一种基于区块链技术的多阶段级联无线安全认证方案

胡兆鹏 丁卫平 高 瞻 朱晓辉 王杰华
(南通大学计算机科学与技术学院 江苏 南通 226019)

摘 要 区块链技术具有去中心化、去信任、匿名、数据不可篡改等优势。为了更有效地保证用户能够安全识别并连接无线网络,文中提出了一种基于区块链技术的多阶段级联无线安全认证方案(MWSASB)。MWSASB方案设计多阶段级联协议过程,即注册阶段、登录与认证阶段以及交易阶段,并利用工作量证明机制PoW算法和延长最长链的方法,将用户信息产生交易记录在不可篡改且去中心化的区块链账本中。首先,在注册阶段,用户输入注册信息,在去中心化网络中利用密码学技术以及共识机制使得注册信息存储在区块链的每一个节点上;同时,在登录与认证阶段,用户输入登录信息,用户与区块链服务器进行登录与认证,在认证成功后以同样的方式将登录信息存储在区块链的每一个节点上。其次,在交易阶段,利用共识机制确保注册信息和登录与认证信息以交易形式安全记录在区块链中。最后,对MWSASB方案进行安全性和运算量分析。实验结果表明,在安全性方面,MWSASB方案具有无线安全认证等安全属性,有效避免了各种常见的网络攻击,如中间人攻击、DDoS攻击等;在运算量方面,利用区块链不可篡改机制,使用密码学算法和共识机制进行加密认证,能有效减少运算次数,提升安全认证效率。

关键词 区块链,去中心化,无线安全认证,多阶段级联,共识机制
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/jsjkx.181102170

Multi-stage Cascade Wireless Security Authentication Scheme Based on Blockchain Technology

HU Zhao-peng DING Wei-ping GAO Zhan ZHU Xiao-hui WANG Jie-hua
(College of Computer Science and Technology, Nantong University, Nantong, Jiangsu 226019, China)

Abstract Blockchain technology has the advantages of decentralization, trust removal, anonymity and non-tamperable. In order to more effectively ensure that users can safely identify and connect to the wireless network, this paper proposed a multi-stage cascade wireless security authentication scheme (MWSASB) based on blockchain technology. The MWSASB program designs a multi-stage cascade protocol process: registration phase, login and certification phase, and transaction phase. And it records the transaction of users' information in the non-tamper and decentralized blockchain ledger by using workload proof and the extension of the longest chain. Firstly, during the registration phase, the user enters the registration information Then the cryptographic technology and the consensus mechanism are used to store the registration information on each node of the blockchain in the decentralized network. At the same time, during the login and authentication phase, the user inputs the login information, then login and authenticate with the blockchain server. After successful authentication the login information is also stored on each node of the blockchain. Secondly, in the transaction phase, the registration information and the login and authentication information are used to ensure that their information are securely recorded in the blockchain in the form of transactions. Finally, the security and computation of the MWSASB are analyzed. The results show that the MWSASB has security attributes such as wireless security authentication and can effectively avoid various common network attacks such as man-in-the-middle attacks, DDoS attacks, etc. In terms of computation, blockchain cannot be tampered with and cryptographic algorithm and consensus mechanism can be used for encryption verification, which can effectively reduce the number of calculations and improve the efficiency of security authentication.

Keywords Blockchain, Decentralization, Wireless security authentication, Multi-stage cascade, Consensus mechanism

---

到稿日期:2018-11-25 **返修日期**:2019-04-08 **本文受江苏省六大人才高峰项目**(XYDXXJS-048),**南通市应用基础研究计划项目**(GY12016015)**资助**。

胡兆鹏(1994—),**男**,**硕士**,**主要研究方向为信息安全、区块链技术**;**丁卫平**(1979—),**男**,**博士**,**副教授**,**主要研究方向为数据挖掘、机器学习和粒运算**;**高 瞻**(1972—),**男**,**博士**,**副教授**,**主要研究方向为虚拟现实、人机交互和计算机图形学**;**朱晓辉**(1976—),**男**,**硕士**,**副教授**,**主要研究方向为计算机软件与理论**;**王杰华**(1965—),**男**,**教授**,**硕士生导师**,**主要研究方向为信息安全、物联网技术、医学信息处理**,E-mail:wang.jh@ntu.edu.cn(**通信作者**)。

1　引言

随着信息安全技术和无线网络设备的飞速发展，用户可以随意地通过无线网络设备进入网络[1]。但随着无线网络的逐渐开放化，网络环境充满了不确定性，各种网络攻击与伪装手段等不安全因素也随之而来。网络安全问题越来越受到人们的重视[2]，确保网络通信和数据安全的第一道防线就是在诸多无线网络设备中准确识别出用户身份。身份认证就是网络系统中信息安全的基础[3]。

1981 年，Lamport[4]最先提出了一种口令身份认证方案，该方案解决了在不安全信道中通信的安全问题。然而该方案存在一些缺点：(1)不能抵御重放攻击；(2)Hash 的计算量较大。此后，许多研究者为了提高认证协议的安全性，减少认证协议的运算量，提出了大量的认证协议。这些传统的无线安全认证协议主要分为 3 类。(1)基于口令的无线安全认证技术[5]。(2)基于口令和智能卡的无线安全认证技术[6]。Xiong 等[7]于 2014 年提出了一种改进的基于智能卡的远程用户密码认证方案，用于克服之前的安全缺点；Jaewook 等[8]于 2016 年提出了一种基于智能卡的高效且安全的密码认证方案，利用密码学技术使智能卡更具安全性。(3)基于口令、智能卡和生物特征的无线安全认证技术[9-10]。2018 年，Yin[11]在生物模糊提取技术的基础上，提出了一种椭圆密码曲线的身份认证方案，该方案使用椭圆曲线算法完成了双方密钥认证的验证，有效避免了中间人攻击等网络常见攻击，但无法避免口令猜测攻击。综合以上研究成果，基于这 3 种模式的无线安全认证方案都存在亟需解决的安全隐患。

区块链技术最早出现在中本聪发表的“Bitcoin：a peer-to-peer electronic cash system”一文中[12]，该文详细介绍了区块链具有去中心化、点对点传输、共识机制以及密码学技术等特点。现今，区块链有望彻底重塑人类社会活动形态，被应用到物联网、人工智能以及身份认证等领域。2016 年，文献[13]指出区块链技术的发展对身份认证的发展和应用有着极大的促进作用。2018 年，Liu 等[14]从区块链的信息安全领域出发，综述了区块链应用于身份认证技术的研究进展，提出了基于区块链身份认证的 3 种模式。(1)基于区块链的传统方式认证技术。2018 年，Zhou 等[15]提出了基于区块链技术的生物特征和口令双因子认证方案，用 Hash 算法和椭圆曲线算法对生物特征利进行认证，减少了公钥算法签名与验证的次数，提高了认证效率。(2)基于区块链分布式的 PKI 认证技术。2014 年，Fromknecht 等[16-17]提出了基于区块链的分布式 PKI 认证系统，将用户身份与证书相关联来解决传统 PKI 系统面对的去中心化问题。(3)基于区块链技术的金融功能实现认证技术。2017 年，Raju 等[18]提出使用以太坊的匿名账户钱包，通过公钥地址来实现网络用户的身份管理。区块链技术虽然还处于初级阶段，但其独有的特点使得与身份认证的结合必将成为未来的主要认证形式，发展前景很大，具有很高的研究价值。但相关研究还存在不足之处，如文献[15]对生物特征及口令的加解密操作需要大量使用密码学技术，存在效率低下、时效性差等缺陷；而且，当前成果大多基于理论研究，在真实环境中的实现尚不可知。

针对传统无线安全身份认证技术的 3 种形式，本文使用区块链技术解决传统无线身份认证的安全问题；针对目前基于区块链技术身份认证的 3 种形式，本文使用多阶段级联、工作量证明和延长最长链相结合的方式，更加简单、方便地解决区块链中身份认证的效率问题。结合以上两个问题，本文提出一种基于区块链技术的多阶段级联无线安全认证方案(MWSASB)。首先，通过使用区块链密码学技术对用户认证信息进行加密和解密；然后，利用共识机制确保用户信息以交易形式安全记录在区块链中；最后，对 MWSASB 方案进行了安全性和运算量分析。区块链具有去中心化、点对点传输、共识机制以及密码学技术等优点，解决了当前中心化架构所存在的安全性和效率低的问题。同时，本文将用户信息以交易的形式存储在区块链分布式账本中，数据一旦被存储到区块链中，将不会被篡改或丢失，从而能够有效地进行身份认证。

2　区块链技术

区块链本质上是一个分布式共享账本，由所有当前参与的节点来共同维护交易及数据库。它使交易基于密码学原理而不是基于信任，使得任何达成一致的双方都能够直接进行交易，不需要第三方的参与。简单来说，区块链技术主要包含 3 个概念[12]。

(1)区块链交易：在区块链的网络中，对其进行任何操作(注册、登录与认证)，都会生成交易并附上交易号 Tx-id，利用共识机制将其记录在区块中。

(2)区块：记录一些或所有的最新交易，且未被其他先前的区块记录。

(3)区块链：区块会被加入到记录的最后，并且与前一个区块相连，一旦写上就不能被改变或删除。之后不断地有新的区块与前一个区块相连，从而形成一条记录数据的链。

2.1　区块链交易

区块链交易实际上就是区块链账本中对应的一条条数据。本文中的 MWSASB 方案对用户进行安全身份认证，通过密码学技术得到用户地址 U_{addr}，因此本文的区块链交易包括用户地址 U_{addr} 及其他相关信息。区块链交易数据的结构如图 1 所示。

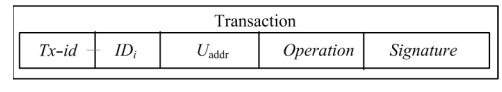

图 1　交易数据结构

Fig. 1　Transaction data structure

图 1 中，$Tx\text{-}id$ 表示该交易的交易号；ID_i 表示用户名，用于标识该用户；U_{addr} 表示用户地址，也叫哈希公钥，在登录与认证阶段，是唯一标识用户信息的凭证；$Operation$ 表示对用户信息的操作，包括注册操作(R)和登录与认证操作(L)；$Signature$ 表示通过私钥对用户信息进行加密签名，用户通过用户地址(哈希公钥)进行解密签名。

2.2　区块和区块链

2.2.1　区块

在区块链技术中心，区块中包含有一定时间内产生的无法被篡改的数据记录信息。数据以区块的形式永久保存[12]。

区块分为区块头和区块体：区块头内主要有版本号、前一个区块哈希值(Prev-Hash)、Merkle tree、时间戳、难度值和参与共识机制的有关数据(Nonce 等)；区块体主要有交易数量、交易(Tx 表示)。

2.2.2 区块链

经过节点验证的区块，将按照时间顺序加入原有区块链中，而区块之间是通过 Hash 值连接的，原有区块链的唯一标识就是这个 Hash 值。新区块通过区块头部中记录的 Prev-Hash 值就能找到原有区块链所连接的区块，周而复始，不断有新区块通过这样的方式找到前一个区块，从而形成一条链式结构，这条链被称为区块链[12]。

3 基于区块链技术的多阶段级联无线安全认证方案

区块链技术的出现，使得传统中心化方式的安全问题得到有效解决。本节提出了一种基于区块链技术的多阶段级联无线安全认证方案(MWSASB)。如图 2 所示，MWSASB 方案分为 3 个阶段：注册阶段、登录与认证阶段以及交易阶段。在注册阶段，用户输入注册信息，在去中心化网络中，利用密码学技术以及共识机制使得注册信息存储在区块链的每一个节点上。在登录与认证阶段，用户输入登录信息，并与区块链服务器进行登录与认证，在认证成功后，将登录信息同样存储在区块链的每一个节点上。在交易阶段，将注册信息和登录与认证信息以交易的方式存储在区块链中。

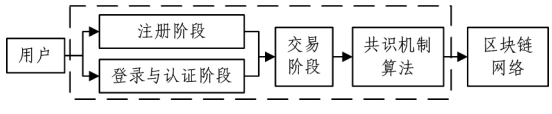

图 2 MWSASB 方案协议的总流程图

Fig. 2 General flow chart of MWSASB protocol

3.1 MWSASB 方案的相关符号定义

为了详细介绍本文方案，表 1 列出了本文所使用的符号参数及其含义。

表 1 方案符号及其含义

Table 1 Description of scheme symbol

符号	含义
U_i	用户 i
S	区块链服务器
N_i	区块链节点 i
ID_i	第 i 个用户的注册/登录与认证时使用的用户名
PW_i	第 i 个用户的注册/登录与认证时使用的口令
n	随机数
$Gen(\ )$	随机私钥生成函数
$E(\ )$	椭圆曲线算法
K_s	私钥(由用户保存)
K_p	公钥
$H(\ )$	哈希函数
U_{addr}/H_{pk}	用户地址(公钥哈希)，用户登录认证的唯一标识
x	哈希运算后的摘要信息
$Sign(\ )$	数字签名函数
y	签名信息
$\|\|$	数据连接运算
R	注册操作
L	登录与认证操作
$A\rightarrow B:m$	A 向 B 在公共信道中发送消息 m
$A\Rightarrow B:m$	A 向 B 在安全信道中发送消息 m

3.2 注册阶段

用户在注册阶段的流程如图 3 所示。

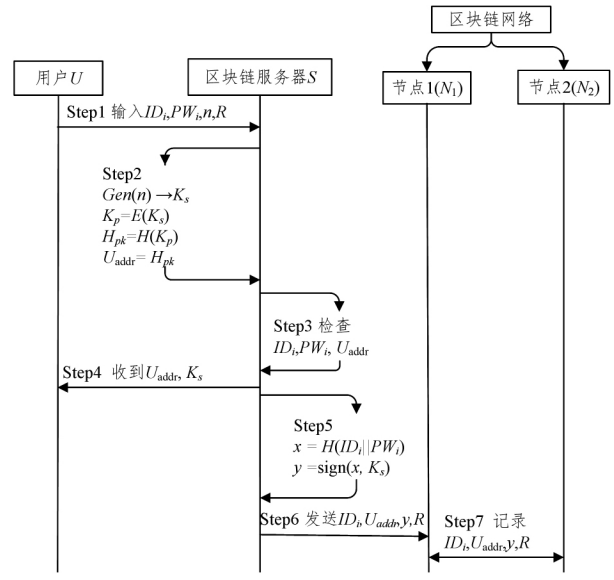

图 3 注册阶段的流程图

Fig. 3 Flowchart of registration phase

Step 1 用户 U_i 输入自己的用户名 ID_i、口令 PW_i 和随机数 n(用户进行注册操作时，系统自动分配随机数)进行注册操作 R，并且通过安全信道传输给区块链服务器 S。

$U_i\Rightarrow S:\{ID_i,PW_i,n\}$

Step 2 区块链服务器 S 收到用户发送的信息，使用随机私钥生成函数 $Gen(\ )$ 对输入的随机数进行处理，产生私钥 K_s，基于私钥通过椭圆曲线算法生成公钥 $K_p=E(K_s)$。由于此时的公钥长度不固定，利用哈希函数对公钥进行哈希运算 $H(K_p)$，得到固定长度，记为 H_{pk}。此时，H_{pk} 就可以作为用户地址 U_{addr}。

Step 3 区块链服务器 S 收到来自用户的 ID_i、PW_i 的消息以及区块链服务器 S 生成的用户地址 U_{addr}，检查用户的身份信息是否已经存在。此时会出现以下两种情况：

(1)如果用户的 ID_i、PW_i 以及对应的用户地址 U_{addr} 已经存在，则注册失败，无法注册；

(2)如果用户的 ID_i、PW_i 以及对应的用户地址 U_{addr} 不存在，则可以注册，并且通过安全信道把用户地址 U_{addr} 和私钥 K_s 传输给用户 U_i。

$S\Rightarrow U_i:\{U_{\text{addr}},K_s\}$

Step 4 用户 U_i 收到来自区块链服务器 S 的信息，包括用户地址 U_{addr} 和私钥 K_s，其中私钥作为交易的重要标识，用户须妥善保存。

Step 5 注册成功后，区块链服务器将用户的 ID_i 和 PW_i 进行哈希运算即 $H(ID_i\ \|\ PW_i)$，记为 x，利用私钥 K_s 对摘要信息 x 加密生成数字签名，记为 y。

Step 6 区块链服务器 S 将 ID_i，U_{addr}，y，R 通过安全信道传输给区块链网络节点，本节以两个节点为例，节点 1 和节点 2 都会收到来自区块链服务器 S 的信息。

$S\Rightarrow N_i:\{ID_i,U_{\text{addr}},y,R\}$

Step 7 区块链节点 N_1 或 N_2 收到信息后，组装成交易并附上交易号 $Tx\text{-}id$ 广播到整个区块链网络中，交易通过共识机制记录在新的区块中，最终形成新的区块链。

在注册阶段，利用随机数、Hash 算法和椭圆曲线算法对

用户信息进行加密与解密，并将其存储在去中心化且不可篡改的区块链网络中。注册阶段的实现过程可以确保用户在注册时信息的安全性，有效避免恶意用户获取合法用户的注册信息以及其他常见的网络攻击。

3.3　登录与认证阶段

用户在登录与认证阶段的流程如图 4 所示。

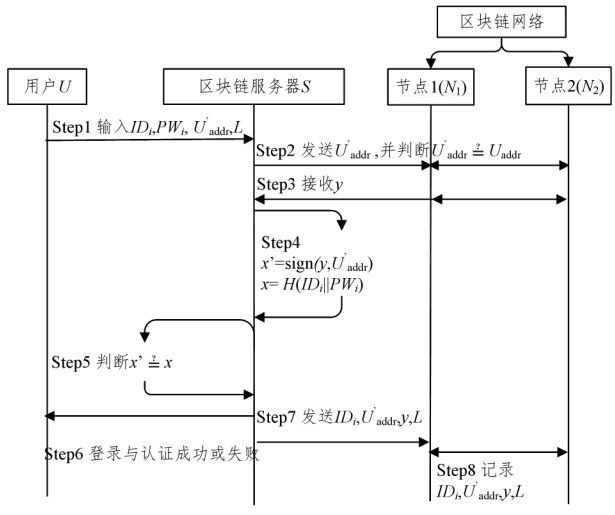

图 4　登录与认证阶段的流程图

Fig. 4　Flowchart of login and authentication phase

Step 1　用户 U_i 输入自己注册成功的用户名 ID_i、口令 PW_i 和用户地址 U'_{addr} 进行登录操作 L，并且通过安全信道传输给区块链服务器 S。

$U_i \Rightarrow S:\{ID_i, PW_i, U'_{addr}\}$

Step 2　区块链服务器 S 收到来自用户 U_i 传输的信息，将 U'_{addr} 通过安全信道发送到任意一个区块链节点 N_1 或 N_2 上，即 $S \Rightarrow N_i:\{U'_{addr}\}$，然后根据用户名 ID_i 查找注册时存储在数据库中的 U_{addr}，并判断 $U'_{addr} \overset{?}{\Rightarrow} U_{addr}$。此时会出现以下两种情况：

(1)如果 $U'_{addr}=U_{addr}$，则表示用户所拥有的用户地址和数据库中存储的用户地址一样，可以往下进行操作，执行 Step 3；

(2)如果 $U'_{addr}\neq U_{addr}$，则表示用户所拥有的用户地址和数据库中存储的用户地址不一样，从而登录与认证失败，请重新输入用户信息，执行 Step 1。

Step 3　如果 Step 2 成功，则区块链服务器 S 会收到来自节点 N_i 通过安全信道发送的信息 y。

$N_i \Rightarrow S:\{y\}$

Step 4　区块链服务器接收到签名信息 y 之后，利用 U'_{addr} 对 y 进行解密，得到摘要信息 x'，并通过哈希函数计算 $x=H(ID_i \| PW_i)$。

Step 5　区块链服务器验证 x' 和 x 是否相等，此时会出现以下两种情况：

(1)如果 $x'=x$，则表示用户 U_i 登录输入的信息和存储在区块链数据库的原始信息一致，登录与认证成功；

(2)如果 $x'\neq x$，则表示用户 U_i 登录输入的信息和存储在区块链数据库的原始信息不一致，登录与认证失败，请重新输入用户登录信息，执行 Step 1。

Step 6　如果登录与认证成功，则区块链服务器 S 通过安全信道给用户 U_i 发送登录与认证成功，执行 Step 7。

$S \Rightarrow U_i:\{$登录与认证成功$\}$

如果登录与认证失败，则区块链服务器 S 通过安全信道给用户 U_i 发送登录与认证失败。

$S \Rightarrow U_i:\{$登录与认证失败$\}$

Step 7　区块链服务器 S 将 ID_i, U'_{addr}, y, L 通过安全信道传输给区块链网络节点。本节以两个节点为例，节点 1 和节点 2 都会收到来自区块链服务器 S 的信息。

$S \Rightarrow N_i:\{ ID_i, U'_{addr}, y, L\}$

Step 8　区块链节点 N_1 或 N_2 收到信息后，组装成交易并附上交易号 $Tx\text{-}id$ 广播到整个区块链网络中，交易通过共识机制记录在新的区块中，最终形成新的区块链。

在登录与认证阶段，分为两个阶段进行认证。第一次认证：用户注册后得到的用户地址 U'_{addr} 与存储在去中心化且不可篡改的区块链网络中的 U_{addr} 进行对比认证；第二次认证：用户收到来自区块链服务器的签名信息中的 x' 与用户登录时产生的 x 进行对比认证。通过登录与认证阶段的实现过程，用户进行了两次认证，更加有效地验证了无线网络中的合法用户，避免了恶意用户的非法连接，同时能够更加有效地避免无线网络中常见的网络攻击，如中间人攻击等。

3.4　交易阶段

3.4.1　注册产生交易阶段

用户在进行注册时，服务器 S 通过密码学技术产生用户地址 U_{addr}，然后将用户名 ID_i、用户地址 U_{addr}、注册操作 R 以及信息签名 $Signature$ 发送给区块链节点，区块链节点在收到上述信息后组成交易 $Transaction$ 并附上交易号 $Tx\text{-}id$，然后将其广播到整个区块链网络。经过共识机制后，有权记账的节点把一定时间内收到的交易记录在新的区块链中，形成全新的区块链。

用户注册产生交易阶段的流程如图 5 所示。

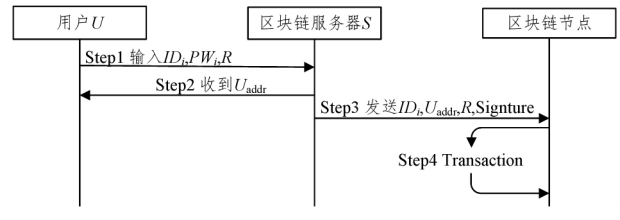

图 5　用户注册产生交易的流程图

Fig. 5　Flowchart for user registration to generate transaction

3.4.2　登录与认证产生交易阶段

在登录与认证阶段，用户向区块链服务器发送用户名 ID_i、登录口令 PW_i、用户唯一标识 U'_{addr} 以及登录操作 L，区块链节点根据用户唯一标识 U'_{addr} 返回签名信息给区块链服务器，区块链服务器通过用户地址 U'_{addr} 对数字签名进行解密，若得到的摘要信息与原始信息一致，则认证成功。随后，服务器将用户名 ID_i、用户地址 U'_{addr}、登录与认证操作 L 以及对信息的签名 $Signature$ 发送给区块链节点，区块链节点在收到上述信息后组成交易 $Transaction$ 并附上交易号 $Tx\text{-}id$，然后将其广播到整个区块链网络。经过共识机制后，有权记账的节点把一定时间内收到的交易记录在新的区块链中，形成全新的区块链。

用户登录与认证产生交易阶段的流程如图 6 所示。

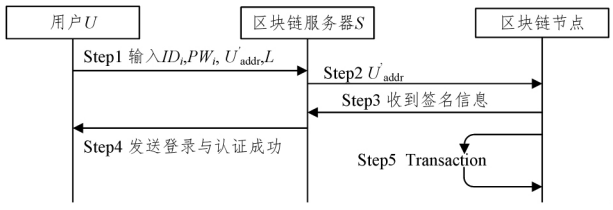

图 6 用户登录与认证产生交易的流程图

Fig. 6 Flowchart of user login and authentication to generate transaction

在交易阶段,用户在注册和登录与认证阶段产生的用户信息以交易形式存储在区块链中,用户信息一旦被存储在区块链中,将无法被篡改。此时,在无线网络环境下,恶意用户将不能攻击合法用户,身份认证信息也能够安全存储,并且共识机制使得认证效率大大提高。

3.5 共识机制

在区块链系统中,没有一个像银行一样的中心化记账机构来保证每一笔交易在所有记账节点上的一致性,即让区块链网络达成共识至关重要。在区块链网络中,使用共识机制来解决这个问题。目前主要的共识机制有工作量证明机制 PoW 和权益证明机制 PoS。PoW 通过证明工作量来决定用户是否拥有记账的权利,工作量越大,则用户越有机会获得记账权利。PoS 通过证明用户拥有代币的数量和时间长度来决定用户是否获得了记账的权利。

针对本文的实际情况,对现有的共识机制进行改进,使用工作量证明机制和延长最长链算法来解决共识问题。

(1)工作量证明规则

1)一段时间内只有一人可以记账成功。

2)通过解决密码学难题(即工作量证明)竞争获得唯一记账权。

3)其他节点复制记录结果。

(2)延长最长链算法

在工作量证明中,如果有两个节点或多个节点同时完成工作量证明,则无法确定哪一个节点获得记账权。此时,通过延长最长链的节点获得记账权。一段时间内的交易经验证后被记录在区块中,通过连接前一个区块成为最新的区块链,其他节点复制该区块链记录账本。延长最长链的 Python 伪代码如算法 1 所示。

算法 1 延长最长链算法

```
def Long-chain(self)->布尔类型
邻居节点信息=self.节点信息
最大长度=自身链长度
新的链条=None
  for 节点 in 邻居节点信息:
    response=requests.get(获取邻居节点链条的信息)
    if response.状态 == 200:
    节点链长度=response.json()['链的长度']
      节点链=response.json()['链的信息']
      if 节点链长度>当前链的最大长度 and 该节点链为有效链
最大长度=节点链长度
新的链条=节点链条
  if 新的链:
    自身链条=新的链条
  return True
return False
```

4 性能分析

4.1 安全性分析

本节将对 MWSASB 方案的安全性进行分析,并将其与其他同类型的无线安全认证方案进行对比。安全性对比如表 2 所列。

表 2 安全性分析

Table 2 Security analysis

攻击类型	文献[11]方案	文献[15]方案	MWSASB
DDoS 攻击	√	√	√
内部攻击	√	√	√
伪装攻击	×	×	√
口令猜测攻击	×	√	√
中间人攻击	√	√	√

注:√表示可以抵御,×表示不可抵御

4.1.1 抵抗分布式拒绝服务(DDoS)攻击

区块链的分布式结构基于点对点的网络架构,如果一个节点出现故障,则不会影响其他节点正常工作,因此不存在单点失效的问题。相对于中心化的服务系统架构,它对拒绝服务攻击更有效,因为一旦节点出现故障,与故障节点连接的用户将无法进入到系统中。

4.1.2 内部攻击

在本文提出的 MWSASB 方案中,用户 U_i 进行注册、登录与认证时,首先输入登录口令,服务器 S 对用户信息进行哈希运算得到 x,假设恶意用户 C 窃听到 x,由于 Hash 函数具有单向性和抗碰撞性,恶意用户 C 很难推出用户信息,因此本文提出的 MWSASB 方案能够有效防止内部攻击。

4.1.3 伪装攻击

在区块链中,由于任意节点之间的活动均受到全网的监督,并且数据库采用分布式存储,对于恶意用户 C 来说,无法伪装进行欺诈活动,因此本文提出的 MWSASB 方案能够有效防止伪装攻击。

4.1.4 口令猜测攻击

在本文提出的 MWSASB 方案中,当用户 U_i 进行注册时,假设恶意用户 C 可以窃听到 ID_i 和 PW_i 等信息,但是随机数 n 是在进行注册操作时系统自动分配的,因此 C 无法得到 n,从而无法得到私钥 K_s 和用户地址信息 U_{addr};当用户 U_i 进行登录与认证时,恶意用户由于无法取得用户地址信息 U_{addr}(用户登录认证的唯一凭证),因此无法进行登录与认证,从而登录失败,故本文提出的 MWSASB 方案能够有效防止口令猜测攻击。

4.1.5 中间人攻击

在本文提出的 MWSASB 方案中,用户在注册、登录与认证时对用户信息和口令 PW_i 进行哈希运算得到哈希值 x,再将该值通过安全信道发送给服务器,以保证认证信息不会被篡改。当服务器与节点通信时,通过安全信道传输 ID_i,U_{addr},y 及相关信息,恶意用户 C 无法对其进行篡改。因此,本文提出的 MWSASB 方案能够有效防止中间人攻击。

4.2 运算量分析

本节将对 MWSASB 方案的运算量进行分析,并将其与其他同类型的身份认证方案如文献[11]和文献[15]中的方案

进行对比。运算量分析主要表现为方案运算简单、系统开销小，因此从 4 个方面（即加密与解密次数、数字签名与验证次数、哈希运算次数和椭圆曲线算法次数）进行运算量分析，如表 3 所列。

表 3　运算量分析

Table 3　Computational analysis

方案	加密与解密次数	数字签名与验证次数	哈希运算次数	椭圆曲线算法次数
文献[11]方案	0	0	23	7
文献[15]方案	4	2	2	3
MWSASB	0	2	3	1

与文献[11]中的方案相比，本文所提出的 MWSASB 方案减少了 20 次哈希运算和 6 次椭圆曲线运算。但是本方案使用区块链技术，在用户注册、登录与认证时产生 2 个交易，并附上 2 个签名，因此 MWSASB 方案多使用 2 次数字签名的运算量来解决文献[11]的网络攻击问题。通过比较发现，使用区块链技术的无线安全认证能够大幅度地减少运算次数，有效解决安全和效率问题。

本文所提出的 MWSASB 方案与文献[15]中的方案都是利用区块链技术进行认证。文献[15]是基于区块链技术的传统安全认证方法，利用 4 次加密与解密运算、3 次椭圆曲线运算、2 次数字签名运算和 2 次哈希运算对生物特征和口令进行认证。而本文的 MWSASB 方案完全使用区块链技术，通过多阶段级联和共识机制的方式降低了传统无线安全认证的复杂过程，比文献[15] 少了 4 次加密与解密运算以及 2 次椭圆曲线算法，只多出 1 次哈希运算，大大提高了运算效率。本方案多出 1 次哈希运算的原因是在登录与认证时对用户信息进行了 2 次认证，提高了本方案的安全性；而文献[15]只进行 1 次认证，使得安全性比本方案更低。根据运算量分析，MWSASB 方案基于区块链技术中的密码学技术，能够有效地降低计算开销和提高无线身份认证的安全性，并利用共识机制算法使得网络节点共识速度得到明显提高。

结束语　基于传统的中心化网络架构，一旦中心节点出现故障或被攻击，整个网络将会遭受破坏，用户的信息无法安全连接到网络设备中。本文提出了一种基于区块链技术的多阶段级联无线安全认证方案。该方案利用工作量证明和延长最长链相结合的共识机制，将用户的信息产生交易记录在不可篡改且去中心化的区块链账本中，并分别设计了用户注册阶段、用户登录与认证阶段和交易阶段 3 个协议过程。根据安全性分析，MWSASB 方案能够有效地避免分布式拒绝服务(DDoS)攻击等常见的攻击方式，使得用户能够在无线网络环境下安全识别网络设备，不被恶意用户攻击。根据运算量对比分析，MWSASB 方案使用了较少的运算量，能够有效地降低运算成本。将 MWSASB 方案应用于实际系统中，在实际的系统中检测 MWSASB 方案的可行性，并对共识机制算法进行进一步研究，提高区块链网络对交易达成共识的效率，将是进一步研究的内容。

参 考 文 献

[1] SARASWATHI S, YOGESH P. Secure and efficient Smart-Card-Based remote user authentication scheme formulti-server environment[J]. Canadian Journal of Electrical and Computer Engineering, 2015, 38(1): 20-30.

[2] CHEN Y L, DU Y J, YANG G. Efficient attribute-based authenticated key agreement protocol [J]. Computer Science, 2014, 41(4): 150-154. (in Chinese)
陈燕俐，杜英杰，杨庚. 一种高效的基于属性的认证密钥协商协议[J]. 计算机科学，2014，41(4)：150-154.

[3] ZHAO Y. Design of Dynamic Password Authentication System [J]. Journal of Luoyang Normal University, 2012, 31(8): 36-37.

[4] LAMPORT L. Password authentication with insecure communication[J]. Communication of the ACM, 1981, 24(11): 770-772.

[5] ASHISH K, HARI O. An improved and secure multiser-ver authentication scheme based on biometrics and smartcard[J]. Digital Communications and Networks, 2018, 4(1): 27-38.

[6] ZHAN L, YAO G X, QIANG H C. Improved mutual authentication scheme based on smartcard for cloud computing[J]. Computer Engineering and Design, 2014, 35(2): 440-444.

[7] XIONG L, JUNGUO L, JIAO Z, et al. A secure remote user mutual authentication scheme using smartcards [C]// Computers, Communications and IT Applications Conference. IEEE, 2014: 89-92.

[8] JAEWOOK J, DONGHOON L, HAKJUN L, et al. Security Enhanced Anonymous User Authenticated Key Agreement Scheme Using Smart Card[J]. Journal of Electronic Science and Technology, 2018, 16(1): 45-49.

[9] LI X, NIU J W, MA J, et al. Cryptanalysis and Impro-vement of a Biometric-based Remote UserAuthentication Scheme Using Smart Cards[J]. Journal of Network and Computer Applications, 2011, 34(1): 73-79.

[10] QU J, PENG Y, TAN X L, et al. Anonymous Rem-ote User Authentication Scheme Based on Bioligical Features [J]. Computer Engineering, 2015, 41(6): 126-129, 135.

[11] YIN Q S, CHEN J H. Improved Identity Authentica-tion Protocol Based on Elliptic Curve Cryptography in Multiserver Environment [J]. Computer Science, 2018, 45(6): 111-116, 150.

[12] NAKAMOTOS. Bitcoin : apeer-to-peerelectron-iccashsystem [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[13] 工信部. 中国区块链技术和应用发展白皮书 [R]. 北京：工信部，2016：23.

[14] LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115.

[15] ZHOU Z C, LI L X, GUO S, et al. A biometrics and password two-factor crossdomain authentication scheme based on blockchaintechnology[J]. Journal of Computer Applications, 2018, 38(6): 100-107.

[16] FROMKNECHT C, VELICANU D. CertCoin: A NameCoin based decentralized authentication system: Technical Report, 6.857[R]. Class Project, Massachusetts Institute of Technology, 2014.

[17] FROMKNECHT C, VELICANU D. Adecentralizpublic key infrastructure with identity retention: Technical Report, 803[R]. Massachusetts Institute of Technology, 2014.

[18] RAJU S, BODDEPALLI S, GAMPA S, et al. Identitymanagement using blockchain for cognitive cellular networks[C]// IEEE International Conference on Communications. IEEE, 2017: 1-6.