•物联网•

DOI:10.15961/j.jsuese.202000780

本刊网刊

# 基于区块链的分布式激励架构研究

何云华[1,2,3], 黄　伟[4], 王伟忠[2*], 张　翠[1], 李　红[3], 孙利民[3]

(1.北方工业大学 信息学院, 北京 100144; 2.中国工业互联网研究院, 北京 100102; 3.中国科学院信息工程研究所 物联网安全北京市重点实验室, 北京 100093; 4.国家工业信息安全发展研究中心, 北京 100040)

**摘　要**:区块链因其去中心化、开放性、不可篡改、匿名性等特征, 被应用于激励机制中解决权威欺骗或信任缺失问题。然而, 现有基于区块链的激励机制设计存在一些设计缺陷或评估缺失等问题。为解决以上问题, 本文提出了一种基于区块链的分布式激励架构, 为激励机制设计提供指导和评估依据。将激励机制视为区块链中的交易, 从付款流向、付款方式、付款金额3方面制定了基于区块链的激励机制的基本需求和额外需求, 包括了贯穿激励交易的整个流程; 并在此基础上设计了场景适配、支付策略、效果评价3阶段的基于区块链的激励机制架构。场景适配阶段通过分析场景的角色关系提取参与方的利益关系, 以适应不同场景的交易验证、报酬流向的差异; 支付策略阶段提供了各类密码货币、定价策略与支付方式的特点及作用, 以指导密码货币的选择、定价机制的设计和付款形式的确定; 效果评价阶段从安全可信、隐私保护、可拓展性等方面分析激励机制的效果, 从而给出较为全面的评估。最后, 利用该架构对群智感知应用实例进行激励机制设计与优化, 评估结果从安全可信、隐私保护、效率提升方面体现出激励设计方案的优化效果, 从而验证本架构的有效性。

**关键词**:激励机制; 区块链; 密码货币; 支付策略; 激励效果

**中图分类号**:TN911.22　　**文献标志码**:A　　**文章编号**:2096-3246(2021)01-0178-10

## Research on Distributed Incentive Architecture Based on Blockchain

*HE Yunhua*[1,2,3], *HUANG Wei*[4], *WANG Weizhong*[2*], *ZHANG Cui*[1], *LI Hong*[3], *SUN Limin*[3]

(1.School of Info. Sci. and Technol., North China Univ. of Technol., Beijing 100144, China; 2.China Academy of Industrial Internet, Beijing 100102, China; 3.Beijing Key Lab. IoT Info. Security Technol., Chinese Academy of Sciences, Beijing 100093, China; 4.National Industrial Info. Security Development Research Center, Beijing 100040, China)

**Abstract**: In order to solve the problem of authority deception or lacking of trust in the incentive mechanisms, the blockchain technology is used due to its decentralization, openness, immutable and anonymity. However, existing incentive mechanisms based on blockchain has design defects or lack of evaluation. To solve the above problems, a distributed incentive architecture based on blockchain was proposed, which can provide guidance and evaluation basis for the design of incentive mechanism. In this architecture, an incentive mechanism was considered as a transaction in the blockchain, and the basic and additional requirements of the incentive mechanisms based on blockchain were formulated from the three aspects of payment flow, payment method and payment amount of the transaction, including the entire process of incentive transactions. Then, a three-stage blockchain-based incentive mechanism framework for scene adaptation, payment strategy, and effect evaluation was designed. In the scene adaptation stage, the interests of the participants were extracted by analyzing the role relationship of the scenario to apply to the difference of transaction verification and payment flow in different scenarios. The payment strategy stage provided the characteristics and functions of various cryptocurrencies, pricing strategies and payment methods to guide the selection of cryptocurrency, the design of pricing strategy and the determination of payment method. The effect evaluation stage was used to analyze the effect of the incentive mechanism from the aspects of

**收稿日期**:2020 – 09 – 10

**基金项目**:国家自然科学基金项目(61802005; 61702503); 北京自然科学基金重点项目(KZ201810009011)

**作者简介**:何云华(1987—), 男, 副教授, 博士. 研究方向: 区块链、物联网安全、工控安全等. E-mail: heyunhua@ncut.edu.cn

* **通信作者**:王伟忠, E-mail: wangweizhong@china-aii.com

**网络出版时间**:2021 – 01 – 13 14 : 44 : 00　　**网络出版地址**:https://kns.cnki.net/kcms/detail/51.1773.TB.20210113.1157.001.html

security and credibility, privacy protection, scalability, etc., so as to give a more comprehensive evaluation. Finally, the architecture was used to design and evaluate the incentive mechanism of the crowdsensing application. The evaluation results show the optimization effect of the incentive design scheme in terms of security and truthfulness, privacy protection, and efficiency improvement, thereby verifying the effectiveness of the architecture.

**Key words**: incentive mechanism; blockchain; cryptocurrency; payment strategy; incentive effect

基于区块链的激励机制是指利用基于区块链的密码货币作为激励手段的激励机制[1]。基于区块链的激励机制利用区块链的去中心化、开放性、不可篡改、匿名性等特性[2–3], 在互不了解的多方间建立可靠的信任关系, 能够解决传统电子货币存在权威欺骗、信任缺失问题, 可以增强系统的安全性和容灾性[4–5]。

目前, 基于区块链的激励机制应用在群智感知、车联网、数据共享等场景已有一些研究[6–8]。区块链作为分布式安全的账本记录了这些应用中的交易, 保证交易的可验证和不可篡改性。然而, 现有基于区块链激励机制设计因缺乏设计原则与架构指导而存在设计缺陷或评估缺失等问题。例如: Jia等[6]提出的群智感知中的位置隐私保护激励机制没有考虑激励的持续性; Li等[7]提出的车联网中的激励机制没有考虑参与区块链的车辆用户和充电提供商的恶意行为; Xuan等[8]提出的数据共享中基于智能合约的激励机制没有考虑共享数据的质量问题。已有一些研究人员提出了激励设计原则[9–10]及区块链相关的架构[11–12]。Yang等[9]从博弈论的角度提出一些激励机制设计原则, 包括计算高效、个体理性、预算平衡、赢利性和可信性, 但只适用于基于博弈模型的定价策略。Zhang等[10]提出了抵抗欺骗、合谋等攻击的安全性原则, 但只适用于基于信誉的激励机制。邵奇峰等[11]提出了区块链技术架构可指导区块链的部署, 但未涉及激励机制设计。徐恪等[12]提出了基于区块链的网络安全体系架构来指导区块链在网络安全方面的应用, 并给出安全激励的设计思路, 但仅考虑了激励机制的安全性。

为此, 本文提出了一种基于区块链的分布式激励架构, 以期规范与指导基于区块链的激励机制的设计。该架构将激励机制视为区块链中的交易, 覆盖了激励交易的全过程, 从交易的付款流向、付款方式、付款金额3个方面制定了基于区块链的激励机制设计的基本需求和额外需求。该架构包括场景适配、支付策略、效果评价3个阶段: 场景适配阶段通过分析场景中的角色关系提取各个参与方之间的利益关系, 以确定交易验证内容、报酬流向、安全薄弱点或隐私泄漏点; 支付策略阶段根据各类密码货币、定价策略与支付方式的特点及作用, 进行选择以满足场景中参与方的利益关系、交易验证和交易流向的支付策略; 效果评价阶段可从安全可信、隐私保护、可扩展性、可持续性和计算高效来分析激励机制是否能够达到对应场景所需求的激励要求。最后, 本文应用该激励架构指导群智感知应用中激励机制实例的设计, 分析并验证该架构的有效性。

## 1　激励机制设计原则

激励机制设计原则用于指导激励机制架构的构建和激励机制的设计。基于区块链的激励机制可被当作参与者之间的一次或多次交易[13], 因此, 可从以下3个问题考虑激励机制设计原则: 1)付钱的流向, 谁给谁付钱; 2)付钱的方式, 怎么付钱效率更高, 选择什么样的付款方式更便捷; 3)付多少钱, 如何设定一个合理的报酬价格。

如图1所示, 本文基于以上问题提出了激励机制的设计需要满足的基本需求: 1)用户之间的利益关系。通过对应用场景的角色分析, 提取和定义应用场景中用户间的利益关系, 如分工关系、验证关系、安全脆弱点、隐私泄漏点等。2)付款方式的安全性, 即如何保证付款过程的安全可靠。依据安全需求不同选择相应的密码货币, 根据场景中的安全脆弱点或隐私泄漏点, 选择或制定不同的付款形式来提升付款过程的安全。3)制定一种合理给予报酬的方案。根据场景中的分工关系、验证工作量等需求, 选择或优化现有的定价策略设定合理的定价机制。

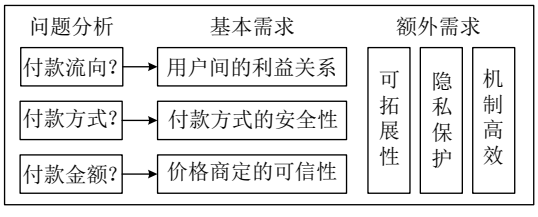


**图 1　激励机制设计原则**

**Fig. 1　Design principles of incentive mechanism**

基于区块链的激励机制的设计除了要满足以上基本需求以外, 还应考虑一些额外的需求: 1)机制的可拓展性保证。激励任务验证的复杂性增加了矿工对交易的验证工作量, 节点数量增加也会导致交易数量激增, 交易的处理数量的增加会超过矿工的处理能力的边际, 因此需要考虑系统的可扩展性。2)隐私保护的需求。用户应在参与交易、任务执行、验证工作过程实现匿名化。矿工可能需要参与、验证交易

信息，即便隐藏信息，也能通过交易中的记录数据、验证过程信息挖掘出参与者私密信息。3）通信计算开销。激励机制中节点之间的交互会增加通信计算开销，隐私保护、安全可信等方法也会增加系统通信计算开销，通信计算开销过大会影响用户体现，因此需要在保证相应的激励效果情况下减少通信计算的开销。

## 2 基于区块链的激励架构

现有的区块链相关的架构[11−12]没有考虑针对激励交易的全流程设计需求。因此，本文在第1节提出的全流程设计原则基础上，设计了区块链的分布式激励架构。如图2所示，该架构分为3阶段：1）场景适配阶段。分析并提取应用场景节点之间的角色、分工、验证、安全和隐私脆弱点等内容。2）支付策略阶段。在场景适配的基础上提供相应的支付策略，包括密码货币选择、定价机制设计、付款方式抉择等。3）效果评价阶段。对激励机制的设计目的与效果进行评估，激励程度的考虑包含安全可信、隐私保护、可拓展性、成本开销等。

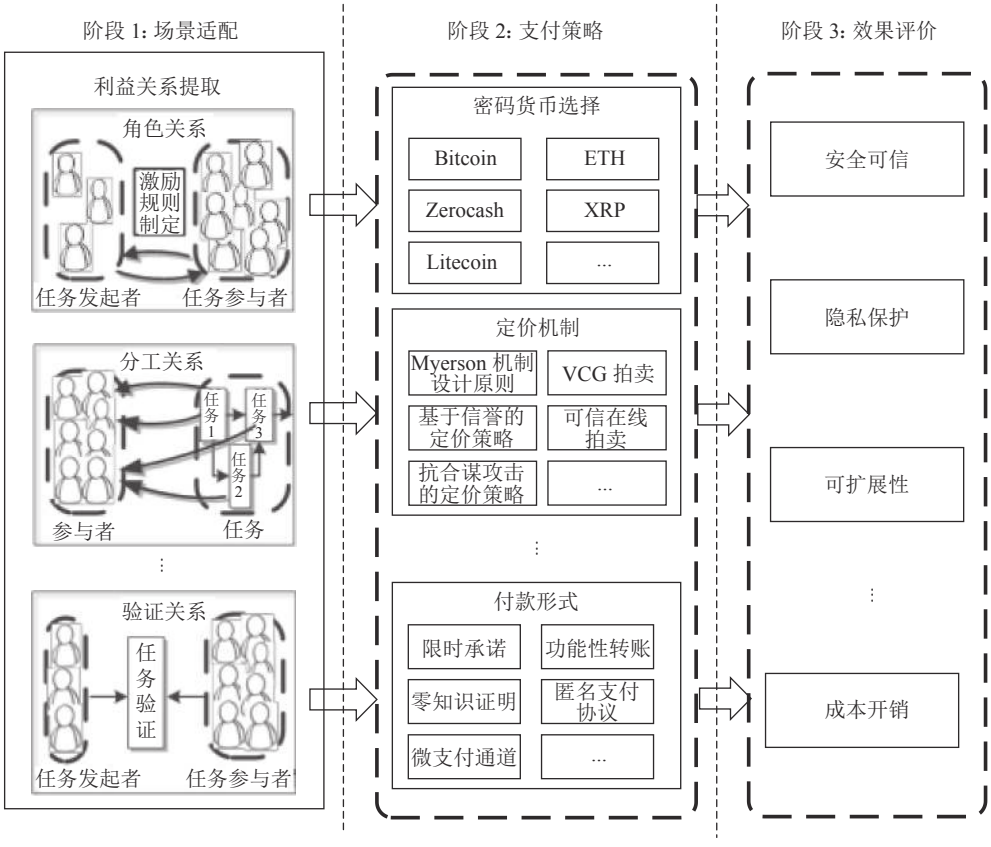


**图 2 基于区块链的分布式架构**

**Fig. 2 Blockchain-based distributed architecture**

### 2.1 场景适配

在3阶段架构中，场景适配属于第1阶段，是激励架构设计的基础。场景适配通过对应用场景的分析，提取出其中节点间的利益关系。基于已有的分布式激励系统研究，本架构通过分析其中角色的关联关系，提取出交易验证、报酬流向、安全与隐私脆弱点等内容。不同的应用场景下，其角色关系及利益关系不同，导致交易验证、报酬流向、安全性、隐私保护的设置不同。下面将以3个示例进行说明。

1）能源互联网中电车充电场景。包括电车用户、电动汽车、充电运营商、充电桩节点、电网等实体。充电运营商制定充电价格，电车用户根据充电价格决定其电动汽车在某个充电桩节点进行充放电[14−17]。电车用户希望降低充电成本，同时保证其电车电量充足；充电运营商期望最大化充电桩的利用率，提高充电收益；电网期望电车充电不影响供电负荷的均衡。如图3所示，电车用户验证充电桩节点的身份，充电运营商验证电车用户身份，身份验证后充电运营商会授权为电动汽车充电或放电，充电交易完成后生成订单，订单信息验证后存储到区块链中，验证工作由区块链矿工完成。在此过程中，区块链记录交易信息可能泄露电车用户的隐私，充电运营商可能推断出电车用户轨迹隐私信息，矿工做验证时可能出安全与隐私问题。报酬流向包括充电运营商到电车

用户、电车用户到充电运营商、区块链网络到矿工节点等。

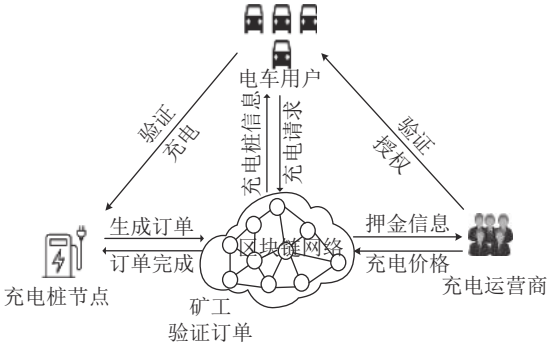


**图 3　电车充电场景**

**Fig. 3　EV charging scene**

2）群智感知中路况感知场景。包括服务提供商、移动感知用户、服务查询者3个角色，服务提供商收集移动用户的实时GPS信息，用于估计道路交通状况，进而为服务查询者提供路况服务[18–21]。服务提供商尽可能收集更多在道路行驶的移动感知用户的GPS位置信息，提升道路交通状况的准确性，并在尽可能短的时间内给予服务查询者响应，提升服务体现；移动感知用户提供GPS信息的同时，不期望自己的位置隐私信息泄露；服务查询者期望得到及时且准确的路况服务。在执行感知任务前，移动感知用户验证服务提供商的身份和同意接受感知任务；移动感知用户上传感知数据后，服务提供商需验证移动感知用户身份和提供数据的质量，然后根据数据质量给予对应移动感知用户相应的报酬；服务提供商、移动感知用户、服务查询者之间的协定可通过区块链的智能合约实现，由区块链矿工来验证。在上述过程中，上传的感知数据易暴露用户的位置隐私，服务提供商验证用户身份时会泄露用户身份信息，报酬给予会关联用户身份和上传的感知数据，矿工验证工作同样存在安全与隐私脆弱点。报酬流向包括服务提供商到移动感知用户，服务查询者到服务提供商等。

3）在延迟容忍网络信息传递场景。包括源节点、目的节点和中继节点，其中，中继节点帮助源节点将消息、文件或视频等内容传递到目的节点[13,22]。源节点期望所传送的内容能够快速且准确地送达目的节点，而且不泄露传送的内容；中继节点期望以较小代价完成转发任务并获得较多的报酬；目的节点期望成功获取完整的传送内容。源节点需验证目的节点接收到所传送的内容，验证中间节点确实帮助转发了传送的内容；目的节点需验证源节点身份和传送内容的完整性；源节点支付中间节点报酬的协定可通过区块链来实现，相关的验证内容记录在区块链上，由矿工进行验证。在此过程中，中间节点转发消息是安全与隐私脆弱点，矿工验证工作也是安全与隐私脆弱点。报酬的流向包括源节点给予中继节点的报酬及矿工验证工作的报酬。

### 2.2　支付策略

激励机制需设计相应的支付策略，以达到更多人参与、高质量参与的目的，或满足安全可信、隐私保护、计算高效等需求。支付策略的设计包括了密码货币的选择、定价机制的设计和付款形式的确定。

#### 2.2.1　密码货币的选择

密码货币的种类多样，不同的密码货币采用的共识机制、效率、特点差异较大。激励机制设计需根据场景需求选择合适的密码货币，现有常用的密码货币有Bitcoin、ETH、Litecoin、XRP、Zerocoin等[4]，如表1所示。

**表 1　主要密码货币的特点分析**

**Tab. 1　Characteristics of major cryptocurrencies**

| 密码货币 | 共识协议 | 块生成速度 | 主要特点 |
|---|---|---|---|
| Bitcoin | PoW | 10 min | 认可度高，但需精心设计扩展交易语法 |
| ETH | PoW/PoS | 15 s | 支持智能合约，方便实现定价策略 |
| Litecoin | PoW | 2.5 min | 哈希算法更安全，更有利于防止51%攻击 |
| Zerocash | 零币协议 | 2.5 min | 零币协议采用零知识证明保护用户隐私 |
| XRP | RPCA | 3 s | 低成本，可拓展性高，安全性差 |

Bitcoin是由中本聪提出的基于区块链技术的加密货币，采用工作量证明PoW共识协议[23]。Bitcoin是首创的加密货币，在密码货币市场份额占比最高，认可度较高。PoW用于解决电子货币的“双花”问题，但PoW共识协议成本较高，需要消耗大量的计算资源。Bitcion网络生成一个新的区块需要10 min，交易得到确认至少需要1 h，存在较大的延时。目前，Bitcoin的交易语法只支持转账，作为激励方式时，应扩充Bitcoin的交易语法，使其支持功能性转账，以确保激励机制的正常运作。

以太币（ETH）是基于以太坊的数字代币，支持可编程智能合约，采用PoW/PoS共识协议[4]。可编程智能合约能够控制区块链上的数字资产进行复杂操作，实现高灵活性ETH交易，赋予了区块链高灵活度的拓展应用功能，以太币的智能合约易于实现激励机制中的定价策略。目前，ETH支持轻客户端快速验证的PoW 算法，以太坊的区块大约每隔15 s 产生，生成块速度仍然很慢。为了解决 PoW 挖矿带来的巨大能源消耗问题，以太坊正在从 PoW 共识机制向 PoS 共识机制转变，但PoS的安全性完全依赖于资产较高的矿工节点，不适用于安全性较高的应用场景。

Litecoin相比于Bitcoin在工作量证明机制算法、

总量上限和区块生成速度上进行了改进。Litecoin在工作量证明机制中使用Scrypt算法取代SHA-256算法[4]。由于挖矿的矿工更加分散，也就更利于防止51%攻击，安全性相对较高。区块速度为2.5 min产生一个，完成一笔交易的时间约为20 min，延时也较大。Litecoin网络适用于延时要求不高而安全性有较高要求的激励机制应用场景。

Zerocash使用zk-SNARKS加密技术实现匿名，使发送方地址、接收方地址和金额彻底隐藏，其交易记录不公开，需要通过使用特定的数据才能解码查看交易记录[24]。Zerocash作为比特币的一种分支保留了其原有的工作量证明机制，但其挖矿算法使用Equihash算法，其更加依赖于计算能力。因此，Zerocash作为激励方式时，其交易规则可以隐藏激励机制中交易双方的身份信息及交易记录，适用于需要更完善的隐私保护的场景。

XRP基于Ripple网络实现交易，相比于Bitcoin的交易数据打包和记录确认速度更快，3 s生成一个区块[4]。其共识机制为RPCA协议共识，将网络中的节点分为普通节点和验证节点，交易的验证和确定只需要验证节点的投票，因此XRP减少挖矿耗费的时间。XRP适用于需要交易延时低的交易系统及高效率支付手段的激励机制场景。

2.2.2 定价策略

定价策略直接决定了参与者的积极性，包括任务参与者的意愿、参与任务做出的贡献等。参与者的报酬分配原则可按照参与者的信誉、完成任务质量或者竞价等方式进行分配。报酬分配时还应考虑激励交易供需关系，供需双方的不诚信行为或自私行为。目前，激励机制中定价策略的设计大致分为3种类型：

1）基于信誉的定价策略。将信誉、信任量化，将其作为主要参数，依据不同场景下的需求设计相应的定价策略，得出任务参与者的报酬价格。该类定价策略依赖的信誉系统可分为集中式[10]和分布式[25]信誉系统。集中式信誉系统由中央机构记录、收集、发布用户的历史交易信息及信誉反馈信息，但其运行成本高，且存在中心信任缺失问题。分布式信誉系统将节点的信誉信息分散存储在交易过的节点上，查询时广播查询信息，由交易过的节点响应并反馈对应的信誉值。这种方式适合于与区块链分布式存储方式结合，将信誉值打包到区块中，并存储在区块链网络。

例如，在能源互联网的电车充电场景中，电动汽车用户的可信度与其朋友数量、其他用户和该用户对充电桩评分的相似性相关[26]。因此，某个电车用户$i$的可信度$C_i(t)$可表示为：

$$C_i(t) = S_i(t) \cdot \frac{F_i}{\sum_{i \in N} F_i} \tag{1}$$

式中，$t$为时间，$S_i(t)$为电车用户$i$与其他用户对充电桩节点评分的相似度，$F_i$为电车用户$i$的朋友数量。

充电桩节点的信誉与所有充过电的电车用户对该节点服务的信任度相关[26]，因此，充电桩节点$j$的信誉$R_j(t)$可表示为：

$$R_j(t) = \frac{\sum_i C_i(t) T_{i,j}(t)}{\sum_i C_i(t)} \tag{2}$$

式中，$t$为时间，$C_i(t)$为电车用户$i$的可信度，$T_{i,j}(t)$为电车用户$i$对充电桩节点$j$服务的信任度。

根据充电桩节点信誉占所有充电桩节点信誉总和的比例，分配报酬奖励。因此充电桩$j$的报酬$r_j$可由式（3）计算：

$$r_j = P \cdot \frac{R_j}{\sum_{j \in V} R_j}, \forall j \in V \tag{3}$$

式中，$P$为区块链网络支付的总报酬，$R_j$为充电桩节点$j$的信誉，$V$为所有接入区块链网络的充电桩节点集合。

2）基于质量贡献的定价策略。根据参与者完成任务的质量或贡献给予相应的报酬。该定价策略的主要任务在于如何准确地评估参与者的质量或贡献，如何将质量或贡献转化为对用户的奖励。质量或贡献主要考察时空覆盖质量[19]、数据质量[27]等层面。时空覆盖质量是指参与者参与时空相关任务时应满足数据采集间隔、区域覆盖率，如车辆移动轨迹收集和城市中环境监测（PM2.5、噪音等）所要求的区域覆盖率和监测时间间隔的要求；数据质量是指参与者提供数据的准确性和可靠性的评估，通常采用贝叶斯推断、期望最大化等评估技术实现。

参与者的报酬与参与者的质量或贡献通常成正比关系，报酬的计算通过归一化的贡献或质量乘以基准报酬实现，例如，通过互信息原理得到归一化的贡献[28]。因此，参与者$k$的报酬$r(q_k)$可表示为：

$$r(q_k) = rc_n(q_k) \tag{4}$$

式中：$q_k$为评估的质量，可由用户期望最大化（EM）算法估计得到；$c_n(q_k)$为数值划分为$n$个区间的归一化的贡献。

3）基于拍卖的定价策略。以拍卖的形式分配任务和给予报酬，通过竞价使任务请求者和任务参与者

利益最优化, 适合于参与者展现不诚信行为或自私行为的场景。基于拍卖的定价策略可分为Myerson拍卖[29]、VCG拍卖[18]、双边拍卖[29]、逆向拍卖[29–30]等。

Myerson拍卖解决竞价机制中出售单个物品的“最优拍卖问题”, 即卖家如何依据拍卖规则与买家的出价获取最大化收益。VCG(Vickrey–Clark–Groves)机制解决竞价机制组合出售多个物品的“最优拍卖问题”, 即卖家如何根据买家对多个物品的估值分配出售多个物品的组合以达到最优收益的目的。VCG拍卖机制基于动态定价策略, 其定价策略是依据通过拍卖者卖给买者带来的损失之和来定价的, 通过激励机制的设计和合理的支付函数引导参与者诚实地上传自己的真实开销和相应参数, 提供更加稳定的交易环境。以上拍卖机制只考虑卖家的利益最大化, 影响参与者的积极性。双边拍卖解决的是众多买者和众多卖者的场景下的最优拍卖问题, 需同时考虑买者和卖者的利益。在双边拍卖中, 拍卖师发布买者的任务需求和出价, 卖者给出可完成的任务和报价, 当买者中给出的最高价与卖者中提出的最低价一致时交易达成。

逆向拍卖更适合被用于激励机制设计。激励机制实质上更侧重于参与者的参与度和做出的贡献, 更偏向于激励参与者一方, 这与逆向拍卖的思想较为契合。在逆向拍卖中, 买方提供任务需求以供出价, 潜在的卖方出价, 然后买方选择满足要求的最低出价的卖者作为交易。例如, 在群智感知应用中, 采用逆向拍卖模型选择参与者和支付奖励[18]。如下面的算法所示, 根据参与者的边际价值和出价差异进行降序排序, 选出前$L$位作为获胜者执行群智感知任务, 获胜者的定价设置为该获胜者能够以相应的位置被选中的最大出价。其中, $S$为获胜用户集合, $U$为参与者集合, $v_i$为参与者$i$参与任务的边际价值, $b_i$为参与者$i$的出价, $p_i$为获胜者的报酬, $U_{-i}$为除去参与者$i$的集合, $i_j$为参与者在排序中的位置为$j$。

**算　法**　群智感知逆向拍卖算法[18]

1 //阶段1: 获胜者选择
2 $S \leftarrow \varnothing, i \leftarrow \arg\max_{j \in U}(v_j(S)-b_j)$;
3 while $b_i < v_i$ and $S \neq U$ do
4　$S \leftarrow S \cup \{i\}$;
5　$i \leftarrow \arg\max_{j \in U \backslash S}(v_j(S)-b_j)$;
6 end
7 //阶段2: 付款确定阶段
8 for each $i \in U$ do $p_i \leftarrow 0$;
9 for each $i \in S$ do
10　$U_{-i} \leftarrow U \backslash \{i\}, T \leftarrow \varnothing$;
11　repeat
12　　$i_j \leftarrow \arg\max_{j \in U_{-i} \backslash T}(v_j(T)-b_j)$;
13　　$p_i \leftarrow \max\{p_i, \min\{v_i(T)-(v_{ij}(T)-b_{ij}), v_i(T)\}\}$;
14　　$T \leftarrow T \cup \{i_j\}$;
15　until $b_{ij} \geq v_{ij}$ or $T = U_{-i}$;
16　if $T = U_{-i}$ then $p_i \leftarrow \max\{p_i, v_i(T)\}$;
17 end
18 return $(S,p)$

多属性逆向拍卖除了考虑拍卖双方的价格属性外, 还需考虑信用、质量、性能等非价格因素的影响。

2.2.3　付款形式

激励交易的付款形式决定着交易的安全性和效率, 在激励机制设计中起着重要作用。由于激励交易采用区块链技术, 激励交易都具备防双花、防篡改的作用, 在安全性上有一定的保障。然而激励交易除了转账之外, 还要求参与者能够完成既定的任务, 这是激励交易的付款形式需要解决的问题。激励交易可能会泄露参与者的隐私, 隐私保护也是付款形式的研究内容之一。另外, 区块链技术中区块确认的速率通常较慢, 因此提升激励交易的付款效率是另一个需要研究的问题。

现有能够实现让参与者完成既定任务的方法包括扩展交易语法支持承诺[1]和智能合约[11]的方式。Kumaresan等[1]提出了基于Bitcoin 的功能转账模型, 通过Bitcoin 构造形式化的模型以支持限时转账、承诺退还、押金补偿等功能, 并通过该这些功能转账模型实现了可证计算、安全计算、公平计算、非交互赏金任务等密码学任务, 但该Bitcoin扩展交易语法不是图灵完备的, 较难实现复杂功能或开销很大。智能合约通过提供相应的方法完成所需要的功能要求, 例如, 在能源互联网的电车充电场景中, 电车充电认证、充电交易过程被写入到智能合约[31], 如图4所示。但是智能合约的编写可能引入安全漏洞, 需对智能合约的安全性进行评估。

为保护激励交易的隐私, 可采用Zerocash实现, 利用非交互式零知识证明方法(zk-SNARKs), 隐藏交易的原地址、目的地址和转账金额[24]。另一种隐私保护方式是通过货币混淆节点打破用户与其他用户之间的交易关系。货币混淆节点通过签名承诺保证“用户$i$在$t_1$时刻发给它的$v$个电子币, 它将在$t_2$时刻之前返回给用户$i$”[32]。但以上方案未考虑节点的任务执行过程及矿工的验证工作会重新建立交易之间的关联性, 泄漏参与者隐私。Wang等[27]提出基于节点协作的交易验证模型, 通过矿工与参与节点之间的多方协作完成对交易的验证, 达到$k$-匿名隐私保护的目的。

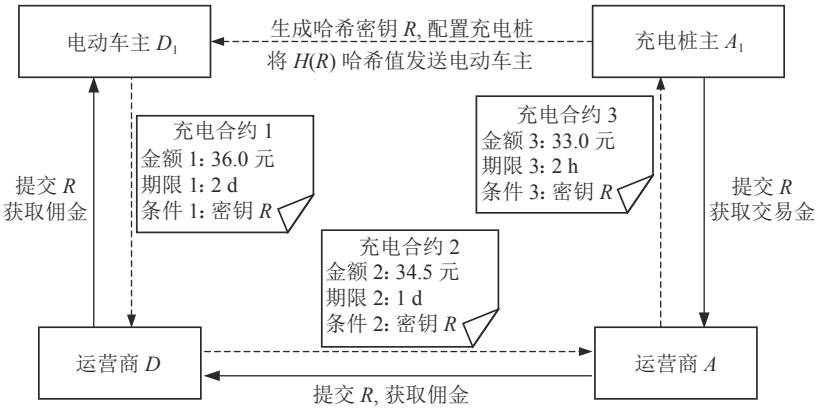


**图 4 电车充电合约[31]**

**Fig. 4 EV charging contract[31]**

现有提升激励交易的效率方法包括微支付通道[33]、改进共识算法[34−35]等方案。Poon等[33]提出在长期具有交易关系的节点之间建立可信的微支付通道，节点通过微支付通道完成交易过程，而不广播到Bitcoin的公有链上，公有链上的交易只记录微支付通道中两节点的Bitcoin总额。Kokoris−Kogias等[34]提出了一种强共识协议，建立在成熟的实用拜占庭错误容忍算法（PBFT）之上，引入联合签名方案减小PBFT轮次的开销和轻量级客户端验证交易请求的开销；该强共识协议能够增加比特币两个数量级的吞吐量，降低交易确认延迟至1 min以内。Zamani等[35]提出了RapidChain共识算法，该共识算法分为引导启动阶段、共识阶段和重构阶段，如图5所示。引导启动阶段只会在开始时运行一次，该阶段创建一个初始随机源，并随机选出一个特殊的委员会，称为参考委员会；再由该参考委员会的成员对节点进行随机分配，构成多个分片委员会。该共识机制采用时间分片技术，并且，每个时间分片又分为多个轮次，每个轮次都可进行区块确认工作，不必频繁重构委员会，从而提升了效率。

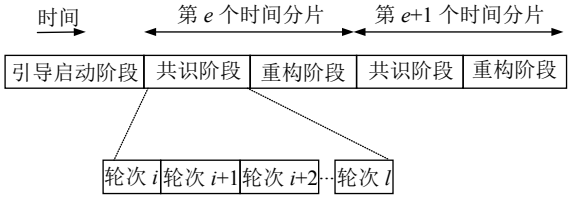


**图 5 RapidChain共识机制[35]**

**Fig. 5 RapidChain consensus mechanism[35]**

### 2.3 效果评估

激励效果是指由激励机制产生的结果，是对激励机制的整体性考虑，针对激励机制在应用场景中的特定需求，通过第2.2节给出相应的技术支撑以达到安全可信、隐私保护、可拓展性、可持续性、计算高效等激励效果。

1）安全可信，保证激励机制设计的安全性和公平性，包括密码货币本身的安全性、支付策略的公平性、支付形式的安全性等，通常通过形式化证明、安全性分析、博弈分析等角度进行评估。

2）隐私保护，保证激励交易中双方的隐私不被泄漏，包括参与者的身份隐私、任务涉及的数据隐私、位置隐私等，常用的评估方法包括$k$-匿名、信息熵、差分隐私等衡量标准。

3）可扩展性，是指激励交易处理的瓶颈问题，这主要是由区块链本身性能受限造成的，通常需要从共识机制、交易验证、广播通信、信息加解密等环节进行优化以提升性能。

4）可持续性，保证参与者有持续长期的动力，通常通过多次模拟实验考察参与者的参与情况和完成任务质量情况，评估参与者是否保持着参与的积累性。

5）计算高效，保证激励交易涉及的相关计算开销较小，包括定价策略的计算开销、身份验证开销、任务验证开销等，通常通过计算复杂度和计算时间衡量。

对于具体应用场景进行评估时，以上激励效果不一定都要评估，需要根据场景利益关系需求决定。例如，在延迟容忍网络信息传递场景中，对于中间节点的激励即在本次消息传递完成后就给予的报酬，可以不用考虑激励的持续性。

## 3 群智感知应用案例分析

本节将提出的激励架构应用到群智感知应用案例，体现该架构对激励设计的指导和优化作用。

### 3.1 利益关系提取

第2.1节列举的场景已经简述了群智感知应用的利益关系，由于本文更关注对安全与隐私脆弱点的优化，因此，下面将主要阐述这两方面的内容。如图6所示，用户上传感知数据而服务器给予激励的过程

可看作为一个交易，交易由矿工验证后打包成区块接入区块链中，根据不同的感知质量，不同的用户得到不同的报酬。服务器期望获得高质量的感知数据；用户期望提供感知数据时获得合理的报酬，尽可能不泄露自身的隐私；矿工执行验证任务获得区块链网络的奖励，矿工还可能冒充用户去领取更多的奖励。群智感知应用在区块链中执行的具体过程如下：首先，服务器预付押金生成感知任务公告合约；然后，用户执行感知任务，上传感知数据给任务公告合约地址；其次，矿工验证感知数据质量，将贡献量化，计算相应的报酬，生成服务器和用户之间的交易；最后，服务器确认感知数据和交易，支付给用户报酬，报酬转入用户的地址。

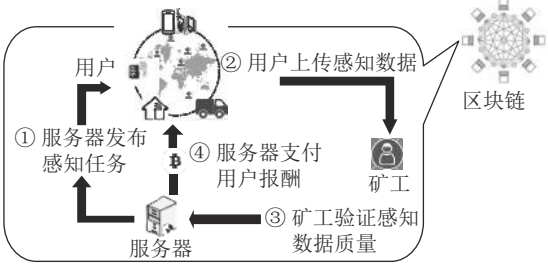


**图 6　群智感知应用利益关系**

**Fig. 6　Interest relationship in crowdsensing**

### 3.2　支付策略确定

根据第3.1节的群智感知应用利益关系可知，目前基于区块链的群智感知过程中数据质量验证工作都由矿工节点完成，矿工节点可能获取用户感知数据，冒充用户领取报酬，或者与其他用户共谋获得更多的报酬。因此，矿工的验证工作应分担给参与用户以保护隐私，并通过节点之间合作达到隐私保护的同时保证节点具有参与的动力，这是激励机制设计面临的问题。

为解决该问题，提出了基于节点协作的隐私保护激励机制。用户形成协作组$G$上传感知数据到区块链P2P网络；矿工验证感知数据和激励交易，验证通过后将感知数据递交给服务器，并给用户组分配报酬（payment），如图7所示。

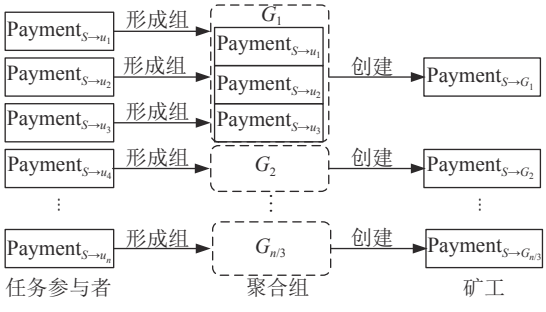


**图 7　隐私保护激励机制**

**Fig. 7　Privacy-preserving incentive mechanism**

本方案可采用以太币作为密码货币，其中，以太坊平台提供了智能合约，可以便于本激励方案的实施；定价策略采用基于质量贡献的定价策略，参照第2.2.2节相关内容的描述。付款形式的具体验证过程分为组内协商阶段和矿工验证组交易阶段。

#### 3.2.1　组内协商

用户与其附近的用户或朋友形成匿名组，匿名组内用户采用签名技术传递感知数据。用户在建立匿名组时，可以根据用户的信誉挑选组成员，或者通过社交关系挑选组成员，从而得到一个彼此相互信任的匿名组。为保证匿名组内用户隐私得到较好的防护，本方案要求组内的用户数量至少为$k$个，从而满足$k$-匿名隐私保护的要求。

感知数据在组内传递时可被监听，为保证感知数据的完整性和安全性，本方案需对感知数据进行签名和加密后传输，但直接采用先签名后加密的方式会带来较大的计算开销。因此，本方案使用双线性映射的签密方案[36]完成组内节点用户感知数据的验证。

#### 3.2.2　组交易验证

组内的用户负责组内节点用户的身份隐私信息验证，而用户的感知数据则整合在一起由矿工验证。本方案使用Hash函数对组内用户的感知数据进行加密以保证数据的安全性。而对于组内用户数据的整合，本方案利用Merkle树的思想归纳组内节点数据。

对于每个组的感知数据，矿工需要验证其合法性和数据质量，对于合法性检查，使用群盲签名算法验证；对于数据质量的估计则使用期望最大化（EM）算法验证。群成员对消息进行签名，矿工收到群成员对消息（$m$）的签名后进行验证。

### 3.3　激励效果分析

由于本方案主要关注安全可信、隐私保护和计算效率方面的激励效果的优化，因此只对这3个方面进行评估。基于节点协作的隐私保护激励机制能够有效防止矿工对组内节点发起的背景知识攻击和链接攻击，以及攻击者在数据发布过程中可能发起的推理攻击。本方案安全性主要依赖于$k$-匿名组的划分和归类形成的组内成员准标志符（quasi-identifier）的相似性，相似性越大，汇总后的感知数据会产生的信息损失越小。

当组内用户数接近网络中实际连接数时，信息损失量越低，匿名化程度越高。以修正的可视度量$C_{\mathrm{MVM}}$衡量数据集的匿名化质量：

$$C_{\mathrm{MVM}}=\sum_{G}(|n_G|-k)^2 \tag{5}$$

式中，$|n_G|$为匿名组的成员数量，$k$为期望达到的匿名

度。对于所有的匿名组$G$来说，通过计算其成员数量与网络实际连接数下匿名度$k$之差的平方度量匿名化质量。当理想情况下所有节点数都为$k$时，$C_{MVM}$为0。

运用Gervais的区块链仿真平台模拟区块链及区块节点数，其中，拥有5—15连接数的节点最多，并以此模拟$k$-匿名化的效率。如图8所示，可知$k$定为10时，匿名效果较好的匿名组数量最多。

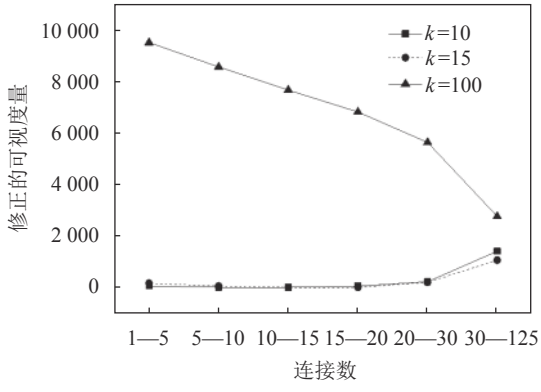


**图 8 不同$k$值下不同组的$C_{MVM}$**

**Fig. 8 $C_{MVM}$ of different groups under $k$**

本方案采用的双线性映射的签密方案与先签名后加密的方法相比，使用隐藏的签名作为一次性密钥节省了一次指数运算，即椭圆曲线上的一次标量乘法运算；而且，发送方的两次指数运算也可以离线进行，从而较大地提升了用户感知数据签密的效率。

## 4 结 论

本文基于激励机制设计原则，依据不同场景中的激励机制设计了基于区块链分布式的激励架构，该架构包括场景适配、支付策略、效果评估3个阶段，并利用该架构对群智感知应用的激励机制在安全可信、隐私保护和计算高效方面进行了优化。下一步的研究将在本架构基础上提供其基本模块的接口函数或工具集，便于相关研究人员使用。

**参考文献：**

[1] Kumaresan R,Bentov I.How to use bitcoin to incentivize correct computations[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security(CCS'14).New York:ACM,2014:31–41.

[2] Salman T,Zolanvari M,Erbad A,et al.Security services using blockchains:A state of the art survey[J].IEEE Communications Surveys & Tutorials,2019,21(1):858–880.

[3] Tschorsch F,Scheuermann B.Bitcoin and beyond:A technical survey on decentralized digital currencies[J].IEEE Communications Surveys and Tutorials,2016,18(3):2084–2123.

[4] Li Xiaoqi,Jiang Peng,Chen Ting,et al.A survey on the security of blockchain systems[J].Future Generation Computer Systems,2020,107:841–853.

[5] Kang Jiawen,Yu Rong,Huang Xumin,et al.Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains[J].IEEE Transactions on Industrial Informatics,2017,13(6):3154–3164.

[6] Jia Bing,Zhou Tao,Li W,et al.A blockchain-based location privacy protection incentive mechanism in crowd sensing networks[J].Sensors,2018,18(11):3894.

[7] Li Lun,Liu Jiqiang,Cheng Lichen,et al.CreditCoin:A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J].IEEE Transactions on Intelligent Transportation Systems,2018,19(7):2204–2220.

[8] Xuan Shichang,Zheng L,Chung I,et al.An incentive mechanism for data sharing based on blockchain with smart contracts[J].Computers & Electrical Engineering,2020,83:106587.

[9] Yang Dejun,Zhang Xiang,Xue Guoliang.PROMISE:A framework for truthful and profit maximizing spectrum double auctions[C]//Proceedings of 2014 IEEE Conference on Computer Communications(IEEE INFOCOM 2014).Toronto:IEEE,2014:109–117.

[10] Zhang Yu,van der Schaar M.Reputation-based incentive protocols in crowdsourcing applications[C]//2012 Proceedings IEEE INFOCOM.Orlando:IEEE,2012:2140–2148.

[11] Shao Qifeng,Jin Cheqing,Zhang Zhao,et al.Blockchain:Architecture and research progress[J].Chinese Journal of Computers,2018,41(5):969–988.[邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018,41(5):969–988.]

[12] Xu Ke,Ling Sitong,Li Qi,et al.Research progress of network security architecture and key technologies based on blockchain[J/OL].Chinese Journal of Computers[2020–09–08].http://cjc.ict.ac.cn/online/cre/xk-2020521134939.pdf.[徐恪,凌思通,李琦,等.基于区块链的网络安全体系结构与关键技术研究进展[J/OL].计算机学报[2020–09–08].http://cjc.ict.ac.cn/online/cre/xk-2020521134939.pdf.]

[13] He Yunhua,Li Hong,Cheng Xiuzhen,et al.A blockchain based truthful incentive mechanism for distributed P2P applications[J].IEEE Access,2018,6:27324–27335.

[14] Zhang Ke,Mao Yuming,Leng Supeng,et al.Optimal charging schemes for electric vehicles in smart grid:A contract theoretic approach[J].IEEE Transactions on Intelligent Transportation Systems,2018,19(9):3046–3058.

[15] Tan Jun,Wang Lingfeng.Real-time charging navigation of electric vehicles to fast charging stations:A hierarchical game approach[J].IEEE Transactions on Smart Grid,2015,8(2):846–856.

[16] Gabay D,Akkaya K,Cebe M.Privacy-preserving authentica-

tion scheme for connected electric vehicles using blockchain and zero knowledge proofs[J].IEEE Transactions on Vehicular Technology,2020,69(6):5760–5772.

[17] Huang Xiaohong,Xu Cheng,Wang Pengfei,et al.LNSC:A security model for electric vehicle and charging pile management based on blockchain ecosystem[J].IEEE Access,2018,6:13565–13574.

[18] Yang Dejun,Xue Guoliang,Fang Xi,et al.Incentive mechanisms for crowdsensing:Crowdsourcing with smartphones[J].ACM Transactions on Networking,2016,24(3):1732–1744.

[19] He Yunhua,Sun Limin,Li Zhi,et al.An optimal privacy-preserving mechanism for crowdsourced traffic monitoring[C]//Proceedings of the 10th ACM International Workshop on Foundations of Mobile Computing(FOMC'14).New York:ACM,2014:11–18.

[20] Jiang Lingyun,He Fan,Wang Yu,et al.Quality-aware incentive mechanism for mobile crowd sensing[J].Journal of Sensors,2017,2017:5757125.

[21] Li Ming,Weng Jian,Yang Anjia,et al.CrowdBC:A blockchain-based decentralized framework for crowdsourcing[J].IEEE Transactions on Parallel and Distributed Systems,2019,30(6):1251–1266.

[22] Chen Binbin,Chan M C.MobiCent:A Credit-based incentive system for disruption tolerant network[C]//2010 Proceedings IEEE INFOCOM.San Diego:IEEE.2010:875–883.

[23] Nakamoto S.Bitcoin:A peer-to-peer electronic cash system[EB/OL].[2020–09–08].https://bitcoin.org/bitcoin.pdf.

[24] Sasson E B,Chiesa A,Garman C,et al.Zerocash:Decentralized anonymous payments from bitcoin[C]//Proceedings of 2014 IEEE Symposium on Security and Privacy.San Jose:IEEE,2014:459–474.

[25] Wang E K,Liang Zuodong,Chen C M,et al.PoRX:A reputation incentive scheme for blockchain consensus of IIoT[J].Future Generation Computer Systems,2020,102:140–151.

[26] Wang Yuntao,Su Zhou,Zhang Ning.BSIS:Blockchain-based secure incentive scheme for energy delivery in vehicular energy network[J].IEEE Transactions on Industrial Informatics,2019,15(6):3620–3631.

[27] Wang Jingzhong,Li Mengru,He Yunhua,et al.A blockchain based privacy-preserving incentive mechanism in crowdsensing applications[J].IEEE Access,2018,6:17545–17556.

[28] Peng Dan,Wu Fan,Chen Guihai.Pay as how well you do:A quality based incentive mechanism for crowdsensing[C]//Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing.New York:ACM,2015:177–186.

[29] Zhang Xinglin,Yang Zheng,Sun Wei,et al.Incentives for mobile crowd sensing:A survey[J].IEEE Communications Surveys & Tutorials,2016,18(1):54–67.

[30] Hu Ying,Wang Yingjie,Li Yingshu,et al.An incentive mechanism in mobile crowdsourcing based on multi-attribute reverse auctions[J].Sensors,2018,18(10):3453.

[31] Qi Linhai,Li Xue,Qi Bing,et al.Shared economy model of charging pile based on block chain ecosystem[J].Electric Power Construction,2017,38(9):1–7.[齐林海,李雪,祁兵,等.基于区块链生态系统的充电桩共享经济模式[J].电力建设,2017,38(9):1–7.]

[32] Bonneau J,Narayanan A,Miller A,et al.Mixcoin:Anonymity for bitcoin with accountable mixes[M]//Financial Cryptography and Data Security.Berlin:Springer,2014:486–504.

[33] Poon J,Dryja T.The bitcoin lightning network:Scalable off-chain instant payments[EB/OL].(2016–01–14)[2020–09–08].https://lightning.network/lightning-network-paper.pdf.

[34] Kokoris–Kogias E,Jovanovic P,Gailly N,et al.Enhancing bitcoin security and performance with strong consistency via collective signing[C]//Proceedings of the 25th USENIX Conference on Security Symposium.Berkeley:USENIX Association,2016:279–296.

[35] Zamani M,Movahedi M,Raykova M.RapidChain:Scaling blockchain via full sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.New York:ACM,2018:931–948.

[36] Young M.Practical signcryption[M].Berlin:Springer Science & Business Media,2010.

（编辑　赵　婧）

引用格式：He Yunhua,Huang Wei,Wang Weizhong,et al.Research on distributed incentive architecture based on blockchain[J].Advanced Engineering Sciences,2021,53(1):178–187.[何云华,黄伟,王伟忠,等.基于区块链的分布式激励架构研究[J].工程科学与技术,2021,53(1):178–187.]