

区块链混币监管技术研究综述

王佳鑫¹, 毛谦昂¹, 颜嘉麒¹, 印杰², 何源³, 张祎⁴(1. 南京大学信息管理学院, 江苏 南京 210023; 2. 江苏警官学院计算机信息与网络安全系, 江苏 南京 210031;
3. 常州市公安局, 江苏 常州 213000; 4. 江苏省公安厅, 江苏 南京 210000)

摘要: 区块链技术的迅速发展与加密货币的兴起不仅挑战了传统的金融和资产管理观念, 也带来了一系列隐私与安全方面的问题。加密货币混币技术作为区块链隐私保护的主要手段, 旨在提升交易的匿名性并保障用户身份的隐私。然而, 这种增强的匿名性也使得加密货币成为洗钱、盗窃、欺诈等犯罪活动的工具。因此, 亟须全面审视加密货币混币服务的识别、检测与监管技术的研究, 以支持执法机构并促进加密货币的安全合规。首先系统梳理了混币服务的技术原理与机制分类, 设计了一套通用的混币工具分类体系, 详细探讨了混币服务可能引发的犯罪活动; 接着重点讨论了基于人工规则、地址聚类、实体分类、异常交易检测和混币服务追溯 5 种混币监管技术的最新学术研究进展, 并总结了现有工业界中与混币监管相关的工具和平台; 最后提出了混币监管目前所面临的挑战, 为未来的研究方向提供展望。

关键词: 区块链; 加密货币; 混币; 隐私保护; 监管技术

中图分类号: TP311

文献标志码: A

DOI: 10.19678/j.issn.1000-3428.0070189

Review of Blockchain-based Coin Mixing Regulatory Technology

WANG Jiaxin¹, MAO Qian'ang¹, YAN Jiaqi¹, YIN Jie², HE Yuan³, ZHANG Yi⁴

(1. School of Information Management, Nanjing University, Nanjing 210023, Jiangsu, China;

2. Department of Computer Information and Network Security, Jiangsu Police Institute, Nanjing 210031, Jiangsu, China;

3. Changzhou Public Security Bureau, Changzhou 213000, Jiangsu, China;

4. Jiangsu Provincial Public Security Department, Nanjing 210000, Jiangsu, China)

【Abstract】 The rapid development of blockchain technology and the rise of cryptocurrencies not only challenge traditional financial and asset management concepts but also introduce significant privacy and security concerns. Coin mixing, a primary privacy protection mechanism in blockchains, is designed to enhance transaction anonymity and protect user identities. However, this enhanced anonymity also enables the misuse of cryptocurrencies for illicit activities such as money laundering, theft, and fraud. Therefore, a comprehensive review of technologies for the identification, detection, and regulation of coin mixing services is urgently required to support law enforcement and promote the secure and compliant use of cryptocurrencies. This paper first reviews the technical principles and mechanisms of coin mixing services and proposes a general classification framework for mixing tools while discussing the criminal activities associated with them. Subsequently, it focuses on recent advances in five key regulatory approaches: manual rule-based methods, address clustering, entity classification, anomalous transaction detection, and mixing service traceability. It also surveys existing industrial tools and platforms related to coin mixing regulations. Finally, it identifies current challenges in the field and suggests directions for future research.

【Key words】 blockchain; cryptocurrency; coin mixing; privacy protection; regulatory technology

0 引言

区块链技术的快速发展以及比特币和以太坊等加密货币的兴起已经在全球引起了广泛关注^[1]。这些技术和应用引入了一种去中心化的金融交易模式, 不仅挑战了传统的货币和资产管理观念, 还引发了关于隐私与安全的新问题^[2]。在区块链隐私保护

技术中, 加密货币混币技术扮演了关键角色, 它旨在通过混淆加密货币交易中的输入地址之间的关联, 以隐匿资金的实际来源和去向, 从而增强加密货币的匿名性, 保护用户的隐私, 使用户能在不暴露个人信息的情况下进行交易^[3]。

然而, 这种匿名性的增强也使得加密货币成为犯罪活动的一个热门工具。犯罪分子通过使用混币

基金项目: 国家自然科学基金(72571131, 72171115)。

作者简介: 王佳鑫(CCF 学生会员), 男, 博士研究生, 主研方向为区块链监管; 毛谦昂(CCF 学生会员), 博士研究生; 颜嘉麒(CCF 会员、通信作者), 教授、博士; 印杰(CCF 会员), 高级工程师; 何源、张祎, 硕士。

收稿日期: 2024-08-04

修回日期: 2024-12-09

E-mail: jiaqiyan@nju.edu.cn

技术进行大规模的洗钱^[4],使得追踪非法资金的来源和流向变得极其困难,从而在全球范围内助推了非法活动的扩散。这些非法活动包括网络勒索、毒品交易、非法武器销售以及恐怖资金的筹集等^[5]。文献[6]评估了 69 个混币服务的公众讨论,结果显示大多数混币服务被揭示为彻底的骗局。实际上,混币技术已成为推动大部分加密货币犯罪活动的关键底层机制^[7]。尽管如此,到目前为止执法机关对这些匿名且复杂的加密货币洗钱服务的干预仍相对困难。因此,针对加密货币混币服务的识别、检测和监管技术研究亟须进行全面梳理。

目前,国内外的研究学者已从区块链隐私保护^[8-13]和安全监管技术^[14-18]两个角度进行了文献综述研究。尽管文献[8-13]提及了混币技术是一种区块链隐私保护手段,但主要集中于阐述增强区块链系统的隐私性技术的原理和工作过程,并没有涉及混币服务的监管技术、策略和应用。文献[14-18]侧重于加密货币交易分析与监管框架的总结,对于细分下的混币服务的技术原理和分类、监管措施和工具的探讨研究均不足。

本文集中探讨了当前加密货币混币检测与识别监管技术的发展现状和最新进展。通过在 Web of Science、Google Scholar、ACM Digital Library、IEEE Xplore、Springer 和 Science Direct 等数据库使用关键词如“加密数字货币(Cryptocurrency)”、“混币(Coin mixing; Coin Tumbling; Coin Shuffling)”、“去混币、去匿名、识别、检测和监管(De-mixing; De-anonymization; Identification; Detection; Regulatory)”、“区块链(Blockchain)”、“比特币(Bitcoin)”和“以太坊(Ethereum)”进行文献搜索,本文筛选了 2015 年至 2024 年的相关研究。搜索结果涵盖密码学、网络与信息安全学、计算机科学和软件工程等多个领域。本文的主要贡献如下:

1)构建了完整的混币技术研究框架,包括技术原理、机制分类、平台评价体系。

2)将混币犯罪活动、学术界现有监管技术和工业界现有监管工具进行系统性关联、分类和总结。

3)系统分析了当前混币监管面临的挑战,对未来研究方向进行了展望,为监管机构和研究人员提供了实践参考。

本文在概述加密数字货币混币技术原理、机制分类、混币平台评价体系、混币可能引发的犯罪活动的基础上,系统介绍每一项工作的背景信息,梳理主要学术研究成果,提供混币监管技术的详细分类,并总结工业界中现有的混币监管工具和平台生态。最

后,本文探讨面临的挑战,为未来研究方向提供展望。

1 区块链混币生态概述

1.1 混币技术原理

混币是一个旨在提高加密货币交易隐私性的过程。在比特币和其他加密货币的公共账本中,交易记录是公开的,这意味着理论上任何人都可以看到交易的发送者、接收者和交易金额。混币服务通过混合多个用户的加密货币,使得追踪原始资金的流向变得复杂。混币技术的工作原理和操作过程包括了以下 3 个阶段:

1)收集阶段:用户首先将需要匿名处理的加密货币发送到混币服务的地址。这些加密货币进入混币服务的“混币池”。用户通常会提供一个或多个新的地址,这些地址属于同一用户,但与发送到混币服务的原始地址没有直接联系。

2)混合阶段:混币服务将来自多个用户的加密货币收集在一起并进行混合。这一过程涉及将所有收到的资金随机重新分配和发送到新的地址,这些新地址由原始用户控制,但与他们原来的地址不再有直接的关联。

3)输出阶段:一旦混合完成,加密货币将从混币服务的池中发送到用户最初指定的新地址。由于在池中的加密货币进行了重新分配,这些新地址接收到的加密货币与原始的发送地址之间的直接链接已经被打乱,无法确定哪些新地址与哪些原始地址相对应。

1.2 混币机制分类

考虑到区块链混币服务的多样化和复杂性,本文可以从治理模式和混币技术两个维度对整体的区块链混币机制进行详细分类和阐述。在治理模式方面,区块链混币服务可以分为中心化混币服务和去中心化混币服务。在混币技术方面,本文将其分类为基于 CoinJoin 技术、环签名技术、零知识证明技术以及其他特殊混币技术。

1.2.1 按治理模式分类

1)中心化混币服务。

中心化混币服务由单一实体或公司控制,该实体负责接收、混合并重新分配加密货币,然后将混合后的资金发送回用户提供的新地址,以消除资金源的可追溯性^[19]。图 1(a)展示了中心化混币服务依赖于一个单一的中心化实体来处理混币的过程。中心化服务通常提供简单易用的界面,处理速度通常比去中心化服务快,也可以提供额外的服务,如地址

定制、多重安全检验等。但是,中心服务提供商会面临单点故障和网络攻击的重大挑战,可能存在用户资金被窃取和身份信息泄露等安全和信任风险。在实际服务中,很大一部分倾向于中心化混币服务,尤其是在比特币生态系统中。例如:BitMix. Biz^[20] 提供比特币和莱特币的混币服务,支持多语言,以增强用户的隐私;Blender. io^[21] 是一个流行的比特币混币服务,以其简单的界面和可靠的混币过程而闻名。

2) 去中心化混币服务。

去中心化混币服务不依赖于任何中心权威,通常使用智能合约或者去中心化网络协议来执行混币操作,提供更高程度的匿名性和安全性^[19]。图 1(b) 展示了去中心化混币服务是不依赖于单一的中心化实体的,而是通过多个参与者的合作来实现的。去中心化混币服务提供更高的隐私保护,使追踪单个用户的活动,难以被单一政府或机构封禁或控制,用户对自己的资金持有更大的控制权,无需信任任何中介。但是,去中心化混币可能需要更长的时间来累积足够的参与者,执行混币操作的速度可能较

慢,存在交易延迟或失败等网络风险。同时,智能合约可能存在编码错误或漏洞等技术风险,这些漏洞可能被利用来窃取资金或破坏系统。例如,JoinMarket^[22] 是一个去中心化的比特币混币服务,通过一个特殊的市场机制使用户能够参与混币,同时为其提供比特币作为混币的“市场制造者”赚取费用。

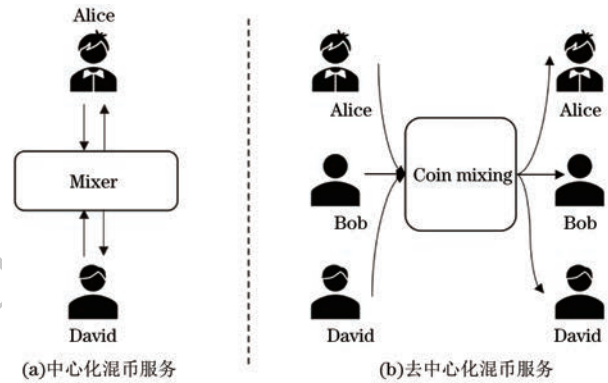


图 1 中心化混币服务和去中心化混币服务

Fig. 1 Centralized and decentralized coin mixing services

中心化混币服务与去中心化混币服务的具体对比如表 1 所示。

表 1 中心化混币服务与去中心化混币服务的对比

Table 1 Comparison between centralized and decentralized coin mixing services

特性	中心化混币服务	去中心化混币服务
匿名性	通常较低,服务提供商可能需要收集某些用户信息以符合监管要求	较高,不依赖单一实体,用户更难以被追踪
信任	用户需要信任服务提供商不会窃取资金并确保交易数据的安全	采用分布式技术,用户无需信任任何中心实体
控制权	服务提供商控制整个混币过程和资金	用户通过智能合约或直接的 P2P 交易保持对资金的控制
易用性	通常用户界面友好,易于操作	需要用户具备更多的技术知识和高级设置
费用	收取较高的服务费以盈利和维持运营	缺乏中心化运营和维护成本,通常费用较低
法律风险	较高,中心化服务可能因违反法律规定被关闭	较低,去中心化结构不易被政府或机构关闭
交易速度	由服务提供商优化流程,交易速度通常较快	取决于网络状况和参与节点,交易速度不稳定
监管合规性	更需要遵守反洗钱等监管要求	匿名性较高,合规性是一大挑战,不易受到传统金融法规的约束
安全风险	单点故障和网络攻击导致资金盗窃、数据泄露	合约漏洞、前端攻击和 51% 攻击等导致交易篡改、资金盗窃等
恢复机制	故障时可以通过服务提供商恢复资金	故障时恢复资金更复杂,依赖技术和社区支持

1.2.2 按混币技术分类

1) 基于 CoinJoin 技术。

CoinJoin 是一种基于比特币协议的混币技术,允许多个用户合并他们的交易为一个单一的交易,以增加匿名性。通过这种方式,每个用户的支付输入和输出都在同一交易中混合,从而使外部观察者难以追踪每个输入与输出之间的直接关系^[23]。具体来说,它的工作原理是多个参与者将他们想要进行的交易提交给中心服务器或去中心化应用,这些交易被组合在一起形成一个大的交易,其中包括所有参与者的输入和输出。为了完成交易,每个参与者需要对整个交易进行签名,只有当所有参与者都签名后,交易才会被广播到网络并执行。CoinJoin

的优点是通过混淆交易的来源和目的地,增加了隐私性和外部追踪的难度;用户之间协作形成交易,不需依赖中心化的混币服务,减少了信任需求。CoinJoin 的缺点是依赖参与者协作,需要信任协调者不记录额外的隐私信息,如果参与者之间存在信任问题或者一方行为不当,可能会影响交易的安全性和隐私性。Wasabi Wallet^[24] 和 Samurai Wallet^[25] 提供的 Whirlpool 服务是一种基于 CoinJoin 的开源、非托管式的比特币钱包,用户可以通过它参与去中心化混币交易,在保护用户隐私方面非常强大^[26]。

2) 环签名。

环签名是一种加密技术,它允许一个成员在一

组用户中生成对消息的有效签名,而无需透露是哪个成员提供的签名^[27]。这种签名提供了强大的匿名性保护,使得外部观察者无法确定具体是哪个用户参与了签名。具体来说,它的工作原理是签名者将自己的公钥与其他非签名者的公钥混合在一起形成一个“环”。签名过程确保签名可以验证整个环的有效性,但无法确定哪个具体的公钥与签名直接相关联。环签名的优点在于提供了高度的匿名性,适用于需要保护个人隐私的场景。用户可以独立地使用环签名进行交易,无需其他用户的协作,保证了签名者的身份在群体中是不可追踪的,但是生成和验证环签名可能比传统的数字签名要复杂、时间消耗更长、计算资源消耗更多。Monero^[28]是环签名技术最著名的应用之一,它使用一种环签名机密交易(RingCT)技术^[29],允许交易的金额和参与者身份同时被隐藏。它还通过引入隐写技术确保每次交易都使用一个新地址,进一步增强了隐私性^[30]。

3)零知识证明(ZKP)。

零知识证明是一种加密协议,允许一方(证明者)向另一方(验证者)证明某个陈述是正确的,而无需透露任何其他有关证明的信息^[31]。这种方法可以在不泄露任何有关底层数据的情况下验证数据的真实性。它具备高度的隐私保护性,可以证明数据的正确性而不透露任何数据内容,适用于对数据保密要求极高的应用场景,如身份验证、数据访问权限验证等,但生成和验证零知识证明可能非常耗费计算资源。Zcash 是一种使用零知识证明技术的加密货币^[32],其目的是解决比特币交易执行过程中利用区块追踪交易记录的问题,同时隐藏用户的个人信息以及交易数据,提供了完全匿名的交易选项。Tornado Cash 是一种基于以太坊的去中心化应用程序,使用零知识证明来确保交易的隐私^[33]。

基于 CoinJoin、环签名和零知识证明混币技术的对比如表 2 所示。

表 2 基于 CoinJoin、环签名和零知识证明混币技术的对比

Table 2 Comparison of CoinJoin-based, ring signature and ZKP coin mixing technologies

特性	基于 CoinJoin 技术	环签名	零知识证明
匿名性	高,因为外界无法确定哪个输入对应哪个输出	非常高,因为外界无法确定是哪个组成成员进行了签名	极高,因为可以隐藏几乎所有交易细节
灵活性	有限,主要用于比特币等加密货币的混币交易	一般,主要应用于 Monero 等隐私币,也适用于电子投票等其他需要匿名保护的场景	较好,广泛应用于多种场景,包括加密货币匿名交易、身份验证、权限控制等其他验证过程
技术复杂性	相对简单,技术实现和理解都不复杂	中等,需要对密码学有一定理解	高,涉及复杂的密码学原理
交易速度	依赖于参与混币的用户数量,可能较慢	一般,受限于环签名计算和验证的时间	取决于实现的算法和系统性能,一些零知识证明的生成和验证可能很耗时
可扩展性	有限,随着参与用户的增多,交易大小增加,可能影响效率	一般,计算成本随环的大小增加	较差,因为零知识证明的计算和存储需求较高
资源需求	较低,主要是合并多个交易的数据处理	中等,需要进行计算密集型的签名和验证	高,生成和验证零知识证明需要大量计算资源
监管风险	较低,技术并不完全匿名,仍可追踪到某种程度	较高,提供了强大的匿名性	较高,提供了强大的匿名性

4)其他技术。

(1)跨链混币技术。

跨链混币服务可以被视为加密货币混币技术的一种特殊形式。这种服务结合了跨链技术(允许不同区块链之间的交互和资产转移^[34])和混币技术的特点,目的是在提供链间资产转移的同时增强交易隐私。这种技术的核心在于能够在不同的区块链之间进行资产的匿名转移,可以有效地“断开”资金流的追踪链,从而扩展混币服务的范围和效能。ShapeShift^[35]和 changenow.io^[36]提供了这类功能,允许用户通过一个简单的接口,进行快速且不留痕迹的跨链转账。

(2)动态混币技术。

动态混币技术侧重于交易过程中参数的实时调整,以优化混币的效率和隐私。这种技术可能包括基于当前网络条件自动调整手续费、根据参与混币服务的用户数量动态调整混币批次的大小,或者实时变更混币池的组合方式。例如,闪电网络(Lightning Network)^[37]通过实时调整网络节点之间的支付通道容量来适应不断变化的支付需求,这种灵活性大大提高了网络的可扩展性和用户的隐私保护^[38]。

1.3 混币平台分析

根据目前使用较多的集中混币平台服务,本文

设计一套通用的混币分类体系,需要综合考虑混币服务的隐私、安全性、效率、成本、治理模式以及合规性等因素。以下是一个具体的分类体系,如表 3 所示,该体系旨在通过多个维度全面评估混币技术:

1) 隐私保护维度。

隐私保护维度关注于如何增强用户在使用混币服务时的匿名性和不可追踪性,这包括:

(1) 混币技术:使用的具体混币技术,如基于 CoinJoin、环签名、零知识证明、其他技术或结合多种混币技术(混币池)等。

(2) 混币过程:描述混币操作的具体实施方式,如何处理输入和输出的关系,包括多对一、一对多、一对一、一对多和环形混币等类别。

(3) 网络节点:混币操作所使用的网络类型,区分为明网节点和 Tor 节点^[39],前者通常速度更快,

后者则提供更高的隐私保护。

(4) 匿名性级别:衡量混币服务提供的匿名性程度,包括完全匿名、部分匿名和非匿名。

(5) 可追溯性:指是否可以追踪到交易的原始参与者,关键在于是否保护用户交易隐私不被外部追踪。

2) 安全性维度。

安全性维度关注于保护混币服务免受各种潜在的网络攻击和欺诈行为的能力,这包括:

(1) 代码安全性:涉及混币服务的智能合约或程序代码是否公开,是否经过安全专家的审计,以及是否存在已知的安全漏洞。

(2) 抵抗攻击能力:重放攻击(Replay Attack)^[40]、拒绝服务攻击(DoS)^[41]等混币服务防御攻击的能力。

表 3 混币平台分类

Table 3 Classification of coin mixing platforms

服务名称	隐私保护					安全性		效率成本		治理运营		互操作性		是否跨链
	混币技术	混币过程	网络节点	匿名级别	可追溯性	代码安全	抵抗攻击能力	混币花费	延迟	治理模式	合规性	部署层级	资产类型	
Helix ^[6]	结合多种混币技术 (混币池)	多对多	Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
BitMix Biz ^[20]		多对多	明/Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
Blender.io ^[21]		多对多	明/Tor	部分	中	未公开	一般	百分比	有	中心化	不符合	主链	BTC	否
TumbleBit ^[42]		多对多	明	完全	难	未公开	中等	动态	有	中心化	不符合	主链	BTC	否
AlphaBay ^[43]		多对多	Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
Bitcoin Fog ^[44]		多对多	Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
CoinMixer ^[45]		多对多	明	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
BestMixer ^[46]		多对多	明	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC/BCH/LTC 等	否
CryptoMixer ^[47]		多对多	明	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
MixCoin ^[48]		多对多	明/Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否
BitLaundry ^[49]	一对多	明/Tor	部分	中	未公开	一般	百分比	有	中心化	不符合	主链	BTC	否	
MixTum ^[50]	多对多	明/Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否	
BitLauder ^[51]	多对多	明/Tor	完全	难	未公开	中等	百分比	有	中心化	不符合	主链	BTC	否	
BlindCoin ^[52]	环签名	环形混币	明/Tor	完全	难	未公开	强	百分比	有	中心化	不符合	主链	BTC	否
Sudoku Wallet ^[7]	零知识证明	多对一	明	完全	难	未公开	强	百分比	有	中心化	不符合	主链	BTC	否
SecureCoin ^[53]		多对多	明	完全	难	未公开	强	百分比	有	中心化	不符合	主链	BTC	否
Xim ^[54]		多对多	明/Tor	完全	难	未公开	强	百分比	有	中心化	不符合	主链	BTC	否
ChipMixer ^[55]		多对多	明/Tor	完全	难	未公开	强	百分比	有	中心化	不符合	主链	BTC	否
Tornado Cash ^[56]		多对多	明	完全	难	公开审计	强	固定	有	去中心化	不符合	主链	ETH/ERC20 等	否
CoinParty ^[57]	多对多	明	完全	难	公开审计	强	动态	有	去中心化	不符合	主链	BTC	否	
ShapeShift ^[35]	跨链	多对多	明	部分	中	部分公开	中等	百分比	有	中心化	部分符合	主链	多种加密货币	是
changenow.io ^[36]	混币	多对多	明	部分	中	部分公开	中等	百分比	有	中心化	部分符合	主链	多种加密货币	是
JoinMarket ^[22]	基于 CoinJoin	多对多	明/Tor	完全	难	公开审计	强	动态	有	去中心化	不符合	主链	BTC	否
Wasabi Wallet ^[24]		多对多	明/Tor	完全	难	公开审计	强	固定	有	去中心化	不符合	主链	BTC	否
Samourai Wallet ^[25]		多对多	明/Tor	完全	难	公开审计	强	固定	有	去中心化	不符合	主链	BTC	否
CoinJoin ^[58]		多对多	明	完全	难	公开审计	强	动态	有	去中心化	不符合	主链	BTC	否
CoinShuffle ^[59]		多对多	明	完全	难	公开审计	强	动态	有	去中心化	不符合	主链	BTC	否

3)效率成本维度。

效率成本维度用于评估混币服务的操作效率和经济成本,这包括:

(1)混币花费:使用混币服务所需的费用,可以是固定费用、百分比费用或动态费用。

(2)延迟:是否存在延迟情况,延迟指交易完成所需的时间,包括网络处理、混币操作和区块链确认等待时间等。

4)治理和运营维度。

治理和运营维度涉及混币服务的管理、控制结构和合规性,这包括:

(1)治理模式:混币服务的管理和决策机构类型,包括中心化服务和去中心化服务。

(2)合规性:服务是否符合反洗钱(AML)和了解你的客户(KYC)的规定,对服务的广泛可用性和用户信任至关重要。

5)互操作性维度。

互操作性维度关注于混币服务在不同区块链技术和资产之间的兼容性和功能性,这包括:

(1)部署层级:标识混币服务是在主链(如比特币链或以太坊主链)还是在 Layer2 解决方案(如闪电网络、侧链)上运行。

(2)资产类型:服务支持的资产类型,如 BTC、BCH、ETH、ERC20、LTC 等,决定了服务的适用范围和用户群体。

(3)跨链功能:是否支持不同区块链间的资产混币,提高用户资产操作的灵活性和隐私性。

1.4 混币引发的犯罪活动

由于 AML 措施和 KYC 执行往往不完善或缺失,混币技术也被犯罪分子用作掩饰非法所得的工具。尽管在多数司法管辖区,加密货币混币器本身并不明确违法,其合规性仍是一个关键问题,暴露了由混币用户方和混币服务提供方构成的加密货币犯罪生态系统。

混币用户利用这些服务来掩盖收取非法利润的加密钱包与中心化交易所钱包之间的联系,从而避免触发反洗钱警报,并掩饰非法活动所得。这些活动包括洗钱、欺诈、盗窃、黑客攻击、赌博、暗网交易、勒索和资助恐怖主义等^[4]。对于这些犯罪分子来说,洗钱是混币技术被滥用最广泛的一种方式,混币技术又是其洗钱手段中最主要的底层机制。这类用户通常没有足够的专业技术自行操作混币技术,因此多依赖提供混币服务方。据 Chainalysis 报告显示^[60],2023 年所有从非法地址转出的资金中有 14%流向了混币服务,而这些混币服务中有 37%的

资金来自非法地址,相较于 2021 年的 12%,这一比例有一定增加。尽管 2023 年政府监管力度得到了加强,依然约有 3.3 亿美元的被盗资金转入了混币器,占总被盗资金的 23.6%,较 2022 年的 38.7%有所下降。2024 年 9 月,美国 FBI 指控来自佛罗里达州迈阿密和加利福尼亚州洛杉矶的两人自 8 月起合谋从一名受害者那里窃取和洗钱超过 2.3 亿美元的加密货币,并主要通过混币服务对被盗加密货币进行洗钱^[61]。

混币服务方为上述的混币使用方提供服务,帮助他们隐藏非法资金的来源和流向。作为服务提供者,这些平台或个体有责任执行严格的 AML 措施和进行恰当的 KYC。不幸的是,并非所有的混币服务提供者都遵循这些规定,部分混币服务提供者可能因为监管松懈、追求利益或技术匿名性而忽视这些重要的合规责任。2021 年 4 月,美国司法部逮捕并指控 Bitcoin Fog 的运营商洗钱、经营无证汇款业务^[62]。同年 8 月,Helix 混币器的运营商承认洗钱罪,并同意没收价值超过 2 亿美元的 4 400 多个比特币^[63]。2022 年 5 月至 2022 年 8 月^[64-65],美国财政部外国资产控制办公室(OFAC)因 Blender.io 和 Tornado Cash 参与朝鲜黑客集团 Lazarus 的洗钱活动对其实施制裁。2023 年 3 月,美国司法部关闭暗网混币器 ChipMixer,并指控其洗钱超过 30 亿美元,涉及勒索软件攻击和暗网市场交易等非法活动^[66]。同年 11 月,OFAC 对 Sinbad.io 实施制裁,该混币器被指控为朝鲜黑客组织 Lazarus 洗钱^[67]。随后,Lazarus 越来越多地使用跨链桥和 YoMix 混币器进行洗钱活动。据 Chainalysis 报告^[60],总体来说,2023 年通过跨链协议洗钱金额达 7.438 亿美元,较 2022 年翻了 2 倍多。2024 年 3 月,Bitcoin Fog 运营商被判共谋洗钱罪,被美国司法部依法制裁^[68]。同年,Samourai Wallet 被美国检察院指控执行了超过 20 亿美元的非法交易,并促进丝绸之路等非法暗网市场的超过 1 亿美元的洗钱交易、网络服务器入侵、网络钓鱼计划以及多个去中心化金融诈骗协议的活动^[69]。

2 区块链混币监管技术

混币监管技术的主要任务是解析并识别混币交易背后的实际活动,即去混币化(De-mixing),以揭露试图隐藏的交易路径和资金流。本文总结了目前基于人工规则、地址聚类、实体分类、异常交易检测和混币追溯 5 种混币监管技术,分别叙述其中最新的研究进展和应用效果。表 4 展示了区块链混币监

管技术代表性研究成果和所用到的方法。

2.1 基于人工规则的混币监管技术

基于人工规则的混币监管技术主要分为 3 类,包括基于统计分析的方法、基于单一服务的启发式方法和通用的启发式方法,每类都具有其特定的方法和应用重点。

2.1.1 基于统计分析的方法

基于统计分析的方法重点关注通过定量与定性统计手段评估混币服务的运作及市场行为,包括市场容量、营销策略以及其与非法活动的关联,以提供对混币服务全面的宏观视角。HOLT 等^[70]探讨了加密货币混币服务在开放网络和暗网上的营销方式及其实践,通过对其中 18 种混币服务的归纳分析,以更好地了解加密货币混币及其在促进互联网非法

交易中的作用。MÖSER 等^[71]初步通过图表分析 Bitcoin Fog、Blockchain.info 和 BitLaundry 等 3 种混币服务的实验数据,并在不完全了解真实身份的情况下探索其反洗钱策略。DE BALTHASAR 等^[72]使用 Chainalysis 工具对 Dark-Launder、Helix 和 AlphaBay 等混币服务进行安全问题分析,并在 Wasabi Wallet 和 Samurai Wallet 中进行的 CoinJoin 交易两跳内观察到了与各种犯罪活动(如黑客和勒索软件等)相关的实体地址。MIEDEMA 等^[73]分析了 BestMixer 在 2018 年 7 月至 2019 年 6 月期间处理的 15 574 笔混币交易,涉及金额达 4 500 万美元。研究发现尽管用户面临高风险,但采取的风险缓解措施有限,仅有 61% 的交易采用了 VPN 或 VPS 等 IP 遮蔽技术。该研究进一步讨论

表 4 混币监管技术研究总结

Table 4 Summary of coin mixing regulatory technology

技术类别	任务目标	适用范围	文献	关键方法	优点	缺点	
基于人工规则	提供混币交易的宏观视角和规则匹配	通用服务	文献[71-73]	定量、定性统计	提供宏观视角	无法精准识别	
		比特币	文献[74-81]	启发式规则	专注于特定的混币服务， 高效且准确率高	扩展性差	
		以太坊	文献[33,82-83]	启发式规则			
		通用服务	文献[84-87]	启发式规则	扩展性好	平衡通用和高效较难；误报率高	
基于地址聚类	识别可能属于同一用户或实体的混币地址	通用服务	文献[88-90]	多输入启发式	简单高效，准确性高	易受混淆攻击影响；忽视交易上下文	
			比特币	文献[91]	找零地址启发式	有效利用比特币交易的找零机制	识别范围有限；误报率高
			文献[92-94]	改进的启发式聚类	识别范围广、误报率低、 识别率高	无法检测新出现和模糊模式的混币服务； 缺乏真实标签，评估验证难	
		以太坊	文献[95]	改进的启发式聚类			
		通用服务	文献[96-99]	网络聚类、社区检测	不依赖于特定的规则，在缺乏明确先验知识的情况下更适合	计算成本高、可扩展性差、误判率高、适应性差、评估验证难	
		基于实体分类	识别分类参与区块链混币交易地址	比特币	文献[100]	机器学习	自动高效；准确性高；能够适应新出现的混币模式和策略
文献[101]	集成学习						
文献[102]	社区异常检测						
文献[103]	网络分析、PU 学习						
通用服务	文献[104]			决策树			
	文献[105]			面向目标建模、角色识别			
以太坊	文献[106]			图神经网络			
基于异常检测	混币异常交易检测			比特币	文献[107]	随机森林	自动、高效、快速、灵活性高
		文献[108]	异常检测				
		文献[109]	LSTM				
		文献[110]	图表示学习				
	洗钱异常交易检测	通用服务	文献[111]	图自动编码器		受限于训练数据规模小，泛化性能较差； 仅限 Elliptic 数据集，非真实交易数据集	
			文献[112]	图同构神经网络			
			文献[113]	集成学习			
			文献[114]	多关系图神经网络			
			文献[115]	异常检测、主动学习			
			文献[116]	改进的 XGBoost			
追溯监管	追踪和溯源资金流向	比特币	文献[117-119]	污点分析	自动、高效、快速	计算资源较多；针对对抗性行为需要改进方案	
		通用服务	文献[120]	社区检测、关键节点识别			
		ShapeShift跨链服务	文献[121]	启发式聚类			

导致了这一行为的可能原因,如信息不对称性和混币服务在犯罪资金兑现过程中的作用,以及这些发现对加密货币安全生态系统的潜在影响。

2.1.2 基于单一服务的启发式方法

基于单一服务的启发式方法通常专注于特定的混币服务,开发特定的启发式技术,以识别和分析这些服务特有的交易模式和行为。这种方法深入到交易细节,利用交易数据的具体特征,有效识别潜在的非法行为和风险。

在比特币的未花费交易输出(UTXO)交易模型中,STOCKINGER^[74]对 Wasabi 和 Samourai 两种钱包服务在广阔的比特币生态系统中的作用、演变以及其潜在的匿名化能力进行了详细探讨,并开发了一套启发式方法来检测这些服务中的 CoinJoin 交易。SCHNOERING 等^[75]开发了一系列启发式方法,旨在检测促进 CoinJoins 协议的混币交易。CONTI 等^[76]对勒索软件相关的比特币交易进行了深入分析,并引入了一个轻量级启发式框架以识别勒索软件犯罪分子所控制的比特币地址。MAKSUTOV 等^[77]提出基于 CoinJoin 交易的去中心化匿名和追踪方法。TIRONSAKKUL 等^[78]通过分析 Wasabi CoinJoin 不同时间段的交易模式和模糊机制的变化,提出一种基于已知交易模式集的检测方法,并在几起著名的加密货币盗窃事件中进行应用,发现有被盗的比特币直接到达检测到的 Wasabi CoinJoin 交易的实例。SHOJAEENASAB 等^[79]通过与 3 个混币器(MixTum、Blender 和 CryptoMixer)进行交易来收集标记数据并统计重复出现的模式,以此检测比特币网络中的混币交易、混币地址、发送者地址和接收者地址。李虎等^[80]开发了一种专门针对 CoinJoin 混币交易的检测方法,即识别交易输出项个数大于输入中 UTXO 个数以及输出项金额中存在大量重复值的多输入多输出交易,并利用 Wasabi 平台数据进行验证和优化,显著提高了检测的召回率和准确率。HONG 等^[81]针对使用最广泛的比特币混币服务之一的 Helix 提出了一种去混币算法,通过利用混币服务的静态和动态参数来去匿名化混币服务的输入和输出地址之间的关系,实验表明该算法能以 99.14% 的准确率识别 Helix 混币服务的输入和输出地址之间的关系。

在以太坊账户模型中,YOUN 等^[33]对 Tornado Cash 中的充值地址进行聚类分析,列出潜在的犯罪地址,并厘清 Tornado Cash 中与洗钱和 NFT 网络钓鱼事件相关的实际情况和损失总额。TANG

等^[82]基于链上数据提取了 Tornado Cash 中两种类型的交易模式,提出了 3 种启发式聚类规则来链接用户的地址以减少用户匿名集的大小。WU 等^[83]开发了一款基于专家启发式构建的应用程序,它可以根据交互历史记录将以太坊地址进行聚类,以识别可能由同一实体拥有的其他地址。同时,该程序可以向以太坊用户显示他们可能受到损害的交易,并通过排除潜在受损的交易来计算每个 Tornado Cash 匿名池的真实大小。

2.1.3 基于通用服务的启发式方法

目前,基于单一服务的启发式方法是特定于所选混币服务的,不能推广到其他混币服务,即大多仅适用于某些特定类型的交易,难以扩展到复杂多样的实际场景,因此不能用作分析混币服务的通用工具。随着混币交易量显著增加,这种人工分析少数混币交易已变得不可行。因此,设计一种更通用、更高效的去混币算法是一个具有挑战性的问题。WU 等^[84]提出了一种用于混币服务的通用抽象模型,通过一个三阶段工作流程详尽描述了混币服务的操作机制,并识别出了两种主要的混币机制,成功地揭示了 ChipMixer、Wasabi Wallet、ShapeShift 和 Bitmix. Biz 4 种代表性服务的混币机制。此外,还提出了一种基于混淆机制的通用启发式算法来识别混币交易的方法,并将其应用在追踪被盗比特币资金流向的案例研究中,结果显示该算法能够识别超过 92% 的混币交易。HONG 等^[85]深入分析了现实世界中的混币服务,并提出了一种通用的比特币去混币算法。该算法综合考虑了混币服务的静态与动态参数,有效地映射了输入地址与相应输出地址之间的关系。YOUSAF 等^[86]利用来自 ShapeShift 的 13 个月数据及 8 个不同区块链的数据,探讨了跨加密货币跨链混币的交易模式及其平台用途,不仅开发了新的启发式方法,还创建了跨加密货币账本的链接,从而识别了各类交易模式,提升了通用性。BÉRES 等^[87]探索了以太坊账户模型中混币交易的地址关联技术,使用交易费用的末 4 位数字、交易时间及金额等多种数据点组合匹配,建立了发送者与接收者之间的关联性。

2.2 基于地址聚类的混币监管技术

地址聚类是一种识别和分析比特币交易行为的技术,通过将多个地址关联到同一实体来追踪资金流。这种方法为混币检测提供了基础数据和分析工具,有助于解析通过混币服务进行的复杂交易模式,识别交易链条中的实体关系。

2.2.1 启发式地址聚类

启发式地址聚类方法是根据某些交易规则,即交易行为的共同特点来推断哪些地址可能由同一实体控制,这些规则通常基于交易数据中观察到的模式和统计关系。MEIKLEJOHN 等^[88]提出了目前主流的地址聚类方法是多输入启发式和找零地址启发式。多输入启发式[如图 2(a)所示]是启发式地址聚类中使用的一种常见规则,该方法基于“如果多个地址共同作为一笔交易的输入,那么这些地址很可能属于同一个钱包或用户”的假设^[89]。因为执行一笔交易需要访问到所有输入地址的私钥,所以多个输入地址共同出现在一个交易中通常意味着它们

是由同一实体控制。通过识别这样的模式,可以将不同的交易和地址链接起来,从而识别出潜在的用户或用户群^[90]。REID 等^[91]引入了用于识别找零地址的启发式算法[如图 2(b)所示]。找零地址启发式基于交易中找零的过程来识别哪个输出地址可能属于发送方,从而帮助区分哪些地址可能由同一个用户控制。在比特币等加密货币交易中,如果发送的金额少于来源地址的总余额,超出的部分将作为找零返回给发送者。因为找零地址通常是新生成的,并且只由原交易的发起者控制,所以通过分析交易输出中的金额大小、输出地址新鲜度(即是否是首次出现)等特征可以来推断哪个地址是找零地址。

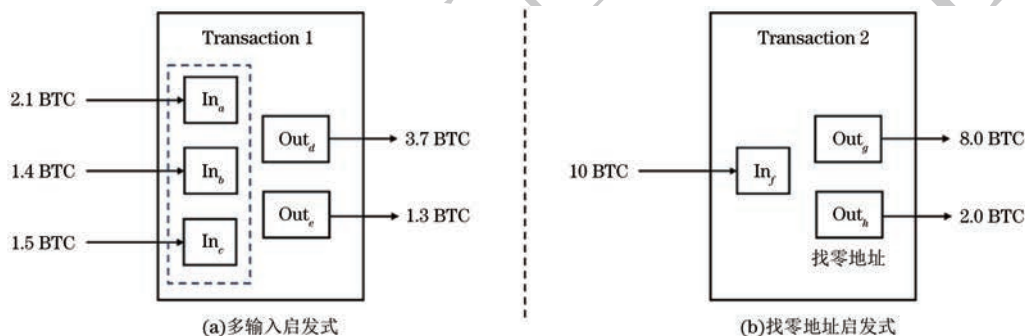


图 2 多输入和找零地址启发式的地址聚类原理图

Fig. 2 Schematic diagram of multiple input and change address heuristic address clustering

在图 2(a)中,用户 A 有多个钱包地址(In_a 、 In_b 、 In_c),并且这些钱包地址在一笔交易中提供了多个输入,然后交易的资金流向多个目标地址(如 Out_d 、 Out_e),这些目标地址可能属于不同的用户地址。在图 2(b)中,用户 A 通过钱包地址 In_f 发送了 8.0 BTC 到接收地址 Out_g ,但原本地址 A 中有 10 BTC。由于找零机制,剩余的 2.0 BTC 会返回到一个新的“找零地址”,因此这个找零地址与用户 A 的原始钱包地址 In_f 相关联,推测均属于同一个用户。

然而,以上传统启发式地址聚类方法仅限于比特币 UTXO 交易模型,且在实际应用中面临识别率低、误报率高的问题,可能会被攻击者绕过,从而导致不准确的结果。与此同时,单一的启发式方法和不完全的启发式条件很难对大量地址进行全面、准确的聚类,只能将标签扩展到有限数量的地址,而无法识别其余地址(不属于同一集群)。ZHANG 等^[92]提出了通过消除后续作为非找零地址被重用的地址来检测一次性找零地址的新启发式方法,该方法适用于两种传统启发式方法无法识别一次性找零地址的交易。针对不同规模的比特币交易数据的实验结果表明所提出的启发式方法对地址减少率的

平均贡献为 0.33%。HE 等^[93]使用 6 种启发式条件对地址和实体进行聚类以分析比特币交易和地址之间的关联,并通过添加条件约束提出了一种改进的找零地址检测算法,与传统找零地址算法进行比较证明了改进算法的有效性,识别的找零地址更加准确,加快了算法收敛速度。LIU 等^[94]创新性地提出了一种基于多条件识别一次性找零地址的聚类方法,并利用链上比特币交易数据进行实验表明所提出的方法比其他启发式方法至少多识别 12.3% 的一次性找零地址,将地址聚类性能提高了 5.7%,并显著降低了识别结果的误报率。VICTOR^[95]基于与存款地址相关的模式、多次参与空投和代币授权机制提出了一种适用于以太坊账户模型的启发式地址聚类方法,实验结果表明所提出的方法可以将所有活跃外部账户的 17.9% 地址聚类在一起。然而,以上改进的启发式方法即使通过改进多个规则可以提高召回率,但是对于新出现和具有模糊模式的混币服务检测是无效的。由于缺乏地址实际上属于同一实体的真实标签,因此很难评估聚类启发式方法的质量。

2.2.2 基于网络方法的地址聚类

基于网络方法的地址聚类是将比特币或其他加密货币的整个交易网络视为一个图形结构。社

区检测是图论中的一种关键技术,用于识别网络中连接紧密的子群体,即社区。在加密货币交易网络中,这些社区可能代表由单个用户或紧密相关的用户群控制的地址集合。与基于启发式的地址聚类方法不同,基于网络的社区检测方法不依赖于特定的规则,有助于在缺乏明确先验知识的情况下发掘新的或非预期的模式。WAHRSTÄTTER 等^[96]使用无监督机器学习 k -means 来分析完整的比特币用户图,以识别可能参与非法活动的可疑行为者,将聚类算法应用于比特币用户图的 CoinJoin 交易,与地面真实数据集的比较研究发现改进的聚类方法能够在最可疑的集群中捕获更多非法活动。WAHRSTÄTTER 等^[97]提出了一种改进的多输入聚类方法,该方法结合了先进的隐私增强技术,通过定量网络分析检验了经过 CoinJoin 调整的比特币用户图,所提出的聚类方法和链下信息的结合与传统多输入聚类相比更具有效性,有助于更全面地了解比特币交易网络中的隐私问题,并为制定加强措施防止洗钱和恐怖主义融资奠定基础。REMY 等^[98]利用社区发现算法和比特币交易网络来重新识别属于同一用户的多个地址,以揭示隐藏在复杂网络交互中的结构和关联。SUN 等^[99]提出了一种基于机器学习的用户身份识别和恶意用户检测方法,该方法利用区块中的交易信息将用户和智能合约聚类成组。然而,基于网络的方法在应对大规模、动态的区块链交易网络时,面临计算成本高、可扩展性差、误判率高、适应性差以及评估验证困难等问题。

2.3 基于实体分类的混币监管技术

基于实体分类的混币监管技术侧重于识别和分类参与区块链混币交易的实体账户。本文将混币账户检测视为实体分类问题,基于机器学习和深度学习的解决方案利用手动提取的特征或图神经网络(GNN)来表征区块链账户地址,从而实现中心化和去中心化混币服务的检测。但是,此类解决方案受限于训练数据规模小、泛化性能较差。王大宇等^[100]提出了一种基于机器学习的解决方案,该方案可以准确地识别比特币地址的类型及混币交易意图。所提出方法的核心是通过一些可靠的启发式方法和一种新颖的先导预测方法,自动化地迭代增加训练集中的比特币地址,从而不断反馈给模型再次训练,稳定提升机器学习模型的性能。评估结果表明所提出的方案在公开数据集中以 0.99 的精度识别混币交易,并在识别比特币地址类型的任务中达到 96.21% Micro F1 分数和 95.67% Macro F1 分

数。XU 等^[101]提出了一种新颖的检测方案来识别属于比特币混币服务的地址。具体来说,该方案基于比特币地址交易网络的构建与可视化,结合多种不同算法模型的优点设计了新的双集成分类模型,同时为了检测更复杂的混币模式,从已建立的比特币地址交易网络中提取交易子图,使用嵌入到模型中的基于内核的图分类方法对子图进行分类。通过构建的混币数据集和 Elliptic 洗钱数据集的综合实验证明所提出的模型可以有效地识别参与混币过程的地址,且对比特币洗钱交易的检测准确率达到 99.84%。PRADO-ROMERO 等^[102]通过建立比特币用户网络,采用社区异常检测方法对混币账户进行识别与分类。WU 等^[103]开发了基于网络、账户和交易特征的网络分析框架来检测属于混币服务的地址,并提出了带属性的时间异构基序算法以更好地表征不同类型地址的交易模式,同时将混币检测任务作为积极的无标记(PU)学习问题来处理以解决样本不平衡标记的问题。然而,所提出检测方法基于已知的混币规则,因此很难检测未知的混币模式。RATHORE 等^[104]开发了基于 C4.5 决策树的高精度模型来识别提供混币服务的地址,针对整个特征集中的每个特征计算信息增益,并选择具有较高信息增益的 8 个特征进行建模,最大限度地减少了整体计算时间,使检测过程能高效地在真实环境中工作。实验表明利用 55 个节点的短决策树模型能够实现超过 97% 的准确率。LIU 等^[105]提出了一种面向目标建模的方法,该方法使用历史比特币交易数据对比特币混币场景下基于代理的洗钱业务流程中不同类型的角色进行建模、挖掘、发现和分析。DU 等^[106]提出了一个名为 MixBroker 的图神经网络框架以研究以太坊上广泛使用的混币服务 Tornado Cash 中的混币交易地址关联问题,旨在通过节点对链接预测的角度破解 Tornado Cash 的匿名性,该机制捕捉了交易图内节点的互联本质,并通过节点嵌入计算账户节点间的关联概率。通过大量 Tornado Cash 中真实混币交易和基于以太坊名称服务(ENS)构建的标签数据进行的实验表明, MixBroker 在以太坊混币交易地址关联任务中的性能优于其他方法。

2.4 基于异常交易检测的混币监管技术

基于异常交易检测的混币监管技术更侧重于交易级别的检测,即识别交易中的异常(混币或洗钱)或不寻常行为(非混币或非洗钱)。STÜTZ 等^[107]基于 Wasabi、Samourai 混币交易数据集和手工提取的交易特征训练随机森林分类器,将混币

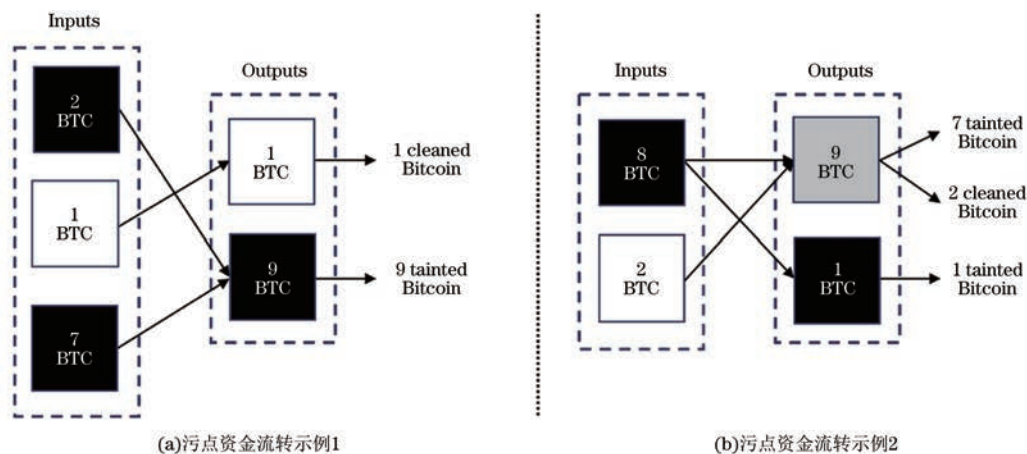
交易检测问题转化为二元分类问题。然而,由于比特币和以太坊结构的差异,这些方法不适用于以太坊混币服务的检测。NAN 等^[108]认为比特币交易图具有社区属性,并将混币服务视为集群异常值,基于真实的比特币交易历史数据创建交易有向图,并提出了一种基于深度学习和局部离群点算法的方法来识别混币交易活动,实验表明所提出的方法优于识别社区的启发式方法。SUN 等^[109]提出一种基于 LSTM 模型的交易数据分类框架,该方案包括基于深度学习的比特币交易特征提取和分类。实验表明与基于规则的方法和基于图神经网络的分类算法相比,所提出的分类方法能更好地发现新类别的混币交易。YANG 等^[110]结合比特币交易的局部特征和全局特征提出了时空混币检测算法以识别混币交易,创造性地构建了包含交易时空特征的全局位置编码,并将其纳入混币检测模型的特征提取过程中,基于 Elliptic 洗钱交易数据集和根据 WalletExplorer 构建的混币交易数据集的实验证明该算法对于不平衡的混币交易检测任务是有效的。

除此之外,与混币服务关联的洗钱交易识别和检测也已有较多的研究工作。YU 等^[111]提出了一种新的区块链洗钱检测方法,该方法通过交易金额评估交易的重要性,结合图自动编码器来学习交易的结构信息,并设计了交易分类损失和结构重建损失以优化学习过程,在 Elliptic 数据集上的测试结果显示所提出的方法性能上超过了现有最先进的技术,保持了良好的可扩展性。LO 等^[112]提出了一种基于自监督的 DGI (Deep Graph Infomax) 和图同构网络(GIN)的图神经网络框架,并结合随机森林算法来检测非法行为反洗钱交易,在 Elliptic 数据集上的实验结果表明所提出的方法在关键分类指标方面优于最先进的方法。ALARAB 等^[113]利用具有交易节点和有向资金流的比特币交易时间序列图对经典监督学习方法的性能进行了比较分析,以检测网络中的洗钱交易,所提出的集成学习方法结合了给定的监督学习模型,其性能优于经典的机器学习方法。HYUN 等^[114]提出了一种检测加密货币混币异常交易的新方法,该方法结合边方向和特征设计了基于多关系图神经网络的异常检测模型。此外,开发的自适应邻居采样器旨在提高定位性能和控制计算成本。LORENZ 等^[115]基于局部离群因子(LOF)、 k 近邻(k -NN)、隔离森林(IF)和 OCSVM (One-Class SVM)等 7 种常见的异常检测算法,联合主动学习策略,在现实限制标签访问的情况下对

Elliptic 数据集进行洗钱活动的检测任务。VASSALLO 等^[116]改进 XGBoost 算法以更好地处理动态的洗钱交易,对各种集成算法和启发式算法进行比较发现所提出的方法提高了交易级别的召回率。

2.5 混币服务的追溯监管技术

混币服务的追溯监管技术指通过污点分析(如图 3 所示的污点资金流转示例)等特定技术手段对加密货币混币活动进行监控和分析,以识别、追踪和溯源资金流向。这些技术对于打击混币服务和其他非法活动具有重要的实践意义。TIRONSARKKUL 等^[117]提出了一种新的基于污点分析的地址跟踪策略,该策略通过改进传统技术追踪经过混币服务的比特币,用于混币服务中的地址关联,同时结合地址聚类 and 逆向污染技术,通过引入交易特征的过滤标准减少误报结果的数量,有效地追踪了 9 个混币服务的交易,研究显示提出的方法能显著降低潜在交易输出的数量。TIRONSARKKUL 等^[118]提出了一种改进的比特币污点分析追踪方法,该方法适应地址所有权的上下文并避免追踪无关交易。具体来说,该团队引入了一种结合地址画像的比特币污点分析方法,提出了两种基于上下文的污点分析策略,设计了一组基于假设行为和区块链内可识别模式的指标,使用 26 个历史已知的比特币盗窃案例的样本数据进行实验,揭示盗窃案件中独特的交易行为,实验显示了提出的方法在揭示非法比特币的花费和混币策略方面的潜力。WU 等^[119]通过搜索网络犯罪源账户,包括交易所黑客、DeFi 开发者和诈骗者,利用污点分析技术逐层跟踪下游的各种交易和地址。在跟踪结束时,对服务提供商进行机器学习的识别和分类,进而观察到制造假币、冒充投机者等不断升级的洗钱方式。WU 等^[120]提出了一个通用、可扩展的交易跟踪工具 Tracer,该工具通过子图搜索方法解决交易跟踪任务,并采用一种新颖的排序方法推断多关系区块链交易图中图搜索过程中账户之间的相关性,利用 Kucoin 交易所遭到黑客攻击的大量被盗资金交易进行实验显示总共有 13.8K ETH 被转移到 Tornado Cash 的 100 ETH 池中,与慢雾专家的结论类似。ZHANG 等^[121]开发了一个基于地址关联的通用追溯框架,专门用于处理 ShapeShift 上的超过 170 万笔跨账本交易,还设计了一套跨账本聚类的组合启发式方法,并成功地形成了 24 925 个跨账本集群,所提出的方法已被成功应用于 9 个真实的交易平台,展示了其在实际环境中的有效性和适用性。



(a)污点资金流转示例1

(b)污点资金流转示例2

图 3 污点资金流转示例

Fig.3 Examples of tainted fund circulation

在图 3 中,每个图显示一笔交易的输入、输出及资金流动方向。输入中的白色模块代表干净的比特币,黑色模块代表污染的比特币。输出的颜色表示污染程度,白色模块为干净,黑色模块为完全污染,灰色模块为混合状态。

3 区块链混币监管工具

近年来,工业界中各种区块链混币和洗钱监管工具也应运而生,这些工具旨在提高交易透明度和合规性。Chainalysis Reactor^[122]是一款拥有业内最广泛的混币器覆盖范围和分析工具的软件。它能够追踪和分析各种混币器,从而帮助用户识别和了解涉及混币的交易行为。不仅如此,Chainalysis 公司的 KYT^[123]产品还可以帮助用户深入挖掘区块链上的交易数据,揭示潜在的洗钱活动或其他违规行为。Clain 公司的 Probe^[124]利用其先进的交易过滤引擎,帮助用户对交易进行去混币,即解析混币交易中的混淆和匿名化操作,以揭示交易的真实流向和参与方,用户能够更加清晰地理解和分析区块链上的交易活动,从而提高对加密货币市场的洞察力和理解。Elliptic 公司提供的加密货币钱包筛查和监测软件^[125]能够帮助用户监控加密货币钱包的活动,及时发现可疑行为。MistTrack^[126]作为一个适用于所有人的加密货币追踪和合规平台,具有反洗钱功能,能够帮助用户进行合规监管,确保其交易符合法规要求。CipherTrace^[127]提供加密货币反洗钱解决方案,并提供交易监控、钱包筛查和风险评估功能,支持合规和风险管理,类似的工具还包括 Crystal Blockchain^[128]、Scorechain^[129]、TRM Labs 系列^[130]、QLUE^[131]等。这些工具的综合应用可以提高用户在加密领域的安全性和合规性水平。混币监管工具总结如表 5 所示。

4 挑战与展望

在当前阶段,区块链混币检测面临着一系列挑战,这些挑战涵盖了多个维度,影响着混币行为的识别和分析。针对当前阶段区块链混币检测面临的挑战,本文从以下 5 个方面进行展望。

4.1 标签信息的完善

混币服务通常只涉及比特币网络中一小部分地址,并且往往不会公开这些地址的真实身份或标签信息。这种不完整的标签信息意味着大多数地址的真实身份仍然是未知的,从而增加了混币行为的识别难度,导致混币过程中涉及的地址难以被追踪和分析,限制了混币检测工具的准确性和可靠性。因此,需要加强区块链社区、混币服务方和监管机构之间的合作,分享混币地址及其标签信息,提升数据的全面性和准确性;利用深度学习技术,从已有的区块链交易数据中提取更多潜在的标签信息;鼓励用户和企业报告可疑地址,通过建立奖励机制,激励社区参与标签信息的完善。

4.2 混币交易动态性的关注

混币交易的动态性是指混币服务在其操作中展现出高度灵活性和适应性。混币平台通常会实时调整其策略,例如分割和合并交易,以响应外部监管压力或技术变化,从而最大限度地混淆交易的追踪路径。由于涉及的交易数量和结构变化多端,这种动态过程使得识别混币行为变得更加困难。具体来说,一些混币服务会通过合并来自多个源的交易或将单一的大额资金拆分成多个小额交易来增加交易链的复杂度和追踪的难度。此外,区块链技术本身的发展也给混币检测带来了额外挑战。区块链的协议更新或分叉可能引入新的隐私特性,如隐私增强的加密方法或匿名交易技术,这些都可能改变交易

表 5 混币监管工具总结
Table 5 Summary of coin mixing regulatory tools

公司-工具	主要功能	优势	局限性
Chainalysis-Reactor	识别混币服务相关地址和交易； 帮助反洗钱和合规工作	覆盖多种主流区块链； 提供详细的交易图谱； 可追溯到真实身份,适用执法部门	对隐私币(如 Monero、Zcash)分析能力较弱； 对新型混币技术适应存在滞后
Chainalysis-KYT	实时监控和标记潜在的洗钱、诈骗、 混币和其他非法活动	实时风险评分和警报； 全球范围交易监控,覆盖多个币种	对于混币服务中“假阳性”可能较高,容易误报； 对小额交易识别不够敏感
Clain-Probe	基于机器学习的交易分析,自动标 记与混币相关的交易	针对性强,专注于混币检测； 算法效率高,部署灵活	市场占有率相对较低； 功能单一,对复杂混币模式的分析有限
Elliptic-Wallet Screening/ Transaction Monitoring	通过行为分析技术追踪洗钱、欺诈 和混币交易； 提供可疑交易分析报告	适用于全球多种区块链； 支持法币入金与出金追踪,增强跨 境交易监控	对隐私币和复杂匿名交易的监控效果较差； 需要额外配置和人工干预； 对新兴混币服务覆盖不足
SlowMist-MistTrack	识别与混币相关的地址和交易,并 提供资金流向分析	高效处理多个交易平台和网络之间 的资金流动	需要大量的计算资源； 对于完全匿名交易(如使用隐私币)存在盲点
Mastercard-CipherTrace	识别洗钱、欺诈和混币服务的追踪 和风险分析	适用于多种主流和隐私币； 提供强大的报告功能	对隐私币(如 Monero、Zcash)的分析能力有限； 系统响应速度待优化
Bitfury Group-Crystal Blockchain	专注于识别与洗钱、混币等非法行 为相关的交易分析与可视化	直观界面,适合不熟悉技术的团队； 强大的报告功能,便于监控和调查	对一些新兴币种和去中心化平台支持较弱； 对于非常复杂或匿名化交易支持不充分
Scorechain SA-Scorechain	提供 AML 合规工具； 识别与混币、洗钱相关的交易	灵活性强,用户可自定义检测规则； 提供资金流动路径报告	数据覆盖和算法精准度低； 对一些新兴区块链和去中心化交易所支持不足
TRM Labs-TRM Labs 系列	实时监控和监测加密交易,特别关 注洗钱及混币服务； 提供风险评估调查工具	支持多种主流区块链,提供详细的 交易报告和风险分析； 强大智能合约分析能力	对于混币行为和复杂的匿名交易存在分析盲区； 对新兴币种或链上的支持灵活性和广度不足
BIG (Blockchain Intelligence Group)-QLUE	识别与非法活动相关的地址和交易； 追踪资金流动并生成风险报告	支持多个主流和隐私币； 提供多种报告和警报功能	数据覆盖面和支持的币种相对较少； 在处理混币跨链资金流动时精确度有所限制

的基本方式,使得依赖于传统分析方法的现有混币检测工具失效。因此,可以开发监控技术,追踪混币服务的动态变化,及时发现异常交易行为;对于基于以太坊的混币服务,深入研究和解析智能合约,通过智能合约行为模式识别混币活动;持续跟踪区块链协议的更新,快速调整混币检测工具以适应新隐私特性。

4.3 效率和通用性检测的平衡

混币服务由不同的第三方平台提供,而不同平台采用的操作模式和技术策略存在较大差异,可能使用各种不同的算法和技术来增加交易的匿名性,如通过更换地址、更改交易的时间间隔,以及调整转账金额等手段来混淆交易链,导致了混币模式的多样性,从而使得开发一个能够广泛适用于多种类型混币操作的通用检测工具变得极为复杂。同时,这种多样性增加了计算开销和开发维护成本,无法保证检测工具的灵活性、效率和可靠性,这使得平衡检测工具效率和通用性成为具有挑战性的任务。因此,可以设计模块化检测系统,不同模块针对不同类型的混币操作进行优化,提升整体效率;开发自适应算法,根据交易特点动态调整检测策略,提高通用性和效率;利用分布式计算资源,减轻单个检测工具的

计算负荷,提高检测速度和灵活性。

4.4 验证可行性的提高

混币服务账户的特征往往难以被准确验证。即使预测地址属于混币服务,由于缺乏足够的上下文信息,验证这些地址的真实身份或背后的交易目的往往十分困难。通常来说,一个地址可能只是作为交易的一部分而被用于混币服务,而没有更多的信息来揭示其背后的用户或其资金的最终用途,增加了检测混币服务的实际运营和行为的复杂性。在某些情况下,合法的交易活动因为其复杂性或与混币服务的偶然相似性而被错误地标记为可疑活动,增加了监管机构和执法机构在混币检测过程中的误报率,从而影响了监管机构和执法机构的判断和行动。因此,可以结合多种验证手段,如链下社交信息、跨平台数据比对,提升验证的准确性;引入更多的上下文信息,如交易时间、频率、交易对手等,以全面了解交易背景,提高验证效果;建立健全的误报处理机制,通过反馈和学习不断改进检测算法,减少误报率。

4.5 新型混币技术的适应

随着监控技术的发展,混币服务提供者也在不断地开发新的伪装技术和反监控措施,如闪电网络

等提供了更高级的匿名性和更快的交易速度,跨多个区块链的复杂交易路径增加了检测复杂度和难度。这些新型混币技术不仅加大了监管和执法机构的工作难度,也提出了技术和策略上的挑战。即便是使用最先进的分析工具,也难以有效地识别和追踪这些通过高级隐私保护技术进行的混币交易。因此,需要跟踪最新的混币和反监控技术,提前布局检测方案;开发跨链分析工具,处理复杂的跨链交易路径,提高检测的覆盖面和准确性;研究并破解新型隐私保护技术,增强对高级匿名交易的识别能力。

5 结束语

本文全面审视了混币服务的技术基础和机制分类,并构建了一套分类体系来综合评估各种混币工具。本文首先深入分析了混币服务可能触发的犯罪行为,并详尽讨论了 5 种主要的混币监管技术——基于人工规则、地址聚类、实体分类、异常交易检测及混币服务追溯的最新研究成果,以期增强对这些复杂交易的监控和透明度,进而抑制非法行为的发生;接着总结了目前工业界中与混币监管相关的各类工具和平台,为监管机构进行混币洗钱监管的实践提供了有效的支持与策略建议;最后就标签数据的完善、算法的通用性及效率、结果验证和相关政策制定等方面提出了未来研究可能的方向,旨在推动加密货币混币监管技术的进步,确保金融安全与合规。

参考文献

- [1] 倪雪莉, 马卓, 王群. 区块链矿池网络及典型攻击方式综述[J]. 计算机工程, 2024, 50(1): 17-29.
NI X L, MA Z, WANG Q. Overview of blockchain mining pool networks and typical attack modes [J]. Computer Engineering, 2024, 50(1): 17-29. (in Chinese)
- [2] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115.
LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115. (in Chinese)
- [3] 李旭东, 牛玉坤, 魏凌波, 等. 比特币隐私保护综述[J]. 密码学报, 2019, 6(2): 133-149.
LI X D, NIU Y K, WEI L B, et al. Overview on privacy protection in Bitcoin[J]. Journal of Cryptologic Research, 2019, 6(2): 133-149. (in Chinese)
- [4] SEE K. The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers [J]. Journal of Financial Crime, 2024, 31(2): 416-426.
- [5] CHAWKI M. Cybercrime and the regulation of cryptocurrencies[M]//ARAI K. Advances in information and communication. Berlin, Germany: Springer International Publishing, 2022: 694-713.
- [6] CRAWFORD J, GUAN Y. Knowing your Bitcoin customer: money laundering in the Bitcoin economy[C]//Proceedings of the 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE). Washington D. C., USA: IEEE Press, 2020: 38-45.
- [7] PAKKI J, SHOSHITAISHVILI Y, WANG R Y, et al. Everything you ever wanted to know about Bitcoin mixers (but were afraid to ask) [M]//BORISOV N, DIAZ C. Financial cryptography and data security. Berlin, Germany: Springer, 2021: 117-146.
- [8] 宋靖文, 张大伟, 韩旭, 等. 区块链中可监管的身份隐私保护方案[J]. 软件学报, 2023, 34(7): 3292-3312.
SONG J W, ZHANG D W, HAN X, et al. Supervised identity privacy protection scheme in blockchain[J]. Journal of Software, 2023, 34(7): 3292-3312. (in Chinese)
- [9] 赵楷, 胡煜环, 闫俊桥, 等. 基于区块链的版权保护研究综述[J]. 计算机工程, 2025, 51(8): 1-15.
ZHAO K, HU Y H, YAN J Q, et al. Overview of copyright protection research based on blockchain [J]. Computer Engineering, 2025, 51(8): 1-15. (in Chinese)
- [10] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
ZHU L H, GAO F, SHEN M, et al. Survey on privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186. (in Chinese)
- [11] FENG Q, HE D B, ZEADALLY S, et al. A survey on privacy protection in blockchain system [J]. Journal of Network and Computer Applications, 2019, 126: 45-58.
- [12] WANG D, ZHAO J D, WANG Y J. A survey on privacy protection of blockchain: the technology and application[J]. IEEE Access, 2020, 8: 108766-108781.
- [13] PENG L, FENG W, YAN Z, et al. Privacy preservation in permissionless blockchain: a survey [J]. Digital Communications and Networks, 2021, 7(3): 295-307.
- [14] 王佳鑫, 颜嘉麒, 毛谦昂. 加密数字货币监管技术研究综述[J]. 计算机应用, 2023, 43(10): 2983-2995.
WANG J X, YAN J Q, MAO Q A. Overview of cryptocurrency regulatory technologies research[J]. Journal of Computer Applications, 2023, 43(10): 2983-2995. (in Chinese)
- [15] 陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战[J]. 计算机研究与发展, 2018(9): 1853-1870.
CHEN W L, ZHENG Z B. Blockchain data analysis: a review of status, trends and challenges [J]. Journal of Computer Research and Development, 2018(9): 1853-1870. (in Chinese)
- [16] HOU W H, CUI B, LI R. A survey on blockchain data analysis [C]//Proceedings of the IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). Washington D. C., USA: IEEE Press, 2021: 357-365.
- [17] YADAV S P, AGRAWAL K K, BHATI B S, et al. Blockchain-based cryptocurrency regulation: an overview [J]. Computational Economics, 2022, 59(4): 1659-1675.
- [18] WU J J, LIU J L, ZHAO Y J, et al. Analysis of cryptocurrency transactions from a network perspective: an overview [J]. Journal of Network and Computer Applications, 2021, 190: 103139.
- [19] ZIEGELDORF J H, MATZUTT R, HENZE M, et al. Secure and anonymous decentralized Bitcoin mixing [J]. Future Generation Computer Systems, 2018, 80: 448-466.
- [20] BitMix.Biz[EB/OL]. [2024-07-18]. <https://bitmix.biz/>.
- [21] Blender.io[EB/OL]. [2024-07-18]. <https://blender.io>.

- [22] JoinMarket[EB/OL]. [2024-07-18]. <https://github.com/JoinMarket-Org/joinmarket-clientserver>.
- [23] MAURER F K, NEUDECKER T, FLORIAN M. Anonymous CoinJoin transactions with arbitrary values[C]//Proceedings of the IEEE Trustcom/BigDataSE/ICSS. Washington D. C., USA: IEEE Press, 2017: 522-529.
- [24] Wasabi Wallet [EB/OL]. [2024-07-18]. <https://wasabiwallet.io/>.
- [25] Samourai Wallet [EB/OL]. [2024-07-18]. <https://samouraiwallet.com/>.
- [26] HOUY S, SCHMID P, BARTEL A. Security aspects of cryptocurrency wallets—a systematic literature review[J]. ACM Computing Surveys, 2024, 56(1): 1-31.
- [27] LIU J K. Ring signature[M]//LI K C, CHEN X, SUSILO W. Advances in cyber security: principles, techniques, and applications. Singapore: Springer, 2018: 93-114.
- [28] CAO T, YU J S, DECOUCHANT J, et al. Exploring the Monero peer-to-peer network [M] // BONNEAU J, HENINGER N. Financial cryptography and data security. Berlin, Germany: Springer, 2020: 578-594.
- [29] SUN S F, AU M H, LIU J K, et al. RingCT 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero [C] // Proceedings of ESORICS' 17. Berlin, Germany: Springer, 2017: 456-474.
- [30] LI Y N, YANG G M, SUSILO W, et al. Traceable monero: anonymous cryptocurrency with enhanced accountability[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 679-691.
- [31] SUN X Q, YU F R, ZHANG P, et al. A survey on zero-knowledge proof in blockchain[J]. IEEE Network, 2021, 35(4): 198-205.
- [32] KAPPOS G, YOUSAF H, MALLER M, et al. An empirical analysis of anonymity in Zcash[C]//Proceedings of the 27th USENIX Security Symposium. New York, USA: ACM Press, 2018: 463-477.
- [33] YOUN M, CHIN K, OMOTE K. Empirical analysis of cryptocurrency mixer: Tornado Cash [C] // Proceedings of the Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE). Washington D. C., USA: IEEE Press, 2024: 2324-2331.
- [34] OU W, HUANG S Y, ZHENG J J, et al. An overview on cross-chain: mechanism, platforms, challenges and advances[J]. Computer Networks, 2022, 218: 109378.
- [35] ShapeShift[EB/OL]. [2024-07-18]. <https://app.shapeshift.com>.
- [36] changenow.io[EB/OL]. [2024-07-18]. <https://changenow.io/>.
- [37] 陈艳姣, 朱笑天, 于永瑞, 等. 区块链闪电网络实证分析: 拓扑、发展和收费策略[J]. 软件学报, 2022, 33(10): 3858-3873.
- CHEN Y J, ZHU X T, YU Y R, et al. Empirical analysis of lightning network: topology, evolution, and fees[J]. Journal of Software, 2022, 33(10): 3858-3873. (in Chinese)
- [38] DIVAKARUNI A, ZIMMERMAN P. The lightning network: turning Bitcoin into money[J]. Finance Research Letters, 2023, 52: 103480.
- [39] ALSABAH M, GOLDBERG I. Performance and security improvements for tor: a survey [J]. ACM Computing Surveys, 2017, 49(2): 1-36.
- [40] DASGUPTA D, SHREIN J M, GUPTA K D. A survey of blockchain from security perspective[J]. Journal of Banking and Financial Technology, 2019, 3(1): 1-17.
- [41] RAIKWAR M, GLIGOROSKI D. DoS attacks on blockchain ecosystem [C] // Proceedings of Parallel Processing Workshops. Berlin, Germany: Springer, 2022: 230-242.
- [42] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: an untrusted Bitcoin-compatible anonymous payment hub [C] // Proceedings of 2017 Network and Distributed System Security Symposium. San Diego, USA: Internet Society, 2017: 1-12.
- [43] BARAVALLE A, LEE S W. Dark Web markets: turning the lights on AlphaBay [C] // Proceedings of WISE' 18. Berlin, Germany: Springer, 2018: 502-514.
- [44] Bitcoin Fog [EB/OL]. [2024-07-18]. <https://bitcoinfo.info/>.
- [45] CoinMixer[EB/OL]. [2024-07-18]. <https://coinmixer.app/index.htm>.
- [46] BestMixer[EB/OL]. [2024-07-18]. <https://bestmixer.io>.
- [47] CryptoMixer[EB/OL]. [2024-07-18]. <https://cryptomixer.io>.
- [48] BONNEAU J, NARAYANAN A, MILLER A, et al. MixCoin: anonymity for Bitcoin with accountable mixes[M] // CHRISTIN N, SAFARI-NAINI R. Financial cryptography and data security. Berlin, Germany: Springer, 2014: 486-504.
- [49] BitLaundry[EB/OL]. [2024-07-18]. <https://bitcoinlaundry.net/>.
- [50] MixTum[EB/OL]. [2024-07-18]. <https://mixtum.io/>.
- [51] BitLaunder[EB/OL]. [2024-07-18]. <https://whir.to/?ref=rs1aalji>.
- [52] VALENTA L, ROWAN B. BlindCoin: blinded, accountable mixes for Bitcoin [M] // BRENNER M, CHRISTIN N, JOHNSON B, et al. Financial cryptography and data security. Berlin, Germany: Springer, 2015: 112-126.
- [53] IBRAHIM M H. SecureCoin: a robust secure and efficient protocol for anonymous Bitcoin ecosystem[J]. International Journal of Network Security, 2017, 19(2): 295-312.
- [54] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for Bitcoin [C] // Proceedings of the 13th Workshop on Privacy in the Electronic Society. New York, USA: ACM Press, 2014: 149-158.
- [55] ChipMixer[EB/OL]. [2024-07-18]. <https://chipmixer.com>.
- [56] Tornado Cash [EB/OL]. [2024-07-18]. <https://tornadoeth.cash/>.
- [57] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: secure multi-party mixing of Bitcoins [C] // Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. New York, USA: ACM Press, 2015: 75-86.
- [58] CoinJoin[EB/OL]. [2024-07-18]. <https://coinjoin.io>.
- [59] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[C]//Proceedings of ESORICS' 14. Berlin, Germany: Springer, 2014: 345-364.
- [60] Chainalysis-crypto-crime-2024[EB/OL]. [2024-07-18]. <https://go.chainalysis.com/crypto-crime-2024.html>.
- [61] Indictment charges two in \$230 million cryptocurrency scam[EB/OL]. [2024-07-18]. <https://www.justice.gov/usao-dc/pr/indictment-charges-two-230-million-cryptocurrency-scam>.
- [62] Individual arrested and charged with operating notorious darknet cryptocurrency "Mixer" [EB/OL]. [2024-07-18]. <https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer>.
- [63] Ohio resident pleads guilty to operating darknet-based Bitcoin 'Mixer' that laundered over \$300 million [EB/OL].

- OL]. [2024-07-18]. <https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million>.
- [64] U.S. treasury issues first-ever sanctions on a virtual currency mixer, targets dprk cyber threats [EB/OL]. [2024-07-18]. <https://home.treasury.gov/news/press-releases/jy0768>.
- [65] U.S. treasury sanctions notorious virtual currency mixer tornado cash [EB/OL]. [2024-07-18]. <https://home.treasury.gov/news/press-releases/jy0916>.
- [66] Justice department investigation leads to takedown of darknet cryptocurrency mixer that processed over \$ 3 billion of unlawful transactions [EB/OL]. [2024-07-18]. <https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3>.
- [67] U.S. sanctions crypto mixer sinbad.io for role in North Korean laundering activities [EB/OL]. [2024-07-18]. <https://www.chainalysis.com/blog/crypto-mixer-sinbad-sactioned-north-korean-laundering/>.
- [68] Bitcoin Fog operator convicted of money laundering conspiracy [EB/OL]. [2024-07-18]. <https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy>.
- [69] Founders and CEO of cryptocurrency mixing service arrested and charged with money laundering and unlicensed money transmitting offenses [EB/OL]. [2024-07-18]. <https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering>.
- [70] HOLT T J, LEE J R, GRIFFITH E. An assessment of cryptomixing services in online illicit markets[J]. *Journal of Contemporary Criminal Justice*, 2023, 39(2): 222-238.
- [71] MÖSER M, BÖHME R, BREUKER D. An inquiry into money laundering tools in the Bitcoin ecosystem [C] // *Proceedings of the APWG eCrime Researchers Summit*. Washington D.C., USA: IEEE Press, 2014: 1-14.
- [72] DE BALTHASAR T, HERNANDEZ-CASTRO J. An analysis of Bitcoin laundry services [M] // LIPMAA H, MITROKOTSA A, MATULEVIČIUS R. *Secure IT systems*. Berlin, Germany: Springer, 2017: 297-312.
- [73] MIEDEMA F, LUBBERTSEN K, SCHRAMA V, et al. Mixed signals: analyzing ground-truth data on the users and economics of a Bitcoin mixing service [C] // *Proceedings of the 32nd USENIX Security Symposium*. New York, USA: ACM Press, 2023: 751-768.
- [74] STOCKINGER J. Analysis of decentralized mixing services in the greater Bitcoin ecosystem [J]. *The Journal of the British Blockchain Association*, 2020, 3(2): 1-15.
- [75] SCHNOERING H, VAZIRGIANNIS M. Heuristics for detecting CoinJoin transactions on the Bitcoin blockchain [EB/OL]. [2024-07-18]. <https://arxiv.org/abs/2311.12491>.
- [76] CONTI M, GANGWAL A, RUJ S. On the economic significance of ransomware campaigns: a Bitcoin transactions perspective [J]. *Computers & Security*, 2018, 79: 162-189.
- [77] MAKUTOV 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 the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. Washington D.C., USA: IEEE Press, 2019: 274-277.
- [78] TIRONSAKKUL T, MAAREK M, EROSS A, et al. The unique dressing of transactions: Wasabi CoinJoin transaction detection [C] // *Proceedings of the European Interdisciplinary Cybersecurity Conference*. New York, USA: ACM Press, 2022: 21-28.
- [79] SHOJAEENASAB A, MOTAMED A P, BAHRAK B. Mixing detection on Bitcoin transactions using statistical patterns [EB/OL]. [2024-07-18]. <https://arxiv.org/abs/2204.02019>.
- [80] 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.
- 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. (in Chinese)
- [81] HONG Y, KWON H, LEE J, et al. A practical de-mixing algorithm for Bitcoin mixing services [C] // *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*. New York, USA: ACM Press, 2018: 15-20.
- [82] TANG Y J, XU C, ZHANG C, et al. Analysis of address linkability in tornado cash on Ethereum [M] // LU W, ZHANG Y, WEN W, et al. *Communication in computer and information science*. Singapore: Springer, 2022: 39-50.
- [83] WU M K, MCTIGHE W, WANG K L, et al. Tutela: an open-source tool for assessing user-privacy on Ethereum and tornado cash [EB/OL]. [2024-07-18]. <https://arxiv.org/abs/2201.06811>.
- [84] WU L, HU Y F, ZHOU Y J, et al. Towards understanding and demystifying Bitcoin mixing services [C] // *Proceedings of the Web Conference 2021*. New York, USA: ACM Press, 2021: 33-44.
- [85] HONG Y, KWON H, LEE S, et al. Poster: de-mixing Bitcoin mixing services [C] // *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*. New York, USA: ACM Press, 2018: 15-20.
- [86] YOUSAF H, KAPPOS G, MEIKLEJOHN S. Tracing transactions across cryptocurrency ledgers [EB/OL]. [2024-07-18]. <https://arxiv.org/abs/1810.12786>.
- [87] BÉRES F, SERES I A, BENCZÚR A A, et al. Blockchain is watching you: profiling and deanonymizing Ethereum users [C] // *Proceedings of the IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Washington D.C., USA: IEEE Press, 2021: 69-78.
- [88] 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*. New York, USA: ACM Press, 2013: 127-140.
- [89] SQUAREPANTS S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2024-07-18]. <http://dx.doi.org/10.2139/ssrn.3440802>.
- [90] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin [M] // SADEGHI A R. *Financial cryptography and data security*. Berlin, Germany: Springer, 2013: 34-51.
- [91] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system [C] // *Proceedings of the IEEE 3rd International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. Washington D.C., USA: IEEE Press, 2012: 1318-1326.
- [92] ZHANG Y H, WANG J, LUO J. Heuristic-based address clustering in Bitcoin [J]. *IEEE Access*, 2020, 8: 210582-210591.

- [93] HE X, HE K T, LIN S W, et al. Bitcoin address clustering method based on multiple heuristic conditions [J]. *IET Blockchain*, 2022, 2(2): 44-56.
- [94] LIU F, LI Z H, JIA K, et al. Bitcoin address clustering based on change address improvement [J]. *IEEE Transactions on Computational Social Systems*, 2024, 11(6): 8094-8105.
- [95] VICTOR F. Address clustering heuristics for Ethereum[M]//BONNEAU J, HENINGER N. *Financial cryptography and data security*. Berlin, Germany: Springer, 2020: 617-633.
- [96] WAHRSTÄTTER A, GOMES J, KHAN S, et al. Improving cryptocurrency crime detection: CoinJoin community detection approach [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023, 20(6): 4946-4956.
- [97] WAHRSTÄTTER A, TAUDS A, SVETINOVIC D. Reducing privacy of CoinJoin transactions: quantitative Bitcoin network analysis [J]. *IEEE Transactions on Dependable and Secure Computing*, 2024, 21(5): 4543-4558.
- [98] REMY C, RYMB, MATTHIEU L. Tracking Bitcoin users activity using community detection on a network of weak signals[M]//CHERIFI C, CHERIFI H, KARSAI M, et al. *Complex networks & their applications VI*. Berlin, Germany: Springer, 2017: 166-177.
- [99] SUN H Y, RUAN N, LIU H Q. Ethereum analysis via node clustering[M]//LIU J K, HUANG X. *Network and system security*. Berlin, Germany: Springer, 2019: 114-129.
- [100] 王天宇, 殷婷婷, 李赞, 等. BATscope: 比特币恶意地址及混币交易识别[J]. *信息安全学报*, 2023, 8(4): 1-16.
- WANG D Y, YIN T T, LI Y, et al. BATscope: identification of Bitcoin malicious addresses and mixing transactions[J]. *Journal of Information Security Research*, 2023, 8(4): 1-16. (in Chinese)
- [101] XU C, XIONG R T, SHEN X D, et al. How to find a Bitcoin mixer: a dual ensemble model for Bitcoin mixing service detection [J]. *IEEE Internet of Things Journal*, 2023, 10(19): 17220-17230.
- [102] PRADO-ROMERO M A, DOERR C, GAGO-ALONSO A. Discovering Bitcoin mixing using anomaly detection [M]//MENDOZA M, VELASTIN S. *Progress in pattern recognition, image analysis, computer vision, and applications*. Berlin, Germany: Springer, 2018: 534-541.
- [103] WU J J, LIU J L, CHEN W L, et al. Detecting mixing services via mining Bitcoin transaction network with hybrid motifs [J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, 52(4): 2237-2249.
- [104] RATHORE M M, CHAURASIA S, SHUKLA D. Mixers detection in Bitcoin network: a step towards detecting money laundering in crypto-currencies [C]//*Proceedings of the IEEE International Conference on Big Data*. Washington D.C., USA: IEEE Press, 2023: 5775-5782.
- [105] LIU M D, CHEN H, YAN J Q. Detecting roles of money laundering in Bitcoin mixing transactions: a goal modeling and mining framework[J]. *Frontiers in Physics*, 2021, 9: 665399.
- [106] DU H B, CHE Z, SHEN M, et al. Breaking the anonymity of Ethereum mixing services using graph feature learning [J]. *IEEE Transactions on Information Forensics and Security*, 2024, 19: 616-631.
- [107] STÜTZ 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*. New York, USA: ACM Press, 2022: 254-267.
- [108] NAN L H, TAO D C. Bitcoin mixing detection using deep autoencoder [C]//*Proceedings of the 3rd International Conference on Data Science in Cyberspace (DSC)*. Washington D.C., USA: IEEE Press, 2018: 280-287.
- [109] SUN X W, YANG T, HU B. LSTM-TC: Bitcoin coin mixing detection method with a high recall [J]. *Applied Intelligence*, 2022, 52(1): 780-793.
- [110] YANG H Z, LI Z Z, GOU G P, et al. Bitcoin mixing service detection based on spatio-temporal information representation of transaction graph [C]//*Proceedings of the IEEE International Performance, Computing, and Communications Conference (IPCCC)*. Washington D.C., USA: IEEE Press, 2023: 210-219.
- [111] YU L, ZHANG F J, MA J J, et al. Who are the money launderers? Money laundering detection on blockchain via mutual learning-based graph neural network [C]//*Proceedings of the International Joint Conference on Neural Networks (IJCNN)*. Washington D.C., USA: IEEE Press, 2023: 1-8.
- [112] LO W W, KULATILLEKE G K, SARHAN M, et al. Inspection-L: self-supervised GNN node embeddings for money laundering detection in Bitcoin [J]. *Applied Intelligence*, 2023, 53(16): 19406-19417.
- [113] ALARAB I, PRAKONWIT S, NACER M I. Comparative analysis using supervised learning methods for anti-money laundering in Bitcoin [C]//*Proceedings of the 5th International Conference on Machine Learning Technologies*. New York, USA: ACM Press, 2020: 11-17.
- [114] HYUN W, LEE J, SUH B. Anti-money laundering in cryptocurrency via multi-relational graph neural network [C]//*Proceedings of Advances in Knowledge Discovery and Data Mining*. Berlin, Germany: Springer, 2023: 118-130.
- [115] LORENZ J, SILVA M I, APARÍCIO D, et al. Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity [C]//*Proceedings of the 1st ACM International Conference on AI in Finance*. New York, USA: ACM Press, 2020: 1-8.
- [116] VASSALLO D, VELLA V, ELLUL J. Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies [J]. *SN Computer Science*, 2021, 2(3): 143.
- [117] TIRONSARKUL T, MAAREK M, EROSS A, et al. Tracking mixed Bitcoins [M]//GARCIA-ALFARO J, NAVARRO-ARRIBAS G, HERRERA-JOANCOMARTI J. *Data privacy management, cryptocurrencies and blockchain technology*. Berlin, Germany: Springer, 2020: 447-457.
- [118] TIRONSARKUL T, MAAREK M, EROSS A, et al. Context matters: methods for Bitcoin tracking [J]. *Forensic Science International: Digital Investigation*, 2022, 42: 301475.
- [119] WU J J, LIN D, FU Q S, et al. Toward understanding asset flows in crypto money laundering through the lenses of Ethereum heists [J]. *IEEE Transactions on Information Forensics and Security*, 2024, 19: 1994-2009.
- [120] WU Z Y, LIU J L, WU J J, et al. TRacer: scalable graph-based transaction tracing for account-based blockchain trading systems [J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 2609-2621.
- [121] ZHANG Z Y, YIN J Y, HU B, et al. CLTracer: a cross-ledger tracing framework based on address relationships [J]. *Computers & Security*, 2022, 113: 102558.
- [122] Chainanalysis Reactor [EB/OL]. [2024-07-18]. <https://>

app.chainalysis.com/login?redirect=reactor.

[123] Chainalysis Know Your Transaction (KYT) [EB/OL]. [2024-07-18]. <https://www.chainalysis.com/chainalysis-kyt-certification/>.

[124] Clain Probe [EB/OL]. [2024-07-18]. <https://clain.io/products/probe>.

[125] Elliptic crypto-wallet-monitoring [EB/OL]. [2024-07-18]. <https://www.elliptic.co/crypto-wallet-monitoring-screening-software>.

[126] MistTrack[EB/OL]. [2024-07-18]. <https://misttrack.io/>.

[127] CipherTrace[EB/OL]. [2024-07-18]. <https://home.ciphertrace.com/>.

[128] Crystal Blockchain [EB/OL]. [2024-07-18]. <https://crystalintelligence.com/>.

[129] Scorechain[EB/OL]. [2024-07-18]. <https://www.scorechain.com/>.

[130] TRM Labs [EB/OL]. [2024-07-18]. <https://www.trmlabs.com/>.

[131] QIUE[EB/OL]. [2024-07-18]. <https://blockchaingroup.io/qiue/>.

文字编辑 陆燕菲
栏目编辑 宋 圆

计算机工程
www.ecice06.com