文章编号：2096-1472(2020)-11-37-04
DOI:10.19644/j.cnki.issn2096-1472.2020.11.011

基于区块链的身份认证系统设计与实现

韦智勇[1]，周立广[2]

(1.南宁职业技术学院财经学院，广西 南宁 530008；
2.南宁市第二人民医院五象医院，广西 南宁 530219)
✉122570724@qq.com; 1960480023@qq.com

摘　要：随着区块链技术的高速发展，该技术已运用到各行各业中，而身份认证也成为全球科学界关注的热点。本文主要使用超级账本技术，对区块链的身份认证系统进行设计与实现，首先对系统进行需求分析，确定系统功能，包括用户模块、信息查询与修改、信息认证与授权、区块信息查询等，然后对系统进行深入的分析，对各功能模块进行详细的设计，最后通过功能测试，各功能模块达到预定的目标，而且系统运行稳定高效，对于用户而言系统操作简便、快捷，整个系统安全有效。

关键词：区块链技术；超级账本；身份认证
中图分类号：TP311.5　**文献标识码**：A

Design and Implementation of Identity Authentication System based on Blockchain

WEI Zhiyong[1], ZHOU Liguang[2]

(1.*School of Finance and Economics*, *Nanning College for Vocational Technology*, *Nanning* 530008, *China*;
2.*Wuxiang Hospital of Nanning Second Peoples Hospital*, *Nanning* 530219, *China*)
✉122570724@qq.com; 1960480023@qq.com

Abstract: With its rapid development, blockchain technology has been applied to all aspects of life. Identity authentication has also become a hot topic in the global scientific community. This paper proposes and implements an identity authentication system based on blockchain by using super account technology. Firstly, system requirements are analyzed to determine system functions, including user module, information query and modification, information authentication and authorization, block information query, etc. Then, the system is analyzed in depth, and each functional module is designed in detail. Finally, results of function test show that each function module achieves the design goal, and the system runs stably and efficiently. For users, the system is easy to operate and the whole system is safe and effective.

Keywords: blockchain technology; super book; identity authentication

1 引言(Introduction)

随着互联网技术的发展，网络技术已在应用于各个领域中，也走进了老百姓生活当中，基于互联网技术的研究犹如雨后春笋般的快速增长，同时在网上进行的各种业务与日俱增，例如：网上在线办理各种业务需要进行个人身份认证，认证方式一般可用企业提供的账号通过微信、身份证信息等方式进行身份认证，但是由于企业提供的账号本身具有虚假性，输入的信息也有可能存在被修改的风险，而开具实体证明又给工作带来诸多不便[1]。另外，信息造假是一个普遍的现象，好多求职的人对学历信息进行造假，开具一些假的工作简历证明文件，以达到鱼目混珠的目的，虽然一些用人单位通过调查的方式查询求职者身份的真实性，但由于查找方式较为烦琐而且成本较高，背景查询也无法做到万无一失。

伴随着区块链技术的问世，为解决这一难题指明了方向。为了解决身份认证问题，在系统设计时可建立区块链技术的网络架构，对于后台数据库的构建也采用这一方式进行，区块链技术的核心就是去中心化，数据存储可通过共识去信任化的方式进行。区块链是一种点对点的存储传输模式，具有分布式存储的特点，存储后的数据是通过区块链网络的节点进行统一管理，不会被某一节点进行修改[2]。

目前，区块链在社会运用已非常广泛了，例如比特币，其后台技术就是区块链，在全球的许多金融机构业务都包含有区块链技术的应用，此外在一些领域，例如通信、物流、防伪设计、期货交易、企业信息管理、政务信息发布、医疗救助等，这些都使区块链技术在各行业得到了快速的发展。

2 相关技术(Related technology)

2.1 区块

在基于区块链技术的数据存储中，数据存储是以区块作为主体而进行的，每个区块链结点的结构一般都包含区块头和区块体两部分，区块头主要存放该节点唯一的标志识别信息和服务版本信息，同时也包含了前一结点的哈希值，这样可通过哈希值，把所有的数据都通过链式存储的结构方式进行数据存储[3]。区块体主要用于数据的载体，数据单元主要存放各种信息及类别，不同的区块链应用都对应不同的数据类型，例如，金融交易类则存放交易信息、转账人、金额数量、交易时间等。每个结点的哈希值主要是通过Merkle树进行计算生成，对于每个结点，如果数据信息要更改，则所有的区块信息都要进行修改，否则无法进行数据更新操作，因此，区块链的这个结构可有效确保数据的安全性。

2.2 共识机制

共识机制是区块链的各个结点为了达到共同的目标而采取的同一口径，每个结点都必须遵循这一规定，这些规定中标明了各种事务是否合法有效，一般都以区块链的协议方式存在，共识机制主要是通过共识算法来实现，随着区块链技术的不断深入研究，各种共识算法层出不穷，例如，Pow算法、PBFT算法、POS算法和DPOS算法等，Pow算法主要是通过计算哈希值来确定该工作量；POS算法是基于代币的共识算法，新区块链的生成都由最高股权参与者进行维护，提高区块链的可靠性；DPOS算法是对POS算法的一种改进，维护者通过投票选举的方式进行产生，这样可节省的交易的时间，提高了效率；PBFT算法主要是先选出一个主节点，一般要在取得共识前进行，由于主结点与其他结点进行交互，达成共识后由主结点生成新的区块[4]。

2.3 智能合约

智能合约是用区块链的技术进行的一种数字化合约方式，一般通过程序代码写入区块链中，主要通过特定的运行机制来保障交易的进行，该合约的操作不受外界的干扰，智能合约的方式首先通过双方的合约内容进行协商，如果双方达成一致认可，系统将通过程序代码按照合约逻辑把合约内容发布在系统中。合约一旦确立，写入系统后，合约将自动生效，外界将无法进行修改[5]。因此，订立合约时双方必须要严谨，另外合约双方无须到场进行面签，只要双方在网上通过智能合约系统便可完成，这就保证了智能合约的安全性和高效性。

2.4 超级账本

超级账本是区块链技术的一个开发框架，框架的选取是区块链技术系统的基础和关键核心，关系系统开发的成败。例如在比特币交易中，交易过程需要虚拟代币，这种方式可以实现去中心化，但由于浪费资源、效率低下，所以不适合响应市场需求，而超级账本不需要代币，交易双方可以加入共识机制进行记账、验证交易信息即可，这种方式对本系统的开发更加切合实际[6]。

3 系统设计分析(System design analysis)

3.1 系统设计原则

由于区块链具有防止数据篡改、提高系统安全性及去中心化的特点，故本系统也是根据区块链技术的这些特性进行系统设计，同时就遵循以下原则：

(1)数据录入必须安全有效。必须保证数据录入系统过程中的安全性及有效性，如果数据录入错误，数据在系统中的转换将会出错，则会导致后面的各功能模块出现数据错误[7]。

(2)确保数据的安全性。对于所有交易信息，做到数据操作的可追溯性，同时利用区块链数据不可篡改的特点，确保后台数据库的数据安全，防止被篡改。

(3)合约的流程化。对于交易双方如果达成一致，则可以通过智能合约进行签订合同，在此，必须要保证整个交易流程的逻辑透明，防止外界各种因素的干扰[8]。

3.2 系统需求分析

本系统需求分析，主要根据数据录入和修改、系统授权、信息认证、系统管理和后台存储等功能模块进行探讨。对于数据信息的录入，用户首先必须通过系统注册才能登录到本系统，系统用户主要包括个人用户和机构用户，用户通过账号登录到系统，账号要严格管理；数据修改主要是对数据库的相关信息进行修改，这个操作必须通过“补丁”的形式进行数据更新，不能直接修改数据，操作记录都将保存在账本中；系统授权主要是用户登录系统时通过用户定制信息的认证授权，用于通过身份管理系统注册用户身份信息，即可直接授权登录使用；信息认证主要对用户的个人信息进行认证，如学历学位信息、职称、身份证信息、学习及工作履历等，对于比对进行用户的真实身份认证，如果信息是真实存在的，系统会自动给用户传递密钥和电子签名，通过信息授权的方式给用户使用该系统[9]；系统管理主要对用户的账号信息进行增加或删除，对区块链的数据进行永久的保存，对历史数据进行必要的维护；后台存储主要对把用户的数据、简历信息、履历信息、身份认证信息等，在进行数据校验后，以区块的形式保存到后台数据库中。

对于系统功能需求外，系统的性能需求也要求同步跟上，主要包括两个方面，一是系统的处理信息的效率，当用户操作该系统时，当该业务处理正常通过时系统才能授权给用户进行下一步的业务操作，这里如果系统的性能差或效率低，则会导致进程卡死在系统内部，严重影响各功能的正常使用。二是系统响应速度[10]。用户在操作该系统时，通过操作流程向系统发出指令，系统必须要规定的时间内响应该指令，如果响应时间太长，同时也会造成系统效率低而影响业务进行，由于本系统设计是基于联盟链技术开发的，响应的速度应更加快一些。

3.3 系统架构设计

本文所设计的系统主要采用分层的架构进行设计，主要有基层平台、合约层、业务管理层和用户层，共四层结构。系统架构图如图1所示。

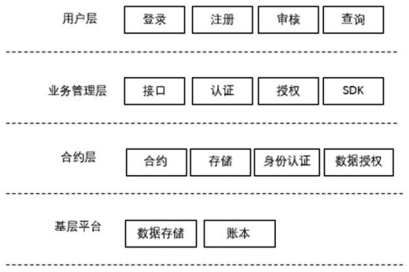

图1 系统架构图

Fig.1 System architecture

基层平台由用户端结点、CA结点、账本数据块组成的分布式区块链网络，对于CA节点而言，只有PKI权限的用户才能对该结点进行维护，另外还有基于账本数据存储的状态数

据库系统，该系统把账本的区块数据存储在该数据库中，同时包括各类用户数据信息、区块链内部代码等[11]。

合约层主要是用户双方进行的信息操作，根据链码来实现的，该层主要对双方信息进行认证比对，正确后才能进入下一层操作[12]。

业务管理层主要是为客户端提供后台服务的，主要功能是进行区块链的网络传输，由合约层请求后调入链码，完成交易双方的合约操作，同时也给用户层提供接口，处理来自用户支的指令。

用户层主要是提供用户的交互应用，通过网页界面与用户进行交互，该层基于WEB开发，主要运用网络编程语言进行编写程序代码，该层主要面对用户提供系统登录、授权审核等，并向下一层提供接口。

3.4 系统运行流程设计

本系统开发设计，主要采用Java++语言进行前端网页开发，对于智能合约方面，主要solidity语言，同时也包括了网络接口及网络构建等，具有运行流程如图2所示。

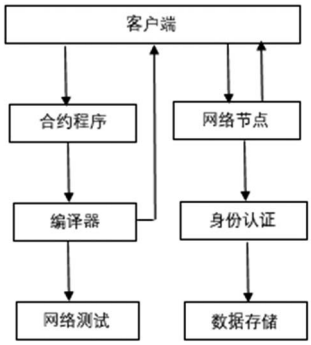

图2 系统运行流程图

Fig.2 System operation flow chart

在系统的运行流程图中，智能合约代码用solidity语言实现，合约文件的后缀名为.sol，通过合约接口程序将数据传输入智能合约编译器中，把合约内容转换为数字代码，然后将合约的数字代码传输到系统前端，将合约的内容部署到网络中，可通过这个结果进行系统测试，当完成身份认证后，将合约的内容保存到后台的数据库中[13]。

3.5 系统功能模块

基于区块链的身份认证系统功能模块主要分成用户模块、查询与修改模块、认证与授权管理、数据存储模块四大功能。

(1)用户模块。用户使用本系统一般都要通过自己的账号及密码输入后登录，作为新用户而言，必须要先注册自己的账号，把自己的个人身份及相关信息输入系统中，这样才可获得相应的系统账号，本系统的用户主要包括个人用户和单位用户，对于单位用户，除了个人用户的所有功能外，还可给个人用户进行信息认证，两种用户的使用系统的流程大体一致，但由于数据结构不相同，程序的接口也不一样。

(2)查询与修改模块。查询功能主要包括系统的数据及相关信息查询，一些公开的信息无须操作权限，可直接输入关键字进行查询，但有关数据信息必须要求有访问权限才能进行查询，获取权限通过请求后，由管理员分配权限，各用户的权限范围均可在系统首页中查询；修改功能主要是对原来的数据进行更新，该功能实现主要通过记账的方式进行，这时，为了确保数据安全，系统要验证其操作合法性，对修改的操作都保存在账本中，便于今后进行数据追溯，同样该功能也必须有相应的权限方可操作。

(3)认证与授权管理。认证功能主要是对用户身份信息、工作履历等个人信息，对于单位用户而言，首先要对本单位的员工信息也进行认证，认证通过后，也要提交到系统进行认证，这样可确保用户身份的真实性，有效地防止了信息造假行为发生；授权功能主要是用户提供一个身份认证的接口程序，用户可通过该接口进行数字签名，确保签名的用户与系统中的用户是同一用户，确保数据真实有效，系统授权主要通过密钥签发来实现。

(4)数据存储模块。主要是存储用户的个人数据及相关信息，个人用户信息一般包括证件信息、居住地址、学习经历、工作履历、联系方式、电子邮箱等，本系统的数据的存储在区块链的状态数据库中，而存储时的链码则通过超级账本进行保存，对数据进行存储操作时，都通过接口向账本发出请求即可，同时方便系统管理员对数据的维护。

4 系统的实现(Implementation of the system)

4.1 系统的运行环境

本系统的运行环境是使用Ubuntu 16.04.1 LTS操作系统，开发工具选择VS Code，同时Node.js版本使用8.16，电脑配置方面，处理器为双核，内存64G，网络方面，所有的终端都连接在区块链的配置网络中。

4.2 系统的功能实现

4.2.1 网络节点构建

区块链网络构建主要包括两个部分，一是区块链网络部署，另外一个是智能合约系统的部署。区块链网络的部署首先利用证书生成工具CP，生成MSP证书，进而可以生成创世区块，通过启用超级账本部署其他的网络节点，注册节点为区块链的网络管理节点，从而可实例化链码，可通过接口向外界提供[14]。

4.2.2 Node程序的实现

由于业务层需要提供网络页面服务，用Node的SDK与其他层进行数据传输，因此必须设计一些Node的应用程序，使系统的各模块提供必需的信息服务，由于身份认证系统使用express作为服务框架，先将URI请求的路由处理SDK与区块链网络底层平台交互，定义路由的方法，这样可达到了系统的功能服务。

4.2.3 合约设计

智能合约是实现双方交易的系统核心功能，交易双方身份数据的修改均由智能合约模块来完成，这样可能防止外界的各种干扰，确认交易信息的安全性，用户通过操作界面与区块链系统进行交互，交互的过程由系统后台的程序与区块链层对接与沟通，业务逻辑的实现要通过后台程序调用的方式提供链码，把运行的结果存储在超级账本内。

4.2.4 Web应用开发

Web开发主要是使操作者通过页面交互对系统进行操作与管理，本文为个人用户与系统管理员设计移动端的前置页面功能，实现Web开发主要通过交互式协议与接口开发。个人用户端主要通过账号登录，系统授权方式可通过系统生成的二维码进行操作后登录系统使用；单位用户则需要通过API接口进行认证后才能访问系统；对于系统管理员，主要是通过Vue.js单页应用认证后，其中页面还包括审批注册信息的功能。

4.3 系统测试

4.3.1 测试环境

本系统通过台式电脑中运行系统程序，进行各功能测试，运行环境是Windows 10操作平台，电脑硬件配置为I5四核处理器，8G内存，开发工具为VS Code，Node.js版本为10.15.0,使用谷歌浏览器。

4.3.2 功能测试

系统测试一般包括有白盒测试与黑盒测试，本文主要使用黑盒测试法，对系统的核心功能模块进行测试，检测是否能正常运行，核心功能主要包括用户模块、查询与修改模块、认证与授权管理等。

用户模块功能测试主要是通过用户在交互界面中输入合法与非法的用户信息，输入后进行提交，系统则对合法的用户信息有“提交成功”的提示，而对于非法的用户信息时则系统显示“提交失败”的提示；对于数据信息修改功能测试，主要是输入联系方式的信息，例如：电话号码等，分别输入合法的和非法的电话号码，合法的显示“修改成功”，而非法的显示“信息无法保存”，而对于重复使用的身份证号码，系统显示“该证件已注册，保存失败”；对于数据查询功能，测试方法为用已授权和没有授权的账号分别登录系统测试，已授权的可以正常显示所要查询各种数据信息，没有授权的显示“该功能没有授权，无法查询”；对于信息认证功能测试，主要在系统中输入用户的工作履历信息，则在系统谁后，系统会添加到用户的个人资料当中；授权功能测试，主要是测试系统对用户身份是否授权，用户输入个人信息后，系统会自动生成二维码，用户使用手机扫描二维码后，系统会要求用户进行电子签名，完成后系统会弹出“授权成功”的提示。

通过用户模块、查询与修改模块、认证与授权管理这几项功能进行系统测试，根据各项数据表明系统各项功能界面交互友好、系统运行稳定，运算数值正确，没有发现明显的错误，达到了预期的效果。

4.3.3 性能测试

系统在进行了功能测试后，同样也要对系统的整体性能进行测试，本文主要测试系统的响应时间。测试主要是在区块链的读写端口通过接口程序进行，本文测试工具采用Apache公司开发的Jmeter软件，对用户接口和查询接口分别进行测试，测试中采用多线程单次操作的方式进行。测试结果如图3所示。

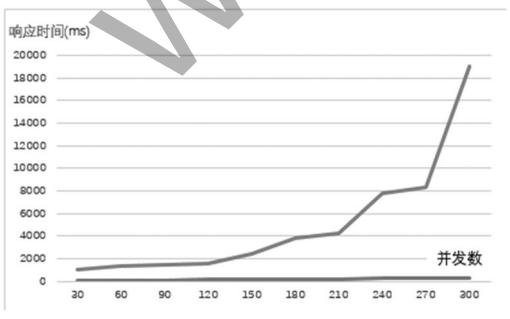

图3 系统响应时间与并发数关系图

Fig.3 Relationship between system response time and concurrency number

由如图3所示，随着进程的加大，系统的响应响应时间也会增加，但均在正常的范围之内，为此系统性能达到要求[15]。

5 结论(Conclusion)

由于区块链技术具有分布式存储、防止篡改、中心化的特点，基于区块链技术的一系列优点，本文将区块链技术和WEB开发技术结合一起设计实现了身份认证系统，通过把目前的身份认证系统存在的问题进行剖析，把超级账本技术作为本系统开发的框架，本系统通过融入区块链技术，无论从哪个方面，都解决了身份认证的难题，例如信息造假现象，该系统的设计取得了一定的成果，但由于目前区块链技术仍处于一个的发展阶段，技术尚不成熟，还有待改进，例如对不同环境的系统安全问题，必须有相应的安全策略，另外对于智能合约双方不能不能修改业务逻辑及数据信息，但是不能根据业务需要定制相应的功能等，这些问题在今后都要逐步加以完善。

参考文献(References)

[1] 周平,杜宇,李斌,等.中国区块链技术与应用发展白皮书[M].中国区块链技术和产业发展论坛,2018:42-44.

[2] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2019(4):481-494.

[3] Zhu XY, Badr Y. Identity Management Systems for the Internet of Things:A Survey Towards Blockchain Solutions[J]. Sensors, 2018,18(12)83-86.

[4] 张亮,刘百祥,张如意,等.区块链技术综述[J].计算机工程,2019,45(05):1-12.

[5] 欧阳丽炜,王帅,袁勇,等.智能合约:架构及进展[J].自动化学报,2019,45(03):445-457.

[6] 谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2019(9):192-195.

[7] 顾燕.基于区块链的身份认证系统的设计与实现[D].北京邮电大学,2018.

[8] 任安军.运用区块链改造我国票据市场的思考[J].南方金融,2018,24(03):39-42.

[9] 王皓,宋祥福,柯俊明,等.数字货币中的区块链及其隐私保护机制[J].信息网络安全,2017,17(7): 32-39.

[10] 潘维,黄晓芳.基于智能合约的身份管理及认证模型[J]. 计算机工程与设计,2020(04):915-919.

[11] Kubilay M, Kiraz M, Mantar H. CertLedger: A new PKI model with Certificate Transparency based on blockchain[J]. Computers & Security, 2019,85:333-334.

[12] Lee J. BIDaaS: Blockchain Based ID As a Service[C]. IEEE Access, 2018(6):2274-2278.

[13] Chen YL, Li H, Li KJ, et al. An improved P2P file system scheme based on IPFS and Blockchain[C]. IEEE International Conference on Big Data. IEEE, 2017:2652-2657.

[14] 郭良俊.HUE-Cloud身份认证系统的设计与实现[D].江苏:东南大学,2018.

[15] Tse D, Zhang Bowen, Yang Yuchen, et al. Blockchain application in food supply information security[C]. IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).IEEEE,2018:1357-1361.

作者简介：

韦智勇(1983-)，男，硕士，信息系统项目管理师.研究领域：区块链应用，大数据技术.

周立广(1974-)，男，硕士，高级工程师.研究领域：云计算，大数据分析.