

区块链混币技术新进展与挑战

张 孝 张晓璇 杨子涵 李沛谦 陈晋川

(中国人民大学信息学院 北京 100872)

摘 要 区块链中所有交易数据均记录在公开账本上,可能导致用户交易隐私泄露。为了增强交易匿名性,可以采用区块链混币来解耦交易输入与输出之间的关联。然而,混币在提升用户隐私保护程度的同时,也存在被非法交易活动利用的风险。2021年以来,区块链混币生态呈现出显著的范式转型,已突破早期单一追求匿名的传统范式,迈入系统隐私与鲁棒性增强、个性化隐私定制、监管合规设计以及跨领域应用拓展的多目标新阶段。本文系统分析了区块链混币技术演进路径,首次提出了区块链混币三层分类体系,并基于此体系揭示了密码学原语对交易隐私保护的不同作用。重点讨论了2021年以来混币生态在多目标阶段的四个主要方向上的新进展,以及在技术与监管层面所面临的挑战。最后,讨论了兼顾监管需求和隐私保护的区块链混币发展方向和技术路径。

关键词 区块链;混币;隐私保护;密码学原语;监管合规

中图法分类号 TP309

DOI号 10.11897/SP.J.1016.2026.02151

Emerging Trends and Challenges in Blockchain Coin Mixing

ZHANG Xiao ZHANG Xiao-Xuan YANG Zi-Han LI Pei-Qian CHEN Jin-Chuan

(School of Information, Renmin University of China, Beijing 100872)

Abstract All transaction data in blockchain systems are recorded on a public ledger, which may lead to the exposure of users' transaction privacy. To enhance transaction anonymity, blockchain Coin Mixing can be employed to decouple the association between transaction inputs and outputs. While improving the effectiveness of user privacy protection, Coin Mixing inherently carries risks of being exploited for illicit activities. Since 2021, the blockchain Coin Mixing ecosystem has exhibited a significant paradigm shift, transcending the early traditional paradigm of solely pursuing anonymity and entering a new multi-objective stage of system privacy and robustness enhancement, regulatory compliance design, privacy customization, and cross-domain application expansion. This paper systematically analyzes the evolutionary trajectory of blockchain Coin Mixing. For the first time, we propose to distinguish between two basic models—Combination-based and Relay-based—and further construct a three-layer classification framework encompassing these two categories. Combination-based Coin Mixing focuses on the structural fusion of transactions to break associations, while Relay-based Coin Mixing emphasizes the use of smart contracts or mixing intermediaries to break temporal correlations. Based on this framework, this paper analyzes the differentiated impacts of various cryptographic primitives on privacy protection from three dimensions: masking external observers, masking participants, and masking intermediaries. Re-

收稿日期:2025-06-11;在线发布日期:2026-05-11。本课题得到教育部中央高校青年教师科研创新能力支持项目(No. SRICSPYF-ZY2025001)、国家自然科学基金联合基金项目(No. U24B20144)、国家重点研发计划重点专项课题(No. 2022YFB2702102)资助。

张 孝,博士,教授,中国计算机学会(CCF)会员,主要研究领域为数据库体系结构、大数据管理与分析、数据基准测评、区块链。E-mail: zhangxiao@ruc.edu.cn。张晓璇,博士研究生,主要研究领域为区块链、区块链隐私保护。杨子涵,硕士研究生,主要研究领域为区块链隐私保护。李沛谦,硕士研究生,主要研究领域为区块链隐私保护。陈晋川(通信作者),博士,教授,中国计算机学会(CCF)会员,主要研究领域为分布式数据管理、区块链。E-mail: jchen@ruc.edu.cn。

search indicates that masking external observers primarily relies on techniques such as ring signatures and zero-knowledge proofs; masking participants is more common in Combination-based Coin Mixing, achieved through decryption mixing networks and multi-round mixing; and masking intermediaries often utilizes blind signatures and multi-intermediary architectures. Furthermore, this paper explores in depth the four main directions defining the current multi-objective stage and highlights their common evolutionary characteristics. First, system privacy and robustness enhancement schemes focus on improving privacy strength within existing blockchain architectures, achieving forward secrecy and severing transaction links without introducing external trust assumptions, thereby resisting sophisticated de-anonymization threats while expanding the anonymity set. Second, regulatory compliance design represents a proactive shift where protocols reserve audit interfaces or traceability means at the beginning of their design. These schemes aim to meet individual privacy expectations while responding to anti-money laundering and sanctions compliance requirements through selective disclosure or trusted regulation. Third, personalized privacy customization signifies a transition from fixed system parameters to user-centric privacy services, granting users the right to autonomously configure anonymity levels and transaction timing to improve overall user experience and acceptance. Fourth, cross-domain application expansion indicates that the core de-association concept of Coin Mixing is evolving into a general-purpose tool for privacy computing. This paper conducts a comprehensive assessment of the challenges brought by illicit transaction exploitation, the evolution of de-anonymization techniques, and changes in regulatory systems. Based on these challenges, we explore development goals centered on enhancing privacy, improving services, and achieving regulatory compliance. We propose two technical pathways: constructing a hardware-independent full-process regulatory system covering ex-ante compliance checks, in-process behavior monitoring, and ex-post auditable accountability; and hardware-assisted solutions using Trusted Execution Environments to process raw transaction data, combined with side-channel protection and hierarchical auditing mechanisms. We also emphasize the necessity of adopting post-quantum cryptography to address emerging threats such as Shor's algorithm. Finally, this paper summarizes the paradigm evolution of the Coin Mixing ecosystem and provides a reference for designing Coin Mixing schemes that reconcile regulatory requirements with user privacy.

Keywords Blockchain; Coin Mixing; privacy protection; cryptographic primitives; regulatory

1 引 言

区块链又称分布式账本,是加密数字货币的底层基础设施,基于分布式共识协议和密码学技术,在一个去中心、去信任的环境中可靠记录用户的交易。在比特币、以太坊等公有链^①中,用户以匿名身份参与,链上只记录账户地址,不暴露用户在物理世界的真实身份。然而交易金额、时间戳、输入地址、输出地址等交易细节,均会被记录在链上公开可见。攻击者有可能通过启发式方法或机器学习等链上追踪技术^[1-5]发现账户地址之间的关联,在一定程度上威胁用户隐私。

为了应对这个问题,区块链社区提出了混币(Coin Mixing),目的是屏蔽交易中输入地址和输出地址的关联,从而隐藏资金流动路径,为用户提供交易隐私保护服务。区块链混币的基本原理是将一个交易的信息和多个其他交易混杂在一起,使得外部观察者不能识别交易中输入地址和输出地址之间的对应关系。

例 1. 如图 1 所示,假设 Alice 需要向 Bob 转账 0.1BTC。在常规交易中,链上记录会直接显示 Alice 向 Bob 转账 0.1BTC 的交易细节。然而若采用

^① 本文主要讨论公有链,因为联盟链的用户都需要明确身份,没有匿名化需求。

混币技术, Alice 可与另一用户 Carey 合作(后者向 David 转账 0.1BTC), 通过混币技术将两笔交易合并。如图 1 右侧所示, 经过这种处理, 外部观察者仅能看到 Alice 和 Carey 共同向 David、Bob 发起多输入多输出交易, 既无法确认 Alice 的资金流向是 Bob 还是 David, 也无法判断 Carey 的收款方归属, 从而掩盖真实交易关系。

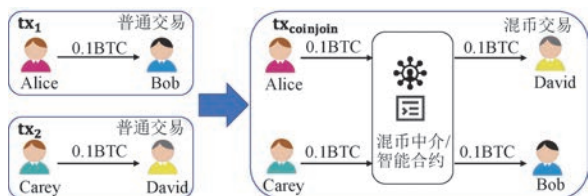


图 1 混币交易示例

第一个区块链混币技术 CoinJoin 由比特币核心开发者 Gregory Maxwell 在 2013 年提出^[6]。在过去十多年间, 涌现出数十种混币技术。通过系统分析混币技术的演进脉络, 我们发现其发展轨迹与用户需求的层次化演进存在显著的正相关关系。对应地, 技术演进路径也可划分为四个特征鲜明的阶段, 各阶段分别对应不同层次的需求迭代(见第 6 节)。

值得注意的是, 2021 年后区块链混币呈现出显著的范式转型特征。相较于 2021 年之前几乎完全聚焦于单一匿名性增强的研究范式, 新一代技术开始向兼顾多种需求的多目标体系演进。从数据来看, 在近年涌现的代表性方案中, 仅有 31% 的研究持续聚焦于底层架构以增强隐私与鲁棒性^[7-10]; 而绝大多数方案则致力于打破传统框架, 向多元化需求发散。具体而言, 包括主动引入审计机制以平衡隐私与监管要求(31%)^[11-14]、提供参数可定制个性化匿名服务(23%)^[15-17], 以及将混币机制拓展至医疗或数字交易等跨领域应用场景(15%)^[18-19]。

监管兼容性混币技术的出现, 说明混币运营者意识到: 健康发展的区块链混币需要和监管机构相向而行。RBSmix^[13]引入监管角色, 采用用户身份信息加密分片存储、多方验证及盲化处理确保隐私, 在执法机构请求时由监管成员协作解密分片追踪非法交易。Railgun^[11]通过链上反洗钱筛查拦截黑名单资金并强制退回, 同时在提现时生成加密的“无罪证明”供监管机构验证资金合法性。

切换到混币监管视角, 我们可以发现, 近年来监管层从技术和司法两方面增强了对区块链混币的管控。技术层面, 越来越多机器学习和深度学习手段被用来实现“混币去匿名”。包括启发式方法^[20-24]、

深度学习^[25-28]、机器学习^[29-30]等技术, 重构参与混币交易的账户地址之间的关联, 在一定程度上削弱了混币的隐私保护效果。司法层面, 多位混币系统的运营者受到监管机构警告, 甚至被逮捕入狱。可以想见, 区块链混币如果一味只追求交易隐私保护, 忽视监管层的要求, 继续充当非法交易的帮凶, 那迟早会成为重点打击对象并逐渐被压缩生存空间。

现有的关于区块链混币的综述所覆盖的内容基本都是在 2021 年之前^[31-33]。虽然部分综述^[34-35]涵盖了少量 2021 年之后的混币技术, 但是并没有讨论混币生态和混币技术的最新发展趋势, 也没有分析区块链混币系统面临的挑战。

此外, 现有的混币综述工作对混币技术的分类相对简单, 通常按中心化和去中心化分为两类^[32-35], 或者按使用的密码学技术分为多类^[31-35]。单纯按中心和去中心来分类过于简单, 难以清晰展示不同类型混币技术的实现思路和技术演进路径。采用混币使用的密码学技术来分类虽然细化了类别, 但是密码学技术是底层的实现机制, 而不是上层应用形态, 因此采用密码学技术分类并不直观。比如同样使用环签名, CoinMingle^[36]是将多个交易聚合在一起保护隐私, DCmix^[8]则是将原始交易拆分为两个交易, 借助托管地址转发实现交易匿名化。两者的服务形式差异明显, 划入同一类别非常牵强。

本文首次提出将混币技术分为合并型和中转型两种。合并型混币通过将多个交易合并为多对多交易实现, 中转型混币则是将单一交易拆分为两个看似无关联的交易。两类混币在表现形式上差异显著, 采用的技术也存在本质区别。

在此基础上, 本文进一步提出三层分类体系, 按如何实现合并以及如何实现中转型形成第二层分类, 最后再按是否存在中心节点进行第三层分类。通过层次化细粒度的分类目录, 不但有利于对混币技术的发展进行梳理, 而且还使得密码学原语在分类树上自然形成聚集, 从而为进一步分析密码学原语在混币技术隐私保护中的作用奠定了基础。

本文主要贡献包括:

(1) 系统梳理了混币技术及其发展趋势, 聚焦近五年区块链混币生态的新进展, 指出其发展已发生显著的范式转型: 从单一注重隐私保护, 拓展至多元化服务, 特别是监管兼容性。

(2) 首次提出明确区分合并型和中转型两个区块链混币模型, 进一步构建包含这两类模型的三层分类体系, 并基于此体系清晰展示混币技术的发展趋势。

(3)系统地剖析了不同密码学原语在混币技术隐私保护中的差异化作用机制,聚焦三重维度:屏蔽参与者、屏蔽中介及屏蔽外部观察者。

(4)讨论了区块链混币面临的三大挑战,指出未来区块链混币发展的方向,并提出一个平衡监管需求和隐私保护要求的区块链混币技术路线。

本文后续章节的组织架构如下:第2节系统梳理区块链混币技术相关研究,重点指出现有综述工作的局限性,并阐述混币技术涉及的密码学基础;第3节提出混币的三层分类体系,通过合并型-中转型基础模型分类混币,并对密码学原语的应用进行分析;第4节与第5节分别针对合并型和中转型混币展开介绍,通过技术分析与应用系统及其实例(如Wasabi Wallet、Tornado Cash等案例)揭示其技术特征;第6节系统归纳混币技术发展的四阶段演进规律,重点剖析2021年后的混币特征;第7节从非法交易、监管技术、制度约束三个维度论述核心挑战并提出平衡监管需求与隐私保护要求的区块链混币技术路线;最后第8节总结研究贡献。

2 相关工作与背景知识

本节首先介绍之前有关区块链混币技术的综述工作(2.1节),并和本文工作进行对比。之后将介绍区块链混币技术所使用的主要密码学原语(2.2节),包括混洗、盲签名、环签名等,这些技术将用于隐藏区块链交易中输入和输出之间的关联。

2.1 区块链混币技术综述

由于早期的区块链交易主要集中在比特币,因此很多关于区块链混币技术的综述也聚焦于比特币。Simin Ghesmati等人对基于比特币平台的混币技术进行整理分析^[31],将区块链混币技术分为中心化混币、基于原子交换的混币、基于CoinJoin的混币与基于阈值签名的混币四类,并从隐私、安全和效率三方面进行了对比分析。Jaswant Pakki等人的工作同样只分析了基于比特币平台的混币技术^[32],分为学术界的混币技术(Academic Mixing Techniques)和公共混币服务(Public Mixing Services),认为公共混币服务并未发展出原创性技术突破,其核心机制本质上是对传统混币模式的工程改良,而非技术革新。然而,随着混币生态的不断发展,现在已有很多原创混币技术来自工业界,比如Tornado Cash^[37],门罗币(Monero)^[38]等。因此,本文在梳理混币技术时不再特意区分学术界和工业

界。具体而言,在第4节和第5节中,我们将先介绍原创的混币技术,然后介绍采用这些技术的混币应用系统。

随着以太坊的兴起,涌现出很多基于以太坊平台的混币技术,在部分综述工作^[33-34]中,均包括了基于比特币和以太坊的混币技术。Giannikou等人^[33]将区块链混币技术分为中心化和去中心化两类,讨论了Mixcoin、Blindcoin、CoinJoin等混币技术的工作原理,分析了它们的安全性,但是这篇文章覆盖面比较窄(只覆盖了不到20%的混币技术),并且也没有分析实际混币系统的运行状况。Alireza Arbabi等人的工作^[34]也是按学术界和工业界来分别介绍混币技术,认为学术研究以去中心化为核心理念,致力于通过技术手段降低中心化监管,强调隐私保护与抗审查性,但技术复杂度较高。而工业界的混币技术普遍采用简单聚合再分配的模式,技术门槛低、实施便捷,侧重操作可行性与成本效益的平衡。

与Arbabi等人的工作^[34]相比,本文工作不仅仅讨论了比特币和以太坊平台上的混币技术,也会覆盖Monero、Dash等区块链系统。此外,我们也增加了对2021年之后涌现出来的混币技术的分析比较,并首次梳理了混币技术的发展脉络。最近的工作^[35]主要讨论了有关混币的监管技术,同时介绍了少量混币技术,涵盖比特币、以太坊以及少量跨链混币系统,但对Dash、Monero等其他独立平台并未涉及。

如表1所示,本文对区块链混币技术和实际运行的区块链混币应用系统进行了全面梳理,覆盖了比特币、以太坊、Monero、Dash等主流区块链平台。在分类体系方面,首次提出区分“合并型”和“中转型”,并由此将混币技术的分类体系扩展到三层。此外,本文还分析了区块链混币技术的演变过程,重点讨论了近五年来区块链混币产业的新动向,并分析其对监管带来的挑战,展望了区块链混币技术未来的发展趋势。

表1 混币相关综述对比

综述工作	平台	技术分类 体系	覆盖的技术/ 系统数
Simin Ghesmat 等人 ^[31]	比特币	1 层	44
Jaswant Pakk 等人 ^[32]	比特币	1 层	29
I Giannikou 等人 ^[33]	比特币和以太坊	1 层	8
Alireza Arbabi 等人 ^[34]	比特币和以太坊	1 层	31
本文	比特币、以太坊、 门罗币、Dash、跨链	3 层	62

2.2 混币技术涉及的密码学原语

区块链混币的核心目标是隐藏原始交易中输入和输出之间的关联,且隐藏关联之后的交易还需要能够在区块链平台上执行。已有的区块链混币技术主要通过密码学技术来实现上述目的,包括混洗、盲签名、环签名和零知识证明等,下面我们将逐一予以介绍。

2.2.1 混 洗

混洗(Shuffle),也称为洗牌,通过将多个数据对打乱再重新输出,使得外部观察者不能定位原始数据对中的关联关系。在洗牌差分隐私模型(Shuffle Model Differential Privacy)^[39]中,混洗技术通过随机排序切断用户身份与输出结果之间的关联,从而有效提供隐私保护。在区块链混币中,混洗是最重要的保护交易隐私的方法之一,常用于将多个区块链交易合并在一起并打乱,使得外界不能观察到原始交易的输入和输出之间的关联。比如,Coin-Shuffle^[40]和 CoinParty^[41]中,采用混洗技术将用户的输出加密后打乱,以切断原始交易的输入与输出之间的关联。

2.2.2 盲签名

盲签名(Blind Signature)是由 Chaum^[42]提出的密码学原语,它通过独特的签名过程实现隐私保护:消息发送者首先使用盲化因子对原始消息进行盲化,从而隐藏原始消息内容;签名者对盲化后的消息进行签名而不获知实际内容;最后发送者去盲化获得对原始消息的有效签名。这一机制保证了签名者在无法知晓消息内容的情况下完成签名。不同的密码学方案可实现盲签名,包括基于 RSA^[43]、BLS^[44]、Schnorr^[45]等算法的实现。

在电子投票系统中,选民匿名获取一个唯一的序列号,并对序列号进行盲化,交由官方机构对盲化后的序列号进行签名。选民对签名进行去盲化后得到官方对序列号的签名。签名与序列号共同组成选民的资格证,选民可凭借资格证进行投票。通过盲签名,既保证了选民身份可信,又切断了选民身份与其投票之间的关联,保护其隐私^[46]。很多区块链混币中需要第三方服务商对原始交易进行签名,此时可以通过盲签名来隐藏原始交易中隐私信息。例如 Blindcoin^[47]、Blind-Mixing^[48]、TumbleBit^[49],都使用盲签名技术来避免混币中介知晓输入输出关联。

2.2.3 环签名

环签名(Ring Signature)^[50]允许签名者使用自己的私钥以及包括自己的公钥在内的多个公钥进行

签名。这种签名方式将签名者的公钥隐藏在公钥集合中,以隐藏其身份信息。验证者可以通过签名以及对应的公钥集合来确认签名的有效性,但无法识别出签名者的公钥。

在电子投票系统中,可采用环签名技术,允许群组成员代表整个群体生成有效签名^[51]。该方法不仅满足投票结果的可验证性要求,同时通过签名者身份匿名机制实现强隐私保护。在车载自组织网络领域,通过环签名技术可以实现车辆节点在隐匿真实身份的前提下对消息进行匿名签名^[52]。该机制既可以通过密码学验证确保消息来源的可信性、有效抵御虚假消息注入攻击,还能确保攻击者无法通过签名信息反推车辆身份。

环签名技术为区块链混币也提供了关键技术支撑。门罗币(Monero)^[38]通过将签名者的公钥隐匿于预定义的环境成员集合中,增强了交易图的不可链接性,使得外部观察者无法追溯交易发起方。Coin-Mingle^[36]通过构建动态环结构实现交易输出信息的混淆,将环签名与零知识证明相结合,在保证交易有效性的同时达到更强的匿名性保障。

2.2.4 隐匿地址

隐匿地址(Stealth Address)是一种由交易双方共同生成的一次性地址,每次交易时,发送方利用接收方的公钥和随机数生成一个唯一的一次性地址,资金被转入该地址。只有接收方能通过私钥识别并控制该地址的资产。

其中用户拥有两对密钥,分别是支付密钥与查看密钥。支付密钥用于签名交易,查看密钥用于生成隐匿地址。隐匿地址的生成公式为 $P = H(rA)G + B$ 。其中 r 为随机数, A 为接收方的查看公钥, B 为接收方的支付公钥。接收方可在区块链中寻找属于自己的交易,使用支付私钥即可计算对应的隐匿地址。

在 Monero^[38]中,支付方将资金发送到接收方的隐匿地址中,防止攻击者将地址与真实的用户身份相关联,且在每次接收资金时都会生成新的隐匿地址,即使同一用户多次收款,链上数据仅显示无关联的地址序列。

2.2.5 零知识证明

零知识证明(Zero Knowledge Proof, ZKP)^[53]是一种密码学技术,允许证明者在不泄露某消息具体内容的前提下,向验证者证明自己知道该消息。这种证明过程确保信息的保密性,同时验证者能够确信证明者拥有相关知识,而无法获取其他细节。

在混币技术中,应用较为广泛的零知识证明变体是零知识简洁非交互式知识论证(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, zk-SNARK)^[54]。该技术具备三个关键特点:首先,它是非交互式的,证明者与验证者之间仅需一次通信即可完成证明;其次,具有简洁性,生成的证明尺寸小且验证速度极快;最后,它具有论证性,满足计算可靠性的严格要求。

零知识证明可以解决电子投票系统的局限性^[55],例如篡改或侵犯选民隐私。在选举中,维护投票过程的完整性对于保持民主原则至关重要。使用非交互式零知识论证的电子投票系统提供了一种安全的方法来验证选票,同时保证选民匿名。

Tornado Cash^[37]通过 zk-SNARK 使智能合约可以验证票据所有权:用户可以证明他们拥有对对应存款金额的票据,而不需要透露他们的身份或存款的具体细节。

2.2.6 匿名通信网络

匿名通信网络(Anonymous Communication Networks, ACNs)是一类旨在保护用户隐私和隐藏通信关系的网络技术,通过加密、路由混淆或消息混合等手段,防止外部观察者追踪用户的身份或通信内容。其中, Tor 网络(The Onion Router)^[56]和解密混合网络(decryption mixnets)^[57]是两种典型的匿名网络技术。

Tor 网络基于洋葱路由技术,通过多层加密和动态路由转发,隐藏用户 IP 地址。Blind-Mixing^[58]运行在 Tor 网络上,加密用户与混币中介之间的通信数据,隐藏用户的真实 IP 地址,同时也防止混币中介通过用户真实的 IP 地址发现存款交易与取款交易之间的关联。Monero 同样使用 Tor 网络隐藏用户真实的 IP 地址,使交易无法直接与用户身份相关联。

解密混合网络(Decryption mixnets)^[57]通过多个混合节点共同进行加密-解密过程实现消息匿名传递:发送者首先使用混合节点的公钥对消息进行多层嵌套加密;每个混合节点依次用私钥剥离一层加密并对消息顺序随机重排;最终经过所有节点的顺序混淆和层层解密后,原始消息被匿名传递到接收端。这种方式确保任何单一节点都无法关联输入与输出消息,从而切断消息发送者与消息之间的关联。

在 CoinShuffle^[40]中,混币参与者同时扮演混合节点的角色,对交易输出地址进行层层加密并随机

打乱顺序,以切断交易输入方与输出方之间的关联。CoinParty^[41]相较于 CoinShuffle 引入了混合对等体,由混合对等体对输出地址进行加密并打乱,切断交易输入输出之间的关联。

2.2.7 多重签名

多重签名技术(Multi-signature)是一种基于公钥密码学的分布式授权机制,其核心特征在于要求多个实体共同参与才能完成数字签名验证。该技术采用 $m-of-n$ 阈值结构,规定在预设的 n 个签名者中至少需要 m 个有效签名($m \leq n$)才能生成合法签名,通过分散签名权的设计模式实现风险共担与权限约束。该技术已广泛应用于加密货币交易(如比特币多重签名钱包)、智能合约执行等场景,显著提升了数字资产管理的安全性。

区块链混币中也引入多重签名来增强混币系统的安全性。例如在 CoinSwap^[59]、TumbleBit^[49]中,用户资金需暂时托管至中介的地址,其采用多重签名技术,需要用户与混币中介共同签名才能释放资金。这种方式可以防止混币中介挪用资金。

上述密码学原语作用于混币的不同阶段,对于交易隐私保护的作用也存在差异,比如盲签名主要用于向混币中介屏蔽原始交易输入输出之间的关联,环签名主要用于避免外部观察者追溯交易的发起方,匿名通信网络主要用于隐藏用户的 IP 地址等。已有工作很少对此进行分析讨论,我们将在第 3.3 节详细分析密码学原语对混币技术隐私保护的不同作用。

除了上述密码学原语,近来也有混币技术采用了可信执行环境(Trusted Execution Environment, TEE)^[60]。TEE 是一种基于硬件隔离的安全计算技术,旨在为敏感数据和关键代码提供高度安全、独立的运行环境。TEE 通过在硬件层面创建隔离的内存区域,确保敏感数据的计算和存储仅在该区域内进行,并且只能通过严格授权的接口访问。Obscuro^[61]是首个基于 TEE 的区块链混币技术,确保了混币模块的身份可信和操作环境安全,防止假冒和恶意攻击,保护密钥和敏感数据,从而保障混币过程的公平性和安全性。

3 区块链混币系统模型与分类体系

3.1 系统模型

区块链混币系统是一类基于区块链平台的应用,其目的是隐藏区块链交易输入方和输出方之间

的关联^[62]。混币系统的输入是一个或多个原始交易,输出是一个或多个经过转换之后在区块链平台执行的交易。混币系统保证通过区块链平台达成原始交易的结果,但不在区块链平台记录原始交易输入和输出之间的关联信息。

区块链混币系统中通常有以下三类角色:

(1)参与者:参与者是指主动参与混币的用户,目的是通过混币来保护自己的交易隐私。

(2)中介:中介是混币系统的运营者,负责对交易进行混洗或转发,以保护参与者的隐私。

(3)外部观察者:混币系统之外的任何实体,他们只能观察到区块链上的交易记录,但不能获取混币过程中产生的其他任何信息。

混币系统的目的为隐藏原始交易输入输出之间的关联,因此本文在介绍实现混币系统的技术时,需要分析该技术是否做到、如何做到:

(1)隐藏输入地址:(其他)参与者、中介和外部观察者不能识别出哪些地址是原始交易的输入。

(2)隐藏输出地址:(其他)参与者、中介和外部观察者不能识别出哪些地址是原始交易的输出。

(3)隐藏交易关联:(其他)参与者、中介和外部观察者不能识别出原始交易输入地址和输出地址之间的关联关系。

上面我们强调“其他”参与者,因为原始交易的发起人也是混币的参与者,其必然知道原始交易的

全部细节。如果能够同时隐藏输入和输出地址,那自然可以隐藏交易关联。然而由于混币系统是运行在区块链平台上,对所有角色都隐藏输入和输出非常困难,因此绝大多数混币系统要么隐藏输入,要么隐藏输出,或者是只隐藏交易关联。我们将在第3.3节详细介绍。

区块链混币系统有很多种实现方式,但本质上都是基于k匿名技术:给定 n 个原始交易 $A_i \rightarrow B_i (i = 1, \dots, n)$,经过混币处理之后,只能识别出 k 个可能的交易 $A'_j \rightarrow B'_j (j = 1, \dots, k)$ 。每个原始交易被识别出来的概率都是 $1/k$,从而实现交易匿名。

如图2所示,区块链混币系统基本模型是通过混币中介或合约将多个交易混杂在一起,使得外界不能识别原始交易输入和输出的关联。从具体表现形式来看,可以分为合并型和中转型两类。合并型混币将多个原始交易合并为一个多输入多输出的交易,如图中所示,用户原始交易 $A_i \rightarrow B_i$ 被混币中介/智能合约处理,将 A_1, A_2, A_3 等输入地址与 B_1, B_2, B_3 等输出地址混合,代表系统包括CoinJoin^[63]、CoinShuffle^[40]、CoinParty^[41]等。中转型混币技术则将原始交易拆分为两个交易:存款交易和取款交易,用户在 t_i 时刻存款,在 $t_j (j > i)$ 时刻取款,其代表性系统包括Mixcoin^[64]、Tornado Cash^[37]、Blindcoin^[47]等。

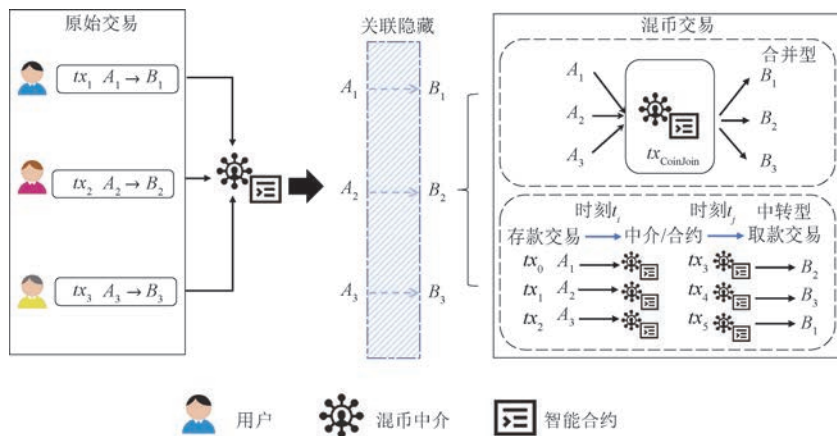


图2 区块链混币系统模型

虽然形式各异,合并型和中转型都满足上述的 k 匿名原理。合并型混币中, n 个原始交易被合并为一个 n 输入 m 输出的交易,则可能的交易为 $n \times m$ 个,每个交易被识别概率为 $1/(n \times m)$ 。中转型混币中,假设在最大中转延迟内,经由该混币中介完成 n 个存款交易, m 个取款交易,即产生了 n 个形如 $A \rightarrow \text{Agency}$ (混币中介/智能合约)的交易与 m 个形

如 $\text{Agency}' \rightarrow B$ 的交易。那么可能的交易仍为 $n \times m$ 个,每个原始交易被识别的概率同样是 $1/(n \times m)$ 。

3.2 分类体系

如表2所示,本文提出区块链混币的三层分类体系,相对于之前工作,本文提出的分类体系可以深刻揭示密码学原语在混币中的作用,也可以更清晰地观察隐私保护的粒度。具体内容我们将在后续章节介绍。

表 2 混币技术分类体系及隐私保护效果对比

混币技术	类型	实现方式	中心节点	年份	平台	屏蔽参与者 (输入 输出 关联)	屏蔽参与者 (输入 输出 关联)	屏蔽参与者 (输入 输出 关联)
Coinjoin ^[63]	合并型	合并真实交易	不需要	2013	比特币	- - 交易合并	- - -	无中介
CoinShuffle ^[40]				2014	比特币	- - 交易合并	- - 解密混合网络	无中介
CoinShuffle++ ^[65]				2016	比特币	- - 交易合并	- - 解密混合网络	无中介
ValueShuffle ^[66]				2017	比特币	- - 交易合并	- - 解密混合网络	无中介
CoinMingle ^[36]				2018	比特币	环签名 隐匿地址 交易合并	- 环签名 -	无中介
CoinChain ^[7]			需要	2022	独立	- - 交易合并	- - 多轮混合	无中介
Dash ^[67]				2015	独立	- - 多中心	- - 多中心	- - 多中心
Obscuro ^[61]				2020	比特币	- - 交易合并	- - TEE	- - TEE
CLSCmix ^[17]				2023	比特币	- - 交易合并	- - 无证书签名	- - -
CMixing ^[15]				2024	比特币	- - 交易合并	- - -	- - -
Medishuffle ^[19]	中转型	合并虚拟交易	不需要	2025	比特币	- - 交易合并	- - 多项式洗牌	- - 多项式洗牌
Monero ^[38]				2015	独立	环签名 隐匿地址 -	无其他混币参与者	无中介
Xim ^[68]		合并原子交易	不需要	2014	比特币	- - 原子交换	- - 多轮混合	无中介
Coinparty ^[41]				2015	比特币	- - 交易合并	- - 解密混合网络	无中介
mpXim ^[10]				2023	比特币	- - 原子交换	- - 多方混合	无中介
SecureCoin ^[69]		托管式	不需要	2017	比特币	- - 转发	- - -	无中介
DCmix ^[8]				2023	比特币	环签名 隐匿地址 转发	无其他混币参与者	无中介
CoinSwap ^[59]			需要	2013	比特币	- - 转发	无其他混币参与者	- - -
Mixcoin ^[64]				2014	比特币	- - 转发	无其他混币参与者	- - -
Blindcoin ^[47]				2015	比特币	- - 转发	无其他混币参与者	- - 盲签名
CoinFA ^[16]				2024	比特币	- - 转发	无其他混币参与者	- - 多中介
TumbleBit ^[49]				2017	比特币	- - 转发	无其他混币参与者	- - 盲签名
Lockmix ^[70]				2020	比特币	- - 转发	无其他混币参与者	- - 盲签名
Coinlayering ^[71]				2020	比特币	- - 转发	无其他混币参与者	- - 多中介
AuditPCH ^[14]				2025	兼容	- - 转发	无其他混币参与者	- - 同态加密
ZeroCoin ^[72]		存取式	不需要	2013	比特币	- ZKP ZKP	无其他混币参与者	无中介
ZeroCash ^[73]				2014	比特币	ZKP ZKP ZKP	无其他混币参与者	无中介
Zcash ^[74]				2016	独立	ZKP ZKP ZKP	无其他混币参与者	无中介
Méobius ^[75]				2018	以太坊	环签名 隐匿地址 转发	无其他混币参与者	无中介
Tornado Cash ^[37]				2019	以太坊	- - ZKP	无其他混币参与者	无中介
MixEth ^[76]			需要	2019	以太坊	- - ZKP	- - 可验证混洗	无中介
Railgun ^[11]				2021	以太坊	ZKP ZKP ZKP	无其他混币参与者	无中介
zkMixer ^[12]				2025	以太坊	- - ZKP	无其他混币参与者	无中介
Blind-Mixing ^[48]				2015	比特币	- - 转发	无其他混币参与者	- - 盲签名
RBSmix ^[13]				2022	比特币	- - 转发	无其他混币参与者	- - 盲签名
Sofitmix ^[9]				2023	比特币	- - 转发	无其他混币参与者	- - ZKP
MixBuy ^[18]				2024	兼容	- - 转发	无其他混币参与者	- - 同态加密

本文采用合并型和中转型作为第一层分类标准,因为两者在表现形式和技术原理上都存在明显差异,对后续分类具有决定性影响。表现形式上的差异,我们已在图 2 展示并在上一节介绍,此处不再赘述。技术原理方面,合并型混币主要采用解密混识证明等技术。

第二层分类标准则是依据具体的实现方式,即如何实现合并,如何完成中转。对于合并型混币,分为三类:合并真实交易、合并虚拟交易以及合并原子交易。对于中转型混币,分成两类:托管式中转和存取式中转。第三层分类标准则聚焦于技术细节,即是否存在中心节点。下面将进行详细介绍。

3.2.1 合并型混币

合并型混币即将多个原始交易合并为一个多输入多输出的交易结构,从而隐藏原始交易中真实的输入输出关系。按照合并的交易类型可分为合并真实交易、合并虚拟交易与合并原子交易,如图 3 所示。

(1) 合并真实交易

合并真实交易通过将多个用户的真实交易聚合为单一的多输入多输出交易,从而有效隐藏原始交易的输入输出对应关系。如图 3(a)所示,多名用户的原始交易经过混币后转变为一个多输入多输出的交易。其基本流程如算法 1 所示,具体包含以下阶段:首先,由参与者自发或在混币中介协助下组成

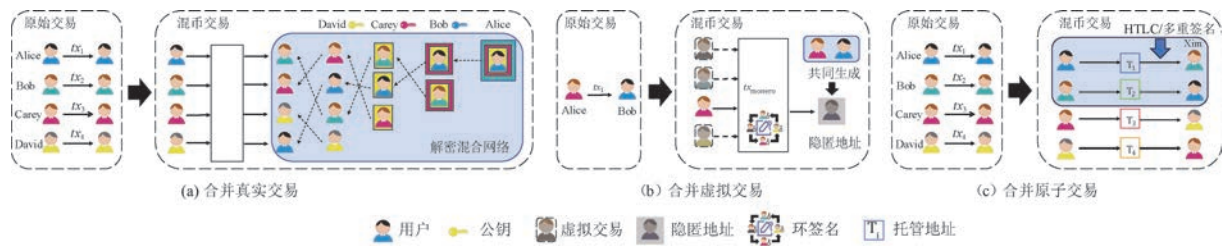


图3 合并型混币示意图

混币群组(第1行);其次,构建一个多输入多输出的聚合交易(第2行);然后,由所有参与者分别对该交易进行签名(第3~5行);最后,当全部签名完成后,最终交易被广播至区块链网络并完成上链(第6行)。根据组织方式的不同,合并真实交易可分为去中心化与中心化两种实现模式。

去中心化实现中,混币过程完全由参与者协作完成,无需可信中介。参与者通常通过点对点网络协商或广播机制自发组成混币群组,并在群组内部通过密码学协议协同构建聚合交易。为了打破交易之间的可追踪性,参与者采用解密混合网络等匿名通信技术对输出地址进行混洗,从而实现地址映射关系的随机。

中心化实现则依赖专门的混币中介来组织和协调交易生成。由于中介的可信性问题,这类方法通常采用多重防护机制以降低风险,例如:进行多轮混币操作以增加混淆层级、引入多个中介节点分散信任,或利用可信执行环境(TEE)等硬件安全技术来保证交易正确性与隐私性。

算法1. 合并真实交易(Combine Real Transactions)

输入: participants $P = \{p_1, p_2, \dots, p_n\}$, inputAddresses A_{in} , outputAddresses A_{out} , values V

输出: broadcast transaction tx

1. $G \leftarrow \text{FormGroup}(P, \text{coordinator})$
2. $tx \leftarrow \text{BuildTransaction}(A_{in}, A_{out}, V)$
3. $\Sigma \leftarrow \emptyset$
4. FOR $i \leftarrow 1$ to n DO
5. $sig_i \leftarrow \text{Sign}(tx, p_i, sk)$
6. $\Sigma \leftarrow \Sigma \cup \{sig_i\}$
7. END FOR
8. $\text{BroadcastOnChain}(tx, \Sigma)$

解密混合网络作为合并真实交易类型混币的主要技术,通过对交易输出进行层层加密并打乱顺序,最终实现混洗效果。该技术旨在解决两种问题:防止混币参与者通过内部信息推测真实交易关系以及防范可能发生的拒绝服务攻击(DoS)等安全威胁。

这些问题的解决关系到混币技术的实际隐私保护效果和系统稳定性。

(2) 合并虚拟交易

合并虚拟交易的混币类型中引入了虚拟交易参与者,不再合并多个实际的真实交易,如图3(b)所示,图中的虚拟交易节点表示从区块链历史中随机选取的虚拟交易输入,它们与发送方的真实输入共同构成环签名集合,从而掩盖真实来源。在具体实现上,该技术主要依赖环签名和隐匿地址。

算法2. 合并虚拟交易(Combine Virtual Transactions)

输入: sender s , receiver r , value v

输出: broadcast virtual transaction tx

1. $a_{\text{stealth}} \leftarrow \text{GenStealthAddr}(s, pk, r, pk)$
2. $C \leftarrow \text{SelectRandomKeys}(\text{blockchain.history})$
3. $R \leftarrow C \cup \{s, pk\}$
4. $tx \leftarrow \text{BuildTransaction}(R, a_{\text{stealth}}, v)$
5. $sig \leftarrow \text{RingSign}(tx, R, s, sk)$
6. $\text{BroadcastOnChain}(tx, \{sig\})$

其基本流程如算法2所示:首先,交易接收方与发送方协同生成一次性隐匿地址,用于接收当前交易资金,该地址仅能由接收方的私钥支配(第1行);其次,系统从区块链历史中随机选取若干过往交易的公钥(第2行),并将这些公钥与发送方的真实公钥共同组成一个环(第3行)。这些历史交易输入仅用于掩盖真实来源,不会发生实际资金转移,因此被称为“虚拟交易”;然后,发送方利用环签名算法对包含隐匿地址的交易进行签名(第4~5行);最后,将签名后的交易结构广播至区块链网络(第6行)。通过环签名与隐匿地址的协同使用,实现了交易双方信息的双重隐私保护。

合并虚拟交易与合并真实交易相比,不需要等待其他用户协同,效率较高,且可以隐藏交易的发送方与接收方的身份,其匿名程度较高。

(3) 合并原子交易

图3(c)展示了合并原子交易的形式,与前两种方式不同,该模型强调交易的原子性与协同签名机

制:所有交易必须同时成功或同时回滚。

在具体实现上,合并原子交易主要依赖阈值签名这一关键技术(算法 3):首先,参与者通过 P2P 网络或广播协议寻找并筛选潜在的混币合作者(第 1 行);其次,建立原子交易,将资金转入随机选择的其他用户输出地址(第 2~5 行);然后,由所有参与者协同生成阈值签名,以确保交易的安全性与不可否认性(第 6~8 行);最后,在签名验证通过后,系统正式提交交易至区块链(第 9~12 行);若检测到恶意参与者或网络攻击,系统将触发回滚机制,将资金退回至原始用户的输入地址(第 13~15 行)。

算法 3. 合并原子交易(Combine Atomic Transactions)

输入: participants $P = \{p_1, p_2, \dots, p_n\}$, inputAddresses A_{in} , outputAddresses A_{out} , values v

输出: broadcast atomic transaction set $\{tx_1, tx_2, \dots, tx_n\}$

1. $C \leftarrow \text{FindCollaborators}(P2P \text{ network})$

2. $A_{out}^{rand} \leftarrow \text{RandomPermute}(A_{out})$

3. FOR $i \leftarrow 1$ to n DO

4. $tx_i \leftarrow \text{BuildAtomicTx}(A_{in}[i], A_{out}^{rand}[i], v)$

5. END FOR

6. FOR $i \leftarrow 1$ to n DO

7. $sig_i \leftarrow \text{ThresholdSign}(tx_i, C)$

8. END FOR

9. IF $\text{VerifyAllSigns}(\{sig_1, \dots, sig_n\})$ THEN

10. FOR $i \leftarrow 1$ to n DO

11. $\text{BroadcastOnChain}(tx_i, \{sig_i\})$

12. END FOR

13. ELSE

14. $\text{RollBack}(A_{out}^{rand}, A_{in})$

15. END IF

3.2.2 中转型混币

中转型混币技术通过将交易过程分解为两个独立阶段,阻断时间关联,完成输入与输出的隔离,如图 4 所示,中转型混币按中转机制可分为托管式与存取式两类。

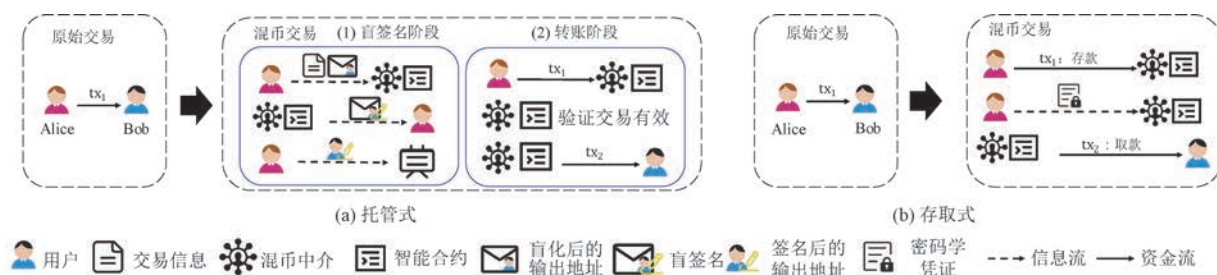


图 4 中转型混币示意图

(1) 托管式中转

该技术在用户将数币转给中介后,由中介主动发起向收款方的交易,其核心在于构建可信的资金转发机制。多采用中心化架构,由混币中介协调交易流程并完成数币中转,但也存在少量基于协议或合约的去中心化实现。图 4(a)展示了托管式中转的典型流程,作为发送者的用户首先将资金发送至中介或智能合约生成的托管地址,中介或智能合约在验证交易合法性后再将资金发送到目标输出地址。

其基本流程如算法 4 所示,包含以下几个步骤:首先,用户向中介节点或智能合约提交交易请求;其次,系统生成临时托管地址以接收用户资金(第 1 行);然后,系统等待用户将资金转入托管地址后,对托管交易 tx_{in} 进行有效性检查(第 3 行);若用户正确完成转账,系统将资金转入目标输出地址并签名(第 4~5 行);最后,将交易广播至区块链网络并完成上链(第 6 行)。在整个过程中,系统通过密码学手段确保中介无法获取完整的交易信息,从而保障

用户隐私与资金安全。

针对中介可信度问题,该技术采用了多种防护措施,代表性技术有盲签名和多中介架构。盲签名技术可对敏感交易信息加密,使中介在签名时无法获取完整交易细节;多中介架构可以增加交易路径复杂度,从而防范单点信息泄露。

少数托管式中转技术不依赖中介节点,而是通过公告板或协议组建混币群组:由群组共同生成托管地址,待验证交易合法性后方将资金转出。

算法 4. 托管式中转(Escrowed Relay)

输入: sender s , receiver r , value v

输出: broadcast escrow transfer transaction tx_{out} if the deposit is confirmed

1. $a_{escrow} \leftarrow \text{GenEscrow}(s, addr, v, r, addr)$

2. IF $\text{VerifyDepositStatus}(a_{escrow}, v) = \text{success}$ THEN

3. $tx_{out} \leftarrow \text{BuildTransaction}(a_{escrow}, r, addr, v)$

4. $sig_{agency} \leftarrow \text{Sign}(tx_{out}, agency, sk)$

5. $\text{BroadcastOnChain}(tx_{out}, \{sig_{agency}\})$

6. END IF

(2) 存取式中转

存取式中转技术中,用户与混币中介或智能合约交互,并由收款方自主取出资金。其核心在于用户如何在不泄露自己真实身份与交易信息的前提下,向混币中介或智能合约证明其取款权限。图 4(b)展示了该技术的典型流程,其关键在于将存款与取款阶段完全分离。用户在存款时生成零知识证明并提交凭证,收款方在稍后时刻利用该证明完成取款。

算法 5. 存取式中转 (Deposit-Withdrawal Relay)

输入: sender s , receiver r , value v

输出: broadcast deposit transaction tx_{dep} and, after proof verification, broadcast withdrawal transaction tx_{wd}

1. $\pi \leftarrow \text{GenZKProof}(s, sk, v)$
2. $tx_{dep} \leftarrow \text{BuildDepositTx}(s.addr, contract.addr, v)$
3. $sig_s \leftarrow \text{Sign}(tx_{dep}, s.sk)$
4. $\text{BroadcastOnChain}(tx_{dep}, \{sig_s\})$
5. $\text{SubmitProofToSystem}(\pi)$
6. IF $\text{VerifyZKProof}(\pi)$ THEN
7. $tx_{wd} \leftarrow \text{BuildWithdrawTx}(contract.addr, r.addr, v)$
8. $sig_r \leftarrow \text{Sign}(tx_{wd}, r.sk)$
9. $\text{BroadcastOnChain}(tx_{wd}, \{sig_r\})$
10. END IF

其基本流程可分为两个阶段(算法 5):

阶段 1: 存款: 首先, 用户生成零知识证明, 用于后续取款时的身份与资金所有权验证(第 1 行); 其次, 将资金转入指定的存款地址, 签名后广播上链(第 2~4 行)。

阶段 2: 取款: 首先, 用户利用之前生成的零知识证明, 向系统证明其拥有相应的取款权限(第 5 行); 其次, 系统在验证零知识证明正确后, 将资金转入用户提供的目标地址(第 6~8 行); 最后, 交易被广播至区块链网络并完成上链(第 9 行)。该流程确保了用户在存款与取款的过程中, 均无需暴露交易的关联信息, 从而实现了更强的隐私保护。

该技术主要存在两种实现模式: 大部分采用去中心化设计, 完全基于智能合约运行, 用户通过零知识证明与链上合约直接交互; 少数技术保留中心化节点, 但借助盲签名等技术确保中介无法获取完整的交易信息。这两种模式都致力于解决同一个核心问题: 如何防止资金存取操作被关联追踪。

存取式中转技术多数使用零知识证明, 允许用户向验证者(智能合约或中介节点)证明自己拥有取款权限, 同时不泄露交易信息。

表 2 展示了已有的混币技术。从中可以发现:

(1) 比特币平台占绝对优势, 70% 的混币技术运行在比特币上, 说明比特币平台用户更关心交易隐私。

(2) 中转型略多于合并型, 中转型更为便捷, 不需要等待其他用户组团。

(3) 合并型中, 很少使用中心化设计(33%)。中转型中, 中心化方案则超过一半, 并且广泛采用盲签名技术来防范中介知晓原始交易信息。

3.3 密码学原语在交易隐私保护中的作用分析

如上节所述, 不同混币技术依赖不同密码学原语实现交易关联性隐藏, 而密码学原语的选择本质上取决于需屏蔽的目标角色。本节将从混币技术所需要屏蔽角色的视角, 分析混币技术如何针对三类关键角色——外部观察者、参与者、中介设计隐私保护机制。

区块链混币的核心目标在于向外部观察者、其他参与者及中介隐藏交易信息(包括输入地址、输出地址或输入输出间关联)。隐藏任意一项即可实现隐私保护, 且隐藏越多, 隐私保护强度越高。如表 2 所示, 不同混币技术在屏蔽角色能力上存在显著差异: 合并型技术因依赖群体协作, 需同时应对外部观察者与内部参与者威胁, 因此采用解密混合网络或多中心架构等技术屏蔽这两类角色; 而中转型技术则因为多数需要混币中介参与, 故将隐私保护重心置于屏蔽中介, 主要采用零知识证明、盲签名等手段。下文将解析三类角色的屏蔽机制及其密码学实现。

屏蔽外部观察者是区块链混币系统最基础的要求。当前所有混币技术均不同程度实现了对外部观察者的屏蔽: 其中合并型混币主要通过交易合并实现, 而中转型混币则依赖第三方转发切断输入输出关联。此外, 去中心化的中转型混币, 比如 Zero-coin、Zerocash 和 Zcash 还通过零知识证明来隐藏输入地址和输出地址。也有多个技术采用环签名来向外部观察者屏蔽输入地址, 包括 Méobius、DC-mix、Monero 和 CoinMingle, 这些技术也结合隐匿地址技术屏蔽原始交易输出地址。

屏蔽(其他)参与者主要通过解密混合网络(CoinShuffle、CoinParty、CoinShuffle++、ValueShuffle)和多轮混合(Xim、CoinChain、Dash)实现。其中 CoinMingle 较为特殊, 其采用环签名避免其他参与者识别输出地址。上述技术均属于合并型混币。中转型混币多数没有其他参与者, 但 MixEth 采用可验证混洗, SecureCoin 使用解密混合网络来

防止其他参与者识别原始交易输入和输出之间的关联。

屏蔽中介指的是技术上防止混币中介识别原始交易的内容,大部分中心化混币技术都实现了对中介的技术屏蔽。这里面最常使用的技术是盲签名(Blindcoin、Blind-Mixing、TumbleBit、Lockmix、RBSmix)以及多中介架构(CoinLayering、CoinFA)。

上述分析表明,密码学原语在混币中的作用呈现显著差异,其技术逻辑可归纳为两个层面:

(1)针对不同威胁主体的隐私保护机制差异:混币系统根据防御对象(外部观察者、参与者、中介)选择特定密码学原语。例如,环签名、隐匿地址与零知识证明侧重屏蔽外部观察者;解密混合网络专用于隔离参与者信息;盲签名则聚焦中介身份隐匿。

(2)密码学原语与混币类型的适配性差异:解密混合网络主要适用于合并型混币(需聚合多用户交易并防范参与者知晓真实的关联信息);零知识证明更适用于中转型混币(通过匿名凭证验证转入方所有权)。这种技术分化源于混币架构的底层原理:合并型混币因多参与者特性需防范参与者知晓真实的关联信息,而中转型混币的存取机制天然依赖零知识证明实现所有权验证。

此外可以看出,我们提出的三层分类体系很好地体现了混币技术脉络,并自然而然地将密码学原语聚集在不同子类中,这也从另一个侧面说明了这一分类体系的合理性。

4 合并型混币

在第3节中我们已经介绍了合并型混币中每一类别的基本技术原理,本节将介绍各个类别的代表性技术和应用系统,最后介绍一个典型应用——Wasabi Wallet。

4.1 合并型混币技术

合并型混币利用比特币的交易结构,将多个原始交易合并为一个多输入多输出的交易。根据被合并的交易类型,又分为合并真实交易、合并虚拟交易与合并原子交易三类。

4.1.1 合并真实交易

合并真实交易中,所有被合并的转账操作最终都将在合并后的混币交易中执行。此类混币技术中最重要的就是打包多个交易的环节,因为负责打包的角色有可能知晓原始交易的内容,从而泄露交易隐私。

根据打包环节是否由中心节点完成,可以进一步细分为去中心化和中心化两类。

(1)去中心化

此类混币没有中心节点,打包环节由多个参与者共同完成。其鼻祖是2013年出现的CoinJoin^[6],在此基础上随后衍生出多个系列。CoinMingle^[36]的核心原理虽然也是形成一个多输入多输出的交易,但它采用了环签名和隐匿地址来进一步保护隐私。CoinShuffle^[40]则在CoinJoin的基础上,使用解密混合网络防止混币参与者知晓真实的交易关系,但是CoinShuffle通信效率较低。为此,CoinShuffle++^[65]使用DiceMix以提高混合效率。进一步地,ValueShuffle^[66]在CoinShuffle++的基础上,通过兼容机密交易来隐藏交易金额。值得注意的是,在此类混币技术中,只有CoinChain^[7]是基于侧链来实现的,并且它使用固定金额防止金额追踪。下文将对各个技术进行简单介绍。

CoinJoin^[6]由比特币核心开发者Gregory Maxwell提出。其核心思想是将多个用户的交易合并为一笔交易,使得外部观察者难以追踪每一笔数币的来源和去向。但是,CoinJoin要求输出金额相等,很容易被识别为混币交易。此外,CoinJoin中每个参与者都会知晓真实的交易输入输出关系,存在隐私泄露的风险。

CoinMingle^[36]是一种基于环签名、隐匿地址的去中心化混币技术,其核心创新在于互认委托策略的引入,通过多方协同的匿名交互机制,有效避免了隐私泄露问题。CoinMingle采用输入量容忍机制,允许用户在无需预先计算的情况下参与混币;同时,在洗牌阶段通过密码学方法有效阻止了个人信息的泄露。

CoinShuffle^[40]针对CoinJoin中参与者知晓真实交易信息的问题进行了改进。为此,其核心是引入解密混合网络,通过分层加密与多轮混淆操作多次打乱交易输出地址的顺序,从而避免混币参与者知晓其他参与者的原始交易信息。

CoinShuffle++^[65]弃用了CoinShuffle的线性通信模式,采用基于DiceMix协议的并行化混合机制。该机制允许所有参与者的交易数据在混合过程中同步处理,而非依赖顺序操作,从而降低通信延迟。

ValueShuffle^[66]在CoinShuffle++的基础上进行了改进,使其能够与机密交易兼容。具体而言,ValueShuffle进一步隐藏了交易金额,从而提供了更强的隐私保护。

CoinChain^[7]是一种基于侧链的匿名加密货币技术,旨在通过结构化混币机制增强交易隐私性。具体来说,参与者首先在链下达成协议,然后采用和CoinJoin类似的方式进行交易合并和混合。混币过程实际上完成了CoinID所有权的转移,从而增强了交易的隐私性。

(2) 中心化

合并真实交易类型的混币技术总体以去中心化为主,这主要是由于参与者担忧混币中介可能获取交易内容。目前已知的合并真实交易类型的技术中,仅有少数采用了中心化或半中心化设计,包括Dash^[67]、Obscuro^[61]、CMixing^[15]、CLSCmix^[17]以及Medishuffle^[19]。Dash采用多中心机制,其运行在独立的区块链平台上。而Obscuro作为目前唯一基于TEE的区块链混币技术,通过硬件级安全机制保障混币操作的完整性和数据隐私。CMixing的核心创新在于独特的交易金额分配规则,允许用户动态调节匿名强度。相比之下,CLSCmix通过无证书签名优化了与混币中介交互的认证及保密流程,而Medishuffle则聚焦于特定场景,在混币机制中引入了强制的审计与监管能力。

Dash^[67]通过多中心机制提升了混币系统的隐私保护能力,在交易聚合阶段采用CoinJoin技术将多用户数字货币混合,并通过主节点接力混合打乱交易路径,有效提升了交易链路追溯难度。

Obscuro^[61]是当前唯一一个基于TEE的中心化混币技术。其通过TEE保证代码和数据的一致性和完整性,确保混币操作正确并且保护敏感数据,排除了恶意中介的数字货币盗窃和地址链接攻击。

CMixing^[15]于2024年被提出,其特点在于更加注重用户体验,提供匿名性保证和最小化交易费用的功能。CMixing通过引入 c -分解的概念,允许用户自主选择匿名程度并且有效最小化输出数量。CLSCmix^[17]提出了一种基于无证书签名的混币协议。该方案要求用户以密文发送交易请求,在克服传统公钥基础设施中证书管理负担的同时,确保了只有混币中介能解析用户的输入输出映射。这种设计有效防范了同组其他参与者和外部观察者的隐私窃取,并支持多组用户并发执行。

Medishuffle^[19]是一种专为医疗物联网场景设计的混币方案。其架构中引入了洗牌节点与监管机构,采用基于多项式的群签名代替传统的网络层匿名机制来进行身份认证与多项式洗牌。这种设计赋予了监管机构在发生医疗纠纷或非法交易时,通过

追踪密钥揭露真实用户身份的审计能力。

4.1.2 合并虚拟交易

目前采用合并虚拟交易的只有门罗币,且采用去中心化架构。Monero^[38]也是通过合并多个交易来保护用户交易隐私,但与合并真实交易类别不同,Monero的混币过程通过合并多个交易形成交易包,但其中仅包含一个真实交易,其余均为虚拟交易。Monero^[38]的隐私保护机制主要依赖于环签名和隐匿地址技术。在门罗币上进行的每一笔交易都隐藏了发送者与接收者的身份信息;其中,发送者的身份信息由环签名保护,接收者的身份信息由隐匿地址保护。Monero的混币过程展现出以下优势:首先,用户无需与其他用户进行交互即可独立完成混币操作,这种非交互式设计有效避免了因通信行为导致的隐私泄露风险;其次,其混币机制通过自动选取区块链历史交易中的诱饵输入(Decoy Inputs),在无需人工干预的情况下增强了交易的匿名性,使得外部观察者既无法识别交易双方的真实身份,也难以推断出链上交易间的逻辑关联。

4.1.3 合并原子交易

最后一类合并型混币技术为合并原子交易,其不显式生成一个多输入多输出的交易,而是生成多个相互关联的交易。这些交易通过原子性约束实现“全执行或全回滚”,因此构成一组原子交易,此类技术统称为合并原子交易。代表性技术包括Xim^[68]、mpXim^[10]和CoinParty^[41],均属于去中心化类型。

Xim^[68]是一种基于区块链广告机制的可扩展多轮混币技术,其核心在于利用区块链的全局广播特性构建去中心化广告网络,实现混币参与者的自主发现与匹配。参与者可依据隐私需求灵活选择串行或并行执行策略,以此优化混币效率与匿名强度。

mpXim^[10]是Xim协议的扩展。针对Xim仅支持双方匹配所导致的性能问题,mpXim提出了一种多方发现协议。该协议允许网络中的多个参与者在同一轮次中同时发现彼此,并构建多方联合的原子互换,从而扩大单次混币的匿名集规模,并降低达到高匿名性所需的轮次和时间。

CoinParty^[41]基于阈值ECDSA签名方案与解密混合网络实现混币。该技术通过安全多方计算协议保障混币过程的有效性,即使网络中存在恶意节点,仍能确保一对一交易的混币操作安全完成。

Xim与mpXim均基于阈值签名与哈希时间锁合约(Hashed Timelock Contracts, HTLC)构建公平交换协议,该协议通过密码学手段确保交易各方

权益的公平性与多方互换的原子性。而 CoinParty 则将阈值签名应用于托管地址的分片化管理,通过分布式密钥生成技术将资金控制权分散在多个独立的混合对等体之间,且在资金从托管地址中转出时,需要一定数量的混合对等体签名,在保证交易原子性的同时实现了更高程度的去中心化。

4.2 合并型混币应用系统

本小节所介绍的混币应用系统,均采用了上一小节所介绍的混币技术。我们将首先分析现有合并型混币应用系统所采用的技术原理,然后分析其采用的安全保障机制。

如表 3 所示,目前超过 70% 的合并型混币应用系统采用合并真实交易的方式。其中,明确采用合并虚拟交易的仅 Mixero^[77],采用合并原子交易的仅 Odos^[78],而仅有一个系统 Jupiter^[79] 采用了多种技术,其既有合并真实交易又有合并虚拟交易。合并真实交易实现简单且历史较长,更易被用户接受。此外,我们注意到个别系统(例如 CryptoMixer^[80])因未明确公布技术细节,导致无从判断其具体使用的合并交易方式。这种技术不透明现象在区块链混币领域并不罕见,多数系统的技术说明较为简略,对核心机制的披露尤为有限。

表 3 合并型混币应用系统

混币应用系统	技术原理	支持货币类型	跨链	安全保障			
				信用保障书	无日志	无需注册	Tor 网络
WasabiWallet ^[81]	合并真实交易	BTC	×	?	?	✓	✓
JoinMarket ^[82]		BTC	×	?	✓	✓	✓
GoMix ^[83]		ETH、USDT、SOL 等	✓	?	✓	✓	✓
Anonymix ^[84]		BTC	×	✓	✓	✓	×
Samourai ^[85]		BTC	×	?	✓	✓	✓
ToSwap ^[86]		BTC、ETH、USDT、BNB 等	✓	?	✓	✓	✓
Unijon ^[87]		BTC	×	✓	✓	✓	✓
whir ^[88]		BTC	×	✓	✓	✓	✓
CoinMix ^[89]		BTC	×	✓	✓	✓	✓
JokerMix ^[90]		BTC、DASH	×	✓	✓	✓	✓
Mixero ^[77]	合并真实交易、虚拟交易	BTC、ETH	×	✓	✓	✓	✓
Odos ^[78]	合并原子交易	BTC、ETH 等	✓	?	?	✓	×
CryptoMixer ^[80]	?	BTC	×	✓	✓	✓	✓
Jupiter ^[79]	包含多种技术	ETH、JUP、USDT、USDC 等	✓	?	×	✓	×

我们也看到,几乎所有的合并型混币应用系统都支持比特币平台,只有少数系统同时支持以太坊、USDT 等其他平台。值得注意的是,支持多平台的系统通常具备跨链兼容能力。

在安全保障机制层面,混币系统普遍通过以下四个维度构建安全体系:信用保障书、无日志机制、无需注册以及 Tor 网络应用。

(1)信用保障书通过数字签名技术生成不可伪造的协议文件,其核心作用在于形成用户参与混币的法律证据,通过密码学手段确保协议内容透明且无法篡改。当出现争议时,用户可通过验证签名追溯责任方,以此保障资金安全并防范系统违规操作。

(2)无日志机制保证用户在交易后,混币应用系统不会保留任何与交易相关的记录,防止第三方中介泄露用户隐私。

(3)无需注册保证用户无需提交可关联真实身份的个人信息即可使用系统,实现参与过程的匿名化效果。

(4)Tor 网络使得混币应用系统无法通过 IP 地址关联到用户真实身份,例如交易所无法通过 IP 日

志反推混币参与者。

如表 3 (“✓”表示混币系统具有这种安全保障机制,“×”表示没有,“?”表示并未说明)所示,所有的混币应用系统都不要求用户注册,超过 70% 的混币系统同时支持 Tor 网络与无日志策略,超过 50% 的混币应用系统有信用保障书。

4.3 Wasabi Wallet

Wasabi Wallet 是基于比特币的开源钱包,通过将多个用户的比特币交易混合在一起,使得外部观察者难以追踪资金的来源和去向。

Wasabi Wallet 具有开源和非托管两个特性:

(1)开源:Wasabi Wallet 遵循“不相信即验证”的原则,其代码公布在 Github 平台,用户可以随时检查代码逻辑或自行编译。

(2)非托管:用户始终通过本地客户端生成并加密存储私钥,混币过程中无需向协调服务器或第三方披露密钥信息。

本研究基于 L Wu 等人提供的混币数据集(涵盖 ChipMixer、ShapeShift 及 Wasabi Wallet 三类混

币系统)^[91],重点选取 Wasabi Wallet 子集,筛选出 2017 年 11 月 9 日至 2020 年 3 月 4 日期间的 5000 笔有效交易数据,从时间分布特征、输入输出特征两个维度进行统计分析,以发现用户行为规律与监管需求。

4.3.1 交易活跃时间

本文按小时粒度统计 Wasabi Wallet 的交易次数与单笔平均交易金额,如图 5,活跃时段集中在北京时间凌晨 2 时至正午 12 时,其中 7:00 时单小时交易次数达到峰值;12:00 之后交易活跃度下降,21:00 活跃度最低,单小时交易次数达到最低值 71 次,21:00 后活跃水平上升。

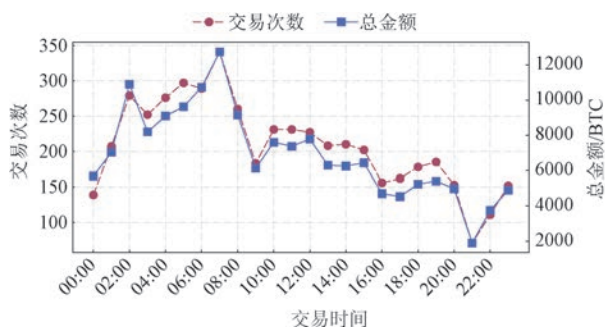


图 5 Wasabi Wallet 交易总金额与交易次数的时间分布

这种时间分布特征与 Tornado Cash 的时间分布特征(见 5.3)基本相同,但 Wasabi Wallet 的交易从 6:00 开始活跃,6:00-12:00 比较符合亚洲作息,这可能表明 Wasabi Wallet 的亚洲用户居多。另外交易总金额的变化趋势也与交易次数的变化趋势基本相同。

4.3.2 输入输出分布

我们统计了所有交易的输入输出个数,如图 6,交易的输入个数大多分布在 70-100 的区间内,最多不超过 160 个,最少不小于 10 个。输出个数分布在 10-300。其中最多分布在 100-130 的区间内。且输出个数的分布类似正态分布,相较于输入,输出个数有明显的增加。

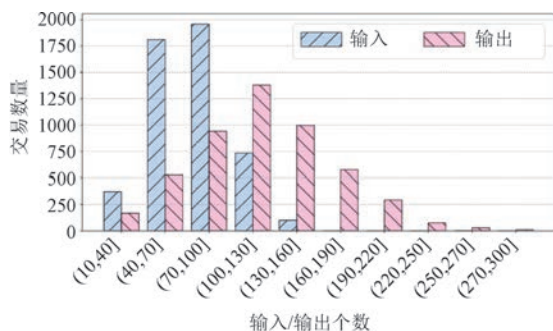


图 6 Wasabi Wallet 输入/输出地址数量分布

4.4 小结

本节介绍了合并型混币的主要技术类别,包括合并真实交易、合并虚拟交易与合并原子交易三种,并对典型系统及其安全机制进行了分析。总体而言,合并型混币主要在交易结构层实现多输入多输出的聚合与混合,基于 k 匿名隐藏用户的真实交易关联。

超过 70% 的合并型混币系统不依赖中介,避免了对中介的信任假设,也消除了单点故障的风险。然而,此类混币方案依赖参与者的同步与协作,易受群体规模、通信延迟及金额一致约束的影响。此外,由于混合规模有限,相较于中转型混币,其匿名保护能力偏弱。

5 中转型混币

中转型混币与合并型混币不同,其借助混币中介或智能合约完成转发从而隐藏真实的交易关联。本节首先介绍中转型混币技术,再介绍其应用系统,最后剖析一个代表性实例,也是目前使用最为广泛的混币应用系统——Tornado Cash。

5.1 中转型混币技术

中转型混币技术将原始交易拆分为存款交易与取款交易,一般通过中介或智能合约来转发。根据第二步交易是由混币中介/智能合约还是用户发起,可以进一步分为托管式中转和存取式中转。

5.1.1 托管式

托管式混币技术可分为中心化与去中心化两类,其中多数混币技术均依赖中心节点,即由混币中介直接将数币转给指定接收者。仅有两种技术不包含中心节点,即通过引入分布式公告板或生成聚合地址完成数币的转发。

(1) 去中心化

去中心化托管式混币技术包含 SecureCoin^[69]与 DCmix^[8],其中 SecureCoin 通过聚集地址技术来构建一个 $m \rightarrow 1 \rightarrow n$ 的特殊转发过程;Dcmix 引入公告板,使参与者通过自主混合完成原始交易的拆解和重构。

SecureCoin^[69]采用“聚合”与“分布”结合的数币交易形式,并融合解密混合网络、聚集地址等技术实现匿名性与不可连接性。通过这种设计,SecureCoin 不仅避免了依赖单一中介的安全风险,还通过多方协作与秘密分享技术增强系统安全性及去中心化特性。

DCmix^[8]基于改进的 Abe-Ohkubo-Suzuki(AOS)环签名变体,在对等网络中实现节点的无条件匿名。该技术将原始交易拆分为两个独立交易,通过环签名与隐匿地址技术切断交易输入输出的关联性,以此隐藏用户真实身份。

(2) 中心化

中心化的托管式混币技术基本过程为:参与者将数币转入混币中介,随后由混币中介将混币转入到指定地址。该过程面临两个问题:首先,如何防范混币中介违约,即中介不按时将数币转至用户指定地址;其次,如何防范混币中介知晓原始交易信息。

Mixcoin^[64]与 Blindcoin^[47]均采用事后追查防范中介违约——即不主动预防违约行为,但违约发生时可通过密码学技术验证并证实违约事实。

Mixcoin^[64]设计问责机制:若中介未按时分配数币,参与者可公开其签名承诺。任何观察者均可验证中介的欺骗行为,从而损害其声誉并影响后续业务。然而,Mixcoin 未解决混币中介知晓原始交易信息的问题。

Blindcoin^[47]在 Mixcoin 基础上引入盲签名技术,通过密码学手段隐藏交易关联性,有效防止中介获取真实交易关系。该协议沿用 Mixcoin 的问责机制,同时通过盲签名技术进一步提升了系统的隐私性和安全性。

CoinSwap^[59]、TumbleBit^[49]、Lockmix^[70]和 AuditPCH^[14]均通过技术手段防止中介违约。其中 CoinSwap 和 TumbleBit 采用了公平交换协议(fairexchange protocol),AuditPCH 采用适配器签名(Adaptor Signature),而 Lockmix 则要求中介先将数币转入指定地址,并通过担保机制对违约用户进行追责。四者之中,仅 CoinSwap 未向中介屏蔽真实交易信息。

CoinSwap^[59]采用基于公平交换协议的机制,虽通过双重托管保障交易完整性,但中介节点全程掌握交易关联信息,因而造成用户隐私泄露的单点信任风险。

Lockmix^[70]采用盲签名算法,有效防止混币中介知晓输入与输出之间的关联,同时通过多方签名机制确保混币中介无法盗取用户数币,并借助匿名网络隐藏用户真实 IP 地址及交易路径,从而避免网络监听者通过流量分析或元数据追踪用户身份或交易关联。

与以上混币技术不同,CoinLayering^[71]和 CoinFA^[16]引入了额外的监管者角色以监管混币中介的

行为,防止混币中介互相勾结盗取用户数币、泄露用户信息。

CoinLayering^[71]引入了监管者角色,负责向用户推荐“混合节点”(mixer),以弥补不同节点之间的成本差异,并监控其行为以防止盗窃。与传统混币系统中由单一中介统一负责混币操作不同,CoinLayering 中的混合节点可以是多个独立参与方,它们共同承担交易混洗或转发的职能。针对混合节点的拒绝服务行为,系统采用用户披露机制进行审计:若混合节点存在拒绝服务行为,监管机构将扣除其保证金并降低其信誉评分。

CoinFA^[16]同样使用了 RSA 来完成谜题的生成与解密,与 TumbleBit 不同的是,该技术借鉴了 CoinLayering 中的分层结构,并引入了监管节点来保证交易的公平性,防止恶意节点作恶。此外,还通过与两个混合节点交互,防止单一混合节点知晓真实的交易关系,从而侵害用户隐私。

5.1.2 存取式

此类混币技术的基本过程是用户将数币转入混币中介(中心)或智能合约(去中心),之后由用户主动发起取款交易,向其出示密码学凭证,由混币中介或智能合约将数币转入指定地址。主要采用去中心化路线。

(1) 中心化

Blind-Mixing^[48]通过椭圆曲线盲签名方案增强比特币交易的匿名性,并通过使用盲签名,有效避免混币中介将取款交易与存款交易关联。

RBSmix^[13]是一种支持监管介入的混币技术,通过中央机构(CA)、监管队伍、混合节点与用户的协同机制实现匿名性与合规性平衡。RBSmix 将用户身份信息分片加密后交由多方监管者交叉验证,并利用盲签名技术防止内部合谋;混币过程中节点仅存储脱敏数据,若检测到非法交易,CA 可联合监管队伍通过分片解密机制追溯真实身份,既保障用户隐私又满足反洗钱监管需求。

SofitMix^[9]是一种支持链下并行支付的兼容比特币的安全混币协议。它引入了一个中心化的混币中介,利用零知识证明来切断交易双方的链接性。结合哈希时间锁与数字签名技术来保证交易存取过程的原子性与公平交换。

MixBuy^[18]是一种不可链接条件支付协议。主要针对买家通过不可信混币中介向卖家支付并换取数字商品的场景。协议通过可随机化谜题与智能合约时间锁,将买家存入混币中介的资金与混币中介

支付给卖家的资金解耦。在保证买卖双方一手交钱,一手交货的公平性的同时,确保混币中介无法知晓买卖双方的具体对应关系。

(2) 去中心化

此类技术最大挑战在于用户调用智能合约将数字货币转入指定地址时,如何证明自己有权使用这笔数字货币,但是又不暴露自己的身份。目前几乎都采用了零知识证明(ZKP)来解决,因为 ZKP 允许证明者向验证者证明某个陈述的真实性,而无需透露陈述本身以外的任何信息。

Zerocoin^[72]、Zerocash^[73]均是基于比特币平台的混币技术。其中,Zerocoin 作为 2013 年提出的比特币侧链协议,通过零知识证明实现混币功能,其机制为用户销毁原币后生成无交易记录的新币,但存在固定面额限制、证明数据量大及易受时序攻击等缺陷。作为改进版本,Zerocash 于 2014 年提出,通过引入 zk-SNARK 技术隐藏交易金额及地址,支持任意金额转账并提升匿名性。而 Zcash^[74]作为 Zerocash 的首个实现,构建了完全独立的区块链,其原生数字货币 ZEC 通过挖矿直接生成,采用可选的隐私交易模式(透明地址与屏蔽地址并存),并通过 zk-SNARK 验证交易有效性。

Zerocoin^[72]通过承诺机制和零知识证明来切断存钱和取钱之间的联系,从而保护用户隐私。用户将 Zerocoin 存入公共 Zerocoin 池中,当需要花费时随机选择等值 Zerocoin,以此阻断存取链路的可追溯性,从而保护用户隐私。

Zerocash^[73]作为 Zerocoin 的升级版,采用 zk-SNARK 技术实现更全面的隐私保护。相较于 Zerocoin 仅隐藏接收者且不隐藏金额的局限性,Zerocash 能完全隐匿交易的发送者、接收者及金额,使得区块链数据无法用于交易追踪。此外,其通过优化 zk-SNARK 技术显著提升交易效率与隐私保护能力。

Zcash^[74]基于 Zerocash 协议,作为隐私保护型数字货币,在 Zerocash 基础上引入选择性透明机制,允许用户自由选择透明地址或隐私地址,既简化隐私交易流程,又提高交易速度,从而在隐私保护、可用性和性能方面显著提升。

Railgun、Tornado Cash、zkMixer、MixEth 和 Méobius^[75]都是基于以太坊的混币技术。

Railgun^[11]是以零知识证明为核心的混币技术,其可以完成动态反洗钱筛查,通过 1 小时链上冻结期自动检测数字货币来源,并结合 Chainalysis 和 OFAC

黑名单拦截非法资金;当发现可疑交易时自动退回原地址,同时生成加密“无罪证明”供监管机构验证合法性。

Tornado Cash^[37]是一种基于以太坊的去中心化隐私保护技术,旨在通过零知识证明实现数字货币交易的匿名化。其核心功能是打破交易中存款地址与提款地址之间的可追溯性,从而保护用户隐私。Tornado Cash 混币过程的核心在于零知识证明技术的应用;通过该技术,用户可以在不泄露个人信息的情况下进行数字货币转移。

zkMixer^[12]同样是基于以太坊的去中心化混币,其与 Tornado Cash 的逻辑基本相同,但是它在存款进入匿名池之前添加了“预验证”阶段,由验证者网络进行审查和批准,会对每笔可疑存款进行冻结、退款或没收的投票表决。

MixEth^[76]的零知识证明技术用于验证混洗负责人是否正确地对输出地址进行了混洗。相比之下,在 Tornado Cash 中,零知识证明的作用是允许用户在不泄露真实身份的情况下证明其有权提取数字货币。

Méobius^[75]采用可链接环签名证明自己对其某笔数字货币的所有权。虽然零知识证明在隐私保护强度与抗分析能力上显著优于可链接环签名,但其效率瓶颈与可信设置依赖限制了应用范围;而环签名通过轻量级验证和动态匿名集合平衡了隐私与性能,更适合需快速响应的场景。

5.2 中转型混币应用系统

本小节将对混币应用系统进行分类研究,按照技术原理分为托管式中转与存取式中转,并分析其安全保障机制。

如表 4(“√”表示混币系统具有这种安全保障机制,“×”表示没有,“?”表示并未说明)所示,中转型混币应用系统以托管式为主,大约占 72%。从运行平台来看,约 77%只运行在比特币上,这和合并型类似。且多数应用系统无需用户注册,支持 Tor 网络、不保留用户交易日志;同时,少数使用信用保障书。

下面我们介绍三个代表性的中转型混币应用系统,分别属于托管式(Coinomize),存取式(ChipMixer)和混合方式(Bitcoin Blender)。

Coinomize^[102]是一个自动转发的混币应用系统。用户输入最多五个比特币地址,然后将要混合的数字货币发送到新生成的地址。Coinomize 混合用户的数字货币,且不会保存用户的任何日志与 IP 地址。混合过程完成后,Coinomize 将在用户选择的时间延迟内发送比特币到指定地址。

表 4 中转型混币应用系统

混币应用系统	技术原理	支持货币类型	跨链	安全保障			
				信用保障书	无日志	无需注册	Tor 网络
YoMix ^[92]	托管式	BTC	×	?	✓	✓	✓
CoinMixer ^[93]		BTC	×	✓	✓	✓	✓
BitCloak ^[94]		BTC	×	✓	?	✓	✓
Bitcoin Laundry ^[95]		BTC	×	?	✓	✓	✓
Mixer, money ^[96]		BTC	×	✓	✓	✓	✓
MixTum ^[97]		BTC	×	✓	✓	✓	✓
FastSwap ^[98]		BTC, ETH, USDT, BNB 等	✓	?	✓	✓	×
Mixtura ^[99]		BTC	×	✓	✓	✓	✓
Cee, Cash ^[100]		BTC, ETH, USDT, BNB 等	✓	?	✓	✓	×
BestSwap ^[101]		BTC, ETH, XMR, USDT, HUSD 等	✓	?	✓	✓	×
Coinomize ^[102]	存取式	BTC	×	✓	✓	×	✓
Tumbler ^[103]		BTC	×	?	✓	✓	✓
Tornado Cash ^[37]		ETH, DAI, cDAI, USDC, USDT 和 WBTC	×	✓	✓	✓	✓
BitcoinFog ^[104]		BTC	×	✓	✓	×	✓
ChipMixer ^[105]	可托管 可存取	BTC	×	✓	✓	✓	✓
Bitcoin Blender ^[106]		BTC	×	✓	✓	×	✓

ChipMixer^[105]旨在通过随机化交易路径增强用户匿名性。其核心特点包括:用户对混币过程的完全自主控制、确保输出数币可互换性以降低被溯源风险、即时访问混合后的数币、无手续费(采用自愿捐赠模式)。

Bitcoin Blender^[106]则为用户提供了存取和转发两种方式,根据用户意愿,可设置钱包地址为自动提款,在延迟时间到达时,将会自动将用户的资产转发到用户的提款地址中。并且它为用户提供了使用混币的指南,以更好地提高交易的匿名性,例如:存款到多个地址、延迟提款、提款到多个地址、混合输入与混合输出。

5.3 Tornado Cash

Tornado Cash 是基于零知识证明在以太坊上运行的存取型去中心化混币,其拥有区块链上最庞大的隐私资产池^[107]。Tornado Cash 的核心机制为用户将数币存入智能合约后,可凭借零知识证明在任意时间将资产提取至新地址,从而切断资金流的链上关联。

本研究基于 Du 等人^[108]构建的数据集,该数据集覆盖 2019 年 12 月 16 日至 2022 年 3 月 31 日期间的 225979 条 Tornado Cash 交易数据与 103 条真实的存款-取款交易对。基于此,本研究重点针对交易活跃时段分布及存款至取款的时效间隔展开分析。

5.3.1 交易活跃时间

如图 7 所示,我们将 Tornado Cash 的原始交易数据分为存款和取款两部分,并按小时统计交易发生的次数及每笔金额。通过分析,发现以下规律:存款与取款交易次数基本呈现同步波动,二者均于北

京时间 7:00 达到峰值,对应欧洲中部时间 22:00-23:00、北美东部时间 14:00-15:00 以及亚洲主要地区上午时段(如东京 8:00、新加坡 7:00),形成跨时区协同的交易高峰。交易总金额的变化趋势与取款、存款次数的趋势基本相同,在 7:00 达到峰值后呈下降趋势,直到 16:00 才逐渐上升。

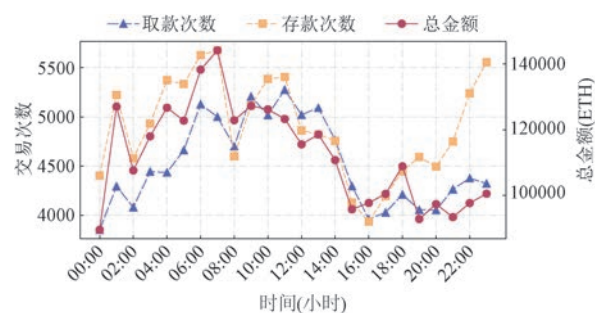


图 7 Tornado Cash 交易总金额与交易次数的时间分布

5.3.2 交易间隔分布

交易间隔指的是用户存款到取款的时间间隔。Tornado Cash 存取交易存在一对一与多对多两种形式:前者指用户使用单一账户存款并取款,后者则为用户在不同时间通过多个账户存款并取款。

通过数据清洗排除取款时间早于存款时间的错误记录后,最终保留有效存款-取款交易对 86 组,其中包含 32 组一对一交易与 54 组多对多交易。

如图 8 所示,本研究通过分析两种交易形式的存取间隔分布发现,虽然二者均呈现长尾分布特征,但一对一交易的时间间隔总体较短,而多对多交易由于多次存入和取出操作,导致存取时间间隔显著延长。

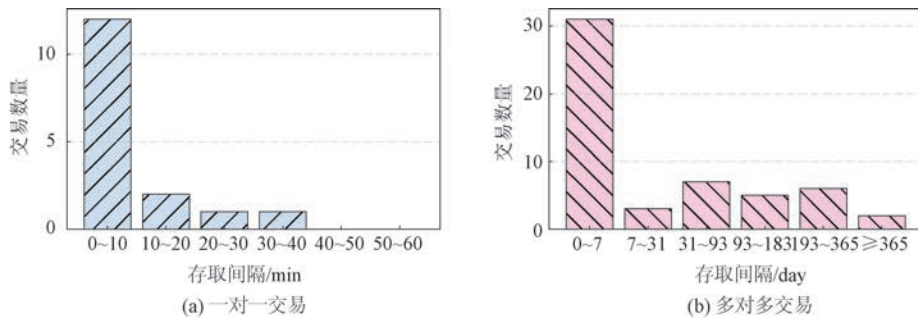


图8 Tornado Cash 交易间隔分布

具体而言,在一对一交易中,68.75%的交易在24小时内完成,其中约50%的存取操作集中在1~36分钟区间,平均间隔仅10分48秒。相比之下,多对多交易中35%的存取间隔在30分钟以内,而55%分布在72小时以内。值得注意的是,大部分交易时间集中在一周内,这表明用户普遍偏好即存即取模式。

尽管长期间隔更利于匿名性,但47%的用户选择在1天内完成交易,64%的用户在1周内完成,这一现象表明多数用户倾向于快速操作。究其原因,短期取款虽能快速实现匿名性,但其时间间隔较短,可能增加时序分析攻击的风险;反之,长期取款通过延长资金沉淀时间可有效降低交易关联性,从而增强隐私保护效果,但过长的延迟会带来资产价格波动风险及流动性问题。

5.4 小 结

本节介绍了中转型混币的两类技术,包括托管式与存取式混币技术,并进行了系统分析,介绍了其代表性技术及应用系统。中转型混币通过在交易过程中引入混币中介或智能合约,将原始交易拆分为存款与取款(或转发)两个阶段,从而在时间维度上切断交易关联。

中转型混币具备更强的隐私保护能力,可实现输入与输出的完全解耦。部分方案还通过智能合约自动化执行,进一步提升系统安全性与透明度。然而,相比合并型混币,中转型混币的实现复杂度以及计算成本更高。另外,大约80%的托管式混币技术需要混币中介,有单点故障的风险,存取式混币虽然大多不依赖于混币中介,但是需要复杂的证明生成与验证过程,导致部署与使用成本上升。

6 混币发展趋势及新的进展

本节首先介绍区块链混币发展的趋势,之后重

点介绍近五年来新的进展(即第四阶段)。

用户的需求在不断提高,相应地混币发展需要根据用户需求变化进行调整。具体而言,用户需求可解构为:(1)基础功能性需求——实现有效的混币操作;(2)安全增强需求——构建多维度隐私保护机制;(3)效率优化需求——提升交易处理速度和操作便捷性;(4)个性化需求——支持参数可定制与增值服务。对应地,技术演进路径也可划分为四个特征鲜明的阶段,各阶段分别对应不同层次的需求迭代。

6.1 区块链混币发展的四个阶段

如图9所示,我们将混币技术的发展趋势概括为四个阶段,分别为基础技术探索、隐私保护增强、中转混币主导和多目标综合发展。

在基础技术探索阶段(2013~2014年),四种主流混币框架首次被提出。最早的合并型混币CoinJoin,通过聚合多方交易输入输出来模糊地址关联性。最早的存取式中转型混币ZeroCoin,引入零知识证明来遮蔽交易链路。最早的托管式中转型混币CoinSwap和Mixcoin也在这一时期出现,分别采用原子交换技术与可追责的第三方混合服务实现数币转发。同期也出现了第一个合并原子交易的混币Xim。此阶段的混币技术几乎全部集中于比特币平台。

在隐私保护增强阶段(2015~2017年),混币技术开始采用更多密码学工具来提升对交易隐私的保护。Monero将环签名技术引入混币,通过将用户公钥隐匿于群体公钥集合中实现发送者身份隐藏,同时结合隐匿地址技术保护接收者身份;Blindcoin、TumbleBit都使用盲签名技术,有效防止混币中介获取真实交易信息;CoinShuffle++、ValueShuffle以及SecureCoin都引入解密混合网络以避免其他参与者知晓原始交易输入和输出之间的关联。Dash则通过多中心的方式来合并交易,避免外界观察者和其他参与者知晓交易信息。

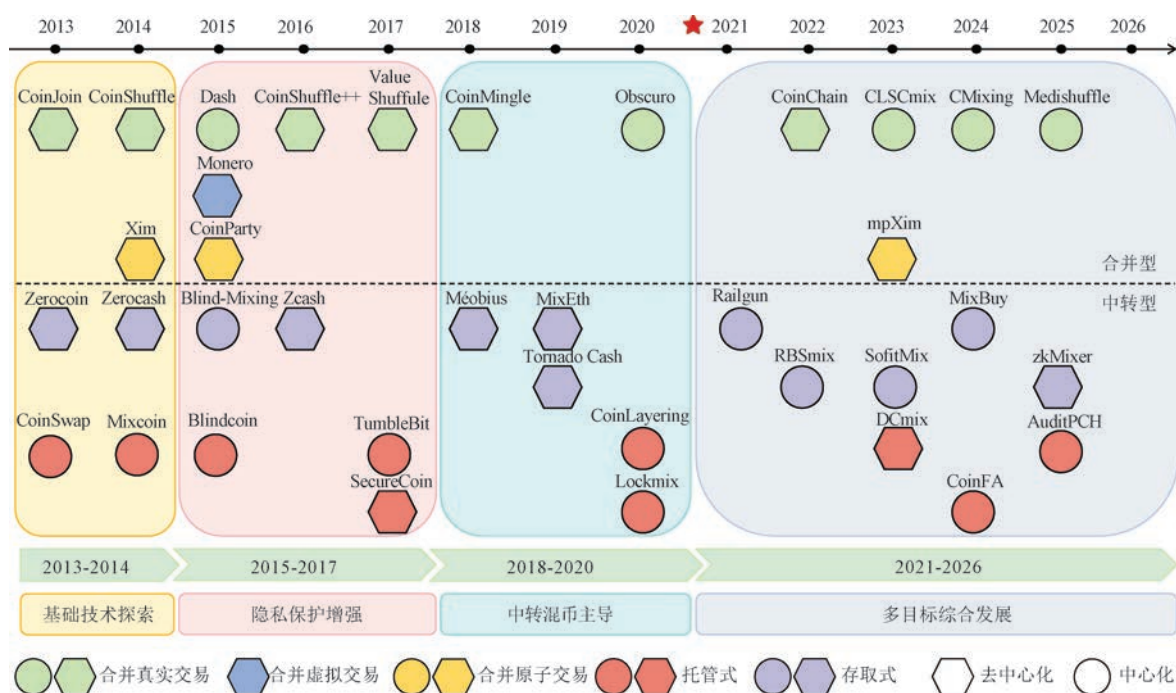


图9 混币技术时间线

2018 年到 2020 年期间出现的混币技术大多为中转型,我们称其为中转型混币主导阶段。相较于需要多个用户同时参与且周期较长的合并型混币,中转型混币凭借其单用户独立操作特性更为便捷。MixEthereum、Tornado Cash、Mebius 均为基于以太坊平台的去中心化混币,Obscuro、Lockmix 和 Coinnewline nLayering 则运行于比特币平台。这些技术均延续了对隐私保护的重视:通过零知识证明(Tornado Cash 和 MixEthereum)、盲签名(Lockmix)、环签名(Mebius)、多中介(CoinLayering)以及可信执行环境(Obscuro)等技术有效提升了交易的匿名化程度。

2021 年以来,区块链混币生态呈现出显著的范式转型,步入多目标综合发展新阶段。这一时期的技术演进不再单一追求匿名,而是转向提供更丰富的系统功能与服务体验,主要体现为:增强系统隐私保护与鲁棒性、提供可定制的个性化隐私参数、平衡隐私保护与监管合规需求,以及推动混币机制向医疗、数字交易等跨领域应用拓展。具体分类分析将在下一节详细展开。

6.2 近五年来区块链混币的新进展

2021 年以来,区块链混币沿着多条路径持续演进,整体上呈现出从单一保护匿名向增强系统隐私与鲁棒性、个性化隐私定制、监管合规设计以及跨领域应用拓展的发展态势。根据技术侧重点的不同,新出现的混币系统可大致归为四类。第一类在传统

加密货币框架内通过侧链、链下通道或新型密码学协议提升隐私强度与鲁棒性;第二类引入监管角色或链上筛查机制,尝试在隐私性与合规性之间建立平衡;第三类放弃固定的混币参数设置,转向为用户提供个性化隐私服务,例如可配置的匿名选项与交易时机;第四类则不再局限于传统的加密货币交易场景,而将混币思想应用于医疗数据共享、数字商品公平交换等其他领域。

(1)增强系统隐私保护与鲁棒性。代表性工作有 CoinChain^[7]、DCmix^[8]、SofitMix^[9]与 mpXim^[10]等方案,它们着力于在比特币等加密货币现有架构内增强隐私保护和系统鲁棒性。CoinChain 利用侧链将用户资金映射为固定面额代币,并通过链下协商切断锚定过程中的关联。DCmix 通过层次化密钥树实现前向安全,结合环签名和隐匿地址隐藏交易关系,防止事后密钥泄露导致的追溯。SofitMix 采用链下托管与零知识证明构造不可链接的支付通道,配合经济惩罚机制保障安全。mpXim 将传统双方配对扩展为多方参与的去中心化混币流程,通过广告发现、列表合并与费用激励提升单轮混币成功率。尽管具体实现手段各异,此类方案的共同目标是在不引入外部信任假设的前提下,尽可能扩大匿名集并抵御日益复杂的去匿名化威胁。下面以 DCmix 为例介绍如何增强混币过程的隐私保护。

DCmix^[8]:防止交易链路追踪并确保前向安全性。其创建层次化确定性密钥树,使节点能在不同

的混币操作中使用不同的密钥来完成签名。即使私钥泄露,攻击者仍无法解密之前使用该私钥协商的会话密钥保护的通信数据。DCmix 通过将原始交易拆分为两个交易,并利用环签名与隐匿地址技术切断原始的交易关系,隐藏真实的用户身份。

DCmix 的混币过程包含以下步骤:

①初始化:每个节点生成一个密钥树,请求节点在公告板上广播混币请求,与响应节点共同组成混币群组。

②生成聚集地址:混币群组中的每个节点从自己的密钥树中选择叶子密钥,共同生成聚集地址。

③生成环签名:收集群组中所有用户的公钥生成环签名,环签名中的公钥来自密钥树的另一个分支,而形成环签名所需的私钥则来自请求节点。

④创建交易:请求节点创建交易,将数字货币转发至聚集地址中,并使用环签名进行签名。

⑤数字货币转出:混币群组验证交易合法后,进入转出阶段。请求节点在密钥树中选择一组公私钥生成一次性地址,并将数字货币进行转出。

(2)平衡隐私保护与监管合规需求。此类方案以 Railgun^[11]、zkMixer^[12]、RBSmix^[13]与 AuditPCH^[14]为代表,主动在协议设计中融合了监管审计能力。Railgun 与 zkMixer 均在资金进入匿名池前设置延迟筛查窗口,利用链下制裁名单数据库或验证者网络对存款来源进行合法性检查,仅在通过筛查后才允许进入零知识证明保护的隐私交易环节。RBSmix 引入了中央机构与监管者角色,将用户身份信息分片加密并由多个监管者协同盲化签名,日常混币时混币节点仅接触盲化身份,一旦发现非法输出地址,执法机构可启动跨监管者解密流程以锁定真实身份。AuditPCH 则在支付通道架构中嵌入可链接随机化谜题,混币中介无法关联发送方与接收方,但监管者持有陷门即可还原完整的支付链路。四类方案均体现出一种明确的趋势:混币协议在设计之初便为受信任的监管实体预留了审计接口或追溯手段,以求在满足个人隐私期望的同时回应反洗钱与制裁合规的要求。下面以 AuditPCH 为例介绍此类混币。

AuditPCH^[14]:通过引入可链接随机化谜题这一密码学原语,在保障混币中介无法知晓发送方与接收方的关联的同时,从而使得监管者可以追溯交易链路。AuditPCH 的混币流程包含以下步骤:

①建立支付通道:发送方与接收方分别与混币中介在区块链上建立支付通道并锁定资产。监管者

生成系统参数和用于审计的陷门(私钥)。

②链下中继支付:发送方希望向接收方付款时,混币中介会为接收方生成一个谜题。接收方和发送方依次对该谜题进行随机化处理,使得混币中介无法将最终提交的谜题与初始谜题关联。发送方随后向混币中介发起一笔条件支付,该支付的有效性取决于混币中介能否解开随机化后的谜题。

③解谜:混币中介利用其私钥解开谜题,完成发送方至混币中介的支付。解开的秘密经发送方传递给接收方,接收方凭此最终完成混币中介至自身的支付,确保交易的原子性。在此过程中,混币中介会记录下所有谜题和支付凭证作为审计线索。之后发送给监管者。

④监管:监管者利用其持有的陷门,将通道内看似无关的支付对进行密码学链接,从而还原出发送方到接收方的交易关系,实现有效监管。

(3)提供参数可定制的个性化隐私服务。CMixing^[15]、CoinFA^[16]与 CLSCmix^[17]区别于以往系统强制统一面额或固定周期的做法,转而将选择权交还给用户。CMixing 引入 c -分解概念,允许交易者指定输出金额的混淆强度参数,协调者据此规划 CoinJoin 交易结构。CLSCmix 支持用户自主设定混币等待时长,并利用无证书签名技术使得参与者无需在线等待协议完成。CoinFA 进一步允许付款人与收款人自定义混币金额,通过多混合节点交互与谜题-解密机制实现灵活的资金交换。这类方案的出发点在于,不同用户对匿名程度的实际需求存在显著差异,固定的系统参数难以同时满足时效性与安全性的双重期望,因而将选择权交还给用户有助于提升整体的使用体验与接受度。下面我们以 CMixing 为例介绍此类混币。

CMixing^[15]:通过用户可选的匿名保证提升用户体验。在 CMixing 中,引入了 c -分解的概念。 c -分解要求来自同一原始输出且金额为 x 的分解输出比例不超过 c 。CMixing 的混币过程包含以下步骤:

①发送请求:用户填写原始交易的详细信息和隐私要求(c 值),并向一个活跃的协调者请求。

②制定混币交易策略:协调者对交易请求进行分组,并使用协调算法为每组创建一个混币交易。如果协调者需要协调的金额超过预算,则混币交易失败。

③生成输出:每个交易者根据 CoinJoin 交易计划生成分解的输出,并提交这些输出。协调者将使用这些 UTXO 进行交易。

④组装交易:协调者将来自同一 CoinJoin 交易计划的已用交易输出和分解输出组合在一起,创建 CoinJoin 交易,并通知交易者。如果交易者同意混币交易,则对其进行签名。

⑤提交混币交易:如果协调者收集到所有交易者的签名,则将混币交易提交至区块链,并通知交易者。

(4)混币技术向跨领域应用拓展。MixBuy^[18]与 Medishuffle^[19]将混币的去关联化思想从单纯的价值转移延伸至具体的业务场景。MixBuy 针对数字商品交易中的公平交换问题,在半信任公证人协助下构建了不可链接的条件支付流程。Medishuffle 面向医疗物联网数据共享的隐私与审计要求,采用基于多项式的群签名代替传统多层加密,患者、医院等参与者在逻辑分组内通过洗牌方式混淆数据输出地址。这两项工作表明,混币思想作为一种去关联化的通用工具,已开始渗透至隐私计算、数据共享等更广泛的领域。下面我们介绍 MixBuy 的工作过程。

MixBuy^[18]:在存在混币的场景下实现的不可链接条件支付方案。该方案不仅隐藏了资金的流向,还保证了买卖双方的公平交易(即买方付款必得商品,卖方交货必得货款)。MixBuy 引入了一个半信任的公证人节点,其混币过程包含以下步骤:

①建立共享地址与商品准备:买方与混币中介建立包含买方资金的共享地址,混币中介与卖方建立包含混币中介资金的共享地址。卖方将数字商品加密,并向买方提供该加密商品及零知识证明。

②谜题承诺:混币中介生成一个包含向卖方付款签名的可随机化谜题并发送给卖方;卖方对该谜题进行随机化盲化处理后,将新谜题发送给买方。

③谜题链接:买方将盲化谜题发给混币中介,混币中介将其重加密为“认证谜题”(只有当公证人证明买方已付款时才能解开)并发给卖方。卖方确认后,将商品解密密钥也加密为一个认证谜题发给买方。

④证明与解谜:买方链上发布向混币中介的付款交易。公证人监控到该交易后发布认证信息。买方利用该认证信息解开谜题获取商品解密密钥;同时,卖方利用该认证信息解开谜题获得混币中介的付款签名,从而在链上提取资金。

新的进展表明:当前混币技术已从单纯追求绝对匿名向增强系统隐私性与鲁棒性、用户个性化隐私定制、监管合规技术与跨领域应用的多目标体系

演变。一方面,侧链扩展、前向安全密钥、零知识证明与多方配对等机制提升了协议自身的抗攻击能力与执行效率;另一方面,监管接口的预置与场景化适配成为新系统不可或缺的组成部分。在多重演进趋势中,如何在匿名保护与可监管性之间取得切实可行的平衡,已构成当前区块链混币发展的最大挑战,我们将在下一节对此进行详细探讨。

7 核心挑战分析

区块链混币本意是为了保护用户的交易隐私,从技术层面提供匿名化支持,然而却被不法分子利用,成为洗钱等非法交易的温床。为了维护金融秩序,监管方从技术和司法两方面加强了对非法交易活动的监控和打击,这些措施也影响了混币系统的正常运营,对区块链混币生态带来了严峻的挑战。

7.1 非法交易带来的挑战

近年来,利用混币系统转移非法资金的事件屡见不鲜。虽然全球监管机构加大了打击力度,但混币仍是加密犯罪生态中重要的洗钱工具。根据 Chainalysis 发布的《2025 年加密犯罪报告》,虽然受到制裁影响,但混币服务长期占据勒索软件季度洗钱资金流的 10% 至 15%^①。在 2024 年“私钥泄露”类案件中(占被盗资金总额 43.8%),混币被黑客作为具有显著偏好的核心洗钱路径,其使用频率远超去中心化交易所。同时,新型替代混币器层出不穷,例如在 Sinbad 被封停后,YoMix 混币器的资金流入在短短一年内激增了 5 倍以上,其中约三分之一的流入资金直接与加密货币黑客攻击相关^②。

混币频繁被网络诈骗分子用于洗钱。2023 年 9 月,号称“区块链创新项目”的华英会骗局崩盘,涉案金额高达 2.8 万亿元人民币,超过广州市 2022 年全年 GDP。该犯罪团伙要求投资者将 USDT 打入临时生成的钱包地址后,通过混币转移到币安、OKX 等境外交易所,成功切断资金追踪路径^③。类似手法在江苏句容警方破获的网络诈骗案中也有体现,犯罪分子同样利用混币资金池混淆 1200 余万元涉案资金的流向^④。

在暗网非法交易领域,犯罪分子同样利用混币

① <https://go.chainalysis.com/rs/503-FAP-074/images/2025-Crypto-Crime-Report.pdf>.

② <https://www.chainalysis.com/blog/2024-crypto-money-laundering/>.

③ <https://zhuanlan.zhihu.com/p/1898036961345777760>.

④ <https://www.chinanews.com.cn/sh/2023/02-01/9944757.shtml>.

切断交易路径。2025 年香港警方破获的 3.2 亿美元跨境洗钱案中,犯罪集团通过暗网市场 Nemesis Market 接收非法资金后,使用 CoinMixer 进行多轮混币操作,最终将资金转移至东南亚极端组织^①。调查显示,暗网市场与混币器往往通过智能合约实现自动化结算,其中 Helix 的服务器日志显示,每日有超过 2000 笔非法资金在此“漂白”,涉及 AlphaBay 等暗网市场、华尔街 OTC 柜台以及东南亚赌场资金^②。

黑客攻击后的资金转移同样依赖混币系统。据统计,近年来全球加密领域黑客窃取资金规模呈现出增长趋势,从 2023 年的 560 亿美元、2024 年的 500 亿美元,攀升至 2025 年的 590 亿美元,并在 2026 年激增至 1540 亿美元^③。例如,2023 年价值 2 亿美元的 Mixin Network 被盗案,其黑客沉寂两年后,在 2026 年 2 月仍选择将约 385 万美元的比特币分 20 次通过 Tornado Cash 进行洗钱^④。2025 年 Bybit 交易所 15 亿美元 ETH 被盗案中,黑客先通过 THORChain 跨链桥将 ETH 转换为比特币,再经由 eXch 等混币器清洗,利用比特币网络的匿名性切断资金链^⑤。TRM Labs 的数据进一步证实,尽管面临制裁,Lazarus 集团等犯罪组织在实施了 Ronin 桥 6.25 亿美元大劫案后,依然依赖 Tornado Cash 和比特币混币服务进行赃款变现,导致涉制裁混币池中的非法资金比例继续攀升^⑥。

7.2 监管技术对交易隐私保护带来的挑战

交易隐私保护是用户对区块链混币最基础的要求。近年来,学术界提出多种区块链混币去匿名化方法,希望通过识别混币交易或重建输入输出地址关联来还原原始交易。

识别混币交易是在区块链中识别出哪些交易是由混币交易系统产生的,目前主要采用启发式方法和机器学习与深度学习。

启发式方法是指通过设计特定的启发式规则来过滤区块链交易或地址,并通过统计混币相关信息(比如交易金额、交易时间、交易模式等)来寻找与混币相关的交易和地址^[109-113]。其中,Tippe 等人^[112]利用图数据库技术剖析了混币的“剥离链”与延迟分配等交易模式,为混币追踪提供了实证支持;Ziegler 等人^[113]则开发了开源取证框架 Dakar,内置多种启发式算法以实现 CoinJoin 交易的自动化提取与标签化,有效降低了分析门槛。在实际应用中此类方法成效显著,如 Lei Wu 等人^[111]成功识别出了 9335 笔与 Chipmixer 相关的混币交易,其识别率超

过 92%。

机器学习与深度学习通过挖掘区块链交易数据的统计特征与网络模式,结合分类模型和集成策略,实现混币交易检测。具体方法包括社区异常检测^[114]、随机森林^[115]、无标记学习^[116]、双集成模型^[117]、深度神经网络^[118-119]等,其中 Hanzhi Yang 等人^[119]设计了 STMD(Spatio-Temporal Mixing Detector)方法,其准确率、召回率、F1 Score 均达到了 98%以上。

重建输入输出地址关联指通过分析交易特征,建立资金存入地址与提款地址之间的关联关系,从而揭示资金流转的隐蔽路径。主要技术包括启发式方法和深度学习。

启发式方法的核心目的是通过人工设计的规则或特征(如资金守恒假设),实现重建输入输出地址关联的目标。启发式方法主要包括:直接建立映射、污点分析、地址聚类三种方法。

第一类启发式方法是直接建立映射,即基于交易数据特征设计确定性关联规则,直接建立输入输出地址映射^[20,120-122]。其中 Yousaf 等人设计的方法^[20]针对跨链混币建立跨链地址关联规则,能够同时识别出存款和取款交易的平均成功率达到 81.91%,其他方法都是针对单个区块链平台。

第二类启发式方法是污点分析,通过标记某一地址为污染源,追踪从该地址输出后的所有交易分支。Wu 等人^[123]提出了一种基于污点分析的综合资金追踪框架 ETTracker,通过构建统一多边有向图并结合图神经网络进行资金追踪。此外,Arango 等人^[124]提出了一种污点分析规则 HOLO,优先标记最高和最低金额的输入,以应对混币中常见的“剥离链”干扰,最终 OI 启发式平均减少 78% 无关地址,HOLO 成功标记 46% 暗网关联地址。

第三类启发式方法是地址聚类,通过分析区块链上的交易模式,将多个看似独立的地址归并为同一用户或实体。Larionov 等人^[125]针对共享发送混币对共同花费和一次性找零等经典聚类规则的干扰问题,引入了解卷技术,一定程度上修正了启发式聚类中的误报现象。Wu 等人^[126]根据交互历史将以

① <https://baijiahao.baidu.com/s?id=1827863046244750878>。

② <https://baijiahao.baidu.com/s?id=1826811340206957213>。

③ <https://www.chainalysis.com/reports/crypto-crime-2026/>。

④ <https://finance.yahoo.com/news/3-85-million-ethereum-mixin-175053959.html>。

⑤ <https://www.120btc.com/zxgg/543835151.html>。

⑥ <https://www.trmlabs.com/resources/blog/tornado-cash-volume-dramatically-reduced-post-sanctions-but-illicit-actors-are-still-using-the-mixer>。

太坊地址聚集在一起,认为被聚集的交易之间存在关联,该方法将 Tornado Cash 各资金池的平均匿名集大小减少了 37%。

深度学习方法主要将交易数据建模为图结构,利用图神经网络(GNN)的嵌入学习自动挖掘地址间的关联。Du 等人^[108]提出的 MixBorker 框架将混币重连转化为链路预测问题。针对其在高阶信息利用和时间建模上的不足,Wang 等人^[127]提出 MixLinker,引入张量长短期记忆网络进行多维建模,提升了重连性能。进一步地,Tu 等人^[128]针对标签噪音与稀缺挑战提出 HiLoMix 框架,通过构建异构属性混币交互图并结合频率感知对比学习,显著增强了模型的鲁棒性。实验结果显示,HiLoMix 的 AUC 达到 0.9137,F1 分数达到 0.8382。

在 2024 年 3 月美国司法部(DOJ)针对混币器 Bitcoin Fog 的定罪案件中,执法部门通过数据取证软件(如 Chainalysis Reactor)运用了共同花费启发式聚类技术,并结合链下情报(如 IP 地址关联和交易所服务器记录),成功实现了对平台操控者的去匿名化追踪。法庭证据明确还原了该混币系统自 2011 年以来处理的超过 120 万枚比特币(涉案时值约 4 亿美元)的洗钱网络^①。

7.3 监管制度带来的挑战

在立法方面,全球监管机构正通过立法填补混币监管空白。欧盟于 2023 年正式通过《加密资产市场监管法案(MiCA)》及配套的《资金转移条例(TFR)》^②,并在 2024 年颁布《新版反洗钱条例(AMLR)》^③。该法律框架强制加密资产服务商(CASPs)执行旅行规则(Travel Rule),要求每笔转账必须穿透识别发起人与受益人身份,并明确禁止 CASPs 为混币等匿名增强工具提供服务。美国则通过《银行保密法》将混币视为“货币传输业务”,要求其遵守 KYC 和 AML 规则,并联合 Chainalysis 等公司开发 UTXO 追踪协议,专门破解比特币混币交易^④。中国最高检首次将虚拟货币洗钱列为重点打击对象,司法机关在 2023 年对涉虚拟货币案件采取“穿透式”监管原则,强化法律适用^⑤。

在司法方面,2022 年 Tornado Cash 协助黑客组织 Lazarus 洗钱 4.55 亿美元,美国司法部耗时两年才通过区块链分析工具锁定资金流向^⑥,2024 年 5 月其创始人 Roman Storm 因协助洗钱 22 亿美元获刑 64 个月^⑦。Helix 因协助洗钱,其运营者 Larry Harmon 被没收 2 亿美元比特币^⑧。中国司法机关在鄂州虚拟货币诈骗案中,首次采用“链上数据+线

下行为”复合证据链模式,将 34 名被告人的混币操作与 3 万名受害者的资金损失建立关联^⑨。2024 年币安创始人赵长鹏因平台洗钱漏洞被判 4 个月监禁,尽管未直接涉及混币,但暴露了交易所对资金流向的监控失效。

7.4 区块链混币未来发展思考

上一小节我们分析了区块链混币面临的若干严峻挑战。除此之外,如果区块链本身遭受攻击,那么混币系统也不能独善其身。比如量子计算的发展,特别是 Shor 算法的潜在应用,也可能动摇混币所依赖的密码学安全根基,并可能催生新型攻击模式。

面临这些挑战,混币必须采用更先进的安全防护手段,比如采用跨链桥接等跨链混币手段来进一步打断资金路径、躲避监管,更深入地使用零知识证明等密码学工具来增强匿名性、对抗去匿名化攻击,以及采用后量子密码学等技术来应对量子计算的攻击等。

需要强调的是,监管与区块链混币并非完全对立的。监管的矛头主要指向利用混币从事洗钱等非法活动的黑客组织,而区块链混币的初心在于维护合法用户的交易隐私。如果强行要求去混币化,用户合理的隐私保护需求不能被满足,不利于区块链生态繁荣。如果完全无视监管的需要,混币必然继续成为犯罪活动的温床,最终将受到政府的打击。

近年来,部分区块链混币系统开始探索和监管共存之路,其中典型代表是 Railgun 和 RBSmix。这两个混币的特点我们已在前面介绍,此处只介绍一个混币平台主动和监管配合的实例。

2025 年 2 月 12 日,Starknet 生态借贷协议 zk-Lend 遭受黑客攻击导致 500 万美元损失,涉案资金经 Railgun 平台混币后,凭借其强化反洗钱机制被成功追回。Railgun 通过实施严格合规策略,在确保隐私保护的同时满足监管要求,有效阻断了非法资金流动^⑩。

① <https://www.moneylaunderingnews.com/2024/03/blockchain-analysis-and-related-expert-testimony-admissible-in-criminal-trial/>。

② <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>。

③ <https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng>。

④ <https://baijiahao.baidu.com/s?id=1827863046244750878>。

⑤ https://www.spp.gov.cn/spp/2025qgjczh/202501/t20250115_679734.shtml。

⑥ <https://weibo.com/ttarticle/p/show?id=2309404801228017369328>。

⑦ <https://news.qq.com/rain/a/20240516A06HJM00>。

⑧ <https://www.jinse.cn/blockchain/3698745.html>。

⑨ <https://www.chinacourt.org/article/detail/2025/03/id/8764823.shtml>。

⑩ <https://news.qq.com/rain/a/20250214A07ZHH00>。

任何一个持续繁荣的生态,都不可能与国家监管体系对抗。我们相信未来一定会出现更多兼顾监管要求和用户隐私保护需求的区块链混币系统。这些系统既能在技术层面保证合法用户的交易匿名性,又能使得监管机构可以及时发现非法交易活动并追踪相应的账户。

根据上述对区块链混币的发展趋势以及其面临的挑战分析,我们认为区块链混币未来发展目标应包括以下三点:

(1)隐私保护:能有效应对混币去匿名技术带来的挑战,增强对合法用户的交易隐私保护。

(2)服务提升:持续提升混币的性能或提供更多增值服务。

(3)监管合规:根据监管机构要求,对混币交易实施事前-事中-事后的全链路管控。

在增强隐私保护方面,可通过融合跨链混币技术阻断单链交易连续性,同时针对混币需求改进零知识证明与环签名等密码学技术,并在中转型混币中引入随机提款时间机制。

在服务提升方面,需增强系统可扩展性及增值服务能力;例如提供多样化混币模式选择、简化交易流程;支持单次操作完成多链资产混合;引入深度学习驱动的智能混币策略推荐;优化付费模型以降低经济成本等综合措施。

下面我们重点讨论监管合规的实现路径,这也是未来混币系统的核心难点。根据是否依赖于可信执行环境,我们设计了两条技术路线:

(1)不依赖可信执行环境,构建覆盖事前、事中、事后的全流程监管体系:

①事前:在执行用户的混币请求之前,先根据监管要求以及反洗钱机构提供的信息进行合规性检查,具体可以分为账户合规和交易合规。所谓账户合规,可以采用黑白名单结合可验证计算(或零知识证明),确保参与混币交易的账户不在已知的非法账户名单中。部分可验证计算技术,如Merkel树,可能需要向混币系统或监管方披露账户地址。采用零知识证明能够避免暴露交易账户地址,但会引入较为昂贵的计算开销。所谓交易合规,则是在混币合约中考虑监管的要求,屏蔽触犯监管规则的交易。最新的工作^[12]中,已看到采用零知识证明技术实现此类功能。事前监管需要事先明确监管要求(黑白名单,监管规则),灵活性较差,并且也需要公开监管的具体要求。

②事中:在单个混币交易或一系列混币交易(比如某次洗钱行动)的执行过程中分析评估混币交易

的行为,如果触犯监管要求,则实时阻断交易。一方面,可以采用机器学习技术分析链上公开记录的交易数据,实时评估混币交易违法的可能性。另一方面,可以设计监管友好的混币合约,允许监管方动态施加监管规则,或在合约中嵌入监管审计功能,向监管方定向传送不在链上记录的数据,以帮助监管方更好地发现可能的违法交易并实施及时管控。

③事后:通过非对称加密,属性基加密等技术将涉案账户信息(包括这些账户过往的历史行为)提交给监管机构,以帮助监管方迅速追责。在AuditPCH^[14]等系统中,所有混币交易的数据都需要采用监管方公钥加密存储,向监管方公开。但是这种做法必然导致用户交易隐私的泄露,混币系统需要在监管能力和用户隐私保护之间合理取舍。

(2)依赖可信执行环境,即混币系统运行在可信执行环境中。

由于可信执行环境的存在,混币系统可以拿到原始交易的信息。因此发现非法交易时,混币系统能够将原始交易的全部数据(包括账户)提交给监管机构。根据系统所采用的TEE硬件,须设计相应的侧信道攻击防范技术,比如代码随机化、恒定时间编程等,以增强对交易数据的保护。此外,为平衡隐私保护和监管需求并权衡性能和安全,也需要设计合理的披露策略。比如,设计分级审计机制,根据混币交易的风险等级设计不同的披露策略。此外,由于TEE的远程证明依赖于硬件厂商提供的信任根,为了降低单点依赖风险,还需要考虑自定义信任根或多重信任链技术以降低对硬件的依赖。

8 总 结

本文系统探讨了区块链混币技术的核心机制,其通过切断交易输入输出间的关联性有效隐藏资金流向路径,为用户提供可靠的隐私保护。首先,本文将混币技术划分为合并型与中转型两大基础模型,并在此基础上构建了三层分类框架,系统揭示技术原理差异。基于该框架深入剖析了密码学技术在混币机制中的应用特征与作用方式,进而系统梳理技术演进脉络。本文总结并分析了近五年来混币生态发生的范式转型:即系统设计已从单纯追求匿名的传统模式,演变为兼顾多目标的复杂体系。最后,本文指出当前面临的三大核心挑战,并指出未来区块链混币发展的方向,提出平衡监管需求与隐私保护的技术路线。

参 考 文 献

- [1] Philip Koshy, Diana Koshy, Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic//Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2014:469-485
- [2] Fergal Reid, Martin Harrigan. An analysis of anonymity in the bitcoin system. Security and privacy in social networks. Springer, 2012:197-223
- [3] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, Srdjan Capkun. Evaluating user privacy in bitcoin//Proceedings of the 17th International Conference on Financial Cryptography and Data Security. Okinawa, Japan, 2013:34-51
- [4] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names//Proceedings of the 2013 Conference on Internet Measurement Conference. Barcelona, Spain, 2013:127-140
- [5] Hirshman J, Huang Y, Macke S. Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network. Stanford, USA: Stanford University, Technical Report, 2013
- [6] Dominic Deuber, Dominique Schröder. Coinjoin in the wild: An empirical analysis in dash.//Proceedings of the Computer Security-ESORICS 2021: 26th European Symposium on Research in Computer Security, Part II 26. Darmstadt, Germany, 2021:461-480
- [7] Wai Kok Chan, Ji-Jian Chin, Vik Tor Goh. Coinchain: Effective coin mixing tool for anonymous cryptocurrency//Proceedings of the 8th International Conference on Computational Science and Technology: ICCST 2021. Labuan, Malaysia, 2022: 647-659
- [8] Jingting Xue, Lingjie Shi, Liang Liu, Xiaojun Zhang, Fagen Li. Anonymity-enhancing decentralized protocol for coin mixing based on ring signatures and key derivation. Peer-to-Peer Networking and Applications, 2023,16(6):2761-2774
- [9] Haomeng Xie, Shufan Fei, Zheng Yan, Yang Xiao. Sofitmix: a secure offchain-supported bitcoin-compatible mixing protocol. IEEE Transactions on Dependable and Secure Computing, 2023,20(5):4311-4324
- [10] Wang X, Liao L, Cao D. mpXim: a decentralized mixing scheme based on a multi-party discovering protocol//Proceedings of the 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion. Chiang Mai, Thailand, 2023:263-272
- [11] RAILGUN DAO, Community Contributors. Railgun-on-chain zero knowledge privacy ecosystem. 2021. URL <https://railgun.org/>
- [12] Theodoros Constantinides, John Cartledge. zkmixer: A configurable zero-knowledge mixer with proof of innocence and anti-money laundering consensus protocols. arXiv e-prints, 2025
- [13] Rongyu Xiao, Guozi Sun, Jiale Yang, Yao Wang, Puhe Hao. Rbsmix: A regulatable privacy-preserving method for cryptocurrency. Wireless Communications and Mobile Computing, 2022(1):7125472
- [14] Yuxian Li, Jian Weng, Junzuo Lai, Yingjiu Li, Jianfei Sun, Jiahe Wu, Ming Li, Pengfei Wu, Robert H Deng. Auditpch: auditable payment channel hub with privacy protection. IEEE Transactions on Information Forensics and Security, 2024, 20:1251-1261
- [15] Wangze Ni, Yiwei Zhao, Pengze Chen, Lei Chen, Peng Cheng, Chen Jason Zhang. Cmixing: An efficient coin mixing platform to enhance anonymity in cryptocurrency transactions//Proceedings of the VLDB Endowment. Guangzhou, China, 2024,17(12):4405-4408
- [16] Xin Yang, Peng Zeng, Kim-Kwang Raymond Choo, Chengjiu Li, Yanzhao Yang. Coinfa: an efficient coin mixing scheme with flexible amounts. The Computer Journal, 2024, 67(12): 3141-3150
- [17] Far S B, Asaar M R, Haghbin A. A blockchain-based coin mixing protocol with certificateless signcryption. Peer-to-Peer Networking and Applications, 2023,16:1106-1124
- [18] Diego Castejon-Molina, Dimitrios Vasilopoulos, Pedro Moreno-Sanchez. MixBuy: Contingent payment in the presence of coin mixers. Cryptology ePrint Archive, Paper 2024/953, 2024
- [19] Yuan Chang, Tom H. Luan, Yinbin Miao, Qian Chen. Medishuffle: auditable coin mixing scheme for internet of medical things. IEEE Internet of Things Journal, 2025,12(18): 39088-39104
- [20] Haaron Yousaf, George Kappos, Sarah Meiklejohn. Tracing transactions across cryptocurrency ledgers//Proceedings of the 28th USENIX Security Symposium (USENIX Security 19). Santa Clara, USA. 2019:837-850
- [21] Alex Biryukov, Daniel Feher, Giuseppe Vito. Privacy aspects and subliminal channels in zcash//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019:1813-1830
- [22] Zhang Zongyang, Li Weihai, Liu Haitao, Liu Jianwei. A refined analysis of zcash anonymity. Ieee Access, 2020,8:31845-31853
- [23] Minjae Kim, Jinhee Lee, Hyunsoo Kwon, Junbeom Hur. Get off of chain: Unveiling dark web using multilayer bitcoin address clustering. IEEE Access, 2022,10:70078-70091
- [24] Wang Kai, Cheng Yakun, Michael Wen Tong, Niu Zhenghao, Pang Jun, Han Weili. Exploring unconfirmed transactions for effective bitcoin address clustering//Proceedings of the ACM Web Conference 2024. Singapore, 2024:1880-1891
- [25] Wang Kai, Pang Jun, Chen Dingjie, Zhao Yu, Huang Dapeng, Chen Chen, Han Weili. A large-scale empirical analysis of ransomware activities in bitcoin. ACM Transactions on the Web (TWEB), 2021,16(2):1-29
- [26] Ismail Alarab, Simant Pragoonwit, Mohamed Ikbil Nacer. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain//Proceedings of the 5th In-

- ternational Conference on Machine Learning Technologies. Beijing, China, 2020:23-27
- [27] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I Weidele, Claudio Bellei, Tom Robinson, Charles E Leiserson. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv preprint arXiv:1908.02591, 2019
- [28] Wai Weng Lo, Gayan K Kulatilleke, Mohanad Sarhan, Siamak Layeghy, Marius Portmann. Inspection-l: self-supervised gnn node embeddings for money laundering detection in bitcoin. *Applied Intelligence*, 2023, 53(16):19406-19417
- [29] Jourdan M, Blandin S, Wynter L, Deshpande P. Characterizing entities in the bitcoin blockchain//Proceedings of the 2018 IEEE International Conference on Data Mining Workshops. Singapore, 2018:55-62
- [30] Gibran Gomez, Pedro Moreno-Sanchez, Juan Caballero. Watch your back: Identifying cybercrime financial relationships in bitcoin through back-and-forth exploration//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York, USA, 2022:1291-1305
- [31] Simin Ghesmati, Walid Fdhila, Edgar R. Weippl. Bitcoin privacy-a survey on mixing techniques. *IACR Cryptology ePrint Archive*, 2021, 2021:629
- [32] Jaswant Pakki, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, Adam Doupe'. Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask). Nikita Borisov and Claudia Diaz, editors. *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2021:117-146
- [33] Giannikou I P. Cryptocurrencies and Mixing Services. National and Kapodistrian University of Athens, Athens, Greece, 2021
- [34] Alireza Arbabi, Ardeshtir Shojaeinasab, Behnam Bahrak, Homayoun Najjaran. Mixing solutions in bitcoin and ethereum ecosystems: A review and tutorial. arXiv preprint arXiv:2310.04899, 2023
- [35] Wang Jia-Xin, Mao Qian-Ang, Yan Jia-Qi, Yin Jie, He Yuan, Zhang Yi. A review of blockchain-based coin mixing regulatory technology. *Computer Engineering*, DOI:10.19678/j.issn.1000-3428.0070189(in Chinese)
(王佳鑫,毛谦昂,颜嘉麒等.区块链混币监管技术研究综述.计算机工程,DOI:10.19678/j.issn.1000-3428.0070189)
- [36] Mixue Xu, Chao Yuan, Xueming Si, Gang Yu, Jinhua Fu, Feng Gao. Coinmingle: A decentralized coin mixing scheme with a mutual recognition delegation strategy//Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Shenzhen, China. 2018:160-166
- [37] Tornado Cash. Tornado cash: Non-custodial ethereum privacy solution. <https://github.com/tornadocash/tornado-core>, 2023. URL <https://github.com/tornadocash/tornado-core>
- [38] N. van Saberhagen. Cryptonote v 2.0, 2013. URL: <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>
- [39] Yang Ruilin. Researches on personalized shuffle differential private data protection. Guangzhou University, Guangzhou, 2024(in Chinese)
(杨蕊琳.个性化的洗牌差分隐私数据保护研究.广州大学,广州,2024)
- [40] Ruffing T, Moreno-Sanchez P, Kate A. Coinshuffle: practical decentralized coin mixing for bitcoin//Proceedings of the 19th European Symposium on Research in Computer Security. Wroclaw, Poland, 2014:345-364
- [41] Jan Henrik Ziegeldorf, Fred Grossmann, Martin Henze, Nicolas Inden, Klaus Wehrle. Coinparty: Secure multi-party mixing of bitcoins//Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. Antonio, USA, 2015:75-86
- [42] Chaum D. Blind signatures for untraceable payments//Proceedings of the Advances in Cryptology. Santa Barbara, USA, 1983:199-203
- [43] Masayuki Abe, Eiichiro Fujisaki. How to date blind signatures Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany, 1996:244-251
- [44] Renas Bacho, Julian Loss. On the adaptive security of the threshold bls signature scheme//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles, USA, 2022:193-207
- [45] David Pointcheval, Jacques Stern. Provably secure blind signature schemes//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany, 1996:252-265
- [46] FU Shuo-Ya, Cui Zhe, Li Mei-Juan. Application of anonymous qualification certificate with blind signature in electronic voting. *Journal of Computer Applications*, 2024, 44(S1):118-123(in Chinese)
(付铄雅,崔喆,李美娟.基于盲签名的匿名资格证在电子投票中的应用.计算机应用,2024,44(S1):118-123)
- [47] Luke Valenta, Brendan Rowan. Blindcoin: Blinded, accountable mixes for bitcoin//Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable. San Juan, Puerto Rico, 2015:112-126
- [48] QingChun ShenTu, JianPing Yu. A blind-mixing scheme for bitcoin based on an elliptic curve cryptography blind digital signature algorithm. arXiv preprint arXiv:1510.05833, 2015
- [49] Heilman E, Alshenibr L, Baldimtsi F, Scafuro A, Goldberg S. Tumblebit: an untrusted bitcoin-compatible anonymous payment hub//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2017:1-15
- [50] Noether S, Mackenzie A, The Lab. Ring confidential transactions. *Ledger*, 2016, 1(1):1-18
- [51] Zhang Y H, Feng S Y, Cao J, et al. Sm2 threshold ring signature scheme for electronic voting. *Journal of Nanjing University of Posts and Telecommunications (Natural Science*

- Edition), 2024, 45(3):67-76(in Chinese)
(张应辉, 封舒钰, 曹进等. 面向电子投票的 SM2 门限环签名方案. 南京邮电大学学报(自然科学版), 2024, 45(3):67-76)
- [52] Ming Luo, Yanzibo Zhou. An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for vanets. *IEEE Transactions on Vehicular Technology*, 2022, 71(9):10001-10015
- [53] Oded Goldreich, Silvio Micali, Avi Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design//*Proceedings of the 27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*. Toronto, Canada, 1986:174-187
- [54] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Eran Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again//*Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. Cambridge, USA, 2012:326-349
- [55] Jens Groth. Non-interactive zero-knowledge arguments for voting//*Applied Cryptography and Network Security: Third International Conference, ACNS 2005*. New York, USA, 2005:467-482
- [56] Dingledine R, Mathewson N, Syverson P F. Tor: The second-generation onion router//*Proceedings of the USENIX Security Symposium*. San Diego, USA, 2004: 303-320
- [57] Pance Ribarski, Ljupcho Antovski. Mixnets: Implementation and performance evaluation of decryption and re-encryption types. *Journal of Computing and Information Technology*, 2012, 20(3):225-231
- [58] Xianrui Qin, Shimin Pan, Arash Mirzaei, et al. Blindhub: Bitcoin-compatible privacy-preserving payment channel hubs supporting variable amounts//*Proceedings of the 2023 IEEE symposium on security and privacy (SP)*. Sanfrancisco, USA. 2023:2462-2480
- [59] Gregory Maxwell. Coinswap: Transaction graph disjoint trustless trading, 2013. URL <https://bitcointalk.org/index.php>
- [60] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: What it is, and what it is not//*Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. Helsinki, Finland, 2015:57-64
- [61] Muoi Tran, Loi Luu, Min Suk Kang, Iddo Bentov, Prateek Saxena. Obscuro: A bitcoin mixer using trusted execution environments//*Proceedings of the 34th Annual Computer Security Applications Conference*. San Juan, USA, 2018:692-701
- [62] Liang X B, Wu J H, Zhao Y, et al. Review of blockchain data security management and privacy protection technology research. *Journal of Zhejiang University (Engineering Science)*, 2022, 56(1):1-15(in Chinese)
(梁秀波, 吴俊涵, 赵昱等. 区块链数据安全管理和隐私保护技术研究综述. 浙江大学学报(工学版), 2022, 56(1):1-15)
- [63] Gregory Maxwell. Coinjoin: Bitcoin privacy for the real world. <https://bitcointalk.org/index.php>, 2013. URL <https://bitcointalk.org/index.php>
- [64] Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A Kroll, Edward W Felten. Mixcoin: Anonymity for bitcoin with accountable mixes//*Proceedings of the Financial Cryptography and Data Security*. Christ Church, Barbados, 2014:486-504
- [65] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. P2p mixing and unlinkable bitcoin transactions. *Cryptology ePrint Archive*, 2016
- [66] Tim Ruffing, Pedro Moreno-Sanchez. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin//*Proceedings of the Financial Cryptography and Data Security*. Sliema, Malta, 2017:133-154
- [67] Evan Duffield and Daniel Diaz. Dash: A privacycentric cryptocurrency, 2015
- [68] George Bissias, A. Pinar Ozisik, Brian N. Levine, Marc Liberatore. Sybil-resistant mixing for bitcoin//*Proceedings of the 13th Workshop on Privacy in the Electronic Society*. Scottsdale, Arizona, USA, 2014:149-158
- [69] Ibrahim M H. Securecoin: a robust secure and efficient protocol for anonymous bitcoin ecosystem. *International Journal of Network Security*, 2017, 19(2):295-312
- [70] Zijian Bao, Wenbo Shi, Saru Kumari, Zhi-yin Kong, Chien-Ming Chen. Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity. *International Journal of Information Security*, 2020, 19(3):311-321
- [71] Ning Lu, Yuan Chang, Wenbo Shi, Kim-Kwang Raymond Choo. Coinlayering: An efficient coin mixing scheme for large scale bitcoin transactions. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(3):1974-1987
- [72] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin//*Proceedings of the 2013 IEEE Symposium on Security and Privacy*. San Francisco, USA, 2013:397-411
- [73] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. Zero-cash: Decentralized anonymous payments from bitcoin//*Proceedings of the 2014 IEEE Symposium on Security and Privacy*. San Jose, USA, 2014:459-474
- [74] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox, et al. Zcash protocol specification. GitHub; San Francisco, USA, 2016, 4(220):32
- [75] Meiklejohn S, Mercer R. Möbius: Trustless tumbling for transaction privacy. *Proceedings on Privacy Enhancing Technologies*, 2018, 2018(2):105-121
- [76] István Andrá's Seres, Da'niel A. Nagy, Chris Buckland, Péter Burcsi. MixEth: efficient, trustless coin mixing service for ethereum. *Cryptology ePrint Archive*, 2019:341
- [77] Mixero.io. https://mixero.io/mix_coinjoin
- [78] Odos. <https://www.odos.xyz/>
- [79] Jupiter. <https://jup.ag/>

- [80] Cryptomixer. <https://cryptomixer.io/>
- [81] Wasabi wallet. <https://wasabiwallet.io/>
- [82] Joinmarket. <https://www.joinmarket.cloud/index.html>
- [83] Gomix. <https://gomix.io/>
- [84] Anonymix. io. <https://anonymixbtc.com/>
- [85] Samourai. <https://web-samouraiwallet.io/>
- [86] Toswap. <https://toswap.io/cn/>
- [87] Unijion. <https://bitcoin-rtg.ru/>
- [88] Whir. <https://whir.to/>
- [89] Coinmix. <https://coinmix.cash/>
- [90] jokermix. <https://jokermix.to/>
- [91] Lei Wu, Yufeng Hu, Yajin Zhou, Haoyu Wang, Xiapu Luo, Zhi Wang, Fan Zhang, Kui Ren. Towards understanding and demystifying bitcoin mixing services//Proceedings of the Web Conference 2021, Ljubljana, Slovenia, 2021:33-44
- [92] Yomix. <https://yomix.io/zh/bitcoin-mixer-blender>
- [93] coinmixer. <https://www.coinmixer.app/zh/>
- [94] Bitcloak. <https://bitcloak.me/ru/>
- [95] Bitcoin laundry. <https://bitcoinlaundry.top/>
- [96] Mixer. money. <https://mixer.money/en/>
- [97] Mixtum. <https://mixtum.io/?mix>
- [98] Fastswap. <https://www.fastswap.cc/?Language=en>
- [99] Mixtura. <https://www.mixturo.money/>
- [100] Cce. cash. <https://cce.cash/exchange>
- [101] bestswap. <https://bestswap.net/>
- [102] Coinomize. <https://coinomize.co/>
- [103] mixertumber. <https://mixertumber.pro/>
- [104] Bitcoinfog. <https://bitcoinfog.info/>
- [105] chipmixer. <https://www.chipmixer.hk/en>
- [106] Blender. <https://bitcoin-blender.io/index.html>
- [107] Blanker. Tornado cash: the holy grail of privacy transactions. <https://blanker.blog/p/tornado-cash> (in Chinese) (Blanker. Tornado cash: 隐私交易的圣杯. (2021-05). <https://blanker.blog/p/tornado-cash>)
- [108] Du H, Che Z, Shen M, Zhu L, Hu J. Breaking the anonymity of ethereum mixing services using graph feature learning. *IEEE Transactions on Information Forensics and Security*, 2023,19:616-631
- [109] Ardeshir Shojaeinasab, Amir Pasha Motamed, Behnam Bahrak. Mixing detection on bitcoin transactions using statistical patterns. *IET Blockchain*, 2023,3(3):136-148
- [110] Artem A Maksutov, Maxim S Alexeev, Natalia O Fedorova, Daniil A. Andreev. Detection of blockchain transactions used in blockchain mixer of coin join type//Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). Saint Petersburg and Moscow, Russia, 2019:274-277
- [111] He X, He K, Lin S, Yang J, Mao H. Bitcoin address clustering method based on multiple heuristic conditions. *IET Blockchain*, 2022,2(2):44-56
- [112] Pascal Tippe and Christoph Deckers. Unmixing the mix: Patterns and challenges in bitcoin mixer investigations. *Forensic Science International: Digital Investigation*, 2025,52:301876
- [113] Ziegler M H, Nowostawski M, Katt B. Dakar: a coinjoin forensic software. *SoftwareX*, 2026,33:102523
- [114] Mario Alfonso Prado-Romero, Christian Doerr, Andre's Gago-Alonso. Discovering bitcoin mixing using anomaly detection//Proceedings of the Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. Valparaíso, Chile, 2018:534-541
- [115] Rainer Stutz, Johann Stockinger, Pedro Moreno-Sanchez, Bernhard Haslhofer, Matteo Maffei. Adoption and actual privacy of decentralized coinjoin implementations in bitcoin//Proceedings of the 4th ACM Conference on Advances in Financial Technologies. Cambridge, USA, 2022:254-267
- [116] Jiajing Wu, Jieli Liu, Weili Chen, Huawei Huang, Zibin Zheng, Yan Zhang. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2021,52(4):2237-2249
- [117] Chang Xu, Ruting Xiong, Xiaodong Shen, Liehuang Zhu, Xiaoming Zhang. How to find a bitcoin mixer: A dual ensemble model for bitcoin mixing service detection. *IEEE Internet of Things Journal*, 2023,10(19):17220-17230
- [118] Xiaowen Sun, Tan Yang, Bo Hu. Lstm-tc: Bitcoin coin mixing detection method with a high recall. *Applied Intelligence*, 2022,52(1):780-793
- [119] Hanzhi Yang, Zhenzhen Li, Gaopeng Gou, Junzheng Shi, Gang Xiong, Zhen Li. Bitcoin mixing service detection based on spatio-temporal information representation of transaction graph//Proceedings of the 2023 IEEE International Performance, Computing, and Communications Conference (IPCCC). Anaheim, USA, 2023:210-219
- [120] Yujia Tang, Chang Xu, Can Zhang, Yan Wu, Liehuang Zhu. Analysis of address linkability in tornado cash on ethereum//Proceedings of the China Cyber Security Annual Conference. Beijing, China, 2021:39-50
- [121] Béres F, Seres I A, Benczúr A A, Quintyne-Collins M. Blockchain is watching you: Profiling and deanonymizing ethereum users//Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures. Virtual, Austria, 2021:69-78
- [122] Hong Y, Kwon H, Lee J, Hur J. A practical de-mixing algorithm for bitcoin mixing services//Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts. Incheon, Republic of Korea, 2018:15-20
- [123] Changhao Wu, Junwei Xu, Kai Wang, Weili Han, and Hongfeng Chai. Ettracker: A fund tracking framework for anti-money laundering on ethereum. *Expert Systems with Applications*, 2026,296:128900
- [124] Cha'beli Castan? o Arango, Roberto Luna-Garcia, Steven Cutchin, Gaby G Dagher. Towards deanonymization of mixing services in bitcoin//Proceedings of the 2022 IEEE

- 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). Irvine, USA, 2022:1-6
- [125] Larionov N, Yanovich Y. Shared send mixers untangling in bitcoin clustering heuristics adjustment//Proceedings of the 2024 IEEE International Conference on Blockchain and Cryptocurrency. Dublin, Ireland, 2024:225-229
- [126] Mike Wu, Will McTighe, Kaili Wang, Istvan A Seres, Nick Bax, Manuel Puebla, Mariano Mendez, Federico Carrone, Toma's De Matthey, Herman O Demaestri, et al. Tutela: An open-source tool for assessing user-privacy on ethereum and tornado cash. arXiv preprint arXiv:2201.06811,2022
- [127] Shuilong Wang, Laurence T. Yang, Debin Liu, Ruonan Zhao, Xianjun Deng, Cannian Zou, Xiaoxuan Fan. Improving ethereum mixing address linking with tensor computation, neighbor data utilization, and asymmetric information modeling. IEEE Transactions on Information Forensics and Security, 2025,20:8658-8671
- [128] Tu X, Duan T, Miao S, Zhang H, Sun Y. Hilomix: robust high-and low-frequency graph learning framework for mixing address association//Proceedings of the AAAI Conference on Artificial Intelligence. Vancouver, Canada, 2026: 15788-15796



ZHANG Xiao, Ph. D. , professor. His main research interests include database architecture, big data management and analytics, data benchmarking and evaluation, and blockchain.

ZHANG Xiao-Xuan, Ph. D. candidate. Her main research interests include blockchain and blockchain privacy protection.

YANG Zi-Han, M. S. candidate. His main research interests include blockchain privacy protection.

LI Pei-Qian, M. S. candidate. His main research interests include blockchain privacy protection.

CHEN Jin-Chuan, Ph. D. , professor. His main research interests include distributed data management and blockchain.

Background

Blockchain, as a decentralized distributed ledger system, ensures data integrity through timestamps and a hash-linked chain structure. While users participate anonymously, all transaction data remain publicly visible on-chain. This transparency, while ensuring system trustworthiness, introduces significant privacy risks: attackers may reconstruct associations between account addresses through on-chain tracing techniques such as heuristic methods or machine learning, thereby threatening user privacy security.

To address this challenge, the blockchain community proposed Coin Mixing. Its primary objective is to obscure the correlation between input and output addresses in transactions, thereby concealing fund flow paths and providing transactional privacy protection. The fundamental principle involves blending a transaction's information with multiple other transactions, making it impossible for external observers to identify correspondences between input and output addresses.

Since the introduction of the first Coin Mixing, CoinJoin, in 2013, this field has undergone multi-phase evolution. Post-2015 marked the privacy enhancement stage, where cryptographic tools such as blind signatures, ring signatures, and zero-knowledge proofs significantly improved

anonymity assurance capabilities. Between 2018 and 2020, decentralized Coin Mixing technologies saw substantial growth. Since 2020, innovations including trusted execution environments (TEEs) and regulatory-compliant designs have propelled the technology into a multi-objective optimization phase.

This paper systematically analyzes the evolutionary trajectory of blockchain Coin Mixing technologies. We introduce, for the first time, a three-tier classification framework for blockchain mixing systems and elucidate the distinct roles of cryptographic primitives in transactional privacy protection. The study focuses on recent advancements in the Coin Mixing ecosystem and examines challenges from both technical and regulatory perspectives. Finally, we discuss development goals and technical pathways that balance regulatory requirements with privacy protection in blockchain Coin Mixing systems.

This survey is part of our research supported by the Scientific Research Innovation Capability Support Project for Young Faculty (Grant No. SRICSPYF-ZY2025001), the Joint Fund of the National Natural Science Foundation of China (Grant No. U24B20144), and the National Key R&D Program of China (Grant No. 2022YFB2702102).