文章编号：2096-1472(2023)-04-38-04
DOI:10.19644/j.cnki.issn2096-1472.2023.004.009

一种基于量子密钥的区块链身份认证方法

万 华，周 虎，朱德新，孙 羽

(长春大学电子信息工程学院，吉林 长春 130022)
✉3303077196@qq.com; 291253464@qq.com; 38925023@qq.com; 353130273@qq.com

摘 要：针对当前区块链系统存在的用户身份非法访问、身份伪造等影响区块链系统安全的问题，基于量子密钥安全性和可靠性高的特性，提出并设计了一种利用量子密码技术实现区块链系统身份认证的方案，方案中用户每次登录区块链系统时可通过比对客户端量子密钥散列值和量子密钥云服务器散列值的一致性完成身份认证，从而确保了区块链系统每次交易用户身份的合法性和安全性。实验结果表明，利用量子密码技术能够实现区块链系统用户身份安全认证，为区块链身份安全认证提供了一种新的思路。

关键词：区块链；量子密钥；身份认证
中图分类号：TP311 **文献标识码**：A

A Blockchain Authentication Method based on Quantum Key

WAN Hua, ZHOU Hu, ZHU Dexin, SUN Yu

(*School of Electronic and Information Engineering*, *Changchun University*, *Changchun* 130022, *China*)
✉3303077196@qq.com; 291253464@qq.com; 38925023@qq.com; 353130273@qq.com

Abstract: Illegal user identity access and identity counterfeiting affect the security of the current blockchain system. Based on the high security and reliability of the quantum key, this paper proposes to design a solution to realize the authentication of the blockchain system by using quantum cryptography technology. In the solution, users can complete authentication by comparing the consistency between the hash value of client quantum key and the hash value of quantum key cloud server each time they log in to the blockchain system, thus ensuring the legitimacy and security of user identity in each transaction of the blockchain system. The experimental results show that quantum cryptography technology can realize the user authentication of the blockchain system, which provides a new idea for blockchain security authentication.

Keywords: blockchain; quantum key; authentication

1 引言(Introduction)

互联网的发展使信息化的服务逐渐渗透到人们生活的方方面面，传统活动逐渐被网络活动所代替，在此过程中，一大批新的技术涌现，区块链技术便是其中之一。伴随着比特币[1]而兴起的区块链技术是一种广泛应用于数字加密货币、医疗溯源、公证防伪、金融的基础架构和计算范式，有望实现信息互联网向价值互联网的转变[2−5]。然而，互联网复杂、开放的特性，使得区块链系统经常存在恶意节点介入[6]、用户非法访问[7]等安全隐患，极大地阻碍了区块链技术的发展。由于区块链中账本数据采用公开交易记录、多节点共识确认的方式进行存储和验证，因此区块链系统用户身份的合法性至关重要。针对目前区块链系统存在的身份伪造、用户非法访问等问题，引入身份认证机制，是保障区块链安全的一种重要解决方案[8−9]，特别是近年来量子密码学[10−11]的发展给区块链身份认证提供了一种新的简单、安全、易行的途径。因此，本文设计了一种基于量子密码学的技术，即利用量子密钥作

为唯一身份标识，通过比对设备间量子密钥散列值的方式，实现用户区块链系统身份安全认证的方法。

2 相关知识介绍(Introduction to related technologies)

区块链技术：区块链技术是以比特币为代表的数字加密货币体系的核心支撑技术。区块链技术的核心优势是去中心化、不可篡改、不可伪造、共识确认等，通过运用时间戳、数据加密、分布式共识和经济激励等手段，实现在无信任的分布式系统中去中心化的点对点交易、协调和协作，为中心化机构普遍存在的高成本、低效率等问题提供了解决方案。

量子密钥分配技术：量子密钥是量子力学理论的集大成者，它的来源核心依赖于量子密钥分发系统，量子密钥分发系统可以在空间分离的用户之间以信息理论安全的方式制备和共享具备真随机性的量子密钥。量子密钥分配技术历经多年发展，已形成量子密钥分配终端、量子密码云服务网络等成熟的产业化设备，能为用户提供安全量子密码，成为信息安全的重要基础设施。

RSA非对称加密算法：RSA是一种非对称加密算法，密钥分为公钥(Public Key，PK)和私钥(Secret Key，SK)两个部分，公钥可以向外公开，任何人都可以获取，私钥必须私密保存。公钥和私钥之间具有严格的数学关联，因此是成对出现的。其中，用于生成公钥和私钥的算法是公开的。

3 系统总体设计(Overall system design)

为了利用量子密钥实现区块链系统的身份安全认证，本系统模型分为量子密钥云服务器模块、用户模块、客户端模块、移动端模块、密钥分配中心模块和区块链系统模块共六大模块。基于量子密钥的区块链身份认证系统模型图如图1所示。

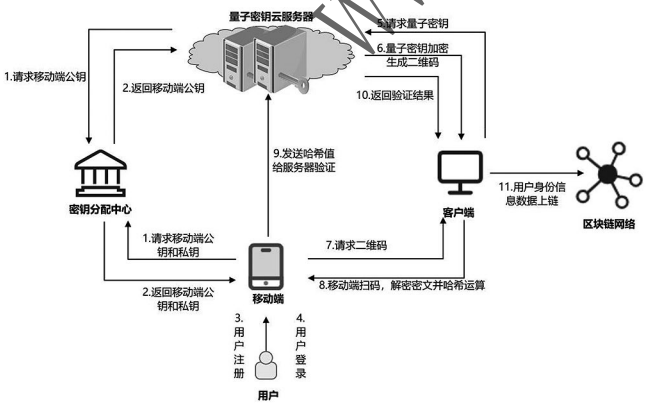


图1 区块链身份认证方案模型

Fig.1 Blockchain authentication solution model

区块链身份认证系统各个部分模块详细介绍如下。

(1)量子密钥云服务器：本模块主要负责为区块链用户身份认证提供量子密钥服务，它按照顺序依次生成一连串固定长度的量子密钥序列，并按顺序两两一组依次对量子密钥进行异或加密运算，并将运算结果发送至客户端，同时负责对移动端发送过来的哈希散列结果进行比对。

(2)密钥分配中心：本模块主要负责为在认证过程中需要事先在量子密钥云服务器和移动端共享的初始量子密钥序列加密。密钥分配中心会利用RSA非对称加密算法为移动端生成用于加密量子密钥的公钥和私钥，量子密钥云服务器首先会向密钥分配中心发送移动端公钥的请求，密钥分配中心响应请求并发送移动端加密公钥给量子密钥云服务器，其中本方案默认密钥分配中心是完全可信的。

(3)移动端：本模块主要负责用户信息注册和登录，成功注册的用户会获得登录移动端的权限，登录成功后开启二维码扫描功能，扫描客户端界面展现的二维码，利用量子密钥解密异或加密运算的结果获得量子密钥明文，并将量子密钥明文进行哈希散列运算发送给量子密钥云服务器。

(4)客户端：本模块主要负责向量子密钥云服务器申请二维码，并将二维码呈现到客户端界面。

(5)区块链网络：在量子密钥云服务器比对散列值成功后，主要负责将区块链身份验证成功的用户信息以键值对的方式写入区块链账本中。

(6)用户：区块链系统认证的实体组成部分。

区块链身份认证系统时序图如图2所示。

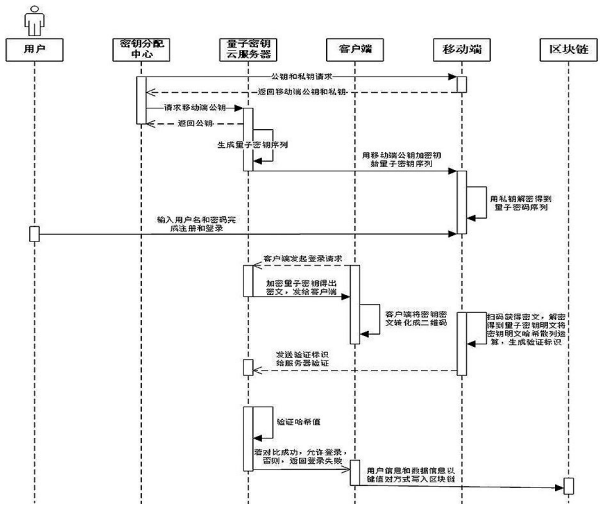


图2 区块链身份认证系统时序图

Fig.2 Timeline diagram of the blockchain authentication system

4 认证算法详细设计(Detailed design of authentication algorithms)

用户进行区块链系统的身份认证之前，需要在应用程序后台提交注册信息，获取登录平台的账号和密码等凭证，用户成功登录后，开始进行基于量子密钥区块链身份认证。区块链系统用户身份认证流程如下：①公钥和私钥请求。②量

子密钥云服务器初始化、初始量子密钥序列生成、加解密初始量子密钥序列。③用户身份信息注册、登录。④量子密钥异或加密、生成二维码。⑤应用程序扫码、解密和进行散列运算。⑥散列值比对、验证、用户信息数据上链。具体的量子密钥认证方案流程如图3所示。

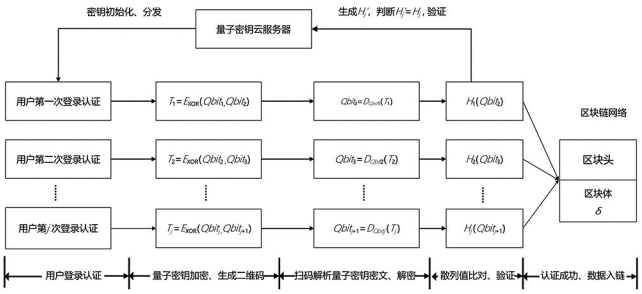


图3 量子密钥身份认证方案

Fig.3 Quantum key authentication solution

(1)每次用户登录时，密钥分配中心为来自应用程序移动端和量子密钥云服务器的请求响应一对用于加密和解密的密钥对。①量子密钥云服务器发起移动端公钥请求。②移动端发起公私钥请求。③密钥分配中心响应请求，根据RSA非对称加密算法初始化一对公私钥(PK_i,SK_i)，其中$1\leqslant i\leqslant r$，r为登录的次数；将公钥PK_i发送给量子密钥云服务器保存，(PK_i,SK_i)发给移动端保存。

(2)量子密钥云服务器系统初始化并生成一连串的量子比特$Qbit$并设置每256比特分割为一个量子密钥序列。分割后的量子密钥序列依次为$Qbit_1,Qbit_2,Qbit_3,\cdots$，其中$Qbit_1$为此次认证的初始量子密钥序列，$1\leqslant j\leqslant r+1$，$r$为登录的次数。

(3)量子密钥云服务器和移动端加解密初始量子密钥。①量子密钥服务器验证PK_i的签名，判断是否合法。②验证通过后，对量子密钥序列$Qbit_j$明文使用RSA公钥加密$C_j=E_{RSA}(Qbit_j)$，将密文C_j发送给移动端。③移动端解密密文，$Qbit_j=D_{RSA}(C_j)$，并将明文$Qbit_j$保存下来。

(4)用户在移动端输入身份信息$attr$向后台数据库提交注册申请。

(5)注册完成后，用户使用注册时提交的身份信息$attr$登录移动端，后台比对验证成功后完成登录。

(6)点击客户端登录界面，发起客户端登录请求。

(7)服务器响应客户端登录请求，对已经分割好的量子密钥序列$Qbit_1,Qbit_2,Qbit_3,\cdots$，依次进行异或加密生成密文$T_j=E_{XOR}\left(Qbit_j,Qbit_{j+1}\right)$，并根据密文$T_j$生成二维码。

(8)移动端扫描二维码并解析二维码信息。①移动端扫描二维码并解析二维码信息得到密文T_j，其中j是扫码的次数。②根据预先保存好的初始密钥$Qbit_j$对密文解密，$Qbit_{j+1}=D(T_j)$，得到明文$Qbit_{j+1}$。③对明文$Qbit_{j+1}$进行散列运算，$H_j(Qbit_{j+1})$，得到散列值H_j，发送至量子密钥云服务器。④删除之前保存的初始量子密钥序列$Qbit_j$，用$Qbit_{j+1}$代替$Qbit_j$作为新的初始量子密钥序列。⑤移动端保存$Qbit_{j+1}$，等待下一次的登录认证使用。

(9)量子密钥云服务器将自身的$Qbit_{j+1}$进行散列运算得到$H_j'(Qbit_{j+1})$，比对H_j和H_j'，若比对成功，表明身份验证成功。

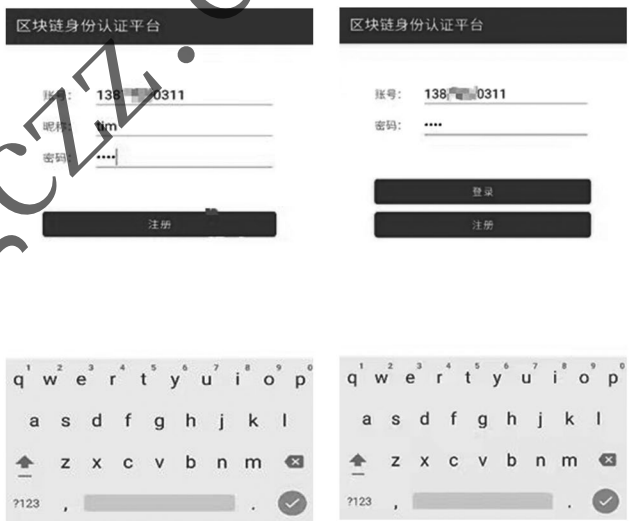
(10)用户成功完成区块链身份认证后，将比对成功的散列值和用户身份信息M以键值对的方式写入区块链区块中，其中区块信息$\delta=\{Key:H_j,Value:M\}$。

5 系统实现(System implementation)

5.1 移动端模块

5.1.1 用户注册、登录

用户注册后可利用用户名和密码登录移动端，只有合法的用户才能登录移动端完成后续区块链系统登录，用户注册和登录界面如图4(a)和图4(b)所示。



(a)用户注册 (b)用户登录

图4 用户身份注册和登录

Fig.4 User registration and login

5.1.2 移动端解密、散列运算

量子密钥云服务器利用移动端公钥将量子密钥序列加密后，移动端接收密文结果，用自身提前保存好的私钥解密得到量子密钥明文并将它作为解密密钥预存在移动端中，然后移动端开启二维码扫描，将嵌在二维码中的密文信息解密获得明文，并将取得的明文进行哈希散列运算。

5.2 密钥分配中心模块

当用户注册并成功登录后，密钥分配中心主要负责为移动端模块和量子密钥云服务器模块分配移动端设备的公钥和私钥，其中公钥用于加密量子密钥序列，私钥用于解密量子密钥序列。本系统使用的移动端公私钥如图5所示。

```
-----BEGIN RSA Private Key-----
MIICXQIBAAKBgQDlf1XKBxd8efsR2c1vHzCQvSV5kQMyChHx4+76SSezexVzQTr0
+2dpT0DOobvgSIbmndf5Y/xD26a2x5ZbaNZ4iORTnnA4+aBMvIclwwE4UvTuZAqO
WBlE1ZTCBZRTIPpyEFsPMLRsDYTNU5/M524PERw0NojFW2Yl/gJjutoaRQIDAQAB
AoGBANZgax/sHflN7MURAoDRzsj1luMHHcgJdhfRxnOQEIDs8e2Wul8L1N6fhLdA
h0KMHU+hlJTG3Gf677F/oSlENkne//YJzqVFL3fXdfIZelFCHbAFbpf+kED2NtnJ
0AxcgUGMHarM4O3JDsMRmLBDaPSfU25+AlVymKGjMLsj0KJFAkEA+L+N9ZhsACKI
n2gvATf9t/nGpIJMusSSgd0/3m05xrt/3FnicxZj2LfDiaZhgxyWMtqXk2xS7PTX
qEXuCvnlRwJBAOwwG8qJTBHnuexYrW/z1D928Q4bsGMqmwIC3wNrtBLLbRsuWrMW
wmarcR4S2m2oxgYR8xNNiuLnIPsYmi7EOhMCQA1kAnheJDI9qa0rJpyiLv5ga9kf
SpIjUt+60V1f8+RG47MxA4e+hNF90wDt/AHa4BsMuWwuQKiQ5ashWJcurLECQQCX
tKL1KdEZoxzx6VellBkdlplo9XILkD82QH/cY56rf8yZ6+FILPM7HR2wMm3oh8KB
/Z+DI4h1C/5MKlZGebXPAkBjdBB8HmubuYXSqqnlV3Ic1zIdnkammGke2JC8bUdX
+6uDfmf9xUJ7zQYwvdtT15jGJbBiNHxbAKhJkt//QX3n
-----END RSA Private Key-----

-----BEGIN RSA Public Key-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlf1XKBxd8efsR2c1vHzCQvSV5
kQMyChHx4+76SSezexVzQTr0+2dpT0DOobvgSIbmndf5Y/xD26a2x5ZbaNZ4iORT
nnA4+aBMvIclwwE4UvTuZAqOWBlE1ZTCBZRTIPpyEFsPMLRsDYTNU5/M524PERw0
NojFW2Yl/gJjutoaRQIDAQAB
-----END RSA Public Key-----
```


图5 移动端公私钥

Fig.5 Mobile public key and private key

5.3 量子密钥云服务器模块

移动端对量子密钥序列密文T_j解密后得到量子密钥明文，并将明文进行散列运算得到散列值发送给量子密钥云服务器，量子密钥云服务器将自身存储的量子密钥散列后与接收到的散列值进行比对，如果两者的散列值相等，则表示认证成功，用户允许进入区块链系统；否则，拒绝进入区块链系统。表1表示的是一些用户认证成功的信息。

表1 用户认证情况统计表

Tab.1 Statistics table of user authentication

用户名	散列值	状态
12345678995	4315061d50098d78a6d77c43dd82b940f6469fcf6f9a82866deeb1b68d6f62a4	验证成功
13879240311	af2aef7071ca92fd7c9b80f9eb2263ffacf7d6dae5d0612e1ba4bbc04e04f647	验证成功
12356987412	937ed244c1cc696205c938138dad7e6ef4c0437ca777802ff9f0aa301dab0b50	验证成功
15978964523	f7b4376217ab252b6f5add22ab842ae4ba303f7cc79a4f805defe2163ae627be	验证成功

5.4 区块链平台模块

区块链平台模块主要负责将成功加入区块链的用户身份信息以键值对的方式打包成交易写入区块中，其中键*Key*为账户的散列值，具有唯一性。*Value*为用户账户名、昵称和密码。打包并成功写入区块链中的键值对用户数据信息具有唯一标识用户的作用。区块链用户身份信息写入成功界面如图6所示。


```
tinmy@tinmy-virtual-machine:~/go/src/github.com/hyperledger/fabric-2.2.0/fabric-samples/test-network$
 peer chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --caf
ile ${PWD}/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts
/tlsca.example.com-cert.pem -C mychannel -n basic --peerAddresses localhost:7051 --tlsRootCertFiles $
{PWD}/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt --peer
Addresses localhost:9051 --tlsRootCertFiles ${PWD}/organizations/peerOrganizations/org2.example.com/p
eers/peer0.org2.example.com/tls/ca.crt -c '{"function":"adduser","Args":["22ad02bcf792c2be2bd7fb88ebd
65b97fb47635aafe5378b18499fbd276b90cf","13879240311","password","tinmy123","eventadd"]}'
2022-12-09 23:13:37.223 CST [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke succes
sful. result: status:200 payload:"The user was added successfully!"
```


图6 区块链用户身份信息

Fig.6 Identity information of blockchain users

6 结论(Conclusion)

本文针对当前区块链系统中存在的用户身份非法访问、身份伪造等问题设计了一种利用量子密钥作为唯一认证标识实现区块链系统用户身份安全认证的方法，并实现了用户身份信息安全上链可查询验证。实验结果表明，依托量子密码技术，利用量子密钥这一载体，可以实现区块链系统用户身份安全认证。同时，对于已经上链的用户信息可以起到很好的隐私保护。

参考文献(References)

[1] 蔡晓晴,邓尧,张亮,等.区块链原理及其核心技术[J].计算机学报, 2021,44(1):84−131.

[2] DUTTA P, CHOI T M, SOMANI S, et al. Blockchain technology in supply chain operations: Applications, challenges and research opportunities[J]. Transportation research part e: Logistics and transportation review, 2020, 142:102067.

[3] 诗钦,霍如,黄韬.区块链技术研究综述：原理、进展与应用[J].通信学报,2020,41(01):134−151.

[4] 刘敖迪,杜学绘,王娜.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018,29(07):2092−2115.

[5] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481−494.

[6] 田国华,胡云瀚,陈晓峰.区块链系统攻击与防御技术研究进展[J].软件学报,2021,32(05):1495−1525.

[7] 王俊生,李丽丽,颜拥,等.区块链技术应用的安全与监管问题[J].计算机科学,2018,45(S1):352−355,382.

[8] GAO S, SU Q, ZHANG R, et al. A privacy−preserving identity authentication scheme based on the blockchain[J]. Security and Communication Networks, 2021, 2021:1−10.

[9] 姚前,张大伟.区块链系统中身份管理技术研究综述[J].软件学报,2021,32(07):2260−2286.

[10] LIANG M, YANG L. Public−key encryption and authentication of quantum information[J]. Science China Physics, Mechanics and Astronomy, 2012, 55(9):1618−1629.

[11] 王永利.量子计算与量子密码的原理及研究进展综述[J].计算机研究与发展,2020,57(10):2015−2026.

作者简介：

万　华(1995−)，男，硕士生.研究领域：区块链身份认证，量子通信.

周　虎(1998−)，男，硕士生.研究领域：区块链身份认证，机器学习.

朱德新(1982−)，男，硕士，讲师.研究领域：区块链，量子密码技术.

孙　羽(1996−)，男，硕士生.研究领域：可搜索加密.