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

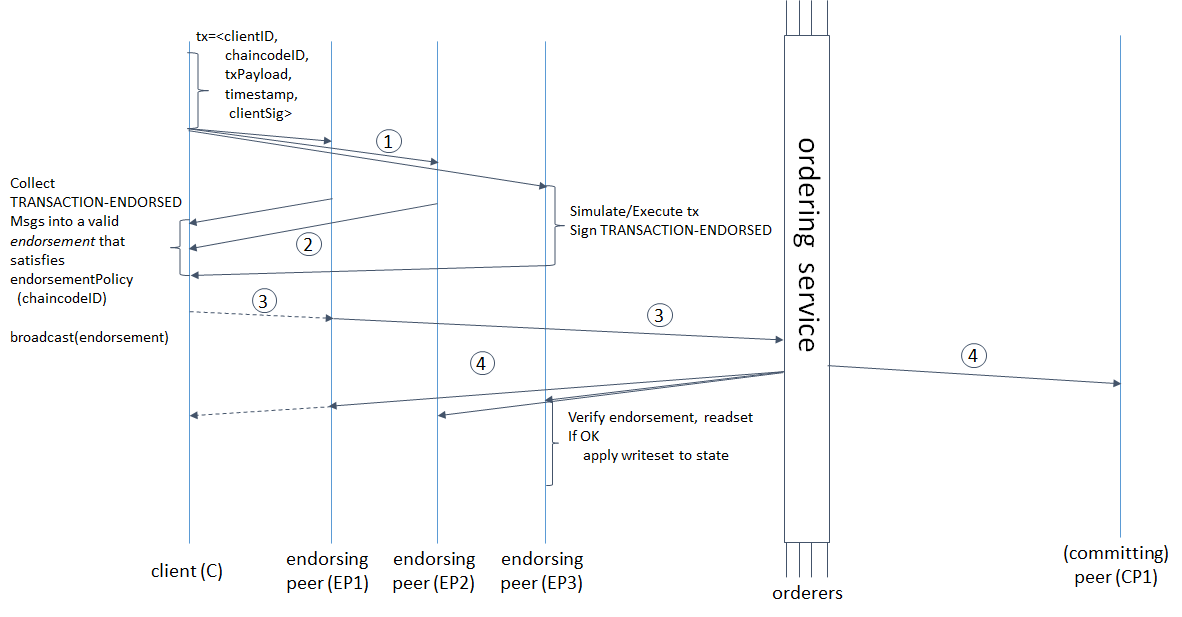
1.3.2 技术路线

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。

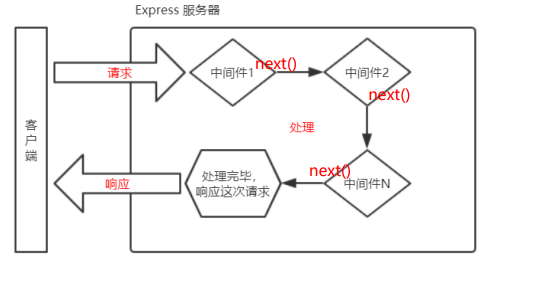
Fabric的交易流程如图2.2所示：

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

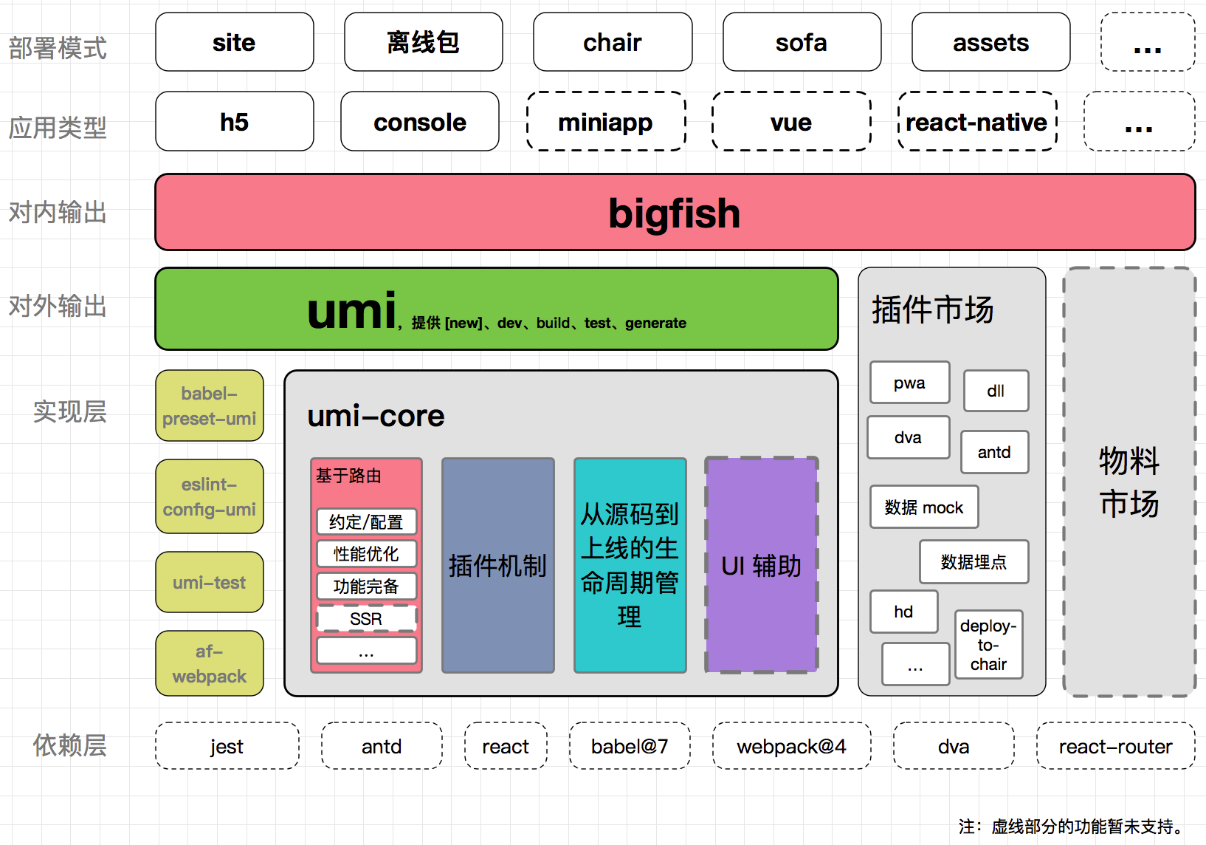
Umi是一个可插拔的企业级react应用框架，其完善的插件体系包含从开发到构建的每个生命周期。Umi是蚂蚁金服的底层前端框架，并经过业界的沉淀与验证，Umi架构如图2.2所示

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。

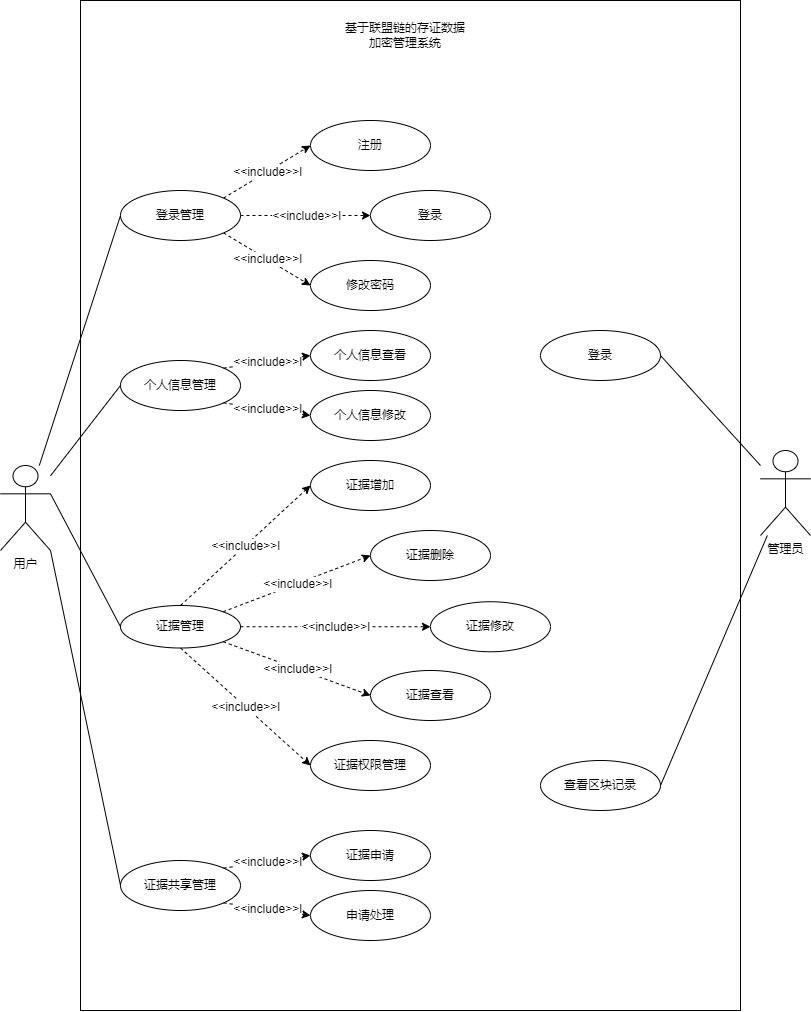
3 系统需求分析

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

通过对基于联盟链的存证数据加密管理系统的整体分析，运用分层思想将整个系统分为区块链网络层，业务逻辑层与用户界面层。

区块链网络层主要利用联盟链的不可篡改等特点来对整个系统的数据进行存储，提高系统的安全性。系统采用Hyperledger Fabric构建区块链网络层，故采用状态数据库存储数据。

业务逻辑层需要与区块链网络层进行交互，并且需要对用户界面层发起的HTTP请求进行解析并响应，是数据与业务逻辑的结合处，是该系统运转的核心。

用户界面层为供用户进行操作的PC端图形界面，依赖于业务逻辑层所提供的对数据进行访问的能力，给用户展示相关的数据与对这些数据进行操作的入口。

4.2 区块链网络层设计

区块链网络层的设计主要在于网络结构，帐本与智能合约。

网络结构为区块链网络的拓扑结构，采用1个ca节点，1个orderer节点，2个组织，每个组织含有1个背书节点与1个peer节点的网络配置。

账本与智能合约可抽象为数据与一系列的可更新与查阅该数据的函数。根据该系统的功能模块的设计，账本将存储元数据，用户，证据，证据申请四个对象。元数据存储证据对象，证据申请对象的总数，用于生成新的证据对象，证据申请对象的id。用户对象是对登录模块，个人信息模块中需要的用户数据进行数据抽象的结果。证据对象是对证据管理模块，证据权限模块的证据这一客体进行数据抽象的结果。证据申请对象是对证据分享模块的用户间进行证据共享的过程进行数据抽象的结果。智能合约则是对这些数据对象进行增删改查的操作。

4.3 业务逻辑层设计

业务逻辑层需要区块链网络层进行数据交互，并且提供给用户对数据进行访问的能力。将业务逻辑分离，解耦，最终将业务逻辑层抽象为FabricController，UserController，EvidenceController，ApplicationController。

FabricController负责与区块链网络层进行数据交互，并将交互后的结果进行解析。因网络IO时间占比较大，故对数据进行缓存以提高系统响应速度，缩短响应时间。是整个业务逻辑层访问数据的基础，其他controller皆依赖于FabricController。

UserController负责管理与用户相关的业务，如用户的注册，登录，修改密码，查看与修改个人信息等。

EvidenceController负责管理与证据相关的业务，其中包括对证据的增删改查，证据的加密解密。

ApplicationController负责管理证据的共享业务。ApplicationController主要是对区块链网络层的账本中的证据申请对象进行处理，而EvidenceController是对账本中的证据对象进行处理，两者所处理的数据不同。

4.4 用户界面层设计

对于一个系统，用户界面层是用户唯一可感知的系统分层，是系统与用户交互的桥梁，一个系统的好坏除了性能指标外，是否操作友好也是关键评判标准。

用户界面层使用UmiJs实现与业务逻辑层中userController相对应的的注册界面，登录界面与修改密码界面，与个人信息管理界面，与EvidenceController对应的证据管理界面，与ApplicationController相对应的证据库界面与证据申请界面。

4.4 功能模块设计

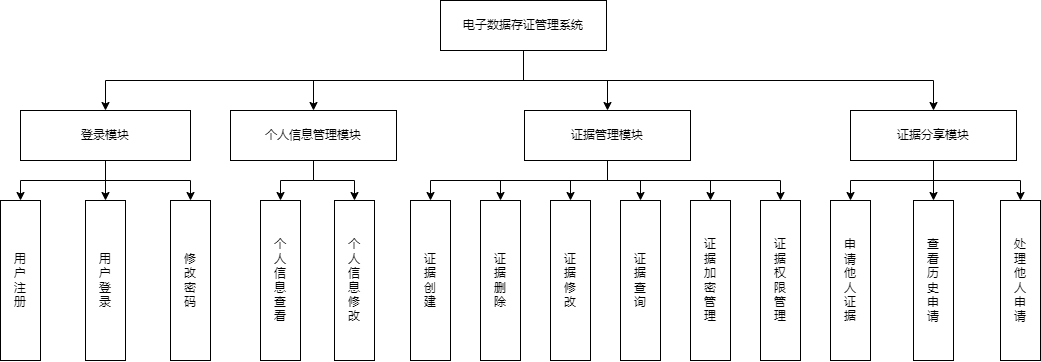
系统功能模块设计如图4.2所示

图4.2 系统功能模块设计图

该系统主要包含以下4个功能模块。登录模块，个人信息管理模块，证据管理模块，与证据共享模块。登录模块需要实现用户注册，登录，修改密码的功能。个人信息管理模块则是需要实现用户对个人信息进行查看于修改的功能。而最核心的证据相关模块则是需要实现对证据的增删改查，权限管理，加密管理与证据共享等功能。

4.5.1 登录模块设计

该系统的登录模块主要包含以下功能：

1. 用户注册：用户初次使用该系统时，需要注册账号用来登录。
2. 用户登录：用户注册后，可凭借该账号登录进入该系统以使用相关功能。
3. 修改密码：当用户登录后可修改密码，修改密码成功后会跳转到登录页面，此时用户需要重新登录才可继续使用该系统。当用户忘记密码时，可通过验证邮箱方式修改密码。

用户登录数据结构如表4.1所示

表4.1用户登录数据结构表

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 字段描述 |
| id | string | 账号id |
| password | string | 账号密码 |
| identity | number | 账号身份  0代表管理员  1代表常规用户 |

其中账号身份，。

4.5.2 个人信息管理模块设计

该系统的个人信息管理模块主要包含以下功能：

1. 个人信息查看：用户登录后可以查看自己账号的详细信息，其中包括自己创建的总证据数、各种证据类型数量，与总证据数的比例等。
2. 个人信息修改：用户可以选择修改自己账户的部分信息，其中包括性别，生日，身份证号等。但不包括账号创建时间。

用户信息数据结构如表4.2所示

表4.2用户信息数据结构表

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 字段描述 |
| id | string | 账号id |
| createTime | number | 创建时间 |
| updateTime | number | 更新时间 |
| idCardNumber | string | 身份证号 |
| name | string | 用户姓名 |
| gender | number | 用户性别 |

4.5.3 证据管理模块设计

该系统的证据管理模块主要包含以下功能：

1. 证据创建：用户登录后可进入证据创建页面完成对应表单创建对应证据的数据抽象。其中表单包括对证据类型的选择，例如图片，文档等、证据权限的设置、证据文件的上传等。
2. 证据查看：用户登录后可在个人证据界面查看到自己创建的所有证据的详细信息以及对证据进行操作的入口。证据查看功能也包括了证据的下载。
3. 证据删除： 用户登录后可在个人证据界面查看到自己创建的所有证据的详细信息以及证据删除按钮。点击后，需要进行密码验证，验证成功则将在数据库中将该证据的isDelete字段设为1，用户在7天内可选择恢复。若7天后用户不选择恢复的话，证据将自动从数据库中删除。
4. 证据修改：用户登录后可在个人证据界面查看到自己创建的所有证据的详细信息以及证据修改按钮。点击后，即可在证据对应信息展示处修改。确认修改后需要进行密码验证，验证成功将在数据库修改该证据信息。
5. 证据加密管理：用户在创建证据时可选择该证据文件的加密方式，也可选择不加密。证据创建成功后在个人证据界面将显示证据所有字段的明文数据。可在个人证据界面批量选择证据字段的加密方式，确认选择字段的加密方式后，需要进行密码验证，验证成功则将自己的所有证据对应字段的值统一加密。

证据权限管理：证据在创建时可选择将该证据公有或私有。若选择将该证据设置为共有证据，其他所有用户将在证据库界面查看到该证据经过该证据的创建者选择性加密后的信息。若选择将该证据设置为私有证据，只有自己在个人证据界面查看到该证据。

证据数据结构如表4.3所示

表4.3证据数据结构表

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 字段描述 |
| id | number | 证据id |
| creatorId | string | 创建者的用户id |
| description | string | 证据描述 |
| type | string | 证据类型 |
| name | string | 证据文件名称 |
| extension | string | 证据文件拓展名 |
| size | number | 证据文件内存大小 |
| encryption | string | 证据文件加密方式 |
| createTime | number | 创建时间 |
| updateTime | number | 更新时间 |
| isDelete | number | 是否已删除  1表示已删除  0表示未删除 |
| isPrivate | number | 是否私有  1表示私有  0表示公开 |
| access | map<userId,string[]> | 用户权限字典  键：用户id  值：用户所拥有的权限 |

4.5.4 证据共享模块设计

该系统的证据共享模块主要包含以下功能：

1. 证据申请：用户可在证据库界面申请查看目标证据目标字段的权限或申请下载目标证据的权限。申请成功后等待目标证据的创建者处理该申请，目标证据的申请者同意后，将获取相对应权限。
2. 处理申请：在他人申请界面可处理其他用户对自己证据相关权限的申请。可选择同意或拒绝，若选择同意需要填写该证据对于申请者的有效时间。

证据申请数据结构如表4.4所示

表4.3证据申请数据结构表

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 字段描述 |
| id | number | 证据申请的id |
| evidenceId | number | 证据id |
| done | number | 流程是否已完成  1表示已完成  0表示待处理 |
| code | number | 表示申请是否通过  1表示已通过申请  0表示该申请未通过 |
| expire | number | 若申请已通过，表示  该权限的过期时间 |
| type | string | 申请的类型  “download”表示申请下载  其他值为证据字段名称 |
| applicantId | string | 申请人的id |
| transactorId | string | 处理人的id |
| createTime | number | 创建时间 |
| endTime | number | 处理人处理该申请的时间 |

4.6 本章小结

本章首先根据分层思想将系统划分为区块链网络层，业务逻辑层，用户界面层，并依次阐述了对应分层的设计。之后对该系统进行功能模块划分，将该系统划分为登录模块，用户信息管理模块，证据管理模块与证据共享模块，并依次阐述了对应功能模块的功能与实现该功能需要的数据结构。

5 系统实现

本章将对该系统的各个功能模块的实现辅以流程图进行详细的说明。

5.1 智能合约的实现

智能合约主要实现对账本数据中的个人信息，证据，证据申请的初始化以及创建，删除，修改，查询。以及一些工具函数，比如isAuthorized判断该用户是否有权限使用该系统，encrypt对数据进行加密，getId当新建证据或证据申请时，获取新证据的id。

智能合约涉及的主要函数如表5.1所示

表5.1智能合约函数表

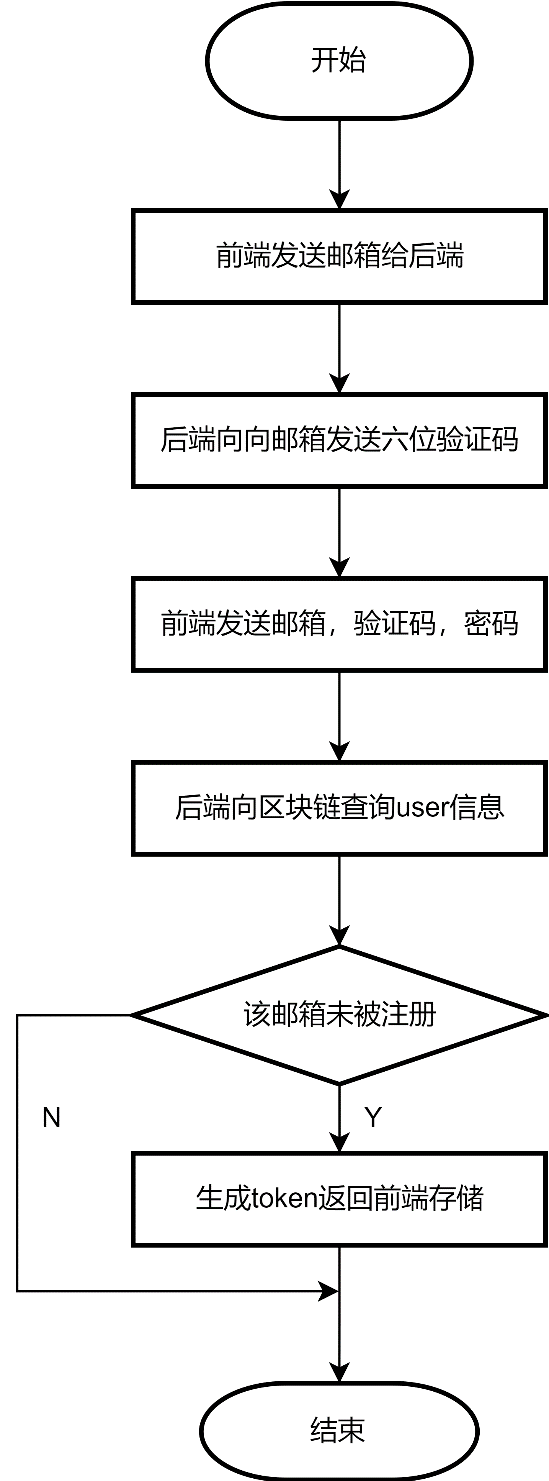
|  |  |
| --- | --- |
| 函数名 | 函数描述 |
| initLedger | 初始化账本 |
| createUser | 创建用户 |
| updateUser | 更新用户信息 |
| getUser | 查询用户信息 |
| createEvidence | 创建证据 |
| deleteEvidence | 删除证据 |
| updateEvidence | 更新证据信息 |
| getEvidence | 查询证据信息 |
| getEvidencesOfUser | 查询用户的所有证据 |
| getAllEvidences | 获取所有用户的公有证据 |
| encryptEvidences | 加密证据的相关信息 |
| decryptEvidencesField | 解密证据已加密字段值 |
| createApplicaton | 创建对证据的申请 |
| shouldCreateApplication | 判断当前对某证据的申请是否通过  不通过的情况有已申请，处理者未批准或  申请通过，权限未过期 |
| updateApplication | 当处理者处理后用于更新证据申请的信息 |
| getApplicantsApplications | 获取所有申请者id为参数的证据申请 |
| getTransactorsApplications | 获取所有处理者id为参数的证据申请 |
| isAuthorized | 判断某用户是否有权限使用该系统 |
| encrypt | 对证据文件或对证据信息进行加密 |

5.2 登录模块的实现

登录模块是该系统的基石，系统一切功能都将基于注册或登陆后前端存储的鉴权数据。登录模块主要含有注册，登录，修改密码三个功能。主要需要实现用户界面层的注册，登录，修改密码界面，业务逻辑层的UserController以及区块链网络层账本中的user数据以及智能合约对账本中user数据的处理。

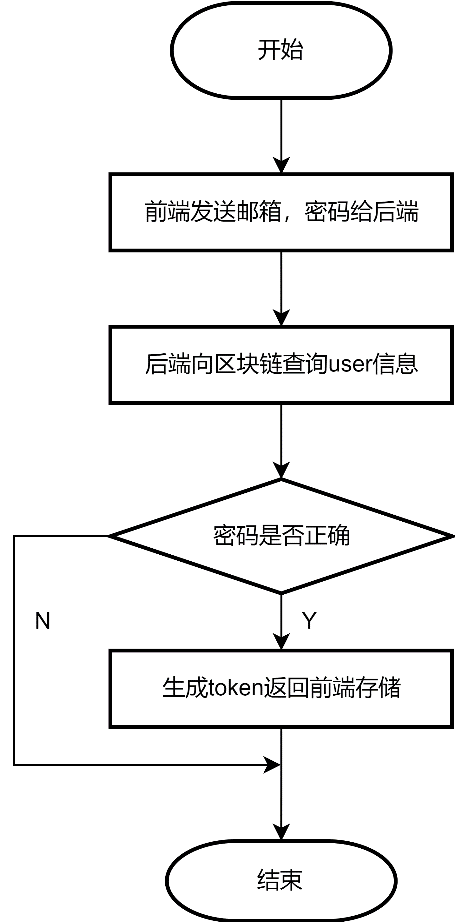
该系统的用户鉴权则是采用JWT技术，当注册或登陆成功后，后端会通过用户的账号等信息来生成token，并返回给前端存储。前端随后向后端发起的任意HTTP请求都将携带该token作为请求头的authorization属性。后端收到前端发起的除了注册与登录的任意HTTP请求也都会先判断该token是否有效，如果该token无效，则会返回给前端设定好的状态码，该系统选用304，并附带token已过期的提示信息。反之，则会正常处理该请求。前端也将会对所有的HTTP响应做出拦截，当检测到状态码为304，即为鉴权失败时，将无条件跳转到登录界面，需要用户重新登录以获取新的token。

当用户初次使用该系统时需要注册，注册需要先对邮箱进行验证。验证方式为后端向用户在注册表单内填入邮箱发送验证码，用户需要在注册表单内填入收到的验证码以及登录用的密码。向后端发送表单后，后端需要确认该邮箱未注册，确认该邮箱未注册后则注册成功，否则注册失败。该系统的注册流程图如图5.1所示。

图5.1注册流程图

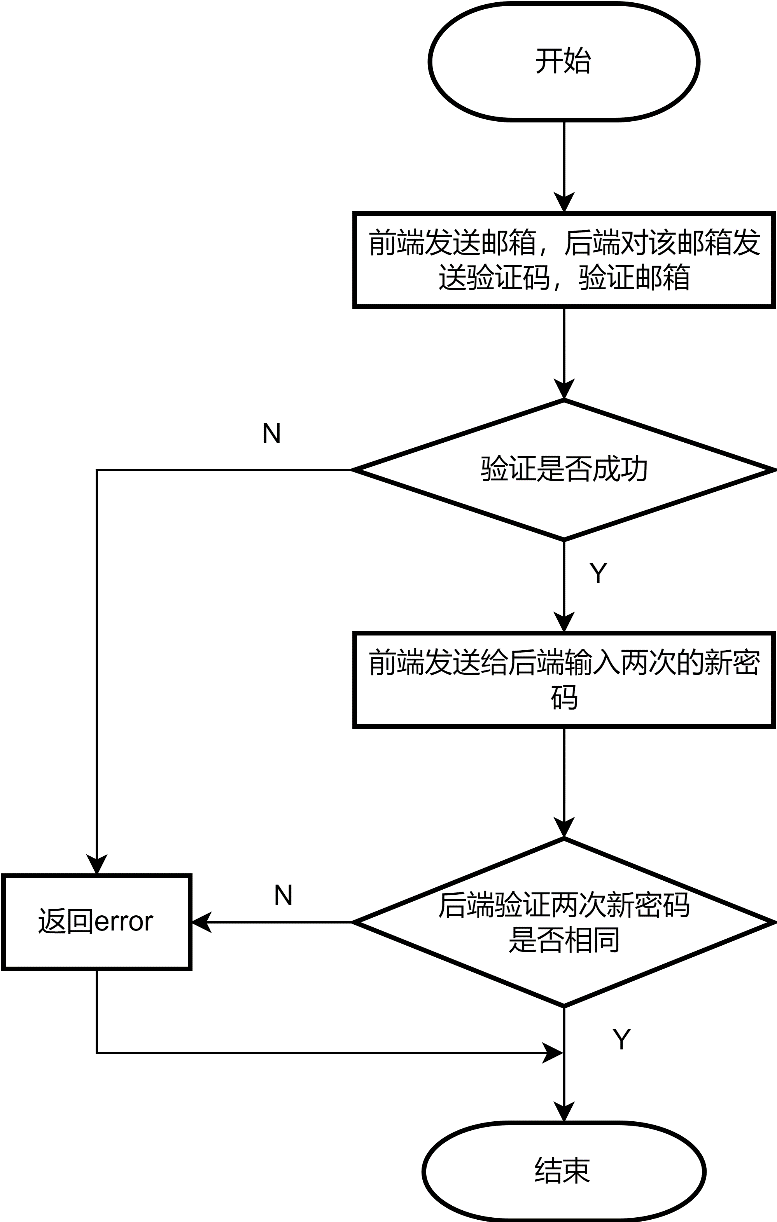
用户注册成功后，可凭借注册成功的邮箱密码进行登录。

该系统的登录流程图如图5.2所示。

图5.2登录流程图

用户在登录后可以选择修改密码，修改密码首先需要验证邮箱，验证成功后输入两次相同的新密码后提交修改，后端验证两次输入的新密码相同后invoke智能合约的updateUser函数修改用户密码。

该系统的修改密码流程图如图5.3所示。

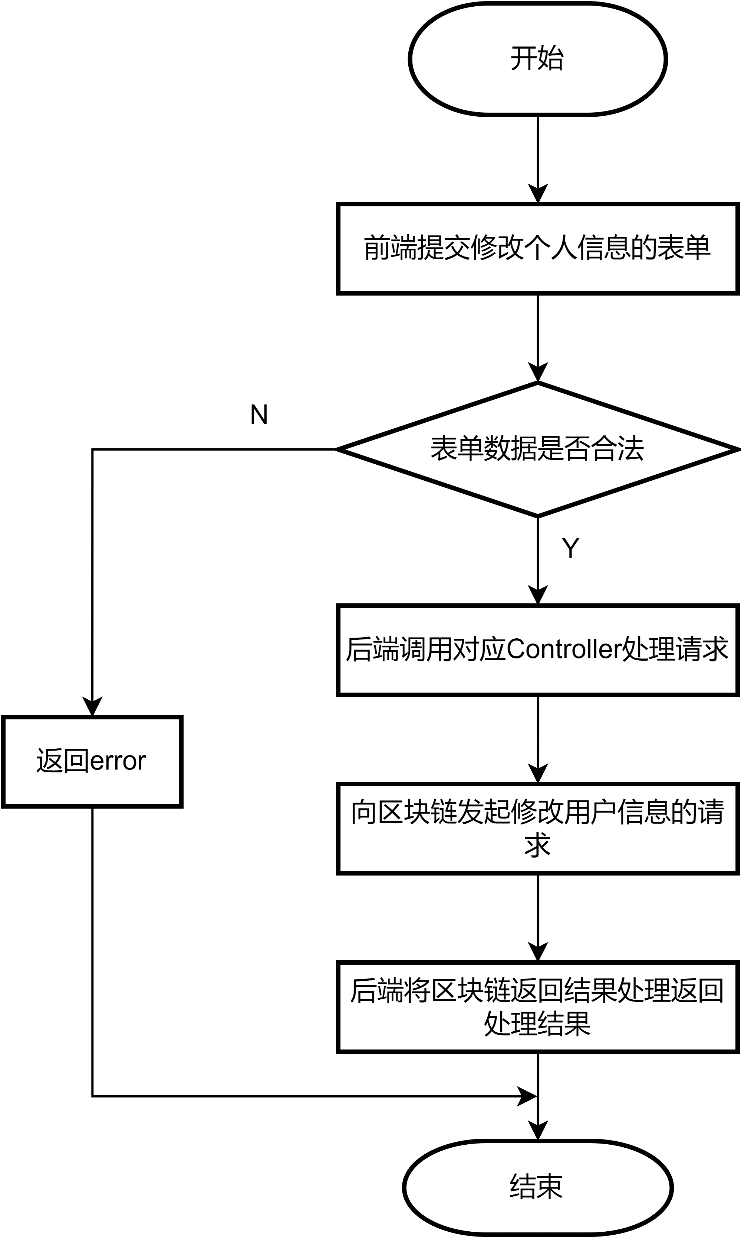
图5.3修改密码流程图

5.3 个人信息管理模块的实现

个人信息模块主要包含个人信息查看，个人信息修改这两个功能。主要需要实现用户界面层的操作台界面的个人信息模块，业务逻辑层的UserController与FabricController中关于修改用户信息的部分，区块链网络层智能合约中个人信息相关的部分。该模块只可对账本中的用户信息进行查看与修改，而证据管理模块与证据分享模块可对账本中的对应数据进行删除。

修改个人信息功能流程如下，用户需要在修改个人信息表单内填写修改后的个人信息。在填写表单数据时，前端会检测用户输入的数据是否合法，若不合法将不可提交表单。用户提交合法的表单数据至后端后，后端对应的Controller将对该表单数据及逆行再次检测。若检测成功，将向区块链发起修改个人信息的请求，区块链处理后将处理结果返回给后端，后端将该结果处理后再将后端处理的结果响应给前端，前端将显示修改个人信息成功与否。

该系统的修改个人信息流程图如图5.4所示

图5.4修改个人信息流程图

5.4 证据管理模块的实现

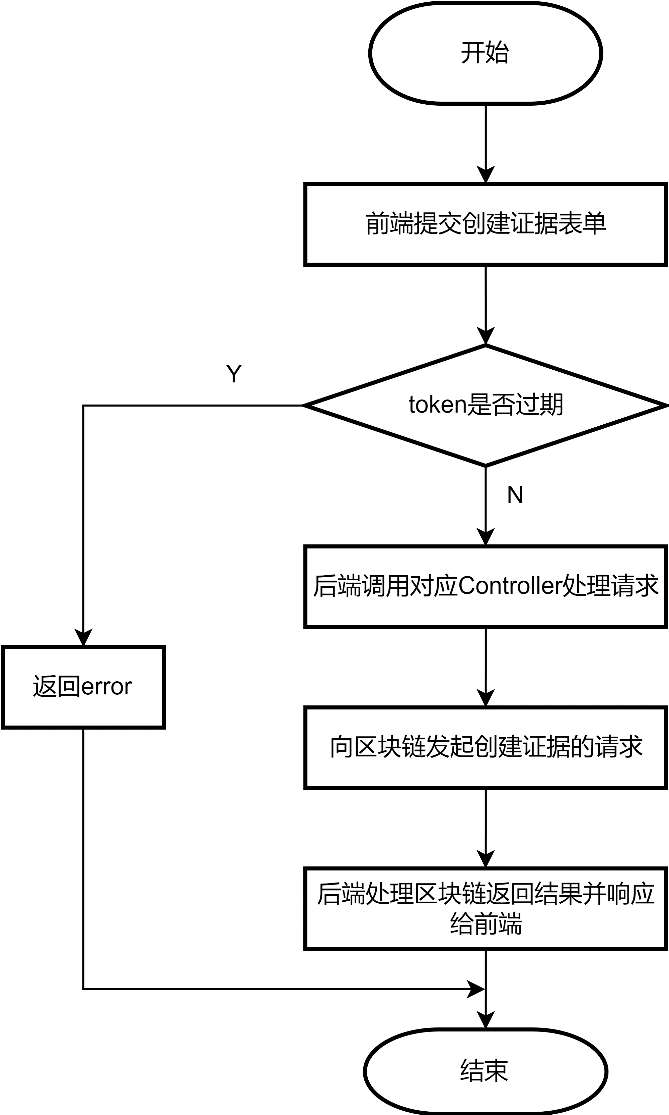
证据管理模块是该系统的核心，该功能模块主要包含证据的创建，删除，修改，查看，加密等功能。主要需要实现用户界面层的证据创建界面与个人证据管理界面，业务逻辑层的EvidenceController与FabricController中证据相关的部分，区块链网络层中证据相关的部分。

证据的创建，删除，修改，查看功能的实现的逻辑流程均为前端发起功能对应的HTTP请求，后端查验token成功后调用EvidenceController对应的处理方法。在对应的处理方法中，invoke或query区块链智能合约中的函数，invoke方法会对账本进行修改，query则是对账本进行查询，在智能合约对应的函数中对账本中的数据进行创建，删除，修改或查询。区块链将结果返回给后端，后端根据其结果响应前端。

以创建证据功能为例，用户进入证据创建界面填写对应的表单。表单内容包含证据类型选择，证据描述，证据加密算法，证据是否私有，证据文件上传。证据类型选择限制了上传的文件的格式，证据是否私有则控制了该文件的基础权限。证据加密算法控制了该证据文件将被采取何种加密算法加密。若证据选择私有，则其他用户无法在证据库界面查询到该证据，若证据选择公开，则证据可被其他用户在证据库界面查询到并申请相关权限。

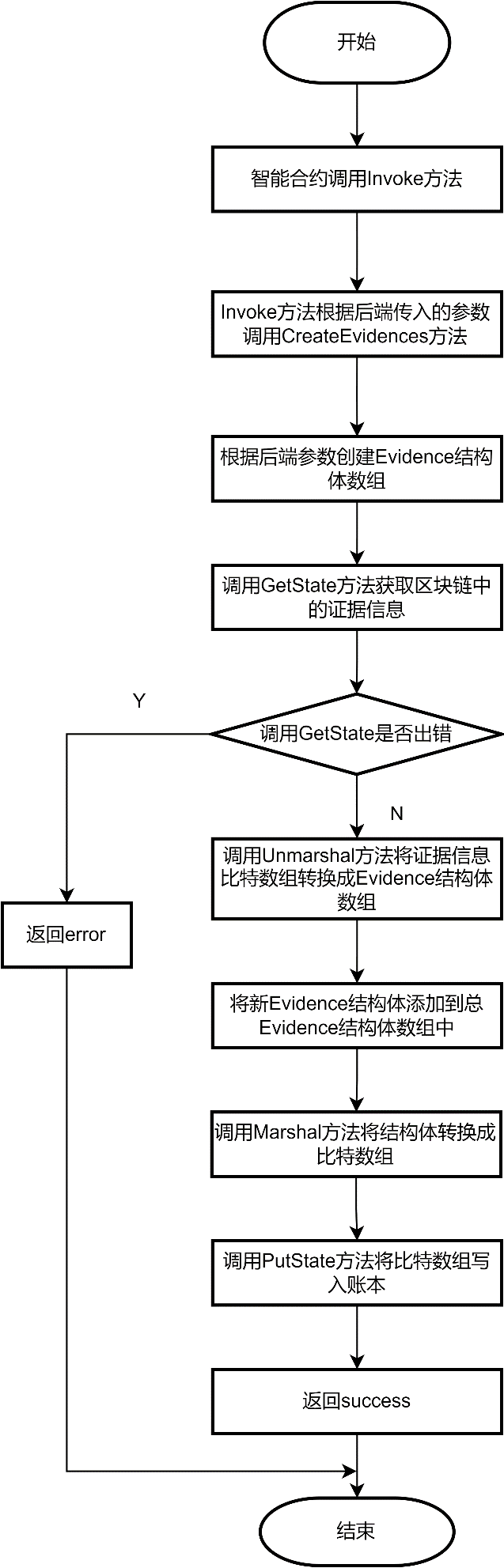
当用户填写好表单后向后端发起HTTP请求，由于此次请求设计文件上传，故使用formData数据格式 作为HTTP的POST请求的请求体。后端接受到formData格式的请求体后将使用解析formData的中间件将formData中的文件数据解析为Buffer，将其他非文件的key-value形式的数据解析为对象。将其中代表文件的数据根据文件格式转换为对应格式编码的字符串，例如证据为图片文件会将buffer读取为base64编码格式的字符串，之后将对应格式编码的字符串按照用户选择的加密算法加密。将加密后的字符串写入文件，并将前端传入的其他非文件的数据处理后invoke智能合约中的createEvidences函数并传入相关参数。区块链处理后端发起的请求，随后将处理后的结果返回给后端，后端根据区块链层调用成功与否响应前端对应的提示信息。

该系统的创建证据流程图如图5.5所示

图5.5创建证据流程图

区块链收到后端发起的请求后，首先会执行链码中的Invoke函数，之后根据请求的参数去调用智能合约中对应的createEvidence函数，智能合约中的函数可通过第一个预设参数stub调用其核心方法GetState并传入比特数组获取，写入区块链账本则需要调用另一核心方法PutStatue以key-value形式写入，其value也是需要比特数组对象。Go语言内置包encoding/json提供了Marshal方法实现将比特数组转换为结构体与对应的Unmarshal方法将结构体转化为比特数组。

智能合约创建证据流程图如图5.6所示

图5.6智能合约创建证据流程图

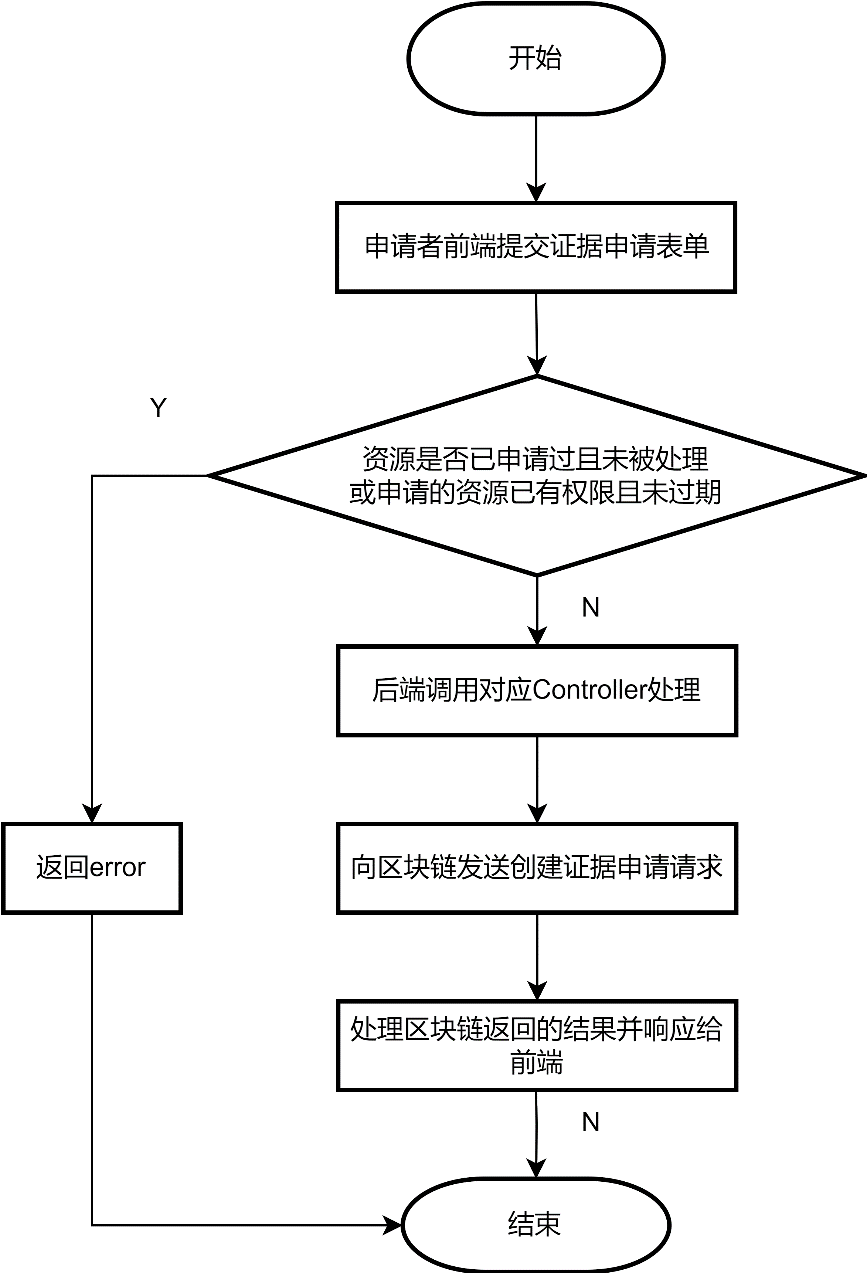
5.5 证据共享模块的实现

证据共享模块是为了用户间能够安全的进行证据信息共享。该功能模块主要包含向公开证据发出申请与处理他人申请两个功能。主要需要实现用户界面层的证据库界面，我的申请界面以及申请处理界面。证据库界面显示所有公开的证据，用户可在该页面向其他公开证据发出申请。我的申请界面显示我向其他人的公开证据发出的申请，可查看我发出的申请的进度，申请通过后，可在证据库界面与我的申请界面查看自己申请的信息。申请处理界面显示其他人向我的公开证据发出的申请，可选择同意或决绝。业务逻辑层则需要实现ApplicationController，其中包含对申请的创建，删除，处理等功能。区块链网络层则需要实现智能合约中与申请相关的函数，包含对账本中的

申请进行创建，删除，处理等。

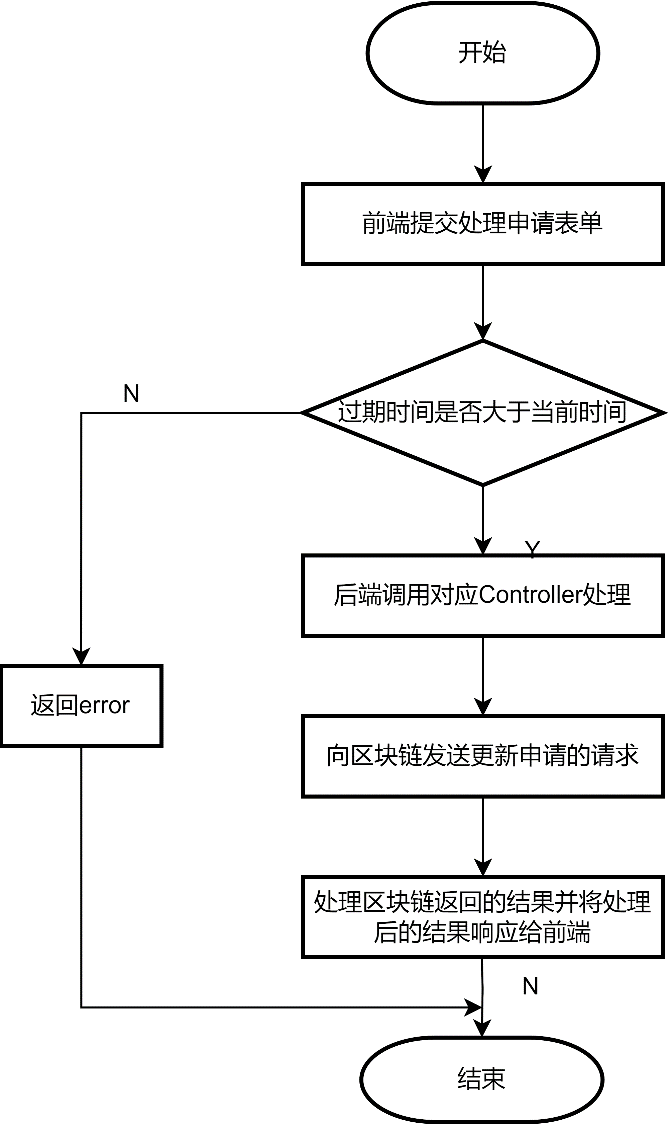
申请证据功能流程如下，申请者发送创建证据申请表单，如果后端查询到被申请的证据是否已申请过且处理者未处理，或者申请者已经有被申请资源的权限且未过期。则申请失败。反之，后端对应的ApplicationController将会处理该请求，ApplicationController会向区块链发起Invoke createApplication请求，区块链收到请求后将结果响应给后端，后端处理区块链返回的结果并将处理后的结果响应给前端。

申请证据流程图如图5.7所示

图5.7申请证据流程图

处理证据申请流程如下，若同意申请则需要填写权限过期时间，前端会检验过期时间是否大于当前时间，若拒绝则不填写表单。前端发起处理申请的HTTP请求后，若发出同意申请的请求，后端将再次检验权限过期时间是否大于当前时间。若过期时间小于当前时间，将返回处理错误，并返回提示信息。反之，后端对应ApplicationController将会处理该请求，ApplicationController会向区块链发起Invoke updateApplication请求，区块链收到请求后将结果响应给后端，后端处理区块链返回的结果并将处理后的结果响应给前端。

处理证据申请流程图如图5.8所示

图5.8处理证据申请流程图

5.6 本章小结

本章结合前两章的内容，详细介绍了智能合约中，登录模块，个人信息管理模块，证据管理模块，证据共享模块的流程与实现方式。第一节主要介绍了智能合约中的各个函数的名称与功能，第二节辅以流程图详细阐述了登录模块的注册，登录与忘记密码功能，第三节主要介绍了该模块的个人信息修改功能，第四节的证据管理模块是核心模块，以创建证据为例详细说明了从前端到后端，后端到区块链交互的全部流程。

6 系统测试

本章主要对该系统的测试环境，单元测试与系统测试进行说明，同时对用户界面进行了展示。

6.1 测试环境

操作系统：ubuntu 22.04.2 LTS

区块链网络：HyperLedger Fabric

开发语言：前端使用TypeScript，后端使用Node 16.19.0，智能合约使用Go 1.20

6.2 功能测试

6.2.1 登录模块测试

登录模块包含注册，登录，修改密码功能。测试用例如表6.1所示

表6.1登录模块测试用例表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 测试目的 | 测试内容 | 预期结果 | 测试结果 |
| A-1 | 用户能否注册 | 输入合法数据 | 新用户注册成功 | 通过 |
| A-2 | 用户能否注册 | 输入非法数据 | 注册失败并显示错误信息 | 通过 |
| A-3 | 用户能否登录 | 输入注册成功的账号 | 登录成功并进入主界面 | 通过 |
| A-4 | 用户能否修改密码 | 在修改密码界面内更改密码 | 修改密码成功并显示提示信息 | 通过 |
| A-5 | 用户能否使用新密码登录 | 输入新密码登录 | 登陆成功并进入主界面 | 通过 |

注册时用户需要输入合法的邮箱与两次相同的密码以及邮箱验证码，点击注册按钮完成注册。当输入的数据不合法或两次密码不相同或邮箱验证码错误，界面上方将显示具体信息。注册界面如图6.1所示

登陆时用户输入已注册的邮箱与密码点击登陆后即可进入系统主页。当输入的邮箱未注册或密码错误，界面上方将显示具体信息。登录界面如图6.2所示

6.2.2 个人信息管理模块测试

个人信息管理模块主要包含查看个人信息，修改个人信息功能。测试用例如表6.2所示。

表6.2个人信息管理模块测试用例表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 测试目的 | 测试内容 | 预期结果 | 测试结果 |
| B-1 | 用户能否查看个人信息 | 进入个人信息界面 | 显示个人信息 | 通过 |
| B-2 | 用户能否修改个人信息 | 输入合法数据 | 个人信息修改成功并显示提示信息 | 通过 |
| B-3 | 用户能否修改个人信息 | 输入非法数据 | 个人信息修改失败并显示错误信息 | 通过 |

图6.5查看个人信息界面

6.2.3 证据管理模块测试

证据管理模块主要包含证据的创建、删除、修改、查询、加密功能。测试用例如表6.3所示。

表6.3证据管理模块测试用例表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 测试目的 | 测试内容 | 预期结果 | 测试结果 |
| C-1 | 能否创建证据 | 输入合法文件 | 创建成功后跳转个人人证据界面 | 通过 |
| C-2 | 能否创建证据 | 输入非法文件 | 创建失败并显示错误信息 | 通过 |
| C-3 | 能否删除证据 | 点击删除 | 删除成功并更新证据列表 | 通过 |
| C-4 | 能否修改证据信息 | 输入合法数据 | 修改成功并更新信息 | 通过 |
| C-4 | 能否修改证据信息 | 输入非法数据 | 修改失败并显示错误信息 | 通过 |
| C-5 | 能否查看个人证据 | 进入个人证据界面 | 显示个人证据信息 | 通过 |
| C-6 | 能否加密证据信息 | 修改证据信息加密算法 | 修改后显示修改成功并更新证据信息 | 通过 |

6.2.5 证据共享模块测试

证据共享模块主要包含证据申请与处理申请功能。测试用例如表6.4所示

表6.4证据共享模块用例表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 测试目的 | 测试内容 | 预期结果 | 测试结果 |
| D-1 | 能否查看他人公开证据 | 进入证据库界面 | 显示所有用户公开证据 | 通过 |
| D-2 | 能否申请他人证据 | 点击申请下载或申请查看证据信息 | 点击申请后界面上面显示提示信息 | 通过 |
| D-3 | 能否查看我的申请的进度 | 进入我的申请界面 | 可看到我的申请的进度 | 通过 |
| D-4 | 能否处理他人申请 | 进入他人申请界面处理他人申请 | 点击同意后，申请人将获得权限。点击拒绝后，申请人获得提示信息 | 通过 |

证据库界面如图所示，可查看所有用户的公开证据，且含有申请按钮与解密按钮申请证据的权限

我的申请界面如图所示，可查看我的申请的进度

他人申请如图所示，可处理他人发起的申请

6.3 本章小结

测试是保障软件质量的一种有效的手段，本章详细介绍了各个模块的功能测试，对各个模块进行了用例测试与分析。分别对于前文提及的登录模块，个人信息管理模块，证据管理模块与证据分享模块进行了功能测试，经过不断的发现、分析、总结并解决问题，最终使系统致臻完善。

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