基于隐私保护的法定数字货币激励机制

陈 晓, 吕欣冉, 刘 志

(中汇信息技术（上海）有限公司,上海 201203)

摘 要: 多国央行已开展基于分布式账本技术的法定数字货币研究，唯有英国公开了法定数字货币框架 RSCoin 的交易记账架构,并设计激励机制鼓励授信机构提供协作记账服务。但是，RSCoin 中的激励机制没有考虑授信机构差异性的服务成本，也没有给出明确的报酬分配方案。本文充分考虑授信机构差异性的隐私成本，首先建立央行和授信机构的激励模型，明确授信机构的报酬，首次提出一种既保护授信机构隐私成本，又保证授信机构诚实报价的激励机制 POPTIM。POPTIM 先通过编码哈希方法对授信机构的协作报价进行加密，然后基于隐私保护排序算法选择待支付的授信机构，最后基于同态加法算法计算各授信机构获得的报酬。通过理论分析可知，POPTIM 机制具有隐私安全、计算高效、满足授信机构个体理性和保证授信机构诚实报价的性质。

关键词: 分布式账本技术；隐私保护；数字货币；激励机制；保证诚实报价的机制

中图法分类号: TP311

A Truthful Incentive Mechanism for Digital Currency based on Privacy Protection

CHEN Xiao, LV Xin-Ran, LIU Zhi,

(CFETS Information Technology(Shanghai).Co., Ltd. Shanghai 201203, China)

Abstract: Many national central banks have conducted legal digital currency research based on distributed ledger technology, but only the UK has disclosed the accounting structure of the legal digital currency framework RSCoin, and proposed the incentive mechanisms to encourage mintettes to provide honest collaborative accounting services. However, this mechanism does not take into account the differential service costs of mintettes, nor does it give a definite compensation distribution. This paper fully considers the privacy costs of the mintettes, establishes the incentive model of the central bank and mintettes, and clarifies the methods to compensate mintettes. To our knowledge, in the legal digital currency research area, we first propose an incentive mechanism POPTIM, that not only protects the private cost of the mintettes, but also guarantees the mintettes report their truthful bidding prices to the central banks. In POPTIM, we first encrypts the biddings of mintettes by coding hash encryption method, then adopt privacy-preserving sorting algorithm to select the winner mintettes, and finally calculate the reward of mintettes based on the homomorphic addition algorithm. Based on analysis, we show that the mechanism is privacy security, computationally efficient, individually rational and truthful simultaneously.

Key words: distributed ledger technology; privacy security; digital currency; incentive mechanism; truthful mechanism

随着比特币的诞生，分布式账本技术（Distributed ledger technology，简称 DLT）作为一种新型数字账本技术逐渐进入公众视野，为法定数字货币的实现提供了新颖的技术视角。法定数字货币在发行成本、流通安全性、监管效率等方面有着天然的优势，为货币政策、金融监控措施的制定提供有力支持。首先，节省了纸质货币的印制和运输成本，商业银行也可以通过电子化方式直接完成货币转移，减少了大额运钞的设备和人力。其次，法定数字货币在流通过程中，既满足消费者的数字化、智能化消费体验需求，又有利于央行可以实时掌控货币流通的完整、真实数据。最后，DLT 技术简化了支付环节和提高了结算的完成度，大大降低交易成本和结算风险，提高了跨境支付的实时性。

目前，多国政府及其央行已对分布式账本技术发表了积极看法，并以降低货币体系运行成本、扩大电子应用领域、以及巩固全球经济金融领先地位为目标，尝试采用 DLT 来建设法定数字货币原型系统，比如，英国、德国、法国、加拿大、新加坡和中国等[1]。还有一些国家的央行虽未公开发布法定数字货币的研究，但已有相关人员公开支持了基于 DLT 的法定数字货币设想，以探索全球贸易交换媒介的替代品，比如美国。

虽然多数国家已开展法定数字货币研究，但英国央行提出的 RSCoin 系统[2]是目前唯一公开的包含交易记账过程的法定数字货币框架。在 RSCoin 框架中，央行通过采用向提供协作服务的授信机构给与一定的报酬，并对懒散或行为不当的授信机构给与经济处罚的方式，鼓励授信机构提供诚实的协作服务。此框架的激励机

制没有考虑授信机构提供协助服务的差异性成本，也没有给出明确的报酬分配方案，这不利于充分鼓励授信机构提供服务。

本文基于 RSCoin 框架,充分考虑授信机构隐私的差异性成本，建立央行和授信机构的激励模型，明确授信机构的报酬确定方案，首次既保护授信机构隐私成本，又保证授信机构诚实报价的激励机制 POPTIM（private cost protection truthful incentive mechanism）。POPTIM 先通过编码哈希加密方法对授信机构的协作报价进行加密编码，然后基于隐私保护排序算法选择待支付的授信机构，最后基于同态加法算法计算各授信机构获得的报酬。通过理论分析可知，POPTIM 机制具有隐私安全、计算高效、满足授信机构个体理性、以及保证授信机构诚实报价的性质。

1 现状与分析

1.1 基于分布式账本的法定数字货币研究

目前，新加坡金融管理局、欧洲央行和日本央行、美国、英国等都陆续投入基于分布式账本的法定数字货币的研究。

1.1.1 英国

在 RSCoin 框架中[2]，记账的参与方由中央银行、授信机构、和终端用户三方构成，如图 1 所示。为减轻央行核实交易和维护系统的压力，RSCoin 采用了“央行—商业银行”的二元分层体系结构，由多家授信机构核实交易并存储部分交易数据，而央行维护完整的全部交易数据。下面简要介绍各参与方的主要作用：

- 央行完全控制货币的产生，拥有总账本的完全控制权，并通过管理和汇总从授信机构获得的交易数据，向整个系统发布最终交易数据。央行定期向整个系统发布授信机构列表 $M=\{m_1,m_2,...\}$，并由其附属机构向移动用户提供告知维护交易输入授信机构集合 I 和输出授信机构集合 O 的服务[13]；
- 授信机构负责收集和校验终端用户提交的交易信息，可将已验证的交易写入初级账本，并提交到央行。每个授信机构都保存未消费交易输出 UTXO（unspent transaction outputs）、消费交易输入集合 PSET 和初级账本交易集合 TXSET；
- 终端用户负责发起交易和转发授信机构之间的交易验证信息，终端用户先从央行附属机构获得交易输入授信机构和输出授信机构列表，然后向能验证输入交易的授信机构集合 I 发起交易验证，并收集验证信息，之后向记录交易和提供交易输出的授信机构集合 O，发送交易及验证信息递。

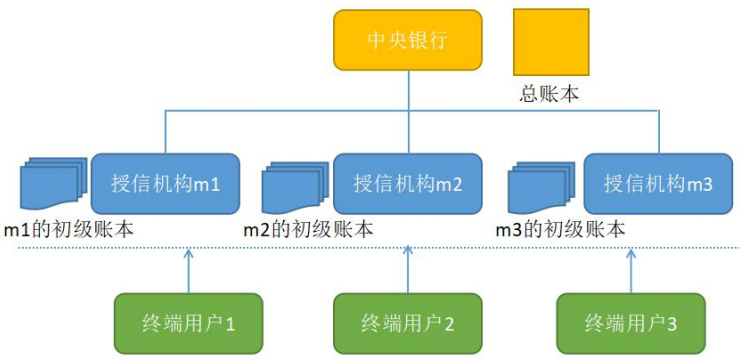

图 1 RSCoin 总体结构图[11]

在文献[2]中，央行向提供服务的授信机构给与一定的报酬，但没有考虑代理机构协作成本的差异性，也没有给出明确的报酬分配方案，这不利于充分鼓励授权代理机构提供优质服务，也不利于中央银行预算方案的制定。

1.1.2 新加坡

2016 年 11 月，新加坡金融管理局（Monetary Authority of Singapore，简称 MAS）启动了 Ubin 项目，致力于探讨 DLT 在金融生态系统的实用性，以降低跨境支付和证券结算的风险和成本。该项目采用分阶段研究模式，目前已完成了前两个阶段的探索。在第一阶段中，该项目研发了一个基于以太坊 DLT 平台及连续存托凭证货币模型的数字新币原型系统，并集成在现有的 MAS 支付结算的基础设施中，实现了使用数字新币进行银行同业间实时支付结算的目标[3]。数字新币原型系统由 MAS 与银行同业机构共同运行，由电子支付系统（MAS Electronic Payment System，简称 MEPS+）和基于以太坊的 DLT 系统组成。第二阶段中，该项目重点探索了在保护交易隐私的前提下，基于 DLT 的实时支付结算（Real Time Gross Settlement，简称 RTGS）系统实现多边净额结算的能力[4]。

1.1.3 美国

2013 年 4 月 13 日，JP Koning 在一篇博客中首次提出了基于分布式账本的 FEDCoin 模型，以降低支付系统对中心化处理的依赖[5]。2015 年，美国圣路易斯联邦储备银行副总裁 David Andolfatto 在 P2P 金融系统国际研讨会上，公开支持 FEDCoin 模型，以实现全球任何人都可以通过数字钱包和互联网访问，使用 FEDCoin 进行低成本的点对点交易[6]。虽然目前该设计仍处于理论阶段，但是货币专家 Doug Casey[7]认为只有美联储发行法定数字货币，才能最大程度地巩固美国经济中心的地位。FEDCoin 模型取消了“央行—商业银行”二元结构，允许个人或企业直接在央行开户[8]，从而可增强美联储对广义货币总量的控制能力。

1.1.4 欧盟与日本

2016 年 12 月，日本央行（Bank of Japan,BOJ）和欧洲中央银行(European Central Bank, ECB) 第一次公开发布了名为“Stella”的联合研究项目,如文献[9]。第一阶段的研究中，日本央行和欧洲中央银行认为，DLT 在金融基础设施的应用将使得金融交易更加安全、快速，同时可降低交易成本。2018 年 3 月，BOC 和 ECB 发布了 Stella 的第二阶段研究成果，这一阶段主要是探讨在基于 DLT 的目前国际债券标准结算方式 DVP(Delivery Versus Payment,券款对付)的概念性设计。DVP 指在债券交易的结算日，交易双方同步进行债券交割与资金支付，是交易双方风险对等的一种高效率低风险的结算方式。

1.2 比特币等虚拟代币的激励机制

目前，多数的虚拟代币都有激励机制。多数虚拟代币通过“挖矿奖励”和获得记账交易费来鼓励记账节点积极参与记账活动，例如，比特币、以太币等。也有一些虚拟代币通过“交易即挖矿”的方式分配虚拟代币，以提高社区的活跃程度，例如 FT（FCoin Token）。

1.2.1 比特币

比特币由中本聪在 2009 年首次提出，是一种支持 P2P 支付结算的虚拟代币[10]。比特币的发行不依赖于某个机构，而是根据指定算法，由记账节点（俗称“矿工”）通过大量的计算而产生。一旦矿工从待加入的交易池中，找到符合一个交易集合构成新区块，其计算的哈希值符合特定规则（俗称“挖矿成功”），则可获得一定的比特币。比特币的总发行量为 2100 万，在最开始的四年，每个挖矿成功的记账节点将奖励 25 个比特币，每过四年就减少一半。大约到 2140 年的时候，比特币将完成发行。除了挖矿奖励，记账节点还会获得打包交易的手续费作为额外奖励。所有交易在被打包形成新区块时，需要向矿工支付一定的费用。因此，随着系统的运行，矿工的奖励来源逐渐依赖交易手续费。

1.2.2 以太币

以太币是以太坊平台产生的虚拟代币。以太坊[11]是在 2014 年初 Vitalik Buterin 在北美比特币大会上首次谈及,是分布式账本技术 2.0 的一个成功的案例。以太坊也采用挖矿奖励和交易费的形式来鼓励记账节点积极记账。以太坊的挖矿奖励是采用“普通区块奖励+叔块奖励+叔块引用奖励”的机制，矿工构造普通区块的奖励是 5 以太币。如果普通区块包含了叔块，每包含一个叔块还可以得到额外固定奖励 5/32 以太币。在以太坊中，交易发送这在发送每个交易时会设定费用，这些费用将是记账节点的奖励。

1.2.3 FT

FT 是虚拟代币交易平台 FCoin 发行的通证，是 FCoin 社区治理的基石[12]。FT 总发行量为 100 亿，其中 51%比例按照“交易即挖矿” 逐步分配给交易用户；而其余 49%比例的 FT 则通过预先发行的方式被基金、团队、合作伙伴及私募投资者所持有。“交易即挖矿”实际上就是一种基于平台币的个人交易手续费返还机制。通过此机制，平台会持续不断的将大部分收入分配给 FT 的持有者。同时，通过发起智能合约投票，FT 持有者也有权参加社区管理，例如参与业务决策。

2 系统模型与重要概念

本节先介绍 POPTIM 激励模型，然后再介绍本文的预备知识。

2.1 激励模型

POPTIM 激励机制参与方与 RSCoin 相同，也是央行、授信机构与终端用户。参与角色除了具有 RSCoin 中的职责外，授信机构还会向央行提供加密报价，央行根据授信机构的报价以及统计的服务质量，确定提供报酬的授信机构以及相应金额。

与 RSCoin 相同，在 POPTIM 中也需多个授信机构分别验证每个交易输入唯一和有效，才能记入总账本。这是由于一笔交易可能有多个交易输入，即一笔交易的付款方可能汇集多个未消费交易输出 UTXO，才能凑足向收款方支付的数额。例如，一笔交易是 Alice 向 Bob 支付 10 元，Alice 使用从 Cal 获得的 8 元以及从 Den 获得的 2 元作为交易输入。授信机构分别验证交易输入资金没有被消费过才认为是有效，即确认 Alice 使用的 8 元和 2 元是 UTXO。为防止授信机构提供虚假信息，提高交易的可信性，一个交易输入需要多个授信机构分别检验此输入是否属于 UTXO，然后以类似投票计数的方式，根据少数服从多数的规则，确定此交易输入是否是新的可以加入账本的有效交易。

为鼓励授信机构积极参与记账活动，央行可采用投标的方式，通过引入竞争选择性价比高的授信机构给与一定的报酬。在提供交易验证和构建初级账本过程中，授信机构 m_i 会消耗分别消耗的资源成本 c_i 和 $c_i^{'}$。此成本是授信机构的隐私信息，且各个授信机构的参与成本不同。如果央行主观给定统一固定的报酬，既不利于吸引成本较高的授信机构参与，也不利于央行在保证一定服务质量的基础上，尽可能的降低报酬支付。

假设新加入系统的授信机构 m_i 将提供验证和保存单个 UTXO 的报价分别为 b_i 和 $b_i^{'}$。为保护授信机构的隐私成本，授信机构将报价 b_i 和 $b_i^{'}$ 加密后，再向央行提交。虽然授信机构根据自身存储的信息，参加多次单位任务的竞选。但是考虑到任务具有同质性，授信机构只需向央行提交一次加密报价。受网络传输的影响，授信机构 m_i 在不同时间 t 的服务质量 q_{it} （如返回交易验证结果正确性和速度等）可能会不同。

基于 RSCoin 交易记账过程，以交易输入 1 和交易输出 2 为一个交易为例，本模型的交易记账与激励机制的主要过程如下图所示：

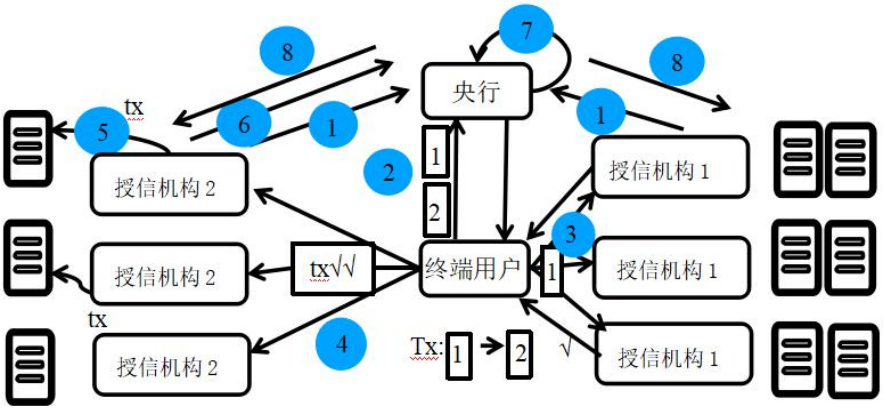

图 2 交易验证及激励过程

（1）对于新加入的授信机构根据 3.2 节介绍的加密算法，将加密处理后的 b_i 和 $b_i^{'}$，向央行发送加密报价 $B_i(b_i)$ 和 $B_i(b_i^{'})$，央行保存其加密报价，而对于已加入系统的授信机构，央行读取已存储的加密报价；

（2）终端用户向央行询问获知验证交易输入 1 的授信机构集合 I_1 和记录未消费交易输出 2 的授信机构集合 O_2；

（3）终端用户向授信机构集合 I_1 发送验证交易输入 1 的请求，并统计验证结果；

（4）当验证结果足够一致时，终端用户向授信机构集合 O_2 发送交易输入 1 的验证结果和交易；

（5）当 O_2 中的授信机构验证信息后，将未消费输出交易记录在 UTXO 列表中，并将交易添加在初级账本中。

（6）O_2 中的授信机构向央行发送初级账本、I_1 的交易验证结果。

（7）按照一定原则，央行将初级账本加入总账本，并根据观察记录 O_2 和 I_1 授信机构的记账质量。

（8）央行根据 3 节介绍的授信机构选择规则与算法、授信机构报酬确定算法，确定 I_1 和 O_2 集合中给与报酬的授信机构以及加密报酬。即计算在 $T_i - T_{i-1}$ 期间，需要向所有授信机构支付的报酬，数据格式如图 3 所示。为增加报酬确认算法的可信性，授信机构选择算法和报酬确定算法也可以写入智能合约。

授信机构 ID	获胜的交易编号	时间戳	加密报酬金额

图 3 授信机构单次获得的加密报酬统计格式

2.2 预备知识

结合本文场景，下面介绍机制设计的重要概念。

（1）计算高效[15]：针对任意一个 UTXO 记录，能够在多项式时间内选择授信机构集合并确定其报酬。

（2）个体理性[16]：针对任意一个 UTXO 记录，被选择的授信机构验证或形成初级账本获得的效用是非负

的。

（3）弱占优策略（weakly dominate strategy）[16]无论其他授信机构采用何种投标策略，授信机构利用某一个投标策略获得的效用不低于其他投标策略获得的效用。

（4）保证诚实报价机制（truthful mechanism）[17]：无论其他授信机构的报价策略，风险中性的授信机构，其诚实报价获得的效用不低于其他策略获得效用。

（4）0 编码[15]：令 S 二进制表示 $s=s_n s_{n-1}...s_1$ 如下，则 $\mathrm{E}_s^0=\{s_n s_{n-1}...s_{i+1}1 \mid s_i=0,1\le i\le n\}$ 是其 0 编码集合，其中 n 为位数。

（5）1 编码[15]：令 S 二进制表示 $s=s_n s_{n-1}...s_1$ 如下，则 $\mathrm{E}_s^1=\{s_n s_{n-1}...s_i \mid s_i=1,1\le i\le n\}$ 是其 1 编码集合，其中 n 为位数。

3 激励机制设计

针对 RSCoin 框架，本节考虑终端用户发起交易动态到达、保护授信机构成本隐私的情况，设计激励机制 POPTIM，实现央行和授信机构的预期效用最大化。虽然一笔交易待验证的输入（之前产生的 UTXO）可能有多个，也可能会产生多个新的 UTXO，但每个 UTXO 可以独立记录和验证。由于鼓励授信机构参与验证交易输入和将交易输出写入初级账本的方法相似，本文以验证单个交易输入的 UTXO 为例介绍 POPTIM。

3.1 授信机构选择规则

为提高系统的安全性，抵抗拜占庭攻击，交易输入和输出的每个 UTXO 都需至少被一定数量的授信机构一致性验证和记录保存。假设一个 UTXO 需要至少被 $k(k\ge 2)$ 个授信机构一致性验。如果授信机构 m_i 提供真实的交易认证，服务质量 $q_i=1$，否则 $q_i=0$。央行希望向性价比最高的 k 个授信机构支付报酬，以实现自身效用 π_0 最大化，如公式（1）。其中，α 为服务质量转换为效用计算的参数，W 为选择的授信机构集合，且 $|W|=k$。

$$\max \pi = \sum_{i\in W}(\alpha q_i - b_i) \tag{1}$$

3.2 授信机构投标方案

授信机构根据协助成本和预期效用函数，确定投标价格。授信机构 m_i 的预期效用函数 u_i，如公式（2）所示。由于授信机构也是自私理性的，希望在参与过程中实现自身收益最大化，因此会确定最优的投标价格，并告知央行。根据下文理论分析可知，在本激励机制中，授信机构的最优投标价格为隐私成本价格。

$$u_i = b_i - c_i \tag{2}$$

为保护授信机构 m_i 投标价格 b_i 的隐私性，授信机构采用文献[19]的编码哈希加密方法和文献[20]的 Paillier 加法同态加密方法，将生成安全比较报价元组 B_i 提交给央行。具体的加密过程概述如下：

（1） m_i 使用私有密钥 K_i 对报价 b_i 进行加密，生成 $K_i(b_i)$；

（2） m_i 对报价 b_i 进行 0-1 编码，得到 0 编码报价 $\mathrm{E}_{b_i}^0$ 和 1 编码报价 $\mathrm{E}_{b_i}^1$。

（3） m_i 使用散列消息身份验证码(Hashed Message Authentication Code,简称 HMAC)的密钥 g_i 对 $\mathrm{E}_{b_i}^0$ 和 $\mathrm{E}_{b_i}^1$ 哈希运算，生成安全比较 0 编码报价 $H_{g_i}(E_{b_i}^0)$ 和安全比较 1 编码报价 $H_{g_i}(E_{b_i}^1)$。

（4）使用文献[17]加法同态加密方法，使用央行的公钥以及在一定范围内的随机数，对报价 b_i 进行加密，生成同态密文报价 $\mathrm{P}_A(b_i)$.

（5） m_i 将加密处理后的报价相关密文，安全比较报价 $B_i(b_i)=\{\mathrm{K}_i(b_i),bH_{g_i}(E_{b_i}^0),H_{g_i}(E_{b_i}^1),P_A(b_i)\}$ 向央行提交。

3.3 授信机构选择算法

在将授信机构提交的初始账本加入最终账本过程中，央行能知晓提供正确服务的授信机构集合 M，即对于在集合中的授信机构，服务质量为 1， $q_i=1,\forall m_i\in M$。

为最大化自身收益，央行在授信集合 M 中，选择报价最低的前 k 个授信机构支付报酬。由文献[18]可知，当且仅当 0-1 编码集合 E_x^1 与 E_y^0 有同一个元素时，则 $x>y$。而根据文献[18]的衍生文献[19]可知，当且仅当 $H_{g_x}(E_{b_x}^1)\cap H_{g_y}(E_{b_y}^0)\neq\varnothing$，则 $x>y$。因此，我们可以对加密报价进行两两比较。在此基础上，可以使用诸如归并排序、堆排序等排序算法，根据授信机构提交的安全比较报价中的安全比较编码报价进行排序。例如，文献[16]对安全比较编码进行归并排序，然后选择报价最低的前 k 个授信机构 M_k 支付报酬。

3.4 授信机构报酬确定

由于授信机构的参与成本是私有信息，作为自私的授信机构总希望能尽可能多的获得报酬，可能会存在虚高报价的情况。如果授信机构虚高报价，央行将会根据虚假的信息来选择授信机构，这不利于系统稳定。

为了鼓励授信机构提供真实的报价（即成本价格），我们采用 Vickery 拍卖的支付原则，被选择的授信机构的报酬等于他给其他竞争者带来的外部性。假设 m_i 在选择中获胜，其带给其他竞争者的外部性等于没有其报酬计算公式如公式（3），其中 $\pi_{(k+1)}$ 为授信机构向央行提供第 $(k+1)$ 高的非负效用， $q_{(k+1)}$ 和 $b_{(k+1)}$ 分别为此授信机构的服务质量和报价。

$$p_i=\alpha q_i-\pi_{(k+1)}=\alpha q_i-(\alpha q_{(k+1)}-b_{(k+1)}) \tag{3}$$

由授信机构选择算法可知，央行从提供正确服务的授信机构 M 中选择需要支付的授信机构。因此，公式（3）可以整理为公式（4），即第一个落选的授信机构提供的报价。

$$p_i = b_{(k+1)} \tag{4}$$

根据授信机构提交的安全比较报价元组 $B_{(k+1)}(b_{(k+1)})$，央行在获胜信息记录中记下报酬 $p_i = \mathrm{P}_A(b_{(k+1)})$。

由加法同态的性质可知，$\mathrm{P}_A(x+y) = \mathrm{P}_A(x) \oplus \mathrm{P}_A(y)$，其中在文献[17]的 Paillier 中，$\oplus$ 指密文的相乘运算。所以，在 T_i 时刻，根据央行的投标获胜信息记录，将授信机构在 $T_i - T_{i-1}$ 期间获得的加密报酬相加再解密，获得金额就是此授信机构在这段时间获得的报酬。

4 激励机制分析

本节分别分析 POPTIM 具有的隐私安全、计算高效、满足授信机构个体理性和保证授信机构诚实报价的性质。

4.1 隐私安全

在本机制中，授信机构 m_i 的隐私成本信息经过加密处理（如 4.2 描述），形成安全比较报价 $B_i(b_i) = \{\mathrm{K}_i(b_i), H_{g_i}(E_{b_i}^0), H_{g_i}(E_{b_i}^1), P_A(b_i)\}$。对于密文 $K_i(b_i)$ 和 $P_A(b_i)$ 说，私钥只有 m_i 持有，央行利用密文破解相应明文数据难度大。对于经过 0-1 编码和 HMAC 处理的 $H_{g_i}(E_{b_i}^0)$ 和 $H_{g_i}(E_{b_i}^1)$，由于哈希运算的逆向推理计算复杂，因此获得明文报价的难度也大。因此，本文的激励机制能在保护隐私的情况下，对密文排序和密文相加。

4.2 计算高效

在本机制中，最复杂的计算是在授信机构选择算法中，对安全比较 0 编码报价和安全比较 1 编码报价进行比较运算。相较于传统的堆排序，在比较过程中还需要对编码集合进行是否存在交集的检验。令二进制编码长度为 n，则密文交集检验的计算复杂度为 $O(n^2)$。令授信机构集合个数为 $|M|$，选择算法的计算复杂度为 $O(n^2|M|\log|\mathrm{M}|)$。根据计算高效的定义，本机制具有计算高效性。

4.3 个体理性

在授信机构选择算法中可知，已选获胜的授信机构报价明文与首次落选的授信机构报价明文的关系为 $b_{(1)} \le b_{(2)} \cdots \le b_{(k+1)}$。其中 $b_{(\mathrm{i})}$ 为第 i 个获胜授信机构的报价。由授信机构报酬确定算法可知，已选获胜的授信机构获得报酬为 $b_{(k+1)}$。由于本机制能够保证候选用户诚实报价，即 $b_{(i)} = c_{(i)}$，则根据公式（2）中授信机构的效用计算可知，已获胜的授信机构获得的效用 $u_{(i)} = b_{(k+1)} - c_{(i)} \ge 0$ 为非负。因此，本机制能保证个体理性。

4.4 保证诚实报价机制

如文献[18]介绍，在本文采用的 VCG 机制中，提供真实价格（即最低价格 $b_{(i)} = c_{(i)}$ ）是授信机构的弱占优策略。由弱占优策略的定义和保证诚实报价机制的定义可知，本机制能够保证授信机构诚实报价。

5 激励机制扩展

结合我国法定数字货币研究，介绍 POPTIM 激励机制在我国法定数字货币的适用性，以及扩展的激励机制。

5.1 适用性分析

我国数字货币研究所的姚前所长在文献[19]指出，我国遵从 “中央银行—商业银行”的二元结构建设法定数字货币体系。这种以分层组网架构实现交易记录的管理，与 RSCoin 框架有相似之处，都可以采用本文建立的投标模型，将央行抽象是发布任务的采购方，授信机构或商业银行是完成任务的投标方。因此，如果我国央行也在线选择协助记账的授信机构，那么本 POPTIM 机制也可适用于我国法定数字货币系统。

5.2 基于信贷拍卖的扩展

姚前所长在文献[23]提出了我国法定数字货币发行设计框架，指出央行可通过信贷拍卖机制向商业银行或授信机构发行法定数字货币。因此，除直接获得报酬外，商业银行近期承担的协作服务数量和质量，可以直接或间接影响商业银行在信贷拍卖中获得的法定数字货币，从而鼓励商业银行积极参与协作。

5.3 基于数字纪念币的扩展

除了直接支付报酬外，央行还可以根据授信机构提供协作的数量和质量，确定向授信机构购买数字纪念币的数量。为激励授信机构参与数字货币和数字纪念币，授信机构可以对一定数量的数字纪念币以自主定价的方式发放。有别于现有的实体纪念币，数字纪念币的形态可以随着持有人的变化、交易的次数、时间而发生演变，这增加数字纪念币的独特性，提高了数字纪念币交易的趣味性，以及熟悉纪念币的收藏价值。例如，工商银行与建设银行数字签名发出的数字纪念币，主体形态相同，但可能颜色会有变化；不同购买人购买数字纪念币也可能会使纪念币的形态发生变化。

当市场对数字纪念币的预期强烈时，授信机构可以通过买卖数字纪念币的差额获得收益，从而可以获得除了验证交易或构建初级账本之外的收入。随着期望收藏和交易数字纪念币的用户增多，授信机构获得的记录报酬会增多，同时数字纪念币价值提升，也使得日后首次发放数字纪念币获得的收益更大，从而形成了数字纪念币和法定数字货币生态的自主良好。

由于我国人口较多，直接运行法定数字货币系统的风险和压力较大，而通过运行法定数字货币系统积累经验，可以为法定数字纪念币的发行和运营奠定坚实基础。这是因为数字纪念币与法定数字货币有一定的相似性，例如其记账结构依然可以遵循“中央银行—商业银行”的二元体系，公民也可直接参与等，其运营经验具有借鉴意义。而数字纪念币的发行数量具有可控性、经济风险较低且可由授信机构在不同时间发放，系统并发性压力低，因此，数字纪念币上线运营的压力远小于便于实践运行。

6 总结与启示

在法定数字货币研究领域，本文基于 RSCoin 框架，充分考虑授信机构差异性的隐私成本，建立央行和授信机构的激励模型，明确授信机构的报酬确定方案，首次提出在不泄露授信机构隐私成本信息的基础上，能够保证授信机构诚实报价的激励机制 POPTIM。理论分析此机制具有隐私安全、计算高效、满足授信机构个体理性和保证授信机构诚实报价的性质。除此之外，针对我国法定数字货币“央行—商业银行”的二元分层体系结构，本文分析了 POPTIM 机制具有适用性，并提出了利用信贷拍卖和数字纪念币对 POPTIM 激励机制的扩展设计。

References:

[1] Central banks:DLT and CBDCs[R],R3 reports,2017.1.

[2] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies[C]. 2015.

[3] Darshini D,Stanley Y.,A. Lewis.The future is here project Ubin :SGD on distributed ledger[R]. deloitte.

[4] Accenture. Project ubin phase 2[R],The Association of Banks in Singapore, 2017.11

[5] JP K. Why fed is more likely to adopt bitcoin [EB/OL]. http://jpkoning.blogspot.ca/2013/04/why-fed-is-more-likely-to-adopt-bitcoin.html.2013.4

[6] Rod G. Fedcoin CAD-coin versus[R],R3 reports,2016.11.15

[7] Wendy M. Fedcoin: the U.S. will issue e-currency that you will Use [EB/OL].https://news.bitcoin.com/FEDCoin-u-s-issue-e-currency/.2017.1.12

[8] JP K. FEDCoin: A central bank-issued cryptocurrency[R],R3 report,2016.11

[9] European Central Bank and Bank of Japan,Project Stella, securities settlement systems: delivery-versus-payment in a distributed ledger environment[R],2018.3

[10] https://www.bitcoin.org/bitcoin.pdf

[11] WOOD G. Ethereum: a secure decentralisedgeneralised transaction ledger[R]. 2014.

[12] https://baijiahao.baidu.com/s?id=1602874327108940671&wfr=spider&for=pc

[13] Cai Wei De, Zhao Zihao, Zhang Qi, et al. [J]. Bank of England Digital Currency RSCoin [J]. Financial Electronization, 2016 (10): 78-81.

[14] Yao Qian: Analysis of the Central Bank's Encrypted Currency-RSCoin System [EB/OL]. http://www.sohu.com/a/148005571_747927.2017.6.11.

[15] Wang J, Tang J, Yang D, et al. Quality-aware and fine-grained incentive mechanisms for mobile crowdsensing[C]. 2016 IEEE 36th International Conference on Distributed Computing Systems

[16] Zhang Wei Ying. Game theory and information economics. Ge Zhi publishing house.2012

[17] Yang D, Xue G, Fang X, et al. Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. In: Proceedings of the 18th international conference on Mobile computing and networking[C]. Istanbul, Turkey, 2012: 173-184

[18] Lin H Y, Tzeng W G. An efficient solution to the millionaires problem based on homomorphic encryption[C] //International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2005: 456-466.

[19] Ren Hui, Dai Hua, Yang Geng. Cloud Privacy Protection Sorting Method Based on Security Comparison Code [J]. Computer Science, 2018, 45 (5).

[20] O’Keeffe M. The paillier cryptosystem[J]. Mathematics Department April, 2008.

[21] Krishna Vijay. Auction Theory [M]. Translated by Luo Deming and Xi Xican. Beijing: Renmin University of China Press, 2010

[22] Yao Qian, Tang Yingwei. Some thoughts on the central bank's statutory digital currency [J].Financial Research, 2017 (7): 78-85.

[23] Yao Qian. Optimization of the Current Monetary System and Issuance Design of the Legal Digital Currency [J].International Finance Research, 2018 (4).

附中文参考文献:

[13] 蔡维德, 赵梓皓, 张弛, 等. 英国央行数字货币 RSCoin 探讨[J]. 金融电子化, 2016 (10): 78-81.

[14] 姚前：中央银行加密货币-RSCoin 系统之分析 [EB/OL].http://www.sohu.com/a/148005571_747927.2017.6.11.

[17] 张维迎. 博弈论与信息经济学.格致出版社.2012

[19] 任晖, 戴华, 杨庚. 基于安全比较码的云环境隐私保护排序方法[J]. 计算机科学, 2018, 45(5).

[21] Krishna Vijay.拍卖理论[M]. 罗德明，奚锡灿译. 北京：中国人民大学出版社, 2010

[22] 姚前, 汤莹玮. 关于央行法定数字货币的若干思考[J]. 金融研究, 2017(7):78-85.

[23] 姚前. 法定数字货币对现行货币体制的优化及其发行设计[J]. 国际金融研究, 2018(4).