文章编号：2095-2163(2023)04-0084-07 中图分类号：TP311.1 文献标志码：A

基于区块链的长租房可靠交易系统设计与实现

邵子尧，姜 怡，南林娜，范宇晗，彭 力
（江南大学 物联网工程学院，江苏 无锡 214122）

摘 要：针对当前长租房系统中出现的难以维权、信息不对称等问题，同时改善用户的使用体验，开发一套基于区块链的长租房可靠租赁交易系统。从用户的实际需求与利益出发，系统基于区块链技术的不可篡改性、自治性等特点，依托于共识机制，并通过智能合约进行交易，同时根据现实需求对当前区块链网络结构与共识算法进行优化。能够解决租房过程中“第三方信任”的问题，可以提高平台的用户可信度、改善国内长租房整体环境，响应国家政策、保障民生，推动国内长租房市场健康蓬勃发展。

关键词：区块链；租房；安全；交易系统

Design and implementation of reliable transaction system for long-term rental housing based on blockchain

SHAO Ziyao, JIANG Yi, NAN Linna, FAN Yuhan, PENG Li
(School of Internet of Things Engineering, Jiangnan University, Wuxi Jiangsu 214122, China)

【Abstract】 In view of problems such as difficulty in safeguarding rights and information asymmetry in the current long-term rental system, meanwhile for improving the user experience, the paper develops a set of long-term rental housing transaction system based on blockchain. The system is based on the actual needs, interests of users and the characteristics of blockchain technology, such as immutability and autonomy. Relying on the consensus mechanism, transactions are conducted through smart contracts. Furtherly, the current blockchain network structure and consensus algorithm are optimized according to the actual needs. It can solve the "third party trust" problem in the rental process, improve the credibility of users of the system and the environment of domestic rental houses, respond to national policies, protect people's livelihood, and promote the healthy and vigorous development of China's rental market.

【Key words】 blockchain; renting; safety; trading system

0 引 言

随着国内城市化进程不断加快，租房市场已成为刚性需求市场。根据《2021 年中国房屋租赁市场分析报告》，近年来受国家支持力度的加大、利好政策的出台等影响，国内房屋租赁行业得到较快的发展。2017 年 7 月，住建部等九部门联合印发《关于在人口净流入的大中城市加快发展住房租赁市场的通知》[1]，鼓励 2020 年，租房市场规模将达到 2.71 万亿元，到 2023 年国内房屋租赁总面积将会达到 83.82亿平方米，租赁人口达到 2.48 亿人[2]。

因此，中国租赁市场发展迅速。但是研究可知，大部分租赁市场不规范，市场供需不平衡，导致许多的社会资源被浪费。国内房屋租赁体系主要可分为 4 类[3]：全国性租房类门户网站、全国性房地产中介的专用系统、全国性共享式短租平台、由政府主导和筹备的房屋租赁平台以及公租房。但由于租房信息登记不全、房源安全监管不到位、虚拟且隐蔽的网络环境等风险的存在，导致国内现有的租房系统存在一定问题。其主要问题可表述为[4]：缺乏沟通，造成信任不足。在房屋租赁场景中有着多种信任需求，对于不同主体需求可得探讨阐释如下：

基金项目：国家自然科学基金（61873112）。

作者简介：邵子尧(2001-)，男，本科生，主要研究方向：物联网工程；姜 怡(2001-)，女，本科生，主要研究方向：物联网工程；南林娜(2001-)，女，本科生，主要研究方向：计算机科学与技术；范宇晗(2001-)，男，本科生，主要研究方向：工业工程；彭 力(1967-)，男，博士，教授，主要研究方向：控制科学与工程。

通讯作者：彭 力 Email：pengli@ jiangnan.edu.cn

收稿日期：2022-05-16

（1）交易信息的完整性与防伪。

（2）房源信息在房主与用户之间传递的完整性与真实性。

然而，房主与租客之间有着天然的信息壁垒，而两者的交易又只通过第三方平台实现，相互间的信息交流是否真实可靠只依赖于第三方平台的可信度，因此交易存在未知风险，可信度评估上还需不断完善。同时，租赁双方用户的信息真实性与隐私安全性也得不到保障[5-7]。

1　区块链技术

1.1　区块链介绍

区块链第一次出现是在 2008 年，那时“中本聪”在密码学论坛上公开了了《比特币：一种点对点的电子现金系统》一文[8]。

区块链作为一种典型的分布式账本技术，通过共识等多边形自治技术手段支持数据验证、共享、计算、存储等功能[9]。区块链以区块作为存储单位，依据时间戳从早到晚组成了一个单项链式结构。可利用共识机制实现网络中各节点之间的信息共享；使用非对称式加密技术保证信息的完整性、不可篡改性与安全性；通过对挖出区块的矿工进行奖励，激励矿工去生成区块；利用在链上部署智能合约实现区块链的自治性。总体来说，区块链构成了一种全新的、自治的分布式基础架构与计算范式[10]。

1.2　区块链技术优势

1.2.1　去中心化

与其他的分布式一致性协议相比，区块链最显著的优势就是去中心化。区块链利用 POW 算法等共识机制解决拜占庭将军问题，其开放性网络允许任意节点接入并下载账本，同时，当小部分节点被恶意入侵时，区块链网络仍然能够实现一致性。

1.2.2　不可篡改性

区块链中的区块都是用哈希作为本区块的信息摘要，哪怕一个字节的变化都会导致区块哈希发生极大改变。攻击者对区块进行更改会造成链分叉等现象，但若攻击者没有控制系统中超过 51% 的节点，错误也将很快得到改正。

1.2.3　可溯源性

由于所有的交易都按时间顺序存储在区块上，同时具有不可篡改性，因而用户可以查询到所有交易最原始的信息。

1.2.4　可编程性

以太坊（Ethereum）平台上支持的智能合约为区块链增添了可编程属性[11]，将区块链构建成一个可编程的数据共享平台[12]。因而区块链的交易可以摆脱第三方的束缚，同时也减少了人力人本。

1.3　P2P 网络

区块链的底层网络技术采用的是 peer-to-peer 网络，简称 P2P 网络。这是一种分布式网络通信技术，又称对等网络。网络结构如图 1 所示。图 1 中，实线表示物理连接，虚线表示逻辑连接。与传统的客户端/服务器端（client/server，C/S）结构不同的是，在 P2P 网络中各个节点之间没有主从之分，地位都是对等的，每一个节点既可以是服务器端、也可以是客户端。

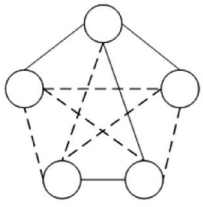


图 1　P2P 网络

Fig. 1　P2P network

2　系统设计

2.1　系统架构

基于区块链的租房平台的系统架构如图 2 所示。由图 2 可知，顶部是用户操作模块，其中包括信息展示与软件交互界面，用户可以通过本模块进行登录注册；房源提交、搜索与核查；预定房源、订单查看和核查；心愿单管理操作。左边是功能模块，是通过服务器来实现，根据客户端传递来的操作请求进行对应处理并返回对应数据，相关数据存储在本地数据库中。右边是区块链模块，需要将房主签名后的房源信息 HASH 和利用智能合约、多重签名生成的订单摘要信息生成区块后上链、并广播至网络中其他节点。区块信息通过节点的本地数据库进行存储。

2.2　区块链与功能模块设计

2.2.1　数字签名

为了保证信息的完整性与保密性，对于上链信息要进行数字签名处理，数字签名算法如下：

$$ApplyECDSASign(PK,Data) \rightarrow Signature$$

首先，在用户注册的时候通过本地 ECDSA 椭圆曲线加密算法生成随机公私钥对（PK 与 SK），SK 保存在用户本地，将注册信息与 PK 通过可信链路上传至服务器，服务器将其存储到个人信息数据库中。

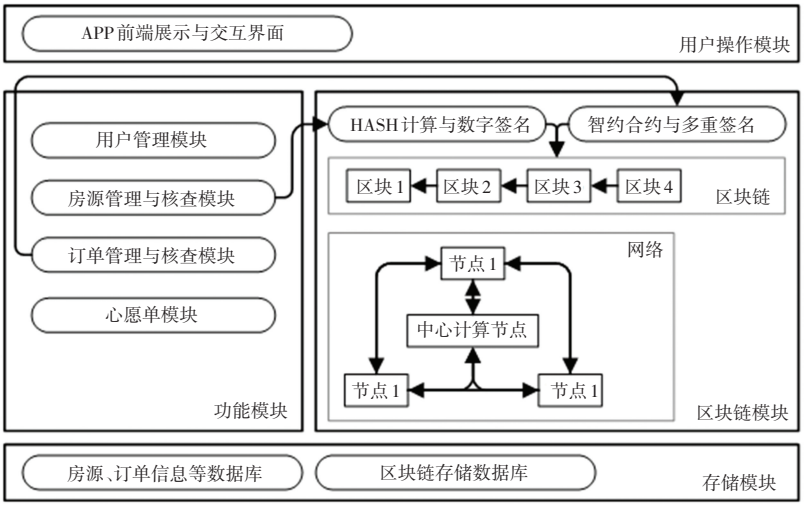


图 2 系统架构图

Fig. 2 System architecture diagram

在房源发布模块中,房主在提交房源时,要在本地利用 SK 对已填写的房源信息进行数字签名,并将签名后的信息与原信息一起上传至服务器,服务器正确接收后需要通过房主 PK 对信息进行验证,验证无误再进行此后的操作。

在交易模块中,当智能合约达成交易时,需要将交易信息以及租金暂存期间的银行流水信息在征得房主与用户同意的情况下,在本地利用其 SK 进行多重签名,签名后的信息返回至服务器后,服务器将其上链。

2.2.2 CPow 算法与弱中心化网络

CPow(Center-Pow)算法是本系统根据租房平台现实需求对于 Pow 算法的改进。

对于租房系统应用的区块链来说,块的生成是必要的,同时也是非奖励性质的,因此各节点之间不存在生成区块的竞争关系,而 Pow 是通过挖矿奖励驱动矿工,与本系统需求不符。基于此,本区块链将 Pow 算法改进为 CPow 算法。改进后的算法区块生成只由一个中心计算节点负责,并由平台保证节点生成区块的积极性,其他节点只负责存储以及验证区块。

CPow 算法在区块链实现过程为:

(1)选取一个 Hash 算法,例如 SHA-256。

(2)确定一个难度系数以确定目标 *HASH*。

(3)选取一个随机 *nounce* 与区块中所有信息(*data*, *time*, *prehash*, *hash* 等)拼接后由指定的中心计算节点计算 *HASH*。

(4)如果计算出的 *HASH* 小于目标 *HASH*,则说明找到了难题的解,将结果广播至其他所有主节点。

(5)如果计算出的 *HASH* 大于目标 *HASH*,则将 *nounce* 加 1 后继续计算,直到计算出难题的解。

同时,考虑到用户对于房源信息检查低延迟的需求,本系统应用的区块链网络为弱中心化网络,其具体结构如图 3 所示。

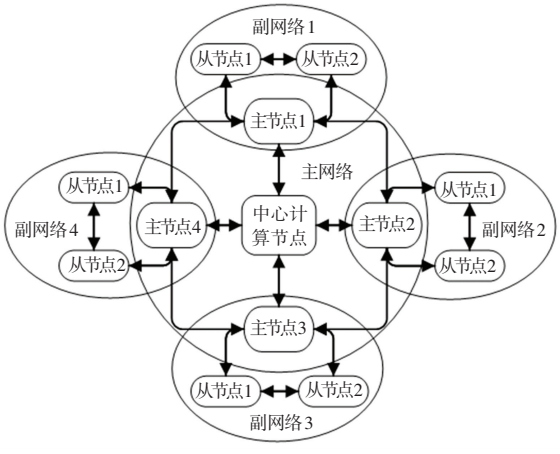


图 3 网络结构图

Fig. 3 Network structure diagram

整体区块链网络是由一个中心计算节点和 n ($n \geqslant 2$) 个普通节点构成。其中,中心计算节点相较于普通节点有生成区块的能力,并且拥有最高的安全等级。网络不允许未得到授权的节点加入。

同时,n 个节点中 m 个节点($m < n/2$) 各为一组,组成一个副网络,各个副网络中的节点只与本副网络中的节点核对账本,同时副网络随机挑选出一个节点作为主节点,各个主节点组成一个主网络进行

账本核对。系统根据当前账本核对最小时长 T，设置核对间隔 Ts，所有主副网络每隔 Ts 进行一次账本核对。因此，节点内的账本最长不可信时间为 Ts。

账本核对时，只核对每个节点所有区块信息整体 *Hash*，增强核对效率。并只认为被超过二分之一节点认同的 *Hash* 为正确 *Hash*，其余错误节点开始进行区块链的同步工作。

用户核查信息时，只需随机链接至某一主节点进行验证。

2.2.3　区块生成与共识

考虑到存储空间限制和空间的充分利用，区块只存储数字签名后的信息。区块由以下信息组成：*FreHash*（前区块哈希）、*Hash*（本区块哈希）、*Data*（上链信息）、*Nounce*（随机数）、*TimeStamp*（时间戳）。

当智能合约需要达成交易时，服务器先获取到需要上链的 *Data*，由中心计算节点生成区块，将其发送到所有节点进行共识，各个普通节点收到区块信息后对区块信息进行验证，信息验证无误将其上链，并对其上属节点进行回应。主节点接收到所有副节点应答后回应服务器，服务器接收到所有主节点的应答后，上链结束。

2.2.4　信息核查

当用户需要对房源信息或者订单信息进行核查时，客户端会向服务器发送信息核查请求，其中包括 *Code*（操作码）、*House_id*（房源编号）/*Order_id*（订单编号）、*User_id*（操作用户编号）。服务器接收到消息后，从房源 / 交易数据库中取出对应区块的 *Hash*，查找对应区块，将房源信息 / 订单信息、*Data*、*PK* 进行验证，验证通过，向客户端返回验证通过信息；验证失败，向客户端返回错误信息，同时服务器报 *System Error*（系统错误），等待系统管理员进行错误核查与解决。信息核查算法如下：

if　*verifyECDSASign*(*PK*,*Data*,*Signature*)　==　*true*

　return *True*(*Data*)；

else　if　*verifyECDSASign*(*PK*,*Data*,*Signature*)　==　*false*

　return *Error*(*Data*)；

else

　return *Error*(*System*)；

2.2.5　智能合约

本系统使用数字签名作为授权的手段。房源信息经过房主签名方可认定其有效；订单信息需经过房主、用户分别签名字后方可认定其有效。

本系统交易过程使用的智能合约流程如下：

（1）用户作为交易的发起方，先对交易进行数字签名，并预支付租金。

（2）系统将交易信息按照交易时间从早到晚的顺序存入交易信息数据库。

（3）系统对交易信息数据库内的信息条目从前至后进行读取。若交易时间未达 48 h，系统等待；若交易信息已达 48 h，系统提示房主进行签名，让事务能够顺利提交。

（4）系统将生成的区块广播至所有节点进行共识。

此外，如果在 48 h 内用户认为房源信息不真实或改变租房计划等，可以申请取消交易，系统就会将对应订单的 *Validity*（有效性）位置 *False*（错误）。这样一来，当 48 h 后系统读取此订单时，会自动将此订单抛弃，用户租金返还。就可以有效保护用户的权益，给予用户核查房源真实性的机会与取消交易的权利。合约流程如图 4 所示。交易自动检索与区块生成过程如图 5 所示。

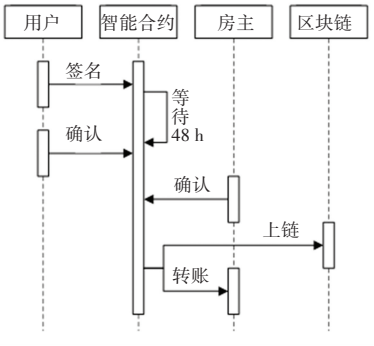


图 4　智能合约时序图

Fig. 4　Sequence diagram of smart contract

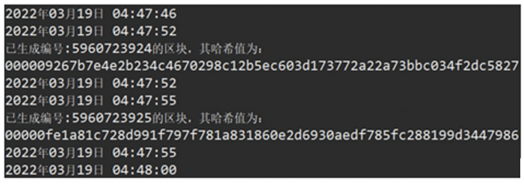


图 5　交易自动检索与区块生成示意图

Fig. 5　Schematic diagram of automatic transaction retrieval and block generation

2.2.6　网络核对与同步

网络核对方法如下（主网络核对完成后、再进行副网络核对）：

（1）系统根据上一次整体网络同步结束时间与开始时间的差值 T 与系统设置的额外同步时间 *EXT*

确定 2 次核对开始之间的时间间隔 Ts。数学计算公式具体如下：

$$Ts = T + EXT \quad (1)$$

(2)每个节点都将各自所有节点摘要信息额外存入一个 JSON 文件之中，每当收到新区块，都将信息存入此文件之中。数学计算公式具体如下：

$$INFOall\_new = INFOall\_old + CODE\_INFO \quad (2)$$

(3)当 Ts 倒计时结束，通过 SHA-256 算法计算文件 HASH，数学计算公式具体如下：

$$Abstract\_self = SHA256(INFOall) \quad (3)$$

(4)将自己的 Abstract 发送给所在网络中所有节点并接收其他所有节点发送来的摘要，同时进行区块信息有效性判别。其中，为被超过二分之一节点认同的 Hash 为正确 Hash，本节点信息正确，则返回正确；本节点信息错误，则会根据被网络认定为正确的信息进行信息同步，并返回错误。研发给出的代码如下：

```
INFO_SYNCHRONIZATION(){
  abstract_send(self_Abstract,all_other_code);
  while(! code_list.isEmpty()){
    code = code_list.get();
  if(Abstract_receive(Code) == self_Abstract){
    num ++;
  }
  if(num > n/2)
    return True;
  else
    System.synchr();
    return False;
}  }
```

这样子可以使得网络核查速度加快同时不会浪费过多的带宽资源。

3 系统实现

本系统根据实际需求，分为以下 4 个模块：用户管理模块、房源管理与核查模块、订单管理与核查模块、心愿单管理模块。

3.1 用户管理模块

打开软件后，点击个人中心，可以进行用户登录，或者点击注册，正确输入真实个人信息后点击提交，注册成功，注册成功后可进行登录，如图 6~图 8 所示。

在登录成功后，进入个人中心点击查看密钥，便可查看自己的 PK 与 SK，如图 9 所示。

图 6 个人中心

Fig. 6 Personal center

图 7 登录

Fig. 7 Login

图 8 注册

Fig. 8 Registered

图 9 查看密钥

Fig. 9 Viewing the key

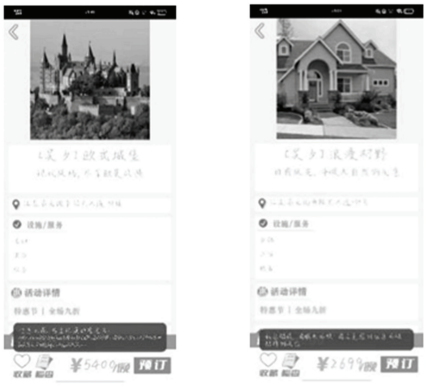
3.2 房源管理与核查模块

在个人中心界面点击“提交房源”，点击“房源地址”，完善相关信息；点击“房源概况”，完成相关信息；点击“房源介绍”，完善相关信息；勾选“用户须知：提交需授权 SK 对上传信息进行签名，点击“提交”，完成房源信息提交，如图 10 所示。

图 10 房源提交

Fig. 10 Housing submission

搜索到自己感兴趣的房子后，进入房源详细信息界面就可以对房源信息进行核查，若房源信息无误，如图 11(a)所示；若房源信息错误，见图 11(b)。



（a）房源信息无误　　（b）房源信息错误

图 11　房源核查

Fig. 11　Verification of housing supply

3.3　订单管理与核查模块

在房源详细信息界面可以进行预定，在交易详情中可以查看已有订单。点击对应订单条目，可以进行订单信息的核查，如图 12、图 13 所示。

图 12　房源预定　　图 13　订单详情

Fig. 12　Room reservation　　Fig. 13　Order details

3.4　心愿单管理模块

搜索到符合条件的房源，点击对应房源信息条目的心形按钮、即可收藏，再次点击、取消收藏；或者进入感兴趣的房源详细信息界面，点击“收藏”，收藏成功，再次点击取消收藏。回退至主页面；点击“心愿单”，点击刷新按钮，即可查看所有收藏房源，如图 14 所示。

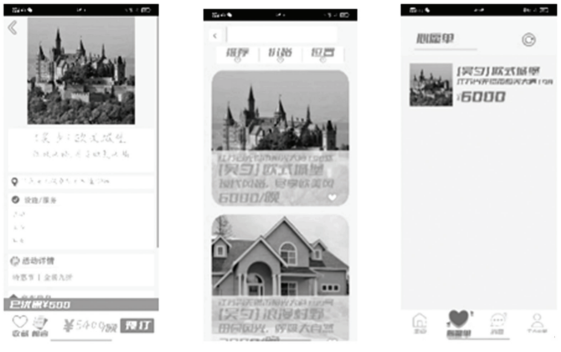


图 14　心愿单管理

Fig. 14　Wish list management

4　系统测评

4.1　运行成本分析

假设每一天生成区块的个数为 Num，每一区块平均计算成本为 $Cost$，节点总数为 $N(N \geqslant 3)$，区块总长度为 L，区块的平均信息量为 $Info$，由于验证成本相较于区块生成极小，因此忽略区块验证的成本。

两者核对账本的运行成本计算公式为：

$$ALLCOSTcheck = SHA256cost(L * Info) \quad (4)$$

对于 Pow 算法来说，运行成本计算公式为：

$$ALLCOSTpow = Num * Cost * n + ALLCOSTcheck \quad (5)$$

对于 CPow 算法来说，运行成本计算公式为：

$$ALLCOSTcpow = Num * Cost + ALLCOSTcheck \quad (6)$$

假设 Num、$Info$ 与 $Cost$ 保持不变，因此可以得到 2 种算法运行成本与节点总数关系如图 15 所示。

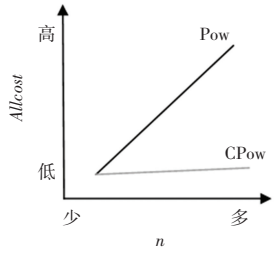


图 15　*Allcost* 与 *n* 关系

Fig. 15　Relation between *Allcost* and *n*

由图 15 中可以发现，随着节点个数的增加，Pow 算法的运行成本线性上升，而 CPow 算法运行成本增加缓慢。因此，CPow 算法在运行成本方面与 Pow 算法相比有着显著优势。

4.2　安全性分析

在本系统中，更改未来的区块需要攻破中心计算节点；更改已生成的区块，需要在 Ts 时间内攻破网络中二分之一的节点。

这里假设中心计算节点由于具有很高的安全级别难以被攻破，同时假设区块总长度为 L，区块的平均信息量为 $Info$，系统设置同步额外时间为 ExT，网络延迟为 WiT。Ts 的计算公式如下：

$$Ts = SHA256time(L * Info) + ExT + WiT \quad (7)$$

由于现代计算机哈希计算速度极快，因此可以忽略 $SHA256time(L * Info)$ 项，得到 Ts 如下：

$$Ts \approx ExT + WiT \quad (8)$$

由于系统安全性和 Ts 负相关，可以得到关系图如图 16 所示。

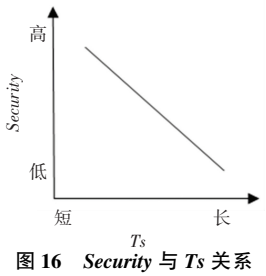


图 16 *Security* 与 *Ts* 关系

Fig. 16 Relation between *Security* and *Ts*

由图 16 可知,随着 ExT 增大,节点之间互相锚定的时间变长,Ts 的增加带来了区块链安全性的下降。此外,长度越长,链的可恢复程度也就越低。

同时,随着 ExT 减小,节点之间互相锚定的时间越来越短,Ts 减小,系统安全性越来越高,却使用了过多的系统资源。

因此,ExT 是本系统运行效率与安全性的重要参数,应当慎重考虑。

5 结束语

由于国内长租房领域未臻成熟,各类租房平台也有待规范,不仅难以保障租客、房主的利益,也在一定程度上关系到社会的安定与和谐。本文从租客与房主本身的利益出发,设计出一套基于区块链的长租房可靠租赁交易系统,可以保障租客、房主的利益,改善了用户的使用体验。本系统也对当下租房平台的设计产生了一定的指导作用。

参考文献

[1] 中华人民共和国住房和城乡建设部.《关于在人口净流入的大中城市加快发展住房租赁市场的通知》建房[2017]153 号[EB/OL]. [2017-07-20]. http://www.mohurd.gov.cn/wjfb/201707/t20170720_232676.html.

[2] 乐家栋. 万科:战略转型谋突破,收敛聚焦待新春[J]. 中国房地产,2019(02):32-38.

[3] 赵彬. 住房租赁交易服务系统的设计与实现[D]. 大连:大连理工大学, 2018.

[4] 牟春燕.郭丽华. 区块链技术下的房地产租赁平台发展研究[J]. 商业经济,2020(03):91-93.

[5] 李培培. 从房屋租赁模式看我国房屋租赁市场的发展[J]. 商业经济,2018(03):114-115.

[6] 陈秋竹,邓若翰. 长租公寓"租金贷":问题检视、成因探析及规制路径[J]. 南方金融, 2019(512):4.

[7] 单小虎,唐海燕,郑重. 房地产企业竞速布局长租公寓的挑战与对策[J]. 中国房地产,2018(08):13-19.

[8] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2018-10-05]. https://bitcoin.org/bitcoin.pdf.

[9] 韩璇, 袁勇,王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报,2019,45(01):206-225.

[10] 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.

[11] BUTERIN V. A next-generation smart contract and decentralized application platform [EB/OL]. [2018-10-05]. https://github.com/ethereum/wiki/wiki/White-Paper.

[12] YUAN Yong, WANG Feiyue. Blockchain and cryptocurrencies: model, techniques, and applications [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421-1428.

(上接第 83 页)

试函数并与其他 5 个算法进行仿真测试验证,实验结果表明 RLSSA 具有良好的收敛速度、收敛精度及鲁棒性。

参考文献

[1] 王龙龙. 基于改进鸟群算法在图像分割中的应用[D]. 赣州:江西理工大学,2019.

[2] EBERHART R, KENNEDY J. A new optimizer using particle swarm theory [C]// Proceedings of the Sixth International Symposium on Micro Machine and Human Science. Nagoya, Japan:IEEE,1995.

[3] MANIEZZO D V, COLORNI A. Ant system: Optimization by a colony of cooperating agents[J]. EEE Transactions on Systems, Man,and Cybernetics, B,Cybern.,1994, 26(1):29-40.

[4] MIRJALILI S, MIRJALILI S M, LEWIS A. Grey wolf optimizer [J]. Advances in Engineering Software, 2014,69: 46-61.

[5] KAVEH A, DADRAS A. A novel meta-heuristic optimization algorithm[M]. England:Elsevier Science Ltd., 2017.

[6] XUE Jiankai, SHEN Bo. A novel swarm intelligence optimization approach: sparrow search algorithm [J]. Systems Science & Control Engineering An Open Access Journal, 2020, 8(1):22-34.

[7] 吕鑫,慕晓冬,张钧,等. 混沌麻雀搜索优化算法[J]. 北京航空航天大学学报,2021,47(08):1712-1720.

[8] LIU Jianhua, WANG Zhiheng. A hybrid sparrow search algorithm based on constructing similarity [J]. IEEE Access, 2021, 9: 117581-117595.

[9] 钱敏,黄海松,范青松. 基于反向策略的混沌麻雀搜索算法[J]. 计算机仿真,2022,39(08):333-339,487.

[10] OUYANG Chengtian, LIU Yujia, ZHU Donglin. An adaptive chaotic sparrow search optimization algorithm[C]// 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). Nanchang:IEEE, 2021:76-82.

[11] MA Jie, HAO Zhiyuan, SUN Wenjing. Enhancing sparrow search algorithm via multi-strategies for continuous optimization problems [J]. Information Processing & Management: Libraries and Information Retrieval Systems and Communication Networks: An International Journal, 2022(2):59.

[12] LIANG Qiankun, CHEN Bin, WU Huaning, et al. A novel modified sparrow search algorithm based on adaptive weight and improved boundary constraints[C]// 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS). Chengdu:IEEE, 2021: 104-109.

[13] 毛清华, 张强. 融合柯西变异和反向学习的改进麻雀算法[J]. 计算机科学与探索, 2021, 15(06): 1155- 1164.

[14] 周向阳,罗雪梅,王霄. 应用改进状态转移算法优化多阈值图像分割[J]. 计算机仿真,2022,39(01):486-493.