离，其中核心业务通道部署了定制化智能合约

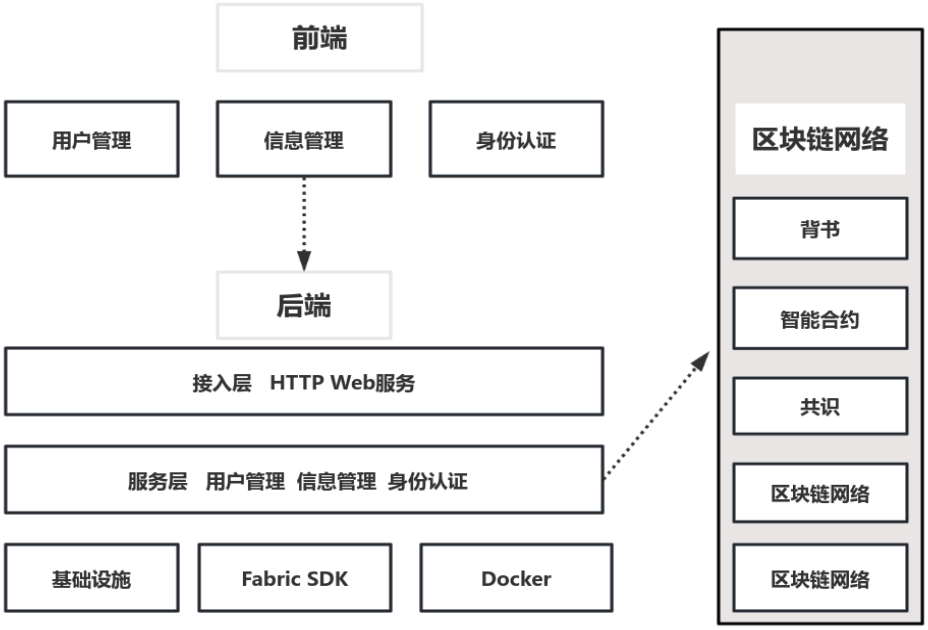


图1　系统总体构架示意图

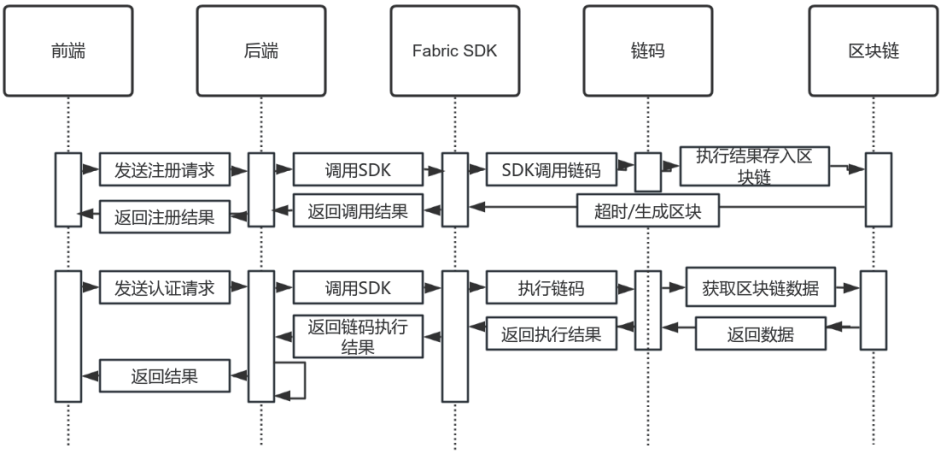


图2　系统时序图

链码，负责执行数据加密存证、权限校验及审计追溯等操作。针对Fabric　2.0版本后Solo/Kafka共识的官方弃用问题，系统采用Raft共识集群实现最终一致性。该方案通过动态选举Leader节点保障排序服务的高可用性，但需借助FabricConsensus扩展组件解决频道配置更新时的版本兼容性约束。在Gradpro业务频道中部署的gradpro链码，通过脚本实现数据采集接口标准化，支持结构化字段校验与多条件查询优化。前端路由管理采用React-Router　V6构建声明式导航体系，集成JWT令牌验证中间件实现动态权限拦截，未授权访问请求将自动重定向至认证中心[3]。

系统界面层开发了高度模块化的数据录入组件库，涵盖个人档案、职业经历及教育背景等业务场景。通过封装Ant Design的DatePicker、Select等控件形成可复用的智能表单模组，支持数据类型校验与自动填充功能。如图2所示，用户流程始于身份认证阶段：客户端提交加密凭证后，CA认证中心通过Fabric SDK调用链码完成区块链存证，随后签发访问令牌。业务请求经Protobuf编码后传输至Gin中间件，服务端通过解析请求参数构造链码调用提案，经背书节点验证后提交排序服务打包上链。整个过程实现客户端零明文数据处理与服务端无状态事务管理，确保敏感信息全链路加密。

2.2 身份认证设计

系统登录界面采用双因素认证机制完成用户身份核验，成功认证后激活数据检索功能模块。用户输入查询条件后，前端应用构造Protobuf格式的检索请求，经HTTPS加密通道传输至Gin中间件服务层。服务端通过Fabric　SDK调用智能合约，在区块链分布式账本中执行链上数据查询，并将查询结果序列化为二进制数据流返回。前端接收二进制载荷后，利用预定义的Protobuf模式文件进行反序列化操作，同时执行AES-GCM算法解密数据内容，生成结构化JSON对象供界面层处理。此外，界面引擎根据数据分类标签，如基础档案、职业轨迹等动态匹配展示模板，采用卡片式布局呈现核心字段。用户可通过交互式详情按钮触发模态窗口，查看经权限过滤的完整数据项及区块链存证哈希值，确保信息透明可验证。

2.3 加密安全方案设计

FirstSource数据保护方案采用混合加密架构，结合对称加密算法与椭圆曲线数字签名实现多维安全防护。在数据封装阶段，发起方首先生成随机对称密钥K，对明文信息实施AES-256加密操作，该设计充分发挥对称加密在加解密速度与低计算开销方面的优势，尤其适配物联网设备的资源约束特性。加密后的密文与原始数据的SHA-3哈希值共同构成数据元组，随后使用ECDSA算法对数据包进行签名。具体签名过程可表述为SIG{T}=Sign_Sks( Hash(T) ||AES_K(T) )，其中Sks为发送方私钥，通过将哈希摘要与密文绑定签名，既确保数据完整性防篡改，又实现发送方身份可追溯认证。在密钥分发环节，系统采用分层加密策略增强安全性。对称密钥K通过接收方公钥Pkr进行椭圆曲线加密，生成ENCPkr(K)密文块，该过程利用非对称加密的密钥安全传输特性[4]。

此外，为了验证通信有效性，接收方需对解密数据重新计算哈希值并返回校验和。发送方通过比对校验和确认数据完整性与解密正确性，该机制可同步检测传输过程中的数据损坏或恶意篡改行为。方案中的对称密钥由物联网终端按预设周期动态生成，结合基于硬件安全模块的密钥生命周期管理，实现前向安全性保障与密钥轮换自动化如表1所示。

表1 FirstSource混合加密方案核心机制对照表

| 分类 | 技术要素与实现逻辑 | 功能目标 |
| --- | --- | --- |
| 技术组成 | 对称加密+ 椭圆曲线数字签名 | 兼顾加密效率与安全性，适配物联网资源限制场景 |
| 核心机制 | 1.数据完整性<br>2.数据机密性<br>3.身份认证 | 防篡改、防窃取、防伪造 |
| 流程步骤 | 1.生成随机对称密钥K<br>2.加密数据并哈希签名<br>3.嵌套加密K<br>4.接收方私钥解密K并验证哈希 | 端到端加密通信与密钥安全传递 |
| 优势特性 | 1.对称加密高效低耗<br>2.非对称加密保障密钥安全<br>3.动态密钥轮换机制<br>4.哈希-签名双重验证 | 高吞吐、前向安全、抗重放攻击 |
| 适用场景 | 物联网设备数据流、资源受限环境下的安全传输 | 支持轻量化终端与高频率密钥更新需求 |

2.4 权限系统设计

本系统采用前后端分离架构，依托SpringBoot框架构建高可用微服务后端，结合Vue3实现响应式前端界面，通过标准化API接口实现业务逻辑与交互界面的解耦协同。权限控制体系围绕四大核心模块展开：身份治理模块集成多维度用户生命周期管理，涵盖生物特征认证、分布式会话管理及跨平台账号同步功能；角色配置模块构建动态权限继承网络，支持多层级角色关系建模与权限冲突自动检测机制；细粒度授权模块采用策略驱动模式，分离界面操作权限与数据访问权限，实现基于属性规则的行级数据过滤与字段级脱敏控制；组织架构模块通过树形拓扑映射企业部门层级，建立部门间数据沙箱隔离与跨组织权限穿透机制，形成多维立体化权限管理体系。在技术生态层面，系统数据存储层支持MySQL、达梦及Oracle等异构数据库引擎，通过抽象化数据访问层实现多源数据无缝切换。在容错机制方面，建立全局异常拦截链路，采用分层异常分类策略与标准化错误码体系，结合分布式日志追踪技术实现故障快速定位与自愈处理[5]。

## 3 系统实现与验证

本系统采用Fabric生态中的Caliper性能评估套件，基于Node运行环境完成基准测试。具体实施时需部署Caliper-Benchmark组件至指定路径，通过配置文件建立测试连接通道，可精确测量交易确认率、响应时延及系统吞吐量等关键性能参数。

在性能测试维度，通过对用户身份信息提交模块进行压力测试，系统在单节点环境下展现出约450笔/秒的峰值处理能力。数据分析表明，当前架构的并发处理瓶颈主要源于硬件资源配置限制，通过升级服务器计算单元、优化存储I/O性能以及扩展网络带宽等措施，可有效提升整体吞吐量。在系统兼容性验证方面，采用Chrome、Firefox等主流浏览器进行端到端传输测试，完整采集了涵盖协议版本、资源加载时序、数据包完整率在内的多维指标。测试数据显示，身份认证模块在常规网络环境下可保持98.6%的请求成功率，但存在0.7%的异常中断概率，主要归因于TCP长连接稳定性不足。

## 4 结语

综上分析，本研究基于区块链技术构建去中心化身份认证与权限管理系统，通过模块化链码设计、混合加密方案及动态权限模型，有效解决了传统中心化架构的信任依赖与数据隐私风险。实践表明，系统在单节点环境下可实现450笔/秒的吞吐量峰值，身份认证成功率高达98.6%，验证了区块链技术在可信身份管理领域的应用潜力。

**参考文献：**

[1]张朝阳,王建祥,侯乃明,等.基于大数据与区块链的智能平台身份认证技术[J].高技术通讯,2024,34(12):1279-1285.

[2]王雨鑫,郑东,韩刚,等.基于区块链的车联网多因素跨域认证方案[J].信息安全研究,2024,10(11):1074-1080.

[3]张秋荟,高迁.大数据与区块链技术在智慧城市数据安全管理中的应用探索[J].信息记录材料,2024,25(11):117-119+123.

[4]朱金玉.区块链技术在网络安全与隐私保护中的应用探索[J].中国宽带,2024,20(10):115-117.

[5]李强,赵峰,宋卫平,等.基于区块链的异构跨域双向身份验证研究[J].电子设计工程,2024,32(21):181-184+191.

**作者简介：**

荆宇（1992.6—）；性别：女；民族：汉；籍贯：山东；学历：研究生；职称：无；职位：首席技术官；研究方向：绿色能源与区块链技术。