文章编号：2096-1472(2023)-05-45-04
DOI:10.19644/j.cnki.issn2096-1472.2023.005.010

基于联盟链的行程溯源校验系统的设计与实现分析

蔡超萍，康晓凤，王 可，张百川，王 宇

(徐州工程学院信息工程学院，江苏 徐州 221000)
✉syldyx2020@163.com; kxfeng07@163.com; admi1n@163.com;
aesp3j0@gmail.com; wy2550384694@163.com

摘 要：为有效控制传染病毒，精准检测传染病例的个人行程轨迹尤其重要，但恶意伪造行程码的开源项目困扰了溯源工作，因此数据防伪成为溯源工作中急需解决的问题。基于Hyperledger Fabric框架搭建联盟链，开放远程过程调用协议(Remote Procedure Call，RPC)服务提供链码，实现与区块链上数据的交互，采用智能合约与共享账本技术，实现区块溯源。系统的Web端前端后分离，前端使用VUE和Element-UI技术实现图形化用户界面，后端使用Spring身份控制技术分离权限，采用椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm，ECDSA)进行签名，实现防篡改和数据保护功能。

关键词：区块链；联盟链；行程溯源；数字签名
中图分类号：TP315 **文献标识码**：A

Design and Implementation of the Itinerary Traceability Verification System based on Consortium Blockchain

CAI Chaoping, KANG Xiaofeng, WANG Ke, ZHANG Baichuan, WANG Yu

(*School of Information Engineering, Xuzhou Institute of Technology, Xuzhou* 221000, *China*)
✉syldyx2020@163.com; kxfeng07@163.com; admi1n@163.com;
aesp3j0@gmail.com; wy2550384694@163.com

Abstract: In order to effectively control the infectious virus, it is particularly significant to accurately detect the personal itinerary path of infected cases. However, the open-source project that maliciously forges the itinerary code has troubled the traceability work. Therefore, data anti-counterfeiting has become an urgent problem to be solved in the traceability work. Based on Hyperledger Fabric framework, the consortium blockchain is built and RPC (Remote Procedure Call) service is opened to provide the chain code, so that the interaction with the data on the blockchain is realized. Intelligent contract and shared ledger technology are adopted to realize the block traceability. The frontend of Web application of the system is separated from the rear end, with the front end using VUE and Element-UI technology to achieve a graphical user interface, and with the rear end using Spring identity control technology to separate permissions. The Elliptic Curve Digital Signature Algorithm (ECDSA) is adopted for signature, achieving tamper resistance and data protection functions.

Keywords: blockchain; consortium blockchain; itinerary traceability; digital signature

1 引言(Introduction)

行程码对防控病毒传播起到了至关重要的作用。一些不法分子恶意伪造行程码，给疾病管控部门的传染病防控工作带来了巨大的困难，也给社会卫生安全带来了严重威胁。为了避免类似事件的发生，行程码的数据防伪就成为行程溯源工作中亟待解决的问题。

本系统通过提供请求者IP(Internet Protocol，网际互联协议)位置的API(Application Programming Interface，应用程序编程接口)，返回json格式的地理位置(精确到区)信息，后端通过工具类JsonUtil处理此信息，再结合打卡时间和用户姓名生成行程对象，行程对象上传到区块链后，根据返回的哈希值生成公钥和私钥，使用私钥对json字符串加密，并把

基金项目：2022年大学生创新训练计划基金项目(xcx2022190，xcx2022192)。

加密结果和公钥写入数字二维码，达到防止伪造行程码的目的。由于区块链具有信息不可篡改的特点，所以可以根据区块的哈希值对用户的行程溯源。Web应用前后端分离，前端使用VUE和Element-UI技术实现图形化用户界面，后端使用Spring身份控制技术分离权限，同时采用ECDSA算法进行签名，实现防篡改和数据保护功能。对比RSA(Rivest-Shamir-Adleman)算法，ECDSA(Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法)既保障了信息安全，又降低了算法复杂度[1]。

2 联盟链和ECDSA简介(Introduction to consortium blockchain and ECDSA)

联盟链是一种基于区块链技术的分布式账本技术，也是一种特殊的区块链[2]，由一组受信任的参与者组成，能安全地共享数据和信息，同时具有如下优势：可以防止未经授权的访问和篡改，提供更高的安全性；可以减少交易的确认时间，提供更快的交易速度；其成本相较于公共区块链更低，能够减少网络中的节点数量，减少硬件需求；可以提供高扩展性，支持更多的参与者和应用程序。

ECDSA是一种基于椭圆曲线密码学的数字签名算法，也是一种公钥密码体制[3]，用于确保数据的完整性和可靠性。ECDSA使用椭圆曲线算法生成公钥和私钥，其安全性取决于椭圆曲线的安全性即阶的选择，因为它使用更少的计算量生成公钥和私钥，并且可以提供更高的安全性，所以安全性比RSA更高[3]。ECDSA的签名过程非常简单，首先对消息进行哈希计算，其次使用私钥对哈希值加密形成签名，最后使用公钥对签名进行验证。

3 系统设计与实现(System design and implementation)

本系统的核心技术为ECDSA算法和Hyperledger Fabric联盟链技术，核心模块包括Web端和联盟链。Web端分前后两个部分，Web前端采用广泛使用的JavaScript库VUE3结合Element-UI构建网页，后端采用Spring-Boot搭建控制层，并采用Redis缓存数据。联盟链部分在前端加载Fabric Client库与Fabric Ca Client，通过RPC(Remote Procedure Call，远程过程调用协议)服务与另一台服务器上的联盟链的Order和Peer节点进行通信，并在本地SQL(Structured Query Language)数据库保存一份与上传数据相同的备份[4]。综合使用以上技术设计实现了本系统，包括用户管理、行程生成、行程校验和行程溯源四大模块，系统模块如图1所示。

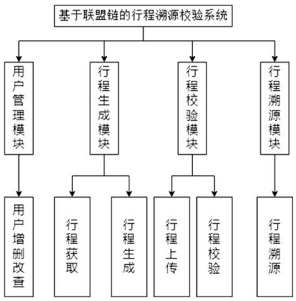

图1 系统模块

Fig.1 System module

3.1 用户管理模块

本系统没有直接提供注册功能，通过直接添加数据库的特权用户分别管理低级权限的用户。在Spring中使用@PreAuthorize注解控制用户权限[5]，规定只有拥有某项权限的用户才可以调用某项函数。Spring Security的访问控制原理是基于角色的访问控制(Role-Based Access Control，RBAC)，它将用户分配到不同的角色，并为每个角色分配不同的权限，从而实现访问控制。同时，在目录API中定义后端Controller层中对应的响应所需的路由，在后端使用@RequestController等注解指定相应的方法。在SQL数据库创建用户时，使用role字段赋予操作函数的具体权限，在具体函数中为超级管理员添加对用户进行“增、删、改、查”的权限，具体实现界面如图2所示，超级管理员可以管理普通用户。

角色编号	角色名称	权限字符	显示顺序	状态
1	超级管理员	admin	1	
2	普通角色	common	2	

图2 角色管理界面

Fig.2 Role management interface

3.2 行程生成模块

Web端的前端使用VUE加载地图插件vue-amap，并且向百度、高德、谷歌等厂商申请用于定位API所需的密钥，如图3所示。本系统在前端使用Axois技术通过用户IP向路由请求获取地理位置，逻辑代码再根据地理位置信息生成行程对象，通过工具类TimeToString获得实时时间写入行程对象，前端通过文本框获取用户输入的姓名等详细信息，并返回给后端写入对象，再将数据写入Peer节点。本系统有两个Peer节点，一个用于存储地址的随机编号，另一个用于存储用户的行程信息。Hyperledger Fabric提供了两种创建数据库的选择，即goleveldb(默认)与CouchDB，本系统使用-s参数创建了两个CouchDB数据库。

```
//高德地图方法
VueAMap.initAMapApiLoader({
    key: '[redacted]',
      v: '[redacted]'
});
```

图3 IP定位使用密钥

Fig.3 The key used for IP location

Hyperledger Fabric架构的通信过程如图4所示，应用向CA(Certificate Authority，证书授权)服务器发起注册，在提交行程的业务流程中向Peer节点发出提交交易的申请，同时Orderer节点对交易进行排序。区块链采用Docker搭建，通过编

写配置文件生成证书等文件，创建TraceChannel通道，在服务器中开放17051端口为交互式CLI(Command Line Interface，命令行接口)，开放17050端口为Order节点，开放两个数据库端口为Peer节点的交互接口，具体端口与节点域名如图5所示。系统采用Go语言编写链码，完成后将部署智能合约部署到联盟链，使用Hyperledger Fabric shim包实现链上数据的“增、删、改、查”业务，由于区块链具有防篡改特性，因此此业务并不是真实意义上的“增、删、改”操作，而是覆写。

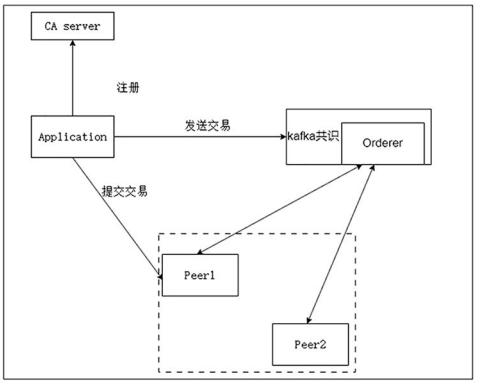

图4 Fabric架构通信

Fig.4 Fabric architecture communication

```
0.0.0.0:7051->7051/tcp, :::7051->7051/tcp, 0.0.0.0:17051->17051/tcp, :::17051->17051/t
0.0.0.0:9051->9051/tcp, :::9051->9051/tcp, 7051/tcp, 0.0.0.0:19051->19051/tcp, :::1905
4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp, :::7984->5984/tcp
4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp, :::5984->5984/tcp
0.0.0.0:7050->7050/tcp, :::7050->7050/tcp, 0.0.0.0:17050->17050/tcp, :::17050->17050/t
```

图5 具体节点

Fig.5 Specific nodes

3.3 行程校验模块

行程校验部分的主要算法为ECDSA公钥签名算法[6]。ECDSA是基于椭圆曲线上的离散对数问题，可分解为EC(Elliptic Curve，椭圆曲线)上的DSA(Digital Signature Algorithm，数字签名算法)问题。在本系统中，主要采用基于蒙哥马利曲线的一种椭圆曲线加密算法，即secp256r1[7]。该算法利用蒙哥马利曲线的特性实现安全加密，从而保护数据的安全性。Web端的后端定义了HEX编码、ECDSA签名、json处理、QRCode生成等工具类，并在控制类的逻辑代码中直接调用，降低了代码复用率。在ECDSA工具类中，系统利用java.security包中的KeyPairGenerator类获得的实体与随机数生成方法SecureRandom生成的随机数一起生成密钥对，其中私钥用于签名，公钥用于验证签名[8]。将签名所生成的哈希值写入行程对象的属性，并重写toString方法，将对象转换成json格式之后写入QRCode(QuickResponse Code，快速响应码)，QRCode的内容如图6所示。生成的QRCode保存在Download目录中，前端可以通过请求/Download路由调用后台的Download方法下载二维码。虽然行程码中的明文信息可以伪造，但是目前的计算能力还无法伪造数字签名。

图6 行程码具体内容

Fig.6 Details of the itinerary code

本系统支持用户上传行程码，大型企业机构可以通过上传ZIP压缩文件的方式批量校验行程码。Web应用的前端使用Axios与后端Java程序进行交互，实现文件上传、行程新增等功能。Web端的后端接收到上传文件后，通过文件类型调用重载的两个analyse函数。ZIP文件解压后，将文件名存入数组，再利用循环调用校验函数调用QRCode中的analyseQR方法返回二维码的具体信息。系统会将其反序列化还原为对象，并根据对象的时间、姓名与编号等属性在数据库内综合查询得到私钥[9]，然后调用ECDSA工具类中的verifyECDSA进行检验签名，ECDSA验签逻辑如图7所示，验签的结果以布尔值的形式通过/verify路由响应给Web应用的前端进行判断，并以弹窗的形式返回校验结果。

参数的选择与生成
可信方选择一个足够大的有限域p，在有限域上生成椭圆曲线，在曲线上生成一个G点，这个点的阶为q
密钥生成
1. 选取私钥s，$1<s<q$ 2. 计算$Q=sG$，Q为公钥
签名过程
1. 在有限域上生成随机数k，将明文编码为m 2. $R=kG$，计算哈希值，结果为s_1 3. $s_2=((m+s\times s_1)\times k^{-1}) \bmod q$
签名验证
1. V_1是$m\times s_2^{-1}$在有限域q上的同余式，V_2是$s_1\times s_2^{-1}$在有限域q上的同余式 2. 计算$V_1\times G+V_2\times Q$在有限域q上的哈希是否为s_1

图7 ECDSA签名逻辑

Fig.7 ECDSA signature logic

3.4 行程溯源模块

本系统使用Hyperledger Fabric在服务端搭建区块链，使用kafka共识机制，提高容错能力[10]，共识模式如图8所示。首先使用Fabric框架生成网络证书与节点证书，证书包括网络连接使用的TLS(Transport Layer Security，传输层安全性协议)证书与用于用户鉴权的CA证书，其中TLS证书也会被fabric-ca-client使用，然后使用CA创建授权用户身份与成员关系服务提供者MSP(Membership Service Providers)。使用TLS证书与MSP配置Peer和Order节点信息，Peer节点既可以保存并验证账本，又能运行智能合约，实现业务逻辑；Order节点用于验证交易并在验证成功之后提交交易至账本。本系统中的数据库为couchDB，couchDB可以对json数据进行富文本查询，使用Fabric2.4编写链码，在区块链中将链码作为外部服务，添加索引到链码之后启动网络，创建通道后

启动链码。

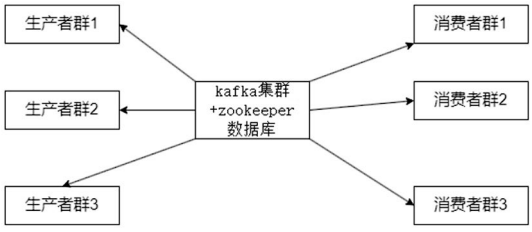

图8 kafka共识模型

Fig.8 Kafka consensus model

行程溯源部分的实现是依据区块链具有防篡改的特性，所有已上传到联盟链的数据不可更改，用户可以根据生成的区块链哈希值与区块中记录的前一个区块的哈希值进行溯源。在连接到区块链之后，通过区块号获得区块的详细信息，比如区块的编号、哈希、区块高度等信息。在Web应用的前端使用VUE定义javascript脚本，通过queryBlockBuHash函数将从区块链上获取的具体信息在blockchain.vue通过VUE自定义的渲染模板渲染前端界面，如{{ blockInfo.data.header.number }}。使用bin目录下的cryptogen工具生成节点证书，文件夹crypto-config中存放生成的证书。系统使用nodejs版本的sdk(Software Development Kit，软件开发工具包)与服务端的联盟链进行交互，一方面使用fabric-client完成Peer、Order与事件流之间的交互，另一方面使用fabric-ca-client与CA进行交互。在enrollAdmin.js中注册管理员，使用fabric-ca-client的enroll方法登记一个管理员，有了管理员账户之后，可以通过用户名、组织证书注册信息生成privateKeyPEM和signedCertPEM，将当前的用户通过setUserContext方法设置成客户端的实例，并且注册普通用户之后将生成的公私钥放在key-store目录下，将相对路径传入fabric-client的newDefaultKeyValueStore方法的第二个参数KEYSTORE_PATH，之后通过setStateStore方法生成KeyValueStore对象之后赋值给store_path对象。该对象生成之后，再生成newCryptoSuite对象用来存储用户的密钥与证书。获得用户的证书之后，就可以持久化登录，通过getUserContext方法判断用户状态是否为持久化登录，控制台输出判断结果。登录之后，可以使用区块编号作为参数通过channel对象的queryBlock方法查询区块的具体信息。本系统给出了三种查询的方法，一是通过区块哈希查看具体信息，这里的实现依靠调用queryBlockByHash方法完成；二是通过前文所说的通过区块编号查询区块具体信息，通过queryBlock实现；三是查询通道区块的信息，通过调用queryInfo达成。完成上述准备工作之后，创建channel，采用newPeer方法与newOrderer方法，通过grpc协议连接服务器中联盟链打开的提供RPC服务的端口，即可通过channel提供的各种方法实现各种查询及交易发送等功能[11]。行程溯源实现界面如图9所示，左侧显示区块的数据哈希与前一块的数据哈希，右侧显示联盟链配置的节点域名的具体信息与应用场景。

图9 区块溯源界面

Fig.9 Block traceability interface

4 结论(Conclusion)

在科技飞速发展的今天，使用区块链技术可以为生物医学研究提供一个安全的、去中心化的数据存储和共享平台，促进传染病的研究与防治。使用行程码帮助传染病溯源工作精确定位患者，降低了病毒的传染速度与规模，但恶意伪造行程码的开源项目给溯源工作的开展造成了巨大的困难。本系统采用Hyperledger Fabric联盟链技术与ECDSA公钥签名算法结合传统的JavaWeb技术实现了权限管理、区块溯源、数字签名等功能，同时具有行程溯源和校验的功能，使用本系统可以有效预防行程码的伪造行为。

参考文献(References)

[1] 王志文.Vue+Elementui+Echarts在项目管理平台中的应用[J].山西科技,2020,35(6):45-47.

[2] 张长贵,张岩峰,李晓华,等.区块链新技术综述:图型区块链和分区型区块链[J].计算机科学,2020,47(10):282-289.

[3] 金川杰.面向区块链的高效数字签名算法研究[D].成都:电子科技大学,2021:10-20.

[4] 於志勇,林力强,陈艳,等.面向Hyperledger Fabric的SQL访问框架[J].计算机科学,2021,48(11):54-61.

[5] 康剑萍,王沈敏,杜竹青.PKI技术在信息安全中的应用[J].自动化仪表,2020,41(04):107-110.

[6] 陈泽宁,张亮,张双俊,等.基于区块链和去中心属性密码的访问控制身份方案[J].中国科学:信息科学,2021,51(08):1345-1359.

[7] 陈曼.基于蒙哥马利域的ECC算法的优化[J].网络安全技术与应用,2021,9:36-38

[8] 孟春岩.在超椭圆曲线上实现DSA数字签名[J].软件,2019,40(03):134-136.

[9] 朱小松.基于椭圆曲线密码体制的对称存储加密密钥保护方案[J].软件导刊,2017(03):153-156.

[10] 孟吴同,张大伟.Hyperledger Fabric共识机制优化方案[J].自动化学报,2021,47(8):1885-1898.

[11] MELO W S, SANTOS L, BENTO L, et al. Using blockchains to protect critical infrastructures: a comparison between Ethereum and Hyperledger Fabric[J]. International Journal of Security and Networks, 2022, 17(2):77-91.

作者简介：

蔡超萍(2002-)，女，本科生.研究领域：信息安全.

康晓凤(1978-)，女，硕士，副教授.研究领域：信息安全.

王 可(2001-)，男，本科生.研究领域：信息安全.

张百川(2002-)，男，本科生.研究领域：信息安全.

王 宇(2003-)，男，本科生.研究领域：信息安全.