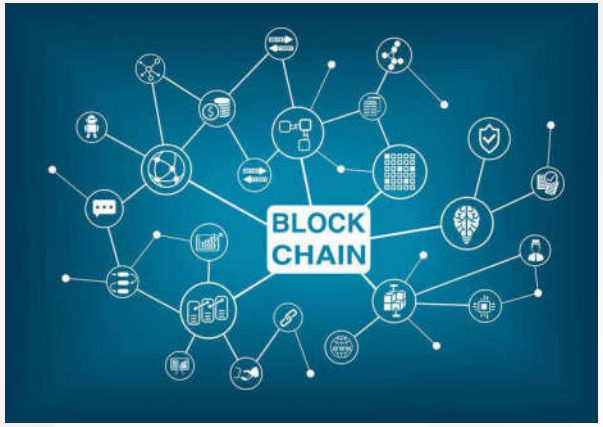
基于区块链的存证系统

团队名称：南山老火锅
指导老师：徐光侠（教授）
团队成员：熊宇、陈云龙、刘文婧、赖恩梅、王有臻、邓思铭

目录 content

01 综述

01 综述



区块链技术

2008年，Nakamoto S.第一次提出区块链的概念，主要特征有去中心化、不可篡改性、匿名性、自治性等。2016年10月，在工信部发布的《中国区块链技术和应用发展白皮书（2016）》中，区块链技术被确定重点发展的前沿性技术。

电子证据

2012年“电子数据”被《民事诉讼法》纳入证据的法定种类之一，标志着电子证据在诉讼中取得了合法地位。2016年9月，最高人民法院、最高人民检察院、公安部结合司法实际，根据《中华人民共和国刑事诉讼法》等有关法律规定，制定《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》。

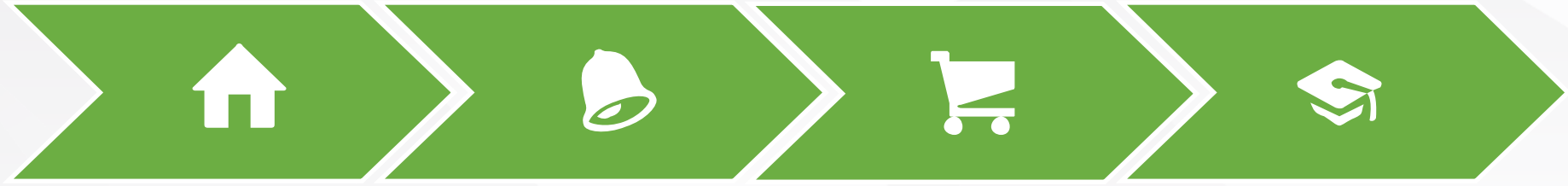
电子证据的保全

由于电子证据与传统证据相比更加脆弱易失，容易被篡改和销毁，因此深入研究电子证据的保全对指导司法工作具有重要意义。证安链将结合电子证据保全的需求与区块链本身具备的去中心化和不可篡改特性，结合区块链技术分布式的结构，解决当前电子证据保全过程中面临的取证，存证困难问题，通过系统保证电子证据的原始性、客观性、有效性，进而推动电子数据的存证保全和司法落地。

02 项目说明

02 项目说明

2.1 设计思路



考虑到区块链技术的安全性，将区块链技术与电子证据保全 进行结合可以补足传统电子证据保全的不足之处。

考虑到目前已经拥有成熟的区块链平台和较为完备的区块链底层结构，再对区块链底层进行搭建就会将项目的工作变得繁琐冗余。所以本项目的区块链技术部分决定采用以太坊的技术。

项目使用 Spring Boot + Spring MVC + Spring Security 作为基础架构， Bootstrap作为前端响应式框架。在以太坊平台的基础上采用 solidity 编写 项目所需智能合约，实现电子证据的保全。

证安链致力于提供适用于电子证据保全业务的服务，并不再上添加除存、取、 分析等必要动作之外的功能，保证代码的简洁清晰。

02 项目说明

2.2 项目模型

项目采用 EEPM 系统架构为电子证据提供”信任“与”安全“。实现电子证据保全服务器的去中心化，提供数据安全保障没信息不可篡改、可溯源的机制。该模型的底层采用通过以太坊平台调用智能合约与区块链数据交互，达到数据存储，完成证据保全相关逻辑的目的，项目整体架构如图1所示。

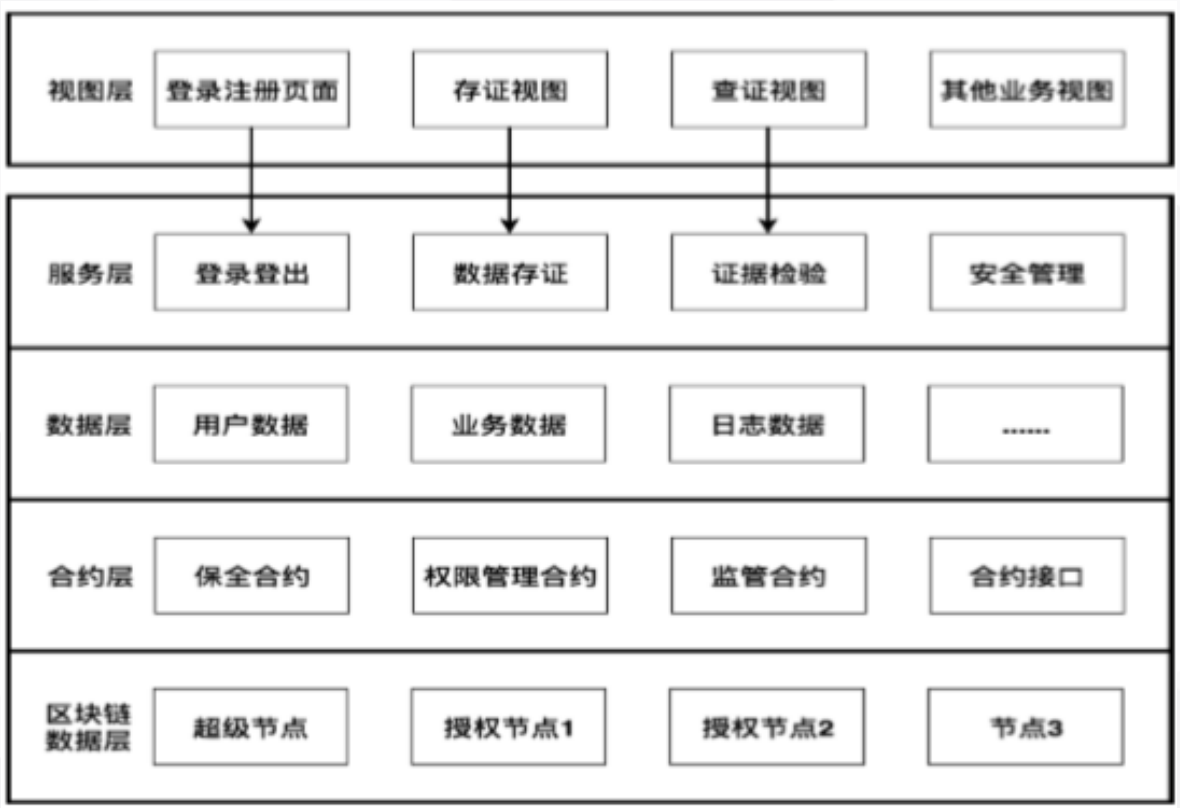


图1 EEPM电子证据保全模型架构图

02 项目说明

2.2 项目模型

整个模型依赖与以太坊技术，但是依然需要在节点管理中做出个性化配置。在理想环境下，EEPM 模型结构中不同的节点可以由不同计算能力的服务器构成，各节点应具有以下特征：

1 节点间采用联盟链设计，加入节点需要获取授权

2 节点角色应当由国家权力机关、高校、律师协会、网络安全协会等具有高可信度，且相互制约的权利机关，团体组织构成

3 节点需要具有备份与宕机授权机制，保证系统同步进程，维持数据完整性

02 项目说明

2.2 项目模型

节点间通信需要解决拜占庭容错问题，EEPM 系统则采用联盟链为底层结构，内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定。而预选节点间采用基于以太坊的更高效率的 PoS 共识算法，保障数据一致性。宏观如图2 所示：

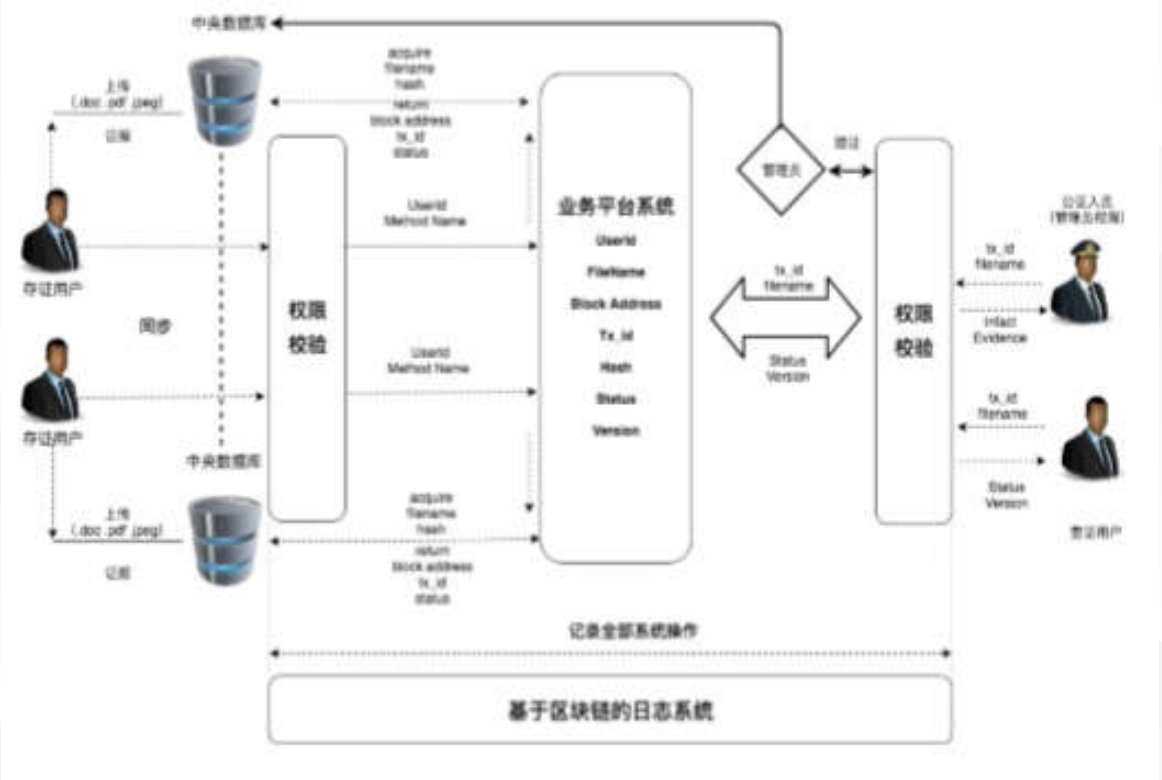


图2 EEPM模型图

02 项目说明

2.3 数据库架构

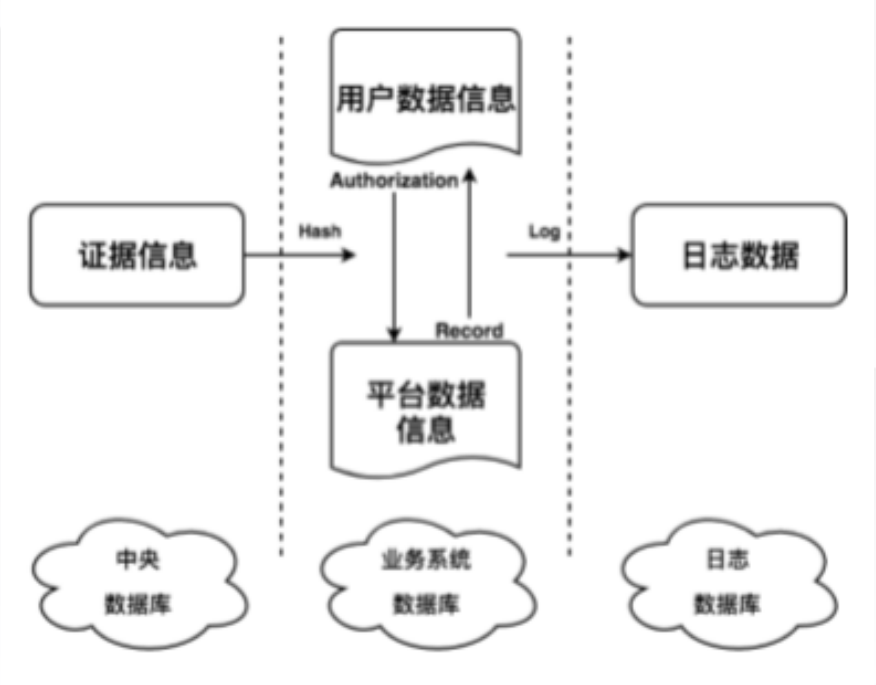


图3数据库架构图

项目数据由四部分数据组成，分别为完整的证据信息、用户数据信息、平台业务数据、日志数据。

模型中仅保存证据信息的Hash值，采用独立式数据库架构，将完整的证据信息保存在中央数据库或用户认为可信任的第三方数据库中，同时要求数据库采用多备份的原则，保障数据的安全性，提高信息的抗灾能力。

日志信息的存储独立于业务系统，同时以区块链技术背书，让所有日志信息上链，保障日志信息的准确性，可靠性，不可篡改性。分离式数据库架构可以保障当业务系统故障、宕机时，依然能够独立地获取完整日志信息。

02 项目说明

2.4 系统角色特征

存证用户：

主要面向在离线环境提取电子证据的专业证据提取人员以及对文件、合同等电子数据有保全需求的普通证据保全人员 。

普通查证人员：

根据证据编号，利用节点查询区块并验证区块链系统中保全的Hash摘要值是否与目标证据匹配 。

高级调查员：

在电子证据作为合法证据呈现时，根据证据编号，获取调用智能合约权限并对证据关键信息进行提取，同时向证据中心数据库请求读取完整证据信息，并分析电子证据得出结论 。

系统管理员：

管理员具有分配电子证据调查权限的能力，同时可以对系统中的账户信息进行管理 。

02 项目说明

2.4 系统角色特征

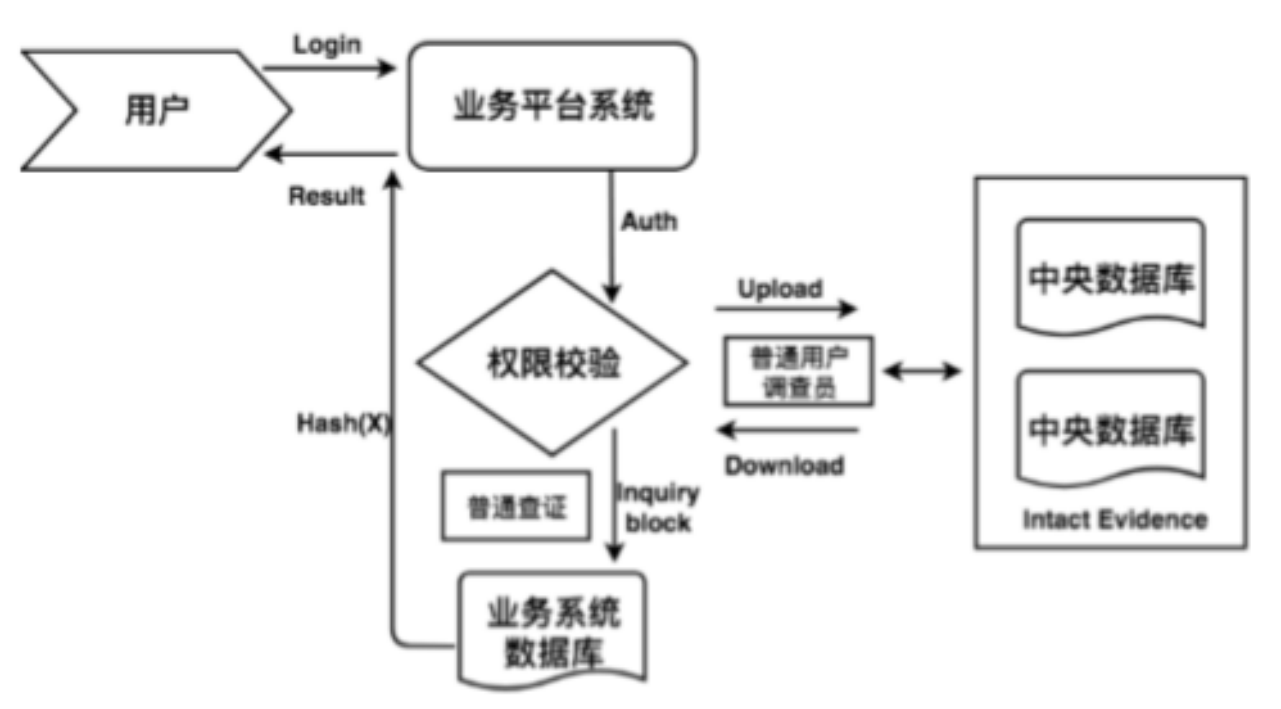


图4 用户业务模型

02 项目说明

2.5 系统安全性

EEPM 模型系统要求全站采用 HTTPS 协议。这样的优势是不仅能够建立一个安全的信息传输通道，保证数据传输的安全。还能使用户能够及时确认网站的真实性。凡是采用 HTTPS 协议搭建的 B/S 系统，都可以通过浏览器地址栏的锁头标志来验证网站的真实信息，也可以通过 CA 机构查询。对于整个模型而言，HTTPS 协议能有效防范中间人攻击并保障数据在传输过程中的安全。基于 B/S 模式的模型系统 HTTPS 信息如图所示。

图5 https协议

03 智能合约安全分析

03 智能合约安全分析

1、虽然提示有private修饰器，在以太坊中，不存在隐私性，矿工可以访问合约中所有的代码和数据。

2、但是在智能合约中使用了多种权限控制修饰器来限制不同角色的权限。

3、即使矿工可以访问数据，获取到密钥也不能上传修改证据的分析结果。

4、整个合约中，给不同的角色赋予了严格的权限，没有相应的权限是访问和修改的。

03 智能合约安全分析

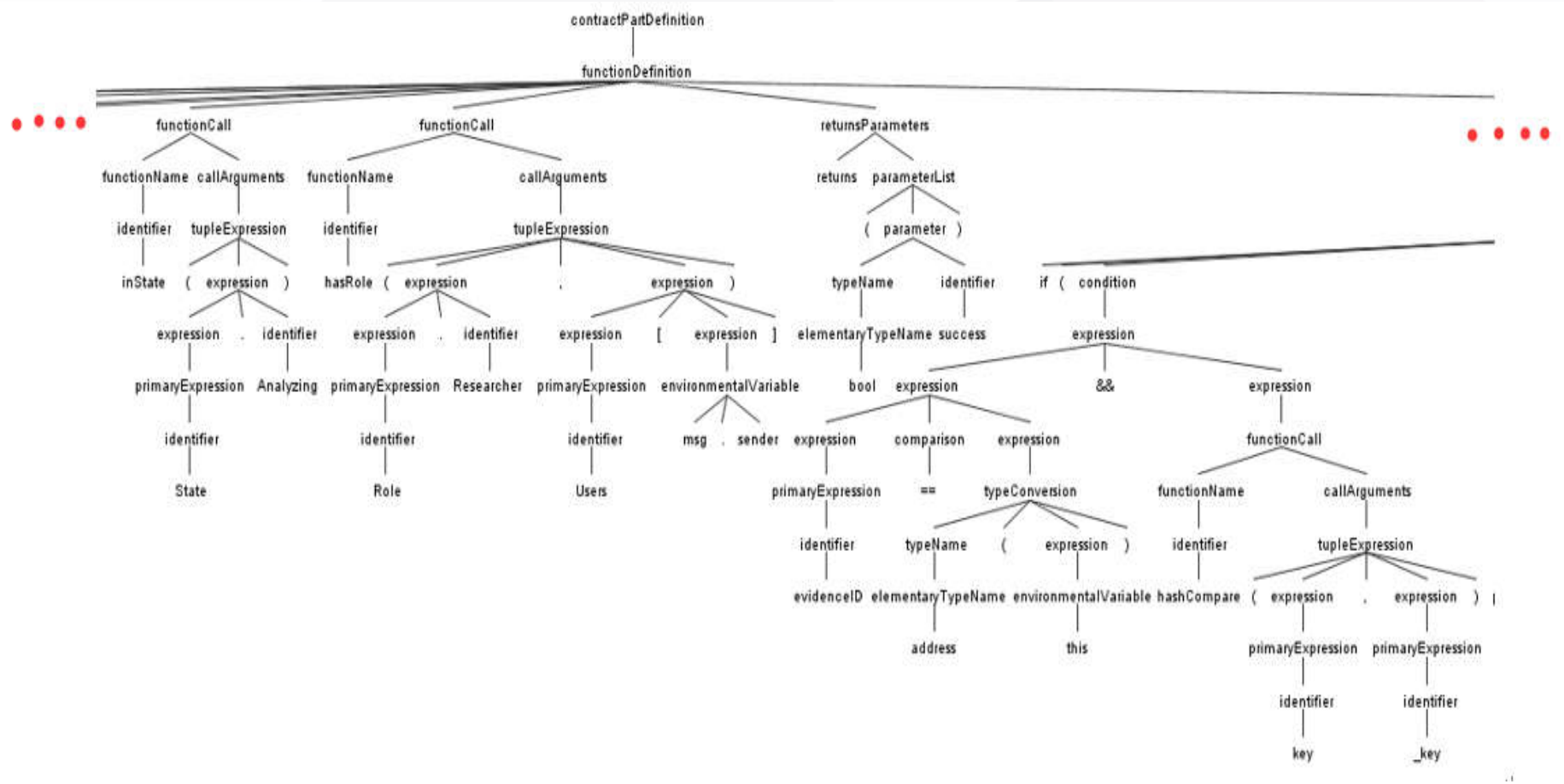
```
function uploadAnalysisResult(string memory _AnalysisResult, address evidenceID, string memory _key)
public checkRoleState inState(State .Analyzing)
hasRole(Role.Researcher, Users[msg.sender]
) returns (bool success){

    if (evidenceID == address(this) && hashCompare(key, _key)) {
        analysisResult = _AnalysisResult;
        evidenceState = State.Analyzed;
        emit Analyzed(msg.sender, name, address(this));
        return true;
    }
    return false;
}
```

```
modifier inState(State _state) {
    require(
        evidenceState == _state,
        "Invalid state."
    );
    _;
}

modifier hasRole(Role role, User memory user){
    require(
        user.role == role,
        "You do not have sufficient permissions to call this."
    );
    _;
}

modifier checkRoleState() {
    require(
        Users[msg.sender].roleState == RoleState.Normal,
       "RoleState is locked."
    );
    _;
}
```

如图所示，checkRoleState， inState(State .Analyzing)，hasRole(Role.Researcher,Users[msg.sender])这几个权限进行限制，仅当满足调用者是研究者且状态正常时，才能调用次函数。而研究者权限是管理员赋予的，在这些过程中的权限控制都使用的是mgs.sender和自定义的角色权限，这些都是我们合约的优势以及安全处。然后当调用函数执行时仅当证据地址是此合约地址，并且密钥相等是才能正确上传，进一步验证了我们合约的安全性。

03 智能合约安全分析

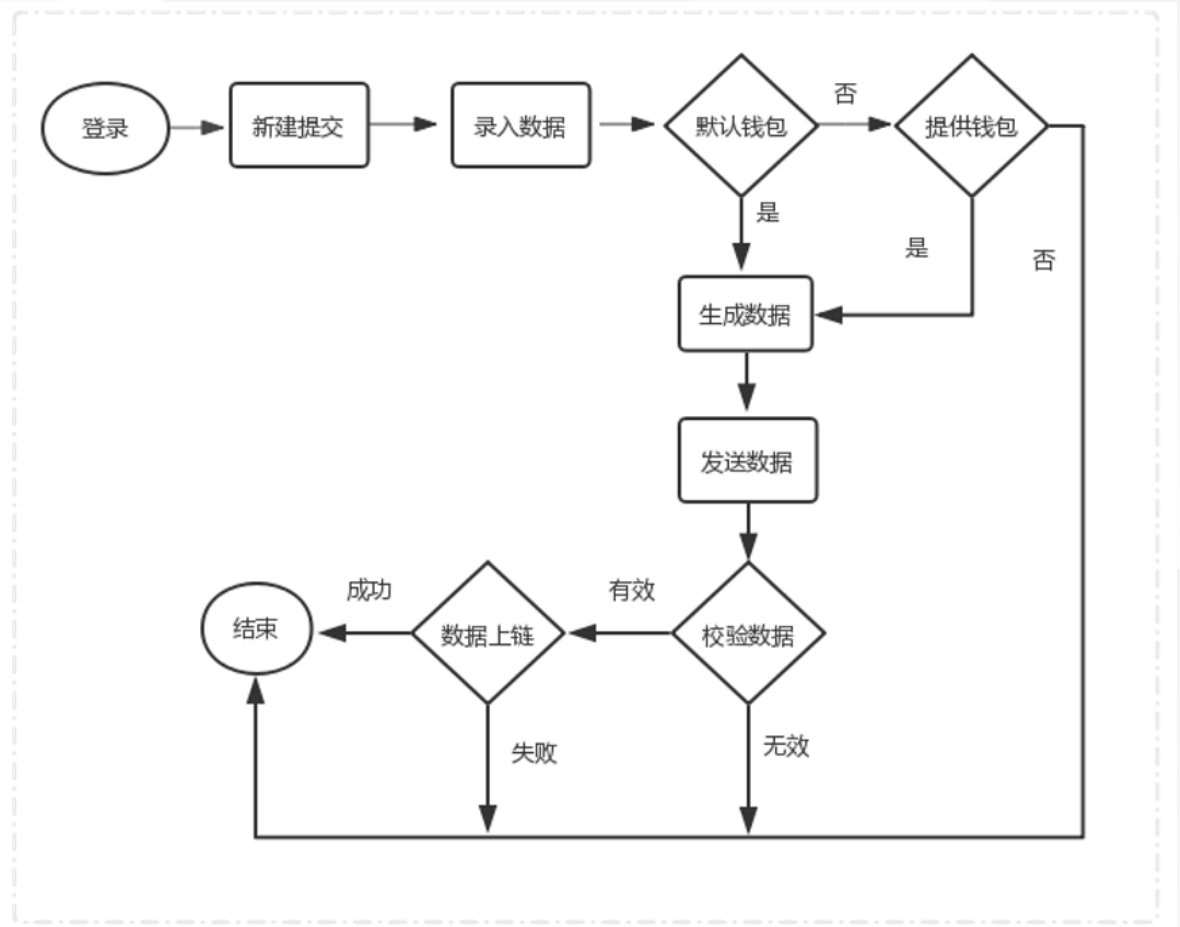
- 根据下面这个函数的抽象语法分析树，更清晰地证明我们合约的安全性。



04 项目实现

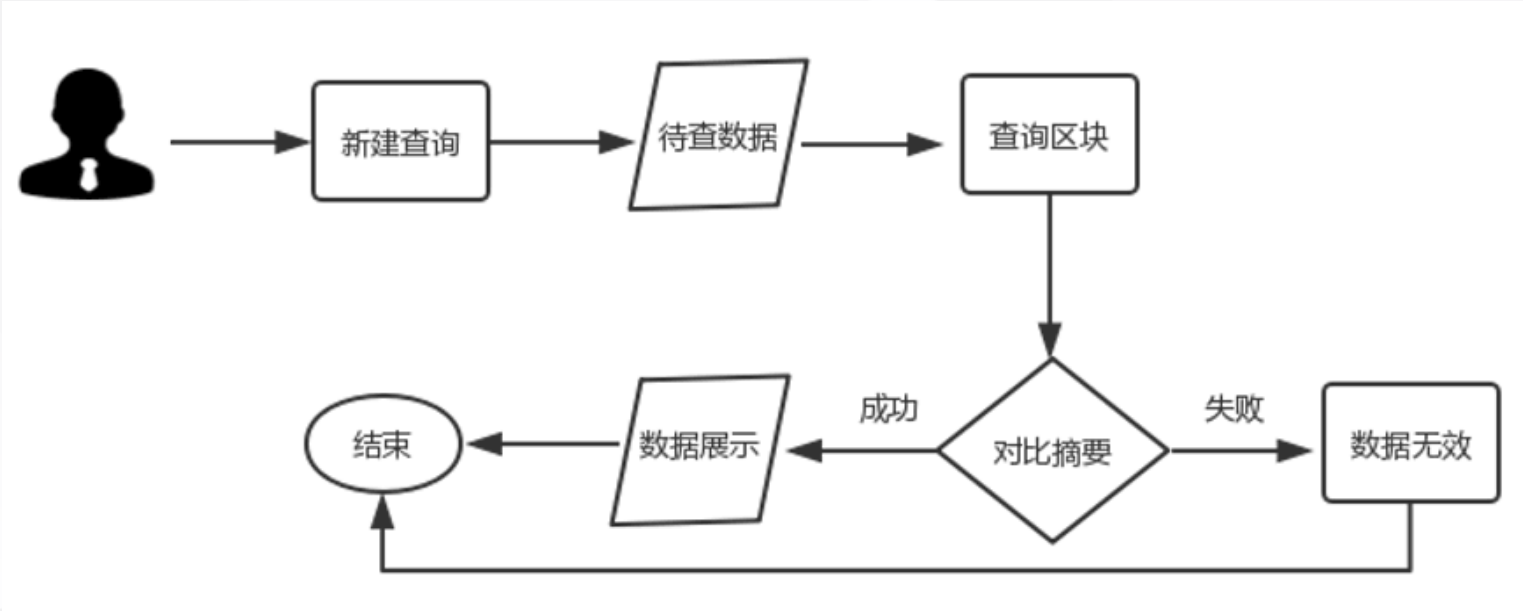
04 项目流程

- 用户提交证据流程图



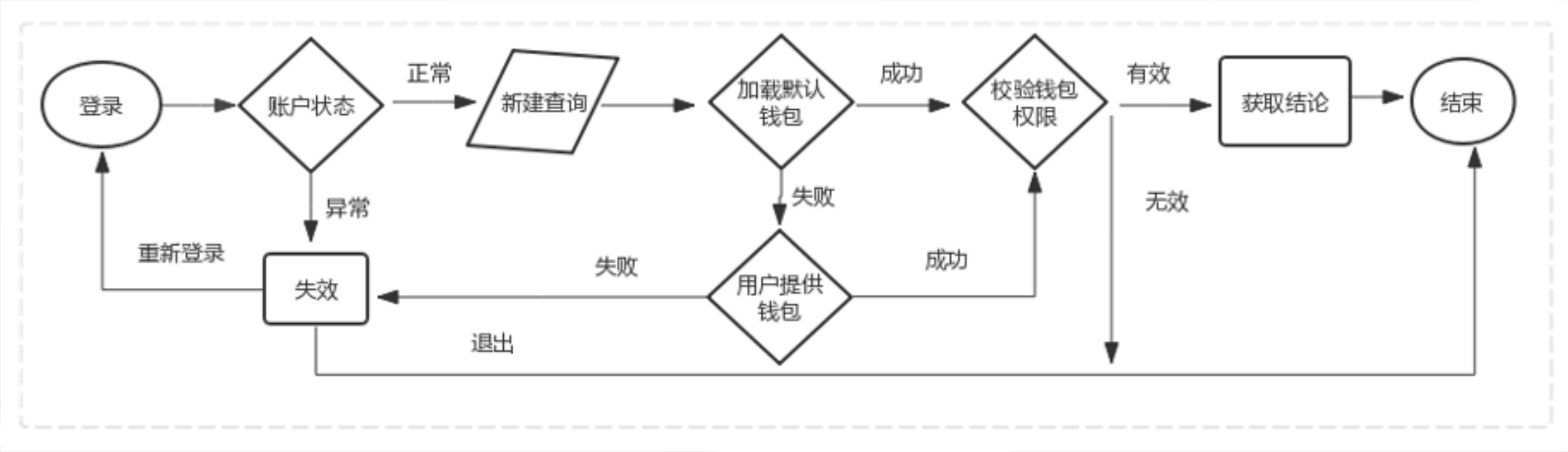
04 项目流程

- 用户查询证据流程图



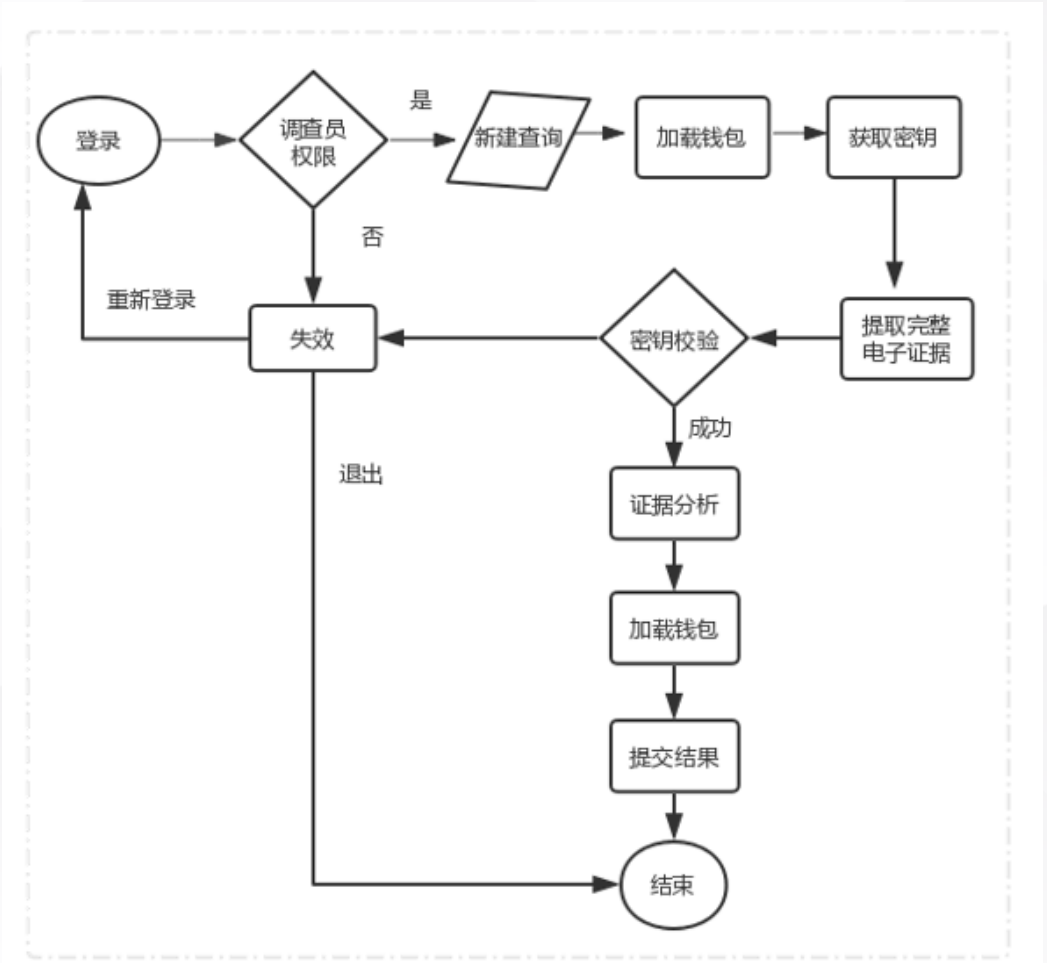
04 项目流程

- 用户获取证据分析结论流程图



04 项目流程

- 调查员分析证据流程图



05 总结

05 总结

项目源代码已经开源上传至Github，项目源代码地址：

https://github.com/ybeario/blockchain_ultra

项目展示地址：

https://www.ybear-web.com

欢迎加入本开源项目。

单击此处输入标题

指导老师

徐光霞（教授）

项目设计

熊宇、陈云龙、刘文婧、赖恩梅、王有臻、邓思铭

项目开发

熊宇、陈云龙、邓思铭

特别致谢

杜江（教授）

CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS
重庆邮电大学
1950

感谢评委
请多多指正