

基于 CoinJoin 实现的混币交易检测方法 ——以 Wasabi 平台为例

李虎^{1,2,3}, 陈云芳^{1,2,3}, 张伟^{1,2,3}

(1. 南京邮电大学计算机学院, 江苏 南京 210023; 2. 南京邮电大学软件学院, 江苏 南京 210023;
3. 南京邮电大学网络空间安全学院, 江苏 南京 210023)

摘要: 混币技术为加强用户交易隐私而设计, 但对“加密货币”监管使用的地址聚类规则造成严重干扰, 因而常被黑客用作洗钱工具实现资金逃逸, 这引发了金融监管部门对混币交易检测的关注。目前混币交易检测工作大多停留在单纯的数据分析与统计阶段, 对混币交易的内部细节缺乏清晰的认知, 并且没有可信的验证数据, 因而检测方法的效果缺少可信度。CoinJoin 是去中心化混币的代表性思想, Wasabi 是基于此思想实现的商用方案中比较流行的一种。结合 CoinJoin 概念及其限制交易匿名集大小和混币金额的特点, 提出了 CoinJoin 混币交易的通用检测方法: CoinJoin 混币交易为多输入多输出交易, 具有交易输出项个数大于输入中 UTXO 个数和输出项金额中存在大量重复值的特点。将 CoinJoin 的通用检测方法及相关研究中提到的 Wasabi 混币交易的部分特征相结合, 得到了对于 Wasabi 的基础检测方法并完成检测。从 Wasabi 平台服务接口处获得可信验证数据集, 对该数据集分析并完成两项工作: 一是对 Wasabi 基础检测方法中的规则参数进行调准; 二是提出交易输出项金额中重复值的最高频次与输入中 UTXO 个数比值的新指标, 该指标可用来衡量用户参与混币金额的自由度。在这两项工作的基础上, 得到用于 Wasabi 的改进检测方法。实验表明: Wasabi 基础检测方法的召回率为 94.2%, 准确率为 67.2%; 经过可信验证数据集的分析反馈, 改进检测方法的召回率达到 100%且准确率在 99%以上。根据通用检测方法对整个 CoinJoin 类型的混币交易的总市场规模进行预测评估, 得出结论: 当今市场中 CoinJoin 混币交易占有比特币交易的数量上限为 1.9%, 金额上限为 3.7%。

关键词: CoinJoin; Wasabi; 混币交易检测; 地址聚类

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023089

Detection method of mixed coin transaction based on CoinJoin ——take the Wasabi platform as an example

LI Hu^{1,2,3}, CHEN Yunfang^{1,2,3}, ZHANG Wei^{1,2,3}

1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

收稿日期: 2022-10-26; **修回日期:** 2023-03-09

通信作者: 张伟, zhangw@njupt.edu.cn

基金项目: 国家重点研发计划 (2019YFB2101701)

Foundation Item: The National Key R&D Program of China (2019YFB2101701)

引用格式: 李虎, 陈云芳, 张伟. 基于 CoinJoin 实现的混币交易检测方法——以 Wasabi 平台为例[J]. 网络与信息安全学报, 2023, 9(6): 140-153.

Citation Format: LI H, CHEN Y F, ZHANG W. Detection method of mixed coin transaction based on CoinJoin——take the Wasabi platform as an example[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 140-153.

2. School of Software, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
3. School of Cyberspace Security, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: Designed to enhance the privacy of user transactions, mixed coin technology has created disruptions to the address clustering rules typically used for cryptocurrency regulation. Consequently, hackers have begun utilizing mixed coin technology as a tool for money laundering and fund evasion, which has raised concerns among financial regulators regarding the detection of mixed coin transactions. Currently, most detection methods for mixed coin transactions rely on data analysis and statistics, lacking a comprehensive understanding of the internal workings of these transactions. This lack of knowledge may undermine the credibility and effectiveness of detection methods due to the absence of reliable verification data. CoinJoin, a decentralized mixed coin concept, represents one approach, and commercial implementations like Wasabi have gained popularity. Drawing from the characteristics of CoinJoin and its restriction on the size of anonymous transaction sets and mixed coin amounts, a general detection method for CoinJoin mixed coin transactions was devised. Such transactions typically involved multiple inputs and outputs, with more output items than UTXOs in the input, and a high occurrence of duplicate values among the output amounts. A basic detection method for Wasabi was developed by combining the generic detection method for CoinJoin with specific features of Wasabi, as identified in related studies, to complete the detection process. A trusted validation dataset was acquired from the Wasabi platform service interface, and this dataset was analyzed to achieve two objectives. First, the alignment of rule parameters in the Wasabi base detection method was accomplished. Second, a new metric was proposed, measuring the ratio of the highest frequency of duplicate values in the output amount of transactions to the number of UTXOs in the input. This metric assessed the level of user participation in mixed coin transactions, providing a measure of user freedom. Using these two approaches, significant progress is made in the detection of mixed coin transactions. The experiments show that the recall rate of Wasabi's basic detection method is 94.2% and the accuracy rate is 67.2%. After the analytical feedback from the credible validation dataset, the recall rate of the improved detection method reaches 100% and the accuracy rate is above 99%. The total market size of the entire CoinJoin type of mixed coin transactions was evaluated and predicted based on a common test methodology. It is concluded that the number of CoinJoin mixed coin transactions in today's mixed coin market represents 1.9 per 1 000 of all Bitcoin transactions and 3.7 per 1 000 of the transaction value at most.

Keywords: CoinJoin, Wasabi, mixed coin transaction detection, address clustering

0 引言

2008 年, Nakamoto 在文献[1]中提出比特币。比特币具有去中心化、开放性、安全性、独立性和匿名性等特征, 现今已取得巨大成功。2021 年 11 月 8 日, 比特币的总市值达到 12 373 亿美元, 交易市场十分庞大。文献[2]表明, 匿名性是比特币能够取得巨大成功的重要原因之一。

比特币的隐私保护基于用户匿名, 即用户可以使用哈希算法由公钥来创建自己的交易地址而无须担心被他人得知该账户与其本人的从属关系。但为了解决“双花”问题并实现其交易不易篡改的特性, 每个用户的交易记录(包括交易双

方的账户信息和交易金额)都会被记录在比特币链上以供查询和验证。针对这一特点, 文献[3-5]根据若干条源自比特币交易结构特征的启发式规则设计出了地址聚类技术, 可以根据交易记录分析将属于同一用户的交易地址聚类到同一集合内, 证明了这种以账户匿名性提供的隐私保护是不够安全的。此外, 货币交易所被监管机构要求实了解客户(KYC, know your client)和反洗钱(AML, anti-money laundering)政策, 比特币保护金融隐私受到了强烈质疑。针对如何满足区块链“数字货币”不断增强的隐私保护需求, 从是否兼容现有的货币体系的角度分, 有两种解决方案。

兼容性方案的设计表现为不改变现有货币体系,即采用某些特殊的交易方式来增强隐私保护,如混币技术通过在一次交易中引入无关的第三方周转或混淆自己的交易记录以达到应对地址聚类技术的目的。用户无须更换自己使用的货币体系,仅需要在交易时采取相关手段即可保护自己的隐私,该方案的特点体现为兼容性。

不兼容性方案直接抛弃原有的隐私保护力度不足的“货币”,如比特币,转而通过在新的“加密货币”系统中引入其他密码学技术来实现对用户交易隐私的保护,如采用环签名和加密地址的 Monero 币^[6]、采用零知识证明的 ZeroCash^[7]以及从硬件层次出发在区块链系统中引入可信执行环境(TEE, trusted execution environment)来保护高价值数据^[8]。

随着兼容性和不兼容性两种方案的发展和应用,“加密货币”的隐私保护力度逐步加强,但其因此面临金融监管等诸多争议。

不兼容的方案,如 Monero 币等以隐私保护为特色的“加密货币”。根据国际机构金融行动特别工作组的监管要求,日本和韩国的金融部门已要求“加密货币”交易所将 Monero 币等强隐私保护币种摘牌下架以确保其遵守 AML 政策^[9]。

作为兼容性方案中的代表性技术,混币领域已经出现多例黑客盗币后通过混币器隐匿洗钱交易路径的案例^[10],这使得金融监管机构对混币器的态度发生了改变,其成为众多严格遵守 KYC 和 AML 政策的交易所的防范对象。2019 年 12 月,币安交易所暂停了一个用户账户,原因是这名用户试图将比特币发送到 Wasabi 钱包;2020 年 10 月,美国金融犯罪执法网络局对提供比特币混币服务的 Helix 创始人 Larry Dean Harmon 罚款 6 000 万美元,检方指控其违反反洗钱规则;2022 年 8 月,美国财政部将以太坊混币器 Tornado Cash 和一系列与该服务相关的地址添加到美国特别指定国民名单中进行限制。

除了政府部门的金融管制,在技术监管层面,对于使用环签名和零知识证明的 Monero 和 ZeroCash,文献[11]从网络通信层次出发,使用远程旁道攻击得到用户交易内容和身份信息,破坏

交易的不可链接性和用户匿名性;文献[12]利用环签名机制在交易使用的关联性上存在隐私问题,分析 Monero 币用户的使用习惯,对环匿名交易进行可追踪分析,找出了部分用户的真实地址。至于使用可信执行环境来实现隐私保护的区块链系统,除了存在降低系统性能的问题,还因节点间信息传输的一致性而存在适用范围的局限性问题,其更适用于共识机制较为确定的联盟链,被用来保护高敏感和高价值数据^[13],因此对其监管需求并不迫切。

对于兼容性方案中的混币技术,其依托于比特币庞大的体量,仍有巨大的市场,但对其监管方向的研究目前并不丰富。从合法用户的角度看,混币技术只是其追求隐私保护的工具体,并不反对监管需求,因此需要新的与监管兼容的混币方法;从监管的角度看,限制混币的行为本身只能影响到有一定规模的商用混币,而任何用户群体都可以私下组织进行混币,如地下钱庄,因此与其对其进行限制不如研究其技术内核寻找缺点而进行监管。综上,无论是从用户角度还是从监管角度出发,对混币的研究都具有重要意义。开展混币研究的前提是获取混币交易的样本,这是目前的研究难点之一。前文已提到过,混币交易是兼容现有货币体系的,其实质仍是一个正常的交易,除了通过特殊的交易参与模式保证混淆交易双方的交易关系外,混币服务商一般不会对外标记混币交易,因为作为一个正常的交易发布正是混币交易隐私保护的外衣,这就造成了混币研究的困境,即缺少真实样本。

不同于以往从样本分析提取特征得到检测方法的技术路线,本文从 CoinJoin 混币交易模型本身及其安全性分析出发设定检测条件,并结合真实的混币样本做检测方法改进,不仅得到具有高准确率的检测方法,而且为这些检测方法提供理论和实践支撑,有助于更好地理解 CoinJoin 混币交易内核。本文提出的检测方法并不依赖于特定的 CoinJoin 混币实现(如本文采用的 Wasabi)的数据特征,可以据此对所有实现 CoinJoin 思想的混币进行检测。本文贡献如下。

1) 建立了 CoinJoin 类型混币安全性分析的数学模型,以此为基础分析了当前混币服务基于

安全性考虑而做出的改变，据此提出了 CoinJoin 类型混币交易的通用检测方案。

2) 将得到的通用检测方案与 Wasabi 混币服务的真实混币交易样本结合，得到用于 Wasabi 的混币检测方案，检测召回率达到 100%，准确率达到 99.0% 以上，这论证了所提通用检测方案的正确性。

3) 根据所提通用检测方案对当前市场上的 CoinJoin 混币服务规模进行了预测评估：其交易数量和交易金额占有所有交易的上限分别为 1.9% 和 3.7%。

1 背景知识

1.1 地址聚类技术

地址聚类技术是针对比特币弱匿名性的对抗技术，从用户角度来看，其又被称作交易账本关联攻击，本节介绍具体的聚类规则以及实现流程。

地址聚类的核心思想是：通过分析区块链账

本数据，利用用户常见的交易规律建立启发式聚类规则，构建账户地址与交易之间以及用户与账户地址之间的一对多对应关系，从而打破用户真实身份与账户地址间的匿名性。目前公认的启发式聚类规则有 3 条^[4-5]。

1) 对于一个具有多输入地址的交易，通常认为所有的输入地址都来自同一个用户个体或用户集合。

2) 一个 Coinbase 交易（比特币系统奖励矿工的交易，是区块内的第一个交易，只有输出没有输入）中的多个输出地址属于同一个用户的钱包地址集合。

3) 交易中找零地址和输入地址属于同一个用户。

根据这 3 条聚类规则和已经公开的交易记录，可以将所有地址划分为以用户或群体为基本单位的地址集合，地址聚类流程如图 1 所示。

一旦某个用户的某个地址与其真正身份产生关联关系，那么该地址所在的地址集合中的所

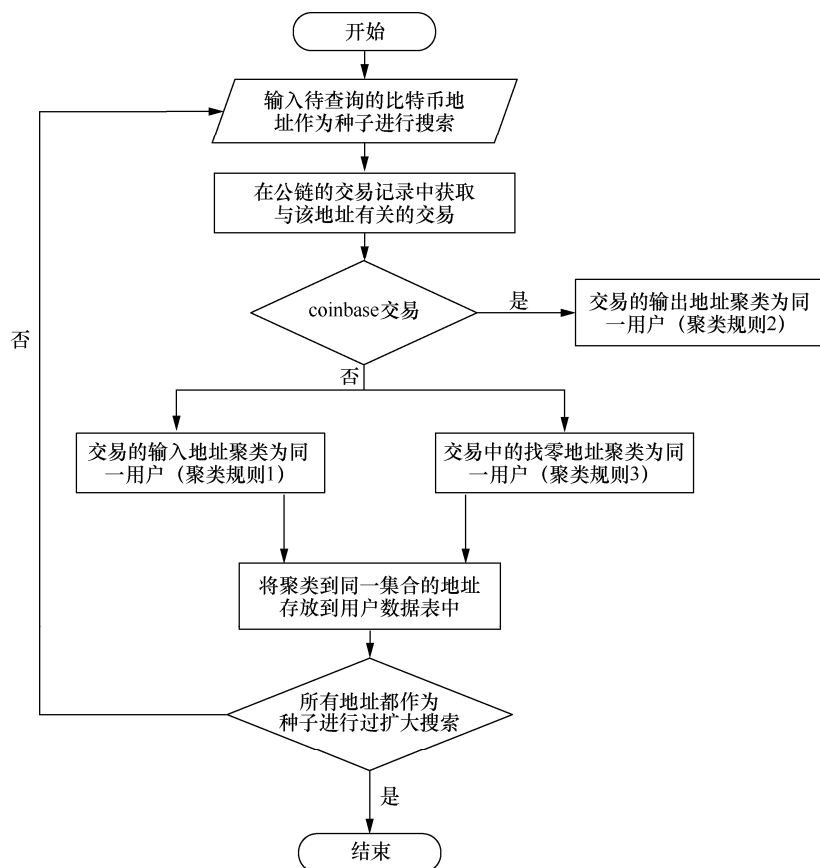


图 1 地址聚类流程

Figure 1 Process of address clustering

有地址即可确定身份。这种关联关系十分常见,如点对点之间的转账或者社交软件中的无意泄露。文献[4]在高校中构建了模拟的“加密货币”使用环境,通过搜集用户使用记录,并利用聚类规则进行分析挖掘得到40%左右用户的真实身份,对比特币的隐私保护提出挑战。

地址聚类技术打破了比特币由匿名性维护的弱隐私保护,一定程度上将比特币从隐私保护的代变变为半透明的金融工具。但是混币技术通过混合多笔交易共同发布来割裂交易中输入输出的强对应规则,以此破坏了地址聚类中最重要的多输入聚类的规则,有效地对抗了地址聚类。可以预见:如果地址聚类技术不加以改变,参与混币的人数越多,混币交易在链上出现越多,地址聚类的效果就会越差,结果表现为一个特定用户产生的地址集合中会包含许多其他用户的账户地址,聚类的准确率无法得到有效保障。目前已有相关实验表明,如果简单使用现有地址聚类方法在公链上进行聚类实验,最大的用户地址集合中包含1200万个交易地址^[14],这显然是受到了混币的影响而导致的非正常结果。

1.2 混币的概念和分类

混币技术的目的是在现有账户和交易混合后的账户之间创建随机的映射关系,从而打破交易中输入地址与输出地址的强对应关系,能够实现这一目的的技术,都可以称之为混币技术。

根据是否引入完全控制混币资金的第三方(中心化节点),商用混币体系分为中心化混币和去中心化混币。中心化混币技术有速度快和金额自由的优点,但存在用户需要信任服务商,中心化节点服务存在瓶颈且易被政府监管等问题;而去中心化混币技术则与其相反,其拥有较高的隐私保护力度,用户无须信任服务商,但存在速度较慢和金额受限等问题。

中心化混币即用户将原交易中的输入金额以及输出地址和对应手续费以一个交易的方式,交付到混币服务商提供的接收账户地址上,而混币服务商再通过另一个交易的方式将对应金额转入用户提供的输出地址上,中心化混币过程如图2所示。通过引入中间人的方式来达到混淆交易记录的目的,这个过程可能会重复多遍以

增强隐私。在这个过程中,用户要对混币服务商具备相当高的信任度,因为用户要承担服务商卷钱跑路和对外披露交易细节的风险。中心化混币服务的代表有BitLaundry、BlockChain.info、BitcoinFog等。

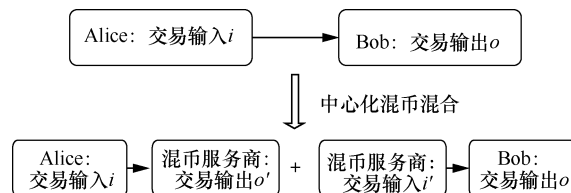


图2 中心化混币过程
Figure 2 Centralized mixed coin process

去中心化混币有多种实现思想^[15],如CoinJoin、PayJoin、CoinSwap等。其中的代表是CoinJoin思想^[16],其将多个交易聚合为同一个交易发布(即引入其他人的交易细节)从而达到输入与输出地址间的混淆,去中心化混币过程如图3所示。目前较为成熟的基于CoinJoin思想的商用方案有Wasabi^[17]、Samourai^[18]和JoinMarket^[19]等,本文选择Wasabi作为混币技术的研究对象。需要注意的是:这里提到的去中心化混币并不是完全没有第三方参与的,如果想达到一定的参与规模(即商业级别)的混币,仅靠用户自发地寻找其他用户完成混币效率是极其低的,会将自己的交易细节泄露给共同参与者,因此第三方中间节点的存在是必不可少的。但相对于中心化混币中处于支配位置的中心节点,去中心化混币的中心节点更多的是扮演一个辅助型角色,参与者并不需要信任该中心节点,中心节点无法对参与者造成经济和隐私上的损失。

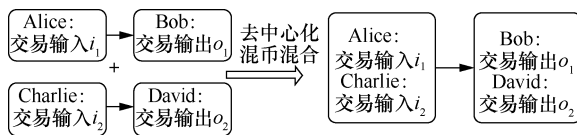


图3 去中心化混币过程
Figure 3 Decentralized mixed coin process

混币并不局限于比特币,在支持智能合约的币种中,混币的方案与比特币有所不同,其中心化的方案反而盛行,因为有智能合约担当中心化混币服务中的中间节点,用户更容易相信混币的公平和隐私性,如已经受到制裁的Tornado

Cash^[20]。但其并非纯智能合约模式的运行，在取款时仍需要中继（relayer）角色的参与，而该角色则由某些用户担任。

1.3 混币检测

与混币检测相关的研究主要聚焦在两个方面。其一是从应用出发研究商用的混币服务：如文献[21]对市场上主流的 3 款 CoinJoin 混币服务商（Wasabi、Samourai 和 JoinMarket）进行服务研究和使用探索，展示了参与这些平台混币的流程以及交易中的一些数值特点；文献[22]对 Wasabi 和 Samourai 两大服务商的混币交易进行检测，其检测设计基于对混币交易样本的分析，但是其用于分析的混币样本并不具备可信度；文献[23]对混币服务的交易模式进行划分，通过混币服务提供的公共应用程序接口（API，application program interface）获取相关服务商的混币交易数据并进行实验分析工作。其二是从理论出发研究混币交易的内在结构和数据特点：如“加密货币”数据网站使用基于交易数据的结构特征进行 CoinJoin 混币交易检测，并在交易详情页给出一个该交易是否有可能是 CoinJoin 混币交易的标签，但其准确度不高；文献[24]以区块数据构建交易图和用户图，从图分析角度论证了原始 CoinJoin 混币交易的分解和追踪的可行性，但未提出相关的分解或者追踪方法；文献[25]简单假设输入输出数量超过 5 的都为 CoinJoin 交易，该规则显然过于粗略，仅仅关注和匹配混币交易的部分特征。如上所述，目前对混币检测的相关研究存在缺陷：首先是使用的规则集不够完备，对混币检测的效果不佳；其次是缺少真实的混币样本以供分析和验证检测结果。

2 无验证的 Wasabi 混币交易检测

对 CoinJoin 具体实现方案的研究，本文采用 Wasabi 钱包内置的混币服务作为研究对象，Wasabi 是一个开源的、非托管的，以隐私为中心的桌面版比特币钱包，可实现无信任的 CoinJoin。其基于 ZeroLink 架构^[26]实现了 CoinJoin 类型的混币方案，在比特币混币服务中非常流行，同时可以通过爬虫程序爬取交易接口的方式获取到真实

的混币交易样本以供研究，这是本文选择 Wasabi 作为研究对象的重要原因。

混币服务商通常不会主动向外公开混币交易的相关数据，并以此作为混币交易的隐私性保障之一，所以对于混币交易的检测研究来说，没有真实的参考数据集来验证混币交易检测结果是首先要解决的问题。以往的相关研究中也注意到了这一点，但都没有给出完美的解决方案。“加密货币”数据网站中给出的“隐私性保障”一栏中会指出某个交易可能是混币交易，但其不能给出这个可能性的大小；文献[22]采用 GitHub 上公开的数据作为参考集来验证检测结果，然而该数据由检测工作获得，有效性未知。

尽管如此，仍要研究无验证 Wasabi 混币交易检测，但检测规则的分析与提取并非基于现今的相关工作，而从 CoinJoin 模型本身的安全性分析出发，这保证了本文提取到的检测规则具有理论支撑，不会偏离真实结果，并且这是加深对 CoinJoin 混币认知，揭开其面纱的重要过程。

本文采用真实的 Wasabi 混币交易样本集合来对检测结果验证并加以改进，得到准确率更高的检测方法，检测方法技术路线如图 4 所示。

2.1 CoinJoin 模型安全性分析

CoinJoin 的思想在 2013 年被提出，从最初的仅简单把多个交易聚合发布以实现混币效果，到出现了根据混币交易中子交易输入输出金额的对等关系进行逆向还原的对抗手段，再到现在的商用 CoinJoin 方案限制参与人数和参与金额来提升其交易的隐私性。通过其发展历程，可以认识到属于 CoinJoin 混币交易的某些本质特征，并将其量化作为检测规则。

设定一个交易为 $t = (I, O, v)$ ，其中 I 为输入地址集合， O 为输出地址集合， v 为地址与对应交易金额的映射关系。为了简化模型，忽略手续费的影响，针对一个具体的交易 t ，有如下关系成立。

$$\sum_{i \in I} v(i) = \sum_{o \in O} v(o) \quad (1)$$

CoinJoin 交易为普通交易的合集，设定 CoinJoin 混币交易为 t_{mix} 。

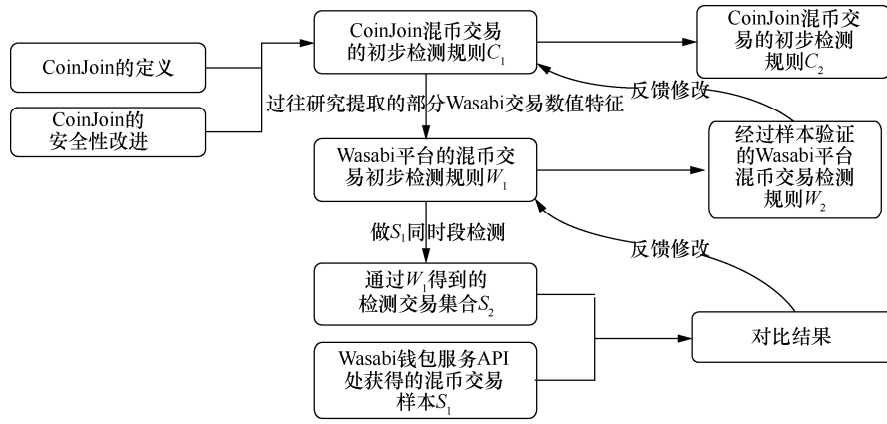


图4 检测方法技术路线
Figure 4 Technical route of detection method

$$t_{\text{mix}} = \{t_1, t_2, \dots, t_n\} \quad (2)$$

逆向分解一个 CoinJoin 交易，即将其还原到初始的未聚合状态，可供分析的信息仅有 t_{mix} 本身。分解的过程即还原映射关系，定义一个分解方案为 m_i 。

$$m_i = t_{i1} \cup t_{i2} \cup \dots \cup t_{in} \quad (3)$$

如果一个分解方案是可行的，应有如下关系。

$$\forall T_{ik}, (k \in [1, n]), \sum_{i \in I_{ik}} v(i) = \sum_{i \in O_{ik}} v(o) \quad (4)$$

$$I_{i1} \cap I_{i2} \cap \dots \cap I_{in} = \emptyset \quad (5)$$

$$I_{i1} \cup I_{i2} \cup \dots \cup I_{in} = I_{\text{mix}} \quad (6)$$

$$O_{i1} \cap O_{i2} \cap \dots \cap O_{in} = \emptyset \quad (7)$$

$$O_{i1} \cup O_{i2} \cup \dots \cup O_{in} = O_{\text{mix}} \quad (8)$$

所有可行的分解方案的合集为

$$M = \{m_1, m_2, \dots, m_n\} \quad (9)$$

显然， M 的规模 n 越大，得到该混币交易的正确分解路径的可能性就越低。目前针对原始的混合方案，可以根据其数值的对应特征进行逆向还原，CoinJoin Sudoku^[27] 就是这样的一个工具，可以以很高的置信度还原部分交易。因此为了对抗数值特征分析，产生了扩大交易匿名集和设定混币金额两种解决方案。

(1) 扩大交易匿名集

假设混币交易的输入集 I_{mix} 中共包含 n 个输入地址，那么理论上有效分解方案的个数上限为

$$\begin{aligned} |M|_{\text{max}} &\leq C_n^0 + C_n^1 + \dots + C_n^{n-1} = \\ (1+1)^n - C_n^n &= 2^n - 1 \end{aligned} \quad (10)$$

可见，随着输入集中输入地址的增加（即参与人数的增加），可能存在的分解方案个数以指数级别扩增。因此，扩大交易匿名集是一个有效增加破解混币交易难度的手段。在 Wasabi 提供的混币服务中，匿名集大小设定为 100^[21]，这可能会降低混币效率，但是可以更加有效地保护用户隐私。

(2) 设定混币金额

前文已提到混币破解还原主要依赖于其子交易的输入与输出金额的对应相等关系，那么限制用户的混币金额相等可有效增加破解难度，即在金额相同的情况下，会有一个输出可能对应多个输入的组合关系，极大增加有效划分的个数。

在图 5 所示的混币交易 a 中，Alice、Bob 和 Charlie 这 3 个用户参与混币。该交易为未限制混币金额的情况，即 3 人的混币金额都为其输入金额，该情况下有效的分解方案个数为 6。图 6 所示的混币交易 b 将混币金额限制为 1 BTC（比特币），不同于混币交易 a，多个相同金额的交易输出每一个都可以映射到任意交易输入，从而得到更多满足式(3)中定义的有效分解方案，这种情况下有效分解方案个数为 17。可见，限制参与混币的金额是提高混币安全性的重要手段，Samourai 钱包采用了这一方案，其以时效性为目的，设置了不同金额的混币池，每个混币交易只有 5 个参与者，但严格限制混币金额相同，故其能在交易匿名集较小的情况下实现优秀的隐私保护。

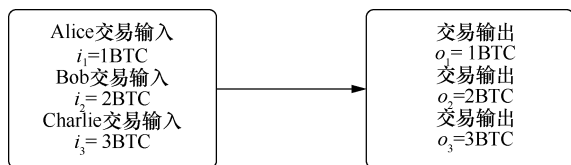


图5 混币交易 a (unlimited混币金额)

Figure 5 Mixed coin transaction a

(unlimited amount of mixed currency)

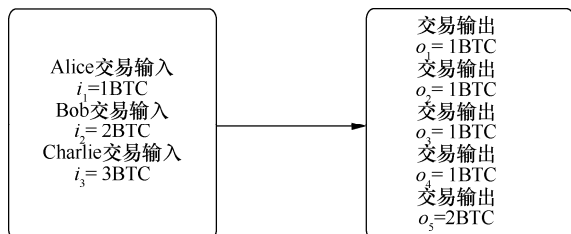


图6 混币交易 b (限制混币金额为 1BTC)

Figure 6 Mixed coin transaction 'b' (limited to 1BTC)

2.2 无验证的 Wasabi 混币交易检测

根据 2.1 节的模型安全性分析, 可以初步得到检测规则集合 $C_1 = (c_{11}, c_{12}, c_{13}, c_{14})$ 。

c_{11} : CoinJoin 交易的本质是多个普通交易的聚合, 它的具体表现形式一定是一个多输入多输出 (MIMO, multiple input multiple output) 交易。

c_{12} : 作为多个普通交易的聚合, CoinJoin 交易至少存在一个对应多个交易聚合的分解方案。

c_{13} : CoinJoin 交易在作为一个 MIMO 交易的同时, 其输入的规模会有下限来保证达到混币服务商设定的匿名集大小, 该下限由各混币服务商设定, 会有所不同。

c_{14} : CoinJoin 交易的输出中会存在多个相同的金额来提高隐私保护力度。

检测规则集合 C_1 描述的是对 CoinJoin 类型混币检测的基本规则, 其中, 出于对 CoinJoin 安全改进的考虑, c_{13} 和 c_{14} 涉及混币服务自定义的实现细节。

将对客户端的使用、公开技术文档和此前相关研究的学习与 C_1 中的检测规则相结合, 可以得到 Wasabi 的初步混币检测规则集合 $W_1 = (w_{11}, w_{12}, w_{13})$ 。

w_{11} : 如果交易是由 Wasabi 产生的混币交易, 那么它是 MIMO 交易, 且输入输出的个数都在 10 以上。

w_{12} : 如果交易是由 Wasabi 产生的混币交易, 那么它的输出中会存在重复金额, 且重复金额的最高频次大于 10 且小于输入的个数。

w_{13} : 如果交易是由 Wasabi 产生的混币交易, 那么它不存在输入地址复用为输出地址。

检测规则 w_{11} 对应 CoinJoin 交易 MIMO 的本质与现今匿名集规模的限制, 由于考虑的是无验证样本的情况, 该阈值为 10 (参考其他相关研究得来); 检测规则 w_{12} 对应混币服务商对混币金额的限定, 即令 CoinJoin 混币交易输出中存在大量相同的金额; 规则 w_{13} 中所述的将输入地址复用为输出地址操作, 在比特币官方文档中被定义为不推荐使用, 因为该操作会降低交易的隐私性, 而混币作为用户追求隐私保护的一种操作, 有理由相信这种操作在混币服务中应被禁止, Wasabi 设计所依赖的 ZeroLink 框架中也禁止这一操作。

2.3 检测结果

本文获取了 2021 年 12 月 16 日至 2022 年 2 月 12 日期间所生成的比特币区块, 并根据 2.2 节中的检测规则集合 W_1 做了检测工作, 在此期间共检测到 1 786 个“疑似”由 Wasabi 发布的混币交易。

3 可验证的 Wasabi 混币交易检测

3.1 验证集数据来源

Wasabi 的官网文档中公开了 5 个混币交易来给用户展示其混币的效果。除此之外, 仅有文献 [23] 提到的 Wasabi 客户端混币过程中与服务器进行交互时提供的 API, 通过该接口可查询当前时段的 Wasabi 已广播至网络但仍未被矿工收入区块的混币交易, 该类交易被 Wasabi 命名为 unconfirmed-coinjoins。

该接口的工作机制是每当 Wasabi 内部中一个混币流程完成后, 便发布到比特币网络中并同时更新在该接口中, 当该混币交易经过矿工打包上链后即在接口中返回的结果中清除该交易。所以, Wasabi 发出的混币交易在接口列表中消失的时机是比特币的下一个区块生成时, 已知比特币的区块平均生成时间为 10 min, 为了避免数据遗漏, 本文在两台服务器上部署爬虫程序以 2 min 为周期持续爬取该接口得到由 Wasabi 发布的混币交易集合, 并将两个集合取并集, 以此作为本文检测的验证集。

Wasabi 交易爬虫程序如算法 1 所示。

算法 1 Wasabi 交易爬虫程序

输入 待爬取接口地址 address, 程序终止时

间 T

输出 爬取时段获得的交易列表 Transactions

1) $t \leftarrow$ 当前时间;

2) **while** $t < T$

3) Transactions $\leftarrow$ httpget(address); //向接口发送请求, 获取到当前 unconfirmed-coinjoins 列表;

4) **for** transaction in Transactions

5) **if** the transaction is valid & transaction is not in Transactions //该交易已上链即认为有效;

6) 将 transaction 加入 Transactions 中;

7) **end if**

8) **end for**

9) 程序休眠 2 min;

10) **end while**

11) **return** Transactions

3.2 验证集数据分析

在 2.3 节进行检测工作的同时段, 通过算法 1 中的 Wasabi 交易爬虫程序进行 API 内容爬取, 得到 Wasabi 在该时间段内共发布了 1 263 个混币交易。类比机器学习中的概念, 将这 1 263 个 Wasabi 混币交易按照发布时间平均分为 10 部分, 随机取其中 7 部分作为训练集, 用来分析 Wasabi 混币交易的数值特征, 并以此对无验证的 Wasabi 混币交易检测方法做反馈修改; 将剩余的 3 部分混币交易作为测试集, 用来验证修改后的检测方法。为了避免单次实验结果存在的偶然性, 重复该实验 5 次, 下文取其中一次进行实验分析方法的展示。为了保存实验数据以及保证本文实验结果的可验证性, 通过爬虫程序得到的 Wasabi 混币交易列表公开于 Gitee。

将爬取得到的 Wasabi 混币交易的前 7 部分作为训练集, 后 3 部分作为测试集, 通过对训练集中的交易进行数据分析, 得出 Wasabi 混币交易中 4 个有趣的现象。

现象 1: 交易的输入个数下限为 21。交易中输入个数分布直方图如图 7 所示, 可以发现交易中的输入与输出个数几近于正态分布, 最常见的输入个数区间为 (50, 80], 除了 3 个特例^{注1}, 其他

输入个数下限为 21, 可见 Wasabi 对匿名集的大小有严格限制。而 3 个比较特殊的交易样本的输入规模分别为 4、7、10, 其发布时间均为 2021 年 12 月 18 日并被记录在同一区块 714 627 内, 时间和结构上的巧合使人有理由猜测这 3 个交易可能是 Wasabi 内部实验所发布的, 因此不影响对交易规模下限的推断。为避免干扰, 后面的分析将不包括这 3 个特例。

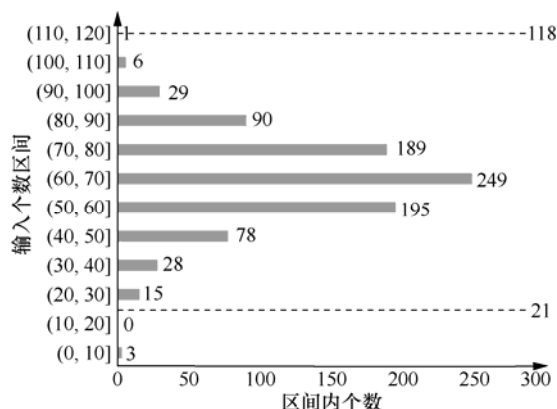


图7 交易中输入个数分布直方图
Figure 7 Distribution histogram of the number of inputs in the transaction

现象 2: 交易中输出个数与输入个数比值散点图如图 8 所示, 绝大多数落在区间 [1.1, 1.9], 其符合本文之前对这种比值的解释说明。仅有第 320 个交易输出个数与输入个数的比值达到了 2.12, 该交易规模的解释是有多个参与用户以倍数于设定混币金额的面值参与混币, 并同时接收多个设定混币金额的输出, 导致比值过大的情况。

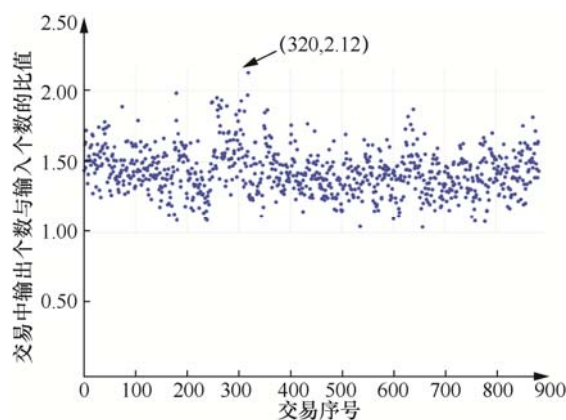


图8 交易中输出个数与输入个数比值散点图
Figure 8 Scatter chart of the ratio of the number of outputs to the number of inputs in the transaction

注1: 3 个特殊交易的 hash 值: 7894537b4bd8619b8f6a66d37c4f8e9e05396bed7ca1acb26d85a7739797e4fc5dabc88c00da843ecaa18f992e087d76d6896046a96c007ace5bfdad9f17a5dd575f2effe85657f972034f2518435a6f878259631e33757ae7ab b17311cf4f3f。

现象 3：设定的混币金额（即输出中重复出现金额）的最高频次的下限为 10，交易输出中重复金额的最高频次分布直方图如图 9 所示。

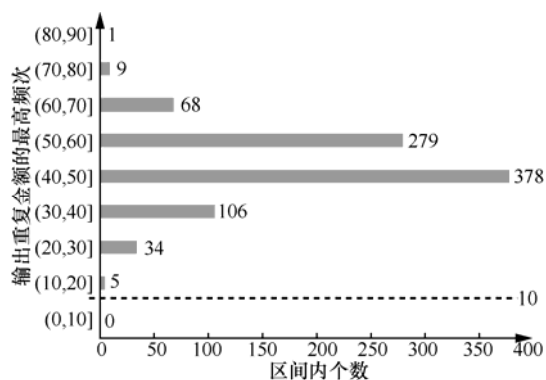


图 9 交易输出中重复金额的最高频次分布直方图
Figure 9 Highest frequency distribution histogram of repeated amount in transaction output

现象 4：输出中重复金额最高频次与输入个数的比值散点图如图 10 所示。输出中重复金额的最高频次与输入个数的比值位于区间 $[0.57, 0.97]$ 。在混币交易中，该比值是值得关注的指标，它代表混币服务中用户参与混币金额的自由度，该指标低，意味着用户可以灵活选择参与混币的金额，相反则表示用户必须接受服务商设定的混币金额。该值最高可达到 1，表示一个混币交易中所有用户的混币金额必须相同，Samourai 混币服务采取的是这种模式。

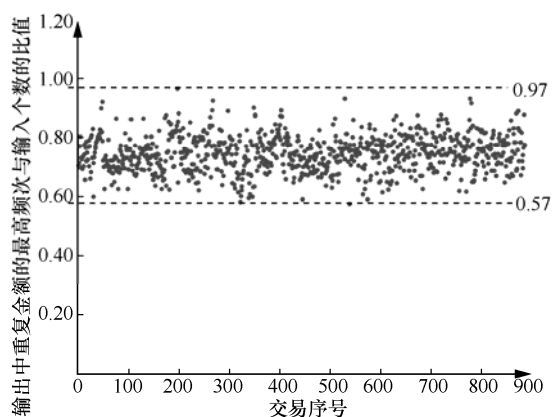


图 10 输出中重复金额最高频次与输入个数的比值散点图
Figure 10 Scatter chart of the maximum frequency of repetitive amounts in output and the number of inputs ratio

以上对训练集混币交易结构的分析可以验证本文对 CoinJoin 交易发展方向的解释，并为 Wasabi 检测规则的设计提供帮助。

3.3 经验证的检测方法改进

在分析检测结果之前，定义本文混币检测工作效果评判的两个重要指标：准确率和召回率。在本文的混币检测工作中，存在两个交易集合：通过爬虫程序得到的“真实”混币样本集合和在爬虫爬取的对应时间段内使用混币检测规则检测到的“疑似”混币样本集合。正是“真实”样本集合的存在才使得分析混币检测实验的效果成为可能。这两个集合的交集为检测正确的混币交易，将检测正确的混币交易数目与检测得到的总交易数目的比值定义为准确率，反映检测方法检测混币交易的精准度；将检测正确的混币交易数目与爬取得到的总交易数目的比值定义为召回率，反映检测方法对于混币交易检测的完备性。

定义 S_1 为爬取得到的“训练集”， S_2 为 2.3 节中检测得到的交易集合中对应 S_1 时间段的交易集合， W_1 规则集合检测结果如图 11 所示。

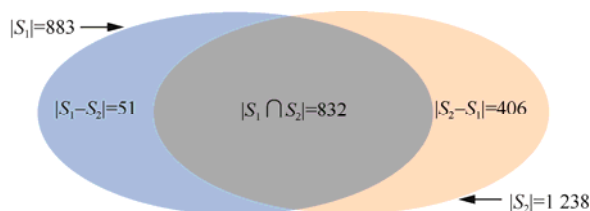


图 11 W_1 规则集合检测结果
Figure 11 Detection result of W_1 rule set

其中， $S_1 \cap S_2$ 为正确检测的部分， $S_1 - S_2$ 为应被检测却未被检测到（即漏检）的部分， $S_2 - S_1$ 为不应被检测却被检测到（即误检）的部分，可以得到无验证情况下设计的检测规则对于 Wasabi 混币交易的检测准确率 $\text{Precision}_1 = |S_1 \cap S_2| / |S_2| = 67.2\%$ ，召回率 $\text{Recall}_1 = |S_1 \cap S_2| / |S_1| = 94.2\%$ 。

对误检集合 $S_2 - S_1$ 中的 406 个交易进行进一步分析，发现以下误检原因。

(1) 无验证的检测规则中未明确限定交易中输出个数大于输入个数

该类交易在误检集 $S_2 - S_1$ 中存在 247 个，在训练集 S_1 中不存在，占据错误识别中的 60.8%。可以得到结论：在 Wasabi 混币交易中输入个数一定小于输出个数。如果从理论上对该结论进行验证，其本质上对应的是混币服务商对混币参与者参与金额的限制。

在 CoinJoin 混币交易中,出于隐私保护的目,有一些操作是要极力避免的,如在混币交易中使用高于设定金额的资金作为输入(如图6的混币交易b中设定混币金额为1 BTC的情况下,Charlie以3 BTC作为输入)或使用多个低于设定金额的BTC组合作为输入(如图12的混币交易c设定混币金额为3 BTC的情况下,以1 BTC+2 BTC作为输入)。

不按照预设的混币金额进行混币的操作泄露隐私体现在两方面。一是根据数值特征以高置信度确定某些输入输出间的对应关系,即变相地在混币交易中部分使用地址聚类技术。在图12的混币交易中,混币金额设定为3 BTC,但是仍能够以极高的概率确定在该交易中1 BTC和2 BTC的输入地址为同一人所持有。由此可以对这些用户应用地址聚类的第一条和第三条聚类规则。二是在某些用户的非常规操作导致自身隐私泄露后,实质上减小了匿名集,使其他正常参与混币的用户隐私受到侵害。

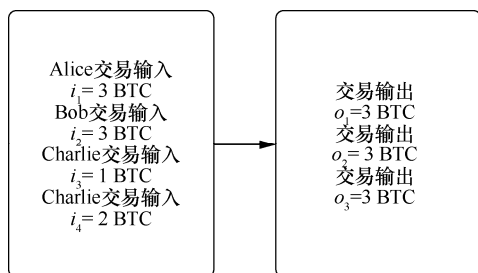


图12 混币交易c(违背混币规则)

Figure 12 Mixed coin transaction 'c' (violating the mixed coin rule)

事实上,在混币交易中使用高于设定金额的未花费交易输出(UTXO, unspent transaction output)作为输入这一操作虽然不推荐,但为了追求混币服务的灵活性(即提供任意金额的混币),这不可避免使用多个低于设定金额的UTXO组合作为输入,则因易于隐私泄露而被禁止。

(2) 无验证的检测规则中限定的输入规模10过小,以及未对输入规模的上限做规定

在3.2节中的分析已提到,除了3个特例,训练集 S_1 中的输入个数下限为21,而在误检集中除去误检原因(1)的交易后输入规模小于21的交易有136个,占比33.5%;同时在训练集 S_1 中,并不存在输入个数在118以上的交易,而在误检

集中存在5个,占比1.2%。

Wasabi对混币交易的规模进行了限制,即其要求匿名集至少达到一定的规模(即21)才可以进行一个混币交易(事实上文献[21]中表示Wasabi的匿名集设定为100,最长等待时间为1 h,显然21是其未公开的匿名集下限)。从安全性分析,混币交易的输入和输出规模越大,可能存在的划分集合 M 就会包含越多元素,每个参与混币的用户得到的隐私保护程度就会越高。

(3) 无验证的检测规则中未对交易输出中重复金额的最高频次与输入个数的比值做限制

在3.2节对训练集进行数据分析发现的现象4中,已分析过该比值的意义,并指出该值在Wasabi交易中的分布区间为[0.57,0.97],而无验证的检测方法中并未考虑这一点。经检验,误检集中该比值不属于区间[0.57,0.97]的数量为10,占比2.5%。

(4) 验证集 S_1 未必是完备的

经过以上3个误检原因的筛除后,剩余的8个误检样本经过分析后并没有发现明显的误检原因,因此可以猜测可能是 S_1 本身并不完备。在3.1节中论证了该接口发布的交易数据的准确性与完备性,但是因为网络波动等,由爬虫爬取接口得到的交易集合 S_1 并不完全等价于接口发布的交易集合。因此这8个交易,可能的确由该接口发布但并未被爬虫程序捕捉到,从而造成了误检。

对漏检集合 $S_1 - S_2$ 中的交易分析可以得到以下漏检原因:Wasabi中允许输入地址复用为输出地址,而无验证的检测规则中否定了这一行为。

这个现象正如本文所述那样是不被推荐使用的,但是服务平台并未强制限制,而某些混币用户可能会误做出这种操作,这体现了本文使用真实交易作为训练数据集的重要作用。

经过以上误检和漏检的规则分析,可以得到可验证的Wasabi混币交易检测规则集合 $W_2 = (w_{21}, w_{22}, w_{23}, w_{24})$ 。

w_{21} : 如果交易是由Wasabi产生的混币交易,那么它是MIMO交易,且输入个数位于区间[21, 118]。

w_{22} : 如果交易是由Wasabi产生的混币交易,

那么它的输入个数一定严格小于输出个数。

w_{23} : 如果交易是由 Wasabi 产生的混币交易, 那么它的输出中会存在重复金额, 且重复金额的最高频次大于 10 且小于输入的个数。

w_{24} : 如果交易是由 Wasabi 产生的混币交易, 那么它输出中重复金额的最高频次与输入个数的

比值位于区间[0.57,0.97]。

3.4 经改进的检测方法结果

得到“训练集”混币交易的样本分析反馈后, 分别用修改过后的 Wasabi 混币交易检测方法在“测试集”样本对应的区块上进行 Wasabi 混币交易检测, 5 次实验结果如表 1 所示。

表 1 Wasabi 混币交易检测结果
Table 1 Detection results of Wasabi mixed coin transaction

训练集 组成部分	测试集 组成部分	测试集 交易个数	检测集 交易个数	正确检测 个数	漏检个数	误检个数	检测 准确率	检测 召回率
1、2、3、4、5、6、7	8、9、10	380	382	380	0	2	99.5%	100%
1、3、4、6、7、8、9	2、5、10	378	381	378	0	3	99.2%	100%
1、2、3、5、7、8、10	4、6、9	378	380	378	0	2	99.5%	100%
1、2、5、6、7、9、10	3、4、8	380	381	380	0	1	99.7%	100%
2、3、4、6、8、9、10	1、5、7	379	383	379	0	4	99.0%	100%

从监管视角看, 对所有混币交易进行监管, 混币交易检测的召回率是一个重要指标, 由于本文使用的检测方法在数值范围上足够精准, 因此在检测的准确率和召回率上都表现优秀。然而从统计学意义上讲, 在检测方法不够精准时, 检测工作的准确率和召回率是一对负相关的指标, 可以通过降低其中一个而使另一个指标达到更好的效果, 因此可以放宽检测规则中某些参数的限制来获得最终的关于 Wasabi 混币检测的规则集合 $W_3 = (w_{31}, w_{32}, w_{33}, w_{34})$ 。

w_{31} : 如果交易是由 Wasabi 产生的混币交易, 那么它个 MIMO 交易, 且输入个数位于[20, 120]内。

w_{32} : 如果交易是由 Wasabi 产生的混币交易, 那么它的输入个数一定严格小于输出个数。

w_{33} : 如果交易是由 Wasabi 产生的混币交易, 那么它的输出中会存在重复金额, 重复金额的最高频次大于 10 且小于输入的个数。

w_{34} : 如果交易是由 Wasabi 产生的混币交易, 那么它输出中重复金额的最高频次与输入个数的比值位于[0.50,0.99]。

本文的实验结果验证了对于可以分析具体交易样本的混币交易平台, 能够得到召回率达到 100%的检测方法。同时, 为了在其他未训练的样本检测上获取高召回率, 本文放宽了检测规则中的一些指标限制来得到最终的 Wasabi 混币检测

方案 W_3 , 但在检测的准确率上仍保持相当高的水平。

4 CoinJoin 混币交易总体规模估计

在当今的币圈, 拥有众多参与者的混币交易每天都在进行。从监管的角度, 评估混币交易的流行程度以及获得相关的交易量数据很有必要, 下面依据本文的检测方法对混币交易的市场规模进行预估。

根据检测规则分析, 可以看到 Wasabi 的具体检测规则是在 CoinJoin 通用检测规则集合 C_1 的 c_{13} 和 c_{14} 两条规则上进行了特殊的数值规定, 据此可以放宽这种数值的限制来对所有 CoinJoin 类型的混币交易做检测, 这可能会导致检测到一些与混币交易类似的普通交易, 即得到的检测结果是一个上限。本文在区块高度为 714 364~722 936 的区块上(对应爬取时段发布的区块)进行了检测, 期望以此检测结果来预估当前 CoinJoin 混币在比特币交易中的总体规模, 以提高人们对混币市场规模的认知。

采取的预测方法有以下两方面: 一是从交易数量出发, 以天为时间单位得到混币交易数量占总交易数量的份额; 二是从交易金额出发, 以天为时间单位得到混币交易金额占总交易金额的份额。

在整个检测期间共得到混币交易 24 265 个,

图 13 为 2021/12/16—2022/2/12 期间每天的 CoinJoin 混币交易数以及混币交易金额, 在此期间平均每天产生 423 个混币交易, 平均每天的交易金额为 1 474.94 BTC。数据显示, 混币交易的数目受到节日的影响, 如交易数量和交易金额都在圣诞节前后达到峰值。根据该时段平均每天的

交易个数与交易金额^[28], 可以得知从交易数量来看, CoinJoin 混币交易占有所有比特币交易的 1.9‰; 从交易金额来看, 占有所有交易的 3.7‰, 该结论符合 CoinJoin 混币的特征: CoinJoin 混币交易为多个普通交易的聚合交易, 因此其交易金额高于平均交易金额。

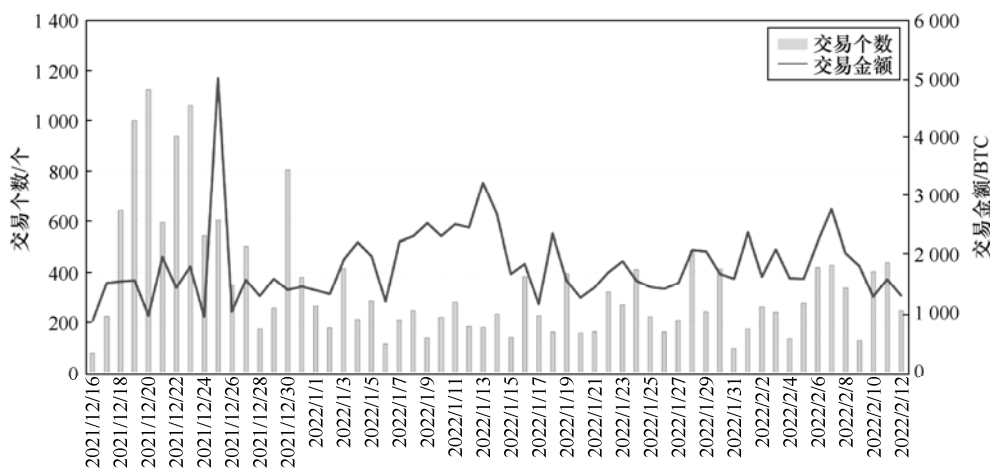


图 13 2021/12/16—2022/2/12 每天的 CoinJoin 混币交易数以及混币交易金额
Figure 13 Daily CoinJoin mixed coin transaction quantity and mixed coin transaction amount of 2021/12/16—2022/2/12

在区块链分析公司 Chainalysis 的一份报告中显示^[29], “加密货币”混合器收到的总每日价值的 30 天移动平均值在 2022 年 4 月达到 5 180 万美元的历史新高, 这一数量是 2021 年同一时间接收数量的两倍。根据市值换算, 与本文得到的结果属于同一数量级, 从侧面论证了检测方法的可靠性。除此之外, 在对 CoinJoin 类型混币交易的检测中, 对 Wasabi 混币交易的召回率达到 100%, 这也符合预期, 即 Wasabi 混币交易的本质是 CoinJoin 混币交易。

5 结束语

相较目前已有的相关检测算法, 本文提出的检测算法在准确率和召回率上优势明显, 检测实验结果具有高可信度。本文所使用的基于规则的检测方式仍有待改进之处, 如对于特定服务提供的混币交易的数值依赖性强, 易被针对而需要调整。但如文中所述, 基于 CoinJoin 的不同混币服务在数值设计上的微调并没有改变其基本模型, 本文提出的检测规则可以根据相关样本数据进行调整。由于区块链的不易篡改性, 在某时期内产生的交易不会改变并永久在链上存留。从监管角

度出发进行交易资金回溯或者特定交易分析, 本文方法仍有较大价值。此外, 混币相关的研究并不局限在比特币上, 在以太坊上基于智能合约的混币器已经成为主流, 这是未来的研究方向之一。

参考文献:

- [1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Bitcoin, 2008, 4(2): 15.
- [2] BENJAMIN M B. Price dynamics and speculative trading in bitcoin[J]. Research in International Business and Finance, 2017, 43: 15-21.
- [3] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system [M]. New York: Springer New York, 2013.
- [4] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in bitcoin[C]//17th International Conference on Financial Cryptography and Data Security. 2013: 34-51.
- [5] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]//Proceedings of the 2013 Conference on Internet Measurement Conference. 2013: 127-140.
- [6] NOETHER S. Ring signature confidential transactions for Monero[J]. Cryptology ePrint Archive, 2015/1098.
- [7] SASSON E B, CHIESA A, GARMAN C, et al. ZeroCash: Decentralized anonymous payments from bitcoin[C]//Proceedings of the 2014 IEEE Symposium on Security and Privacy. 2014: 459-474.

- [8] SABT M, ACHEMLAL M, BOUABDALLAH A. Trusted execution environment: What it is, and what it is not[C]//Proceedings of 2015 IEEE Trustcom/BigDataSE/Isp. 2015: 57-64.
- [9] FAFT. The FATF Recommendations[EB].
- [10] SATER S. Do we need KYC/AML: The bank secrecy act and virtual currency exchanges[J]. Ark L Rev, 2020, 73: 397.
- [11] TRAMER F, BONEH D, PATERSON K. Remote side-channel attacks on anonymous transactions[C]//Proceedings of the 29th USENIX Security Symposium. 2020: 2739-2756.
- [12] MOSER M, SOSKA K, HEILMAN E, et al. An empirical analysis of traceability in the monero blockchain[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(3): 143-163.
- [13] 王晨旭, 程加成, 桑新欣, 等. 区块链数据隐私保护: 研究现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119.
- WANG C X, CHENG J C, SANG X X, et al. Data privacy-preserving for blockchain: state of the art and trends[J]. Journal of Computer Research and Development, 2021, 58(10): 2099-2119.
- [14] 孙小文. 面向交易维度的比特币地址关系分析算法的研究与实现[D]. 北京: 北京邮电大学, 2021.
- SUN X W. Research and implementation of bitcoin address relationship analysis algorithm oriented to transaction dimension[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
- [15] GENKIN D, PAPADOPOULOS D, PAPAMANTHOU C. Privacy in decentralized cryptocurrencies[J]. Communications of the ACM, 2018, 61(6): 78-88.
- [16] MAXWELL G. CoinJoin: bitcoin privacy for the real world[C]//Post on Bitcoin forum. 2013: 110.
- [17] TIRONSAKKUL T, MAAREK M, EROSS A, et al. The unique dressing of transactions: Wasabi coinjoin transaction detection[C]//Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference. 2022: 21-28.
- [18] STUTZ R, STOCKINGER J, MORENO-SANCHEZ P, et al. Adoption and actual privacy of decentralized CoinJoin implementations in bitcoin[C]//Proceedings of the 4th ACM Conference on Advances in Financial Technologies. 2022: 254-267.
- [19] MOSER M, BOHME R. The price of anonymity: empirical evidence from a market for Bitcoin anonymization[J]. Journal of Cybersecurity, 2017, 3(2): 127-135.
- [20] NADLER M, SCHAR F. Tornado cash and blockchain privacy: A primer for economists and policymakers[J]. Available at SSRN 4352337, 2023.
- [21] GHESMATI S, FDHILA W, WEIPPL E R. Usability of cryptocurrency wallets providing coinJoin transactions[J]. IACR Cryptol ePrint Arch. 2022: 285.
- [22] STOCKINGER J, HASLHOFER B, MORENO_SANCHEZ P, et al. Pinpointing and measuring Wasabi and Samurai coinjoins in the bitcoin ecosystem[J]. arXiv preprint arXiv: 2109. 10229, 2021.
- [23] WU L, HU Y F, ZHOU Y J, et al. Towards understanding and demystifying Bitcoin mixing services[C]//Proceedings of the Web Conference 2021. 2021: 33-44.
- [24] MAKSTOV A A, ALEXEEV M S, FEDOROVA N O, et al. Detection of blockchain transactions used in blockchain mixer of coin join type[C]//Proceedings of 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019: 274-277.
- [25] MEIKLEJOHN S, ORLANDI C. Privacy-enhancing overlays in bitcoin[C]//Proceedings of International Conference on Financial Cryptography and Data Security. 2015: 127-141.
- [26] FICSOR A. ZeroLink: The bitcoin fungibility framework[EB].
- [27] ATLAS K. Weak privacy guarantees for sharedcoin mixing service[J]. CoinJoin Sudoku, 2014.
- [28] BLOCKCHAIN. Blockchain Charts[EB].
- [29] CHAINALYSIS. The Chainalysis 2022 Crypto Crime Report[EB].

[作者简介]



李虎 (1998—), 男, 河南南阳人, 南京邮电大学硕士生, 主要研究方向为区块链安全。



陈云芳 (1976—), 男, 江苏镇江人, 博士, 南京邮电大学副教授, 主要研究方向为人工智能算法、特定应用领域的功能分析、使用智能系统的应用开发。



张伟 (1973—), 男, 江苏泰兴人, 博士, 南京邮电大学教授、博士生导师, 主要研究方向为无人机平台下智能感知与认知、隐私保护与人工智能安全。