学号\_\_\_\_20194824\_\_\_\_ 密级\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**东北大学本科毕业论文**

基于联盟链的存证数据

加密管理系统设计与实现

学 院 名 称 ：计算机科学与工程学院

专 业 名 称 ：计算机科学与技术

学 生 姓 名 ：齐彦乔

指 导 教 师 ：信俊昌 教授

二○二三年六月

**郑 重 声 明**

本人呈交的学位论文，是在导师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料真实可靠。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确的方式标明。本学位论文的知识产权归属于培养单位。

本人签名： 日期：

摘 要

随着人类对矿产品需求的不断增加以及易采资源变得越来越少，开采复杂难采资源是未来采矿的必然趋势。另一方面，随着国家环境保护政策的日益严格，如何合理、高效、经济、安全地进行矿产资源的开发、利用，降低资源的损失、减少矿石的贫化，是矿产资源开发者共同关心的问题。充填采矿法因其具有提高回采率、降低贫化率、控制地压和减缓对环境扰动等显著优点，应用越来越广泛。 (宋体小四号 )

……

……

……

关键词：区块链；存证；数据共享；Fabric

**ABSTRACT**

(**Times New Roman**小二号加粗)

With the constantincrease of the mankind demanding the mineral products, easily mining resource is becoming more and more scarce, and it’s the inevitable trend of mining complex ore body. On the other hand, national environmental protection policy increasingly stringent. How to exploit and utilization mineral resourcesreasonably, efficiently, economically, safely and reduce loss of resource and dilution of ore is the question of mineral developers caring about. Due to the advantages of increasing recovery rate, reducing dilution rate, controlling underground pressure and mitigating of environmental disturbance, filling method is becoming more and more widely used.(**Times New Roman**小四号)

……

……

……

**Key words:** Key words 1; Key words 2; Key words 3; Key words4; Key words 5

（**Times New Roman**小四号加粗）（**Times New Roman**小四号）

**目 录**

[摘要……………………………………………………………….………………………I](#_Toc422211181)

ABSTRACT…………………………………………………………………………….II

1绪论…………………………………………………………………………………….1

1.1研究背景 ……………………………………………………………………………1

1.2国内外充填采矿发展现状…………………………………………………….….…3

1.3国内外充填采矿研究现状……………………………………………….……….…6

1.4本文研究内容和技术路线…………………………………………………..……. 10

1.4.1本文的研究内容……………………………………………………….………. 10

1.4.2本文的研究方法和技术路线…………………………………………………....11

2尾砂胶结充填体力学特性研究………………………………………………....12

[2.1尾砂胶结充填体的物理力学性能及胶凝机理…………………………………... .12](#_Toc422211202)

[2.1.1尾砂胶结充填体的物理力学性能……………………………………………. ..13](#_Toc422211203)

[2.1.2尾砂胶结充填体的胶凝机理………………………………………………….. .15](#_Toc422211204)

[2.2尾砂胶结充填体的力学实验……………………………………………….......... .16](#_Toc422211205)

[2.2.1尾砂物理力学参数测试………………………………………………………. .16](#_Toc422211206)

[2.2.2尾砂胶结充填体力学实验……………………………………………………...17](#_Toc422211207)

[2.3尾砂胶结充填体破坏规律分析………………………………………………........19](#_Toc422211208)

[2.4本章小结……………………………………………………………………........…20](#_Toc422211209)

(各章的名称黑体四号，其余宋体小四号，行间距为1.5倍)

**……**

结论……………………………………………………………………………………..57

参考文献……………………………………………………………………………… 59

附录……………………………………………………………………………………. 62

致谢……………………………………………………………………………………. 72

1 绪论

1.1 研究背景

1.2 国内外研究现状

1.2.1 国外研究现状

1.2.2 国内研究现状

* 1. 本文研究内容和技术路线

1.3.1 研究内容

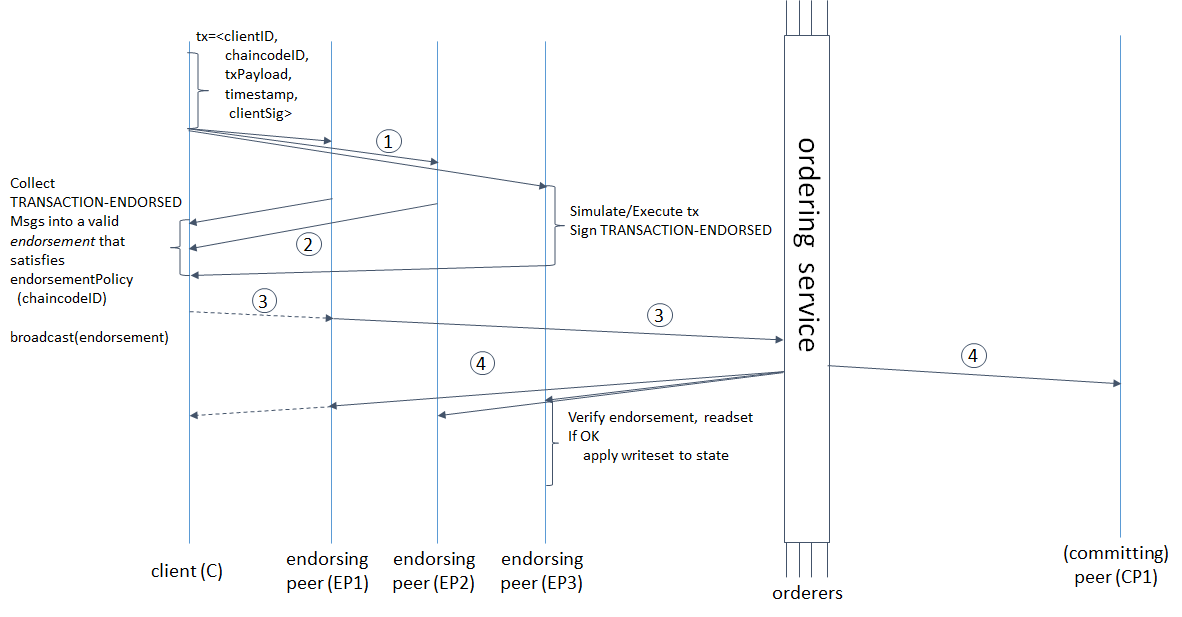
1.3.2 技术路线

2 相关技术介绍

2.1 Hyperledger Fabric 框架

Hyperledger Fabric是一个许可区块链的分布式账本技术。与公共非许可区块链技术的共同点是，它们都有一个账本，使用智能合约对账本进行受控制的访问，与公共非许可区块链技术之间最大的不同点是，Fabric是许可的，参与者需要向可信赖的成员服务提供者（MSP）注册，而不是像公共非许可区块链技术中参与者之间是匿名或完全不信任的。

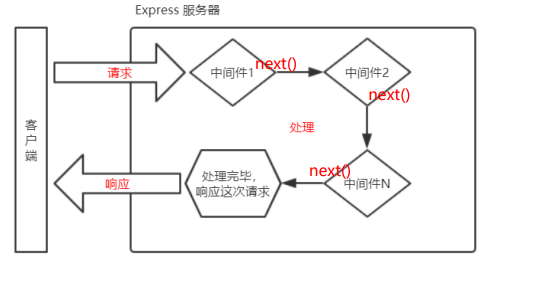
Fabric的交易流程如图2.2所示：

图2.2 Fabric交易流程图

客户端首先要使用组织的证书服务注册与登记，并获取在网络中用于确认身份的加密材料，加入该网络中可正常运行的通道。客户端通过SDK生成交易提案并签名后提交至背书节点。背书节点验证签名后，根据交易提案执行链码生成交易结果。这些结果与签名会作为提案响应返回给客户端。客户端验证背书节点的签名并比较这些提案响应是否相同，当满足用户指定的背书策略后发将交易发送给排序节点。排序节将接收到的交易排序，并将其打包成区块发送给该通道中的所有peer节点。peer节点对区块内的交易进行验证，验证通过后更新账本。

2.2 Express框架

Express是一款开源，灵活，基于Node的web开发框架。以面向切面编程的思想设计框架的结构。该框架解决原生node开发web服务器时，代码过于冗杂的痛点。该框架简单但因其设计思想为面向切面编程，所以故拓展性强，开发者可开发各种中间件以实现不同功能。譬如JWT中间件可实现鉴权功能，Upload中间件可实现后端解析formData中的文件的功能，CORS中间件可实现跨域功能。Express中间件调用流程如图2.1所示

图2.1Express中间件调用流程图

2.3 UmiJS框架

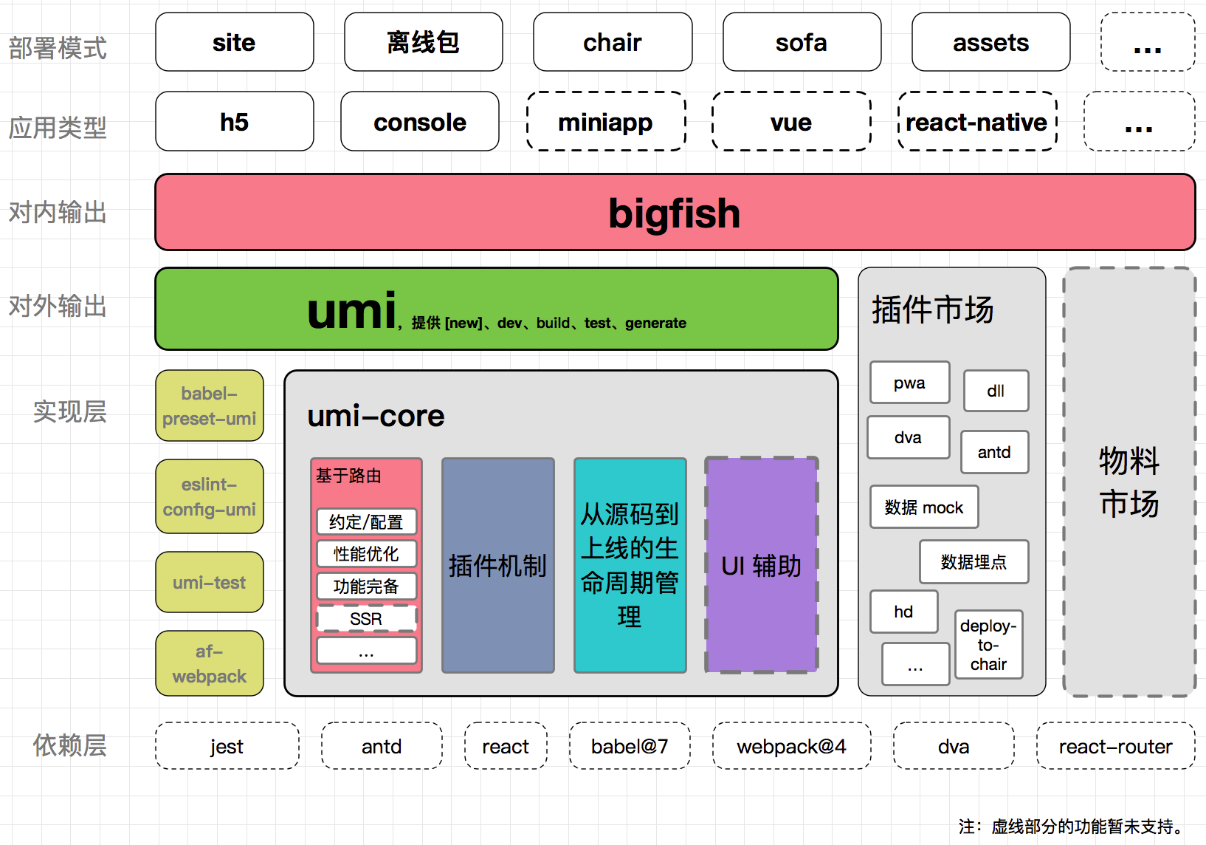
Umi是一个可插拔的企业级react应用框架，其完善的插件体系包含从开发到构建的每个生命周期。Umi是蚂蚁金服的底层前端框架，并经过业界的沉淀与验证，Umi架构如图2.2所示

图2.2Umi架构图

2.4 本章小结

本章对本系统用到的相关技术进行了介绍，包括区块链网络使用的Hyperledger Fabric框架，后端使用基于Node的快速，开放，极简的Express框架。前端使用基于TS的企业级React应用框架UmiJS。

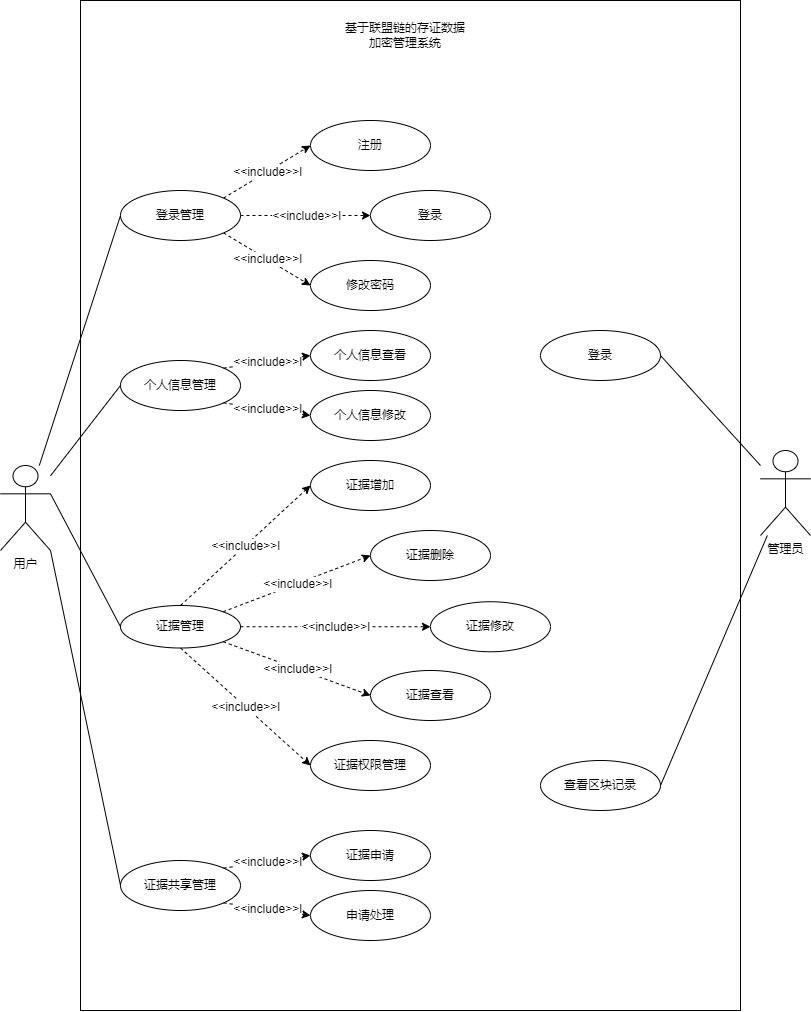
3 系统需求分析

3.1 系统需求概述

基于联盟链的存证数据加密管理系统的基础是存证数据加密管理系统，所以要实现传统存证数据加密管理系统的基本功能，例如登录，证据的增删改查，权限管理，共享等。核心是要将联盟链技术与传统存证数据加密管理系统相结合，在传统存证数据加密管理系统的基础上充分利用联盟链的特点。

3.2 功能性需求分析

依据需求给出本系统的用例图，如图3.1所示

图3.1系统用例图

系统包括普通用户与管理员两种参与者。普通用户注册后才能登录，而管理员的账户密码是系统预设，无需注册。

系统功能性需求如表3.1所示

系统功能性需求表3.1

|  |  |  |
| --- | --- | --- |
| 需求名称 | 需求说明 | 参与者 |
| 注册 | 用户通过邮箱创建账户用于登录 | 用户 |
| 登录 | 用户注册后，可登录进入系统 | 用户 |
| 修改密码 | 用户可修改自己的密码，修改后需重新登录 | 用户 |
| 个人信息查看 | 查看已经录入的个人信息 | 用户 |
| 个人信息修改 | 修改已经录入的个人信息 | 用户 |
| 证据创建 | 通过上传的文件与用户填入的信息创建证据，并可选择其加密方式 | 用户 |
| 证据删除 | 删除指定的证据 | 用户 |
| 证据修改 | 修改指定的证据 | 用户 |
| 证据查看 | 查看指定的证据的详细信息或下载该证据 | 用户 |
| 证据权限管理 | 对指定的证据的权限进行管理，可设置为私有，完全公开，只可下载或只可查看证据信息 | 用户 |
| 证据申请 | 在证据库（包含所有用户公开的证据）中申请其他用户公开的证据。 | 用户 |
| 申请处理 | 当B用户申请A用户公开的证据时，A用户可选择同意或拒绝 | 用户 |
| 管理员登录 | 用预设的账户密码登录进入系统 | 管理员 |
| 查看区块记录 | 查看区块的交易记录 | 管理员 |

3.3 非功能性需求分析

一个完善的系统除了功能性需求之外，还需要一些基本的非功能性需求，包括观感需求，易用性需求，安全性需求。

1. 观感需求

前端界面的设计简洁明了，风格统一，减少不必要的元素，方便用户使用。用户需要进行功能性操作时，能够快速定位至功能入口，用户需要数据录入时，需要对输入进行规范。同时还要考虑浏览器适配问题，保证各个浏览器能够成功运行

1. 易用性需求

系统的所有功能性操作的流程要符合用户习惯以及使用的期望，其将极大提高用户对该系统的接受度，提高转化率。

1. 安全性需求

数据不能被授权用户以外的任何人访问，授权用户可以不受阻止的访问数据，以及产品的强壮度必须得到保证。

3.4 本章小结

本章通过系统用例图阐述了参与者与用例之间的关系，并依此进行了系统的功能性需求分析，并对各项功能性需求进行了说明。在非功能性需求分析中，对观感需求，易用性需求，安全性需求进行了阐述。

4 系统设计

4.1 系统总体设计

4.2 区块链网络层设计

4.3 业务逻辑层设计

4.3.1 登录模块设计

4.3.2 个人信息管理模块设计

4.3.3 证据管理模块设计

4.3.4 证据权限模块设计

4.3.5 证据共享模块设计

4.4 界面交互层设计

4.5 本章小结

5 系统实现

5.1 区块链网络层的智能合约的实现

5.2 业务逻辑层的实现

5.2.1 登录模块的实现

5.2.2 个人信息管理模块的实现

5.2.3 证据管理模块的实现

5.2.4 证据权限模块的实现

5.2.5 证据共享模块的实现

5.3 界面交互层的实现

6 系统测试

6.1 单元测试

6.1.1 登录模块测试

6.1.2 个人信息管理模块测试

6.1.3 证据管理模块测试

6.1.4 证据权限模块测试

6.1.5 证据共享模块测试

6.2 系统测试

6.3 本章小结

7 结论

参考文献

[1]戴军,袁惠新.膜技术在含油废水处理中的应用[J].膜科学与技术,2002,22(2): 59.

[2]毛侠,孙云.和谐图案的自动生成研究[A].第一届中国情感计算及智能交互学术会议论文集[C].北京:中国科学院自动化研究所,2003:277-279.

[3]王湛.膜分离技术基础[M].北京:化学工业出版社,2000:14-21,30.

[4]张志祥.间断动力系统的随机扰动及其在守恒律方程中的应用[D].北京:北京大学,1998.

[5] World Health Organization. Factors regulating the immune response: report of WHO Scientific Group[R]. Geneva: WHO,1970.

[6]河北绿洲生态环境科技有限公司.一种荒漠化地区生态植被综合培育种植方法:中国,01129210.5[P].2001-10-24.

[7] GB/T 16159-1996,汉语拼音证词法基本规则[S].北京:中国标准出版社,1996.

[8]毛侠.情感工学破解“舒服之谜”[N].光明日报,2004-04-17(B1).

[9]陈剑.上博简《民之父母》“而得既塞於四海矣”句解释[EB/OL].简帛研究网站,http://www.bamboosilk.org/Wssf/2003/chenjian03.htm．2003-01-18.

(宋体小四号)

……

……

……

致谢