

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。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, 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 首先通过编码散列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

中图分类号: TP311

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019012

Truthful incentive mechanism for “digital currency” based on privacy protection

CHEN Xiao, LYU Xinran, 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 the incentive mechanisms was proposed 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. The privacy costs of the mintettes were fully considered, the incentive model of the central bank and mintettes were established, and the methods were clarified to compensate mintettes. In the legal digital currency research area, an incentive mechanism POPTIM was proposed firstly, that not only protects the private cost of the mintettes, but also guarantees the mintettes report their truthful bidding prices to the central banks. POPTIM first encrypts the biddings of mintettes by coding hash encryption method, then adopts privacy-preserving sorting algorithm to select the winner mintettes, and finally calculates the reward of mintettes based on the homomorphic addition algorithm. The analysis shows 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

收稿日期: 2018-12-10; 修回日期: 2019-01-15

通信作者: 陈晓, chenxiao_zh@chinamoney.com.cn

论文引用格式: 陈晓, 吕欣冉, 刘志. 基于隐私保护的法定“数字货币”激励机制[J]. 网络与信息安全学报, 2019, 5(2): 30-39.
CHEN X, LYU X R, LIU Z. Truthful incentive mechanism for digital currency based on privacy protection[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 30-39.

1 引言

随着比特币的诞生,分布式账本技术(DLT, distributed ledger technology)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建设法定“数字货币”原型系统,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,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予一定的报酬,并对懒散或行为不当的授信机构给予经济处罚的方式,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,首次提出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先通过编码散列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。

2 现状与分析

2.1 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(MAS, Monetary Authority of Singapore)、欧洲央行(ECB, European Central Bank)和日本央行(BOJ, Bank of Japan)、美国、英国等都陆续投入基于分布式账本的法定“数字货币”研究。

2.1.1 英国

在RSCoin框架中^[2,13],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。

1) 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 $M=\{m_1, m_2, \dots\}$,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^[4]。

2) 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。

3) 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。

在文献[2]中, 央行向提供服务的授信机构给予一定的报酬, 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。

2.1.2 新加坡

2016年11月, 新加坡金融管理局启动了 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^[5]。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 (MEPS+, MAS electronic payment system) 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 (RTGS, real time gross settlement) 系统实现多边净额结算的能力^[6]。

2.1.3 美国

2013年4月13日, JP Koning^[7]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。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^[8]。虽然目前该设计仍处于理论阶段, 但是货币专家 Doug Casey 认为只有美联储发行法定“数字货币”, 才能最大限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^[9-10], 从而可增强美联储对广义货币总量的控制能力。

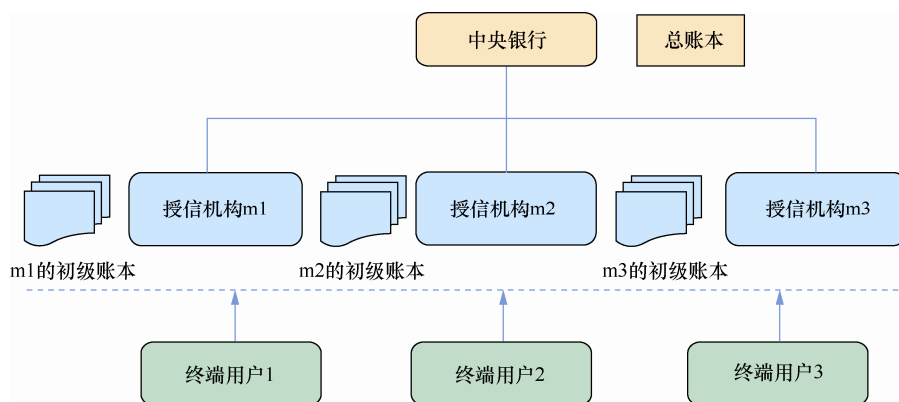


图1 RSCoin 总体结构

2.1.4 欧盟与日本

2016年12月,日本央行和欧洲中央银行第一次公开发布了名为“Stella”的联合研究项目^[11]。在第一阶段的研究中,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,这一阶段主要探讨基于DLT的目前国际债券标准结算方式券款对付(DVP, delivery versus payment)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。

2.2 比特币等虚拟代币的激励机制

目前,多数的虚拟代币有激励机制。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,如比特币、以太坊等。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,如FT(FCoin Token)。

2.2.1 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^[12-13]。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,其计算的散列值符合特定规则(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4年,每个挖矿成功地记账节点将奖励25个比特币,每过4年就减少一半。大约到2140年时,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。

2.2.2 以太坊

以太坊是以太坊平台产生的虚拟代币。以太坊^[14]是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以太坊。如果普通区块包含叔块,每包含一个叔块还可以得到额外固定奖励 $\frac{5}{32}$ 以太坊。在以太坊中,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。

2.2.3 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。FT总发行量为100亿,其中51%比例的FT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,平台会持续不断地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,如参与业务决策。

3 系统模型与重要概念

本节首先介绍POPTIM激励模型,然后介绍本文的预备知识。

3.1 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

6) O_2 中的授信机构向央行发送初级账本 O_2 、 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) 央行根据第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 集合中给予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

3.2 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。

5) 0-1 编码^[18]：令 S 二进制表示 $S = s_1 s_2 \dots s_n$ ($s_i \in \{0,1\}$ 且 $1 \leq i \leq n$)，其中 s_1 为最高位， s_n 为最低位。根据二进制数值 0 和 1 的位置，对 S 进行

0 编码和 1 编码。

6) 0 编码^[18]：令 S 二进制表示 $S = s_1 s_2 \dots s_n$ 如下，则 $E_s^0 = \{s_1 s_2 \dots s_{i-1} 1 | s_i = 0 \wedge 1 \leq i \leq n\}$ 是其 0 编码集合，其中 n 为位数。

7) 1 编码^[19]：令 S 二进制表示 $S = s_1 s_2 \dots s_n$ 如下，则 $E_s^1 = \{s_1 s_2 \dots s_i | s_i = 1 \wedge 1 \leq i \leq n\}$ 是其 1 编码集合，其中 n 为位数。

4 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。

4.1 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 $K (K \geq 2)$ 个授信机构一致性验证。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 最大化，如式(1)所示。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 $|W| = K$ 。

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

4.2 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

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。

$$u_i = b_i - c_i \quad (2)$$

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[18-19]的编码散列加密方法和文献[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 E_{bi}^0 和 1 编码报价 E_{bi}^1 。

3) m_i 使用散列消息身份验证码 (HMAC, hashed message authentication code) 的密钥 g_i 对 E_{bi}^0 和 E_{bi}^1 散列运算, 生成安全比较 0 编码报价 $H_{gi}(E_{bi}^0)$ 和安全比较 1 编码报价 $H_{gi}(E_{bi}^1)$ 。

4) 使用文献[20]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 $P_A(b_i)$ 。

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

4.3 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。

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 至少有同一个元素时, 即 $E_x^1 \cap E_y^0 \neq \emptyset$, 则 $x > y$ 。而根据文献[18]的衍生文献[19]可知, 当且仅当

$H_{gx}(E_{bx}^1) \cap H_{gy}(E_{by}^0) \neq \emptyset$, 则 $x > y$, 因此, 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[19]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。

4.4 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地获得报酬, 可能会存在虚高报价的情况。如果授信机构虚高报价, 央行将根据虚假的信息选择授信机构, 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), 本文采用 Vickery 拍卖的支付原则, 被选择的授信机构的报酬等于给其他竞争者带来的外部性。假设 m_i 在选择中获胜, 其报酬计算公式如式(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。

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

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, 式(3)可以整理为式(4), 即第一个落选的授信机构提供的报价。

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

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 $P_i = P_A(b_{(k+1)})$ 。由加法同态的性质可知, $P_A(x+y) = P_A(x) \oplus P_A(y)$, 其中, 在文献[20]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 $\oplus$ 运算后再解密, 获得金额是此授信机构在这段时间获得的报酬。

5 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。

5.1 隐私安全

在本文机制中, 授信机构 m_i 的隐私成本信息经过加密处理 (如 3.2 节描述), 形成安全比较报价 $B_i(b_i) = \{K_i(b_i), H_{gi}(E_{bi}^0), H_{gi}(E_{bi}^1), P_A(b_i)\}$ 。对于密文 $K_i(b_i)$ 和 $P_A(b_i)$ 来说, 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 $H_{gi}(E_{bi}^0)$ 和 $H_{gi}(E_{bi}^1)$, 由于散列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。

5.2 计算高效

在本文机制中, 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 $O(n^2|M|\log|M|)$ 。根据计算高效的定义, 本机制具有计算高效性。

5.3 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的关系为 $b_{(1)} \leq b_{(2)} \cdots \leq b_{(k+1)}$ 。其中, $b_{(i)}$ 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 $u_{(i)} = b_{(k+1)} - c_{(i)}$ 为非负。因此, 本文机制能保证个体理性。

5.4 保证诚实报价

如文献[21]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, 本文机制能够保证授信机构诚实报价。

6 激励机制扩展

结合我国法定“数字货币”的研究, 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。

6.1 适用性分析

我国“数字货币”研究所的姚前所长在文献[22]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, 将央行抽象为发布任务的采购方, 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。

6.2 基于信贷拍卖的扩展

姚前在文献[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。

6.3 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，这增加了数字纪念币的独特性，提高了数字纪念币交易的趣味性，以及熟悉了纪念币的收藏价值。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，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实践运行。

7 结束语

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。

参考文献:

- [1] CARLO R M. Blockchain and central banks: a tour de table part II[R]. 2017.
- [2] DANEZIS G, MEIKLEJOHN S. Centrally banked cryptocurrencies[J]. arXiv preprint arXiv: 1505.06895, 2015.
- [3] 姚前. 数字货币初探[M]. 北京: 中国金融出版社, 2018.
YAO Q. A glimpse of digital moeny[M]. Beijing: China Financial Publishing House, 2018.
- [4] 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.
CAI W D, ZHAO Z H, ZHANG Q, et al. Bank of england digital currency RSCoin[J]. Financial Electronization, 2016(10): 78-81.
- [5] DARSHINI D, STANLEY Y, LEWIS A. The future is here project Ubin: SGD on distributed ledger[R]. Deloitte Consulting Pte Ltd 2017.
- [6] Accenture. Project ubin phase 2[R]. 2017.
- [7] KONING J. Fedcoin[J]. Moneyness Blog, 2014.
- [8] GARRATT R. CAD-coin versus fedcoin[R]. 2016, 15.
- [9] BECH M L, GARRATT R. Central bank cryptocurrencies[R]. R3 Report, 2017.
- [10] KONING J P. FEDCoin: a central bank-issued cryptocurrency[R]. 2016.
- [11] European Central Bank and Bank of Japan. Securities settlement systems: delivery-versus-payment in a distributed ledger environment[R]. 2018.
- [12] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008: 1-9.
- [13] BÖHME R, CHRISTIN N, EDELMAN B, et al. Bitcoin: economics, technology, and governance[J]. Journal of Economic Perspectives, 2015, 29(2): 213-38.
- [14] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[R]. 2014.
- [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. 2016: 354-363.
- [16] 张维迎. 博弈论与信息经济学[M]. 上海: 格致出版社, 2012.
ZHANG W Y. Game theory and information economics[M]. Shanghai: Gezhi Publishing House. 2012.
- [17] YANG D, XUE G, FANG X, et al. Crowdsourcing to smartphones:

incentive mechanism design for mobile phone sensing[C]//The 18th International Conference on Mobile Computing and Networking. 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. 2005: 456-466.
- [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).
REN H, DAI H, YANG G. 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, 2008(4): 18.
- [21] KRISHNA V. 拍卖理论[M]. 北京: 中国人民大学出版社, 2010.
KRISHNA V. Auction theory[M]. Beijing: Renmin University of China Press, 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.
YAO Q, TANG Y W. Some thoughts on the central bank's statutory digital currency[J]. Financial Research, 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):3-11.
YAO Q. Optimization of the current monetary system and issuance design of the legal digital currency[J]. International Finance Research, 2018 (4): 3-11.

[作者简介]



陈晓(1988-), 女, 山东枣庄人, 博士, 中汇信息技术(上海)有限公司工程师, 主要研究方向为激励机制、区块链, 软件工程。



吕欣冉(1992-), 女, 山东枣庄人, 硕士, 中汇信息技术(上海)有限公司助理工程师, 主要研究方向为区块链、金融工程。



刘志(1988-), 男, 山东威海人, 硕士, 中汇信息技术(上海)有限公司工程师, 主要研究方向为区块链、交易系统研发。