

基于区块链的群智感知众包机制

张珠君^{1,2}, 朱大立^{1,2}, 范伟^{1,2}, 弥宝鑫¹, 彭诚¹

¹中国科学院 信息工程研究所 北京 中国 100084

²中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 众包作为一种基于群智感知技术的数据收集和任务分配模式,可有效提高任务完成的灵活性、多样性,节省运营成本,在移动医疗、环境监测、智能交通等领域有广阔的应用前景。目前的众包形态包括集中式和分布式,集中式众包的云服务器面临中心信任和安全问题,且存在因遵循服务器利益最大化原则导致众包工作者参与积极性低、任务收敛慢的性能问题;分布式众包面临着任务分配不均衡、分布式数据难以保持一致性等问题。针对以上问题,本文提出一种基于区块链的分布式众包机制,具体体现为:(1)建立基于区块链的众包模型,充分利用区块链去中心化、不可篡改等优势,解决中心服务器信任问题,适用于分布式的群智感知网络应用;(2)研究基于PBFT的数据同步机制,在保证数据一致性和算法容错性前提下,提高了共识效率;(3)设计服务质量评分算法和基于服务质量评分的任务分配和报酬发放机制,最大化接包方利益,调动参与者的积极性,提高服务完成率和服务质量。本文为阐明所提区块链众包机制的安全性,分别对系统的抗攻击能力、共识算法的安全性、服务质量评分算法的正确性分别进行了理论分析;为探讨机制的实用性,搭建Hyperledger Fabric并构造多节点环境进行算法仿真,验证了本文共识算法性能的优越性和多任务多用户条件下众包质量及效率上的提升。

关键词 众包; 区块链; 共识; 服务质量评分; 安全性; 可行性

中图分类号 TP309 DOI号 10.19363/J.cnki.cn10-1380/tn.2023.08.15

Blockchain-based Crowdsourcing Mechanism

ZHANG ZhuJun^{1,2}, ZHU Dali^{1,2}, FAN Wei^{1,2}, MI Baoxin¹, PENG Cheng¹

¹ Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Crowdsourcing, as a data collection and task allocation mode based on group intelligence perception technology, can effectively improve the flexibility and diversity of task completion, save operating costs, and has broad application prospects in mobile medical, environmental monitoring, intelligent transportation and other fields. The current forms of crowdsourcing include centralized crowdsourcing model and distributed crowdsourcing model. Centralized crowdsourcing cloud servers face central trust and security issues, and there are performance problems such as low enthusiasm for crowdsourcing workers and slow task convergence due to the principle of maximizing server benefits, while distributed crowdsourcing faces issues such as imbalanced task allocation and difficulty in maintaining consistency of distributed data. In response to the above problems, this paper proposes a blockchain-based distributed crowdsourcing mechanism, which is specifically embodied as: (1) Establish a crowdsourcing model based on the blockchain, make full use of the advantages of blockchain decentralization and non-tampering, to solve the problem of trust in the central server, which is suitable for distributed swarm-aware network applications; (2) Research on PBFT-based data synchronization mechanisms to improve consensus efficiency under the premise of ensuring fault tolerance and data consistency; (3) Design a service quality scoring algorithm and a reward mechanism based on service quality scoring to maximize the benefits of contractors, mobilize participants' enthusiasm, and improve service completion rate and service quality. To clarify the security of the proposed blockchain crowdsourcing mechanism, this paper conducts theoretical analysis on the system's anti attack ability, the security of consensus algorithms, and the correctness of service quality scoring algorithms, respectively. To explore the practicality of the mechanism, Hyperledger Fabric has been built and a multi node environment has been designed for algorithm simulation, verifying the superior performance of the consensus algorithm in this paper and the improvement of crowdsourcing quality and efficiency under multi task and multi user conditions.

Key words crowdsourcing; blockchain; consensus; service quality score; security; practicality

通讯作者: 范伟, 博士, 高级工程师, Email: fanwei@iie.ac.cn。

本课题得到国家重点研发计划(No. 2019YFB1005204)项目资助。

收稿日期: 2021-02-16; 修改日期: 2021-05-19; 定稿日期: 2023-08-09

1 引言

群智感知是利用众多的移动终端感知、获取各类数据的技术^[1]。随着物联网技术的蓬勃发展和各类智能移动终端设备的推广普及^[2], 众包作为物联网环境下一类基于群智感知的任务分配模式, 可有效降低成本, 提高任务完成效率, 在移动医疗、环境监测、智能交通等领域有广阔的应用前景^[3]。

当前的众包技术包括集中式和分布式两种应用模式^[4]。传统的集中式众包模型包括众包人、接包方和云平台^[5]。其中众包人是众包任务的发布者; 接包方竞争参与众包人发布任务的工作者, 通常需要一定的激励机制来调动工作者的积极性, 提高服务质量; 云服务器组成众包业务的服务平台, 负责众包人员管理、任务调试、数据存储等。这种众包模式一定程度上提高了任务完成的灵活性和多样性, 但是面临诸多挑战: (1) 中心服务器安全性上, 云平台面临信任问题^[6], 同时易遭受恶意用户发起的 Sybil 攻击和 DoS 攻击等^[7]; (2) 在数据保护方面, 云中心服务器存储和处理的数据对众包用户不可见, 存在篡改风险^[8], 众包感知用户无法真正监督、保护感知数据的可靠性; (3) 在任务完成积极性上, 由于对工作者的激励机制依赖于云平台服务器, 服务器会优先选择成本最小的竞争者承接任务, 不能最大化工作者效能, 工作者积极性不高, 不利于众包任务的高效执行。随着互联网产业和群智感知技术的发展^[9], 现在已衍生出了分布式众包形态, 通过分布式众包任务处理机制将中心化的安全责任分解给多方参与者^[10], 一定程度上提高了系统整体的抗攻击能力, 但是分布式的众包仍面临数据隐私保护和安全监管的问题^[11]。

基于以上分析, 一个安全且可行的众包模型需要满足以下条件: (1) 分布式处理模式, 以解决中心化信任问题; (2) 数据不可篡改; (3) 交易具有可追溯性; (4) 合理有效的激励机制, 以众包任务工作者效益为中心, 提高竞争积极性, 保障任务的完成率, 同时也能保证众包人的成本利益; (5) 良好的可扩展性, 可适应动态变化的众包参与者群体。

区块链是一种分布式账本技术^[12], 由大量分布式网络节点基于共识机制^[13]维护数据的一致性, 可解决中心化管理带来的安全问题和性能问题^[14]; 区块链共识技术和密码学技术^[15]可保证数据的不可篡改及可追溯^[16]。

因此, 本文提出一种基于区块链的分布式众包机制, 充分利用区块链去中心化、不可篡改^[17]等优势,

保证用户隐私, 并提高网络的可扩展性^[18]。本文的主要贡献包括 3 个方面:

(1) 提出基于区块链的众包机制, 避免了中心服务器的安全隐患, 且具有良好的安全性和实用性;

(2) 研究基于 PBFT^[19]的数据同步机制, 用于交易数据同步, 保证分布式数据的一致性, 具备一定的容错性能, 同时提高了共识效率;

(3) 建立众包工作者服务质量评价方法, 设计考虑服务质量的以参与者为中心的激励机制, 最大化接包方利益, 调动参与者的积极性, 提高服务完成率和服务质量。

2 相关工作

“众包”这一概念最早由美国记者在 2006 年提出, 描述的是一种依赖于互联网的基于大众共同参与价值创造的商业实践。随着移动智能设备的改造普及和网络技术的飞速发展, 众包作为一种基于群智感知数据的服务模式, 有效提高了任务的完成灵活性、速度、质量, 节约了大量生产成本但是在隐私保护、激励机制、安全性都方面还有许多待解决的问题, 吸引了大量学者去研究。目前的众包机制包括集中式众包和分布式众包。

Wang Kun 等人^[20]在 SIoT(社交物联网)中提出一种基于社交云的集中式众包模型, 社交云提供计算和存储功能, 并作为服务提供商来桥接最终用户和感知实体, 感知实体从服务提供商处接收任务和奖励并反馈数据, 并将基于声誉的拍卖机制引入众包中, 通过评估众包参与者的可靠性来执行优胜者选择和付款确定。该模型中社交云存储和处理数据的安全性有待进一步提高。

Liang Bomiao 等人^[21]基于聚合模型的众包机制, 并考虑了分布式系统面临的负载均衡问题。但该机制未考虑和分析隐私数据保护问题。

Li Ming 等人^[22]提出了一种基于智能合约的区块链众包模型, 可有效抵抗 Dos 攻击和 dDos 攻击, 且通过智能合约的实现提高了众包的灵活性。但该模型为充分考虑工作者服务水平的高低, 缺少众包服务质量的考虑。

黄守明^[23]提出了一种基于用户信誉的区块链众包系统, 该系统可通过信誉机制提高用户完成任务的质量, 但是缺少用户信誉机制的具体评判方法, 对众包场景中影响用户信誉的因素也未作具体分析。

为了调动用户完成任务的积极性, 众包激励机制也是一个研究热点。何云华等人^[24]提出一种基于区块链的分布式激励机制, 由矿工验证用户交易,

可有效避免共谋攻击, 并防止了第三方信任问题。不过该机制未充分考虑激励算法完全在区块链中运行的计算复杂度较高与区块链节点计算能力较低之间的矛盾。

Mohannad 等人^[25]提出一种用户信誉评估算法, 并根据信誉奖励用户。但文章未详细描述基于信誉的激励方法, 且容易遭受 Sybil 攻击。

基于以上研究存在的问题, 本文提出一种基于工作者服务质量的区块链众包机制, 可有效抵制 DoS 攻击和 Sybil 攻击, 并且考虑了区块链共识的效率及安全问题, 同时提出了明确的服务质量评分算法和激励方法。

3 区块链众包模型和设计目标

本章提出了区块链众包模型, 并对其可能面临的攻击进行了分析, 同时明确了本文的设计目标。

3.1 区块链众包模型

区块链众包模型如图 1 所示。模型中的角色包括三类: 众包人(任务发布者)、接包方(工作者)、云

平台服务器。区别于传统的依赖云平台完成任务分配的方法, 在本文提出的众包模型中, 众包人和接包方基于区块链完成任务的发布、分配和感知数据处理。

为提高工作者积极性, 本文设计了基于工作者服务质量的激励算法。考虑到众包人、接包方客户端的存储能力、计算能力有限, 由云服务器完成计算复杂度较高的工作者服务质量评分算法和激励算法。在区块链共识完成后将共识结果同步给云平台, 云服务器记录具体的交易数据, 众包人、接包方客户端记录交易指针和交易哈希以保证数据的不可篡改和查询检索。

区块链众包模型中三个角色的具体分工如下:

- (1) 众包人: 发布任务, 预存任务完成报酬, 参与共识, 同步交易数据。
- (2) 工作者: 竞争任务, 接收任务记录交易数据和哈希, 参与共识, 同步交易数据。
- (3) 云平台服务器: 分配客户端标识 ID_U , 记录交易数据, 工作者服务评分, 报酬分配方案制定。

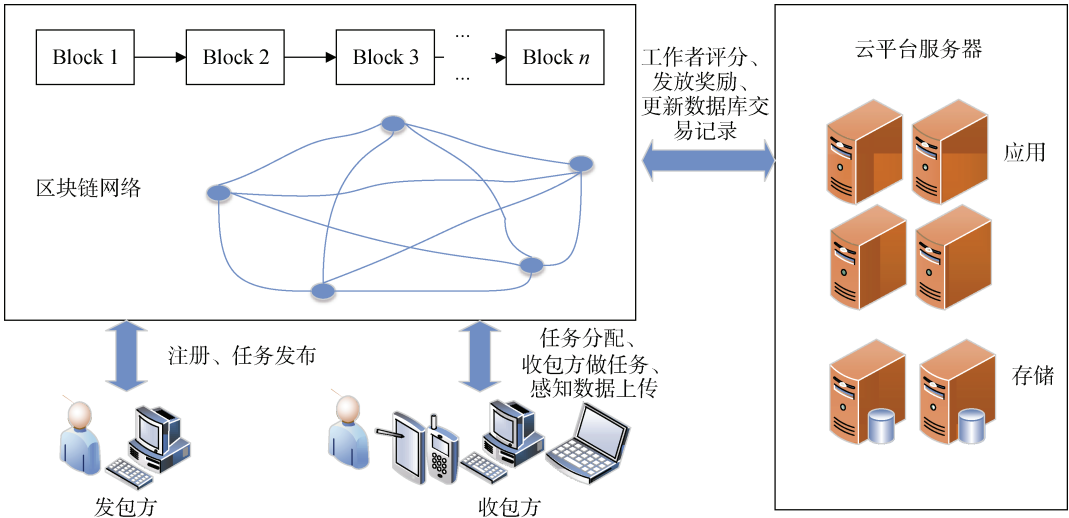


图 1 区块链众包模型
Figure 1 Blockchain-based Crowdsourcing Model

3.2 攻击模型

区块链众包机制安全依赖于分布式各个节点的安全, 在众包系统中, 可能存在恶意的工作者和众包人伪造、发送虚假数据, 以谋取非法利益, 影响众包任务分配和完成。基于群智感知网络和区块链系统面临的常见攻击分析^[23,24,26], 建立了区块链众包攻击模型, 如图 2 所示。

恶意节点攻击: 系统中可能存在恶意竞争现象, 恶意的众包人节点发送虚假的任务信息以争取更多工作者参与工作, 恶意的工作者节点发送虚假的感

知信息, 以谋取更多利益。

Sybil 攻击: 网络中少量攻击的众包人节点或工作者节点伪装成多个系统中的其他合法节点身份, 篡改数据, 导致区块链内存储的数据产生分叉, 影响任务分配和执行。

假冒攻击: 截获合法用户身份信息并实行欺诈行为;
节点捕获攻击: 捕获、破解少量合法节点密钥, 进而攻破整个网络;

重放攻击: 攻击者窃听用户成功验证的信息并重新发给验证者, 以获取更多的利益;

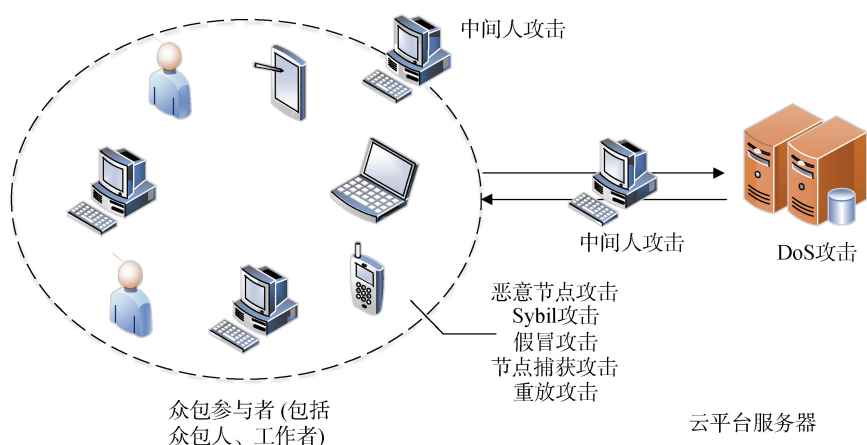


图2 攻击模型
Figure 2 Threat Model

中间人攻击: 有可能存在攻击者窃听、拦截并篡改网络传输的交易数据, 以谋取非法利益;

DoS 攻击: 对中心服务器发起攻击, 破坏众包交易正常进行和数据存储安全。

3.3 设计目标

本文建立基于区块链的群智感知众包机制, 旨在保证系统安全稳定运转、交易信息不被篡改的前提下, 提高众包完成质量和众包效率。本文设计的区块链众包机制应满足以下安全和性能要求。

(1) 安全性

1) 抗攻击能力: 基于 3.2 节分析的众包系统可能面临的攻击, 区块链众包机制应具备一定的抗攻击能力, 可有效抵抗恶意节点攻击、Sybil 攻击、假冒攻击、节点捕获攻击、重放攻击、中间人攻击和 DoS 攻击, 以保证系统安全、稳定运行;

2) 交易数据的一致性: 设计可靠、高效的共识机制, 保证任务发布信息、用户感知信息等交易数据在区块链系统中快速收敛, 保证数据一致性, 不会产生分叉。

(2) 性能

为保证众包任务的高效完成, 同时尽量提高任务完成质量, 提出以下性能要求。

1) 效率: 可调动更多优秀的工作者来竞争众包任务, 发布的任务能尽快找到合适的工作者承接;

2) 服务质量: 提出合理的任务分配和报酬支付方案, 以提高工作者积极性, 促使诚实、可靠的工作者承接任务, 以保证任务顺利、高效完成。

4 区块链众包运行机制

本章重点介绍区块链众包运行机制, 为便于描述, 在表 1 中定义了本文所用的符号。

表1 符号定义

Table 1 Definition of Notations

符号	定义
$S = \{S_1, \dots, S_i, \dots, S_n\}$	众包人集合
$W = \{W_1, \dots, W_i, \dots, W_n\}$	工作者集合
ID_U	用户的唯一标识
PK_U, SK_U	用户的公钥
$hash(M)$	消息 M 的哈希
$sig_{SK_U}(M)$	基于 SK_U 对消息 M 签名
$T = \{T_1, \dots, T_k, \dots, T_n\}$	任务
$score_{W_j T_k}$	工作者 W_j 完成任务 T_k 后获得的服务质量评分
m_k	任务 T_k 的具体内容
t_k	任务 T_k 的期限
t_{W_j}	工作者 W_j 完成任务预计的时间
$score_k$	任务 T_k 设定的用户质量评分阈值
$coin_{S_i T_k}$	众包人 S_i 预存, 用于支付完成任务 T_k 的工作者的押金
$coin_{W_j}$	工作者 W_j 要求的基本报酬

本文设计的基于区块链的众包运行机制如图 3 所示, 包括用户注册、任务发布、任务分配、工作者感知数据收集、工作质量评定及报酬发放 5 个步骤。

4.1 任务发布

用户注册完成后, 当众包人有任务需要执行时, 向区块链网络发布任务信息 $T_k = (m_k, t_k, score_k)$, 包括任务 T_k 的具体内容 m_k 、时间期限 t_k 、工人服务质量阈值 $score_k$ 。

同时, 众包人需要预先在系统中存储押金 $coin_{W_i}$, 用于支付完成任务的工作者报酬。如果众包

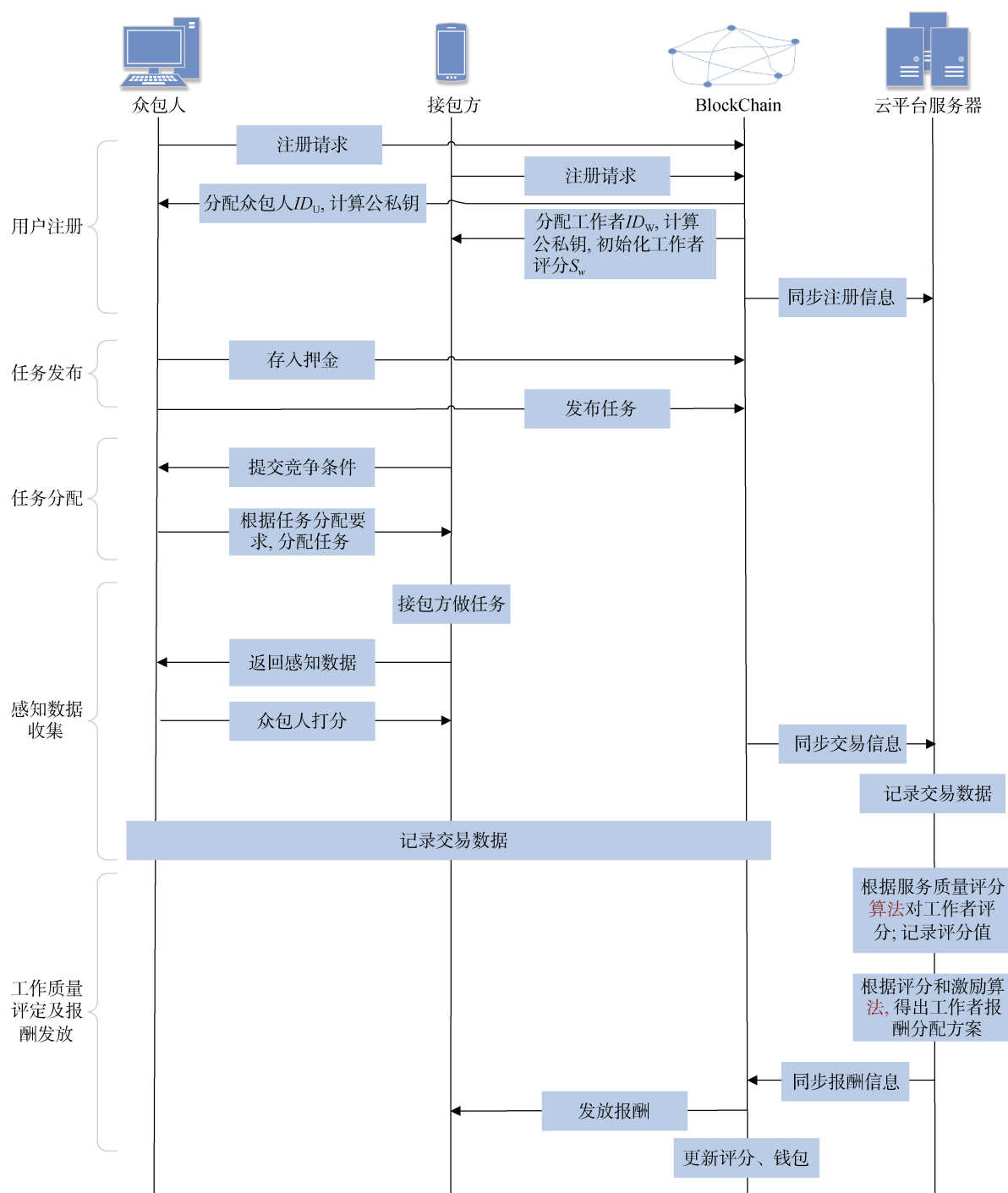


图3 区块链众包运行机制

Figure 3 Crowdsourcing Operating Mechanism

人未成功预存押金, 则不允许其发布任务, 以保证工作者在完成任务后能收到相应的报酬。

最后, 根据众包人提出的任务 T_k 的时间期限、工人服务质量阈值、最多可分配的工作者数量, 输出任务 T_k 的服务要求 $R(T_k)$ 。

值得说明的是, 任务的发布可以看作需要在区块链中确认的一笔交易, 需要通过共识运算保证交易在各节点存储的分布式账本的统一, 进而维持交

易进行的公平、公正和安全。

任务发布的主要过程参见算法 2。

Algorithm 2: Task Release

Input: $T_k = (m_k, t_k, score_k)$

Output: $R(T_k)$

- 1: For $T_k (0 < k < n)$ Do
- 2: $BC.receive(coin_{S_i|T_k})$;

```

3:  If  $false == BC.receive(coin_{W_j})$  Then
4:    goto Final;
5:  Else
6:     $S_i.broadcast(T_k)$ ;
7:     $consensus(T_k)$ ;
8:  If  $flase == consensus(T_k)$  Then
9:    goto Final;
10:  Else
11:     $R(T_k) = func(t_k, score_k)$ ;
12:  End If
13: End If
14: End For
15: Final
16: return  $R(T_k)$ 

```

由于众包对交易的时效要求比较高, 因此本文基于收敛速度快、相对节省资源的 PBFT(Practical Byzantine Fault Tolerance, 实用拜占庭容错)共识算法来构建可信安全的区块链账本。

设定当前网络中共 y 个节点参与共识, f 为可容忍的拜占庭节点数, 即不可信节点数。为提高算法执行效率和共识运算的可靠性, 本文根据上一轮任务的用户服务质量评分较高的节点 $W_{j|max(score)}$ 作为主节点, 当主节点收到任务发布请求时, 向其余用户节点 U 发送共识指令, 启动共识运算。共识开始时, $W_{j|max(score)}$ 在 *pre-prepare* 阶段广播信息 $(b, h, ID_U, hash(b), sig(hash(b)))$, 其中 b 是新区块, 可对应一个任务 T_k , h 是出块序号, ID_U 是节点标识, $hash(b)$ 是区块 b 的摘要, $sig(hash(b))$ 是摘要的签名。当其他作为副节点的用户 U 收到广播消息后进行验证, 验证合法后进入 *prepare* 阶段, 副节点 U 向全网广播消息 $(b, h, ID_U, hash(b), sig(hash(b)))$ 。当节点累计收到 $2f+1$ 条不同节点的不同 *prepare* 阶段广播的消息后, 进入 *commit* 阶段, 对交易信息进行确认, 并广播消息 $(b, h, ID_U, hash(b), sig(hash(b)))$ 。待每个节点收到超过 $2f+1$ 条不同节点在 *commit* 阶段广播的信息后, 对该区块达成共识, 并回应发送任务的众包人。由于在 *prepare* 阶段和 *commit* 阶段只要收到 $2f+1$ 条相同的广播信息即可完成共识, 网络中可能存在假冒或恶意节点, 这些节点广播的信息与共识结果并不相同, 因此在共识完成后, $W_{j|max(score)}$ 根据用户标识 ID_U 筛选出与共识结果计算一致的节

点 $U_x (0 < x \leq y)$ 参与到后续众包过程, 不一致的节点不可参加众包。

基于 PBFT 的众包共识算法参见算法 3。

Algorithm 3: PBFT-based Consensus

Input: $b, S_i, W_j (0 < i < n, 0 < j < m)$

Output: $U_x (0 < x \leq y)$

```

1: While  $(2 * f + 1) < y$ 
2:    $W_{j|max(score)}.select(W_{j|max(score)})$ ;
3:    $W_{j|max(score)}.accept(block, 0)$ ;
4:    $W_{j|max(score)}.broadcast(b, x, ID_U, hash(b), sig(hash(b)))$ ;
5:   For  $(x = 1, x < y + 1, x++)$ 
6:      $U_x.receive(block, l++)$ ;
7:      $U_x.prepare(b, x, ID_U, hash(b), sig(hash(b)))$ ;
8:      $U_x.commit(b, x, ID_U, hash(b), sig(hash(b)))$ ;
9:     If  $l > (2 * f)$  Then
10:       $U_x.mark(input, output, z)$ ;
11:       $U_x.broadcast(b, x, ID_U, hash(b), sig(hash(b)))$ ;
12:     End If
13:   End For
14:    $W_{j|max(score)}.accept(U_x.block, x)$ ;
15: End While
16:  $W_{j|max(score)}.reply(block, S_i)$ ;
17:  $W_{j|max(score)}.lookup(U_x, x++, z)$ ;
18:  $U_x = func(U_1, U_2, ..., U_z)$ ;
19: If  $true == p(U_z, W_{j|max(score)})$  Then
20:    $addBC(block, U_z)$ ;
21: End If
22: Final
23: return  $U_x$ 

```

4.2 任务分配

众包人发布若干个任务 $T = \{T_1, ..., T_k, ..., T_n\}$ 后, 根据发布任务阶段输出的任务 T_k 的服务要求 $R(T_k)$ 来招募并筛选工作者承担任务。同时, 工作者也需提出自己的竞争条件。本文假设某个用户承担某项任务需要的报酬是已知的, 工作者提出的竞争信息包括工作者要求的报酬 $coin_{W_j}$ 、任务执行时间 t_{W_j} 。

众包任务分配的过程如下:

(1) 任务分配条件筛选: 判断任务是否过期, 或者是否已分配给足够的工作者执行。过期任务和已分配的任务, 将不再招募工作者;

(2) 工作者筛选:

① 比较用户注册阶段更新的服务质量评分 $score_{W_j}$ 与任务发布阶段众包人提出的服务质量要求 $score_k$, 服务质量评分 $score_{W_j}$ 低于 $score_k$ 的工作者不会被分配到任务;

② 报酬要求 $coin_{W_j}$ 高于众包人提供的押金 $coin_{S_i|T_k}$ 的工作者, 不会被分配到任务;

③ 工作者提出的任务执行时间 t_{W_j} 超出任务时间阈值 t_k 的, 不会被分配到任务。

(3) 任务分配:

本文设定一个任务仅需一个工作者执行, 对于网络中的任务集合 $T = \{T_1, \dots, T_k, \dots, T_n\}$, 充分考虑任务完成的服务质量要求、完成时间、基本报酬要求等, 对符合要求的工作者按服务质量评分进行排序, 从高到低依次随机分配任务, 同时将已分配的任务锁定, 不可再分配给其他工作者。

任务分配的主要过程参见算法 4。

Algorithm 4: Task Assignment

Input: $R(T_k)$, W_j , $score_{W_j}$, $coin_{W_j}$, t_{W_j}

Output: T_k

```

1: For  $T_k$ ,  $W_j$  ( $0 < k < n, 0 < j < m$ ) Do
2:   If  $((t_k < time(now)) \parallel (true == IsAssigned(T_k)))$ 
3:     goto Final;
4:   Else
5:      $k++$ ;
6:   If  $((score_{W_j} < score_k) \parallel (coin_{S_i|T_k} < coin_{W_j}) \parallel (t_k < t_{W_j}))$ 
7:     goto Final;
8:   Else
9:      $sort(W_j, score_{W_j})$ ;
10:     $random(T_k, W_j)$ ;
11:     $T_k.locked(W_j)$ ;
12:     $T_k.setstate(locked)$ ;
13:     $j++$ ;
14:   End If
15: End For

```

16: **If** $unlocked == getState(T_k)$ **Then**

17: **continue**;

18: **Else**

19: **goto** **Final**;

20: **End For**

21: **Final**

22: **return** T_k

4.3 感知数据收集

由于群智感知众包中工作者集体是移动、多变和随机的, 因此需要充分感知工作者任务完成情况, 以便对工作者完成任务情况进行有效评价, 为后续任务选择工作者选择提供依据。

工作者执行一次任务需要提供的数据主要包括是影响工作者服务质量评价的积极因素和消极因素。积极因素包括: (1)本次任务是否成功完成; (2)超前完成任务的时间, 即任务设定的时间阈值 t_k 与任务完成实际时间 $t_{W_j|T_k}$ 的差值 $\Delta T_{W_j} = t_k - t_{W_j|T_k}$ 。消极作用因素包括: (1)工作者是否及时执行任务, 即开始执行本次任务 T_k 的时间延迟, 定义为工作者开始执行任务时间 $t_{W_j|T_k.begin}$ 与任务分配时间 $t_{T_k.begin}$ 的差值, 即 $\Delta T_{W_j|T_k.begin} = t_{W_j|T_k.begin} - t_{T_k.begin}$; (2)工作者 W_j 在执行本次任务 T_k 过程中遇到外界环境的干扰因素(比如通信链路中断、工作者设备故障等), 本文定义为 $\alpha_{W_j|T_k}$ 。积极因素量化值越大, 服务者质量评分越高; 消极因素量化值越大, 服务者质量评分越低。

基于上述数据定义, 系统收集相关感知数据, 在本地账本中进行同步, 同时上报给云平台, 用于后期云平台进行服务质量评定等操作。感知数据收集的具体过程为:

- (1) 工作者执行任务: 更新任务状态为执行中;
- (2) 收集感知数据: 工作者任务执行后, 返回任务完成数据;
- (3) 众包人评分: 众包人对工作者的任务执行情况进行打分, 该分值掺杂有众包人的主观因素;
- (4) 数据哈希及签名: 对感知数据进行签名、加密和哈希运算;
- (5) 数据同步: 工作者和众包人在本地账本中记录工作者的感知数据, 在区块链中发起共识, 共识算法依据算法 3, 在整个网络节点的区块链账本中同步感知数据;
- (6) 感知数据上报: 受限于工作者和众包人客户端设备的计算、存储条件, 共识完成后, 将共识的感知

数据上报给云服务平台, 由云服务器运行计算复杂度较高的服务质量评分算法, 以评定工作者服务质量。

感知数据收集的主要过程参见算法 5。

Algorithm 5: Perceptual Data Collection

Input: T_k, W_j

Output: $state(W_{j|T_k})$

```

1: For  $T_k, W_j$  ( $0 < k < n, 0 < j < m$ ) Do
2:   If  $T_k$  is started by  $W_j$  Then
3:      $t_{T_k|W_j}.begin = time(now)$ ;
4:      $T_k.setstate(started)$ ;
5:      $\Delta T_{W_j|T_k}.begin = t_{W_j|T_k}.begin - t_{T_k}.begin$ ;
6:      $W_j.excute(T_k)$ ;
7:   If  $T_k$  is completed by  $W_j$  Then
8:      $t_{W_j|T_k} = time(now)$ ;
9:      $\Delta T_{W_j} = t_k - t_{W_j|T_k}$ ;
10:     $T_k.setstate(completed)$ ;
11:     $\alpha_{W_j|T_k}$  is reported;
12:     $score_{W_j|S_i}$  is reported;
13:   Else
14:      $T_k.setstate(uncompleted)$ ;
15:      $T_k.setstate(unlocked)$ ;
16:     goto Final;
17:   End If
18: End If
19:  $state(W_{j|T_k}) = func(T_k.state, \Delta T_{W_j}, \Delta T_{W_j|T_k}.begin, \alpha_{W_j|T_k},$ 
 $score_{W_j|S_i})$ ;
20:  $sig_{SK_{W_j}}(state(W_{j|T_k}))$ ;
21:  $M = Enc(state(W_{j|T_k}), S_i)$ ;
22:  $hash(M)$ ;
23:  $consensus(M)$ ;
24: If  $flase == consensus(M)$  Then
25:   goto Final;
26: Else
27:    $upload(state(W_{j|T_k}))$ ;
28: End If
29: End For
30: Final
31: return  $state(W_{j|T_k})$ 

```

4.5 工作质量评定及报酬发放

为了更好的激励工作者高质量完成任务, 需要对工作者的任务完成情况进行合理、有效的评价, 并根据任务完成情况制定保证分配方案, 分配报酬。需要说明的是, 工作者服务质量评定和报酬分配的方案决策计算复杂度都比较大, 因此由云平台服务器完成。计算完成后, 云服务器再将报酬分配决策同步给区块链进行实际报酬的发放。

4.5.1 工作者服务质量评分算法

4.5.1.1 工作者服务质量评定指标定义

对一个工作者的评价要考虑多个因素, 涉及工作者自身能力和外界环境影响。其中, 工作者自身因素主要指工作者具备的服务水平, 通过历史服务完成度、超前任务时间、任务起始延迟时间体现; 外界环境影响主要考虑链路状态、工作者设备状态等因素的影响。基于工作者评价的影响因素及数据感知阶段工作者上报的数据, 给出与服务质量评价指标相关的定义。

定义 1. 工作者节点成功完成历史任务的次数 $N_{s|W_j}$ 与历史分配的任务总数 $N_{t|W_j}$ 的比值, 称为历史任务完成率, 记作 $R_{s|W_j}$, 即

$$R_{s|W_j} = \frac{N_{s|W_j}}{N_{t|W_j}} \quad (1)$$

定义 2. 工作者节点实际成功完成历史任务的时间与该任务设定的完成期限的差值的平均值, 称为超前完成任务时间差均值, 记作 $\overline{\Delta T_{W_j}}$, 即

$$\overline{\Delta T_{W_j}} = \frac{\sum_{k=1}^{N_{s|W_j}} (t_k - t_{W_j|T_k})}{N_{s|W_j}} \quad (2)$$

定义 3. 工作者节点开始执行任务与任务分配给工作者的时间的差值的平均值, 称为任务延迟执行时间差均值, 记作 $\overline{\Delta T_{W_j|T_k}.begin}$, 即

$$\overline{\Delta T_{W_j|T_k}.begin} = \frac{\sum_{k=1}^{N_{s|W_j}} (t_{W_j|T_k}.begin - t_{T_k}.begin)}{N_{s|W_j}} \quad (3)$$

定义 4. 外界环境对工作者服务的影响, 称为环境影响因子, 记作 β_{W_j} , 即

$$\beta_{W_j} = \frac{\sum_{k=1}^{N_{s|W_j}} \alpha_{W_j|T_k}}{N_{s|W_j}} \quad (4)$$

4.5.1.2 工作者服务质量评分算法

本文设计的工作者服务质量评价基于三方面因素: (1) 众包人在一次任务完成后给出的评价分值

$score_{W_j|S_i}$, 由于此分值受众包人主观情感因素影响, 还需考虑实际任务完成的数据; (2) 工作者完成任务后上传的感知数据; (3) 对工作者的服务质量评价是随时间动态更新的, 近期的任务完成数据影响应高于早期的任务完成数据的影响。

因此, 工作者服务质量评分算法分为三个步骤:

(1) 基于熵值法的感知数据量化评分

工作者感知数据多种多样, 为了更客观有效地量化感知数据对服务质量指标的权重, 本文采用熵值法进行感知数据量化评分。具体流程如下:

① 指标参数计算: 根据 4.4 节获取的感知数据和 4.5.1.1 节定义的服务质量指标, 计算得到各指标参数 $\delta = (R_{s|W_j}, \overline{\Delta T_{W_j}}, \overline{\Delta T_{W_j|T_k.begin}}^{-1}, \beta_{W_j}^{-1})$;

② 指标权重确定: 基于熵值法实现过程, 按照建立数据矩阵→数据非负处理→计算各指标比重→计算指标熵值→计算指标差异系数→计算指标权重, 获取指标权重 w_i ;

③ 计算感知数据量化分数: 最后计算基于感知数据的量化分数, 为各指标参数的加权和, 即

$$score_{W_j|T_k} = \sum_{i=1}^4 w_i \delta_i;$$

(2) 工作者服务质量综合评分

本文设定工作者完成一次任务, 众包人会进行打分 $score_{W_j|S_i}$ 。但是众包人直接评定的分数很容易受人主观感情的影响, 不能完全客观地反应当前工作者的真实表现。因此, 工作者完成本次任务的综合评分为感知数据量化评分 $score_{W_j|T_k}$ 与众包人打分 $score_{W_j|S_i}$ 的加权和, 即

$$score'_{W_j|T_k} = \sigma score_{W_j|T_k} + (1 - \sigma) score_{W_j|S_i} \quad (5)$$

其中, $\sigma \in (0, 1)$ 为权重调节参数, 实际应用中根据具体任务性质及众包人公信度确定。

(3) 引入时间影响因子的工作者综合评分

工作者完成 N 个任务的综合评分受历史任务完成情况影响, 且近期服务质量更能反映工作者当前的服务水平, 因此, 引入时间影响因子, 定义综合评分公式如下:

$$score_{W_j} = \frac{\sum_{k=1}^N \lambda^{N-k} score'_{W_j|T_k}}{\sum_{k=1}^N \lambda^{N-k}} \quad (6)$$

其中, $\lambda \in (0, 1)$ 为时间影响因子, $k \in [1, N]$ 为任务执行数。 k 越大代表执行的任务时间离当时时间越近,

为近期执行任务, λ^{N-k} 越大, 任务评分影响越大。

以上所提工作者服务质量评分算法是基于工作者历史任务完成情况进行的评分, 是对工作者历史表现的评价, 基于历史评价进行任务分配和报酬发放的众包系统有可能面临 On-off 攻击, 即存在某些工作者工作历史表现一直比较优秀, 当获得较高工作者服务质量评分后, 在执行某次任务时发起恶意攻击, 以获利非法利益。为避免此问题, 需要对发起 On-off 攻击的行为进行惩罚。参考目前常见的抗 On-off 攻击评价机制^[27,28], 本文设计了考虑抗 On-off 攻击的服务质量评分更新机制, 如下所示。

$$\Delta s = \max(score_{W_j}) - \min(score_{W_j}) \quad (7)$$

$\max(score_{W_j})$ 为 W_j 获得的服务质量历史评分最大

大值, $\min(score_{W_j})$ 为服务质量历史评分最小值。设置服务质量评分变动阈值 $\Delta s_{threshold}$ 。若 $\Delta s > \Delta s_{threshold}$, 则判定该节点为 On-off 攻击节点, 在一定时间周期 τ 内不允许该类节点继续参与众包, 并将该类节点的信息评分重置为 0.5。

On-off 攻击节点在一定时间内无法获得工作机会, 且在 τ 时间后为获取工作机会, 需要更加诚实、努力工作以重新积累较高的服务质量评分。根据实际应用场景确定 $\Delta s_{threshold}$ 和 τ 的取值。

4.5.1.3 工作者服务质量评分预估

上节提出了基于工作者 W_j 的 k 次历史任务完成情况和众包人评分的服务质量评分算法。基于以上评分, 采用自回归模型^[29], 预测 W_j 执行 $k+1$ 次任务的服务质量。

$$score_{W_j}^{k+1} = c + \frac{\sum_{i=1}^k \gamma^{k-i} score_{W_j|T_i}}{\sum_{i=1}^k \gamma^{k-i}} + \varepsilon_i \quad (8)$$

其中, c 为评分调整因子, 可根据实际应用场景进行调优。 $\gamma \in (0, 1)$ 为历史评分的权重。 ε_i 为均值为 0, 标准差为 σ 的随机误差, σ 对任何 k 均保持不变。

分析公式(8)可知, 任务 T_i 越接近当前任务 T_k , 服务质量评分的权重 γ^{k-i} 越大, 这也符合本文 4.5.1.2(3)引入时间影响因子的工作者综合评分的设计思想。基于预测的 $k+1$ 次任务的服务质量评分可为 4.3 节的任务分配提供依据。

4.5.2 基于服务质量的报酬发放方案

一个优越的群智感知激励机制对调动工作者积极性、提高任务完成质量至关重要。

当前, 群智感知激励机制分为外在激励机制和内在激励机制, 外在激励机制包括经济物质激励和外界条件激励, 内在激励机制包括自我成就满足、兴趣动机激励、社交激励等^[30]。一个有效的内在激励机制比外在激励更持久, 但是内在激励的建立受任务性质、工作者心理等因素影响, 有时还需要工作者与众包人长期合作建立良好关系。相关激励实验^[31]表明: 在单次众包任务执行过程中, 实际物质报酬的外在激励比通过累加虚拟积分增加成就感的内在激励吸引更多的工作者作出贡献。

本文重点讨论外在激励机制, 即通过发放物质报酬的方式激励工作者。外在激励机制又可分为信誉机制和非信誉机制。非信誉机制大多为互惠机制, 采用等价交换原则分配报酬^[24]; 信誉机制通过量化信誉值分配报酬, 可使较高信誉值的工作者获利更多额外的奖励, 激励其提供更优质的服务。

基于以上分析, 本文设计了基于工作者服务质量的基本报酬+奖励金的报酬分配方法, 属于信誉激励机制, 对提供高质量服务的工作者提供更多奖励, 从而激励工作者努力工作, 保证众包完成的质量。

激励算法如下所示:

$$\text{coin}'_{w_j} = \begin{cases} \text{coin}_{w_j} + \frac{\text{score}'_{w_j} - 0.5}{\sum_{j=1}^m (\text{score}'_{w_j} - 0.5)} \times \text{coin}''_{w_j}, & \text{score}'_{w_j} > 0.5 \\ \text{coin}_{w_j}, & \text{score}'_{w_j} < 0.5 \end{cases} \quad (9)$$

其中, coin'_{w_j} 为最终得到的报酬; coin_{w_j} 为任务分配阶段工作者提出的基本工作报酬要求; score'_{w_j} 为将 4.5.1 节计算获得的工作者综合评分 score_{w_j} 标准化为 $[0, 1]$ 的值; coin''_{w_j} 为众包人预存的除支付基本报酬外剩余的押金。

通过公式(9)可知, 只要工作者认真工作, 获得高于 0.5 的标准化服务评分, 即可获得高于基本报酬的奖励, 评分越高, 获得的报酬越高。

4.5.3 工作质量评定及报酬发放

工作质量评定及报酬发放的具体分为 4 个阶段:

(1) 工作者服务质量评分: 选取有效的感知数据和众包人评分, 根据 4.5.1 节定义的工作者服务质量评分算法计算工作者质量分数;

(2) 制定报酬分配方案: 根据 4.5.2 节提出的激励算法, 确定各工作者应获得的报酬;

(3) 报酬发放: 云平台将报酬信息同步给区块链网络, 实际发报报酬;

(4) 数据更新: 更新工作者服务质量评分 score_{w_j} 、众包人和工作者钱包。

感知数据收集的主要过程参见算法 6。

Algorithm 6: Perceptual Data Collection

Input: $\text{state}(W_{j|T_k})$

Output: coin'_{w_j}

```

1: For  $T_k, W_j (0 < k < n, 0 < j < m)$  Do
2:   If  $\text{true} == T_k.\text{getstate}(\text{completed})$  Then
3:      $\text{get}(\text{state}(W_{j|T_k}))$ ;
4:      $\text{score}_{w_j} = \text{func}(\text{state}(W_{j|T_k}))$ ;
5:      $\text{coin}'_{w_j} = \text{func}(\text{score}_{w_j}, \text{coin}_{w_j}, \text{coin}'_{w_j})$ ;
6:      $\text{sync}(\text{coin}'_{w_j})$ ;
7:      $\text{pay}(\text{coin}'_{w_j})$ ;
8:   Else
9:     goto Final;
10:  End If
11:   $\text{update}(\text{score}_{w_j}, \text{wallet}_{w_j}, \text{wallet}_{S_i})$ ;
12: End For
13: Final
14: return  $\text{coin}'_{w_j}$ 

```

5 安全性分析

为了说明本文所提的区块链众包机制的安全性, 本章从系统的抗攻击能力、共识算法的安全性、服务质量评分算法的正确性三个方面进行分析。

5.1 抗攻击能力分析

传统的集中式众包系统易受到 DoS 和 Sybil 攻击, 分布式众包系统面临的常见攻击包括恶意节点攻击、重放攻击、节点捕获攻击、假冒攻击、中间人攻击等。针对以上集中式众包和分布式众包易受到的典型攻击行为, 分析本文所提区块链众包机制的抗攻击能力。

5.1.1 抵抗恶意节点攻击

恶意节点攻击是指区块链网络中的节点向其余节点发送错误的信息, 进而影响交易的顺利执行。在本文所提众包方案中主要存在 2 类恶意节点攻击行为: (1) 在任务分配阶段, 虚假或恶意节点发送错误

的任务发布信息 $T_k = (m_k, t_k, score_k)$, 会直接影响参与众包的工作者的公平竞争和任务的分配, 导致任务无法有效执行; (2) 在感知数据收集阶段, 恶意节点有可能发送虚假的感知信息 $state(W_{j|T_k}) = func(T_k.state, \Delta T_{W_j}, \Delta T_{W_j|T_k.begin}, \alpha_{W_j|T_k}, score_{W_j|S_t})$, 从而计算得到错误的节点服务质量评分, 不仅会使得工作者不能得到合理的报酬, 还会影响工作者竞争到下一次任务的机会。

假设恶意设备 W_{bad} 注入到系统中, 不管在任务分配阶段还是感知数据收集阶段的共识过程中, W_{bad} 都无法提供正确的共识结果。在任务发布阶段, 本文提出的共识算法依据设备标识 ID 会筛选出与最终共识结果不一致的节点即拜占庭节点 W_{bad} , 其会被抛弃不再具有参与任务竞争与分配的机会, 进而不会影响交易最终信息的确认。在感知数据收集阶段, W_{bad} 提供的错误的信息与共识结果矛盾, 很容易发现该恶意节点, 进而遏制其攻击行为。

5.1.2 抵抗 Sybil 攻击

Sybil 攻击是指网络中少量攻击节点伪造模仿多个系统中的合法身份, 以控制网络中大部分节点, 削弱区块链这种通过多个节点保存的冗余数据保证网络数据安全和不可篡改的作用。

用户节点在加入区块链系统前都必须进行注册, 获取唯一标识 ID_U , 并根据 ID_U 生成用户的公、私钥 (PK_U, SK_U) 。每次有新的工作任务, 系统都会重新计算更新用户的公、私钥。注册信息保证了用户身份的唯一, 注册信息验证不通过的用户无法加入区块链, 从而保证节点不可能伪造多重身份加入区块链系统中。

5.1.3 抵抗假冒攻击

假冒攻击是指攻击者截获网络中的通信信息去破解用户密钥, 进而假冒合法用户进行欺诈。本文基于 RSA 计算得到密钥, 基于大质数乘积难以逆向求解, 运算复杂度高, 攻击者很难通过窃听的公钥去计算节点的私钥, 无法假冒合法用户 U 。

5.1.4 抵抗节点捕获攻击

节点捕获攻击是指攻击者通过强大的技术能力或其他途径, 捕获到部分合法节点的身份信息及密钥信息, 进而入侵网络中更多的通信链路, 攻陷整个网络。假设攻击者已获取某些设备节点 U 的私密信息, 但是每个 U 节点都有基于各自 ID_U 和身份信息计算得到的公、私钥 (PK_U, SK_U) , 每个用户的会话密钥也各不相同, 且每次发布新的任务密钥都会

更新。因此, 攻击者很难通过捕获的少量合法节点信息去攻陷更多的网络链路。

5.1.5 抵抗重放攻击

重放攻击是指攻击者将窃听到的成功验证通过的信息重复发给验证者, 以获取更多的利益。本文所提众包方案中节点间的每一次交易信息都包含用户的唯一标识 ID_U 、时间信息等, 并进行哈希运算保证信息不被非法篡改。每一次新的交易上述信息都会发生变化, 攻击者的重放攻击行为极易被发现。

5.1.6 抵抗中间人攻击

中间人攻击是指攻击者通过窃听网络, 拦截并篡改网络通信数据的行为。本文采用私钥对通信数据加密, 即使中间人获得了节点之间的通信信息, 也不会截获解密到私密信息。如果中间人篡改了通信信息, 对方收到篡改信息后无法利用相应的公钥解密, 从而发现攻击行为。

5.1.7 抵抗 DoS 攻击

DoS 攻击是指攻击者通过向服务器发送合法请求, 占用服务器绝大多数服务资源, 进而影响其他用户无法得到相应服务。本文提出的众包方案中, 众包人和工作者直接在区块链网络中完成用户信息注册、众包任务的发布、分配、感知数据的收集、报酬的实际发放, 不需要第三方服务器, 可有效避免 DoS 攻击。交易信息存储在区块链分布式账本中, 仅在交易完成后向云平台服务器同步信息。云服务器主要负责复杂度较高的服务质量评分计算, 实时性要求不高, 且不会影响众包的核心业务流程。

5.2 共识算法的安全性分析

本文采用基于 PBFT 的共识算法进行众包交易信息的同步, 继承了经典 PBFT 算法的容错性, 同时通过选取服务质量评分较高的用户节点作为主节点, 一定程度上提高了主节点的可靠性。因此, 本文所提众包共识算法的安全性主要体现在一致性和可靠性两个方面。

5.2.1 一致性

共识的一致性指的是共识不会分叉。在本文所提的基于 PBFT 的众包共识机制中, 若超过全网 $2/3$ 的节点计算得到一致性结果, 则形成对一组计算数据的共识。在一轮共识中不会出现两个不同的共识结果。

证明: 假设区块链网络中用户节点总数为 $N = 3f + 1$, 则网络中最多有 f 个拜占庭节点。假设网络中的节点 U_1 接收到共识结果 A , U_2 接收到另一个不一致的共识结果 B , 则至少全网 $2/3$ 的节点即 $2f + 1$ 个节点计算得到共识结果 A , 同时至少

$2f+1$ 个节点计算得到共识结果 B 。因此, 至少有 $2f+1+2f+1-3f-1=f+1$ 个节点计算出两个不同的共识结果。得到两个不一致共识结果的节点定义为拜占庭节点, 与前提条件网络中最多有 f 个拜占庭节点矛盾。因此假设不成立, 不会出现超过全网 $2/3$ 的节点计算得出两个不同共识结果的情况, 即共识具有一致性。

5.2.2 可靠性

众包过程中交易共识的安全性主要受两个方面的影响: (1)主节点的可靠性; (2)参与共识的用户节点的安全性。

主节点可靠性保证。共识过程中选取上一轮任务的用户服务质量评分较高的节点 $W_{j|max(score)}$ 作为主节点, 负责发起共识和打包区块。为了竞选成为共识的主节点, 以获得更多服务机会和报酬, 节点只有在新一轮共识中表现诚实、优秀, 有效地生成区块, 完成交易的同步, 才可能获得较高的服务质量评分。如果主节点在一轮共识期间没有生成有效的数据块, 或者甚至恶意篡改了数据和其他不诚实行为, 或者主节点产生的数据块未经表决节点的批准, 则该节点的服务质量评分将下降, 不太可能被下一轮共识选中, 该节点将失去生产区块的机会, 进而影响工作竞争能力和报酬的获取。

共识运算的用户节点安全性保证。在用户注册阶段对节点进行编号, 在任务发布阶段的众包共识算法, 可根据编号确认发出共识结果与最终形成的共识一致的节点, 即非拜占庭节点参与工作的竞争, 如果这类节点竞争到任务, 一定程度上可确保网络事务的安全性, 为众包人提供可靠的服务。随着工作需求的变化, 新的任务会启动新的共识计算和可参与任务竞争的可信工作者的筛选, 以保证每次交易中工作者的安全性。在任务分配阶段, 服务质量评分保证只有符合众包人要求的服务质量评分的工作者才可能被分配到任务, 进而参与感知数据收集阶段的共识, 进一步确保了任务完成的质量和共识算法的安全运行。

5.3 服务质量评价算法的正确性分析

工作者服务质量评分的目的是为区块链分布式众包环境下工作者竞争任务和发放报酬提供合理、公平、科学的依据, 进而鼓励用户更诚实、更努力地工作。为了验证算法的有效性, 本节分析 3 种类型的工作者参与众包的情况: (1) 工作能力强但业务繁忙的工作者; (2) 与众包人关系“好”或“坏”的工作

者; (3) 历史表现较差但近期工作能力和工作条件得到提升的工作者。

(1) 工作能力强但业务繁忙的工作者

对于这类工作者, 虽然其工作能力强, 但由于其工作众多, 有可能耽误竞争到任务的时间进度, 因此这类工作者即相应的服务质量评分应降低, 分配到任务的机会减少。

假设工作者 W_j 的服务质量指标参数 $\delta = (R_{s|W_j}, \overline{\Delta T_{W_j}}, \overline{\Delta T_{W_j|T_k.begin}}^{-1}, \beta_{W_j}^{-1})$ 。根据熵值法, 其感知数据量化得分 $score_{W_j|T_k} = \sum_{i=1}^4 w_i \delta$ 。如果 W_j 工作能力强(历史任务完成率为 $R_{s|W_j}$ 高)、任务完成快(即历史任务超前完成时间差均值为 $\overline{\Delta T_{W_j}}$), 但在某一阶段由于任务众多, 导致任务延迟执行情况比较严重, 则 $\overline{\Delta T_{W_j|T_k.begin}}$ 增大, $\overline{\Delta T_{W_j|T_k.begin}}^{-1}$ 降低, $score_{W_j|T_k} = \sum_{i=1}^4 w_i \delta$ 降低, 其总的服务质量评分会降低, 竞争力降低, 分配到任务的机会减少。

(2) 与众包人关系“好”或“坏”的工作者

对于这类竞争者, 在区块链系统这种根据算法和规则“自动”分配任务的环境中, 其工作能力应得到充分体现, 其竞争到任务的机会不会完全受制于众包人的态度。

假设工作者 W_j 的感知数据量化得分 $score_{W_j|T_k} = \sum_{i=1}^4 w_i \delta$, 众包人打分为 $score_{W_j|S_i}$, 则工作者完成本次任务的评分为 $score'_{W_j|T_k} = \sigma score_{W_j|T_k} + (1-\sigma) score_{W_j|S_i}$ 。其中, $\sigma \in (0,1)$ 为权重调节参数。由于众包人的评分带有极强的主观色彩, 实际应用中, 根据众包人公信度调节 σ 取值。对于众包人关系“好”或“坏”的工作者评分, 可适当调低 σ 取值, 以降低众包人主观因素对工作者实际服务能力评价的影响。

(3) 历史表现较差但近期工作能力和工作条件得到提升的工作者

对于这类工作者, 其近期服务能力得到提升, 其服务质量评分应该得到显著增加, 竞争力提高, 分配任务的机会增多。

假设工作者 W_j 完成本次任务的评分为 $score'_{W_j|T_k} = \sigma score_{W_j|T_k} + (1-\sigma) score_{W_j|S_i}$, 其最终获得的综合服务质量评分为 $score_{W_j} =$

$$\frac{\sum_{k=1}^N \lambda^{N-k} score'_{w_j|T_k}}{\sum_{k=1}^N \lambda^{N-k}}。由于 0 < \lambda < 1, 越接近当前$$

前时间的任务 k 越大, $N-k$ 越小, λ^{N-k} 越大, 对综合服务质量评分的影响越大, 距离当前时间较远的任务完成质量对评分影响较小。如果工作者 w_j 近期服务能力得到提升, 其综合服务质量评分会得到显著增加, 竞争到任务的机会随之增加。

6 性能分析

本章从共识算法的性能和多任务多用户条件下众包的质量及效率验证本文所提的区块链众包机制的实用性。

为分析区块链众包机制的实用性, 本文在 DELL Precision 3550 工作站笔记本上搭建 Hyperledger Fabric 环境, 操作系统为 ubuntu16.04, 安装 docker, 模拟区块链多节点环境, 基于 go 语言编写仿真系统。笔记本配置为酷睿 Core i7 处理器, 8G 内存。

6.1 共识算法仿真与性能分析

实验设定网络中节点数目分别为 10、20、30、40、50、60、70、80、90、100, 对本文所提众包 PBFT、PBFT、dBFT^[32]进行共识消耗时间的观测。如图 3 所示, PBFT 共识需要节点大量反复的交易确认才能完成共识, 且主节点在通信复杂度增加时, 易出错或发生宕机现象; dBFT 引入投票机制, 采用基于持有权益的比例来投票决定记账节点, 在通信时延上较 PBFT 有了较大改进, 但缺点是共识的不稳定性, 当超过三分之一的记账节点不能提供正常服务时, 整个网络则无法正常工作。本文提出的众包 PBFT 机制, 选择服务质量评分高的节点作为主节点, 节省了通过算法选择主节点的过程; 同时过滤发出的验证结果与最终共识结果不一致的拜占庭节点不参与下一轮的共识与任务分配, 促使网络越来越可靠。通过实验仿真发现, 本文提出的众包 PBFT 算法具有更低的共识延迟, 共识稳定性更好。

需要说明的是, 由于节点服务质量评分运算在链下由云平台服务器完成, 本节的仿真是在已计算并设置完成节点服务质量评分前提下进行的, 仅包括发起共识请求到达到一致共识的共识运算过程。

6.2 众包质量及效率分析

本节从众包任务分配的工作者服务质量、众包任务分配效率、任务完成率、任务完成时间等方面对本文所提基于工作者服务质量的区块链众包机制

的有效性和可用性进行分析。实验假设所有参与竞争的工作者皆满足实验设定的所有任务提出的最低服务质量评分要求、基本报酬要求和任务执行时间要求。

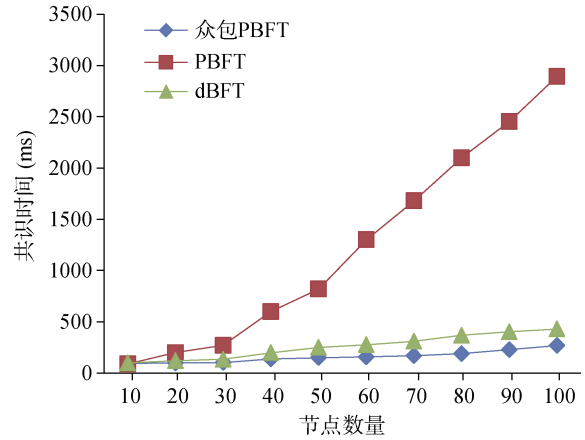


图 4 共识消耗时间比较

Figure 4 Comparison of Consensus Time

6.2.1 众包质量分析

设定系统中共有 10 个任务, 分别有 15、20、25、30、35、40、45、50、55、60 个工作者参与任务的竞争, 平均历史服务质量评分分别为 0.66、0.73、0.82、0.83、0.80、0.79、0.82、0.83、0.78、0.72。比较本文所提的基于服务质量评分的区块链众包机制与不筛选高服务质量评分用户承担任务的区块链众包机制, 在不同数量工作者参与竞争任务条件下算法各运行 10 次, 计算获得任务分配的工作者服务质量平均分。

通过仿真发现, 在不筛选高服务质量评分用户承担任务的区块链众包机制中, 任务随机分配给竞争者, 无法保证高评分工作者分配到任务, 分配到任务的工作者平均历史服务质量评分有时甚至低于所有参加竞争的工作者历史评分。而本文提出的基于服务质量评分的区块链众包机制使得高历史服务质量评分的用户优先分配到任务, 一定程度上可保证任务完成的质量。

6.2.2 众包效率分析

设定系统分别发布 10、15、20、25、30、35、40、45、50、55 个任务, 共有 100 个用户参与任务竞争。比较本文所提的基于服务质量评分的区块链众包机制与不筛选高服务质量评分用户承担任务的区块链众包机制, 在不同数量任务发布条件下在任务分配阶段完成任务分配所需的时间, 以及获得任务分配的工作者服务质量平均分。

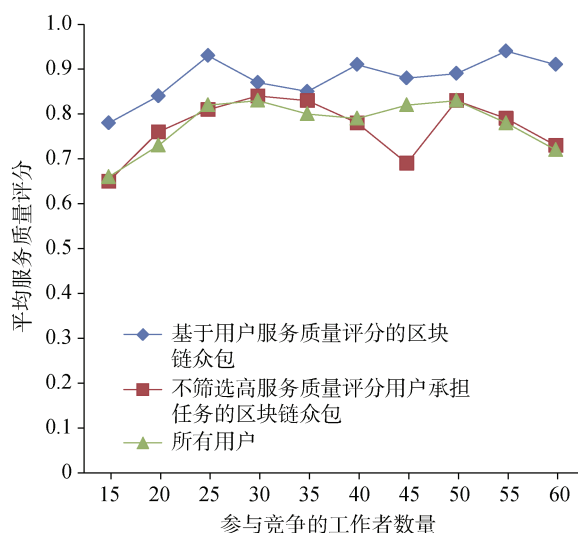


图5 不同数量工作者竞争条件下平均服务质量评分
Figure 5 Comparison of Average Service Quality Score under Different Number of Workers

如图6、图7所示, 基于服务质量评分的区块链众包机制分配任务时间虽然增加了筛选高质量服务评分的过程, 但 $sort(W_j, score_{W_j})$ 采用快速排序法, 计算复杂度不高, 通过仿真发现其任务分配时间与不筛选高服务质量评分用户承担任务的区块链众包很接近, 没有明显多余的时间消耗, 都为毫秒级, 但分配到任务的工作者平均服务质量评分会得到显著提高, 具有较强的实用性。

6.2.3 众包可用性分析

为了验证本文方案在实际环境中的可用性, 本文从 gMission^[33]众包平台上获取包括任务检测信息和工作者感知信息等实验记录, 在此数据基础上增加了服务质量评分的设置。在本组实验中通过改变发布的众包任务数量, 对比本文所提基于服务质量的区块链众包机制与不筛选高服务质量评分用户承担任务的区块链众包机制, 在任务完成率、任务完成时间、竞争到任务的工作者信誉平均分等方面的表现。

分析图8、图9、图10和图11可知, 随着发布任务数的增加, 参与竞争的工作者数量也在增加, 本文所提方案下任务完成率和竞争到任务的工作者服务质量分值始终维持在一个较高的水平。同时, 由于方案选择了更优秀的服务者承担任务, 平均任务完成时间也得到了缩减, 提高了任务完成效率。

7 总结

为解决传统众包面临的单点故障、隐私泄漏和工作者参与积极性低的问题, 本文提出了一种基于

服务者工作质量的区块链众包机制, 描述了众包各环节运行的算法; 为提高众包过程中任务发布及感知数据收集信息的共识效率, 研究了基于PBFT的众

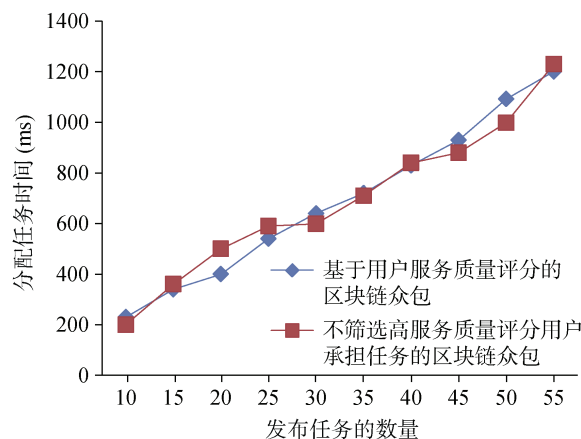


图6 不同数量任务条件下分配任务时间
Figure 6 Comparison of Task Allocation Time under Different Number of Tasks

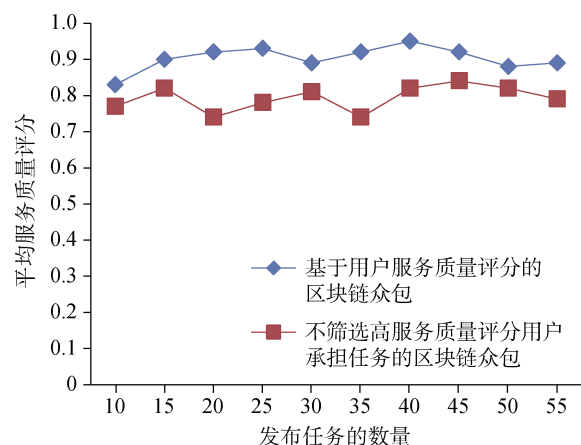


图7 不同数量任务条件下平均服务质量评分
Figure 7 Comparison of Average Service Quality Score under Different Number of Tasks

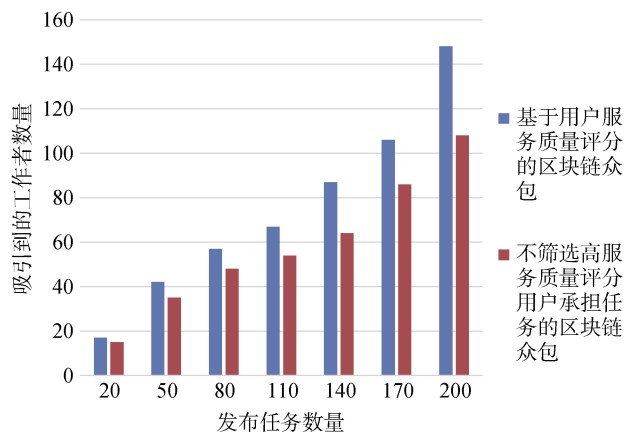


图8 不同数量任务条件下吸引到的工作者数量
Figure 8 Number of Workers under Different Number of Tasks

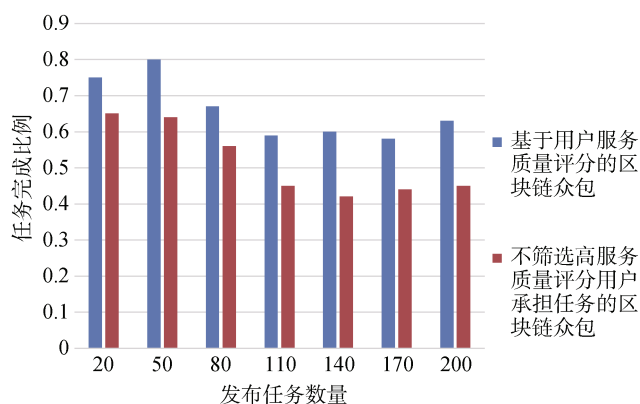


图 9 不同数量任务条件下任务完成率

Figure 9 Task Completion Rate under Different Number of Tasks

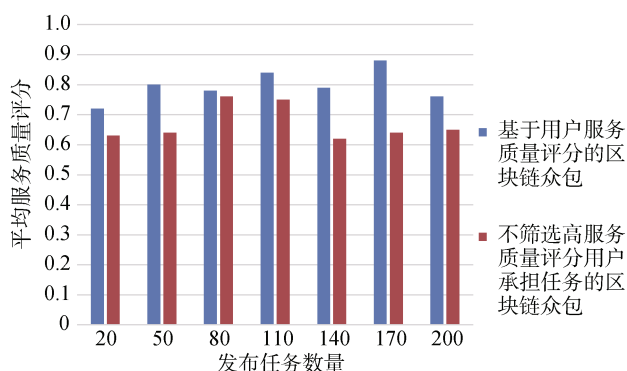


图 10 不同数量任务条件下平均服务质量评分

Figure 10 Average Service Quality Score under Different Number of Tasks

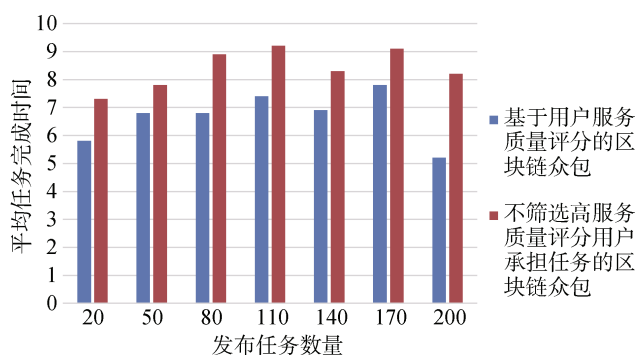


图 11 不同数量任务条件下平均任务完成时间

Figure 11 Average Task Completion Time under Different Number of Tasks

包共识机制; 为提高任务完成质量, 提高工作者服务积极性, 设计了服务质量评分算法和报酬发放机制。最后, 从系统的抗攻击能力、共识算法的安全性、服务质量评分算法的有效性三个方面进行了安全性分析, 并在 Hyperledger Fabric 环境上进行了实验仿真, 验证了本文所提区块链众包机制的实用性。

当前仍处于区块链技术应用落地的探索阶段,

未来仍有很多有意义的工作。众包场景可能更为复杂, 影响工作者服务质量评价的因素更为多样, 因此结合不同的应用需求, 提供有效合理的服务质量评估机制和众包方案是需要持续研究的问题。

参考文献

- [1] Yang D J, Xue G L, Fang X, et al. Incentive Mechanisms for Crowdsensing: Crowdsourcing with Smartphones[J]. *IEEE/ACM Transactions on Networking*, 2016, 24(3): 1732-1744.
- [2] Han K, Zhang C, Luo J, et al. Truthful Scheduling Mechanisms for Powering Mobile Crowdsensing[J]. *IEEE Transactions on Computers*, 2016, 65(1): 294-307.
- [3] Gisdakis S, Giannetos T, Papadimitratos P. Security, Privacy, and Incentive Provision for Mobile Crowd Sensing Systems[J]. *IEEE Internet of Things Journal*, 2016, 3(5): 839-853.
- [4] Liu J W, Shen H Y, Zhang X. A Survey of Mobile Crowdsensing Techniques: A Critical Component for the Internet of Things[C]. *2016 25th International Conference on Computer Communication and Networks*, 2016: 1-6.
- [5] Luo P Y, Zhu Y M, Peng J, et al. A Distributed Auction Approach to Crowdsourced Sensing over Smartphones[C]. *2016 IEEE 22nd International Conference on Parallel and Distributed Systems*, 2017: 1-7.
- [6] Pouryazdan M, Fiandrino C, Kantarci B, et al. Game-Theoretic Recruitment of Sensing Service Providers for Trustworthy Cloud-Centric Internet-of-Things (IoT) Applications[C]. *2016 IEEE Globecom Workshops*, 2017: 1-6.
- [7] Mei C. *The design and implementation of iot security platform based on block chain*[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
(梅晨. 基于区块链的物联网安全平台的设计与实现[D]. 北京: 北京邮电大学, 2018.)
- [8] Skarmeta A F, Hernández-Ramos J L, Moreno M V. A Decentralized Approach for Security and Privacy Challenges in the Internet of Things[C]. *2014 IEEE World Forum on Internet of Things*, 2014: 67-72.
- [9] Xu X L, Liu Q X, Zhang X Y, et al. A Blockchain-Powered Crowdsourcing Method with Privacy Preservation in Mobile Environment[J]. *IEEE Transactions on Computational Social Systems*, 2019, 6(6): 1407-1419.
- [10] Kogias D G, Leligou H C, Xevgenis M, et al. Toward a Blockchain-Enabled Crowdsourcing Platform[J]. *IT Professional*, 2019, 21(5): 18-25.
- [11] Sun Jianguo, Wang Jiaxiang, Yin Guisheng. Overview of network situation awareness technology[J]. *Secrecy Science and Technology*, 2016(4): 17-19.
- [12] Wang W B, Hoang D T, Hu P Z, et al. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks[J]. *IEEE Access*, 2019, 7: 22328-22370.
- [13] Zhao K, Xing Y H. Security Survey of Internet of Things Driven by Block Chain Technology[J]. *Netinfo Security*, 2017(5): 1-6.
(赵阔, 邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. *信息网络安全*, 2017(5): 1-6.)

- [14] Shen X, Pei Q Q, Liu X F. Survey of Block Chain[J]. *Chinese Journal of Network and Information Security*, 2016, 2(11): 11-20.
(沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. *网络与信息安全学报*, 2016, 2(11): 11-20.)
- [15] Yao Y Y, Chang X L, Zhen P. Decentralized Identity Authentication and Key Management Scheme Based on Blockchain[J]. *Cyber-space Security*, 2019, 10(6): 33-39.
(姚英英, 常晓林, 甄平. 基于区块链的去中心化身份认证及密钥管理方案[J]. *网络空间安全*, 2019, 10(6): 33-39.)
- [16] Kshetri N. Can Blockchain Strengthen the Internet of Things?[J]. *IT Professional*, 2017, 19(4): 68-72.
- [17] Kiayias A, Russell A, David B, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol[C]. *Annual International Cryptology Conference*, 2017: 357-388.
- [18] Singh S, Ra I H, Meng W Z, et al. SH-BlockCC: A Secure and Efficient Internet of Things Smart Home Architecture Based on Cloud Computing and Blockchain Technology[J]. *International Journal of Distributed Sensor Networks*, 2019, 15(4): 155014771984415.
- [19] Castro M, Liskov B. Practical Byzantine Fault Tolerance and Proactive Recovery[J]. *ACM Transactions on Computer Systems*, 20(4): 398-461.
- [20] Wang K, Qi X, Shu L, et al. Toward Trustworthy Crowdsourcing in the Social Internet of Things[J]. *IEEE Wireless Communications*, 2016, 23(5): 30-36.
- [21] Liang B M, Liu W J, Sun L, et al. An Aggregated Model for Energy Management Considering Crowdsourcing Behaviors of Distributed Energy Resources[J]. *IEEE Access*, 2019, 7: 145757-145766.
- [22] Li M, Weng J, Yang A J, et al. CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2019, 30(6): 1251-1266.
- [23] Huang S M. *Crowdsourcing process design and consensus algorithm analysis for blockchain Internet of Things*[D]. Chongqing: Chongqing University of Posts and Telecommunications, 2020.
(黄守明. 面向区块链物联网的众包流程设计及其共识算法分析研究[D]. 重庆: 重庆邮电大学, 2020.)
- [24] He Y H, Li M R, Li H, et al. A Blockchain Based Incentive Mechanism for Crowdsensing Applications[J]. *Journal of Computer Research and Development*, 2019, 56(3): 544-554.
(何云华, 李梦茹, 李红, 等. 群智感知应用中基于区块链的激励机制[J]. *计算机研究与发展*, 2019, 56(3): 544-554.)
- [25] Alswailim M A, Hassanein H S, Zulkernine M. A Reputation System to Evaluate Participants for Participatory Sensing[C]. *2016 IEEE Global Communications Conference*, 2017: 1-6.
- [26] Wang Z Y. *Research on blockchain technology applied to smart home information security*[D]. Wuhan: Huazhong University of Science and Technology, 2019.
(王泽远. 应用于智能家居信息安全的区块链技术研究[D]. 武汉: 华中科技大学, 2019.)
- [27] Zhang G H, Yang Y H, Pang S B, et al. Adaptive Security Mechanism for Defending On-off Attack Based on Trust in Internet of Things[J]. *Journal of Computer Applications*, 2018, 38(3): 682-687.
(张光华, 杨耀红, 庞少博, 等. 物联网中基于信任抗 On-off 攻击的自适应安全机制[J]. *计算机应用*, 2018, 38(3): 682-687.)
- [28] Zhang C, Zhu L H, Xu C, et al. TPRR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET[C]. *IEEE Transactions on Services Computing*, 2019: 806-818.
- [29] Gao J M, Guo P P. An Empirical Study of GDP Forecast Based on the Auto-Regressive XGBoost Time Series Model[J]. *Mathematics in Practice and Theory*, 2021, 51(7): 9-16.
(高金敏, 郭佩佩. 基于自回归 XGBoost 时序模型的 GDP 预测实证[J]. *数学的实践与认识*, 2021, 51(7): 9-16.)
- [30] Wang J, Wang L Q, Ma W Q, et al. Survey on Incentive Mechanisms for Crowd-Based Cooperative Computing[J]. *Computer Engineering and Applications*, 2020, 56(6): 1-9.
(王娟, 王丽清, 马文倩, 等. 群智协同激励机制研究综述[J]. *计算机工程与应用*, 2020, 56(6): 1-9.)
- [31] Liu C. Experimental Incentive Mechanisms for Crowd Sensing[J]. *ZTE Technology Journal*, 2015, 21(6): 10-13.
(刘驰. 群智感知中激励机制实验综述及展望[J]. *中兴通讯技术*, 2015, 21(6): 10-13.)
- [32] Li Y N. *Research on data storage application based on blockchain*[D]. Beijing: Beijing Jiaotong University, 2018.
(李亚楠. 基于区块链的数据存储应用研究[D]. 北京: 北京交通大学, 2018.)
- [33] CHEN Z, FU R, ZHAO Z, et al. gMission: a general spatial crowdsourcing platform[J]. *Proceedings of the Very Large Data Base Endowment*, 2014, 7(13): 1629-1632.



张珠君 于 2012 年在北京交通大学通信与信息系统专业获得硕士学位。现在中国科学院大学网络空间安全专业攻读博士学位。现任中国科学院信息工程研究所工程师。研究领域为物联网安全。研究兴趣包括: 区块链技术。Email: zhangzhujun@iie.ac.cn



朱大立 于 2007 年在华中科技大学计算机应用技术专业获得博士学位。现任中国科学院信息工程研究所第四研究室正高级工程师。研究领域为移动互联网安全。研究兴趣包括: 安全智能终端、区块链技术。Email: zhudali@iie.ac.cn



范伟 于 2018 年在中国科学院大学网络空间安全专业获得博士学位。现在中国科学院大学网络空间安全专业攻读博士学位。任中国科学院信息工程研究所高级工程师。研究领域为云计算与大数据安全。研究兴趣包括: 区块链技术。Email: fanwei@iie.ac.cn



弥宝鑫 于 2012 年在北京交通大学电子与通信工程专业获得硕士学位。现任中国科学院信息工程研究所第四研究室工程师。研究领域为移动互联网安全、无线通信安全。研究兴趣包括: 智能终端安全研究、WLAN 通信安全。Email: mibaoxin@iie.ac.cn



彭诚 于 2017 年在北京工业大学电子信息工程专业获得工学学士学位。现在中国科学院大学信号与信息处理专业攻读博士学位。研究领域为移动通信, 通信协议分析, 微弱信号检测与识别等。Email: pengcheng@iie.ac.cn