软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(Suppl.(1)):97−106

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

电子货币激励机制综述*

何云华[1], 耿子烨[1], 李 红[2], 孙利民[2], 李 旭[3]

[1](北方工业大学 计算机学院,北京 100144)

[2](物联网安全北京市重点实验室(中国科学院 信息工程研究所),北京 100093)

[3](北京车网互联科技有限公司,北京 100082)

通讯作者: 李红, E-mail: lihong@iie.ac.cn

摘 要: 电子货币激励机制是信息网络领域普遍采用的方法,在推动资源共享、激发群智感知、促进协作通信等方面有着重要作用,是提升信息网络服务质量与效率的关键.综述电子货币激励机制现有的工作,阐述了电子货币激励机制的挑战,重点介绍了依赖于可信中心的激励机制和基于区块链的分布式激励机制,并探讨了电子货币激励机制中安全可信、隐私保护、可扩展性等问题.

关键词: 电子货币;激励机制;区块链;分布式

中文引用格式: 何云华,耿子烨,李红,孙利民,李旭.电子货币激励机制综述.软件学报,2017,28(Suppl.(1)):97−106. http://www.jos.org.cn/1000-9825/17010.htm

英文引用格式: He YH, Geng ZY, Li H, Sun LM, Li X. Survey on incentive mechanisms based on electronic money. Ruan Jian Xue Bao/Journal of Software, 2017,28(Suppl.(1)):97−106 (in Chinese). http://www.jos.org.cn/1000-9825/17010.htm

Survey on Incentive Mechanisms Based on Electronic Money

HE Yun-Hua[1], GENG Zi-Ye[1], LI Hong[2], SUN Li-Min[2], LI Xu[3]

[1](School of Computer Science, North China University of Technology, Beijing 100144, China)

[2](Beijing Key Laboratory of Internet of Things Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

[3](Beijing CarSmart Technology Co., LTD., Beijing 100082, China)

Abstract: The incentive mechanism based on electronic money, a common method in the field of information network, plays an important role in promoting the resource sharing, stimulating crowd sensing and promoting cooperative communication, and it is the key to improve the quality and efficiency of information network service. This paper summarizes the existing work of the incentive mechanisms, describes the objectives and challenges of the incentive mechanism, and focuses on the incentive mechanism on a trust center and the distributed incentive mechanism based on the block chain. It also discusses the security, credibility, privacy protection and extensibility of incentive mechanism based on electronic money.

Key words: electronic money; incentive mechanism; blockchain; distributed method

激励机制是指通过政策、奖惩、互惠、信誉、电子货币等手段,产生内在动力、促进相互协作,朝着既定目标发展的活动过程.电子货币作为常用的激励方式被广泛应用于网络资源共享、群智感知、协作通信等信息网络领域中.2015 年 11 月,Bitwalking 电子币被提出用于激励个人参与健康行走运动,用户每走 1 万步可获得 1

* 基金项目: 国家重点研发计划(2017YFB0802300); 国家自然科学基金(61702503, 61602053); 北方工业大学青年科技创新基金(1473009)

Foundation item: National Key Technology R&D Program (2017YFB0802300); National Natural Science Foundation of China (61702503, 61602053); Youth Science and Technology Innovation Foundation (North China University of Technology) (1473009)

收稿时间: 2017-05-15; 采用时间: 2017-09-23

个电子币.滴滴公司抓住了移动支付改造传统出租车行业的机遇,通过“烧钱大战”助其迅速攫取司机端和用户端市场.2017 年 7 月,国家互联网金融技术分析平台发布的《2017 上半年国内 ICO 发展情况报告》称,基于区块链密码货币的 ICO 众筹项目募资超过 26 亿元.目前,电子货币关键技术的研究被列入网络空间安全国家重点研究法计划.全球知名的市场研究机构 eMarketer 预测[1],电子支付市场份额将从 2016 年的 1.92 万亿美元上升到 2020 年的 4.06 万亿美元.

虽然电子货币受到的广泛关注和应用,但当其作为激励机制应用于资源共享、群智感知、协作通信时不一定能够提升信息网络服务质量与效率.电子货币激励机制面临着安全可信问题,由于发行主体不确定、不统一,不同类型信誉差异很大的电子货币同时流通,势必会出现鱼龙混杂的现象,导致公众对整个系统的运营持续的消极印象的行为,可致使系统建立和维护客户关系的能力严重受损,甚至为电子假币、伪造欺诈等不法活动提供可能,从而严重影响正常的货币流通秩序,甚至引发社会动乱.电子货币系统维护的机器或人员可能会泄露客户的隐私信息,也可能受到黑客和病毒的攻击,系统一旦被破坏,客户的资料和隐私将泄露,使客户利益受损.另外,基于电子货币的激励机制还可能存在可扩展性问题,电子货币系统单位时间内处理的交易量是受限的,当产生的交易量可能超过系统的处理能力时,会导致系统无法提供正常服务.

1 电子货币激励机制设计原则与挑战

1.1 电子货币激励机制设计原则

电子货币激励机制是指通过制定合理的定价机制来激励用户参与激励任务,定价机制通常根据用户的贡献度来为用户分配相应数额的奖励.定价机制在设计时应考虑以下因素:(1) 计算高效性:在多项式时间内完成激励机制涉及的相关计算任务;(2) 个体理性:在激励过程中,每位用户都是理性的,期望其选择的策略能得到非负效用;(3) 盈利(profitability):激励机制无赤字效应,参与者完成任务带来的价值应该大于等于支付给他的报酬;(4) 可信性:每个参与者在其他人策略不变的情况下不能通过更改其策略来增加效用.前 3 条特性确保激励机制的可行性,可信性能够消除市场操纵的威胁[2,3].

为了保证电子货币激励机制的有效实施,还应考虑相关的保障措施:(1) 安全性,保证激励机制在执行过程中能够抵御假冒攻击、欺骗攻击或合谋攻击;(2) 隐私保护,激励机制不应泄露用户的隐私信息;(3) 可扩展性,激励机制不能太复杂,性能开销不应太大而影响用户体验,可支持对大量用户的激励.

1.2 电子货币激励机制设计挑战

基于电子货币的激励机制在设计时通常不可能满足上述所有设计原则,需根据具体的应用场景有所侧重,设计切实可行的激励机制.基于电子货币的激励机制设计将面临如下挑战:(1) 激励机制的执行可能需要大量的通信和计算资源,由于系统的计算、存储、带宽资源有限,导致激励机制无法成功执行.(2) 激励机制缺少相应的验证过程,自私节点存在不诚实需求等欺骗行为,影响激励效果.(3) 激励过程可能会导致用户隐私泄露等问题,设计激励机制要兼顾安全性与有效性;(4) 激励机制需鼓励尽可能多的用户参与,会增加系统的处理开销,如何利用系统有限的资源处理日益增多的激励交易是具有挑战性的问题.

2 电子货币激励机制

电子货币是指以数字记账的方式代替使用现金交易的货币系统.电子货币有效提高交易的效率,例如消费者无须携带大量现金,商户无须人工点算现金,交易过程主要通过权威机构或区块链技术来记录和维护.在信息网络中,电子货币是普遍采用的激励方式,基于电子货币的激励机制可分为依赖于可信中心的激励机制和基于区块链的分布式激励机制.

2.1 依赖于可信中心的激励机制

激励机制依赖于第三方可信中心,其为每位用户分配一定数额的电子货币,由第三方可信中心作为激励过

程中的权威机构,按照一定规则筛选出部分用户参与激励任务,并在任务完成后,分配给完成任务的用户相应的电子货币作为奖励[4].

2.1.1 可信性

Kang 等人[5]提出一种 P2P 流媒体网络的激励机制,通过 Stackelberg 博弈分析视频上传者和下载者的行为,帮助上传制定最佳的定价策略,为下载者制定最大的响应策略,从而促进 P2P 流媒体网络中视频数据的共享.在 Stackelberg 博弈中,上传者作为博弈的主导者,上传视频数据后给出其定价策略;下载者作为博弈的跟随者,将连接类型、视频数据请求以及可提供的电子货币金额发给上传者,由上传者根据下载者提供的电子货币选出满足条件的下载者并为其提供下载服务.Stackelberg 博弈分为两部分:上传博弈和下载博弈.上传博弈表示如下:

$$\max_{\mu}\sum_{i\in S_k}\mu x_i \qquad \text{s.t.}\sum_{i\in S_k}x_i\leqslant u_k \tag{1}$$

其中,μ 为下载者每单位带宽的价格;x_i 是下载者 i 倾向购买的带宽,是一个关于 μ 的函数 $x_i\triangleq f_i(\mu)$;S_k 为向上传者 k 请求视频数据的下载者集合;u_k 为上传者 k 的可用带宽.上传者制定最佳带宽的定价策略 μ^*,以便最大限度地提高上传者的收入.在下载博弈中,下载者制定最佳响应函数 $\boldsymbol{x}^*$以平衡其成本和对下载视频的满意度,找到 Stackelberg 平衡点$(\mu^*,\boldsymbol{x})$,且满足条件

$$U^{up}(\mu^*,\boldsymbol{x}^*)\geqslant U^{up}(\mu,\boldsymbol{x}^*),U^{down}(x_i^*,\mu^*)\geqslant U^{down}(x_i,\mu^*),\forall i \tag{2}$$

其中,U^{up},U^{down} 分别是上传博弈和下载博弈的效用.通过博弈纳什均衡解的分析,得到下载博弈的最优带宽分配策略,以及上传博弈的最优定价策略,上传者根据最优分配策略制定单位下载带宽价格,下载者根据最优带宽策略选择购买的下载带宽大小,从而最大化上传者和下载者的效用.该机制通过报酬收益来激励自私用户上传视频数据,同时可以最大限度地提高上传者的收入和下载者的效用,并根据每个用户提供的电子货币金额给予不同权限的资源浏览服务.

Yang 等人[2]提出了基于拍卖博弈的 k-匿名激励机制,由关心隐私的用户给予不关心隐私的用户相应的报酬,激励不关心隐私的用户参与匿名组,以协作完成 k-匿名隐私保护,如图 1 所示.该方案设计了拍卖博弈,其中拍卖师为可信第三方,关心隐私用户为买者,其他用户为卖者,买者给实现 k-匿名的竞价 b_i,卖者给出协助完成 k-匿名的要价 a_j,为通过制定筛选条件

$$a_{k-n+2}\leqslant\frac{(n-1)b_n}{k-n+1} \tag{3}$$

从而找到买者出价最低、卖者要价最高的平衡点,筛选出加入 k-匿名组的用户.在 k-匿名组内用户协作完成 k-匿名隐私保护后,拍卖师将进行报酬分配以奖励协助用户.该机制考虑了用户对隐私保护的个性化需求,保证了激励机制设计的计算高效、个体理性、盈利和可信性,但未考虑拍卖师带来的安全威胁.

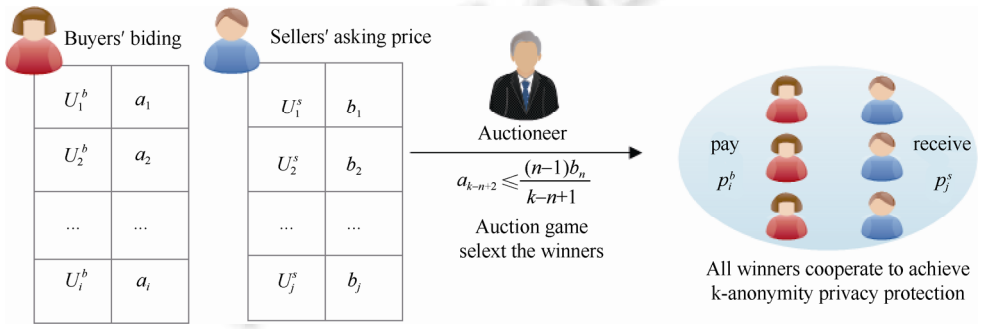


Fig.1 Workflow of the incentive mechanism based on auction game

图 1 基于拍卖博弈的激励机制的流程

Peng 等人[6]提出一种群智感知应用中的激励机制,将感知数据质量引入激励机制设计,根据用户上传的感知数据质量合理分配奖励金额,以促进用户上传高质量的感知数据.如图 2 所示,在该激励机制中,服务提供

商发布感知任务以及感知数据的质量要求,感兴趣的用户 $A=\{a_1,a_2,\ldots,a_n\}$参与感知任务并上传感知数据;服务提供商根据扩展的期望最大化算法来评估每位用户提供的感知数据质量 q_k,根据感知数据的质量和用户的感知代价 c_k筛选出一部分用户 $W\subseteq A$ 来完成感知任务,并根据每个用户的贡献度给予相应的报酬 r_k;若上传的感知数据质量小于容错阈值,服务提供商将从其提供的查询服务中获得相应的价值 V.服务提供商的利润计算如下:

$$\text{Profit} \triangleq \sum_{a_k \in W} (V - r_k) \tag{4}$$

通过最大化公式(4),得到给予用户的最优奖励 r^*,由公式(5)给出:

$$r^* = V - \frac{F(r^*)}{f(r^*)} \tag{5}$$

其中,$f()$为用户感知代价 c_k的概率密度函数,$F()$为感知代价 c_k的累计分布函数.该机制根据用户上传的感知数据质量给予相应的报酬,激励高技能的用户参与感知任务,从而提高服务器提供查询服务的服务质量,然而服务器可能作弊或遭受攻击,影响系统正常运行.

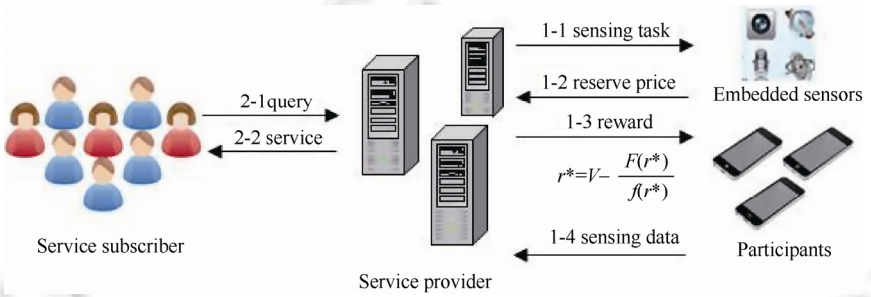


Fig.2 Workflow of the incentive mechanism in Crowdsensing

图 2 群智感知中的激励机制流程

2.1.2 安全性

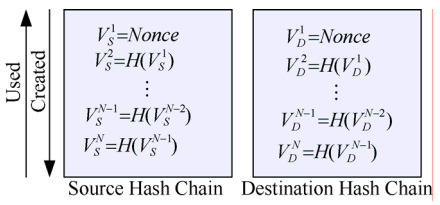


Fig.3 The source and destination nodes' hash chains

图 3 源节点和目的节点的哈希链

Mahmoud 等人[7]提出了一种安全高效的多跳无线网络消息传输激励协议 ESIP,鼓励中间节点帮助源节点传递消息到目的节点.该协议采用公钥技术与哈希链技术相结合的方式保证报酬支付的安全性,确保数据包在转发过程中的完整性、可用性和不可抵赖性,降低了完全由公钥操作保证安全性方案带来的计算开销大的问题.ESIP 协议包括 3 个阶段:预处理、通信和收据兑换.在预处理阶段,结算中心(accounting center,简称 AC)产生一个随机数 μ,并为每个节点 ID_i 分配密钥 $Sk_i=\mu\cdot H(ID_i)$,任意两节点可计算它们之间的共享密钥 $K_{SA}=\hat{e}(Sk_A,H(ID_S))=\hat{e}(H(ID_A),Sk_S)$.在通信阶段,源节点和目的节点通过迭代随机哈希值来生成哈希链,如图 3 所示,源节点利用密钥对其根进行签名,并将签名附加到会话节点标识上,使得发送者无法否认发起会话,中间节点协助转发数据包并获得支付收据.在收据兑换阶段,节点定期将收据提交给 AC,AC 验证收据的可信度,验证通过后,给予节点的相应的奖励,并清除收据信息.

Nix[8]提出了一种高效安全的数据共享激励方法.该方法通过博弈理论激励用户在数据共享中展现诚实行为,采用 VCG 博弈实现对无共谋情形下的高效数据挖掘算法,针对共谋情形下提出了可信安全的激励框架;并为数据共享过程中涉及的外包计算设计安全的查询验证方法.Lai 等人[9]提出了一种安全的 VANET 激励机制(SIRC),实现了车辆节点之间的公平、可靠、安全的协作资源下载.SIRC 机制包括合作下载和转发两个阶段:在合作下载阶段,SIRC 利用被指定验证者签名的电子支票来确保公平、安全的协作;在转发阶段,采用与聚合

Camenisch-Lysyans(CL)签名关联的利润共享模型来激励车辆节点协作转发数据包,在减少认证开销的同时可抵御注入/删除、上传抵赖、拒绝服务等攻击.

2.1.3 隐私保护

Wang 等人[10]提出一种适用于众包系统的隐私保护激励机制.该机制采用文献[11]中的盲签名方案来实现用户匿名上传感知数据,应用延时加密服务(TLC),在给定的时间 T,平台发布公钥,所有用户都可以匿名使用它对上传信息进行加密.如图 4 所示,由系统平台向参与候选人发布任务和预算 B,并且设定工作候选人的竞价阈值 κ,工作候选人上传自己的竞价 b_j 和感知计划 t_i,平台根据边际效应条件

$$\frac{b_j}{t_j} \leqslant \kappa.$$

选择获胜的参与者,并给获胜参与者分配相应的报酬 p_j,获胜参与者上传感知数据.该激励机制中还提出了一种在线信誉更新算法(TORU),根据参与者提供感知数据的真实度更新参与者的信誉值,以便系统平台选择技能高的参与者.

Sun 等人[12]提出一种在线众包应用中异构用户的激励机制,可保证不同时刻到达用户在拍卖博弈中出价隐私.由众包发起者发布需要 n 位用户参与的感知任务,用户按顺序到达,每位用户 u_i 给出其所愿意参加的感知任务和执行对应感知任务的成本 b_i,每个用户完成的感知任务数量可以不同.众包发起者负责维护和更新一个布告板网站,该布告板用于发布在线激励机制的所有公开信息,包括拍卖细节、关于出价和任务数量限制的加密信息,用于验证支付正确性的加密支付阈值算法等.用户利用众包发起者的加密公钥 K_{ppub} 对其执行任务所消耗的成本 b_i、感知任务数量 l_i 和一个随机数 r_i 进行加密,并在签名后发布到布告板上:

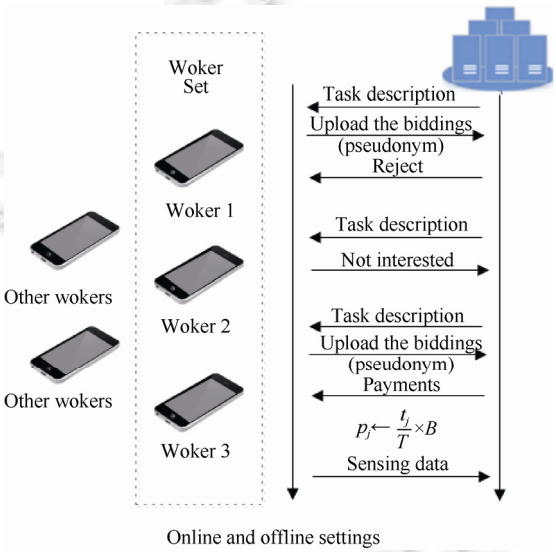


Fig.4 Workflow of the incentive mechanism of uploading sensing data

图 4 感知数据上传的激励机制流程

$$e_i = E_{K_{ppub}}(\tilde{b}_i|\tilde{l}_i|\tilde{r}_i)$$

$$c_i = E_{TPK}(e_i|s_i|TID)$$

$$sign_i(e_i|TID)$$

众包发起者与用户进行密封在线拍卖博弈,在截止时间 T 之前,众包者将所有收到的用户承诺 $c_1,c_2,\ldots,c_n$ 发布到布告栏,通过筛选条件 $\tilde{b}_i < \tilde{p}$,众包者将选出 n 位参与用户,并支付报酬

$$p = PS^{-1}(\tilde{p}).$$

此机制中还引入由 Rabin 和 Thorpe 命名的 Time-Lapse Cryptography Service(TLC)[13],以防止用户与众包发起者共谋而拒绝揭示在线拍卖博弈中选择的任务数量以及对应的成本.

2.1.4 小 结

在依赖于可信中心的激励机制中,可信中心为每个用户分配一定数额的电子货币,这些电子货币可作为用户激励其帮助者或任务完成者的奖励.表 1 给出了依赖可信中心的激励机制中现有文献满足的特性.可信中心在 P2P、DTN 等分布式网络环境中是不现实并难以实现的[10],即使可信中心存在也可能为了利益而作弊或出卖用户的私密信息,而且一旦被攻击者俘获或损坏,将影响整个系统的正常运行[14];现实生活中可信中心隐私泄露和崩溃事件频繁出现,如 2013 年酒店开房记录泄露、2014 年 e-Bay 泄露 1.45 亿用户数据、2016 年 10 月美

国 DNS 服务商 Dyn 遭受 DDoS 攻击.

Table 1 The characteristics of incentive mechanisms based on a trusted center

表 1 依赖于可信中心的激励机制满足的特性

文献	计算高效	个体理性	盈利	可信性	安全性	隐私保护	可扩展性
Ref.[5]		✓	✓				✓
Ref.[2]	✓	✓	✓	✓			✓
Ref.[6]		✓	✓				✓
Ref.[7]					✓		
Ref.[8]	✓	✓			✓	✓	✓
Ref.[9]	✓				✓	✓	✓
Ref.[10]	✓	✓	✓	✓			
Ref.[12]		✓	✓	✓		✓	

2.2 基于区块链的分布式激励机制

在基于区块链的分布式激励机制中,区块链本质上是一个去中心化的分布式账本数据库,由一串使用密码学安全验证和身份认证技术所产生的数据块组成,每个数据块包含交易的有效确认信息[15].基于区块链的密码货币是分布式可证安全的,非常适合作为分布式的激励机制.分布式激励机制不同于集中式,分布式激励机制不依赖于第三方可信中心,用户之间直接通过相应的电子货币交易,以激励其用户协作共同完成激励任务,但其有效实施离不开相应的确保机制.基于区块链的分布式架构下的确保机制,主要涉及到以下 3 个关键特性:即可信性、隐私保护和可扩展性.

2.2.1 可信性(truthful)

激励机制的可信性是所制定的激励策略能够给每个参与者一个激励,使每个参与者都有非负的效用,最大化其利益的同时也能达到所制定的激励目标,没有用户可以从谎报或欺骗中获益[16].

定价机制是常用来实现激励机制可信性的方法.Yang 等人[17]提出采用 Myerson 特性化机制设计原则实现了群智感知应用中的定价机制的可信性,通过牺牲感知服务器的效用,构造具有单调性的用户效用函数,给予获胜用户最大阈值的报酬,从而保证用户不能从谎报或作弊中获利.Anderegg 等人[18]提出了一种 MANET 中可信激励机制,通过 Vickrey-Clark-Groves(VCG)拍卖为最短路径上的中间节点设定相应的奖励,每个中间节点的奖励为其转发开销代价和参与转发给整条路由带来的新增开销代价的总和,每个节点给予的奖励将高于通过作弊或欺骗带来的奖励,从而保证每个中间节点都诚实报告自己的开销或相应的参数.Zhang 等人[19]提出一种可信的云资源分配拍卖机制,通过将支付函数设计成与分配资源和使用时间相关的单调函数和最大化云资源服务竞价者的利益,来保证云拍卖模型的可信性.Li 等人[20]提出一种认知无线电频谱可信拍卖机制,通过保证次用户竞拍价的可信和主用户提供频谱参数的可信来保证机制的可信性.

当密码货币作为激励机制时,由于没有对应的措施来限定节点的转账金额,节点可不按规定的定价策略来转账,造成了激励机制的不可信.Andrychowicz 等人[21]提出扩展 Bitcoin 交易语法,使其支持限时承诺功能,如图 5 所示,承诺方案包括:承诺阶段 *Commit* 和开放阶段 *Open*.在承诺阶段,承诺者 *C* 向账本 *Ledger* 发送交易承诺 $Commit_1$,$Commit_2$,…,$Commit_n$ 和相应金额的电子货币押金 *d*,账本记录 *n* 个未被赎回的交易承诺.在开放阶段,若承诺者 *C* 在某个限定时间 *t* 内完成承诺的任务,则向账本发送交易 $Open_1$,…,$Open_n$,若账本上没有交易 $Open_i$ 的记录证明交易未完成,交易接收者 P_i 将向账本发送交易 PayDeposit_i,从而获得相应金额的电子货币 *d* 补偿.此限时承诺机制还被用于两方[22]和多方安全计算[21],保证协议参与者遵守协议的规定,若参与方在协议执行完之前终止协议,也将会将其押金转给诚实的参与方.Kumaresan 等人[23]提出了基于 Bitcoin 的功能转账模型,通过 Bitcoin 构造形式化的模型来支持限时转账、承诺退还、押金补偿等功能,并通过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(noninteractive bounties)等密码学任务.

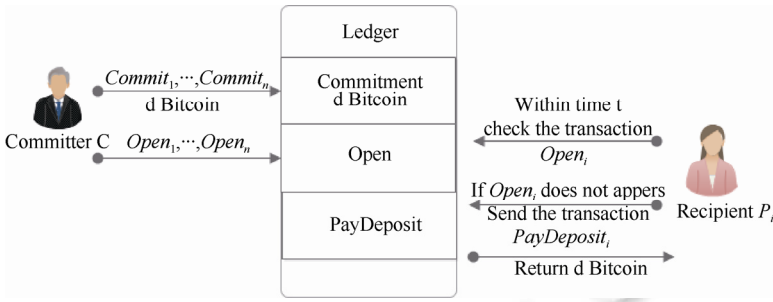


Fig.5 Workflow of time-limited commitment incentive scheme

图 5 限时承诺激励方案流程

2.2.2 隐私保护

激励机制的安全有效实施离不开验证工作,然而节点提供的验证信息会泄露其身份、位置、偏好等私密信息.由于分布式共识数据库记录所有的交易信息,基于区块链的激励机制将面临更严重的隐私问题[24].Biryukov 等人[25]指出 Bitcoin 系统中高达 60%用户的假名可关联到对应的 IP 地址.

已有一些研究工作用于解决密码货币面临的隐私问题.如图 6 所示,链 a 表示正常的 Bitcoin 交易历史,每个交易收链接到前一交易,Miers 等人[26]提出由用户在 Bitcoin 系统中产生新的电子货币 Zerocoin 来隐藏 Bitcoin 交易的关联性,在用户产生 Zerocoin 的同时押付相同数额的 Bitcoin,产生 Zerocoin 的用户根据其持有的秘密随机数,在 Bitcoin 公共的共识数据库上通过零知识证明其花费或回收 Zerocoin,如图 6 所示,从区块链中的数据无法确定产生 Zerocoin 与花费 Zerocoin 之间的联系,从而无法泄露其交易之间的关联性.针对 Zerocoin 泄露支付地址和数额问题,Ben 等人[27]利用一种非交互式零知识证明方法(zk-SNARKs),实现了强隐私保护的账本电子货币 Zerocash,可隐藏交易的原地址、目的地址和转账金额.Bonneau 等人[28]提出基于 Bitcoin 的匿名支付协议,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来保证用户 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,对于被动攻击者该协议能够达到全网络的匿名性,对于主动的攻击者该协议通过多个货币混淆节点来满足强匿名性的要求.

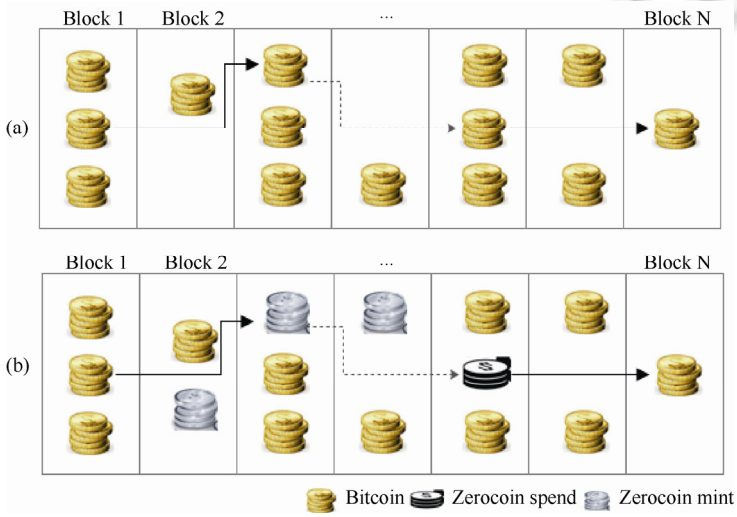


Fig.6 The privacy protection of Zerocoin

图 6 Zerocoin 隐私保护机制

2.2.3 可扩展性

基于区块链的激励机制的安全性依赖于共识机制,共识机制本身需要大量的通信和计算资源,随时间推移

交易数量会不断扩增,而节点的计算、存储和带宽资源有限,从而造成了交易处理瓶颈问题[29].

已有一些研究工作通过改进共识协议来解决交易处理瓶颈问题.Sompolinsky 等人[30]在分析 Bitcoin 交易处理吞吐量与数据块的大小和数据块产生速率之间的关系基础上,优化交易处理的等待时间以增加每个处理周期内的数据块的数量,同时保证安全性,但该方案没有考虑降低交易的验证代价.Poon 等人[31]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.Back 等人[32]提出将 Bitcoin 上的交易转移到其他密码货币的区块链上进行处理,从而增加交易处理的吞吐量.以上方法都运行在Bitcoin共识协议之上,没能解决Bitcoin底层协议的可扩展性.Kokoris等人[33]提出一种强共识协议,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,如图 7 所示,窗口内关键区块的产生者——矿工组成联合签名的成员,对微区块中的交易信息进行签名,从而减小 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 分钟以内.Loi 等人[34]提出一种公有链分布式共识协议,将系统中的节点随机划分成组,并行验证不同的交易,通过拜占庭协议达成组成员的共识,从而增强 Bitcoin 的交易处理能力,使得处理的交易数量随计算能力增强而线性增长,而且该协议能够抵御 1/4 计算能力的拜占庭攻击者.

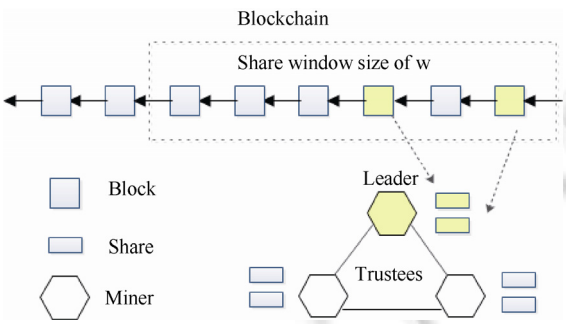


Fig.7 Collective signature scheme

图 7 联合签名方案

2.2.4 小 结

基于区块链的分布式激励机制在保障可信性、隐私保护、可扩展性上的研究工作尚处于起步阶段,未考虑矿工验证工作给激励机制设计带来的挑战.由于交易的验证工作由矿工完成,矿工可能会为最大化自身的利益而发起假冒攻击,甚至发起合谋攻击,造成激励机制的不可信;基于密码货币的激励机制需要矿工参与交易验证工作,矿工能从验证信息和交易关系中挖掘出节点的身份、位置、角色、任务分工等私密信息;虽然已有一些工作通过改进共识协议提高交易处理效率,但并非所有矿工都能验证任务,当交易数量超过矿工的处理能力,仍会出现交易处理瓶颈问题.表 2 给出了现有基于区块链的方案具有特性.

Table 2 The characteristics of incentive mechanisms based on blockchains

表 2 基于区块链的方案满足的特性

文献	计算高效	个体理性	盈利	可信性	安全性	隐私保护	可扩展性
Ref.[21]		✓	✓	✓	✓		
Ref.[23]		✓	✓	✓	✓		
Ref.[26]		✓			✓	✓	
Ref.[27]		✓			✓	✓	
Ref.[28]		✓			✓	✓	
Ref.[30]	✓				✓		✓
Ref.[31]	✓				✓		✓
Ref.[32]	✓				✓		✓
Ref.[33]	✓				✓		✓
Ref.[34]	✓				✓		✓

3 总结与展望

本文综述了基于电子货币的激励机制的现有工作,分析了依赖可信中心的激励方式存在权威欺骗和安全性问题,重点介绍了基于电子货币的分布式激励机制.虽然基于电子货币的激励机制在近几年得到了很多研究,但它仍是当前的研究热点之一,还存在许多问题有待进一步研究.

(1) 激励机制的执行可能需要大量的通信和计算资源,在系统的计算、存储、带宽资源有限的情况下如何设计激励最优方案有待进一步研究;

(2) 基于电子货币的激励机制应用较为广泛,但在激励过程中易泄露用户的隐私信息,在达到激励效果的同时,安全性有待提高;

(3) 激励机制应用在在众包、DTN 等动态网络中参与任务的节点通常是不确定的,若为激励每个节点而生成交易,交易数量将非常庞大,而且并非所有矿工都能验证任务,当交易数量超过矿工的处理能力,仍会出现交易处理瓶颈问题.

References:

[1] EMarketer, Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year. https://www.emarketer.com

[2] Yang D, Fang X, Xue G. Truthful incentive mechanisms for *k*-anonymity location privacy. In: Proc. of the IEEE INFOCOM 2013. IEEE, 2013. 2994−3002.

[3] Wang Y, Cai Z, Yin G, Gao Y, Tong X, Wu G. An incentive mechanism with privacy protection in mobile crowdsourcing systems. Computer Networks, 2016,102:157−171.

[4] Zhang XL, Yang Z. Wei S, Liu YH,Tang SH, Xing K, Mao XF. Incentives for mobile crowd sensing: A Survey. IEEE Communications Surveys & Tutorials, 2016,18(1):54−67.

[5] Kang X, Wu Y. Incentive mechanism design for heterogeneous peer-to-peer networks: A Stackelberg game approach. IEEE Trans. on Mobile Computing, 2015,14(5):1018−1030.

[6] Peng D, Wu F, Chen G. Pay as how well you do: A quality based incentive mechanism for crowdsensing. In: Proc. of the 16th ACM Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2015). 2015.

[7] Mahmoud ME, Shen X. ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks. IEEE Trans. on Mobile Computing, 2011,10(7):997−1010.

[8] Nix R. Efficient incentive compatible secure data sharing. Dissertations & Theses - Gradworks, 2012.

[9] Lai C, Zhang K, Cheng N, Li H, Shen X. SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. IEEE Trans. on Intelligent Transportation Systems, 2017, 1−16.

[10] Wang Y, Cai Z, Yin G, Gao Y, Tong X, Wu G. An incentive mechanism with privacy protection in mobile crowdsourcing systems. Computer Networks, 2016,102:157−171.

[11] Huang Z, Wang Y, Chen K. Generalization and improvement of Nyberg-Rueppel message recovery blind signatures. Journal of China Institute of Communications, 2005.

[12] Sun J, Ma H. Privacy-Preserving verifiable incentive mechanism for online crowdsourcing markets. In: Proc. of the Int'l Conf. on Computer Communication and Networks. IEEE, 2014. 1−8

[13] Rabin MO, Thorpe C. Time-Lapse cryptography. Technical Report, TR-22-06, 2006.

[14] Jacob F, Mittag J, Hartenstein H. A security analysis of the emerging p2p-based personal cloud platform maidsafe. In: Proc. of the 14th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom 2015). 2015.

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

[16] Restuccia F, Das SK, Payton J. Incentive mechanisms for participatory sensing: Survey and research challenges. ACM Trans. on Sensor Networks (TOSN), 2016,12(2):1301−1340.

[17] Yang D, Xue G, Fang X, Tang J. Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones. Biological Cybernetics, 2016 24(3):1732−1744.

[18] Luzi A, Eidenbenz S. Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: Proc. of the 9th Int'l Conf. on Mobile Computing and Networking (Mobicom 2003). 2003.

[19] Zhang H, Jiang H, Li B, Liu MF, Liu CJ, Vasilakos A. A framework for truthful online auctions in cloud computing with heterogeneous user demands. IEEE Trans. on Computers, 2016,65(3):805−818.

[20] Zhang TJ, Li Z, Safavi-Naini R. Incentivize cooperative sensing in distributed cognitive radio networks with reputation-based pricing. In: Proc. of the 33rd Annual IEEE Int'l Conf. on Computer Communications (INFOCOM 2014). 2014.

[21] Andrychowicz M, Dziembowski S, Malinowski D, Mazurek L. Secure multiparty computations on bitcoin. In: Proc. of the 35th IEEE Symp. on Security and Privacy (S&P 2014). 2014.

[22] Andrychowicz M, Dziembowski S, Malinowski D, Mazurek L. Fair two-party computations via bitcoin deposits. In: Proc. of the 18th Financial Cryptography and Data Security (FC 2014). 2014.

[23] Ranjit K, Bentov I. How to use bitcoin to incentivize correct computations. In: Proc. of the 21st ACM Conf. on Computer and Communications Security (CCS 2014). 2014.

[24] Androulaki E, Karame G, Roeschlin M, Scherer T, Capkun S. Evaluating user privacy in bitcoin. In: Proc. of the Financial Cryptography and Data Security (FC 2013), 2013.

[25] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in bitcoin P2P network. In: Proc. of the 21st ACM Conf. on Computer and Communications Security (CCS 2014). 2014.

[26] Miers L, Garman C, Green M, Rubin AD. Zerocoin: Anonymous distributed E-Cash from bitcoin. In: Proc. of the 34th IEEE Symp. on Security and Privacy (S&P 2013). 2013.

[27] Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from bitcoin. In: Proc. of the 35th IEEE Symp. on Security and Privacy (S&P 2014). 2014.

[28] Bonneau J, Narayanan A, Miller A, Clark J, Kroll J, Felten E. Mixcoin: Anonymity for bitcoin with accountable mixes. In: Proc. of the 18th Financial Cryptography and Data Security (FC 2014). 2014.

[29] Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In: Proc. of the 36th IEEE Symp. on Security and Privacy (S&P 2016). 2016.

[30] Sompolinsky Y, Zohar A. Accelerating bitcoin's transaction processing fast money grows on trees, not chains. Cryptology ePrint Archive, Report 2013/881, 2013.

[31] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016. http://lightning:network/lightning-network-paper:pdf,.

[32] Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, Poelstra A, Timon J, Wuille P. Enabling blockchain innovations with pegged sidechains. 2014. https://blockstream:com/sidechains:pdf

[33] Kogias EK, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. In: Proc. of the 25th USENIX Security Symp. (Security 2016). 2016.

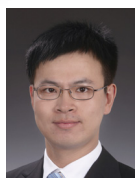
[34] Luu Loi, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proc. of the 23rd ACM SIGSAC Conf. on Computer and Communications Security (CCS 2016). 2016.

何云华(1987－),男,湖北荆门人,博士,讲师,主要研究领域为区块链技术,工控安全,隐私保护.

耿子烨(1996－),女,本科生,主要研究领域为区块链技术,工控安全,隐私保护.

李红(1989－),男,博士,助理研究员,主要研究领域为区块链技术,工控安全,隐私保护.

孙利民(1966－),男,博士,研究员,主要研究领域为物联网技术,工控安全.



李旭(1983－),男,硕士,主要研究领域为物联网,车联网.