软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(12):5477−5500 [doi: 10.13328/j.cnki.jos.006798]

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

基于博弈的加密货币交易市场用户决策优化分析*

毕红亮[1], 陈艳姣[2], 伊心静[2], 汪 旭[2]

[1](西北工业大学 网络空间安全学院, 陕西 西安 710072)

[2](武汉大学 计算机学院, 湖北 武汉 430072)

通信作者: 陈艳姣, E-mail: chenyj.thu@gmail.com

摘 要: 近年来, 随着区块链的快速发展, 加密货币种类和匿名交易的类型不断多元化. 如何在加密货币市交易类型中进行最优决策是用户关注的问题, 用户的决策目标是在确保交易被打包的前提下实现交易费用最小化和隐私最大化. 加密货币交易市场是复杂的, 不同的加密货币技术差异大, 现有的工作都是研究比特币市场, 很少有对Zcash 等其他匿名币市场和用户的匿名需求的讨论. 因此提出一个基于博弈的通用加密货币交易市场模型, 通过结合用户的匿名需求运用博弈论探究交易市场和用户对于交易类型和交易费用的决策. 以最具代表性的可选隐私加密货币 Zcash 为例, 结合 CoinJoin 交易, 对交易市场进行分析, 按照交易流程模拟用户和矿工找到最佳策略的过程, 讨论区块大小、折扣因子和用户数量对交易市场和用户行为的影响. 在多种交易市场类型中对模型进行仿真实验, 并对实验结果进行深入讨论. 以三类型交易市场为例, 交易市场恶性竞价情景下, 参数设置为 $plnum=75$, $\theta=0.4$, $s_t=100$, $s_z=400$ 时, 100% 的用户在交易市场前期 (前 500 轮) 倾向于选择 CoinJoin 交易, 而在交易市场中后期 (1 500–2 000 轮), 隐私敏感度低于 0.7 的用户中有 97% 倾向于选择 CoinJoin 交易, 隐私敏感度高于 0.7 的用户中有 73% 倾向于选择屏蔽交易. CoinJoin 交易和大小在 400 以上的区块大小能有效缓解交易费用的恶性竞争. 所提的交易市场模型能够有效地帮助研究人员理解不同加密货币交易市场博弈, 分析用户交易行为, 揭示市场运行规律.

关键词: 区块链; 博弈论; Zcash; CoinJoin; 交易市场

中图法分类号: TP301

中文引用格式: 毕红亮, 陈艳姣, 伊心静, 汪旭. 基于博弈的加密货币交易市场用户决策优化分析. 软件学报, 2023, 34(12): 5477–5500. http://www.jos.org.cn/1000-9825/6798.htm

英文引用格式: Bi HL, Chen YJ, Yi XJ, Wang X. Game-based User Decision Optimization Analysis of Cryptocurrency Trading Market. Ruan Jian Xue Bao/Journal of Software, 2023, 34(12): 5477–5500 (in Chinese). http://www.jos.org.cn/1000-9825/6798.htm

Game-based User Decision Optimization Analysis of Cryptocurrency Trading Market

BI Hong-Liang[1], CHEN Yan-Jiao[2], YI Xin-Jing[2], WANG Xu[2]

[1](School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China)

[2](School of Computer Science, Wuhan University, Wuhan 430072, China)

Abstract: In recent years, with the rapid development of blockchain, the types of cryptocurrencies and anonymous transactions have been increasingly diversified. How to make optimal decisions in the transaction type of cryptocurrency market is the concern of users. The users' decision-making goal is to minimize transaction costs and maximize privacy while ensuring that transactions are packaged. The cryptocurrency trading market is complex, and cryptocurrency technologies differ greatly from each other. Existing studies focus on the Bitcoin market, and few of them discuss other anonymous currency markets such as Zcash and users' anonymous demands. Therefore, this study proposes a game-based general cryptocurrency trading market model and explores the trading market and users' decisions on transaction types and costs by combining the anonymous needs of users and employing game theory. Taking Zcash, the most representative optional cryptocurrency, as an example, it analyzes the trading market in combination with the CoinJoin transaction,

* 收稿时间: 2022-03-04; 修改时间: 2022-04-26, 2022-07-31; 采用时间: 2022-09-19; jos 在线出版时间: 2023-04-13
CNKI 网络首发时间: 2023-04-13

simulates the trading process about how users and miners find the optimal strategy, and discusses the impact of block size, discount factors, and the number of users on the trading market and user behaviors. Additionally, the model is simulated in a variety of market types to conduct in-depth discussion of the experimental results. Taking a three-type trading market as an example, in the context of vicious fee competition in the trading market, when $plnum$ = 75, θ= 0.4, s_t = 100, s_z = 400, all users are inclined to choose CoinJoin in the early transaction stage (first 500 rounds). In the middle and late part of the market (1 500–2 000 rounds), 97% of users with a privacy sensitivity below 0.7 tend to choose CoinJoin, while 73% of users with a privacy sensitivity above 0.7 tend to choose shielded transactions. CoinJoin transactions and block sizes above 400 can alleviate the vicious competition of transaction fees to some extent. The proposed model can help researchers understand the game of different cryptocurrency trading markets, analyze user trading behavior, and reveal market operation rules.

Key words: blockchain; game theory; Zcash; CoinJoin; trading market

比特币[1]作为第一个分布式电子货币它使用了数签名和加密证明来验证交易. 比特币系统不需要中央托管机构, 所有节点都可以自行验证和交换数据. 任何广播到网络并经过打包确认的交易都将记录在去中心化的分布式公共帐本——区块链中. 区块链作为比特币的核心技术, 具有去中心化、可追溯和防篡改等安全特性. 在比特币交易中, 发送者或接收者的地址是他们公钥的散列, 这使得参与交易的用户获得了一定程度上的匿名保护. 比特币的安全特性吸引了成千上万的用户, 截至 2021 年 2 月, 其市值估计超过 1.086 万亿美元[2], 然而, 比特币提供的匿名性并不是完美的. 在 Nakamoto 协议下, 网络必须将整个交易历史存储在区块链中, 而且这个交易历史对所有区块链矿工和用户都是透明的. 区块链中的交易信息对所有用户都公开可见, 任何人都可以通过关联同一用户的不同账户地址, 潜在地跟踪用户的行为或身份, 并以此来查看比特币在网络中的转移. 加密货币的数据隐私泄露问题已经引起了相关研究学者的广泛关注, 文献 [3] 对区块链的隐私安全问题进行了综述.

随着区块链的发展, 不同加密货币和匿名增强技术的出现促使了加密货币交易种类的增多. 从中心化的混币系统 Mixcoin[4]到去中心化的混币系统 CoinJoin[5]再到基于 CoinJoin 改进的加密货币达世币 (Dash[6]), 混合方案保护了比特币的交易地址, 实现不可连接性, 但存在着不能自定义混合金额, 受到恶意用户影响等缺点. 使用环签名技术的门罗币 (Monero) 和使用零知识证明的 Zcash[7]则通过密码学技术实现了加强的数据隐私保护. 用户在实际的交易过程中, 需要根据自己的需求在不同的交易类型间做出选择. 而现有的工作主要关注于匿名技术之间的理论分析, 缺少对匿名交易和用户决策的讨论.

Arce 等人[8]创新性地利用博弈论刻画比特币中 CoinJoin 交易匿名集的形成, 决策目标是混合费的最小化, 他们的工作对 CoinJoin 交易匿名集进行了理论分析, 提出了第 1 个针对多参与者协调系统的匿名代价解决方案, 但分析局限于参与 CoinJoin 的用户和混合费. 他们给出了用户参与 CoinJoin 的效用方程, 并对用户隐私和匿名费用的关系进行了公式推导. 与该工作相比, 本文期望利用博弈论讨论用户参与不同交易类型 (或使用不同匿名增强技术) 的匿名代价, 为用户提供最优策略, 用户的决策目标是在确保交易被打包的前提下实现交易费用最小化和隐私最大化. 本文给出了用户参与加密货币交易市场的效用方程, 建立了不同交易市场的博弈模型, 并通过仿真实验模拟交易过程, 进一步讨论了交易市场博弈和用户决策.

作为自比特币诞生以来, 最具代表性的具有可选隐私功能的加密货币之一, Zcash[7]在隐私保护方面显示出了独特的优势. 与比特币相类似, Zcash 的交易数据也被发布到一个公开的区块链中. 它利用先进的加密技术 (零知识证明 zk-SNARKS) 为用户提供可选的隐私性和透明性. Zcash 允许在不透露发送方、接收方或交易金额的情况下对交易进行验证. 由于其强大的隐私特性, Zcash 已成为全球使用最广泛的数字货币之一. 依赖于屏蔽池 (Shielded Pool) 的使用, Zcash 交易市场中存在多种交易类型, 用户如何在不同交易类型进行选择是本文的主要研究内容. 因此本文以 Zcash 交易市场为例讨论不同交易类型对用户的隐私保护和用户效用的影响. 出于增强 Zcash 交易市场中非屏蔽交易隐私保护的目的, 本文引入了 CoinJoin, 给出了一个涉及 3 种交易类型的交易市场博弈.

近年来, 加密货币市场快速发展, 庞大的区块链网络、数以万计的实时交易为加密货币交易市场的研究提供了有力的数据支撑, 但对于加密货币交易市场建模和用户分析仍存在几点困难.

• 现有的加密货币市场分析工作大多基于交易市场数据, 通过实证分析展开, 对用户行为的研究不够深入, 存在局限性.

• 加密货币交易市场十分复杂, 用户和矿工数量庞大. 用户发起的交易经过全网广播、验证、审核通过之后才有可能被矿工确认, 如何对交易市场进行合理建模, 简化交易流程仍待解决.

• 交易市场博弈的理论分析十分困难, 由于交易市场的复杂性以及各种可能的参数和假设, 较多用户参与时, 博弈问题的复杂度增加, 对博弈的求解困难.

针对以上问题, 本文提出了一个通用的加密货币交易市场模型, 结合对交易过程的仿真算法和无悔学习算法模拟了用户在加密市场中的博弈行为. 针对 Zcash 交易类型复杂的问题, 本文将 Zcash 中的 4 种交易类型, 重新划分为非屏蔽交易 (unshielded transaction) 和屏蔽交易 (shielded transaction) 两种. 通过仿真实验, 本文的交易市场模型揭示了不同隐私敏感度的用户对交易类型的选择倾向, 讨论了区块大小、折扣因子和用户数量对于交易市场用户和整体的影响.

本文的主要贡献包括 3 个方面.

• 本文提出了一个通用的加密货币交易市场模型, 探讨不同偏好的用户在交易市场中的决策. 据我们所知, 本文是第 1 个使用博弈论分析 Zcash 交易市场的工作. 本文还研究了 Zcash 中的 CoinJoin, 并将这种隐私增强技术与屏蔽池技术进行了比较.

• 本文依照交易的发生流程, 根据网络对用户和矿工的激励机制, 模拟了理性用户和自私矿工的行为, 并给出了交易市场中各阶段的仿真算法.

• 本文在 Zcash 的交易市场模拟中进行了广泛的实验, 给出了隐私敏感度不同的用户在博弈过程中对不同交易类型的倾向, 探究了区块大小、折扣因子和用户数量等因素对于交易市场和用户行为的影响, 为 Zcash 市场的默认费用定价提供了参考.

本文在第 1 节中介绍了博弈论、区块链交易和匿名增强技术的相关工作, 并指出了本文的工作内容. 第 2 节阐述了本文模型构建的准备知识和所构建的通用交易市场模型中的两种博弈 (即合作博弈和非合作博弈). 第 3 节对于交易市场进行了样例分析和整体描述, 并给出了交易市场模型的算法. 第 4 节中分析了交易市场模型的仿真结果, 讨论了交易市场中影响用户行为的因素. 第 5 节对本文的工作进行了总结.

1 相关工作

1.1 博弈论与区块链交易

比特币作为第 1 个去中心化的分布式账本, 为网络用户提供了安全保障. 博弈论是一种研究理性决策者之间战略互动的数学模型. 近年来, 随着人们对加密货币的兴趣日益浓厚, 博弈论在区块链网络中得到了广泛的应用, 如自私挖掘攻击[9]、51% 攻击 (majority attack)[10]和用户挖矿行为[11,12]等.

作为数字货币, 比特币具有金融和商品等多重属性. 比特币系统的参与者在保证其经济属性 (激励兼容性和个体理性) 的同时, 追求自身效用的最大化. 一些研究人员将博弈论应用到加密货币交易和交易收费机制的研究中去, 其中有一些与交易费用和区块大小相关的工作, 关注用户在交易过程中需要支付的费用[13−16], 他们分析了比特币市场的交易记录, 对于交易费用进行了简单的均衡分析.

Arce 等人[8]利用博弈论讨论了用户参与 CoinJoin 的匿名费用. 在文献 [17] 的场景下, Abramova 等人运用博弈论研究了硬币的质量差异对于用户使用混币服务提高其匿名性行为的影响. 沈蒙等人[18]提出了基于动机分析, 利用子图匹配技术识别区块链数字货币的异常交易行为的方法. Malinova 等人[19]研究了比特币不同透明度设计在金融市场交易理论模型中的利弊, 并提出了一个可靠的交易系统. Li 等人[20]研究了非抢先优先排队博弈中的交易费用, 他们关注矿工的开采回报和用户的时间成本, 并对所提出的模型进行了均衡分析. Lavi 等人[21]提出并分析了比特币费用市场中两种基于拍卖的机制, 即垄断价格机制 (MP) 和随机抽样最优价格机制 (RSOP).

目前加密货币交易费用相关工作研究的都是比特币市场, 很少有对 Zcash 等其他匿名币市场的讨论; 区块大小、市场透明度和矿工开采收益等被作为考虑因素, 但对于用户仅讨论了时间成本, 很少考虑用户根本的匿名需求. 因此本文希望结合用户的匿名需求讨论交易市场和用户决策.

1.2 匿名增强技术

区块链是透明的, 区块链的数据对所有人公开. 区块链交易具有可追溯性, 比特币的匿名性也被认为是不完善的: 恶意的攻击者可以通过构造用户及其公钥之间的映射来去除用户的匿名[22]. 文献 [23,24] 讨论了区块链系统中的隐私威胁, 分析了各类隐私保护机制. 为了更好的隐私保护, 研究人员研究了多种提高加密货币匿名性的方法[5,25−28]. 具有代表性的工作是 Maxwell[5]提出的 CoinJoin 概念, 它通过将多用户的加密货币混合到一个交易中, 使得外界很难区分哪些输入对应于哪些输出, 实现了更强的匿名性, 但对于匿名集内部而言, 所有参与方的交易信息公开可见, 匿名集内部存在可链接性. 目前有许多交易平台可以创建 CoinJoin 交易, 比如 JoinMarket 和 Wasabi. CoinShuffle[25]则在 CoinJoin 的思想上进行了改进, 采用级联加密方案对参与者的输出地址进行加密, 提高了匿名集的内部不可链接性, 但 CoinShuffle 的混淆过程要求参与者同时在线, 在实现上的复杂性和匿名成本更高, 且存在 DoS 攻击风险. Xim[26]是一个去中心化的多回合两方混币协议, 极大地提高了匿名集的外部隐私性, 在 Xim 的混币过程中, 用户将公开发布广告, 然后在回应广告的用户中寻找混币同伴. 发布和回应广告都需要收取手续费, 因此 Xim 可以有效地提高攻击者成本, 降低女巫攻击和 DoS 攻击的概率. 此外, 市场上还出现了其他具有隐私保护的加密货币. 达世币 (Dash)[6]添加了通过 CoinJoin 实现的可选的隐私增强交易类型, PrivateSpend. Zcash[7]作为比特币的分支, 使用零知识证明 (zk-SNARKS) 来提供更强的隐私保护, 它可以在不透露发送方、接收方或交易金额的情况下对交易进行验证. Zcash 为用户提供了两种交易地址 (t-address 和 z-address), 其中 z-address 是私有地址, 在交易中会被隐藏; t-address 是透明地址, 对所有用户公开可见. 用户可以任意在 z-address 和 t-address 之间进行资金转移, 根据是否涉及屏蔽池, Zcash 中的交易类型可以初步分为非屏蔽交易 (unshielded transaction) 和屏蔽交易 (shielded transaction), 屏蔽交易除了可以隐藏 z-address, 交易金额也不可见. 门罗币 (Monero) 则通过使用环签名技术的匿名性隐藏交易发送方的身份信息, 使用一次性的隐蔽地址 (stealth address) 隐藏了交易接收方地址, 为用户提供了一种高度匿名的交易.

针对 Zcash 网络, 相关研究者进行了研究分析. Kappos 等人[29]提供了第一个对 Zcash 的深入研究. 他们重点关注于 Zcash 的匿名性保证, 并通过聚类多个地址对其进行分析. Zhang 等人[30]对于 Zcash 进行了改进的匿名分析, 使用了改进的地址聚类方法, 他们的研究结果与 Zcash 诞生的意图相反: 在 Zcash 的实际应用中, 很少有用户使用涉及屏蔽池的交易去增强自身的隐私保护, 而 Zcash 的提出就是为了提供隐藏区块链交易发送者、接收者以及交易金额的交易, 达到更好的匿名保护效果. Biryukov 等人[31]研究了屏蔽交易并分析关于攻击的安全和隐私问题. 文献 [29,30] 对 Zcash 进行深入探索后得出结论: 目前绝大多数的 Zcash 交易活动与屏蔽池无关, 即在实际的交易市场中, 绝大多数的用户选择了非屏蔽交易. 受他们研究的启发, 本文对用户在发起交易时的选择很感兴趣. 非屏蔽交易的交易地址均为 t-address, 在交易市场中公开可见, 这使得非屏蔽交易存在很高被链接追踪的风险, 在非屏蔽交易中引入其他的匿名增强技术可以有效地弥补这一缺陷. 相较于 CoinShuffle、Xim 等匿名增强技术, CoinJoin 广泛应用在比特币中、实现简单、匿名开销低且不需要对加密货币协议进行改动, 为用户提供了简单有效的隐私保护, 理论上可以提升非屏蔽交易的匿名性. 因此本文创新性地在 Zcash 的非屏蔽交易中引入混币技术 CoinJoin, 并在第 2.1.2 节中论述了引入 CoinJoin 的合理性. 本文希望讨论用户对屏蔽交易、非屏蔽交易和 CoinJoin 交易的选择倾向, 深入探讨 CoinJoin 对 Zcash 交易市场的影响.

不同交易类型和匿名增强技术的出现为用户提供了更高的匿名性. 用户在实际的交易过程中, 面临着不可避免的选择. 交易的顺利完成确保了用户获得交易带来的预期价值, 在交易被打包的前提下, 用户的决策目标是实现交易费用最小化和匿名最大化. 本文期望利用博弈论讨论用户参与不同交易类型 (或使用匿名增强技术) 的匿名代价, 为用户提供最优策略.

1.3 本文工作

本文提出了一个基于博弈的加密货币交易市场的模型, 并通过博弈过程的仿真模拟, 分析了用户的行为倾向. 本文的研究目标是利用博弈论和无悔学习来探讨交易市场中不同隐私敏感度用户对交易类型的选择, 从而分析整个市场的变化, 为交易市场的交易费用定价提出参考.

2 系统模型

2.1 预备知识

2.1.1 屏蔽交易和非屏蔽交易

Zcash 通过屏蔽 (shielding) 来保护用户的隐私. 在整个 Zcash 生态系统中, 根据交易使用屏蔽池的情况, 交易被分为 4 类[29]. 它们是透明交易 (transparent transaction, t-to-t)、去屏蔽交易 (deshielded transaction, z-to-t)、屏蔽交易 (shielded transaction, t-to-z) 和私有交易 (private transaction, z-to-z). 其中 z-address 在交易过程中均不可见, 隐私性最强的私有交易还隐藏了交易金额, 与 CoinJoin 等混币技术相比, Zcash 能够有效地降低攻击者通过交易金额链接交易的风险.

本文中, 屏蔽交易这个术语将用于表示上文列出的 Zcash 的后 3 种类型 (即需要使用零知识证明的交易类型), 而术语非屏蔽交易将用于表示透明交易类型. 由于验证时需要进行零知识证明, 屏蔽交易用户发起交易的时间较长, 且交易大小大于非屏蔽交易. 根据 Zcash 的网站[32], 非屏蔽交易大小约为 500 B, 屏蔽交易的大小约为 2 000 B. 本文假设所有屏蔽交易具有相同的大小 s_z, 所有非屏蔽交易具有相同的大小 s_t, s_z 和 s_t 之间的数量关系为 $s_z = 4 \times s_t$.

匿名意味着隐藏身份, 同文献 [8] 一样, 本文使用变量 D_i 描述用户 i 的身份价值. 隐私敏感程度不同的用户具有不同的 D, 如参与交易市场的普通用户使用 Zcash 中的透明交易类型已经能够满足他们的隐私需求, 这类用户对于隐私敏感程度不高, D 较低; 而对于一些不想泄露财产和交易记录的公司或个人, 他们对于隐私更敏感, 具有较高的 D. 本文用 D 作为区分用户的类型的指标, 通过设置 D 来量化用户对匿名的追求.

尽管 Zcash 中屏蔽交易的输入输出并不可见, 屏蔽交易的交易费用对网络上的任何人都是透明的, 独特的费用可能导致恶意链接, 还有泄露隐私的风险. 因此, Zcash 平台建议用户在进行屏蔽交易时使用 0.000 1 ZEC 的默认费用[32], 但通过对 Zcash 交易费用的调查, 我们发现, 出于被快速打包或降低成本的需求, 市场中存在有用户拒绝使用默认交易费用的现象. 考虑到用户可以对交易费用进行自定义, 在本文的博弈模型中, 交易费用是可变的, 其大小取决于博弈中的用户行为.

本文的交易系统考虑了两种类型的参与者: n 个用户和一个矿工. 在 Zcash 中, 用户广播到网络的交易对于任何参与者可见. 本文假设, 在挖到区块的任意时刻, 矿工们从网络中收集到的交易集合是相同的. 本文讨论的内容只关注交易是否打包, 而不关注是谁打包了交易. 不论是哪一位矿工将用户的交易打包到区块中, 对于用户而言没有区别, 矿工的数量并不会对实验产生影响, 因而本文中的交易系统模型只考虑了一个矿工的情况. 在 Zcash 交易市场中, 用户 i 将根据自己的需要启动一个交易 t_i, 类型为屏蔽交易或非屏蔽交易. 如果用户是理性的, 他将只选择最大化其效用的交易类型.

2.1.2 CoinJoin

CoinJoin 是一种匿名化策略, 用来保护比特币用户在交易过程中的隐私. 该技术不需要对比特币的协议进行改动, 相对容易实现. CoinJoin 混合比特币的方式为: 在单一交易中多方提供输入和创建输出, 使得外部各方很难确定输入和输出之间的关系.

未使用的交易输出 (unspent transaction outputs, UTXO) 是比特币最核心的概念之一, 每一个比特币其实都是 UTXO. 在 CoinJoin 协议中, 匿名集中的用户相互协作, 将他们现有的 UTXO (输入), 花在一组新的 UTXO (输出) 上. Zcash 参考了比特币的 UTXO 模型, 拥有交易输入和交易输出的概念, 其中的非屏蔽交易沿用了 UTXO 交易结构, 详细记录了交易的流转信息, 而涉及屏蔽池的交易则引入了 Note 结构, 并通过零知识证明等技术增强了交易的隐私性. 比特币式透明交易 (unshielded transaction) 的使用使 Zcash 能简单地集成现有的支持比特币的工具和基础设施, 因而在 Zcash 中使用 CoinJoin 是合理的. Zcash 中的 CoinJoin 交易等同于混合多个非屏蔽交易来产生一个具有多个输入输出的非屏蔽交易. 为了比较两种匿名技术的优缺点, 本文将 CoinJoin 交易添加到用户的动作集合, 并将其与非屏蔽交易和屏蔽交易进行讨论.

CoinJoin 组合了多个交易, 使得外界很难区分哪些输入对应与哪些输出. 尽管如此, 它提供的匿名性并不是绝对的. 当 CoinJoin 中组合的交易金额相同, 且使用多个输入地址和输出地址时, 匿名集合中的用户成员是难以区分

的. 本文假设有 N 个用户选择参与 CoinJoin 的匿名集合, 且所有参与 CoinJoin 的用户都被视为诚实的, 他们不会泄露其他参与者的身份. 对于单个用户, 他维护自己的匿名 (身份值) 的概率为 $(N-1)/N$, 即任何一个参与匿名集的用户有 $1/N$ 的概率被猜中身份.

对于每个联盟, 使用特征函数描述其总收益. CoinJoin 联盟中每个成员的回报向量是根据他们的身份、匿名集的大小和 CoinJoin 的混合费用来定义的. 用户参加 CoinJoin 时被收取的费用, 称为混合费; 例如, 在 Wasabi 钱包中[33], 用户支付的混合费为 0.003×匿名集大小; 由于混合费远低于交易费用, 本文忽略 CoinJoin 交易过程中混合费的影响.

2.1.3 NTU 博弈

NTU 博弈是效用不可转移的合作博弈. 在一个 NTU 博弈中, N 是参与者的集合, 一个有限非空集合, 对于每个联盟, $\varnothing \neq S \subseteq N$; NTU 特征函数 $V(S)$ 表示该联盟获得的可行收益向量集. 直观上, $|S| \geqslant 2$, 联盟 S 的成员之间相互合作, 但对于联盟的合并或分裂, 成员从各自利益出发的倾向并不一致. 对于每个向量 $x \in V(S)$, 条目 x_i 指定了玩家 i 的最大收益, 玩家 i 应该是联盟 S 的成员.

一个 NTU 博弈是一个数对 (N,V), 其中 N 是所有玩家的集合, V 是 $S \subseteq N$ 中所有联盟函数的集合, $V(S)$ 是与每个联盟 $S \subseteq N$ 对应的特征函数. 在合作博弈中, 满足帕累托标准的联盟结构称为博弈的有效解. 所有有效的解决方案的集合被称为核心 (core). NTU 博弈核心的定义[34]如下.

定义 1. 令 (N,V) 为一个 NTU 博弈, (N,V) 的核心, $C(N,V)$ 被给定为:

$$C(N,V)=\{x \in V(N) \mid \nexists S \subseteq N, \exists y \subseteq V(S),\ \forall i \in S, y \succ_i x\}.$$

2.1.4 无悔学习

无悔学习 (no-regret learning)[35]也叫做参考专家意见, 是重复博弈中常用一种学习类型, 是一种玩家通过不断的决策选择以及根据当前结果与历史决策进行修正和改进的算法. 无悔学习模型可以用来模拟玩家在博弈中的行为. 遗憾 (regret) 定义为决策者回顾中可能采取的最佳动作的效用与执行当前动作的总效用之差. 玩家在每一轮选择一个动作, 然后获得对应的收益, 该算法的目标就是达到整体遗憾的最小化. 当每个玩家各自进行无悔学习时, 重复博弈将收敛为粗相关均衡.

2.2 交易市场

本文将交易市场建模成一个五元组 $\Gamma=<U,T,P,M,\theta>$, 其中,

- $U=\{1,2,\ldots,n\}$ 是参与交易市场的用户集合. 每轮每个用户在市场中均参与发起一个交易, 交易的类型为 a.
- $T=\{t_1,t_2,\ldots,t_m\}$ 是由用户发起的交易的集合, $m \leqslant n$. $A=\{a_1,a_2,\ldots,a_n\}$ 为用户的动作集合, a_i 为用户 i 选择的动作即交易类型, $\forall i \in U$, $a_i \in \{t,z,c\}$, t 代表非屏蔽交易, z 代表是屏蔽交易, c 代表 CoinJoin 交易. 若用户选择的动作为 c, 即用户选择了参加 CoinJoin 的匿名集, 所有匿名集合中的用户共同发起一个总交易, 选择的动作为 t, z 的用户和交易一一对应.
- $P=\{p_1,p_2,\ldots,p_n\}$ 是用户选择交易类型时 3 种交易类型的概率分布的集合. $p_i=\{p_i^t,p_i^z,p_i^c\}$ 是用户选择交易类型时 3 种交易类型的概率分布, $\forall i \in U$, $p_i^a \in [0,1]$, $a \in \{t,z,c\}$. 任意用户选择 3 种交易类型的概率总和为 1, 即 $p_i^t+p_i^z+p_i^c=1$.
- M 是矿工的集合. 如第 2.1.1 节中所述, 本文只考虑一个矿工的情况.
- $\theta \in [0,1/2)$ 是非屏蔽交易身份价值的折扣因子. 选择屏蔽交易的用户被视为在交易过程中保留所有的身份价值, 而对于选择非屏蔽交易的用户, 由于存在链接等去匿名性的可能, 交易过程中其保留的身份价值存在一个折扣因子 θ. 需要明确的是 θ 并不直接影响用户的身份价值, 它只在效用函数计算时, 作为选择非屏蔽交易的用户保留身份价值的一个折扣因子. 选择 CoinJoin 交易的用户保持的匿名性与参与 CoinJoin 匿名集的用户数相关, 参与的用户数越多, 用户在交易中保留隐私的概率越高. 如第 2.1.2 节中所述, 当有 n 个用户参与 CoinJoin 时, 单个用户保持匿名性的概率为 $(n-1)/n$. 参与 CoinJoin 的用户数大于等于 2 时, 才可能构成匿名集. 用户数等于 2 时, 单个用户保持匿名性的概率为 $1/2$. 基于选择 CoinJoin 交易的用户将保持更多匿名性的假设, $\theta \in [0,1/2)$.

• $D_i \in [0,1]$ 表示用户的身份价值. 对于每个用户 i, 本文用 D_i 表示用户的身份价值, 并以此衡量用户的隐私敏感程度. 用户的隐私敏感程度是一个高度抽象的概念, 它取决于不同的用户个体, 因此本文假设 D_i 遵循正态分布, 且 $\forall i \in U$, $D_i \in [0,1]$.

• $F = \{f_1, f_2, \ldots, f_n\}$ 是用户交易费用的集合.

本文遵循加密货币市场交易的过程: 用户们发起交易并将它们广播到网络中后, 各个节点的矿工会收集这些交易并验证每个交易的有效性, 验证成功后的交易会被矿工收集到本地. 当矿工成功挖掘一个区块时, 他将从自己收集的交易中进行选择, 将选出的交易打包到区块中, 并获得 Zcash 奖励.

2.3 市场中的合作博弈

参考 Arce 等人的研究[8], 匿名集合 S, 是由市场中所有参与 CoinJoin 的用户 i ($a_i = c$) 组成的一个联盟. 当用户组成一个匿名集合时, 他们以不可区分的方式共同发起交易, 讨论的焦点是收益在用户之间的分配. 作为一种混币协议, CoinJoin 只有在联盟集合中的所有成员都签署交易时才会发生, 这与合作博弈的存在条件即参与者之间存在具有约束力的协议, 且参与者必须在这些协议的范围内进行博弈一致. 因此应用合作博弈来讨论 CoinJoin 的收益分配是合理的.

匿名集是一个可变规模的联盟, 用户为了更好地隐藏自己的身份而加入了匿名集. 由于市场中不同用户对其身份价值的评估是不同的, 匿名集的用户之间无法进行身份价值的相互比较. 本文把这种场景看作效用不可转移的合作博弈, 也就是 NTU 博弈. NTU 博弈可以通过虚拟权值的效用转移方法 (λ-transfers), 转换为具有可转移效用的合作博弈 (TU 博弈). 这也意味着 NTU 博弈可以通过夏普利值 (Shapley value) 的原始方法求解.

根据前面的定义, D_i 是用户 i 的身份估值, $\forall i \in S$. 在匿名市场中, 联盟 S 的特征函数为:

$$V(S) = \left\{ (x_i) | x_i \leqslant \frac{D_i(|S|-1)}{|S|} \right\} \tag{1}$$

2.3.1 夏普利值

作为合作博弈理论中的一个解概念, 夏普利值 (Shapley value) 最初为可转移效用博弈 (TU 博弈) 定义, 它给出了每个参与者对所有可能形成的联盟价值的平均边际贡献. 给定一个 NTU 博弈 (N,V), 解方法也是应用夏普利值. NTU 的夏普利值 (Shapley NTU value) 作为预期收益分配出现在均衡中, 前提为假设参与者加入联盟的顺序是随机选择的, 即联盟排列组合出现的概率是相同的.

如前所述, CoinJoin 匿名市场是一个边际支付但没有可转让效用的合作博弈[34]. 本文建立了一个 λ-转移博弈 (λ-transfers game). 对于每个玩家联盟, 他们至少可以获得他们在夏普利所定义的诱导 λ-转移博弈中的边际贡献. λ-转移方法可以将 TU 博弈的解推广到 NTU 博弈的场景下. 参考 Arce 等人[8], 现在介绍应用 λ-转移博弈的正式步骤.

首先, 在 $\lambda \in (\mathbb{R}^+)^{|N|}$ 中为每个玩家指定一个非负的权重集, 并创建虚拟转移博弈. 对于每个联盟 S, 虚拟转移博弈的特征函数用 $w(S)$ 表示, 也称为价值函数 (worth function), 其中,

$$w(S) = \max_{x \in V(S)} \sum_{i \in S} \lambda_i x_i \tag{2}$$

比值 λ_i/λ_j 可以看作是参与者之间不可转让效用之间的汇率.

其次, 从 NTU 博弈推导出 TU 博弈的特征函数, $w(S)$. 向量 $[\varphi_i(w,\lambda)]_{i \in N}$ 被视为 TU 博弈的夏普利值. 根据定义, 夏普利值为:

$$\varphi_i(w,\lambda) = \sum_{i \in S, S \subseteq N} \frac{(|S|-1)!(|N|-|S|)!}{|N|!} (w(S) - w(S \backslash \{i\})) \tag{3}$$

TU 博弈的夏普利值具有以下性质, 这些性质使得夏普利值成为 TU 博弈的主要解概念. 即① 唯一性, ② 对称性, ③ 帕累托效率, 大联盟 (指包含所有用户的联盟) 的所有价值都分布在参与者之间.

$$\sum_{i \in N} \varphi_i = w(N) \tag{4}$$

最后, 将结果除以转移权值 λ_i . 当大联盟在 NTU 博弈中可行时, NTU 博弈中的夏普利值 Sh_i (λ-转移值) 为 $[\varphi_i(w,\lambda)/\lambda_i]_{i\in N}$.

2.4 市场中的非合作博弈

本节描述了市场中所有用户交易之间的非合作博弈. 当用户发起的交易被打包进区块并被确认后, 意味着交易完成, 用户会得到本次交易的确认奖励 (保留的身份价值、交易本身的价值等). 确认奖励激励着用户对自己的交易类型和交易费用进行选择. 每个用户都是个人理性的, 所有参与者都是独立行动的, 参与者之间没有合作. 因此, 本文将整个交易系统建模为一个非合作博弈.

就交易而言, 一个 Zcash 交易就是一个广播到网络中的 Zcash 的转移, 它将被收集到 Zcash 的区块中. 在去中心化分布式账本中, 只有当交易被区块收集时, 我们才说这些交易被确认了. 当交易被足够多的确认信息淹没时, 它们就可以被认为是不可逆的. 正是由于这些特性, 提出交易的用户希望矿工尽快将交易打包成块, 会支付较高的交易费用. 较高的交易费用可以激励矿工首先打包该交易, 相反的, 矿商会选择延迟打包低费用交易. 当不断有更高费用的交易进入网络时, 低费用交易将处于长时间无法获得确认的情况下.

在 Zcash 中, 区块的大小是受限制的, 区块的大小 B_s 最大为 2 MB. 为了更好地研究不同类型的交易的影响, 本文的模型假设网络中交易的总规模远远超过区块大小 B_s . 因此, 自私的矿工 m 将选择并打包使自己的利润最大化的交易. 在交易费用主导矿工收益的背景下[12], 这种现象更加明显.

交易费 f_i 和交易大小 s_i 决定了交易被打包的可能性 $Prob_i$. $Prob_i$ 、 f_i 和 D_i 决定了用户的效用 u_i . 用户的效用函数为:

$$u_i=\begin{cases} Prob_i^z(D_i-f_i^z), & \text{Shielded} \\ Prob_i^t(\theta\times D_i-f_i^t), & \text{Unshielded} \\ Prob_i^c(\widehat{Sh}-f_i^t), & \text{CoinJoin} \end{cases} \tag{5}$$

$Prob_i=1$时, 用户的效用函数是线性的. 高 D_i 和低 f_i 都可以让用户获得更大的效用, 这与现实相符. 例如在市场中, D_i 越高, 意味着用户对于隐私更敏感, 他会倾向于选择匿名性更高的交易类型, 也意味着交易完成时用户的身份得到了更好的保护, 用户在实际应用中被恶意链接和跟踪的可能性越低. f_i 表示用户向矿工支付的打包费用, 费用越高, 用户从交易中获得的收益就越少. 根据之前的定义, 3 种交易类型所保留的个人身份价值从高到低依次为 z 、 c 和 t , 这与 3 类交易实际的匿名性是一致的. $Prob_i$ 直接取决于矿工的选择, 基于矿工的个人理性. 本文通过对整个市场的交易费用单价进行排序来量化交易被打包的概率 ($Prob_i$), 根据算法 2 的描述: 交易打包费用单价越高, 交易被打包的概率越高. 作为匿名成本的一部分, 交易费用影响着交易概率. 交易费用与效用之间的关系可以看成是一个二次函数, 而不能直接定性地描述. 本文将在下面的实验中讨论这个关系.

3 市场博弈

在交易市场 Γ 中, 每个用户发起交易时, 将在 3 种交易类型中进行选择. 假设市场中共有 N 名用户, 其中 m 名用户选择加入 CoinJoin 交易匿名集, 即组成合作博弈的联盟 S 共同发起一个 CoinJoin 交易.

- $i=1,2,\ldots,m$ 是一个联盟 S 中的用户编号.
- $\{1,2\}_2$ 是用户 1 和用户 2 的一个联盟.
- $\{1,2,\ldots,j\}_s$, s 是联盟 $\{1,2,\ldots,j\}$ 的大小.

交易市场中的非屏蔽交易和屏蔽交易均由单个用户发起, 与 CoinJoin 交易一起组成交易市场. 各种可能的参数和假设使得对所有交易的非合作博弈的理论分析不可行. 因此本节主要对交易市场中 CoinJoin 匿名集的 NTU 博弈进行了理论分析, 本文在第 4 节中通过仿真实验来模拟两种博弈并分析实验结果.

3.1 3-用户匿名集

本节以一个 3-用户匿名集为例来讨论 CoinJoin 中的 NTU 博弈. 与文献 [8] 不同, CoinJoin 中的所有参与者被简单地视为相同大小的多个输入和输出的提供者, 玩家 1、2 和 3 之间没有区分. 对于单方联盟, NTU 特征函数为:

$$V(\{i\}_1)=\{x_i|x_i\leqslant\theta\times D_i: i=1,2,3\} \tag{6}$$

对于任意单个用户而言, 他们都没有办法单独形成 CoinJoin 匿名集. 当只有一个用户选择 CoinJoin 时, 本文将用户的交易视为简单的非屏蔽交易, 用户 i 保留的身份值为 $\theta\times D_i$.

对于 2-玩家联盟, 在联盟 $\{1,2\}$, $\{1,3\}$ 或 $\{2,3\}$ 中, 每个玩家维持其身份值的概率为 $1/2$. 例如:

$$V(\{1,2\}_2)=\left\{(x_1,x_2)|x_1\leqslant\frac{1}{2}\times D_1,\ x_2\leqslant\frac{1}{2}\times D_2\right\} \tag{7}$$

一旦形成了 CoinJoin 匿名集, 用户们相互提供匿名, 每个用户在大联盟 $\{1,2,3\}$ 中保持匿名的概率增加到 $2/3$.

$$V(\{1,2,3\}_3)=\left\{(x_1,x_2,x_3)|x_1\leqslant\frac{2}{3}\times D_1,\ x_2\leqslant\frac{2}{3}\times D_2,\ x_3\leqslant\frac{2}{3}\times D_3\right\} \tag{8}$$

按照第 2.3.1 节给出的过程, 令 3-用户匿名集用户的权重集为 $\lambda=(\lambda_1,\lambda_2,\lambda_3)=(1,1,1)$. 然后, 我们可以给出与该 λ 对应的价值函数, 并计算夏普利值. TU 博弈的夏普利值的解为:

$$\varphi_1(w,\lambda)=\left(\frac{7}{18}+\frac{\theta}{3}\right)D_1+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_2+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_3 \tag{9}$$

$$\varphi_2(w,\lambda)=\left(\frac{7}{18}+\frac{\theta}{3}\right)D_2+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_1+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_3 \tag{10}$$

$$\varphi_3(w,\lambda)=\left(\frac{7}{18}+\frac{\theta}{3}\right)D_3+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_1+\left(\frac{5}{36}-\frac{\theta}{6}\right)D_2 \tag{11}$$

3.2 任意用户匿名集

本节分析任意数量用户的 NTU 博弈. 对于 CoinJoin 匿名集合下的 NTU 博弈, 令 m 为参与匿名集的用户总数, 则该博弈的 NTU 特征函数为:

$$V(\{1,2,\ldots,m\}_m)=\{(x_1,x_2,\ldots,x_m)|x_i\leqslant\frac{D_i(m-1)}{m},\ i\in\{1,2,\ldots,m\}\} \tag{12}$$

在 λ-转移博弈中, 一个联盟 S 的价值函数是通过设置 $\lambda_i=1$, $\forall i\in S$, 并应用公式 (13)、公式 (14) 得到:

$$w(\{1,2\}_2)=(D_1+D_2)/2 \tag{13}$$

$$w(\{1,2,\ldots,m\}_m)=\sum(D_i)\times(m-1)/m \tag{14}$$

对于匿名集中的所有用户, 现在我们可以通过在第 2.3 节中介绍的过程推导出 NTU 夏普利值:

$$\widehat{Sh}_i=\frac{\varphi_i(w,\lambda)}{\lambda_i}=\varphi_i(w,\lambda) \tag{15}$$

由于夏普利值的计算复杂度很高, 当用户数量较大时, 几乎无法在有效的时间内计算出结果. 因此, 在仿真实验中, 本文使用一个采样过程 (ApproShapley 算法)[36]来估计这里的 NTU 的夏普利值, 并在第 4.1 节给出详细说明.

3.3 核的存在性证明

在合作博弈中, 满足帕累托标准的联盟结构称为有效博弈解决方案. 所有有效的解决方案的集合被称为核心.

如第 3.1 节和第 3.2 节的公式推导所示, 本文将每个用户保留的身份价值 (匿名性) 作为合作博弈的效用. 在规模为 N 的 CoinJoin 中, 每个参与者保持其匿名性的概率为 $(N-1)/N$, 用户 i 期望保留的身份值如下:

$$D_i\times(N-1)/N \tag{16}$$

证明: 对于任何用户 i, 可以确认其大联盟的效用大于任何其他组合 $(S_1,S_2,\ldots,S_t)$, t 是所有联盟组合的数量, $(n_1+n_2+\ldots+n_t=N)$, 核心一定存在 ($i\in S_j$, S_j 为用户数为 j 的联盟, $1\leqslant j\leqslant N$).

$$\frac{N-1}{N}D_i\geqslant\frac{n_j-1}{n_j}D_i \tag{17}$$

社会福利 (social welfare) 在本文中指代整个市场中用户的整体收益, 用来描述整个市场的收益水平. 公式 (18) 证明大联盟的社会福利一定大于其他任何组合.

$$\frac{N-1}{N}\sum_{i\in S}^{N}D_i>\left(\frac{n_1-1}{n_1}\sum_{j\in S_1}^{n_1}D_j+\frac{n_2-1}{n_2}\sum_{j\in S_2}^{n_2}D_j+\ldots+\frac{n_t-1}{n_t}\sum_{j\in S_t}^{n_t}D_j\right) \tag{18}$$

3.4 仿真算法

在本文的模拟中, 用户和矿工都是自私的, 两者唯一的目标都是获得自身的最大效用. 本文模拟了用户如何随着时间的推移找到最优策略的过程. 每一轮, 用户们都会发起他们的交易, 共同形成交易市场. 每场博弈都拥有相同的用户群, 自私的矿工会选择一组交易打包并最大化他的收益. 需要提醒的是, Zcash 中的区块有大小限制. 因此, 本文使用背包算法来模拟矿工打包交易的过程. 每一轮, 都可以得到一组被打包的交易 PT 和一组与之相对应的用户集合. 用户选择策略时不仅可以参考当前这轮博弈, 还可以参考策略在历史上的成功, 本文的模拟假设用户执行无悔学习来寻找最优策略. 在重复博弈过程中, 玩家估计遗憾最小化的价值, 通过无悔学习进行决策, 随着博弈的进行, 最大化他们的长期收益. 表 1 汇总了本节所使用的符号并逐一进行说明.

表 1 符号说明

名称	描述
m	ApproShapley算法采样的采样次数
$\widehat{Shi}_i$	玩家 i 参加合作博弈联盟的夏普利值的估值
$Players$	参与博弈过程的玩家集合
N	进行合作博弈的一组玩家
$Cont$	当前采样次数的计数
$\pi(N)$	玩家集 N 的所有可能排列的集合
O	玩家集 N 的一个排序, 如 $\{1,2,\ldots,n\}$
$Pre^i(O)$	在排序 O 下, 玩家 i 的前导玩家的集合
$x(O)_i$	在排序 O 下, 玩家 i 在联盟中的边际收益
$v(S)$	玩家联盟 S 的价值收益
PT	市场中被矿工打包的交易集合
pti	被打包交易 pt 的编号
uf_i	用户 i 发起的交易费用的单价
$\overline{F}$	市场中所有交易费用单价的集合
$\overline{f_i}$	交易 i 的交易费用单价
loc	表示交易费用单价在 $\overline{F}$ 序列中的位置, $\overline{F}[loc]$表示为第 loc 位置的交易费用单价
$maxloc$	表示 $\overline{F}$ 序列中使得用户效用函数取到最大值的交易费用单价所在的位置为 $maxloc$
$Prob_i^a$	玩家 i 选择 a 交易类型时交易被打包的概率, $a\in\{t,z,c\}$
$rounds$	无悔学习的总轮数
$\mathfrak{R}$	当前交易市场博弈运行的轮次
η	乘法权重算法的因子
$cjnum$	选择参与CoinJoin的玩家数
ε	ε-greedy算法的因子

合作博弈中最重要的解的概念之一是夏普利值. 夏普利值的计算复杂度是指数级的, 在用户集较大时, 计算夏普利值十分困难, 因而本文通过一个采样过程 (ApproShapley 算法)[36]来估计夏普利值. ApproShapley 可以在多项式时间内计算任何联盟的夏普利值, 伪代码见算法 1.

算法 1. 夏普利值的采样估计算法 (ApproShapley).

输入: m, $Players$;
输出: $\widehat{Sh}_i$, $\forall i \in N$.

1. 输入m, 初始$Cont := 0$ and $\widehat{Sh}_i := 0$, $\forall i \in N$.
2. While $Cont < m$
3. 以概率$1/n!$从所有排列集合$\pi(N)$中取排列O
4. For 所有$i \in N$
5. 计算$Pre^i(O)$
6. $x(O)_i := v(Pre^i(O) \cup \{i\}) - v(Pre^i(O))$
7. $\widehat{Sh}_i := \widehat{Sh}_i + x(O)_i$
8. $Cont := Cont + 1$
9. $\widehat{Sh}_i := \widehat{Sh}_i / m$, $\forall i \in N$

本文采用了乘法权重算法 (multiplicative weights algorithm)[37]和ε-greedy 算法[38]作为无悔学习的更新策略. 对于交易市场中的每个用户, 他们通过无悔学习在 3 种交易类型中进行决策, 同时更新交易费用以提高自己发起的交易被打包的概率, 并以此最大化自己效用. 相较于ε-greedy 算法, 无悔学习算法更为稳定, 在仿真实验中为用户选择了更优的策略, 具体内容将在第 4.1 节中讨论.

对于每个用户来说, 他们都遵循相同的交易费用更新规则. 回顾本文在第 2.4 节中给出的效用函数, 每个用户i都可以通过比较交易单位价格uf_i, 量化其交易被打包的概率$Prob_i$, 并更新自己的费用, 以达到效用函数的最大化. 由于自私的矿工受交易费用的激励, 区块包含的一定是一组具有最高单位费用的交易. 例如, 假设有一组交易的单价从最低到最高排序, $\overline{F} = [\overline{f_1}, \overline{f_2}, \ldots, \overline{f_t}]$, 当用户发起交易的交易费用单价$uf_i \in [\overline{f_j}, \overline{f_{j+1}}]$, 该交易被矿工打包的概率为$j/t$. 在鼓励用户更新交易费用的同时, 算法保留了一定的随机性以尽可能最大化效用. 本文的更新规则满足用户以最低成本使交易打包成块的期望. 交易市场中用户交易费用的更新规则的伪代码见算法 2.

算法 2. 费用更新规则.

输入: PT, $Players$;
输出: uf_i.

1. 初始化: $\overline{F} = []$
2. For 所有pt在PT中
3. 计算pt的单位费用, $\overline{f_{pti}}$
4. 添加uf_i到$\overline{F}$
5. 对$\overline{F}$中的元素进行升序排列
6. For 所有i在$Players$中
7. For loc在范围$(1, len(PT))$
8. $uf_i = \overline{F}[loc]$
9. $Prob^a = loc/len(PT)$
10. 计算这一轮所选交易类型对应的效用函数, $u_i = \begin{cases} Prob_i^z(D_i - uf_i \times s_z), & \text{Shielded} \\ Prob_i^t(\theta \times D_i - uf_i \times s_t), & \text{Unshielded} \\ Prob_i^c(\widehat{Sh}_i - uf_i \times s_t), & \text{CoinJoin} \end{cases}$
11. 记录最大化效用函数的$maxloc$
12. 在$\left[\overline{F}[maxloc], \overline{F}[maxloc+1]\right]$范围内随机更新$uf_i$

算法 3 是交易市场博弈的伪代码, 详细描述了每一轮博弈中用户和矿工的行为. 对于玩家集合 (*Players*), 单个用户在初始化时, 根据假设按照正态分布生成每个用户的 D 值, 按照指数分布生成每个用户对应于屏蔽交易和非屏蔽交易的交易费用 f_z 和 f_t. 每一轮次, 通过模拟用户发起交易的行为, 产生 CoinJoin 匿名集的合作博弈和市场的非合作博弈, 自私矿工则通过背包算法决定哪些交易将被打包, 最后用户通过无悔学习算法更新交易选择策略. 算法 3 给出了使用乘法权重算法更新策略来更新用户决策的伪代码, ε-greedy 算法更新策略的伪代码见算法 4.

算法 3. 交易市场博弈 (乘法权重算法更新策略).

输入: $rounds, Players$;
输出: $Players$.

1. 决定轮数: $rounds$
2. 初始化: 初始化一组玩家, 每个玩家的每个动作 a, 权重 $w_a^1 := 1$, $\mathfrak{R}$=1, $\eta \leqslant 1/2$
3. While $\mathfrak{R} < rounds$
4. $cjnum := 0$
5. For 所有 i 在 $Players$ 中
6. 按照概率随机选择当前的动作 $a_i \in \{t, z, c\}$
7. If a_i 是 CoinJoin 交易
8. $cjnum++$
9. If $cjnum > 2$
10. 选择 CoinJoin 交易的用户组成联盟并创建单个 CoinJoin 交易
11. 使用 ApproShapley 算法计算参与联盟博弈的用户的夏普利值估计 $\widehat{Sh}$
12. 矿工对收集到的交易集合进行选择并打包.
13. 计算 $\mathfrak{R}$ 轮所有玩家的收益 $u_i^{\mathfrak{R}}$, $\forall i \in Players$
14. For 所有 i 在 $Players$ 中
15. For 每个 $a' \in \{t, z, c\}$
16. 令 v' 为上一轮次中玩家 i 用 a' 代替 a_i 得到的总收益, $a' = a_i$ 时 $v' = u_i$
17. 计算用户 i 选择所有动作中的最大总收益记为 U_i
18. 计算选择每个动作的遗憾值 $R_{a'} = U_i - v'$, $a' \in \{t, z, c\}$
19. 更新权值: $w_{a'} = (1 - \eta R_{a'}) w_{a'}$ (乘法权重算法更新策略)
20. 按更新的权值更新用户对于 3 种交易类型的选择概率
21. 更新 f_z 和 f_t
22. /* 用户不会选择进行负效用的交易*/
23. If v' 是负的
24. a' 对应的费用 f_z 或 f_t 取上一轮的值
25. Else
26. 取 a' 对应的费用 f_z 或 f_t 使其在过去轮次中最大化效用函数
27. $\mathfrak{R} := \mathfrak{R} + 1$

算法 4. ε-greedy 算法更新策略.

输入: ε, $Players$;
输出: $Players$.

1. For 所有 i 在 *Players* 中
2. 产生 $[0,1]$ 之间的随机数 p_i
3. If $p_i < \varepsilon$
4. 在动作集 $\{t,z,c\}$ 中随机选择行动 a_i
5. Else
6. 选择用户 i 在过去轮次中取得最小遗憾值的动作 a_i

4 模拟仿真

Zcash 通过屏蔽池和零知识证明的使用增强匿名性. 在屏蔽池里的余额和交易地址都是被加密的, 这使得屏蔽交易的地址和交易金额不可见. 此外, 如何在真实的区块链上应用博弈模型, 如何对用户的身份价值进行准确的衡量还待解决, 这些问题都使得目前真实链上的实验难以进行. 本节通过仿真算法模拟了整个交易系统中的两个博弈, 比较了不同的更新策略算法, 对三类型交易市场、传统交易市场和无屏蔽类型交易市场进行了讨论, 评估了用户对不同交易类型的偏好, 在第 4.4 节、第 4.5 节分别分析了 CoinJoin 交易、区块大小 (B_s)、匿名性折扣因子 (θ)、用户总数 ($plnum$) 等参数对于用户和交易市场的影响, 表 2 给出了具体的实验参数说明.

表 2 实验参数说明

名称	描述
N	参与交易市场博弈的用户总数
θ	匿名性的折扣因子
s_t	透明交易的交易大小
s_z	屏蔽交易的交易大小
$rounds$	无悔学习算法的运行轮次
B_s	链上的区块大小
$plnum$	参与交易的用户总数
η	乘法权重算法的因子
ε	ε-greedy算法的因子

具体的模拟流程如下: 假设用户根据各自的交易选择概率 (p), 在 3 种交易类型中进行选择; 选择 CoinJoin 交易的用户会形成匿名集并进行合作博弈, 计算所有参与 CoinJoin 的用户的边际收益 (即参与 CoinJoin 所保留的身份价值), 计算选择屏蔽交易和非屏蔽交易的用户保留的身份价值; 在所有用户都发起了交易之后, 模拟矿工打包交易的全部流程, 判断各用户是否被矿工打包以及根据第 1 个博弈 (合作博弈) 的结果计算各个用户本轮交易所得的效用, 最后通过第 2 个博弈 (非合作博弈) 和无悔学习来更新用户选择 3 种交易类型的概率, 直到找到最优的交易策略. 本文在第 2.3 节和第 2.4 节中对这两个博弈进行了详细讨论.

4.1 更新策略算法的选择

本节运行模拟程序来仿真若干用户和一个矿工参与的 Zcash 交易市场博弈, 对交易市场博弈中的更新策略算法进行了比较, 并关注用户类型 D, 分析了它对用户动作的影响.

本节分别以乘法权重算法 (MW) 和 ε-greedy 算法 (EG) 为无悔学习的更新策略, 设置参数如下: $N=75$, $\theta=0.4$, $B_s=300$, $s_t=5$, $s_z=20$, $rounds=2000$; 对于乘法权值算法更新策略设置 $\eta=0.1$, 对于 ε-greedy 算法更新策略, 设置 $\varepsilon=0.1$. 在博弈过程中, 交易市场随着用户的学习和交易策略动态改变不断波动. 每 10 轮博弈统计一次, 图 1 给出了自私矿工从交易市场打包交易的收益趋势; 图 2 给出了交易市场的社会福利. 如图 1 和图 2 所示, 矿工打包收益的趋势为前期快速增长, 在后期表现为较为平稳的波动, 市场社会福利的变化则表现为前期迅速下降, 后期平稳波动.

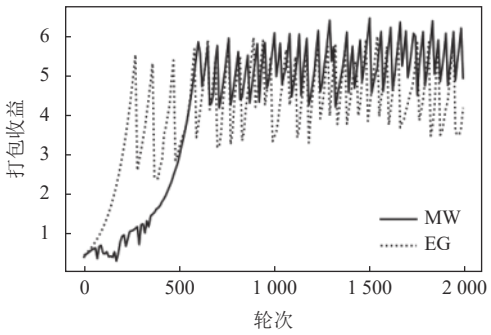


图 1 两种更新策略下矿工的打包收益

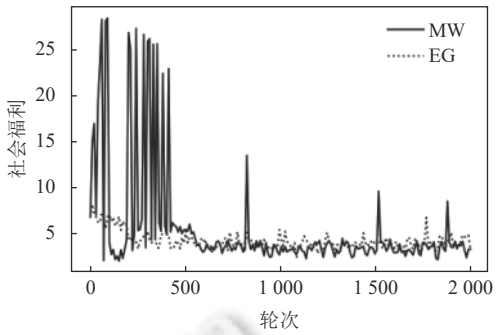


图 2 两种更新策略下交易市场的社会福利

对于初始条件完全相同的用户集合 *Players*, ε-greedy 算法更新策略收敛更快; 在总社会福利相近的情况下, 乘法权重算法更新策略下自私矿工的打包收益稍高, 波动的范围更小, 具有更高的稳定性; 如图 2 所示, 在前 500 轮中, 乘法权重算法更新策略明显为交易市场取得更高的社会福利, 而在 500 轮之后, 两种更新策略下交易市场的整体社会福利差异不大.

通过对整个博弈过程中各个用户所得效用的分析, 本文发现在乘法权重算法更新策略下用户的效用总体更高. 如图 3 所示, 以编号 7 的用户为例, 分别以乘法权重算法 (MW) 和 ε-greedy 算法 (EG) 为更新策略, 统计该用户的效用. 通过对于整个博弈数据的分析可得, 在 ε-greedy 更新策略下, 该用户倾向于选择非屏蔽交易, 而在乘法权重算法更新策略下, 其以 99.83% 的选择概率选择屏蔽交易. 结合图 3 可以得出, 乘法权重算法为编号 7 的用户找到了更优的交易策略.

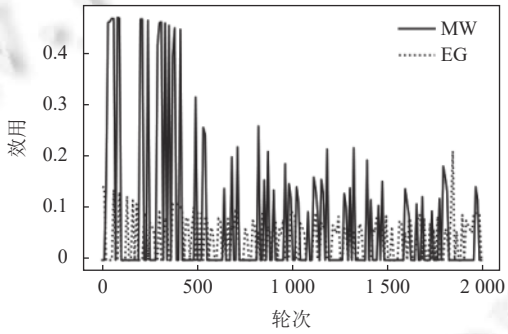


图 3 在两种更新策略下编号 7 用户的效用

本文以乘法权重算法更新策略的实验结果, 作为下文数据分析的依据.

4.2 三类型交易市场分析

根据无悔学习是由时间驱动的特性, 本节对市场博弈的分析也基于时间. 通过观察不同的用户行为, 本文发现具有同等 D 值的不同用户对于交易类型和交易费用的选择有着相似的行为. 因此, 本文根据实验数据, 以用户的 D 值为分类依据, 将用户按 D 值高低分为高、中、低 3 种用户类型, 其中高用户类型的 D 值大于 0.7, 中类型用户的 D 值在 0.4–0.7 之间, 低类型用户的 D 值低于 0.4.

为了使实验配置与真实链上环境更加接近, 本文使用爬虫爬取了 Zcash 交易市场中最近的 10 000 个区块, 并以这 10 000 个区块大小的均值作为后续实验中的 B_s. 本节以乘法权重算法 (MW) 为无悔学习的更新策略, 设置参数如下: $N=75$, $\theta=0.4$, $B_s=6455$, $s_t=100$, $s_z=400$, $rounds=2000$. 实验结果表明, 在三类型交易市场情景下, 100% 的用户在交易市场前期 (前 500 轮) 倾向于选择 CoinJoin 交易, 而在交易市场中后期 (1 500–2 000 轮), 隐私敏感度低于 0.7 的用户中有 97% 倾向于选择 CoinJoin 交易, 隐私敏感度高于 0.7 的用户中有 73% 倾向于选择屏

蔽交易.

表 3 记录了这 3 种用户交易类型的平均概率分布. 如表 3 所示, 高类型用户的倾向随着博弈的进行而变化. 500 轮时, 高类型用户选择 CoinJoin 的概率高于选择屏蔽交易的概率, 在之后的轮次中, 高类型用户选择屏蔽交易的概率不断增加, 并且在 2 000 轮时高类型用户的选择倾向已经由 CoinJoin 交易转变为屏蔽交易. 中、低类型用户的选择倾向均为 CoinJoin 交易, 随着轮次的增加中类型用户对不同交易的选择概率波动不大, 而低类型用户对 CoinJoin 交易的选择概率表现出显著的增加. 原因是在交易市场的博弈开始后, 由于交易费用的竞争, 3 种类型的交易费用单价趋同且不断上升, 如图 4 所示, 交易费用在博弈过程中呈现缓慢增长的趋势. 在 1 400 轮前, 交易费用的增长相对平缓, 交易费用相对较低, 相较于支付 4 倍费用的屏蔽交易, 用户倾向于选择 CoinJoin 交易来最大化自身效用; 而到了 1 400 轮后, 交易费用的增长速度加快, 恶性抬价使得高类型用户只能选择屏蔽交易类型, 在尽最大程度保持匿名性的前提下, 支付更高的交易费用进而提高用户交易被打包的概率, 中、低类型用户则保持对 CoinJoin 交易的选择倾向.

表 3　三类型交易市场的用户交易选择概率

轮次	D	平均 p_z	平均 p_c	平均 p_t
500	高	0.095 041 5	0.904 737 9	0.000 220 6
	中	0.119 687 4	0.876 482 0	0.003 830 6
	低	0.142 505 5	0.818 971 6	0.038 522 9
1 000	高	0.304 377 9	0.695 618 5	0.000 003 5
	中	0.146 237 1	0.853 521 4	0.000 241 4
	低	0.043 860 3	0.948 079 7	0.008 060 0
1 500	高	0.455 052 7	0.544 947 3	0.000 000 0
	中	0.135 658 4	0.864 329 2	0.000 012 4
	低	0.003 070 5	0.995 525 1	0.001 404 5
2 000	高	0.727 205 0	0.272 795 0	0.000 000 0
	中	0.132 006 3	0.867 990 7	0.000 003 0
	低	0.000 880 4	0.998 285 1	0.000 834 5

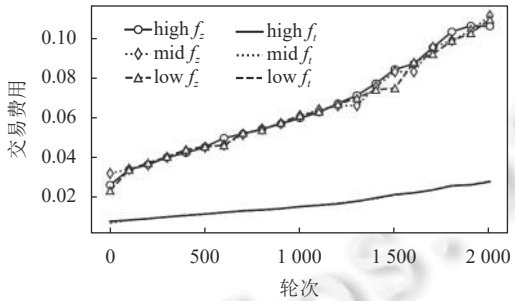


图 4　3 种类型用户的交易费用趋势

在交易市场中, 用户对交易类型的初始选择是任意的. 本文中, 用户选择 3 种交易类型的初始概率为 1/3. 在交易市场形成后, 受区块大小影响, 用户发起的交易之间存在竞争, 受到效用激励, 用户将不断更新自己的费用选择和交易选择策略, 尽可能提高交易被打包的概率以求获得最大效用. 用户通过无悔学习在确保最大效用的前提下, 尽可能地提高交易单元费用, 以增加被打包的可能性. 当不同交易类型的单位费用趋同时, 选择屏蔽交易意味着向矿工支付近 4 倍的交易费用. 因此, 中、低类型用户倾向于 CoinJoin 交易, 在可承受的交易费用增长范围内维持最大的效用. 而高类型用户倾向于支付更多来尽可能保持他们的匿名性, 也就是付更多的费用来提高交易被打包的概率. 整体而言, 与另两种交易相比, 用户对非屏蔽交易的选择倾向不强.

本文选取了高、中、低 3 种用户类型中具有代表性的用户, 编号分别是 59、31、11, 并绘制了这 3 个用户交

易选择的概率分布. p_z, p_t, p_c 分别表示当前用户选择 shielded 类型交易、unshielded 类型交易和 CoinJoin 交易的概率. 图 5(a) 显示从 1 200 轮开始用户 59 号选择屏蔽交易的概率有一个大幅上升并在 1 500 轮达到接近 100%, 图 5(b) 显示用户 31 号选择屏蔽交易概率在 100–500 轮间呈现缓慢增长, 500 轮次之后选择 CoinJoin 交易概率不断增加, 并在 1 500 轮次时接近 100%; 而图 5(c) 低类型用户选择 CoinJoin 交易的概率稳步增加.

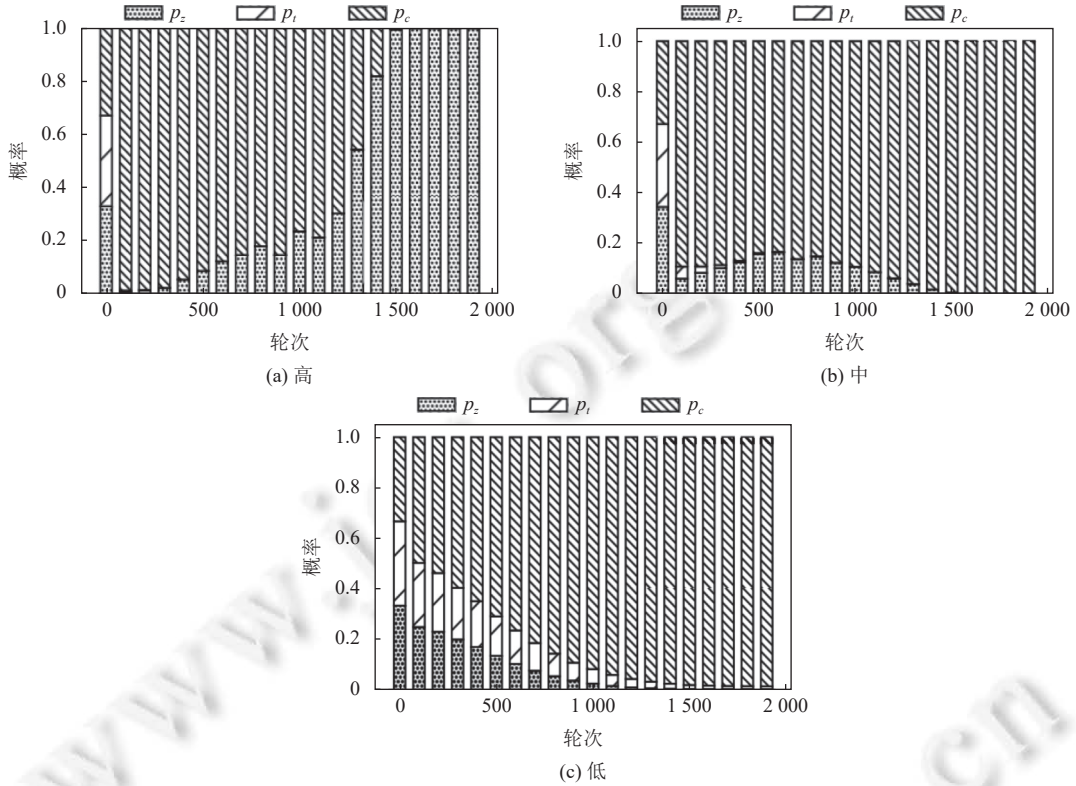


图 5 3 种交易类型的选择概率趋势

由于身份价值 (D) 较高的用户可以负担支付较高的交易费用, 他会倾向于选择屏蔽交易, 因此该类型更有可能在一个抬高交易费用的恶性市场中获得交易价值. 仿真结果与预期相似. 从实验结果可以看出, 对隐私要求较高的用户往往会选择更安全的匿名技术. 同时, 在恶意竞价的市场中, 随着交易费用的不断抬升, 不同用户的选择倾向也随之发生改变. 在该实验参数设置下, 高类型用户对选择屏蔽交易的倾向不断提高, 中、低类型用户对选择 CoinJoin 交易的选择倾向不断提高, 选择概率趋向两极分布.

4.3 无屏蔽类型交易市场分析

Zcash、达世币等以隐私保护著称的加密货币具有可选隐私的特性. 比特币作为市值最高的加密货币, 采用非对称加密算法和哈希算法实现匿名性, 许多模仿比特币的加密货币都采用了和比特币类似的加密算法, 它们提供的隐私不是可选的. 无屏蔽类型交易市场指仅含有非屏蔽和 CoinJoin 两种交易类型的交易市场, 本节对其进行了讨论, 旨在模拟类比特币加密货币的交易市场, 研究非可选隐私加密货币的交易市场博弈.

在与第 4.2 节同样的参数设置下, 仅考虑非屏蔽交易和 CoinJoin 交易进行实验. 本文在观察了所有参与交易的用户对于两种交易类型的选择倾向变化后, 发现用户的选择倾向变化主要有两种形式, 如图 6 所示, 图 6(a)、图 6(b) 分别代表了高 D 值用户和中低 D 值用户对两种交易类型的选择概率趋势. 本文选取用户 41 和用户 58 分别代表 D 值高的用户和 D 值低的用户, 他们的 D 值分别为 0.872 和 0.176. CoinJoin 交易类型和非屏蔽交易类型的不同, 主

要在于参与 CoinJoin 的用户可以通过混币得到更高的匿名性, 图 6(a) 中用户 41 和 58 在交易市场初期均表现出了对 CoinJoin 交易的倾向. 在博弈过程中, D 值高的用户先是表现为倾向于 CoinJoin 交易, 而后该用户对非屏蔽交易的倾向不断增加并保持平稳, 在 1400 轮以后, 用户选择非屏蔽交易的概率接近 100%; D 值低的用户, 则始终表现出对 CoinJoin 交易的选择倾向, 且随着轮次增加, 用户选择 CoinJoin 交易的概率增加, 在 1000 轮左右趋于平稳, 选择 CoinJoin 交易的概率接近 100%. 可见用户对交易的选择还受到隐私要求之外因素的影响, 该现象的出现可能是由于 CoinJoin 交易大小通常大于非屏蔽交易, 而矿工打包交易的区块大小是有限的. 在交易费用很高时, 高 D 值的用户选择牺牲一定的匿名性来提升交易被打包的概率.

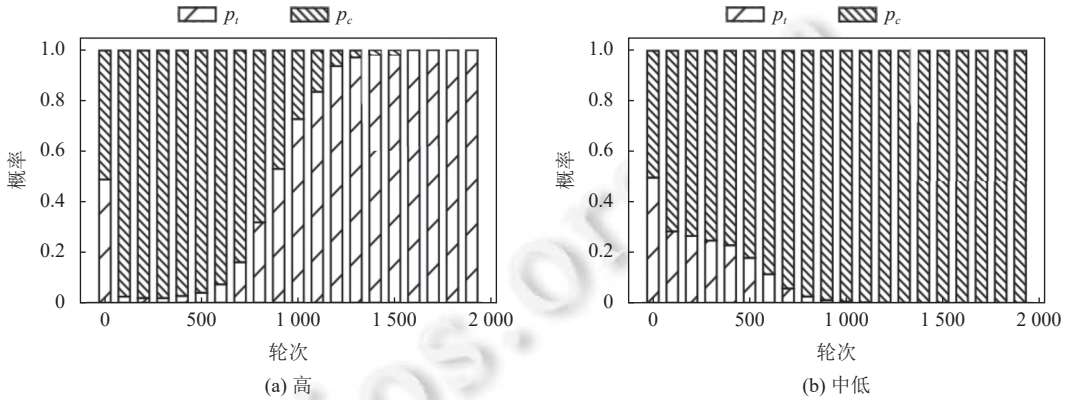


图 6 无屏蔽类型交易市场中两种交易类型的选择概率趋势

4.4 CoinJoin 交易对市场的影响

本节进行了 3 种交易类型的交易市场和基于传统 Zcash 交易类型的交易市场 (即仅考虑屏蔽交易和非屏蔽交易两种交易类型的交易市场) 的对比.

在同样的参数设置下, 依照表 3 中的用户类别划分, 表 4 给出了 3 种用户类型对两种交易选择概率的统计数据. 如表 4 所示, 身份价值 D 更高的用户倾向于选择屏蔽交易, 而身份价值 D 更低的用户倾向于选择非屏蔽交易. 从时间尺度上观察, 在基于传统 Zcash 交易类型的交易市场中, 3 种类型用户的策略均呈现了逐渐偏向非屏蔽交易的趋势. 表 5 记录了 D 值分别最高和最低的 5 位用户在 500 轮和 2000 轮时的交易选择概率, 2000 轮时, 高 D 值的用户表现出了选择屏蔽交易的倾向, 低 D 值用户表现出了选择非屏蔽交易的倾向, 与预期一致.

表 4 传统 Zcash 交易市场的用户交易选择概率

轮次	D	平均p_z	平均p_t
500	高	0.9986255	0.0013745
	中	0.8433690	0.1566310
	低	0.6121681	0.3878319
1000	高	0.9840867	0.0159133
	中	0.4627478	0.5372522
	低	0.3961076	0.6038924
1500	高	0.7664582	0.2335418
	中	0.1471747	0.8528253
	低	0.1948480	0.8051520
2000	高	0.7277568	0.2722432
	中	0.0567590	0.9432410
	低	0.1073900	0.8926100

表 5 10 个用户选择交易的概率

D	编号	第500轮p_z	第500轮p_t	第2000轮p_z	第2000轮p_t
高	41	1.0000	0.0000	1.0000	0.0000
	59	0.9999	0.0001	1.0000	0.0000
	70	0.9964	0.0036	1.0000	0.0000
	30	0.9997	0.0003	1.0000	0.0000
	27	0.9993	0.0007	1.0000	0.0000
低	19	0.5840	0.4160	0.1170	0.8830
	58	0.4256	0.5744	0.1374	0.8626
	67	0.3105	0.6895	0.0737	0.9263
	46	0.4511	0.5489	0.0905	0.9095
	11	0.5849	0.4151	0.1046	0.8954

图 7 给出了 3 种交易类型的交易市场和传统 Zcash 交易类型的交易市场的社会福利统计. 从图 7 可以看出, 在基于传统 Zcash 交易类型的市场中, 社会福利在初始轮次时与三类型交易市场的社会福利接近, 随后表现出波动下降的趋势, 从 400 轮左右开始保持在低水平波动; 而三类型交易市场的社会福利在前 100 轮左右保持快速增长, 随后表现出剧烈波动, 且随着轮次增加, 波动幅度减小, 波动区间的最小值缓慢增加. 从总体上来看, 三类型交易市场的社会福利高于传统交易市场. 可能的原因为当用户动作集包含 CoinJoin 交易类型时, 用户可以通过合作博弈形成 CoinJoin 匿名集来保留选择非屏蔽交易的用户身份价值, 同时由于非屏蔽交易和屏蔽交易的大小差异, 交易市场打包 CoinJoin 交易理论上可以使更多用户发起的交易被打包, 在一定程度上提高了市场用户的总效用. 在 3 种类型的交易市场中, CoinJoin 交易类型为中低类型的用户提供了低成本高匿名性的类型选项, 使得恶意竞价现象得到一定程度的遏制. 而在传统 Zcash 交易市场中, 由于恶性竞价导致的 f_z 和 f_t 的单价趋同现象更为明显, 该场景下 D 值处于较高和较低之间的用户选择屏蔽交易或非屏蔽交易而被自私矿工打包的概率也随着时间趋同, 且在屏蔽交易的成本 (f_z) 过高情况下, 由屏蔽交易保留的匿名也不再能为用户获得相对非屏蔽交易类型更多的效用, 用户的最优策略逐渐趋向于选择非屏蔽交易. 他们的策略选择呈现为: 博弈前期倾向选择屏蔽交易类型, 当交易市场中交易费用抬高到一定程度时, 倾向于选择非屏蔽交易类型.

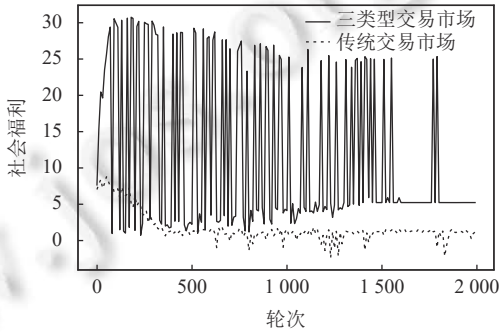


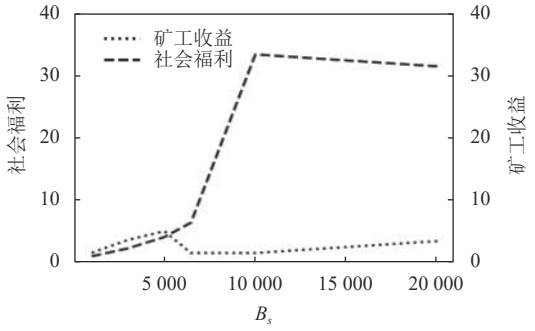
图 7 3 种交易类型的交易市场和传统交易市场的社会福利

4.5 B_s、θ、$plnum$ 对市场的影响

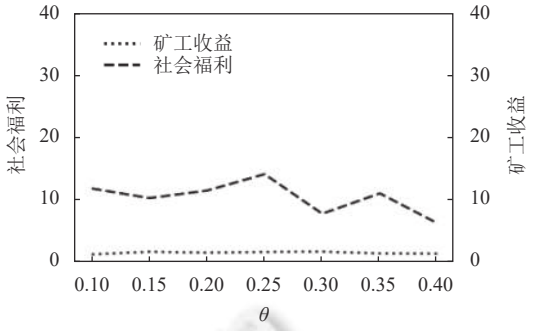
本节讨论了区块大小 B_s (Bsize)、折扣因子 θ 和用户总数 $plnum$ 对加密货币交易市场和用户行为的影响, 在拥有相同用户集和参数设置的三类型交易市场博弈中, 以第 4.2 节的实验设置条件为基准, 本文选取了不同的 B_s、θ 和 $plnum$ 进行对比实验, 并统计了在市场博弈收敛后的 1 750–2 000 轮中矿工收益、社会福利以及用户选择倾向的平均值, 统计结果如下所示. 在实际的区块链交易市场中, 每日活跃的用户数为十万数据量级, 但由于仿真实验的运行需要大量时间, 且时间成本随用户总数的增加而递增, 本节仅选取了用户总数 $plnum$ 为 25、50、75、100、200 的交易市场进行实验.

如图 8(a) 所示, 改变区块的大小 (B_s) 对于交易市场的影响是巨大的. 由图 8(a) 可得, 当 B_s 从 1 000 增加到 5 000 时, 市场的社会福利缓慢上升, 在 B_s 为 10 000 的时候, 市场的社会福利出现了剧烈的变化, 社会福利从 3 左右升到了接近 33 的顶峰. 尽管 B_s 为 20 000 时, 社会福利出现了小幅度的下降, 但从整体上来看更大的区块可以为市场带来更高的社会福利.

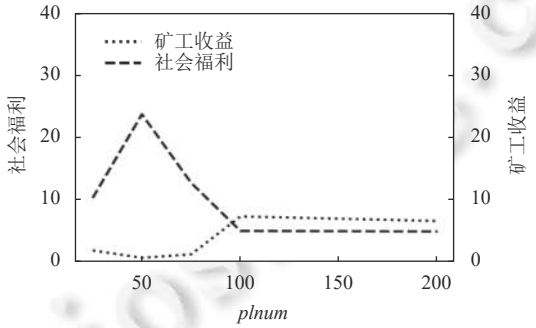
而从图 9(a) 中可以看出, B_s 为 3 000 时交易市场中接近 20% 的用户倾向于选择 CoinJoin 交易, 而 B_s 到了 10 000 时, 接近 100% 的用户倾向于选择 CoinJoin 交易. 当区块的大小足够装下所有的用户共同发起的 CoinJoin 交易时, 相较于屏蔽交易, CoinJoin 在远低于屏蔽交易的成本下, 表现出了接近于屏蔽交易的匿名性保护, 因而用户倾向于选择 CoinJoin 交易; 而当区块的大小小到只能装下很少数目的交易时, CoinJoin 匿名集与屏蔽交易相比, 无法提供给用户足够的匿名保护, 用户对于屏蔽交易的倾向高于 CoinJoin 交易, 非屏蔽交易的倾向远高于另两种交易类型. 因为在这种条件下, 非屏蔽交易被成功打包的概率远高于另两种类型.



(a) 不同 B_s 下的矿工收益和社会福利

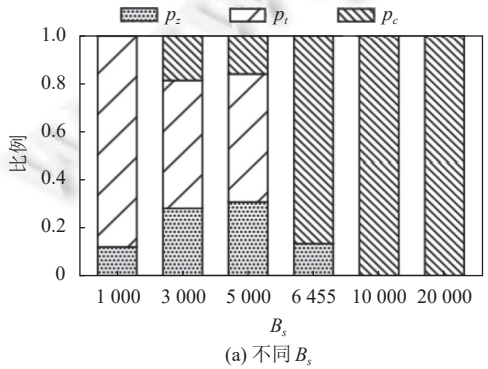


(b) 不同 θ 下的矿工收益和社会福利

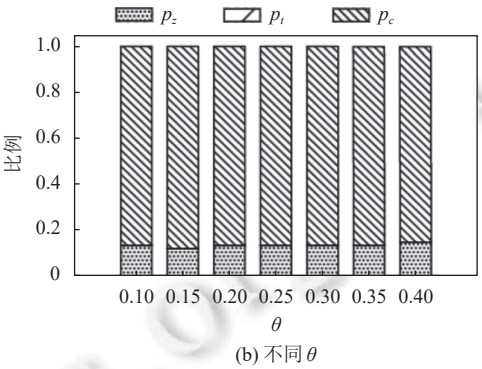


(c) 不同 *plnum* 下的矿工收益和社会福利

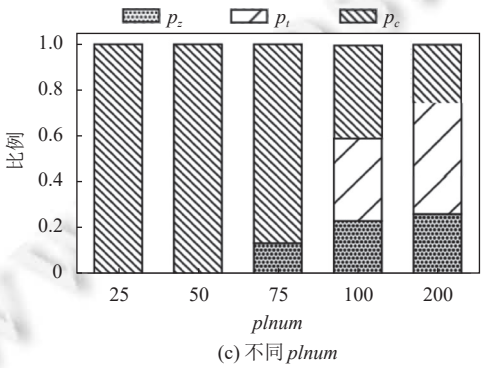
图 8 不同参数下的矿工收益和社会福利



(a) 不同 B_s



(b) 不同 θ



(c) 不同 *plnum*

图 9 不同参数下用户的交易选择倾向

对于矿工而言, 矿工的收益在 B_s 为 5000 时到达顶峰, 6455 时出现明显下降, 之后又呈现了上升趋势并保持平稳; 对整个交易市场而言, 较大区块有效遏制了恶性竞价现象, 整个交易市场的社会福利有了明显的提升. 恶性竞价的现象减缓意味着用户不再需要不断提高自己的交易费用来吸引矿工的快速打包, 用户仅支付少量的交易费用, 就可以确保交易被矿工打包. 由于模拟市场中的玩家数量是固定的, 矿工的打包收益不会因为 B_s 的增大, 而无限制地增长下去. 本文的仿真实验表明用户获得最高效用的理想区块大小 B_s 应该在 10000 左右. 本文还对不同 B_s 下 *plnum* 为 25 的交易市场博弈进行了实验, 图 10 中记录了交易市场的矿工收益和社会福利, 在区块大小为 3000 时交易市场的社会福利最高, 不同用户总数对用户获得最高效用的理想区块大小产生了影响.

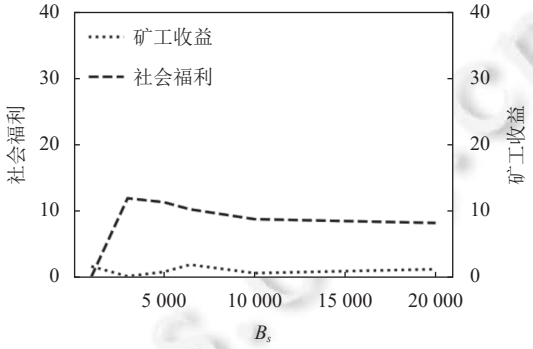


图 10 不同 B_s 下 *plnum* 为 25 时的矿工收益和社会福利

如图 8(b) 所示, 不同 θ 下的矿工收益在总体上没有差别, 不同 θ 下的社会福利呈现出了小范围波动, 随着 θ 的增长, 社会福利的变化趋势先表现为下降, 而后上升, θ 为 0.25 时社会福利达到最高值, 之后又表现出了先下降, 后上升再下降的趋势. 如图 9(b) 所示, θ 的改变对交易市场中用户对于交易类型的选择倾向影响不大. θ 的大小表征了简单非屏蔽交易保留的用户身份价值, 即 $\theta \times D$. 随着 θ 从 0.1 增长到 0.4, 用户选择不同交易的倾向变化不大, 市场中始终呈现出绝大多数的用户倾向于选择 CoinJoin 交易, 而剩余用户倾向于选择屏蔽交易的情况.

从图 9(c) 中可知, 用户总数较大即市场的交易流通量大时, 实验结果与 B_s 较小时十分接近, 用户对于 CoinJoin 的选择倾向下降, 对于屏蔽交易和非屏蔽交易的选择倾向增加, 且倾向选择非屏蔽交易的用户比例最高. 而用户总数较小即市场的交易流通量小时, 实验结果与 B_s 较大时十分接近, 用户倾向于选择 CoinJoin 交易. 社会福利和矿工收益的变化与用户总数 *plnum* 密切相关, 根据图 9(c) 所示, *plnum* 为 25、50、70 时, 交易市场中选择 CoinJoin 的用户为主导, 社会福利在用户总数较小的情况下仍远高于 *plnum* 为 100、200 的交易市场. 矿工收益则表现出了与社会福利相反的趋势.

以不同 *plnum* 下用户的平均屏蔽交易费用为例, 本文统计并讨论了不同市场交易流通量下用户的交易费用变化趋势, 从图 11 中可以看出用户交易费用并不是随着市场交易流通量的增加而增加的, 用户交易费用的变化与市场中用户的交易选择倾向有关. 在 *plnum* 为 100 和 200 的交易市场中用户对 3 种交易类型都表现出了选择倾向, 交易市场中费用的抬价情况表现更为明显, 交易费用快速增长, 并在在 250 轮左右到达峰值并持续波动, *plnum* 为 25、50、75 的交易费用则表现出缓慢增长, 始终保持在较低水平. 2000 轮时 *plnum* 为 200 的交易市场用户平均屏蔽交易费用比 *plnum* 为 25 的交易市场高了 170.11%.

综上所述, 对用户而言, 在区块过小即市场中的交易流通量过大时, 恶性竞争的存在会使用户倾向去选择屏蔽交易, 同时受到区块的大小限制, 更多用户选择非屏蔽交易, 而在理想的情况下, 市场交易流通量较小, 区块大小足够大时, 用户会在保障匿名性的同时选择低成本的 CoinJoin 交易. 同时市场交易流通量大时, 用户决策行为导致市场的交易费用远高于交易流量小时的交易费用, 本文建议 Zcash 根据市场交易流通量为用户提供动态的屏蔽交易默认费用, 在尽可能避免恶意链接的前提下, 减小用户的匿名成本.

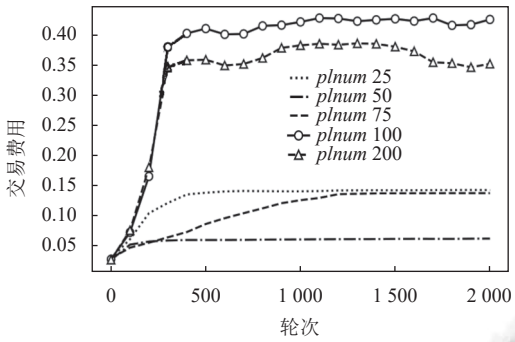


图 11　不同 *plnum* 下的用户平均屏蔽交易费用

5 总　结

本文将博弈论应用于加密货币交易市场中的用户决策优化, 并以 Zcash 为例, 建立了一个通用的加密货币交易市场模型, 对隐私敏感程度不同的用户为研究对象, 通过对交易过程的模拟, 讨论了用户对不同交易类型的策略. 从交易市场的特点出发, 本文建立了两个博弈模型, 一个是研究了匿名集在 CoinJoin 中的边际收益的合作博弈模型, 另一个是讨论交易之间的竞争的非合作博弈模型, 分别模拟了 CoinJoin 匿名集的形成和整个交易市场的交易过程. 此外, 本文的算法适用于任意用户数量的交易市场. 由于本文模型没有对特定的加密货币和交易类型进行建模, 本文的交易市场模型可以扩展到任意种类比特币的加密货币交易市场中去. 本文在第 4 节对三类型交易市场、无屏蔽类型交易市场和传统 Zcash 交易市场进行了模拟实验, 证明了模型对不同加密货币市场的适用性.

本文通过无悔学习算法模拟了用户在加密货币交易市场中的博弈过程, 克服了现有工作对用户行为分析不够深入等问题, 使用 ApproShapley 算法简化了合作博弈的求解过程, 讨论了用户根据不同的隐私需求选择的交易类型的变化趋势. 本文的仿真实验显示了用户根据不同的隐私需求选择的交易类型的变化趋势. 仿真结果表明, 在交易市场中, 用户受到交易被成功打包的收益激励, 他们之间会发生交易费用的恶性竞争, 交易费用的增加会在一定程度上影响用户的交易选择. 身份价值评估, 即隐私敏感度不同的用户有不同的选择. 在本文三类型交易市场场景中, D 值较高的用户更喜欢屏蔽交易, D 值较低的用户倾向于选择 CoinJoin 交易. CoinJoin 交易除了为用户提供了一种交易选择, 还在一定程度上遏制了交易费用的恶性竞争, 使用户获得更高的效用. 此外, 更大的区块大小也能遏制交易费用的恶性竞争, 区块的大小较大或市场交易流通量较小时, 几乎所有用户都倾向选择 CoinJoin 交易. 而在传统 Zcash 交易市场和无屏蔽交易市场中, 随着交易费用不断抬升, 出于对降低费用、提高打包概率的考量, 大多数用户表现出对非屏蔽交易的选择倾向. 本文提供了多种加密货币市场的博弈模型, 除了分析用户交易行为, 能够有效地帮助研究人员理解不同加密货币交易市场博弈, 揭示市场运行规律.

本文的实验结果展示了用户对两种匿名技术选择的差异, 除了 CoinJoin 和 Zcash 外, 还讨论了区块大小、折扣因子和用户数量对交易市场和用户行为的影响. 实验结果表明, 不同的用户数量和区块大小会对用户的选择倾向产生显著影响. 在用户数量小、区块大小大的情况下, 用户倾向于 CoinJoin 交易; 在用户数量大、区块大小小的情况下, 用户的倾向转向屏蔽交易和非屏蔽交易. 此外, 本文讨论了不同交易流通量下交易费用的变化, 为 Zcash 市场的默认费用定价提供了参考. 受到篇幅限制, 本文仅对 Zcash 和 CoinJoin 技术进行了讨论, 而在实际区块链市场中, 门罗币、达世币等加密货币也为用户提供了增强的隐私保护, CoinShuffle、Xim 等匿名技术也可以提高交易的不可链接性. 本文的通用交易市场模型可扩展性强, 未来可以添加其他类型的交易, 还可以应用到其他匿名货币的交易市场, 本文希望在未来的工作中讨论更多类型的匿名技术.

本文在模拟中固定了用户数量, 由于 Zcash 对涉及屏蔽池的交易进行了信息隐藏, 缺少对于用户身份价值的准确衡量标准, 模拟没有在真实链上环境进行, 但本文的模型确实捕捉到了用户在加密货币市场中的行为博弈, 并对不同的市场类型下的模拟结果进行了深入分析和讨论. 如 Spiegelman 等人[39]提出的多币系统挖掘博弈模型, 他

们通过纯理论的博弈分析, 讨论了多币系统中矿工的挖矿行为并提出针对多币系统的奖励设计攻击, 本文基于对交易市场博弈的模拟结果, 给出了缓解市场恶性竞争的区块大小和定价建议, 希望为未来的加密货币交易市场设计提供可能的参考. 由于讨论基于模拟展开, 不可避免地存在一定局限性, 本文希望在未来引入链上环境, 讨论动态用户集合参与市场的过程, 更加真实地模拟用户在交易市场中的行为.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[2] Taskinsoy, J. Bitcoin nation: The world's new 17th largest economy. 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794634

[3] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018, 29(7): 2092–2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[4] Bonneau J, Narayanan A, Miller A, Clark J, Kroll JA, Felten EW. Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Proc. of the 18th Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer, 2014. 486–504. [doi: 10.1007/978-3-662-45472-5_31]

[5] Maxwell G. CoinJoin: Bitcoin privacy for the real world. 2013. https://bitcointalk.org/index.php?topic=279249.0

[6] Duffield E, Diaz D. Dash: A privacy-centric cryptocurrency. Journal of Systems Integration, 2015(1): 19–31. [doi: 10.20470/jsi.v9i1.335]

[7] Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from Bitcoin. In: Proc. of the 2014 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2014. 459–474. [doi: 10.1109/SP.2014.36]

[8] Arce DG, Böhme R. Pricing anonymity. In: Proc. of the 22nd Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer, 2018. 349–368. [doi: 10.1007/978-3-662-58387-6_19]

[9] Gao S, Li ZC, Peng Z, Xiao B. Power adjusting and bribery racing: Novel mining attacks in the Bitcoin system. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 833–850. [doi: 10.1145/3319535.3354203]

[10] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. In: Proc. of the 18th Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer, 2014. 436–454. [doi: 10.1007/978-3-662-45472-5_28]

[11] Lewenberg Y, Bachrach Y, Sompolinsky Y, Zohar A, Rosenschein JS. Bitcoin mining pools: A cooperative game theoretic analysis. In: Proc. of the 2015 Int'l Conf. on Autonomous Agents and Multiagent Systems. Istanbul: Int'l Foundation for Autonomous Agents and Multiagent Systems, 2015. 919–927.

[12] Carlsten M, Kalodner H, Weinberg SM, Narayanan A. On the instability of Bitcoin without the block reward. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 154–167. [doi: 10.1145/2976749.2978408]

[13] Möser M, Böhme R. Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees. In: Proc. of the 2015 Int'l Conf. on Financial Cryptography and Data Security. San Juan: Springer, 2015. 19–33. [doi: 10.1007/978-3-662-48051-9_2]

[14] Houy N. The economics of Bitcoin transaction fees. GATE WP, 1407: 2014. [doi: 10.2139/ssrn.2400519]

[15] Rizun PR. A transaction fee market exists without a block size limit. 2015. https://www.bitcoinunlimited.info/resources/feemarket.pdf

[16] Kroll JA, Davey IC, Felten EW. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proc. of the 12th Workshop on the Economics of Information Security. Washington DC, 2013. 11.

[17] Abramova S, Schöttle P, Böhme R. Mixing coins of different quality: A game-theoretic approach. In: Proc. of the 2017 Int'l Conf. on Financial Cryptography and Data Security. Cham: Springer, 2017. 280–297. [doi: 10.1007/978-3-319-70278-0_18]

[18] Shen M, Sang AQ, Zhu LH, Sun RG, Zhang C. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency. Chinese Journal of Computers, 2021, 44(1): 193–208 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.00193]

[19] Malinova K, Park A. Market design with blockchain technology. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2785626

[20] Li JJ, Yuan Y, Wang S, Wang FY. Transaction queuing game in Bitcoin blockchain. In: Proc. of the 2018 IEEE Intelligent Vehicles Symp. (IV). Changshu: IEEE, 2018. 114–119. [doi: 10.1109/IVS.2018.8500403]

[21] Lavi R, Sattath O, Zohar A. Redesigning Bitcoin's fee market. In: Proc. of the 2019 World Wide Web Conf. San Francisco: ACM, 2019. 2950–2956. [doi: 10.1145/3308558.3313454]

[22] Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system. In: Altshuler Y, Elovici Y, Cremers AB, Aharony N, Pentland A, eds. Security and Privacy in Social Networks. New York: Springer, 2013. 197–223. [doi: 10.1007/978-1-4614-4139-7_10]

[23] Zhang A, Bai XY. Survey of research and practices on blockchain privacy protection. Ruan Jian Xue Bao/Journal of Software, 2020, 31(5): 1406–1434 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[24] Wang CX, Cheng JC, Sang XX, Li GD, Guan XH. Data privacy-preserving for blockchain: State of the art and trends. Journal of Computer Research and Development, 2021, 58(10): 2099–2119 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2021.20210804]

[25] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In: Proc. of the 19th European Symp. on Research in Computer Security. Wroclaw: Springer, 2014. 345–364. [doi: 10.1007/978-3-319-11212-1_20]

[26] Bissias G, Ozisik AP, Levine BN, Liberatore MD. Sybil-resistant mixing for Bitcoin. In: Proc. of the 13th Workshop on Privacy in the Electronic Society. Scottsdale: ACM, 2014. 149–158. [doi: 10.1145/2665943.2665955]

[27] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin. In: Proc. of the 2015 Int'l Conf. on Financial Cryptography and Data Security. San Juan: Springer, 2015. 112–126. [doi: 10.1007/978-3-662-48051-9_9]

[28] Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain Bitcoin transactions. In: Proc. of the 2016 Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2016. 43–60. [doi: 10.1007/978-3-662-53357-4_4]

[29] Kappos G, Yousaf H, Maller M, Meiklejohn S. An empirical analysis of anonymity in Zcash. In: Proc. of the 27th USENIX Conf. on Security Symp. Baltimore: USENIX Association, 2018. 463–477.

[30] Zhang ZY, Li WH, Liu HT, Liu JW. A refined analysis of Zcash anonymity. IEEE Access, 2020, 8: 31845–31853. [doi: 10.1109/ACCESS.2020.2973291]

[31] Biryukov A, Feher D, Vitto G. Privacy aspects and subliminal channels in Zcash. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 1813–1830. [doi: 10.1145/3319535.3345663]

[32] Zcash Foundation and Electric Coin Company. Privacy and convenience. 2021. https://z.cash/

[33] zkSNACKs Ltd. Wasabi wallet-bitcoin privacy wallet with built-in CoinJoin. 2023. https://www.wasabiwallet.io/

[34] Peleg B, Sudhölter P. Introduction to the Theory of Cooperative Games. Berlin: Springer, 2007. [doi: 10.1007/978-3-540-72945-7]

[35] Hart S, Mas‐Colell A. A simple adaptive procedure leading to correlated equilibrium. Econometrica, 2000, 68(5): 1127–1150. [doi: 10.1111/1468-0262.00153]

[36] Castro J, Gómez D, Tejada J. Polynomial calculation of the Shapley value based on sampling. Computers & Operations Research, 2009, 36(5): 1726–1730. [doi: 10.1016/j.cor.2008.04.004]

[37] Arora S, Hazan E, Kale S. The multiplicative weights update method: A meta-algorithm and applications. Theory of Computing, 2012, 8(1): 121–164. [doi: 10.4086/toc.2012.v008a006]

[38] Buşoniu L, Babuška R, De Schutter B. Multi-agent reinforcement learning: An overview. In: Srinivasan D, Jain LC, eds. Innovations in Multi-agent Systems and Applications-1. Berlin: Springer, 2010. 183–221. [doi: 10.1007/978-3-642-14435-6_7]

[39] Spiegelman A, Keidat I, Tennenholtz M. Game of coins. In: Proc. of the 41st IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Washington DC: IEEE, 2021. 954–964. [doi: 10.1109/ICDCS51616.2021.00095]

附中文参考文献:

[3] 刘敖迪, 杜学绘, 王娜, 李少卓. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, 29(7): 2092–2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[18] 沈蒙, 桑安琪, 祝烈煌, 孙润庚, 张璨. 基于动机分析的区块链数字货币异常交易行为识别方法. 计算机学报, 2021, 44(1): 193–208. [doi: 10.11897/SP.J.1016.2021.00193]

[23] 张奥, 白晓颖. 区块链隐私保护研究与实践综述. 软件学报, 2020, 31(5): 1406–1434. http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[24] 王晨旭, 程加成, 桑新欣, 李国栋, 管晓宏. 区块链数据隐私保护: 研究现状与展望. 计算机研究与发展, 2021, 58(10): 2099–2119. [doi: 10.7544/issn1000-1239.2021.20210804]

毕红亮(1989－), 男, 博士, 助理教授, CCF 专业会员, 主要研究领域为物联网感知和安全.

伊心静(2000－), 女, 硕士生, 主要研究领域为区块链, 人工智能安全.

陈艳姣(1989－), 女, 博士, 教授, CCF 专业会员, 主要研究领域为计算机网络, 网络安全.

汪旭(1996－), 男, 硕士, 主要研究领域为区块链, 网络经济学, 网络安全.