区块链数字货币交易的匿名性：保护与对抗

沈 蒙[1] 车 征[2] 祝烈煌[1] 徐 恪[3,4] 高 峰[2] 余聪聪[2] 吴 言[1]

[1](北京理工大学网络空间安全学院 北京 100081)

[2](北京理工大学计算机学院 北京 100081)

[3](清华大学计算机科学与技术系 北京 100084)

[4](北京信息科学与技术国家研究中心 北京 100084)

摘 要 近年来，以区块链技术为基础的加密数字货币持续涌现，受到各方的广泛关注. 与传统的支付方式相比，区块链数字货币具有去中心化特性，支持交易匿名性. 然而，匿名性也为不法行为提供了隐匿的便利条件，使得区块链数字货币日益成为洗钱、勒索等违法犯罪活动的支付媒介. 因此，区块链数字货币匿名性保护和对抗技术是当前研究的热点问题. 本文首先对交易匿名性的内涵进行了深入剖析，将其归纳为不可标识性、不可链接性和不可追踪性三个方面. 以此为指导，对区块链数字货币的匿名性保护技术和匿名性对抗技术进行了介绍，并开展了对比分析. 最后，本文总结了区块链数字货币匿名性研究所面临的挑战和未来的发展趋势.

关键词 区块链；数字货币；匿名性；比特币；以太坊

中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2023.00125

Anonymity in Blockchain Digital Currency Transactions: Protection And Confrontation

SHEN Meng[1] CHE Zheng[2] ZHU Lie-Huang[1] XU Ke[3,4] GAO Feng[2] YU Cong-Cong[2] WU Yan[1]

[1](*School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing* 100081)

[2](*School of Computer Science and Technology, Beijing Institute of Technology, Beijing* 100081)

[3](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

[4](*Beijing National Research Center for Information Science and Technology, Beijing* 100084)

Abstract In recent years, cryptocurrencies based on blockchain technology have emerged and attracted widespread attention from various parties. Compared with traditional payment methods, cryptocurrency has the characteristics of decentralization and supports transaction anonymity. However, anonymity also provides hidden conveniences for illegal activities, making cryptocurrency increasingly a payment medium for money laundering, extortion, and other illicit activities. Therefore, cryptocurrency anonymity protection and countermeasures technology are a hot issue for current research. The research on the anonymity of cryptocurrency transactions mainly focuses on protecting transaction anonymity and the confrontation of anonymity. In terms of transaction anonymity protection, researchers mostly use zero-knowledge proof, Tor network, and other anonymity technologies to

收稿日期：2021-11-04；在线发布日期：2022-05-20. 本课题得到国家重点研发计划(2020YFB1006101)、北京市科技新星计划（Z201100006820006）、国家自然科学基金（61825204，61932016，61972039，62132011，62222201）、北京高校卓越青年科学家计划项目（BJJWZYJH01201910003011）、北京市自然科学基金（4192050）资助. **沈 蒙**（通信作者），博士，教授，主要研究领域为网络安全、数据隐私保护. E-mail: shenmeng@bit.edu.cn. **车 征**，博士研究生，主要研究领域为区块链技术与应用、网络安全. **祝烈煌**，博士，教授，主要研究领域为密码学、网络与信息安全. **徐 恪**，博士，教授，主要研究领域为新一代互联网体系结构，网络空间安全与区块链系统. **高 峰**，博士，主要研究领域为区块链安全. **余聪聪**，硕士研究生，主要研究领域为区块链技术与应用、网络安全. **吴 言**，博士研究生，主要研究领域为网络安全、区块链技术、公钥密码学.

ensure the anonymity of users in the entire transaction process from different perspectives. Regarding the confrontation of anonymity, the researchers mainly combined the transaction information disclosed in the blockchain ledger and the dissemination data in the network layer to analyze the transaction traces left by users in the transaction process from different perspectives. In this paper, we first give an in-depth analysis of transaction anonymity's connotation and summarize it into three aspects: (1) Unidentifiability. For a given transaction, the observer cannot identify the true identity of the transaction participants in the physical world. (2) Unlinkability. For a given two transactions (at most, one of which is sent by the observer), the observer cannot determine whether they are paid to the same user. Also, the observer cannot determine whether the same user-initiated them. (3) Untraceability. For a given transaction, the observer cannot trace the flow of funds between the address to which the transaction was sent and the address to which the transaction was received. Then, we group the existing anonymity protection schemes into three categories according to the different focuses: (1) Unidentifiability protection schemes represented by Tor network, which mainly prevent observers from associating transactions with real-life user identities by hiding node information; (2) Unlinkability protection schemes represented by zero-knowledge proof technology, which mainly prevent observers from associating transactions with real-life user entities by hiding transaction information in the ledger to prevent observers from associating transactions with user entities; (3) Untraceability protection schemes represented by coin mixing technology, which mainly prevent observers from tracking the flow of funds based on the links between transaction participants by severing the relationships between them. At the same time, we also summarize the anonymity analysis methods of digital currencies from three aspects: (1) Unidentifiability confrontation, the observer uses the traffic information generated at each stage of cryptocurrency transactions, combined with the IP address, geographic location, organization's identity, and other information belonging to the P2P node, to identify the real identity information target transaction. (2) Unlinkability confrontation, where the observer discovers the correlation between user addresses and transactions by observing the transaction records in the public ledger based on attributes such as transaction amount, fund flow, and transaction time. (3) Untraceability confrontation, where the observer combines the ledger data and on-chain information to track the fund flow of the transaction. Finally, the paper summarizes the cryptocurrency anonymity research institute's challenges and future development trends.

Keywords blockchain; cryptocurrency; anonymity; bitcoin; ethereum

1 引 言

比特币作为区块链技术的首个应用[1]，开启了加密数字货币时代，各式各样以区块链技术为依托的数字货币层出不穷. 著名区块链数字货币统计网站 CoinMarketCap①的数据显示，2013 年 6 月仅有 14 种数字货币，其中只有 5 种货币的市值超过 100 万美元；而截至到 2021 年 10 月，加密数字货币超过 11600 种，其中排名前十的数字货币市值均超过 350 亿美元，排名第一的比特币总市值更是超过了 1 万亿美元. 区块链数字货币具有去中心化、交易匿名等显著特点，因而获得了众多用户的信任和青睐.

然而，匿名性是一把双刃剑. 一方面，用户在进行交易时无需向第三方代理进行实名注册，有利于保护用户身份及交易的隐私. 另一方面，由于用户身份的隐匿特性，数字货币②常被用于洗钱、贩毒、暴恐犯罪行为[2]，而犯罪者往往不知所踪，这种现象也随着数字货币匿名机制的不断增强而愈演愈烈. 为了应对不法分子的非法交易行为，研究者们

① https://coinmarketcap.com/

② 本文中的数字货币均指基于区块链技术的数字货币

对加密数字货币的匿名机制展开了对抗性分析，以期发现隐藏在数字货币交易背后的真实信息.

当前，针对数字货币交易匿名性的研究主要围绕交易的匿名性保护和匿名性对抗两个方面展开. 在交易的匿名性保护方面，研究者主要采用零知识证明、Tor 网络等匿名性技术从不同的角度保证用户在整个交易过程中的匿名性. 例如，门罗币（Monero）系统通过采用环签名技术隐藏真实的交易输入，实现对交易输入的保护；Dash 币系统[3]通过采用混币技术混淆了交易输入和输出之间的关系，切断了交易输入和输出之间的关联性. 在交易的匿名性对抗方面，研究者主要结合区块链账本中公开的交易信息以及网络层中的传播数据，从不同的角度分析用户在交易过程中遗留的交易痕迹. 例如，通过分析比特币交易网络的拓扑特性可以得到比特币交易之间的关联性[4].

近年来，已有众多综述文献对区块链的隐私问题展开研究[5-11]，如表 1 所示. 这些文章从不同的角度对区块链中的匿名性问题和隐私问题展开研究. 与已有工作不同，本文首次从对抗的角度系统性研究区块链数字货币的交易匿名性. 具体而言，本文对交易匿名性的内涵进行剖析，从交易不可标识性、不可链接性、不可追踪性三方面给出了交易匿名性的完整定义，并以此为指导，系统性地对比分析了区块链数字货币的匿名性保护技术和匿名性对抗技术.

本文后续组织如下：第二节主要对区块链数字货币的背景知识进行介绍，主要包括数字货币的交易流程和数据模型；第三节对交易匿名性的内涵进行了深入剖析，将其归纳为不可标识性、不可链接性和不可追踪性三个方面；之后四、五节分别对当前阶段交易的匿名性保护机制和匿名性对抗技术进行对比分析；第六节，对数字货币交易匿名性研究所面临的挑战及未来的研究趋势进行探讨；最后，在第七节总结全文.

2　数字货币的交易流程

与传统的中心化支付系统不同，基于区块链的数字货币系统是无中心的，它允许交易双方在没有第三方参与的前提下完成交易，而交易记录则会以区块的形式存储在所有参与者可见的公开账本中. 本文将用户利用数字货币进行交易的过程分为三个阶段：交易创建阶段、网络传播阶段和交易验证阶段. 数字货币的交易流程如图 1 所示.

2.1　交易创建阶段

该阶段主要表现为交易发送方通过交易客户端与 P2P 节点进行交互. 交易客户端作为数字货币用户与区块链网络交互的接口，既可以应用程序的形式部署在区块链的全节点中，也可以轻量级数字货币钱包的形式部署在区块链的简单支付验证（Simplified Payment Verification，SPV）节点中. 通过交易客户端，用户可以管理个人的私/公钥和交易地址，还可以查看和花费个人钱包中的可用资金，并能够进一步的生成数字货币的交易. 当前市面上有许多数字货币的交易客户端，例如 BitcoinJ、imToken、

表 1　已有综述文献与本文的对比情况

论文名称	论文主题	侧重
Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies[5]	对比特币系统的协议及其应用的基本结构进行了全方位的分析	比特币协议
区块链隐私保护研究综述[6]	从交易隐私和身份隐私两个方面分别对区块链在网络层、交易层以及应用层存在的隐私问题进行分析	区块链隐私
区块链数据分析：现状、趋势与挑战[7]	就实体识别、隐私泄露、网络画像等 7 个问题对区块链数据的分析方法进行了系统性概述	区块链隐私
数字货币的匿名性研究[8]	从匿名性的角度对中心化的数字货币和去中心化的数字货币进行介绍	非区块链数字货币的匿名性
比特币隐私保护综述[9]	围绕比特币协议分析存在的缺陷，并从比特币协议的角度对现有的隐私增强技术进行分析	比特币隐私
区块链隐私保护研究与实践综述[10]	针对区块链系统中的隐私威胁，分析了现有的隐私保护机制	区块链隐私
Knowledge Discovery in Cryptocurrency Transactions: A Survey[11]	从数据挖掘的角度分析区块链中记录的交易数据	区块链隐私
本文	从对抗的角度系统性地对区块链数字货币的交易匿名性进行梳理总结	区块链数字货币的匿名性

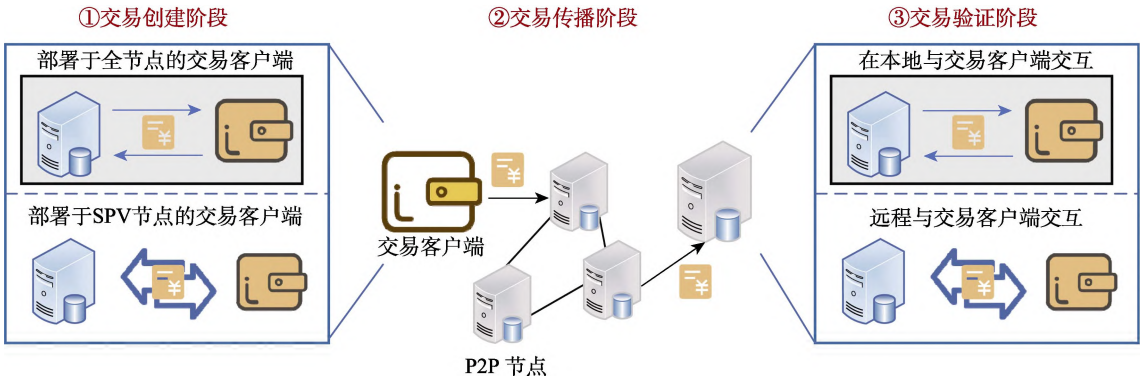

图 1 数字货币的交易流程

Binance 等.

当用户发起交易时，交易客户端首先创建唯一的主密钥，用于生成一系列的密钥对，每个密钥对都包含了一个私钥和一个公钥. 其中，公钥用于生成一个类似于传统银行账号的交易地址，私钥则用于对生成交易进行签名. 交易发送方在利用自己的私钥对交易进行签名后，会通过 P2P 节点广播至区块链网络. 具体而言，根据交易客户端部署的节点类型不同，交易客户端与 P2P 节点的交互可以分为两种情况：

（1）交易客户端部署于区块链全节点时，可在本地直接对所提交的交易进行验证. 区块链的全节点存储有数字货币的完整交易副本，具有验证交易有效性的能力. 因此，部署在区块链全节点上的交易客户端可以直接在本地进行交易验证，并由本地节点广播至网络中的其他节点.

（2）交易客户端部署于 SPV 节点时，需要通过远程连接全节点验证交易. 区块链的 SPV 节点往往是资源受限的个人设备（智能手机、个人 PC 等），并不存储数字货币交易的完整交易副本，仅存储交易的区块头信息. 当部署在 SPV 节点的交易客户端（下称 SPV 客户端）发起交易请求时，需要远程向区块链的全节点请求可能包含交易的区块来对交易进行验证，并在验证通过后由远程的区块链全节点广播至网络中的其他节点. 具体而言，SPV 客户端仅接收与之相关的交易，该功能通过 Bloom 过滤器①实现. Bloom 过滤器是一种空间效率高的概率数据结构[12]，用于测试一个元素的成员资格. 一个 SPV 客户端通过向过滤器中嵌入交易公钥以及公钥哈希值的方式构建一个 Bloom 过滤器. 当连接至一个全节点时，构建的 Bloom 过滤器会按照初始握手协议发送给全节点. 每当全节点收到一笔交易时，它首先检查其输入或输出地址是否与 SPV 客户端的 Bloom 过滤器相匹配. 若匹配，则全节点会将收到的交易转发给 SPV 客户端.

2.2 网络传播阶段

该阶段主要表现为交易在 P2P 节点之间进行传播. 数字货币使用 P2P 网络来传播交易信息，本节以比特币网络为例对数字货币的消息传播机制进行描述，Monero、Zcash、Dash 等大多数衍生的数字货币也继承了这些特性. 交易信息在 P2P 网络中的传播主要包括两个过程：节点路由和交易传播. 节点路由即一个新的 P2P 节点加入数字货币网络时，发现网络中的其他节点并建立连接的过程. 交易传播即一条验证过的交易在区块链网络中按照一定的规则进行传播的过程.

（1）节点路由. 在节点路由阶段，一个新启动的节点首先对协议中硬编码的记录进行 DNS 查询，以发现引导节点的 IP 地址. 然后，它向引导节点询问它们已知节点的 IP 地址列表. 收到 IP 列表后，新节点会与一组随机的节点建立预先配置好的连接，本文将这些节点称为入口节点（Entry Node）. 默认情况下，每个比特币节点会与 8 个入口节点建立外向连接，并通过这些节点向交易网络转发消息. 在加入网络并建立连接后，新节点会向其邻居节点发送一条包含自身 IP 地址的 Add 消息. 邻居节点在收到该消息后会依次将该消息转发给他们各自的邻居节点. 新加入网络的节点也可以随时向其邻居节点查询他们已知的地址列表.

（2）交易传播. 交易信息在 P2P 节点间的传播也被称为中继，具体可分为三个步骤. 首先，拥有最大区块高度的节点会通过 inv 消息将最新交易区块的哈希值转发至网络中；其次，接收节点会根据哈希值检查自己是否存储了该区块；若没有存储，

① Connection bloom filtering,https://github.com/bitcoin/bips/ blob/master/bip-0037.mediawiki 2012

则通过发送 getdata 消息来向发送节点请求区块的全部信息. 最后，发送节点通过 transaction 消息向接收节点转发交易的实际内容. 当接收节点得到交易后会继续重复上述步骤，通过 inv 消息向其邻居节点广播该交易.

需要注意的是，当节点接收到一笔新交易时，会将该交易信息发送给所有的邻居节点，并保留消息转发记录，以保证交易信息仅向每个邻居节点转发一次. 每个 P2P 节点将收到的所有交易保存在一个内存池中. 当接收到一笔新交易时，节点会将接收到的交易哈希与内存池或区块链账本中的哈希值进行比对，若哈希值相同，则拒绝接收该交易.

2.3　交易验证阶段

该阶段主要表现为 P2P 节点与交易接收方之间的交互. 区块链网络中的记账节点会收集所有尚未被记入账本的交易，并对交易进行排序打包生成区块. 在多数的公有区块链系统中，区块的记账权是通过工作量证明机制（Proof Of Work，POW）进行确认的，即由最先计算得出区块哈希值随机数的节点获得记账权. 因此，记账节点通过计算新区块的哈希值而获得记账的权利. 同时，获得记账权的记账节点会获得代币奖励. 当记账节点创建一个区块并获得记账权，就会向区块链网络中的其他节点进行广播，这样具有记账功能的节点就会将其附在内部维护的区块链上.

此时，交易接收方便可确认自己的货币所有权，完成交易. 具体而言，交易用户利用交易客户端访问 P2P 网络节点，通过存储于节点中的区块链账本中再通过识别他们的交易地址或假名来确认货币所有权.

3　数字货币的匿名性定义

匿名性是数字货币的重要属性之一，旨在保护用户的身份信息，隐藏用户与交易地址之间的关联关系. 用户在参与数字货币交易的过程中，无需暴露姓名、身份证号等真实的身份信息，而是将系统生成的假名地址作为交易时的身份标识，这是数字货币交易匿名性的重要体现. 通过分析数字货币交易的特点，本文将数字货币中的交易匿名性归纳为不可标识性、不可链接性和不可追踪性三个方面. 图 2 为数字货币交易匿名性内涵的示意图.

定义 1. 不可标识性. 对于给定的交易，观察者无法标识交易参与方在物理世界中的真实身份.

不可标识性对应于图 2 椭圆框中两个实体间的关系，反应了用户的交易地址及其在现实世界中真实身份之间的关系. 数字货币中的每一笔交易，本质上都是由现实世界中的某一个体或组织机构通过部署有交易客户端的 P2P 节点来处理的，该类节点往往是一台具有 IP 地址、地理位置等明显标识信息的物理服务器. 当观察者能够将数字货币网络中的交易与现实生活中某一 P2P 节点相关联时，便可以根据节点的标识信息对交易参与者在现实世界中的身份进行推测[13-15].

定义 2. 不可链接性. 对于给定的两笔交易（其中最多只有一笔是由观察者发送的），观察者无法判断它们是否支付给同一个用户. 同时，观察者也无法判断它们是否由同一个用户发起.

不可链接性对应于图 2 虚线方框中两个实体间的关系，反应了用户及其交易账户之间的关系. 在数字货币的交易中，每个用户可以利用不同的交易地址参与不同的交易，从而将自己的身份信息隐藏在系统假名中. 但是，公开账本中记录的交易信息可能暴露数字货币地址之间的关联性. 例如，比特币的公开交易中记录有每笔交易的交易金额、资金来源、资金流向等敏感信息，观察者可以利用启发式的分析方法对交易地址进行关联分析[16]. 一旦可以得知地址集群中某一交易地址与用户的关联性，那么便可推知整个地址集群与用户的关联性.

定义 3. 不可追踪性. 对于给定的交易，观察者无法追踪交易发送地址与交易接收地址之间的资金流向.

不可追踪性对应于图 2 圆角矩形框中两个实体间的关系，反应了交易发送方与交易接收方之间的关系. 部分数字货币系统采用了混币、零知识证明等匿名性保护技术来混淆交易发送方与接收方间的关系，从而避免观察者对交易参与方的交易行为进行跟踪. 但是，匿名性技术对交易的保护并不是全面的，观察者利用显露的交易信息依然可以在一定程度上推测交易双方间的关联性. 例如，对 Monero 交易中的输入而言，环签名技术虽然能够通过制造混淆输入的方式来隐藏交易的真实输入，却不能隐藏交易的时间信息，观察者可以借此来推测环签名交易中的真实输入[17].

不可标识性、不可链接性和不可追踪性是交易匿名性内涵的重要组成部分. 不可标识性隐藏了用户的交易地址及其在物理世界中真实身份之间的关系，旨在保护用户的身份隐私；不可链接性隐藏了用户及其交易地址间的关系，旨在保护用户的账户隐私；不可追踪性隐藏了用户与其他用户间的关联关系，旨在保护用户的交易隐私. 上述三者从不同

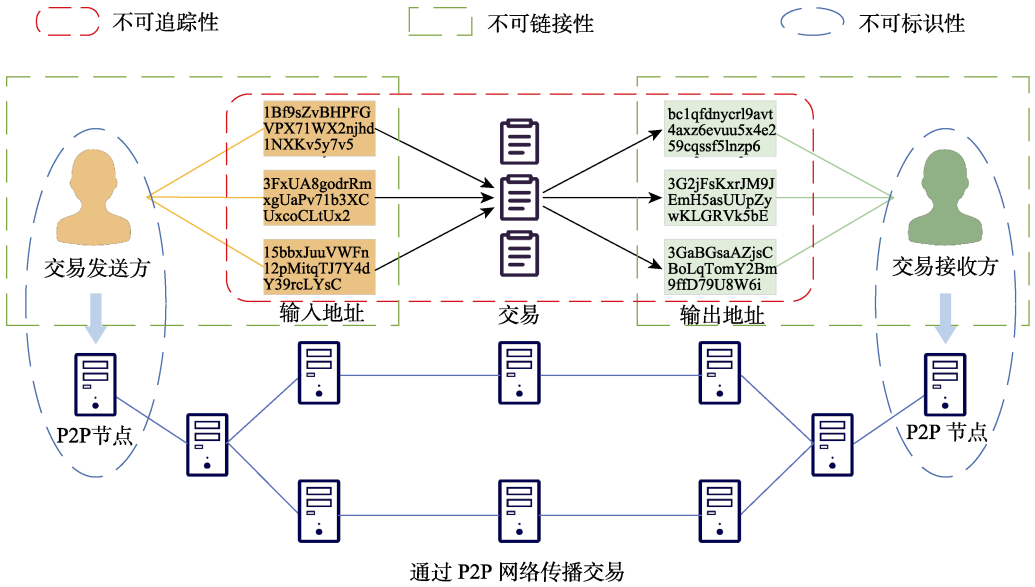

图 2 数字货币交易匿名性的内涵

的方面保护了交易的匿名性，是数字货币的交易匿名性研究时需要重点关注的内容.

4 数字货币交易的匿名性保护方案

为了保护数字货币交易的匿名性，研究者们针对不同层面的显露信息，提出了多种匿名性保护机制. 本节根据保护方案侧重点的不同，将当前阶段的匿名性保护方案归纳为三类：第一类为不可标识性保护方案，该类方案主要通过隐藏节点信息的方式，防止观察者将交易与现实生活中的用户身份相关联；第二类为不可链接性保护方案，该类方案主要通过隐藏账本中的交易信息，防止观察者将交易与用户实体相关联；第三类为不可追踪性保护方案，该类方案主要通过切断交易参与方之间的关系，防止观察者根据交易参与方之间的联系来跟踪资金流向. 各种典型的匿名性保护方案对比情况如表 2 所

表 2 匿名性保护方案对比表

目的	技术名称	实现原理	代表性方案	应用实例	隐藏节点信息	隐藏交易金额	隐藏交易发送地址	隐藏交易接收地址	切断交易双方联系	中间人匿名性
保护不可标识性	匿名网络	结合公钥密码学隐藏网络中的节点信息	Tor	Wasabi Wallet	√	×	×	×	×	–
保护不可链接性	零知识证明	允许用户在不提供有用信息的前提下，向矿工证明交易的合法性	zk-SNARKs	Zcash	×	√	√	√	√	–
	环签名	利用混淆交易隐藏交易中的真实输入	可追溯环签名	Monero	×	×	√	×	×	–
	同态加密	通过操作密文的方式，隐藏交易金额	Pedersen 承诺	Beam	×	√	×	×	×	–
	链下存储	将区块链账本中存储的交易信息转存至链下	闪电网络	Breez Wallet	×	√	√	√	×	×
保护不可追踪性	中心化混币	借助第三方混淆交易发送方与接收方之间的关系	MixCoin	Blockchain.info	×	×	×	×	√	×
	去中心化混币	无需借助第三方混淆交易发送方与接收方之间的关系	CoinJoin	DASH	×	×	×	×	√	√

示. 其中，中间人匿名性指匿名保护方案在借助第三方来隐藏交易信息的过程中，第三方掌握交易地址、交易金额等敏感信息的可能性.

4.1　不可标识性保护方案

数字货币交易的不可标识性强调交易与用户身份之间的关联性. 观察者通常可以利用网络中传播的流量信息将交易与 P2P 节点相关联，因此，针对交易不可标识性的保护方案应该具备隐藏节点信息的能力. 匿名网络是一种结合公钥密码机制的网络信息隐藏技术，当该技术应用于数字货币网络时，可以保护交易的不可标识性. 常见的匿名网络有 Tor、I2P 等.

（1）Tor 网络

Tor（The Onion Router）网络作为匿名网络的一个典型代表，已经出现了与数字货币网络相结合的应用[18]. Tor 是一个由洋葱路由器构成的端到端网络，具有低延迟、匿名性的特点，可以有效防止观察者或消息转发节点将消息的接收者与消息的发送者联系起来. 洋葱路由器作为网络的中继节点负责转发网络中的信息，节点间通过 TLS 协议建立链接. 在 Tor 网络中，用户的信息通过一条由多个洋葱路由器组成的电路（circuits）进行传输，默认由三个节点组成.

当用户希望通过电路向某一服务器发送信息时，首先需要从 Tor 客户端的节点列表中随机挑选三个 Tor 中继节点（入口节点、中间节点和出口节点）组成电路，并与每个中继节点协商传输时的对称密钥. 在向服务器发送消息之前，用户依次采用事先协商的对称密钥对信息进行加密. 当信息沿着电路进行传输时，三个中继节点都对加密信息进行层层解密. 通过这种方式，信息以其原始形式由出口节点最终传送给目标服务器. 在整个传输过程中，每一个中继节点只知道上一跳和下一跳.

部分数字货币的交易客户端内置了 Tor 的网络配置①，如图 3 所示. 图中，Tor 网络作为交易客户端与 P2P 节点连接的中间部分，使得交易客户端可以更隐蔽的与 P2P 节点进行交互而不暴露 SPV 节点的 IP 地址等敏感信息.

（2）I2P 网络

I2P（The Invisible Internet Project）网络是一种采用单向加密隧道的匿名网络，已经作为一种隐藏节点信息的技术应用于 Monero 中②. I2P 是一个由

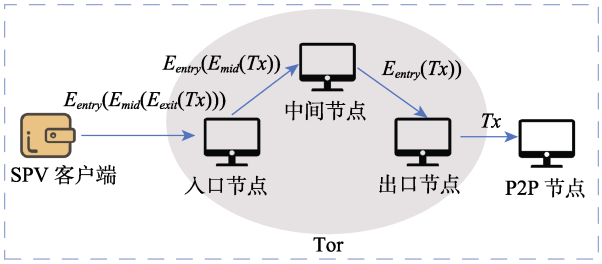

图 3　数字货币中的 Tor 网络

大蒜路由器构成的端到端网络，不仅可以保证消息发送方的匿名性，还可以保证消息接收方的匿名性. 在 I2P 网络中，用户的信息通过一条由输出隧道（Outbound tunnel）和输入隧道（Inbound tunnel）组成的环路进行传输，隧道的默认长度为三跳，该种组合方式使得用户在发送消息和接收消息时都可以保持流量的单向传输.

对于 Monero 中的用户节点而言，由于同步整个区块链账本需要消耗大量的存储空间和时间成本，因此当需要处理交易时用户会选择通过远程节点验证交易. 在与远程节点通信的过程中，用户节点会暴露自己的 IP 地址与交易信息，使得节点的匿名性遭到破坏. 2019 年，Monero 的 0.15 版本中开始采用 I2P 网络来应对这一问题.

图 4 展示了 Monero 系统中的本地节点利用 I2P 网络与远程节点进行通信的示意图. 在 I2P 网络中，消息的收发双方需要事先建立各自的输出和输入隧道. Monero 的本地节点在利用 I2P 网络向远程节点发送消息前，首先需要使用远程节点的公钥对消息进行端到端加密，然后再依次进行三次洋葱式加密. 在消息发送的过程中，消息首先经过输出隧道到达网关节点，该过程中消息会被依次解密. 解密后的消息会经过输入隧道的网关节点发往远程节点，该过程中消息会再次经过三次洋葱式加密. 最终，远程节点通过四次解密得到消息的明文. 远程节点需

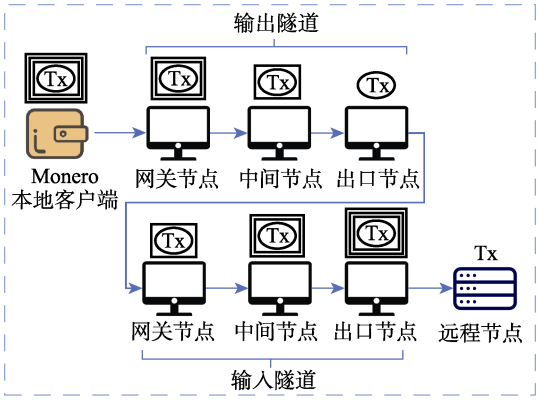

图 4　Monero 中的 I2P 网络

① https://github.com/Kryptsy/Crypto-Wallet

② https://github.com/monero-project/kovri

要将消息返回给本地节点的过程与此类似.

4.2 不可链接性保护方案

数字货币交易的不可链接性强调交易与用户之间的关联性，由于观察者可以通过账本信息来关联用户的相关交易，因而针对交易不可链接性的保护方案应该具备模糊账本信息的能力. 目前已有的不可链接性保护方案包括零知识证明、环签名、同态加密以及链下存储.

（1）零知识证明

零知识证明允许验证者在证明者不提供任何有用信息的情况下证明一个声明是正确的[19]. 该种方案的安全性在理论上是可证明的，只要底层的椭圆曲线加密技术没有被破坏，并且初始化过程（即生成通用参考字符串）是以安全和可信的方式进行，那么该技术的使用就可以认为是安全的[20].

在数字货币的应用中，该技术常用来隐藏公开账本中所记录的交易地址、交易金额等敏感信息，可以阻止观察者利用账本信息推测用户及其交易地址间的关系. 因此，可以作为一种保护不可链接性的方案. 但在一些特殊情况下，该技术也可以保护交易的不可追踪性. 例如，当采用该技术同时隐藏交易双方的交易地址和交易金额时，由于缺少必要的有效信息而使得观察者无法判断交易双方之间的联系，从而无法跟踪交易的资金流向.

非交互式零知识证明[21]（Non-Interactive Zero-Knowledge proof, NIZK）技术是一种不支持证明者和验证者进行交互的零知识证明方案，目前已被应用于数字货币领域，例如 Zerocoin[22]. 该技术允许证明者独自构造并发起交易. 然而，采用 NIZK 构造的零知识证明需要花费较大的存储空间和较长的验证时间.

简明非交互式零知识证明（zero-knowledge Succinct Non-Interactive Arguments of Knowledge, zk-SNARK）对 NIZK 进行了改进，在保证非交互性的同时优化了证明所需的存储空间以及验证所需的时间. 但是，zk-SNARK 需要借助第三方在系统的初始化阶段生成公共参数来构建零知识证明. 当恶意的第三方获得公共参数时会对整个交易系统的安全带来威胁.

2018 年，Ben-Sasson 等人[23]提出了可扩展的透明零知识证明(zero-knowledge Scalable Transparent Argument of Knowledge，zk-STARK)技术，该技术将任意计算的证明转化为验证多项式的阶小于某个度的问题，无需再通过第三方来生成公共参数，实现了初始化阶段的透明性. 然而，该技术生成证明需要更多的存储空间.

为了解决 zk-STARK 存在的这一问题，Bunz 等人[24]提出了新的非交互式零知识证明协议 Bulletproofs，该协议中的零知识证明比 zk-STARK 更节省空间. 在同等电路空间大小的前提下，zk-STARK 达到 60bit 安全所需的证明大小为 200KB，Bulletproofs 达到 120bit 安全所需的证明大小仅为 1KB. 因此，在需要长期存储证明的分布式系统中，该协议可以降低整体的存储成本. 2018 年 10 月，Monero①开始采用 Bulletproofs 技术支持其机密交易的实现，采用之后 Monero 的平均交易大小从 18 KB 减小到 3 KB.

2019 年，Bowe 等人[25]提出了 Halo 协议. 该协议将 Bulletproofs 递归迭代出最终值的过程改为递归迭代展开为多项式，解决了 Bulletproofs 中存在的验证代价高的问题. 2021 年 10 月，该协议作为 zk-SNARKs 协议的替代方案在 Zcash 中上线运行.

（2）环签名

环签名[26]技术允许用户使用自己的私钥和其他成员的公钥对一个事务进行签名，验证者仅可以确人签名者是环的成员，但并不能具体确定签名者的身份. 环签名可以保护签名者的匿名性，常作为一种匿名性保护方案应用于数字货币中.

2014 年，Monero 基于 CryptoNote 协议开发上线. Monero 在创建交易阶段，采用环签名技术来隐藏交易发送方的地址. 具体而言，当交易发送方想要创建一笔 Monero 交易时，系统会从历史交易中抽样若干已被花费的交易输出作为混淆交易（也称为 mixin），与即将被花费的真实输入构成一个环结构. 环结构的大小决定了交易中的匿名集大小，环签名中混淆交易的数量越多，交易的匿名集也就越大. 图 5 展示了匿名集大小为 3 的 Monero 交易. 然而，Monero 交易数据的大小随着环结构尺寸的增加而线性增加，这无疑增加了区块链的存储成本.

2017 年，Monero 将最初的环签名算法替换为可链接环签名，使得环签名大小减小了一半，同时使得区块链存储花费降低了接近一半. 2020 年，Monero 进一步对环签名方案进行升级，采用了简洁可链接自发性匿名群组 CLSAG(Concise Linkable Spontaneous Anonymous Group)签名方案，使得交易大小减小约 25%，同时交易验证效率也提高约 20%.

（3）同态加密

同态加密是一种支持将信息的密文操作映射至明文信息中的匿名性保护方案. 数字货币匿名性保

① https://www.163.com/dy/article/DUOV9B2T0511WD0R.html 2018

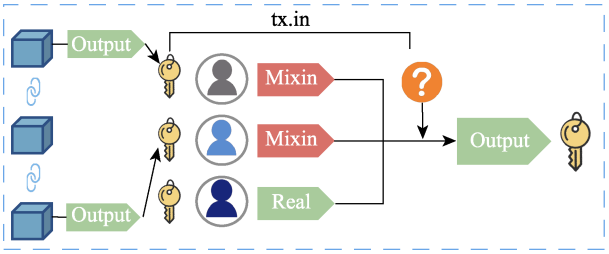

图 5　基于环签名的 Monero 交易[27]

护中常用的同态加密技术有 Pedersen 承诺和 Paillier 加密. 2013 年，Adam①首次将同态加密技术引入数字货币系统，提出了机密交易（Confidential Transactions，CT）的思想，旨在保证交易正常进行的同时隐藏具体的交易金额. 2015 年，Maxwell 在比特币系统中对机密交易的思想予以实现②. 机密交易采用了 Pedersen 承诺. 在机密交易中，交易发送方在将交易金额提交至 P2P 节点之前，使用随机盲化因子对交易金额进行承诺. 交易的验证者通过验证交易的所有输入与所有输出的总和是否为 0 的方式即可验证交易金额是否有效，而无需知道交易的实际金额. 该种方式隐藏了交易金额，降低了观察者进行交易关联分析的可能性.

除在比特币系统实现机密交易技术之外，Monero 在环签名技术的基础上引入机密交易技术，二者的结合形成了环机密交易（Ring CT）技术. 该技术通过 Pedersen 承诺以及范围证明技术，在隐藏交易金额的同时，也保证了公开可验证性.

（4）链下存储

链下存储技术本质上是一种区块链扩容方案，通过将存储在链上的交易数据转移至链下存储，从而缓解区块链网络节点所面临的日益攀升的存储压力. 当人们将不涉及用户隐私的链上交易数据存储于链下时，该种方法便可以作为一种隐藏账本交易记录的隐私保护方法，观察者无法通过观察链上的交易记录来推测交易内容中所蕴含的关联关系，从而提高了交易的不可链接性.

常见的链下存储方案有闪电网络（Lighting Network）③和雷电网络（Raiden Network）④. 其中闪电网络是基于 UTXO（Unspent Transaction Output，未花费的交易输出）模型的链下存储方案，雷电网络是基于账户余额模型的链下存储方案. 闪电网络中，用户之间通过事先沟通好的双向支付通道来进行交易，交易发送方通过向一个中间节点发送一定量的比特币来打开支付通道. 在支付通道关闭后，中间节点将根据交易记录对比特币进行清算. 在整个交易过程中，链上账本仅记录用户之间的总交易金额而隐藏交易次数，保护了用户隐私. 雷电网络则是通过智能合约机制简化了闪电网络中链下支付通道的实现方式.

4.3　不可追踪性保护方案

数字货币交易的不可追踪性强调交易发送方与交易接收方之间的关联性. 当观察者可以获知某一交易地址与其他交易地址所有的交易记录时，便可以追踪该交易地址的资金流向. 针对交易不可追踪性的保护方案应该具备隐藏交易发送方与接收方之间关联性的能力. 目前已有的不可追踪性保护方案主要包括中心化混币和去中心化混币.

混币技术通过混淆交易发送方与交易接收方之间的关系，来提高数字货币的不可追踪性. 自 2010 年以来陆续出现了一系列的混币方案，包括 BitLaundry、Bitcoin Laundry、Bitcoin Fog 以及 CoinJoin. 一般来说，主要有两种类型的混币方案，即中心化的混币和去中心化的混币. 此外，像 ShapeShift 这样的数字资产交易平台还会提供跨链的混币服务.

（1）中心化混币

中心化混币技术的运行依赖于一个中心化的混币服务器. 用户需要向地址池中的一个地址存款，并从另一个地址提款（如图 6 所示）. 该种方式需要借助第三方服务商来提供混币服务，因而存在一系列的信任问题. 首先，不能保证混币服务提供者会将混合币发送到用户指定的地址，导致用户的财产损失；其次，服务提供商可以记录用户输入和输出之间的原始关系. 因此，若第三方服务商作恶，混币交易的不可追踪性将遭到破坏.

为了保证交易在中心化混币过程中的不可追踪性，需要保证交易输入输出地址间的关系对第三方服务商不可见. 2015 年，Valenta 等人[28]在 BlindCoin 协议中引入了盲签名技术，通过盲化输出地址的方式，实现了针对第三方服务商的不可追踪性. 但盲签名增加了额外的计算成本和时间开销.

① Back A. Bitcoins with homomorphic value(validatable but encrypted). https://bitcointalk.org/index.php?topic=305791.0 2013

② Maxwell G. Confidential Transactions. https://people.xiph.org/~greg/confidential_values.txt 2015

③ The Bitcoin lightning network: Scalable off-chain instant payments, https://blog.bitmex.com/wp-content/uploads/2018/01/lightning-network-paper.pdf 2016

④ Raiden Network. What is the raiden network? https://raiden.network/101.html 2018

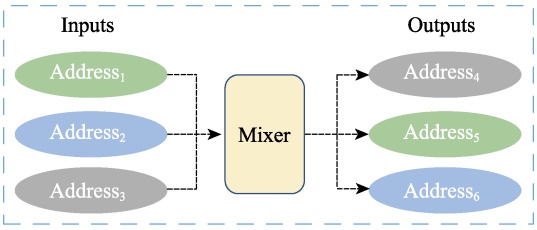

图 6 中心化混币原理示意图

2018 年，Tran 等人[29]通过将混币技术与可信执行环境（Trusted Execution Environment，TEE）相结合提出了 Obscuro 协议，通过将混币的执行操作与混币服务提供商的其他操作相隔离，防止恶意的混币提供商窃取用户存款的行为，同时由于没有增加额外的计算操作，从而具有较高的混币效率.

（2）去中心化混币

去中心化的混币技术由多个分布式的服务器共同执行某一混币协议. 去中心化混币需要用户在网络中寻找其他同样需要混币的用户（如图 7 所示），该种方式允许两个或更多的交易被合并到一个混币交易中. 由于合并以后的交易实际是由多个单独交易的输入和输出组合而成，因此，攻击者想要寻找输出和输入之间的关系将变得更加困难.

2013 年，Maxwell 基于去中心化的思想提出了 CoinJoin 协议. 该协议允许将多笔具有相同金额的交易合并为一笔交易，参与用户在确定自己的输出地址包含在该交易的输出后对交易进行签名，最终形成一笔多签名的比特币交易. 虽然该方法使得外部的观察者无法分析得到交易输入输出之间的关系，但参与混币交易的其他用户却可以得知该关联关系. 在数字货币领域，以匿名性保护为主旨的 Dash 币采用了改进后的 CoinJoin 技术.

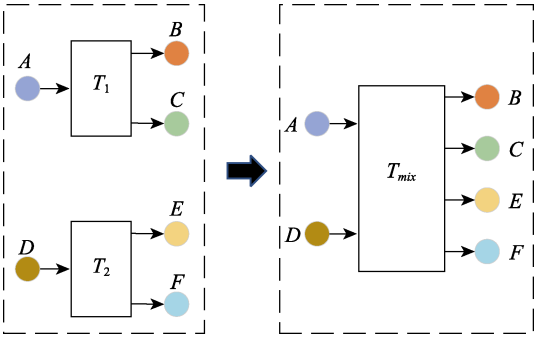

图 7 去中心化混币原理示意图

2014 年，Ruffing 等人[30]在 CoinShuffle 中引入了可审计的匿名群组消息传递协议 Dissent. 该协议首先允许每个用户生成一个临时的公钥对并将公钥进行广播；其次，该协议将参与用户进行排序，每个用户 i 依次使用用户 j（j>i）的公钥对它的输出地址进行多层加密，然后转发至第 i+1 个用户. 第 i+1 个用户在接收到消息后利用自己的私钥从消息中剥离一层加密信息，然后采用相同的方式将自己的输出地址加密后转发至下一个用户. 最终，最后一个用户将所有的消息进行解密获得所有的输出地址，并加入自己的输出地址进行混淆. CoinShuffle 避免了混币系统的内部成员作恶的可能，提供了内部隐私性. 但多次加密增加了系统的计算成本，降低了交易速度.

CoinShuffle++协议通过将 CoinShuffle 中的解密混合网络替换为基于 DC-net（Dining Cryptographer net）设计的 DiceMix 协议[31]，通过密钥共享的方式混淆用户与其交易输出地址之间的关联关系，从而在保证内部隐私性. 由于 DiceMix 协议无需复杂的加解密运算，因此 CoinShuffle++能够在达到与 CoinShuffle 相同安全目标的同时，又能实现很高的交易处理速度.

4.4 匿名性保护案例分析

在实际的数字货币项目中，研发人员通常会综合采用多种匿名性保护方案，从多个层面保障交易的匿名性. 本节以典型的数字货币项目为例，对上述匿名性保护方案在实际数字货币中的应用情况进行介绍和分析. 表 3 展示了典型的匿名性数字货币实现交易的不可标识性、不可链接性以及不可追踪性所采用的匿名性保护方案.

（1）Zerocoin

Zerocoin 是一种采用了零知识证明技术的比特币扩展方案，主要通过铸币交易（mint）和花费交易（spend）两种交易类型来扩展比特币.

当用户有匿名性保护的需求时，可以通过铸币交易将一定数量的比特币转换成 Zerocoin. 用户可以将自己未花费的比特币放在基于零知识证明技术构建的密码累加器中与其他人的资产进行混币，并获得拥有该资产的承诺. 当用户需要花费 Zerocoin 时，可以根据公开承诺和资产金额的方式来证明自己拥有一定数额的资产，矿工验证通过后会将等额的比特币发送至目的地址. 在上述交易的过程中，用户通过公开承诺的方式完成了花费交易，并没有暴露自己的发送地址，因而观察者无法将用户及其花费地址相关联，交易的不可链接性得到了保证.

（2）Zcash

Zcash 是一种采用了零知识证明技术的数字货币，矿工通过验证交易附带的证明，可以在无需掌

表 3　典型的匿名性数字货币概览

数字货币	上线时间	不可标识性	不可链接性	不可追踪性
Zerocoin	2016 年 10 月	–	NIZK	–
Zcash	2016 年 10 月	–	Halo（2021 年 10 月之后）	Halo（2021 年 10 月之后）
Monero	2014 年 5 月	I2P 网络	环签名、环机密交易、一次性地址	环签名、机密交易、一次性地址
Beam	2019 年 1 月	–	机密交易、单向聚合签名	CoinJoin
SERO	2019 年 6 月	–	Super-ZK	Super-ZK

握交易具体金额的情况下验证交易的合法性.

Zcash 提供了两种类型的交易地址供用户选择：一类是透明地址（t-address，下文称 t 地址），该类地址在形式上比特币地址相同；另一类是屏蔽地址（z-address，下文称 z 地址），该类地址不会在公开账本中显示，其作用是证明有一个有效的交易地址参与了交易，存放在 z 地址中的资产被视为在屏蔽池（Shielded pool）中，发送至 z 地址或由 z 地址发出的交易金额都是不可见的. 根据交易地址的不同，Zcash 中的交易可以分为两种类型. 第一类是仅涉及 t 地址的透明交易，该类交易的机制与比特币交易相同，其交易信息都会存储在公开账本中；第二类是涉及 z 地址的屏蔽交易，该类交易使用零知识证明隐匿交易的金额与地址，但会收取额外的交易费用. 图 8 展示了 Zcash 中的四种交易模式，分别为 t-to-t，t-to-z，z-to-t 以及 z-to-z.

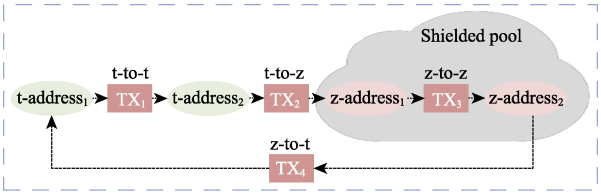

图 8　Zcash 不同类型的交易模式

在 Zcash 的交易中，z 地址的使用方式决定了交易匿名性的保护程度. 当用户采用 z 地址作为其交易发送地址或接受地址时，z 地址的特性使得交易发送方或交易接收方的信息不会记录在账本中，从而避免了观察者利用账本信息推测用户及其控制地址之间的关联关系，保护了交易的不可链接性；当交易的发送方和接收方同时采用 z 地址进行交易时，不仅隐藏了账本中的交易信息，同时也在一定程度上切断了交易双方之间的关联性. 因此，零知识证明技术在屏蔽交易中的使用，不仅可以保护交易的不可链接性，同时也可以起到保护交易不可追踪性的效果.

（3）Monero

Monero 是基于 CryptoNote 协议开发的一种匿名性数字货币，采用了包括匿名网络技术、环签名技术、同态加密技术以及一次性地址（One-time addresses）技术[①]在内的多种匿名性保护技术，这些技术的综合使用从多个层面保护了 Monero 交易的匿名性. 在不可标识性方面，该货币采用匿名网络技术隐藏其网络节点信息，可以有效避免观察者将交易地址及其现实身份相互关联；在不可链接性方面，该货币采用环签名技术隐藏交易发送方的交易地址，采用同态加密技术隐藏交易金额，采用一次性地址技术隐藏交易接收方的地址，这些技术分别隐藏了账本中不同的交易信息，避免了观察者通过账本信息分析用户及其账户间的关联关系；在不可追踪性方面，上述多种技术的综合使用，进一步切断了交易双方之间的联系，防止观察者根据交易参与方之间的关联性来跟踪交易的资金流向.

（4）MimbleWimble

MimbleWimble[②]是一种集成了机密交易技术、混币技术、单向聚合签名技术的隐私保护协议，由化名为 Tom Elvis Jedusor 的研究人员于 2016 年 8 月提出. 目前，基于该协议开发的代表性数字货币有 Grin 和 Beam，并且都于 2019 年年初上线.

MimbleWimble 协议可以较好地解决 Monero 中存在的交易匿名性与可扩展性之间的矛盾. 在 Monero 区块链中，虽然环签名技术保护了 Monero 交易的匿名性，却额外带来了由于交易数据过大而引起的区块整体的扩展性难以提高的新问题. 目前，Monero 已经通过采用 Bulletproofs 技术在一定程度上缓解了该问题，但单笔交易数据的大小依然超过 3kb，而 MimbleWimble 协议在使用 Bulletproofs 技术后交易大小仅约为 2.5kb. 同时，MimbleWimble 协议与交易合并技术（cut-through）的结合使得区块链存储状态更简介，进一步增加了 Grin、Beam

① https://www.getmonero.org/resources/moneropedia/stealthaddress.html

② https://github.com/mimblewimble/grin/blob/master/doc/intro.md

表 4 不可标识性对抗分析方法总览

分 类	方 法	效 果	限 制	数字货币	相关文献
交易创建阶段	通过控制远程节点向客户端返回错误消息，诱使客户端多次发送交易请求，利用请求信息推测交易的真实输入	关联真实输入及其始发节点	当客户端验证服务器身份时，会使该方法失效	Monero	[32]
	观察者通过重传攻击的方式截获并分析客户端发往全节点的 Bloom 过滤器	关联交易及其 SPV 客户端	Bloom过滤器中携带的无关交易会降低该方法的准确度	比特币	[33]
交易传播阶段	利用“超级节点”收集网络中的传播消息，根据消息到达时间推测网络拓扑	关联交易及其始发的服务器节点	不能关联到客户端节点	比特币	[13-15]
	特殊交易仅可被始发节点转发一次而不能被二次转发	关联交易及其始发的服务器节点	异常交易的数量仅占所用交易数据集的 9%	比特币	[40]
	通过构建“地址指纹”标识客户端节点中维护的对等节点地址列表，可标识采用 Tor 网络的用户节点	关联通过 Tor 发送的交易及其始发的服务器节点	“地址指纹”容易随着对等节点地址列表的更新而失效	比特币	[34]
	通过 AS 窃听网络中的传播消息，根据消息分析交易的始发节点	关联交易及其始发节点	无法对加密的交易信息进行分析	比特币、以太坊	[38]
交易验证阶段	客户端处理自己为收款人的交易，会花费额外的时间，可以发现交易与接收节点之间的关联	关联交易及其接收节点	易受到网络波动的影响	Monero 、Zcash	[39]
	客户端处理畸形交易时，会向对等节点返回错误响应	关联公钥及其接收节点	仅可关联已知公钥的交易及其接收节点	Zcash	[39]
	客户端刷新时会向远程节点请求交易列表，当发现与自己相关的未确认交易时会再次向远程节点发起请求	关联交易及其接收节点	交易频率升高时该方法有效性将会降低	Monero	[39]

等数字货币的可扩展性.

（5）SERO

超零币（Super Zero，SERO）[①]是一种采用 NIZK 技术，并且支持图灵完备智能合约的匿名性数字货币，该数字货币不仅支持对交易的匿名性保护，还可以实现对智能合约交易的匿名性保护.

SERO 可以作为 Zcash 的一种改进方案. 虽然 Zcash 在持续地迭代零知识证明协议以解决零知识证明生成过程中出现的各种问题，但由于 Zcash 采用了与比特币网络相同的底层架构，其本质上仍然是一个内置匿名性保护机制的比特币网络，仅可支持简单的数字交易. 同时，仍然存在证明生成时间过长的问题. SERO 使用的零知识证明协议 Super-ZK 通过采用 ALT_BN128 曲线和 Groth16 预处理方案来替代 PGHR13 预处理方案，缩短了整体预处理时间的 1/3，大幅提高了零知识证明的生成速度. 这些改进使得 SERO 不论在应用场景的多样性方面还是在交易速度方面都要优于 Zcash.

5 数字货币交易的匿名性对抗方案

虽然研究者们已经采取了一系列的措施来保护数字货币交易的匿名性，但在实际的交易中，这些保护方案所提供的匿名性是有限的，观察者们依然能够根据交易过程中留下的蛛丝马迹对交易的匿名性进行分析. 针对上节中提到的匿名性保护方案，本节依然从不可标识性、不可链接性和不可追踪性三个方面对当前阶段的匿名性分析方法进行归纳和总结.

5.1 不可标识性对抗

在当前已有的匿名性研究中，不可标识性的对抗分析主要利用数字货币交易的各个阶段所产生的流量信息，并结合 P2P 节点的 IP 地址、地理位置、所属组织等信息，对目标交易真实的身份信息进行标识. 目前已有的分析工作[32-40]分别利用了交易创建阶段、交易传播阶段以及交易验证阶段三个不同阶段的信息对交易的不可标识性进行分析. 表 4 总结了目前已知的不可标识性对抗分析方法.

（1）利用交易创建阶段的信息

在交易创建阶段，用户需要通过交易客户端与 P2P 节点进行交互，从而将交易请求在全网转发. 在二者进行交互的流量数据中携带了具有客户端标识的信息，通过分析这些信息可以推测出交易及其始发节点之间的关联关系. 目前，该类研究主要集中

① https://sero.cash/cn/

于比特币以及 Monero 的交易创建阶段[32-33]. .

在 Monero 的交易创建阶段，交易客户端需要向远程节点发送交易请求，远程节点在接收到交易请求时会对交易请求进行验证. 若验证不通过，节点会中止交易进程并向客户端返回错误响应. 2018 年，Lee 等人[32]控制远程节点向客户端返回错误的响应信息，以诱使客户端多次发送交易请求，通过分析交易请求中包含的公钥信息推测出了交易的真实输入（如图 9 所示），进而可以得到交易真实输入与客户端之间的关联关系. 该方法利用对多个环签名所包含的公钥集合求交集的思路寻找交易的真实输入，其准确率由客户端多次构造的环签名之间的结构差异性来决定.

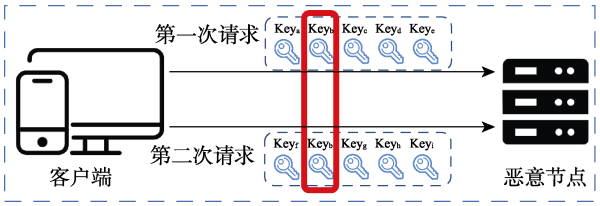

图 9　远程节点攻击示意图

在针对比特币交易创建阶段的不可标识性分析中，观察者通过分析 Bloom 过滤器有可能获知 SPV 节点创建的交易，并且针对某一 SPV 节点获得 Bloom 过滤器数量越多，可推测关于该 SPV 节点的地址信息也就越多. 因此，捕获 Bloom 过滤器成为观察者们进行不可标识性分析的一个前置条件.

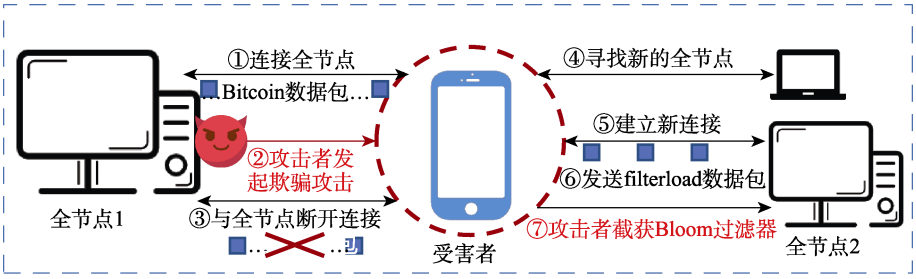

图 10　通过重传攻击获得钱包的 Bloom 过滤器

2021 年，Hu 等人[33]切断了 SPV 节点与某一全节点之间的连接，利用 SPV 节点会自动向新连接的全节点发送 Bloom 过滤器这一规律，捕获了 SPV 节点发往全节点的 Bloom 过滤器；同时，作者进一步将 SPV 节点的网络接口停机超过 5s，利用 SPV 节点在断开网络连接 5s 后会重新发送 Bloom 过滤器这一规律，捕获得到该 SPV 节点的第二个 Bloom 过滤器. 图 10 展示了利用这两种欺诈攻击的方式捕获 Bloom 过滤器的过程. 实验结果表明，通过 Bloom 过滤器可以识别得到客户端所控制的交易地址的信息. 当针对同一 SPV 节点能够获得两个 Bloom 过滤器时，观察者能准确的从交易集中筛选得到属于该 SPV 节点的交易地址. 因此，通过 Bloom 过滤器标识交易的身份信息是有效的.

（2）利用交易传播阶段的信息

在交易传播阶段，交易信息会按数字货币网络中的消息传播规则在 P2P 节点之间转发. 当观察者可以收集到网络中的传播消息时，便可以结合消息内容以及转发消息的次序对交易的始发节点进行推测. 该类研究根据分析方法的不同可分为基于传播协议的分析[14-15]和基于网络设施[34-38]的分析.

基于传播协议的分析依据数字货币中的消息转发规则，根据消息到达观察节点的时间推测消息的始发节点. 一种较为典型的思路是，在数字货币的网络中部署一个可以与 P2P 网络中大多数节点建立连接的“超级节点”，利用可控节点向网络中发送交易，然后根据“超级节点”从相邻节点中接收到该笔交易的时间来推测消息的传播路径，进而分析得到交易的始发节点. 但是，由于该方法需要维持大量连接，并需要不断的向所有连接节点发送消息，这会对交易网络造成严重干扰. 因此，如何隐蔽的利用节点间的转发消息分析始发节点是标识交易身份的主要难点.

2018 年，高峰等人[15]提出了一种基于探针节点的轻量级溯源机制，核心思想是根据已知交易从不同节点转发至探针节点的次序，推测待监测节点的拓扑结构，进而推测待监测节点的始发交易. 图 11 展示了利用探针节点探测网络拓扑的系统架构. 由于探针节点仅接收交易而不发送交易，因此不会对比特币网络的运行造成干扰.

基于网络设施分析的核心思想是在分析交易数据的基础上结合互联网基础设施中的访问痕迹来对交易的不可标识性进行分析.

由于数字货币网络中的任何一笔交易都需要经

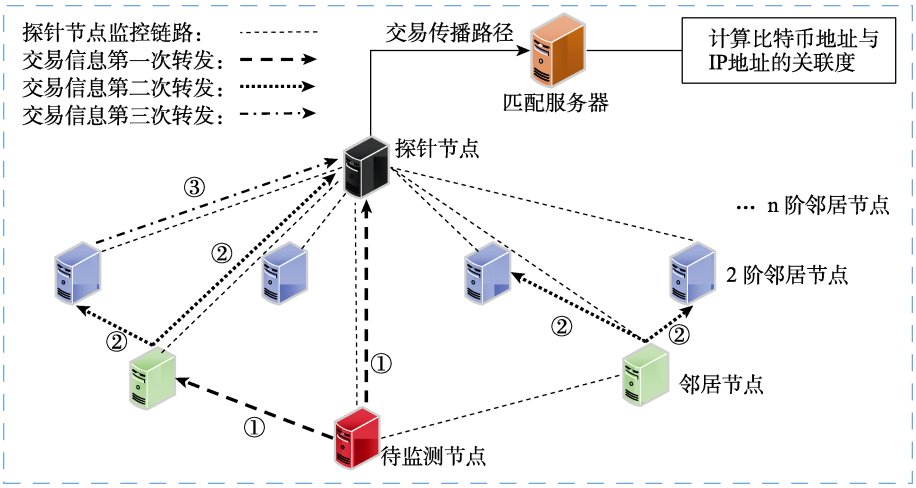

图 11 利用探针节点收集网络中的交易信息[15]

由路由器、节点服务器等网络设备在网络中转发，而在转发交易的过程中会不可避免的在网络设备中留下访问痕迹，这些痕迹会暴露用户的网络层信息. 例如，比特币的节点服务器中存放有对等节点的地址列表，当向其中注入具有标识性的地址组合时，便可通过地址指纹识别该节点[34]，该方法可以用来识别利用 Tor 网络的比特币节点.

另外一种思路是利用交易在转发过程中经由自治系统（Autonomous System，AS）时留下的访问痕迹进行分析. 构成数字货币网络的 P2P 节点分布于不同 AS 中，交易信息在网络中转发时会经过 AS 的网络边界[38]. 因此，拥有网络资源的观察者可以窃听流经 AS 的交易消息，并利用目标节点的始发交易所特有的性质，从窃听得到的海量交易中识别目标节点的始发交易，实现交易及其始发节点的关联. 该种方法不仅可以识别比特币网络中不加密的交易数据，还可以结合未加密的数据包头分析以太坊网络中加密的交易数据.

（3）利用交易验证阶段的信息

在交易验证阶段，交易客户端会验证 P2P 节点转发的交易. 交易客户端在验证不同类型的交易时其运行状态不同. 目前针对交易验证阶段的研究，主要通过观察交易客户端的行为差异来分析交易与接收节点之间的关联性.

交易客户端处理自己为收款人的交易时会泄露交易匿名性信息. Zcash 的交易客户端在处理自己是收款人的交易时，会在执行完交易的解密操作后进一步验证交易的有效性，这一验证行为会暴露交易与客户端之间的关系. 因为客户端在验证交易有效性时需要花费额外的时间，通过观察这一时间差，观察者便可以判断客户端与接收交易之间的关联性. 2020 年，Tramer 等人[39]在客户端收到交易后立即向其发送 ping 消息，通过测量响应时间判断交易关联性. 作者发现该方法能够有效识别交易与客户端的关联性，客户端会多花费大约 1ms 的时间来处理自己为收款人的交易，但该方法容易受到网络波动的影响.

交易客户端处理畸形交易时会泄露交易匿名性信息. Zcash 的交易客户端在处理错误格式的交易时，首先会利用私钥对交易密文进行解密，然后检查字节编码协议的版本. 当发现版本错误时，客户端将会向发送该交易的对等节点返回错误响应. 观察者通过某一节点向其连接的所有 P2P 节点发送错误的交易信息，可以通过是否返回错误响应来判断该公钥与 P2P 节点之间的关联性，因为只有掌握该公钥的交易客户端可以成功解密该交易. 但该分析方式仅可针对已知地址进行分析，受限于观察者已掌握的地址数量.

交易客户端处理未确认交易时会泄露交易匿名性信息. Monero 的交易客户端在自动刷新时，首先会向 P2P 节点请求未确认的交易列表，当收到的交易列表中存在有以自己为收款人的交易时，会再次向 P2P 节点请求关于自己钱包地址的交易内容. 由于 Monero 的交易频率不高，因此两次交易间隔之间客户端与节点的通信行为很容易观察. 该方法在低频交易中具有很好的识别效果，但是随着 Monero 交易频率升高，该方法的效果会逐渐降低.

5.2 不可链接性对抗

目前针对交易不可链接性的分析，主要通过观察公开账本中的交易记录，根据交易金额、资金流向、交易时间等属性发现用户地址与交易之间的关联性. 根据分析所依赖账本数据的不同，已有方法

可分为三类：基于交易输入的分析、基于交易输出的分析以及基于交易模式的分析[41-49]. 表 5 总结了目前已知的不可链接性对抗分析方法.

（1）基于交易输入的分析

目前基于交易输入的分析主要通过多输入的启发式方法，将同一交易的多个输入地址关联至同一用户. 以图 12 为例，图中地址 1、地址 2 和地址 3 为同一笔交易的多个输入，地址 4、地址 5 和地址 6 为同一笔交易的多个输入，依据该方法可以判定它们分别由两个用户实体控制. 该方法成立的前提条件是：用户花费账户中的 UTXO 时需要使用自身的私钥对交易签名，而私钥并不会与他人共享.

表 5　不可链接性对抗分析方法总览

分　类	方　法	效　果	限　制	数字货币	相关文献
交易输入	将同一交易中的输入地址认定为由同一用户控制	关联输入地址	存在假阳性，且无法验证有效性	比特币、Zcash	[41][16]
	若两个或两个以上的地址向交易所控制的同一个地址发送货币，则认为这些地址具有共同的社交关系	关联输入地址	仅适用于交易所场景	所有数字货币	[41]
交易输出	同一交易中，将找零地址与交易输入识别为属于同一用户	关联输出地址	找零地址的判断标准不统一	比特币、Zcash	[44][49]
交易模式	将往返交易模式中的输入输出地址识别为统一用户	关联屏蔽交易的 t 地址	可能将不同用户的 t 地址识别为由同一用户控制	Zcash	[45-46]
	将创始人交易模式中的输出地址识别为由创始人控制的地址	关联屏蔽交易中的创始人地址	仅可通过咨询创始人确定有效性	Zcash	[16]
	将矿工交易模式中的输出地址识别为矿工地址	关联屏蔽交易中的矿工地址	无法验证有效性	Zcash	[16][44][47]

表 6　不可追踪性分析方法总览

分　类	方　法	效　果	限　制	数字货币	相关文献
识别真实输入	利用 0-mixin 交易对拥有更多混淆输入的交易进行级联分析	识别真实输入	受限于官方对最小 mixin 的要求	Monero	[17]
	将最新的公钥所签署的输入识别为交易真实输入	识别真实输入	受限于官方对混淆交易的采样算法	Monero	[17]
跟踪交易资金	通过污点分析的方式来分析交易地址与混币交易之间的关联关系	关联交易参与方	依赖于特定平台所提供的污点分析功能	BTC	[50]
	通过匹配交易输入和交易输出间的交易金额来恢复参与双方之间的关联关系	关联交易参与方	存在多种匹配的情况	所有数字货币	[41][48]
	根据混币交易输出的数量和金额特征分析混币交易的运行机制，并通过种子输入的方式标记混币地址	关联交易参与方	仅适用于完全依靠链上机制运行的混币服务	BTC	[51]
	针对屏蔽交易，通过观察屏蔽交易输入和输出的数量来发现屏蔽交易参与方之间的关联性	关联交易参与方	仅可识别目标地址从屏蔽池第一跳的金额转移	Zcash	[47]
	针对屏蔽交易，利用第三方在零知识证明的生成阶段加入标识信息	关联交易参与方	加入标识信息需要花费大量的计算成本	Zcash	[47]

后来，研究者们也尝试将该方法拓展到其他数字货币的交易匿名性分析中. 2018 年，Kappos 等人[16]采用该方法对 Zcash 中利用 t 地址发起的交易进行聚类分析，因为 Zcash 中的显露交易与比特币交易的形式相同. Klusman 等人①尝试利用多输入法对以太坊中外部账户之间的外部交易进行分析. 但是，由于以太坊中外部账户的交易是以账户状态的方式记录账户中的资金变化[42]，并不存在多地址输入的情况. 因此，多输入法并不适用于对以太坊中的交易分析.

（2）基于交易输出的分析

目前基于交易输出的分析主要通过找零地址的启发式方法，将交易的找零地址与交易的输入地址

① Deanonymisation in ethereum using existing methods for bitcoin https://www.os3.nl/_media/2017-2018/courses/rp1/p61_report.pdf 2018

认定由同一个用户控制. 该种方法的前提条件是UTXO 模型的一个重要特征，即无法分割. 例如，当比特币作为某一交易的输入时必须被一次性花费，分割比特币的唯一方法是使用找零地址，将输入地址中多余的比特币返还给发送方.

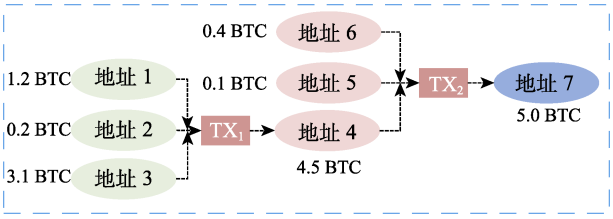

图 12 多输入法判断实例

找零地址法最初是为了分析比特币中的关联交易而提出. 后来，研究者们同样将该方法拓展到其他数字货币的交易匿名性分析中. 最直接的应用是分析 Zcash 中的显露交易. Zhang 等人[44]指出若一个显露交易有两个输出且其中一个输出的金额是另一个输出金额的 20 倍以上，则认为金额较小的地址为找零地址. 该种方法实现思路简单但适用范围小，当 Zcash 的输出地址为 z 地址时，则会因无法观察到输出金额而失效.

2018 年，Kappos 等人[16]在显露交易的研究基础之上进一步的针对 Zcash 中的屏蔽交易展开深入研究. 作者发现当一个用户欲将账户中的一部分货币存入屏蔽池时，剩余货币将会以找零地址的方式返回用户. 基于这一观察，作者提出了新的找零地址规则：若一个（或更多）地址是一个屏蔽交易的输入 t 地址，第二个地址是同一个屏蔽交易的输出 t 地址，且该 t 地址为唯一的输出地址，那么第二个地址与输入地址属于同一实体. 该方法进一步扩大了找零地址法的适用范围，但该方法在面对多输出的交易时效果有限.

（3）基于交易模式的分析

通过分析目前的交易资金在 Zcash 不同类型的地址间的流通方式，本文将当前 Zcash 中的交易总结为以下三种模式：往返交易模式、创始人交易模式以及矿池交易模式.

往返交易模式. 该模式是用户将资金从一个地址发往另外一个地址，短时间后又将资金从另一个交易地址中取回. 用户发起该种交易模式往往出于隐藏自己消费行为的目的. 例如，一定数额的 Zcash 首先从一个 t 地址发送到屏蔽池中，不久之后，相同或具有相似金额的货币从屏蔽池中发至另外一个 t 地址（图 13 所示）. 基于往返交易模式的假设，便可以认为这两个 t 地址属于同一用户[45].

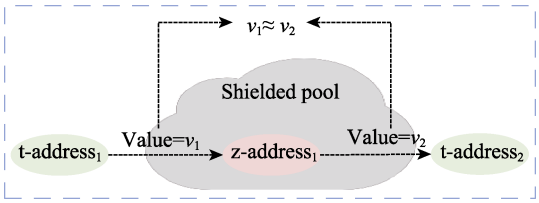

图 13 Zcash 中的往返交易模式

2019 年，Biryukov 等人[46]对往返交易模式进行了更深入的研究，提出了基于交易手续费的分析方法. 作者观察发现 Zcash 中的交易手续费默认为 10^4Zatoshi①. 当后一笔交易与前一笔交易的金额差为 $n\cdot10^4$ Zatoshi 时（n<10），证明用户的资金在屏蔽池中可能经过了 n 个 z-to-z 的交易，并最终转回用户控制的地址中. 该方法发现了往返交易中更明显的金额特征，提高了往返交易模式的辨识度.

创始人交易模式. 这里的创始人指 Zcash 的创始人（Founder）. 创始人交易模式包括了 Zcash 中所有交易金额为 250.0001 ZEC 的 z-to-t 交易. 该模式的提出基于观察 Zcash 创始人控制的交易地址在一段时期内的交易行为，因为 Kappos 等人[16]发现创始人常常以 249.9999 ZEC 为单位向屏蔽池中存入货币，并以 250.0001 ZEC 为单位从屏蔽池中转出. 该模式揭示了创始人从挖矿奖励中取款的行为，通过该模式可以将属于创始人的交易相关联. 但该方法的准确性仅能通过咨询创始人确定，除此以外，尚无其他有效的验证方法.

矿池交易模式. 该模式揭示了矿池向矿工发放挖矿奖励的行为. 由于矿池由大量的矿工节点组成，故矿池给矿工发放挖矿奖励的交易具有大量的输出. 在 Zcash 中，根据矿池控制的交易地址是否在屏蔽池可以分为两种情况. 第一种情况是，矿池将挖矿奖励从屏蔽地址转发至矿工的透明地址[47]. 该种情况在交易形式上表现为 z-to-t 的多输出交易. 针对该情况，Kappos 等人[16]指出若一笔 z-to-t 交易拥有超过 100 个输出，且其中一个输出地址属于已知矿池，则认为所有输出地址都属于矿工. 第二种情况是，矿池直接通过透明地址向矿工地址发送奖励. 该种情况在交易形式上表现为 t-to-t 的多输出交易. 针对该情况，Zhang 等人[44]指出若一笔交易中输出地址个数超过 50 则认为该交易是矿池交易.

① 1 ZEC=10^8 Zatoshi

5.3　不可追踪性对抗

虽然研究者采取了一系列措施以混淆交易参与方之间的联系，但是随着交易分析技术的发展，观察者们开始结合账本以外的信息实现对交易的追踪. 目前已有的研究工作根据目的不同可以分为两类：识别交易的真实输入以及跟踪交易的资金流向. 表 6 总结了目前的不可追踪性对抗分析方法.

（1）识别交易的真实输入

匿名性保护机制可能会隐藏交易的真实输入，例如环签名技术会隐藏 Monero 交易的真实输入. 交易发送方的混淆给追踪交易带来困难. 因此，识别交易的真实输入对交易的不可追踪性分析而言是不可缺少的一环. 目前分析 Monero 真实输入的方法主要有级联分析方法和最新采样分析方法.

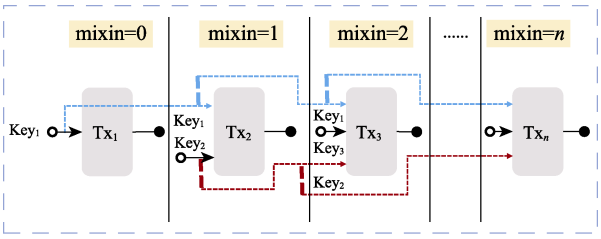

图 14　级联分析示意图

级联分析方法. 该方法是一种针对 Monero 真实输入的典型分析方法[17]，可以利用 0-mixin（即输入中不包含混淆输入）交易迭代的对 1-mixin 交易，2-mixin 交易乃至带有更多混淆交易的输入进行分析. 如图 14 所示，TX_1 是一个 0-mixin 交易，因此可以确认 TX_1 输入中的公钥 Key_1 是已花费的公钥. 当 TX_2 使用公钥 Key_1 作为 mixin 时，可以很容易的推知公钥 Key_2 签署的交易为真实输入. 依此类推，可以推知后续 TX_3 乃至 TX_n 的真实输入. 该分析方法的准确率可达 100%，研究者常将该方法得到的结果作为验证集来检验其他分析方法的准确率. 但是随着 Monero 官方对最小 mixin 数量的不断提高①，该方法的有效性不断降低.

最新采样分析方法. 该方法的思想是，在一个环签名中，位于最新区块的公钥所签署的输入为真实输入[17]. 该方法利用了系统选择混淆交易的采样机制中存在的漏洞，因为基于该采样方法构造的环签名中的公钥往往来自于更早的区块中. Monero 于 2015 年 4 月开始采用三角形分布（Triangular Distribution）采样算法，新的采样算法增加了新的输出公钥作为 mixin 的概率.

（2）跟踪交易的资金流向

跟踪交易的资金流向要求观察者可以将交易的发送方与接收方相互关联. 部分数字货币采用零知识证明、混币等匿名性保护技术来混淆交易发送方与接收方之间的关系. 因此，当前的不可追踪性对抗分析主要围绕这些匿名性技术开展.

目前针对混币交易的对抗分析，主要通过观察混币交易的交易数据，并结合不同混币服务的运行机制和交易特征对混币交易进行实证分析.

2013 年，Moser 等人[50]首次针对混币技术进行实证分析. 作者首先创建以自己所掌握的地址为目的地址的混币交易，当交易完成后，利用 Blockchain.info 提供的污点分析功能对混币交易的发送地址进行分析. 污点分析功能可以通过分析交易图的方式得到指定的交易地址与混币交易之间的关系，进而推测出混币交易的输入与输出之间的联系. 然而，当前混币交易采用了更大的混淆群组和更多的混淆次数，使得早期的污点分析功能很难精确的推测输入与输出之间的关系.

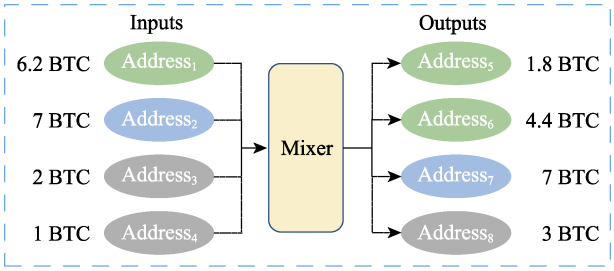

图 15　交易金额匹配识别

2017 年，Chen 等人[48]通过匹配交易金额的方式来恢复混币交易参与方之间的关联关系. 由于用户会向混币服务中存入和取出相同金额的资产，因而可以通过匹配金额组合的方式，分析拥有多个交易输入和输出的混币交易. 如图 15 所示，地址 3 和地址 4 的输入值与地址 8 的输出匹配. 因此，地址 3、地址 4 和地址 8 可能属于同一个用户.

上述思路也同样适用于对跨链交易的资金追踪. 用户会向跨链服务中存入和取出相同金额的数字货币. 2019 年，Yousaf 等人[41]结合跨链交易所提供的交易信息，通过比对跨链交易中转入区块链与转出区块链中交易时间相近的交易所携带的交易金额，将金额相似的交易相匹配. 该方法实现了跨链交易的资金追踪，但可能会在交易输入和输出的区块链账本中发现相近时间段内多笔符合条件的交

① 在 Monero 当前的版本中（v0.17.2.3），系统对于构成交易所需 mixin 的最小数量已提高至 10 个.

易，导致无法确定哪一笔是实际的跨链交易.

2021 年，Wu 等人[51]通过分析 Chipmixer、Wasabi Wallet、ShapeShift 和 Bitmix.biz 等 4 种代表性混币服务的交易信息，根据混币交易输出的数量和金额的特点，将现有混币技术的运行机制划分为混淆和交换两种，并通过跟踪种子输入的方式进一步对混淆机制下的混币地址进行标记和识别. 该分析方法从运行机制的层面对混币交易进行分析，具有一定的通用性. 但是，由于该方法仅考虑了一些完全依赖于链上机制的传统的混币技术，当面向复杂的混币技术（例如 Blindcoin、Mixcoin 等）时，该方法的分析效果是有限的.

针对采用零知识证明的交易分析，目前主要通过观察零知识证明协议的运行情况，并结合显露的交易信息，对 Zcash 中的屏蔽交易进行分析.

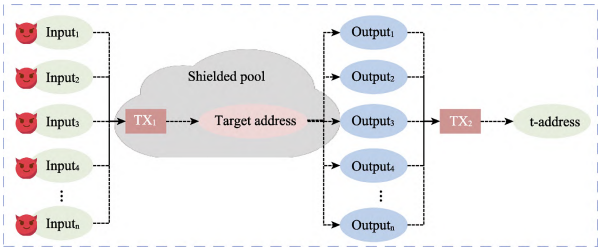

图 16 Zcash 中的“扬尘”攻击

一种分析方法是通过向待观察的 z 地址发送大量的小额输出，该 z 地址的拥有者为了花费这些输出，会创建一个多输入单输出的显露交易. 观察者只需观察网络中拥有多个输出的 z-to-t 交易，即可判断该 z 地址的资金流向. 该方法利用了 Zcash 中运行的 Sapling 协议存在的漏洞，即不能隐藏屏蔽交易输入和输出的数量. 如图 16 所示，观察者可以通过观察屏蔽交易的输出数量来判断目标地址的资金流向，但该方法仅能识别目标地址从屏蔽池第一跳的金额转移，不能识别后续的金额.

另一种分析方法则是在生成 zk-SNARK 证明的过程中嵌入标识性信息，交易验证者在验证交易时便可通过该信息确定该笔交易的发送方. Biryukov 等人[47]观察发现 Sapling 协议允许交易用户在生成 zk-SNARK 证明的过程中仅生成交易所需的签名而将构造证明的复杂操作交给不可信的第三方服务器. 基于这一发现，观察者可以通过第三方服务器在生成证明的过程中嵌入隐藏信息. 该方法只增加了 6%的证明生成时间，几乎不会被监测系统发现. 但嵌入信息所需的计算复杂度是指数级，这会限制嵌入标识信息的规模.

6 未来研究趋势与挑战

数字货币交易的匿名性研究是当前数字货币监管领域内的一个研究热点，从数字货币交易的匿名性保护到针对匿名保护机制的对抗研究，从交易的不可标识性研究、不可链接性研究再到不可追踪性研究，从交易创建阶段的研究到交易验证阶段研究，可以说，数字货币交易匿名性的研究当前处于百家争鸣的状态. 但是，交易匿名性保护的研究与交易匿名性分析的研究始终处于动态发展的状态，二者在对抗博弈的过程中推动交易匿名性研究不断朝着更深入的方向发展. 因此，随着密码保护技术和交易分析技术的不断进步，交易匿名性的研究会面临许多新的挑战.

6.1 交易的匿名性分析

目前匿名性分析的工作已经能够较为全面的从不同的角度对交易的匿名性进行不同程度的分析. 但总体来看，这些研究尚不够深入. 因此，未来关于匿名性分析的研究将会继续围绕数字货币的交易机制提出更深入的分析方法.

从交易不可标识性的角度考虑，目前标识交易身份的方案都是通过读取 P2P 节点之间传播的明文消息来推测交易的始发节点. 当面对加密连接的情况时（如 Ethereum）[38]，该种分析方法将失效. 因此，寻找一种能够从加密流量中提取有效信息的方法是需要解决的一个问题.

从交易不可链接性的角度考虑，目前将交易地址关联至用户实体的启发式方法建立在研究者根据交易规律而做出的假设之上，利用这些分析方法所构建的用户实体是否能够与真实世界中的用户相对应，尚无法验证. 同时，尚缺少具有影响力的公开交易数据集，研究者在自己采集到的交易数据中得出的方法准确率不具备普遍性.

从交易不可追踪性的角度考虑，当前多数的对抗性分析方案仅支持对一跳交易的追踪，无法针对一笔金额的多跳交易实现真正意义上的交易追踪.

基于匿名性分析研究所面临的挑战，本文认为以下三个方面将成为未来的研究趋势：

（1）通用的身份标识方法. 识别数字货币网络中节点之间通讯的加密流量信息，对于交易标识效果的提升是巨大的. 目前，已有许多工作利用加密流量分析技术对用户行为进行识别. 例如，Shen 等人[52]利用加密流量分析技术对以太坊中的 Dapp 进行分类. 这些工作对于识别数字货币交易中节点之间的加密信息具有借鉴意义. 因此，结合加密流量

分析的技术，设计适用于多种数字货币系统的交易标识方法，是未来的研究方向.

（2）可验证的启发式规则. 不可否认启发式的聚类规则在寻找数字货币的用户实体中所发挥的巨大作用，但更加准确的启发式规则可以有效的提高研究人员对于用户实体所控制交易的准确程度. Meiklejohn 等人[49]利用已掌握的数据集对找零地址启发式方法的进一步规范，有效的降低了 23%的假阳性. 因此，通过对用户习惯的观察和交易机制的分析，研究更加准确的启发式方法是未来的一个研究方向.

（3）可持续的资金追踪方法. 当前阶段的资金追踪方法可以在一定程度上克服匿名性保护技术对交易信息的隐藏，对交易金额在特定交易地址之间的资金流动进行追踪. 但是，当一个谨慎的网络犯罪者利用多种匿名性技术连续发起多次资金转移行为时，目前的分析方法不能有效的对犯罪资金进行持续的追踪. 同时，随着匿名性技术和密码保护协议的不断完善，已有的技术对资金追踪的有效性将不断降低. 例如，Mixcoin[53]协议允许将用户的混币金额以特定的概率全部作为手续费，这将导致根据交易金额匹配的方式寻找混币交易双方关联性的方式失效. 因此，如何在匿名性技术限制下有效的追踪交易资金，如何持续的追踪交易都将成为未来的研究热点.

6.2　交易的匿名性保护

零知识证明、环签名等匿名性技术的采用在一定程度上保护了交易的匿名性. 但随着数字货币规模的不断扩大，匿名性保护技术在随着数字货币普及的过程中，会产生一些实际的问题.

首先，匿名性保护技术的使用降低了数字货币的交易效率. 零知识证明、机密交易等匿名性技术的使用会增加完成交易所花费的时间，这将导致用户在使用匿名性货币进行支付时，需要等待很长的时间，这无疑会限制匿名性数字货币的推广. 例如，早期的 Zcash 客户端采用了 Sprout 零知识证明协议，该协议规定用户在交易创建阶段需要花费 40s 的时间来等待零知识证明的生成[47]. 之后矿工在记录交易时，同样需要花费额外的时间对证明进行验证，这无疑大幅度增加了完成交易所需的时间.

其次，匿名性保护技术的使用会限制数字货币交易系统的可扩展性. Zcash、Monero 等数字货币网络中的矿工节点在记录网络中的新发交易时，需要额外的计算量来证明交易的合法性. 因此，匿名性数字货币在进行扩展时，新节点的加入不仅需要具备存储性能，还需要具备极高的处理性能. 这无疑会限制匿名性数字货币的可扩展性.

最后，匿名性保护技术的使用增加了用户理解并且信任数字货币交易系统的负担. 过度的匿名性保护会导致用户对系统安全性的信任危机①. 例如，就比特币系统中的货币总量而言，由于比特币的交易金额是公开可查的，用户可以通过观察公开账本的方式来计算比特币系统中总的交易金额为 2100 万[1]. 但是，当采用零知识证明、机密交易等匿名性保护技术来隐藏交易金额时，用户便无法判断系统的总发币量. 如果数字货币系统被恶意破坏，攻击者可以任意的增发新货币而不被发现，这会给用户的财产带来损失.

基于匿名性保护研究所面临的挑战，本文认为以下三个方面将成为未来的研究趋势：

（1）高效的匿名性保护方案. 目前已有许多针对匿名性技术的研究工作，旨在提高对用户匿名性的保护能力，而匿名性保护技术的计算效率将会是未来研究工作中重要的一环，尤其是零知识证明、机密交易等技术已经广泛应用于数字货币中的密码学技术. 虽然目前已经有一部分工作对匿名性技术的计算效率进行了改进，例如机密交易中新的承诺方案[54]，但仍有进一步研究的空间.

（2）可扩展的匿名性保护方案. 随着匿名性数字货币的逐步推广，用户和交易的数量会越来越多. 例如，2021 年 10 月，Zcash 的日均交易量为 243 万 ZEC，与 2020 年 10 月相比，同比增长了约 74%. 尽管已经有一些针对匿名性技术的可扩展性研究，例如 zk-SNARKs[55]、Monero[56]. 但是考虑到匿名性数字货币的用户数量和交易数量不断攀升，这些研究是不够的. 因此，对于匿名性数字货币可扩展性的研究会成为未来的一个研究热点.

（3）可监管的匿名性保护方案. 采用额外的匿名性保护技术无疑可以提高数字货币交易的匿名性和安全性. 但与此同时，数字货币作为跨境支付、资金转移等金融领域的重要媒介之一，不法分子对数字货币的滥用将对金融秩序造成重大影响，因而支持监管是数字货币所应具备的基础条件. 综合考虑上述两个方面，新型的数字货币匿名性保护方案应同时具备可监管的属性. 目前已有一种名为 Traceable

① Reddit: Question: How to Trust Monero? Accessed: Oct. 23, 2017. [Online]. Available: https://www.reddit.com/r/Monero/comments/6zyndw/question_how_to_trust_monero/

Monero 的新型数字货币系统[57]，该方案允许用户匿名交易的同时支持对异常交易的跟踪，但该方案与 Monero 交易网络并不兼容，实际上并没有改善 Monero 的可监管性. 如何平衡交易匿名性的需求和监管需求，是未来数字货币交易匿名性研究的一个方向.

7 总 结

本文主要从对抗的角度对数字货币交易匿名性的研究进行了系统的梳理和总结，帮助读者全面地认识当前阶段交易匿名性的研究进展. 首先对交易匿名性的内涵进行了深入剖析，将其归纳为不可标识性、不可链接性和不可追踪性三个方面. 以此为指导，对区块链数字货币的匿名性保护技术和匿名性对抗技术进行了介绍和对比分析. 最后，本文总结了区块链数字货币匿名性研究所面临的挑战和未来的发展趋势，相信随着数字货币规模的不断扩大，交易匿名性的研究势必会对金融秩序的有序发展产生深远的影响.

致 谢 在此，我们向对本文研究工作给予支持和建议的同行表示衷心的感谢!

参 考 文 献

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

[2] Foley S, Karlsen J R, Putniņš T J. Sex, Drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 2019, 32(5): 1798–1853

[3] Malte M, Rainer B. Anonymous Alone? Measuring Bitcoin's second-generation anonymization techniques// Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops. Paris, France, 2017: 32-41

[4] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system// Proceedings of the 3rd International Conference on Privacy, Security, Risk and Trust. Boston, USA, 2011: 1318-1326

[5] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys and Tutorials, 2016, 18(3): 2084-2123

[6] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186 (in Chinese)
(祝烈煌, 高峰, 沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展, 2017, 54(10): 2170-2186)

[7] Chen Wei-Li, Zheng Zi-Bin. Blockchain data analysis: a review of status, trends and challenges. Journal of Computer Research and Development, 2018, 55(9): 1853-1870(in Chinese)
(陈伟利, 郑子彬. 区块链数据分析：现状、趋势与挑战. 计算机研究与发展. 2018, 55(9): 1853-1870)

[8] Fu Shuo, Xu Hai-Xia, Li Pei-Li, Ma Tian-Jun. A survey on anonymity of digital currency. Chinese Journal of Computers, 2019, 42(5): 1045-1062(in Chinese)
(付烁, 徐海霞, 李佩丽, 马添军. 数字货币的匿名性研究. 计算机学报, 2019, 42(5): 1045-1062)

[9] Li Xu-Dong, Niu Yu-Kun, Wei Ling-Bo, Zhang Chi, Yu Neng-Hai. Overview on privacy protection in Bitcoin. Journal of Crytologic Research, 2019, 6(2): 133-149(in Chinese)
(李旭东, 牛玉坤, 魏凌波, 张驰, 俞能海. 比特币隐私保护综述. 密码学报, 2019, 6(2): 133-149)

[10] Zhang Ao, Bai Xiao-Ying. Survey of research and practices on blockchain privacy protection. Journal of Software, 2020, 31(5): 1406-1434(in Chinese)
(张奥, 白晓颖. 区块链隐私保护研究与实践综述. 软件学报, 2020, 31(5): 1406-1434)

[11] Liu X, Jiang X, et al. Knowledge discovery in cryptocurrency transactions: A Survey. IEEE Access. 2021, vol 9: 37229-37254

[12] Burton H, Bloom. Space/time trade-offs in hash coding with allowable errors. Communications of the ACM, 1970, 13(7): 422-426

[13] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, USA, 2014: 15-29

[14] Fanti G, Viswanath P. Anonymity properties of the Bitcoin P2P network. arXiv preprint arXiv:1703.08761, 2017

[15] Gao Feng, Mao Hong-Liang, Wu Zhen, Shen Meng, Zhu Lie-Huang, Li Yan-Dong. Lightweight transaction tracing technology for Bitcoin. Chinese Journal of Computers. 2018, 41(05): 989-1004(in Chinese)
(高峰, 毛洪亮, 吴震, 沈蒙, 祝烈煌, 李艳东. 轻量级比特币交易溯源机制. 计算机学报, 2018, 41(05): 989-1004)

[16] Kappos G, Yousaf H, Maller M, et al. An empirical analysis of anonymity in zcash//Proceedings of the 27th USENIX Security Symposium. Baltimore, USA, 2018: 463-477

[17] Möser M, Soska K, Heilman E, et al. An empirical analysis of traceability in the monero blockchain// Proceedings of Privacy Enhancing Technologies. Barcelona, Spain, 2018: 143-163

[18] Seunghyeon L, Changhoon Y, Heedo K, et al. Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web//Proceedings of 26th Annual Network and Distributed System Security Symposium. San Diego, USA, 2019: 1-15

[19] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany:Springer, 2008: 415-432

[20] Bitansky N, Chiesa A, Ishai Y, et al. Succinct non-interactive arguments via linear interactive proofs//Proceedings of the Theory of Cryptography Conference. Berlin, Germany: Springer, 2013: 315-333

[21] Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications//Proceedings of the 20th Annual ACM Symposition On Theory of Computing. 1988. 103−112

[22] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous distributed E-cash from Bitcoin//Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 397–411

[23] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive 2018: 46

[24] Bunz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more//Proceedings of the 2018 IEEE Symposium on Security and Privacy. San Francisco, USA, 2018: 315-334

[25] Bowe S, Grigg J, Hopwood D. Halo: Recursive proof composition without a trusted setup. IACR Cryptology ePrint Archive 2019: 1021

[26] Fujisaki E, Suzuki K. Traceable ring signature//Proceedings of the International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2007: 181-200

[27] Chervinski J O, Kreutz D, Yu J. Analysis of transaction flooding attacks against Monero//Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency. Sydney, Australia, 2021: 1-8

[28] Valenta L, Rowan B. Blindcoin: Blinded, Accountable mixes for bitcoin//Proceedings of the 19th Financial Cryptography. San Juan, USA, 2015:112-126

[29] Tran M, Luu L, Kang MS et al. Obscuro: A Bitcoin mixer using trusted execution environments//Proceedings of the 34th Annual Computer Security Applications Conference. San Juan, USA, 2018: 192-701

[30] 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

[31] Ruffing T, Moreno-Sanchez P, Kate A. P2P Mixing and unlinkable bitcoin transactions//Proceedings of the 24th Annual Network and Distributed System Security Symposium. San Diego, USA, 2017: 43-58

[32] Lee K, Miller A. Authenticated data structures for privacy-preserving monero light clients//Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops. London, UK, 2018: 20-28

[33] Hu Y, Wang S, Tu G H, et al. Security threats from bitcoin wallet smartphone applications: vulnerabilities, attacks, and countermeasures//Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy. Baltimore, USA, 2021: 89-100

[34] Biryukov A, Pustogarov I. Bitcoin over Tor isn't a good idea // Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 122-134

[35] Neudecker T, Hartenstein H. Could network information facilitate address clustering in Bitcoin?//Proceedings of the 21st International Conference on Financial Cryptography and Data Security. Sliema, Malta, 2017: 155-169

[36] Shen M, Duan J, Shang N, et al. Transaction Deanonymization in Large-Scale Bitcoin Systems via Propagation Pattern Analysis//Proceedings of the International Conference on Security and Privacy in Digital Economy. Singapore, 2020: 661-675

[37] Feld S, Schönfeld M, Werner M. Analyzing the deployment of Bitcoin's P2P Network under an AS-level perspective. Procedia Computer Science, 2014, 32: 1121-1126

[38] Apostolaki M, Maire C, Vanbever L. PERIMETER: A network-layer attack on the anonymity of cryptocurrencies// Proceedings of the 25th International Conference on Financial Cryptography and Data Security. Online. 2021

[39] Tramèr F, Boneh D, Paterson K. Remote side-channel attacks on anonymous transactions//Proceedings of the 29th USENIX Security Symposium. Boston, USA, 2020: 2739-2756

[40] Koshy P, Koshy D, McDaniel P. An analysis of anonymity in bitcoin using p2p network traffic//Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2014: 469-485

[41] Yousaf H, Kappos G, Meiklejohn S. Tracing transactions across cryptocurrency ledgers//Proceedings of the 28th USENIX Security Symposium. Santa Clara, USA, 2019: 837-850

[42] YU Ge, NIE Tie-Zheng, LI Xiao-Hua, ZHANG Yan-Feng, SHEN De-Rong, BAO Yu-Bin. The challenge and prospect of distributed data management techniques in blockchain systems. Chinese Journal of Computers. 2019, 44(01): 28-54(in Chinese)
（于戈, 聂铁铮, 李晓华, 张岩峰, 申德荣, 鲍玉斌. 区块链系统中的分布式数据管理技术-挑战与展望. 计算机学报, 2019, 44(01): 28-54）

[43] Androulaki E, Karame G O, Roeschlin M, et al. Evaluating user privacy in bitcoin//Proceedings of the 17th International Conference on Financial Cryptography and Data Security. Berlin, Germany：Springer, 2013: 34-51

[44] Zhang Z, Li W, Liu H, et al. A refined analysis of zcash anonymity. IEEE Access, 2020, 8: 31845-31853

[45] Quesnelle J. On the linkability of Zcash transactions. arXiv preprint arXiv:1712.01210, 2017

[46] Biryukov A, Feher D, Vitto G. Privacy aspects and subliminal channels in Zcash//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019: 1813-1830

[47] Biryukov A, Feher D. Privacy and linkability of mining in zcash// Proceedings of the 2019 IEEE Conference on Communications and Network Security. Washington, USA, 2019: 118-123

[48] Chen L, Xu L, Shah N, et al. Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017: 23-28

[49] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins: characterizing payments among men with no names//Proceedings of the 2013 Conference on Internet Measurement Conference. 2013: 127-140

[50] Möser M, Böhme R, and Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem. In Proceedings of the 2013 APWG eCrime Researchers Summit. San Francisco, USA, 2013: 1-14

[51] Wu L, Hu Y, Zhou Y et al. Towards understanding and demystifying Bitcoin mixing services.//Proceedings of the Web Conference 2021. New York, USA, 2021: 33-44

[52] Shen M, Zhang J, Zhu L, Xu K, Du X. Accurate decentralized application identification via encrypted traffic analysis using graph neural networks. IEEE Transactions on Information Forensics and Security. 2021, 16: 2367-2380

[53] Joseph B, Arvind N, Andrew M, et al. Mixcoin: Anonymity for Bitcoin with accountable mixes//Proceedings of the 18th Financial Cryptography. Christ Church, The Netherland, 2014: 486-504

[54] Ruffing T, Malavolta G. Switch commitments: A safety switch for confidential transactions//Proceedings of the 21st Financial Cryptography. Sliema, Malta, 2017: 170-181
[55] Eli. B, Alessandro C, Eran T, Madars V. Scalable zero knowledge via cycles of elliptic curves. Algorithmica. 2017,79(4): 1102-1160
[56] Kyung A S. An efficient ring signature scheme from pairings. Information Sciences. 2015,300: 63-69
[57] Li Y, Yang G, Susilo W, et al. Traceable monero: Anonymous cryptocurrency with enhanced accountability. IEEE Transactions on Dependable and Secure Computing. 2021, 18(2): 679-691

SHEN Meng, Ph. D., professor. His research interests include network security and data privacy protection.

CHE Zheng, Ph. D. candidate. His research interests include blockchain application and network security.

ZHU Lie-Huang, Ph. D., professor. His research interests include cryptography, network and information security.

XU Ke, Ph. D., professor. His research interests include the next generation of internet architecture, cyberspace security and blockchain system.

GAO Feng, Ph. D. His research interests include Blockchain Security.

YU Cong-Cong, M. S. candidate. His research interests include blockchain application and network security.

WU Yan, Ph. D. candidate. Her research interests include network security, blockchain technology and public key cryptography.

Background

At present, the research on the anonymity of cryptocurrency transactions mainly focuses on protecting transaction anonymity and the confrontation of anonymity. In terms of transaction anonymity protection, researchers mostly use zero-knowledge proof, Tor network, and other anonymity technologies to ensure the anonymity of users in the entire transaction process from different perspectives. For example, Monero protects the transaction input by using ring signature that hides the real transaction input; Dash muddies the relationship between transaction inputs and outputs by employing mixcoin that severs the correlation between transaction inputs and outputs. Regarding the confrontation of anonymity, the researchers mainly combined the transaction information disclosed in the blockchain ledger and the dissemination data in the network layer to analyze the transaction traces left by users in the transaction process from different perspectives. For example, the correlation between bitcoin transactions can be obtained by analyzing the topological characteristics of the bitcoin transaction network.

In this paper, we first give an in-depth analysis of transaction anonymity's connotation and summarize it into three aspects: unidentifiability, unlinkability, and untraceability. Then, we introduce anonymity protection techniques and anonymity countermeasure techniques for cryptocurrency and carry out a comparative analysis. Finally, the paper summarizes the cryptocurrency anonymity research institute's challenges and future development trends.

This work is supported by the National Key R&D Program of China with No. 2020YFB1006101, the NSFC Projects with Nos. 61825204,61932016,61972039, 62132011 and 62222201, the Beijing Natural Science Foundation with No. 4192050, the Beijing Outstanding Young Scientist Program with No. BJJWZYJH01201910003011 and the Beijing Nova Program with No. Z201100006820006.