密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2019, 6(2): 133–149

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

比特币隐私保护综述*

李旭东[1,2], 牛玉坤[1], 魏凌波[1,2], 张 驰[1], 俞能海[1]

1. 中国科学技术大学 中科院电磁空间信息重点实验室, 合肥 230027
2. 中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093

通信作者: 李旭东, E-mail: xudongli@mail.ustc.edu.cn

摘 要: 比特币是利用区块链技术为支撑, 以去中心化方式实现的密码货币. 其通过使用公钥地址作为假名隐藏用户真实身份达到匿名, 然而全网公开的区块链账本对用户隐私构成了极大威胁, 也引起了学术界的广泛关注. 首先, 从隐私保护角度出发, 研究现有的比特币协议存在的缺陷及可能受到的攻击. 然后从不需要修改现有比特币协议的混币技术、离链支付协议, 和修改现有比特币协议的密码学方案, 如隐蔽地址技术、环签名、零知识证明、同态加密, 两个方向探讨对比特币隐私保护做出的改进. 最后展望比特币及区块链隐私保护研究工作.

关键词: 比特币; 区块链; 匿名; 隐私保护; 零知识证明

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000290

中文引用格式: 李旭东, 牛玉坤, 魏凌波, 张驰, 俞能海. 比特币隐私保护综述[J]. 密码学报, 2019, 6(2): 133–149.
英文引用格式: LI X D, NIU Y K, WEI L B, ZHANG C, YU N H. Overview on privacy protection in Bitcoin[J]. Journal of Cryptologic Research, 2019, 6(2): 133–149.

Overview on Privacy Protection in Bitcoin

LI Xu-Dong[1,2], NIU Yu-Kun[1], WEI Ling-Bo[1,2], ZHANG Chi[1], YU Neng-Hai[1]

1. CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230027, China
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Corresponding author: LI Xu-Dong, E-mail: xudongli@mail.ustc.edu.cn

Abstract: Bitcoin is a cryptographic currency supported by the Blockchain technic and implemented in a decentralized manner, and it uses public key address as a pseudonym to hide the real identity of users to achieve anonymity. However, the public Blockchain ledger in the network is available to everyone, thus, it poses a great threat to users' privacy, and has also attracted wide attention from the academic community. In this report, firstly, from the perspective of privacy protection, the limitation and possible attacks of existing Bitcoin protocols are studied. Then, this paper focuses on the improvements of privacy protection in Bitcoin protocol from two aspects: one is not to modify the existing Bitcoin protocol such as coin-mixing technology, off-chain payment protocol, etc., and

* 基金项目: 国家重点研发计划 (2017YFB0802200); 国家自然科学基金 (61702474)
Foundation: National Key Research and Development Program of China (2017YFB0802200); National Natural Science Foundation of China (61702474)
收稿日期: 2018-02-27 定稿日期: 2018-05-24

the other is to make some modifications with cryptography techniques such as stealth address, ring signature, zero-knowledge proofs, homomorphic encryption. Finally, challenges and perspectives of privacy protection of Bitcoin and Blockchain are discussed.

Key words: Bitcoin; Blockchain; anonymity; privacy protection; zero-knowledge proofs

1 引言

比特币的概念最初由中本聪在发表的题为《比特币: 一种点对点的电子现金系统》中提出 [1]. 比特币是借助哈希函数、非对称加密、数字签名、Merkle 树、PoW 共识机制等密码学技术在 P2P 网络上开源实现的具有货币发行、交易和账户管理功能的密码货币. 其隐私概念包括交易匿名和地址不可关联, 交易匿名要求不能将特定的交易与用户真实身份联系起来, 地址不可关联要求同一用户的两个交易不能被关联起来.

比特币通过全网节点共同校验数据区块生成、维护区块链, 具有一致性、不可篡改性、可追溯性. (1) 比特币需要发送方使用私钥签名交易, 经节点广播, 全网达成共识之后被记录到区块链上, 保证信息一致性. (2) 区块链依靠区块间的哈希指针和区块内的 Merkle 树实现链上数据的不可篡改; 基于难度系数的比特币 PoW 共识机制保证单一节点数据难以通过分叉攻击篡改历史交易数据. (3) 区块链上存储着自 coinbase 交易以来的所有交易数据, 基于这些不可篡改的日志类型数据, 可追溯特定地址的历史交易记录.

然而, 一旦比特币用户的身份信息遭到泄露, 这些数据永远保存于整个区块链账本上, 任何人也都可以公开获取. 因此区块链系统应该更加重视隐私问题, 提高隐私保护能力.

为了保护用户隐私, 比特币用户使用假名 (即比特币公钥地址) 参与交易. 公钥地址是标识和区分一个用户的唯一方法. 为了保障交易安全性, 需对每笔交易都进行签名与验证, 签名算法使用了椭圆曲线数字签名算法 (ECDSA). 每个用户可以拥有任意数量的比特币地址, 这些地址由其客户端存储并透明管理. 尽管依赖于假名, 比特币的隐私保护问题依然突出. (1) 公开的区块链账本数据使得攻击者可以提取有关用户身份特征的信息 (公开的交易金额和输入输出地址信息以及它们之间的关联特征使得攻击者可以追踪整个历史交易路径). (2) 比特币通讯协议未加密, 节点传播交易信息时可能会泄露源 IP 地址与比特币地址的对应关系. (3) 轻量级客户端向全节点请求过程可能会泄露节点隐私信息, 同时存在第三方钱包平台窃取、泄露地址交易记录等信息.

目前比特币去匿名的研究主要集中在两种方法上: 一是对区块链的分析, 它从公开的区块链账本获得交易信息, 基于交易内在地址链接关系对其进行聚类分析, 并结合线下信息将比特币地址与个人身份关联起来; 另一种方法是对比特币协议和网络的分析, 它利用了比特币交易传播机制和网络拓扑结构推断交易的源 IP 地址. 针对已有的去匿名攻击方法, 研究人员也提出了一些隐私保护方案, 其中混币技术、离链支付协议可以在一定程度上提高匿名性, 而混币技术根据是否需要可信第三方又可以进一步分为中心化混币和去中心化混币方案, 这些都不需要对现有比特币协议作出任何修改, 然而也都存在缺陷. 隐蔽地址、环签名、零知识证明、同态加密等密码学方案改进比特币协议来达到更好的区块链隐私保护效果.

本文的其余部分组织如下: 第 2 节从区块链、网络层、钱包和轻量级客户端角度介绍现有的比特币隐私保护存在的威胁及对应的保护机制; 第 3 节研究不需要修改现有比特币协议的隐私保护机制, 如混币技术、离链支付协议; 第 4 节研究如何通过零知识证明、同态加密等密码学方案改进比特币协议达到更好的区块链隐私保护效果; 最后, 第 5 节展望比特币及区块链隐私保护研究工作.

2 比特币隐私攻击方法

2.1 区块链分析

Pfitzmann 等首先给出了匿名的定义, 某一主体的匿名意味着该主体的身份在一组匿名集合主体内是不可识别的 [2]. 比特币匿名目的是为了防止攻击者通过 P2P 网络和记录了全部交易信息的区块链发现比特币假名地址与真实用户身份信息之间的链接关系. 比特币匿名性需要满足以下两个要求:

(1) **交易匿名性** 对于任何交易, 无法确认其发送方或接收方所对应的真实身份.

(2) **地址不可关联性** 给定任意两个地址, 无法判断其是否由同一个用户拥有.

然而, 比特币作为公有链, 交易信息全网公开, 比特币账本上记录了从创世区块开始的所有交易信息 (比特币交易将比特币从输入地址转移到输出地址, 交易金额和输入输出地址的链接关系都是公开可见的), 任何人都可以作为比特币 P2P 网络中的全节点获得完整的账本. 这给比特币去匿名技术带来了一个思路, 追溯比特币交易发起人真实身份从理论上来说是可行的.

Reid 等分析比特币交易的特征后提出了交易图、初始用户图、用户图的网络结构概念, 并研究它们对用户匿名带来的影响 [3]. 这里简要介绍如何通过区块链分析形成交易图、初始用户图、用户图:

(1) **交易图** 整个区块链可以看作是无环交易图, 其中每个顶点表示一个交易, 起始点和终点之间的有向边表示上一笔交易的输出对应于下一笔交易的输入. 每个有向边还包括一个比特币值和一个时间戳. 交易图表示区块链交易之间的比特币流动.

如图 1 (a) 所示, 图中 t_1, t_2, t_3, t_4 都代表交易, 其中, t_1 与 t_3 之间的有向边表示 t_1 的一个输出作为 t_3 的一个输入被花费.

交易图是区块链分析中最大的图表, 存储开销很大, 因此在分析之前使用主集方法 [4] 或按权重过滤交易 [5] 是可行的方法.

(2) **初始用户图** 初始用户图中, 每个顶点代表一个公钥地址, 顶点之间的每个有向边代表从一个公钥地址到另一个公钥地址的比特币流动. 初始化视每个公钥地址为一个用户, 并且用户图是可以是循环的.

如图 1 (b) 所示, 每个菱形顶点代表一个公钥地址, 菱形顶点之间的每个有向边代表从一个公钥地址到另一个公钥地址的比特币流动. 交易 t_1 和 t_2 的输出被 t_3 兑换, 最终被发送给公钥 pk_1 的用户和公钥 pk_2 的用户.

(3) **用户图** 用户图通过利用多输入交易的特点 (同一个多输入交易签名通常由同一用户签署, 因此可以很大程度上将交易输入的多个公钥地址聚合到同一用户) 对初始用户图进一步处理, 聚合可能属于同一用户的公钥地址来创建用户图. 用户图中, 每个顶点代表一个用户, 顶点之间的每个有向边表示从一个用户到另一个用户的比特币的流动.

如图 1 (c) 所示, 每个圆形顶点代表一个用户, 并且圆形顶点之间的每个有向边表示从一个用户到另一个用户的比特币的流动. 公钥 pk_1 和 pk_2 由于它们对应于单个交易的一对输入而被收缩成单个顶点用户 u_1.

2013 年, Meiklejohn 等在 Reid 等研究工作 [3] 之上提出了两类启发式聚类分析方法 [6], 基于两个思想: (1) 同一个交易的输入地址由同一用户集群控制, 因为比特币交易通过签名验证交易的合法性, 只有私钥的所有者才拥有合法的公钥地址签名; (2) 一次性找零地址由输入地址的同一用户集群控制.

除了交易图对比特币区块链的分析, Androulaki 等通过攻击实验 AddUnl 来定量分析地址不可链接性 [7]. AddUnl 由攻击者 A 和知道比特币实体的地址分配情况的挑战者 C 组成, 实验按照如下步骤进行:

(1) 攻击者 A 从出现在比特币账本 pubLog 中的地址中选择一个地址 a_0, 并将其发送给挑战者 C.

(2) 挑战者 C 随机选择一个比特 b. 如果 $b = 1$, 则 C 从 pubLog 中随机选择属于同一个用户的另一个地址 a_1; 否则, C 随机选择一个不属于该用户的地址 a_1. 挑战者 C 发送 $< a_0, a_1 >$ 给 A.

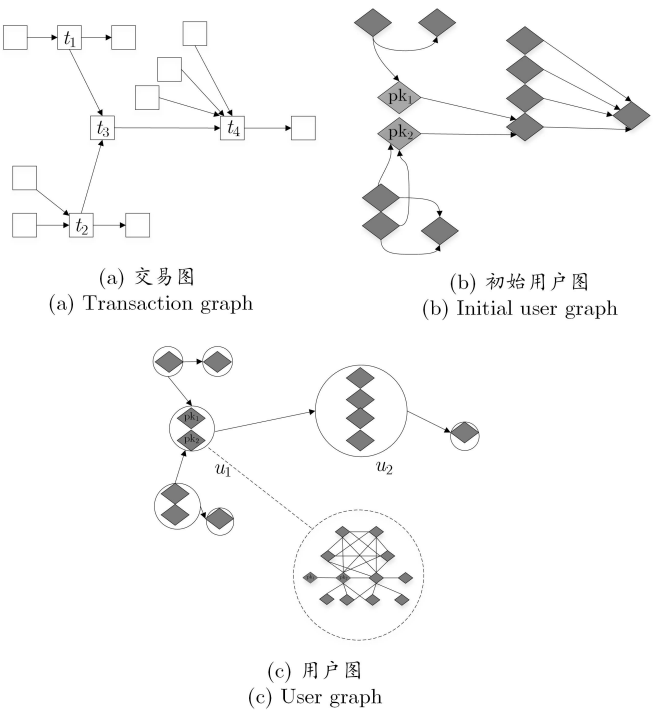
(3) A 对两个地址 $< a_0, a_1 >$ 是否属于同一用户作出响应 b'. 若回答正确 (即 $b = b'$), 则 A 获胜.

若比特币交易满足地址不可链接性, 则对于所有具有概率多项式时间攻击能力的攻击者 A 相对于 A^R (随机猜测结果的攻击者) 获胜的概率可忽略:

$$\Pr[b' \leftarrow A(\mathrm{pbuLog}, K_A) : b = b'] - \Pr[b' \leftarrow A^R(K_A) : b = b'] \tag{1}$$

然后通过 $n_A \times n_A$ 矩阵 E_{link} 来表示 A 的估计, 其中矩阵元素 $E_{\mathrm{link}}[i,j] = \{p_{i,j}\}$ 表示每个地址同一个用户拥有地址 a_i 和 a_j 的概率. 然后引入真实关联矩阵 $\mathrm{GT}_{\mathrm{link}}$, 如果 a_i 和 a_j 属于同一个用户, $\mathrm{GT}_{\mathrm{link}}[i,j] = 1$, 否则 $\mathrm{GT}_{\mathrm{link}}[i,j] = 0$. 通过计算 E_{link} 与真实关联矩阵 $\mathrm{GT}_{\mathrm{link}}$ 的统计距离 $\|E_{\mathrm{link}}[i,*] - \mathrm{GT}_{\mathrm{link}}[i,*]\|$ 来量化比特币提供的不可链接性 $\mathrm{Unlink}_A = 1 - \frac{\mathrm{Succ}_A - \mathrm{Succ}_{A_R}}{\mathrm{Succ}_{A_R}}$, 其中 Succ_A 和 Succ_{A_R} 分别表示攻击者 A 和 A_R 通过最大误差 $\max\limits_{\forall a_i \notin K_A}(\|E_{\mathrm{link}}[i,*] - \mathrm{GT}_{\mathrm{link}}[i,*]\|)$ 表示的在攻击实验中的成功率.

结合来自比特币系统外的信息会进一步提升攻击效果. Reid 等 [3] 还将比特币系统外部信息与流量和



(a) 交易图
(a) Transaction graph

(b) 初始用户图
(b) Initial user graph

(c) 用户图
(c) User graph

图 1 交易图、初始用户和用户图
Figure 1 Transaction graph, initial user graph, and user graph

时间分析等技术结合起来, 以说明各种类型的信息泄漏如何导致系统用户的去匿名. 2013 年, Androulaki 等 [7] 在大学进行模拟实验, 学生使用比特币作为日常交易货币. 研究人员通过基于行为的聚类技术分析比特币交易数据, 实验数据显示, 即使通过不重复使用比特币地址作为隐私保护手段, 依然可以将 40% 的用户真实身份和比特币地址联系起来. 美国普林斯顿大学最新研究 [8] 表明, 如果用户使用比特币与接受数字货币的在线商家进行交易, 商家可以将比特币的支付流通信息轻松地与用户 cookies 相关联, 从而基本消除了比特币交易匿名性质, 找到用户的真实身份.

随着比特币技术的不断发展尤其是各类混合技术的出现, 同一个混合交易的输入地址可以属于多个用户, 也打破了输入输出地址之间的链接关系, 启发式聚类分析已不再完全适用. 但是结合其他比特币去匿名技术, 该方法仍然可以很大程度聚类用户身份地址信息.

2.2 网络层隐私保护

在本节中, 我们从比特币 P2P 网络隐私现状开始分析, 然后阐述研究人员对比特币 P2P 网络机制作出的改进.

比特币采用 P2P 网络架构广播交易和区块. P2P 网络具有可靠性、去中心化和开放性, 是比特币系统稳定运行的保障. 但是 P2P 网络的开放性和弱匿名性等特点使得比特币网络容易受到 Sybil 攻击 [9], 其引入的大量恶意节点会传输非法交易信息以及威胁路由、资源分配等网络通信安全.

除此之外, 现有的比特币网络对用户隐私泄露存在诸多隐患: (1) 比特币节点通过不经加密和身份验证的 TCP 连接与其他网络节点进行通信, 攻击者可以直接监听网络中传播的交易信息内容. (2) 搜集节点之间的拓扑关系, 基于节点拓扑关系攻击者可以进一步分析交易的传播路径, 从而找到其源 IP 地址节点. (3) 比特币网络中节点的 IP 地址信息可以被用来链接到用户真实身份信息.

因此通过将比特币地址映射到源节点 IP 地址成为比特币去匿名的又一思路, 这种技术不依赖于交易之间的联系. 2011 年, Reid 首先指出从 P2P 网络获得的 IP 地址信息可以用来减少比特币系统的匿名性 [3].

受 Kaminsky 等 [10] 的启发, 2014 年, Koshy 等分析了将比特币地址直接映射到 IP 数据的可能风险 [11]. 他们使用 CoinSeer 收集了超过 500 万笔交易的数据的 IP 地址信息. 实验数据未经过地址聚类以便执行纯网络分析, 试图去寻找比特币地址与源 IP 地址的链接关系. 然而由于 P2P 网络节点之间复杂拓扑关系和规模, 攻击效果并不明显.

Lischke 和 Fabian [12] 利用网络 IP 分析来研究对比特币隐私的影响后得出结论, 使用代理或匿名服务 (如 Tor [13]) 时, IP 地址可能保持不可追踪.

然而, Biryukov 等 [14] 的研究显示, 即使使用了 Tor 用户也有可能被去匿名化. 2015 年, Biryukov 等 [15] 的研究展示了一个中间人攻击手段, 声称 Tor 和比特币结合在一起将会比不使用 Tor 面临更大的去匿名风险. 一个拥有少量资源的攻击者可以完全控制使用 Tor 的比特币用户之间的信息流动. 尽管使用了假名, 攻击者依然可以将用户的交易链接在一起, 控制哪些比特币交易和区块被中继到用户, 并且可以延迟广播或直接丢弃用户交易和区块, 在用户连接到比特币网络时得到他们的 IP 地址信息.

Karame 介绍了一种通过将假名 (地址) 与底层客户端的 IP 地址相关联来去匿名化比特币用户的方法 [16]. 这种攻击在文献 [11] 中首次引入, 后来在文献 [14] 中进行了扩展. 攻击分 3 步实行.

(1) 攻击者通过 DoS 攻击 [17] 断开用户与 Tor 或其他匿名网络的连接, 客户端可能利用这些工具来改变连接的比特币节点. 这允许攻击者直接使用网络接收的信息 (例如, 找出网络的拓扑结构).

(2) 推断网络拓扑结构, 在这个阶段, 攻击者将不接受传入连接的比特币客户端作为目标, 并且仅向网络的其余部分展示最少的 (如 8 个) 传出连接. 攻击者的目标是学习从每个目标比特币客户端的八个入口节点获得的信息.

(3) 攻击者使用所获得的网络知识, 结合比特币网络交易的传播机制, 对交易进行去匿名化处理. 作为该攻击的一个实例, Koshy 等在文献 [11] 中找到了比特币网络中 11% 的交易的 IP 地址.

2017 年, Bojja 等 [18] 通过研究比特币网络节点的广播机制对 P2P 网络进行了重构, 以提供稳定的、可查证的匿名性为首要原则. Bojja 等提出了一个简单的网络政策 Dandelion 保证在对网络功能消耗最低的前提下, 实现最佳的匿名性.

2.3 钱包隐私

比特币钱包是一个存储并管理比特币私钥的容器. 与传统钱包不同, 比特币钱包不存储比特币, 而是存储比特币对应的公私钥对, 用户使用私钥去签名交易, 并用公钥生成地址接收发送方的比特币 [19]. 在比特币的使用过程中, 比特币的控制权是通过私钥、比特币地址和数字签名来确立的, 比特币地址可以由公钥生成, 公钥则由私钥衍生, 数字签名只能通过私钥生成. 因此掌握了比特币私钥, 就获得了对该比特币的使用权. 正是因为私钥在比特币系统中有如此高的重要性, 需要用一个专门的软硬件去保护私钥的安全和有序使用, 这也正是比特币钱包在比特币系统中扮演的角色.

中心化比特币钱包不依赖比特币网络, 只依赖自己的中心化服务器, 不同步数据, 所有的数据均从自己的中心化服务器中获得. 其在隐私与安全方面也存在诸多隐患, 用户无法保证服务提供商不保存任何转账记录或者泄露客户真实身份信息. 每一个用户的转账记录和比特币持有记录都存储在第三方数据库中; 即使钱包不要求实名制, 也可以把账户的虚拟 ID 作为识别用户身份的方式: 列在该 ID 下的所有数字货币出入账地址、转账交易记录、持有比特币数量, 都有泄漏风险. 在这种情况下, 虽然钱包平台不知道用户真实身份, ID 某种程度上也就对应了真实身份.

由于区块链的数据量太大 (当前在 200 GB 以上), 全节点钱包严重限制了普通用户的使用场景, 因此, 当前许多比特币钱包客户端开始采用 SPV (simplified payment verification) 模式. SPV 钱包只维护与本地地址相关的区块链数据, 通过请求比特币全节点完成对交易合法性的验证.

目前比较安全的比特币存储方式包括全节点钱包、硬件钱包、分层确定性钱包、多签名钱包等. 全节点 (如 Bitcoin-core 核心钱包) 维护着全部的区块链数据, 完全去中心化, 同步比特币网络所有交易数据; 硬件钱包 (如 Ledger Nano S、Keepkey、Trezor) 是指离线存储私钥, 包含一个脱机部分可以决定是否对交易进行签名; 分层确定性 (hierarchical deterministic) 钱包的原理是利用随机数产生一个主私钥, 之后再由主私钥产生一系列子私钥, 且该过程不可逆, 可以很好地实现权限控制管理; 多签名钱包如 Copay 需要 "m-of-n" 签名实现多私钥和用户控制管理.

2016 年, 开源比特币隐私工程 (Open Bitcoin Privacy Project, 简称 OBPP) 发布了比特币钱包性能报告第二版, 对 20 款比特币钱包进行了测评, 根据这些钱包所提供的安全水平进行了评级. OBPP 评选出了 5 款安全性或者隐私性最好的比特币钱包, Ledger、Breadwallet、Airbitz、Darkwallet、ArcBit. 报告发现, 越来越多的比特币钱包都采用分层确定性架构, 这是专注于保护隐私的比特币钱包的一个重要特征, 它可以帮助客户避免地址重用.

2.4 轻量级客户端隐私

并非所有的节点都有能力储存完整的区块链账本, 许多比特币客户端被设计成运行在空间和功率受限的设备上, 如智能电话、平板电脑、嵌入式系统等, 在这些设备上使用的轻量级密码算法和协议 [20,21] 也是目前重要的研究方向. 对于这样的设备, 通过简化的支付验证 (SPV) [22] 的方式可以使它们在不必存储完整区块链的情况下进行工作. 这种类型的客户端被称为 SPV 客户端或轻量级客户端. 随着比特币的使用热潮, SPV 节点逐渐变成比特币节点 (尤其是比特币钱包) 最常采用的形式.

SPV 客户端不存储整个区块链, 也不验证系统中的所有交易, 只接收其所连接的完整节点为其过滤的交易的子集. 目前, SPV 客户端默认连接到四个不同的随机选择节点. SPV 客户端从一个给定的区块高度请求整个区块或只包含来自每个区块的相关交易的过滤区块. SPV 客户端只执行有限数量的验证, 例如在 Merkle 树中验证区块难度和交易的存在性证明, 并将所有交易和区块的验证工作交给比特币全节点.

由于 SPV 节点需要读取特定交易从而选择性地验证交易, 这样就又产生了隐私风险. 与全节点收集每一个区块内的全部交易所不同的是, SPV 节点对特定数据的请求可能无意中透露了钱包里的地址信息. 例如, 监控网络的第三方可以跟踪某个 SPV 节点上的钱包所请求的全部交易信息, 并且利用这些交易信息把比特币地址和钱包的用户关联起来, 从而损害了用户的隐私. SPV 钱包结合 Bloom 过滤器 (Bloom filter) [23] 解决了客户端检索的问题, 原理是 Bloom filter 可以通过一个采用概率而不是固定模式的过滤机制, 从而可以过滤掉大量无关数据, 减少客户端不必要的下载量.

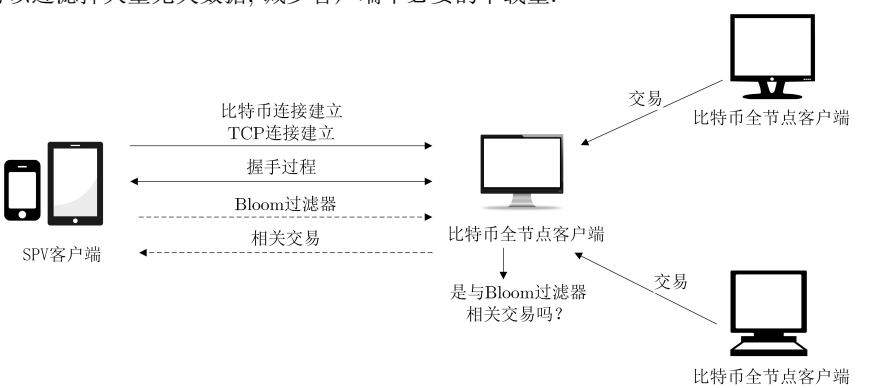


图 2 SPV 客户端操作示意图

Figure 2 Sketch of operation undergone by SPV client

如图2所示, SPV 客户端向比特币全节点发送 Bloom 过滤器, 并接收与本地钱包相关的交易. 然而 SPV 在隐私和安全方面也存在隐患, 因为网络中的关键安全组件外包给系统中的少数节点, 如果所有这些节点都是恶意的, 那么它们可以有效地控制网络上的 SPV 客户端的视图, 并且可以阻塞客户端发送和接收交易. SPV 客户端对 Bloom 过滤器的依赖泄漏了关于比特币用户地址的大量信息, 当用户重新启动 SPV 客户端或者攻击者访问属于同一个 SPV 客户端的多个 Bloom 过滤器时, 这种信息泄漏进一步恶化.

网络层同样也会信息泄露 SPV 客户端的隐私, 攻击者可以尝试通过识别用于外包 Bloom 过滤器的 IP 地址来将不同的 Bloom 过滤器链接到单个钱包. 例如, 如果相同的 IP 地址将两个不同的 Bloom 过滤器外包给常规节点, 则该节点可以直接推断出那些过滤器属于同一个实体. 由于与 SPV 客户端连接的攻击者可以看到客户端发出的交易, 并且可能会使用该交易来了解客户的地址, 所以这种泄漏更加恶化.

源于网络层的信息泄露可以得到遏制. 例如, 当 SPV 客户端发布比特币交易或者外包他们的 Bloom 过滤器时, SPV 客户端可以使用诸如 Tor 的匿名网络隐藏源 IP 地址信息; BIP-150 和 BIP-151 两种比

特币改进方案在比特币 P2P 网络中增加了对 P2P 认证和加密的支持, 其允许用户运行连接到受信任的完整节点的 SPV 客户端, 使用加密和身份验证来保护 SPV 客户端的隐私. 此外, 可以使用身份验证来创建可信比特币节点网络, 并防止中间人攻击.

2014 年, Gervais 等 [24] 研究表明, 现有比特币 SPV 客户端对 Bloom 过滤器的依赖泄漏了关于比特币用户地址的大量信息. Gervais 使用概率 $P_{h_{(N)}}$ 来量化由 Bloom filter B_i 提供的隐私效果, 即攻击者正确地猜测 B_i 中与过滤器匹配的所有正确率 (true positives) 中的任何 N 个, 并且攻击者无先验知识. 这里, N 表示插入到 B_i 中的比特币地址的数量, S 表示集合的基数. 攻击者正确猜测 B_i 的所有地址的概率由式(2)给出. 显然, $P_{h_{(.)}}$ 值越大, SPV 节点的隐私性越小.

$$P_{h_{(N)}} = \prod_{k=0}^{N-1} \frac{N-k}{N+S-k} = \frac{N!S!}{(N+S)!} \tag{2}$$

Gervais 等首先分析了攻击者获取与 SPV 客户端相关的单个 Bloom 过滤器时 SPV 客户端的信息泄露情况, 然后分析攻击者可以获取两个不同的 Bloom 过滤器 B_1、B_2 的情况. 在分析由于获取两个 Bloom 过滤器而导致的信息泄漏时, Gervais 等区分两种情况: (1) B_1、B_2 属于不同用户; (2) B_1、B_2 属于同一个用户. 在 B_1、B_2 对应于同一个 SPV 客户端的情况下, 出现三个子情况: (1) B_1、B_2 使用相同的种子, 过滤器大小相同; (2) B_1、B_2 使用不同的种子; (3) B_1、B_2 使用相同的种子, 但过滤器大小不同.

3 比特币隐私增强协议

在本节, 我们概述并分析增强比特币隐私的协议, 我们首先描述混合服务和混币技术, 然后介绍盲签名和离链支付协议对比特币在隐私保护上的改善, 这些协议都不需要修改现有的比特币协议.

3.1 混币技术

混币技术是一种不需要修改比特币协议的提高比特币匿名性的有效手段, 可以有效抵抗交易图分析攻击. 混币服务将不同用户的比特币混合后, 重新分配到特定的接收地址. 这一过程会破坏交易输入输出地址之间的链接关系. 根据混合过程是否需要可信第三方 (混合服务器) 的参与, 又可以进一步分为中心化混合方案 [25–28] 和去中心化混合方案 [29–35], 下面分别加以介绍.

3.1.1 中心化混合

中心化混合服务平台协助比特币用户去更好地保持匿名以保护隐私, 其引入可信第三方 (混合服务器) 来完成比特币用户的资金收集和分配任务. 目前很多平台 (如 BitcoinFog、BitLaundry、Blockchain.info 等) 都提供比特币混合服务, 其混合服务能够做到匿名性的前提是这些混合平台处于自身利益考虑 (如收取一定的交易费和提高平台声誉) 不保存任何转账记录, 也不要求认证用户的真实身份信息. 当数据外泄或公开时 (遭受黑客攻击或接到监管机构要求), 并不会对用户产生任何影响, 因为其中没有任何转账记录, 使用混合服务的用户的个人身份也无法识别.

除了中心化混合服务平台, Bonneau 等在文献 [25] 中提出 MixCoin, 一种依赖于第三方的中心化混币协议. MixCoin 用户使用标准交易向第三方混合服务方发送一些比特币, 然后从混合服务方接收相应数量的比特币 (扣除相应的交易费), 因此它提供了外部匿名性. MixCoin 使用基于声誉的加密问责技术来防止混合中的用户比特币窃取和协议中断.

然而, 第三方混合服务方可能随时窃取用户比特币, 或者成为对用户匿名的威胁, 因为第三方混合服务方知道用户输入地址和输出地址之间的关联. 交易费的限制使得 Mixcoin 可以抵抗 Sybil 攻击, 但是不提供内部不可链接性, 同时存在用户资金失窃的风险.

由此可见, 中心化混合服务存在诸多问题, 例如:

(1) 额外的混合费用. 随着比特币价格的持续上涨, 其交易费弊端也日益凸显.

(2) 混合服务平台知道输入输出地址之间的链接关系, 无法保证内部不可链接性, 同时也存在服务平台盗窃用户比特币的风险.

(3) 存在服务平台被恶意攻击者侵入的风险, 这会导致比特币失窃和用户隐私泄露.

为了在混合过程中实现内部不可链接性, Valenta 等提出 BlindCoin 协议 [26], 通过使用盲签名来创建用户输入和盲令牌的加密盲化输出地址来改进 MixCoin 协议. BlindCoin 具体混合步骤如下:

(1) 用户 A 通过向服务方发送其请求 (D, T_{A_C}) 来选择混合服务, 请求中包括混合参数 D 以及承诺函数 A_C 加密的盲化令牌 T, T 由输出地址 k_{out}、随机数 n 组成.

(2) 服务方向用户发送 $\{[T]_{A_C}, k_{\text{esc}}, D\}_{M_{\text{priv}}}$, 其中包括盲令牌 T、托管地址 k_{esc} 和混合参数 D, 并用服务方私钥 M_{priv} 签名.

(3) 服务方签名盲令牌 $\{[T]_{A_C}\}_{M_{\text{priv}}}$ 完成证书.

(4) 一旦盲令牌发布到公开日志上, 用户 A 可以通过承诺函数 $A_{C'}$ 来恢复签名的去盲化令牌. 用户 A' 匿名地去盲化 k_{out}, 将签名的令牌发布到公开账日志上.

然而, 为了实现这种内部的无关联性, BlindCoin 需要两次额外的交易来发布和赎回盲令牌, 而且服务商跑路的威胁依然存在. BlindCoin 解决了内部链接性问题, 但代价是盲签名带来的系统开销和混合阶段额外的时间开销. 于是研究人员提出了各类去中心化混合方案 [29–35].

类似 BlindCoin, 研究人员提出基于 RSA 盲签名的比特币混币算法 [27], 使用混币代理并设计协议混淆比特币用户交易使用地址与实际拥有地址之间的联系, 加大攻击者从区块链分析攻击的难度. 系统中引入的可信第三方实现了可控匿名. 同年提出的基于椭圆曲线盲签名方案的中心化混币算法 [28], 在性能上有了进一步的提升.

针对中心化混合服务存在的诸多问题, 研究人员提出了各类去中心化混合方案 [29–35].

3.1.2 去中心化混币

去中心化混合实现比特币匿名的思想是: n 个至少有 υ 比特币的混合节点将输入地址 $I_1, \cdots, I_n$ 混合后输出地址 $O_1, \cdots, O_n$, 使得:

(1) 每个输入节点的输出地址接收到 υ 比特币.

(2) 输入地址和输出地址是不可链接的, 即只有输入节点 i 知道 I_i 和 O_i.

本质上, 这意味着每个输入节点 i 发出交易 $I_i \xrightarrow{\upsilon} O_{\pi(i)}$, 其中 π 是 $\{1, \cdots, n\}$ 上的随机排列.

2013 年, Maxwell 首先提出 CoinJoin [29] 协议, 旨在打破比特币输入输出地址之间的链接. 每笔 CoinJoin 交易是一个标准多签名 (multi-signature) 比特币交易, 每个参与者匿名提供自己的输出地址并检查其是否被包含在该交易输出中, 如果没有则拒绝签名. 所有参与者都完成签名之后, 该交易就会作为正常比特币交易放到区块链上, 外部观察者无法判断输入输出地址之间的对应关系. CoinJoin 提供了很好的外部不可链接性, 也不存在混合费和资金失窃问题. 但是其匿名性取决于混合参与者的数目, 容易受到 DoS 攻击和 Sybil 攻击, 内部不可链接性也无法保证. CoinJoin 在以保护隐私为要旨的加密数字货币达式币 (DASH) 中得到了应用.

Fair Exchange 协议 [30] 由 Barber 等提出, 它是一个双方比特币交换协议, 双方使用比特币脚本和三类比特币交易 (包括保证交易、退款交易和索赔交易) 在不需要互相信任的情况下互相交换比特币.

CoinSwap 协议 [31] 允许双方 (Alice 和 Bob) 不通过直接的可追溯的交易进行比特币转账. 第三方 Carol 从 Alice 收到比特币后, 再使用自己的不相关比特币支付给 Bob. 通过使用多签名托管交易, CoinSwap 可在双方无信任的前提下实现比特币支付. 通过发布在比特币账本上的哈希锁定交易来解决一方不诚实执行协议问题, 避免资金损失. CoinSwap 的匿名性取决于同时参加混合的用户数 (金额相同), 然而 Carol 无利益驱动参与 Alice 和 Bob 之间的交易, 另一方面由于比特币账本的多签名交易可以被识别出来, 加上三方之间转账金额一致, CoinSwap 匿名性也受到一定程度影响.

XIM 是一个双方比特币交换协议 [32], 不需要第三方参与. XIM 中提到了一种在比特币区块链中寻找混合节点的方法, 其采用 Fair Exchange 作为交换协议, 通过收取交易费防止 Sybil 攻击和 DoS 攻击.

2014 年, Ruffing 等提出的 CoinShuffle 协议 [33] 是一个完全去中心化的比特币地址混合方案. 每个节点 i (以预定义的混洗顺序表示的节点 i) 使用节点 $j > i$ 的加密密钥来创建它的输出地址的分层加密. 然后, 从节点 1 开始顺序执行混洗: 每个节点 i 依次从节点 $i-1$ 接收到 $i-1$ 个密文. 然后, 每个节点从密文中剥离一层加密信息, 添加自己的密文再随机混洗结果集. 节点将混合的密文集发送给下一个节点 $i+1$, 最后一个节点执行解密产生一个混洗的输出地址列表并广播此列表.

CoinShuffle 混洗具体过程: 每个节点先选择一个新的比特币地址, 即新的验证-签名密钥对 $(\mathrm{vk}_i', \mathrm{sk}_i')$. 接下来节点 1 对输出地址 vk_i' 创建分层加密 c_1 并发送到节点 2, $c_1 = \mathrm{Enc}_2(\mathrm{Enc}_3(\cdots \mathrm{Enc}_N(\mathrm{vk}_i')))$. C_1 是只有 c_1 的一元向量. 在接收到向量 C_{i-1} 后, 节点 $i \in \{2, \cdots, N\}$ 对向量中的每个消息进行解密, 之后用剩余 $N-i$ 个节点的公钥加密输出地址 vk_i' 获得 c_i, $c_i = \mathrm{Enc}_{i+1}(\mathrm{Enc}_{i+2}(\cdots \mathrm{Enc}_N(\mathrm{vk}_i')))$. 然后节点 i 将 c_i 添加到解密消息向量中, 并随机混洗扩展向量, 获得新的向量 C_i.

CoinShuffle 去中心化的方式实现了内部不可链接性, 能够抵抗 DoS 攻击和防止用户混合资金失窃, 但是匿名性与匿名集合大小有关, 匿名程度低, 也容易受到交叉攻击 [36] 和 Sybil 攻击.

2015 年 Ziegeldorf 等在 CoinShuffle 之上提出了 CoinParty 协议 [35], 基于解密混合网和阈值签名方案, 通过安全多方计算 [37] 模拟可信第三方在用户之间实现安全、匿名的比特币混合. CoinParty 带来的优点是无需混合费, 提高了协议鲁棒性和可扩展性, 缺点是容易受到 DoS 攻击和需要更多的混合时间.

2017 年, Heilman 等提出了一种去中心化、去信任的混币 TumbleBit [34] 协议, 旨在实现快速实时的匿名线下交易. TumbleBit 通过中间节点 Tumber 为交易双方建立支付通道, 但是支付通道信息对 Tumber 隐藏, Tumber 也不知道交易双方的身份. TumbleBit 不需要区块确认 (节约了交易时间), 交易资金保密并且同一支付通道下的多个交易也不能被链接在一起, 同时 TumbleBit 无需对比特币协议作出修改.

我们在表 1 给出了各类去中心化混合方案的技术特点及其优缺点对比.

表 1 去中心化混合方案对比

Table 1 Comparison of decentralized coin-mixing schemes

名称	技术特点	优点	缺点
CoinJoin	多签名交易	抗 theft, 效率高	易受 Sybil 攻击、DoS 攻击
Fair Exchange	多签名托管交易, 哈希锁定	安全, 抗 theft	匿名性弱, 混合时间长
CoinSwap	P2P, 哈希锁定	安全, 抗 theft	匿名性弱, 混合时间长
XIM	基于 Fair Exchange, 匿名混合节点发现, 多轮混合	内部不可链接性, 抗 Sybil 攻击和 DoS 攻击	混合时间长
CoinShuffle	基于 CoinJoin, 解密混合网	内部不可链接性, 抗 DoS 攻击	易受 Intersection 攻击、Sybil 攻击
CoinParty	基于 CoinShuffle, 安全多方计算	鲁棒性, 不可否认性, 可扩展性	混合时间长
TumbleBit	不可链接支付通道	可扩展性, 抗 Sybil 攻击、DoS 攻击、Intersection 攻击	TumbleBit 支付至少需要两个交易

3.2 离链支付协议

离链支付协议是一类基于限制发布的保护方案, 是指不将涉及隐私的历史交易数据记录在区块链上, 既保护了隐私, 又提高了比特币区块容量, 典型应用包括闪电网络、支付通道、Bolt 方案等.

2015 年, Poon 和 Dryja 提出了比特币闪电网络概念 [38]. 通过扩展双向支通道方式 [39], 创造性地设计出了两种类型的交易合约: 序列到期可撤销合约 RSMC (revocable sequence maturity contract) 和哈希时间锁定合约 HTLC (Hashed timelock contract), 实现允许任意数量的节点即时交易. 闪电交易是一种正常的比特币交易, 只是大部分交易并没有发布到区块链上. 因为大量的交易数据是被存储在线下, 闪电交易显著降低了比特币交易成本, 使其能够实现小额快速支付.

用户之间可以开通一个双向支付通道, 通过中间节点在这个通道中进行交易. 只有当交易完成后, 通道的最终状态才会广播给区块链. 广播公开的交易信息包括他们之间的总交易量, 但不会公布他们之间的交易次数, 这种模糊性有利于保护隐私. 但是中间节点会获知交易双方隐私数据, 为解决这个问题, 目前的闪电网络包含在一种 P2P 网络上匿名转播信息的 Sphinx 协议 [40](类似于 Tor) 隐藏所有来自中间节点的路由数据.

Green 等提出的 Bolt [41] 方案通过解除交易在支付通道内的联系解决在小额支付渠道背景下的隐私保护问题. Bolt 通过使用承诺和盲签名两种加密技术, 保证同一通道下的多重支付不能被链接在一起. 但是目前 Bolt 只能支持单跳中介网络, 其去中心化问题也有待完善.

4 密码学方案保护比特币隐私

本节讨论基于密码学的比特币隐私保护技术, 相比之下, 比特币的密码学保护机制消除了对可信第三方的需求, 但代价是在性能方面有所下降.

4.1 隐蔽地址

隐蔽地址首先由 Todd 在文献 [42] 中提出, 思想是每次发送者要发起一笔交易时, 先利用接收者的公钥信息计算出一次性临时中间地址, 然后将币发送到这个中间地址, 接收方再利用自己的公私钥信息找到那笔交易, 从而进行花费. 这样网络上其他的用户包括矿工等就无法确定中间地址到底属于谁的, 但依然可以验证交易的有效性, 而由于这个地址又是一次性的, 每次都重新随机产生, 攻击者也就无法对真实的发送者接收方作任何关联.

隐蔽地址基于椭圆曲线上的 Diffie-Hellman 密钥交换. 当 Bob 想要接收比特币同时保持匿名, Bob 首先生成一个 ECDSA 密钥对 $Q = d \cdot G$(G 是一个公开的生成器), 然后发布公钥 Q 作为静态标识符. Alice 现在生成自己的临时密钥对 $P = e \cdot G$ 并计算共享密钥 $c = H(e \cdot G)$. 然后, Alice 使用 c 导出点 $Q' = Q + c \cdot G$, 将 Q' 转换为比特币地址, 并向其发送比特币. 在交易中, Alice 还将以前生成的点 P 包含在 OP_RETURN 输出 (比特币基本交易类型之一) 中. 对区块链上可能包含 P 的交易, Bob 计算 $c = H(d \cdot P)$ 并检查这是否可以导出有效点 $Q' = (d + c) \cdot G$. 然后 Bob 可以通过计算匹配的私钥 $d' = d + c$ 来花费在 Q' 上的比特币.

CryptoNote [43] 就使用了隐蔽地址技术来实现接收方匿名. 每个 CryptoNote 输出的目的地址 (默认情况下) 是一个公钥, 从接收方的地址和发送方的随机数据派生. 首先, 发送方执行 Diffie-Hellman 交换, 从接收方数据和接收方的一半地址获取共享密钥. 然后, 接收方使用共享密钥和地址的第二部分计算一次性目的地址密钥. 接收方还执行 Diffie-Hellman 交换以恢复相应的秘密密钥. 以 Alice 向 Bob 发起一笔支付为例:

1. Alice 首先获取 Bob 的公钥信息 (A, B).
2. Alice 生成一个随机数 r 并计算一次性公钥 $P = H_s(rA) \cdot G + B$.
3. 接下来 Alice 计算 $R = rG$, 然后生成一笔交易将 P 作为目的地址并将 R 也放入交易中, 也就是说现在交易中包括 R 和 P 两部分信息.
4. Alice 将交易广播到区块链上.
5. Bob 对所有的交易进行检查: 从交易中获得 R, 并通过公钥对应的私钥 (a, b) 计算期望的地址 $P' = H_s(rA) \cdot G + B$, 如果 $P' = P$, 那么该交易就是发给 Bob 的.
6. Bob 找到自己的交易后就可以计算出对应的私钥 $x = H_s(aR) + B$, 然后使用私钥签名交易进行花费.

通过变换 r 的值, 即使 Alice 发给 Bob 很多笔交易, 每笔交易的输出目标地址也是不同的, 这样交易的匿名性就得到了保障 (既无法猜到交易的发送方是谁, 也无法猜到接收方是谁). 由于交易的接收方 (即 Bob) 需要不断检查交易是否是给自己的, 其需要对每笔交易的每个输出进行计算, 这也消耗不少的计算资源. Bob 可以将其一半的私钥 (a, B) 告诉第三方, 由其提供服务对交易进行检查 (即计算 P' 并判断其是否等于 P), 而由于 B 对应的私钥 b 没有公开, 所以第三方也无法花费 Bob 拥有的资产 (即交易输出). 此外, Alice 也可以通过公布 r(或者通过 r 进行签名并由他人验证) 来证明交易的发送方是其本人.

DarkWallet 和 BitShares 也在使用隐蔽地址技术, 然而隐蔽地址技术不对发送方匿名, 为了解决这个问题, CryptoNote [43] 引入了环签名方案将发送方交易隐藏在匿名集合中.

4.2 环签名

2001 年, Rivest 等 [44] 在如何匿名揭示秘密的背景下提出了环签名 (ring signatures) 技术, 环签名是一种特殊的群签名, 没有可信中心, 也没有群的建立过程, 对于验证者来说签名者是完全匿名的. 在环签名方案中, 环中一个成员利用他的私钥和其他成员的公钥进行签署交易, 而验证者只知道签名来自这个环, 但不知到谁是真正的签名者. 环签名解决了对签名者完全匿名的问题, 环签名允许一个成员代表一组人进行签名而不泄漏签名者的信息. 基于环签名的方案为去中心化的账本体系提供了可行的匿名化思路.

与一般数字签名方案类似, 环签名方案包含两个基本的环节:

(1) 环签名 (ring-sign): 对于消息 m, 用户 s 使用一组公开信息 $(P_1, P_2, \cdots, P_r)$ 以及私钥 S_s, 生成签名 σ.

(2) 环签名验证 (ring-verify): 对于验证者, 当其获得消息 m 和签名 σ 时, 判断这个签名是否有效.

CryptoNote [43] 协议正是使用环签名保护用户隐私, 其一次性环签名的签名和验证步骤如下:

(1) 密钥生成 (GEN). 签名者首先随机选择一个私钥 x, 然后计算对应的公钥 $P = xG$, 同时还计算另外一个公钥 $I = xH_p$, 这个公钥 I 称之为 "密钥镜像"(key image), 对于每一个签名来说这个密钥镜像是唯一的, 所以后面也被用来判断签名是否之前出现过.

(2) 签名 (SIG). 签名过程是一个非交互零知识证明过程. 签名者取其他 (部分) 用户的公钥 P_i 形成集合 $S' = \{P_i\}$, $|\{P_i\}| = n$, 和自己的公钥一起组成集合 $S = S' \cup \{P_s\}$ ($s \in [0, n]$ 表示交易发送方的公钥 P_s 在集合 S 中的秘密索引). 然后签名者再随机选择 $\{q_i | i = 0, \cdots, n\}$ 和 $\{w_i | i = 0, \cdots, n, i \neq s\}$, 计算

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases} \tag{3}$$

$$R_i = \begin{cases} q_i H_p(P_i), & \text{if } i = s \\ q_i H_p(P_i) + w_i I, & \text{if } i \neq s \end{cases} \tag{4}$$

接着计算一个非交互式挑战 $c = H_s(m, L_1, \cdots, L_n, R_1, \cdots, R_n)$, 最后签名者再计算响应:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \bmod l, & \text{if } i = s \end{cases} \tag{5}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \bmod l, & \text{if } i = s \end{cases} \tag{6}$$

最终的签名就是 $\sigma = (I, c_1, \cdots, c_n, r_1, \cdots, r_n)$.

(3) 签名验证 (VER). 验证者要验证签名的有效性, 首先计算

$$\begin{cases} L'_i = r_i G + c_i P_i \\ R'_i = r_i H_p(P_i) + c_i I \end{cases} \tag{7}$$

然后验证 $\sum_{i=0}^{n} c_i = H_s(m, L'_0, \cdots, L'_n, R'_0, \cdots, R'_n)$. 如果等式成立, 再通过 LNK 来检测签名是否重复使用; 如果等式不成立, 说明签名是非法的.

(4) 重复检测 (LNK). 检查密钥镜像是否已被使用, 即双重支付检查. 验证者保存已使用过 (即曾经已用于签名的) 的密钥镜像集合 $I = I_i$, 如果签名 σ 中的密钥镜像在集合中存在, 表示该密钥镜像已被使用, 即说明该交易存在双重支付的情况.

CryptoNote 实现的可追溯环签名可以有效防止双花. 在可追溯环签名算法中, 由一个私钥签发的两个签名是可以被关联起来的, 因此, 只要一笔交易双花, 意味着私钥签发了两个不同的签名, 因此可以被检测出来, 从而解决双花问题.

虽然 CryptoNote 加密技术解决了加密货币的许多问题, 提供了良好的匿名性, 但是存在交易规模大和区块链扩展性差的问题. 目前在 CryptoNote 加密货币中实现的环签名大小上存在限制, 因为随着环的尺寸的增加, 交易数据的大小线性增长. 该加密技术的主要缺点是, 它的交易特别是 RingCT [45](环状机密交易) 的交易非常大, 占用了几千字节, 这大大增加了存储区块链所需空间, 目前还无法精简已形成的加密区块链. 使用与比特币完全不同的代码库, 也意味着很难将其整合到现有的比特币生态系统中.

除此之外, 以太坊平台 [46] 也增加了一个类 CryptoNote 环签名, 这样使得以太坊用户拥有类似于门罗币 (Monero) 的匿名能力. 一些基于 CryptoNote 的密码货币例如 Bytecoin 和 DarkNetSpace 使用环签名来隐藏发送方.

4.3 零知识证明

零知识证明最先由 Goldwasser 等 [47] 在 20 世纪 80 年代初提出, 指的是一方 (证明者) 能够在不向另一方 (验证者) 提供任何有用的信息 (在密码货币和区块链中, 这通常是指交易信息数据) 的前提下, 也能使得另一方能够相信某个论断是正确的, 一定程度上保护了自身的隐私. 零知识证明具有 3 条性质:

(1) 完备性. 如果论述是真实的, 诚实的证明者能够以绝对优势的概率使诚实的验证者相信该事实.

(2) 可靠性. 如果论述是错误的, 欺骗性的证明者不能, 或者只能以可忽略的概率使诚实的验证者相信它是真实的.

(3) 零知识性. 证明过程执行完之后, 验证者只获得了 "证明者拥有这个知识" 这条信息, 证明过程中不可向验证者泄漏任何有关被证明知识的内容.

Zerocoin [48] 和 Zerocash [49] 都是通过引入零知识证明而达到匿名目的的加密货币.

4.3.1 Zerocoin

Zerocoin 方案 [48] 把比特币换成一个 Zerocoin 币, 使用承诺隐藏交易细节, 再从另一个比特币地址中换回 Zerocoin 币, 割裂输入地址和输出地址的关系. Zerocoin 通过创建两种新的交易类型来扩展比特币: 铸币交易 (mint) 和花费交易 (spend). 铸币交易允许用户交换一定数量的比特币以制造新的 Zerocoin 币. 每个 Zerocoin 币是使用随机数 r 对序列号 sn 的币承诺 cm, $\mathrm{cm} := \mathrm{COMM}_r(\mathrm{sn}) = g^{\mathrm{sn}}h^r$.

随后, 用户可以发出包括接收地址、序列号 sn 和 NP 语句的非交互式零知识证明的 spend 交易 "我知道秘密 cm 和随机数 r 使得:

(1) cm 过去被铸币 (Zerocoin 币存在于区块链上);

(2) 通过承诺随机数 r 打开 cm(揭露承诺 cm 背后的序列号 sn)."

Zerocoin 构建相应的零知识证明通过累加器累积所有铸币承诺的集合, 然后证明该集合中相应的承诺随机数和集合中元素. 在 Zerocoin 中, 计算累加器的见证 (witness) 需要访问目前为止的所有承诺. 零知识证明并不将花费交易与任何特定的铸币交易 (迄今为止所有铸币交易之间) 相联系. 如果验证正确, 并且序列号以前没有被花费, 则将相应量的比特币发送到目的地址. 同样地, Zerocoin 也存在许多问题:

(1) 功能局限性. Zerocoin 不能用来支付, 不能拆分金额.

(2) 匿名效果. Zerocoin 不能隐藏交易金额和接收方地址.

(3) 性能问题. Zerocoin 的零知识证明, 至少占 45 KB 空间和 450 ms 的验证时间 (128 位密钥长度), 必须全网广播和存储, 并且由每个节点验证, 将带来巨大的区块链容量和验证时间.

4.3.2 Zerocash

针对 Zerocoin 方案的诸多缺陷, 研究人员提出 Zerocash [49] 方案加以改进, 使用 zk-SNARKs (zero-knowledge succinct non-interactive argument of knowledge, 零知识的简洁非交互式知识论证) 保证交易之间的不可链接性, 同时也对交易金额和输入地址保密, 达到了更好的隐私保护效果.

Zerocash 是一个去中心化密码货币协议, 与比特币一样, 用户通过广播和验证支付交易来协作维护电子货币. 然而, 在合并支付交易和验证方式上 Zerocash 与比特币是不同的. Zerocash 扩展了比特币协议, 添加了新的交易类型, 提供了独立的隐私保护货币, 交易不会泄露支付账户、接收账户以及支付金额等信息. Zerocash 创建了一种独立的匿名币, 此外还有一种基础币 Basecoin (非匿名). 每一个用户都可以将 Basecoins 转换为 Zerocash 币 (匿名), 我们将后者称之为 Zerocoins. 之后用户可以将 Zerocoins 发送给其它用户、拆分或合并 Zerocoins.

Zerocash 结构如图 3 所示, 下面从可变金额、匿名传输、验证效率介绍 Zerocash 的改进.

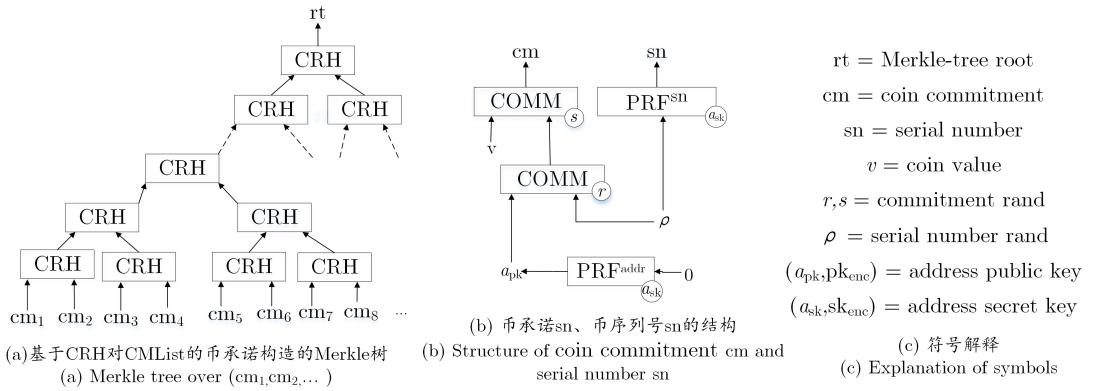
(1) 可变金额. 为完成支付功能, zerocash 使用地址密钥对 $(a_{\mathrm{pk}}, a_{\mathrm{sk}})$, 对应地址公钥和地址私钥. 要铸造一个望值 v 的币, 用户首先随机选择 ρ, 即将币的序列号确定为 $\mathrm{sn} := \mathrm{PRF}(^{\mathrm{sn}}_{a_{\mathrm{sk}}}(\rho))$ 的秘密值. 那么, 用户分两个阶段对元组 (a_{pk}, v, r) 作出承诺:

(a) 对随机数 r 计算 $k := \mathrm{COMM}_r(a_{\mathrm{pk}} \parallel \rho)$;

(b) 对随机数 s 计算 $\mathrm{cm} := \mathrm{COMM}_s(v \parallel k)$.

铸币结果是币承诺 $c := (a_{\mathrm{pk}}, v, \rho, r, s, \mathrm{cm})$ 和铸币交易 $\mathrm{tx}_{\mathrm{mint}} := (v, k, s, \mathrm{cm})$. 由于嵌套的承诺, 任何人都可以验证 $\mathrm{tx}_{\mathrm{mint}}$ 中的 cm 是价值 v 的币承诺 (通过检查 $\mathrm{COMM}_s(v \parallel k)$ 等于 cm), 但不能识别所

有者 (通过地址 a_{pk}) 或序列号 sn(派生自 ρ), 因为它们都隐藏在 k 中. 如前所述, 只有在存入正确金额 v 的情况下, tx_{mint} 才被分类帐本接受.



(a)基于CRH对CMList的币承诺构造的Merkle树
(a) Merkle tree over (cm_1,cm_2,...)

(b) 币承诺sn、币序列号sn的结构
(b) Structure of coin commitment cm and serial number sn

(c) 符号解释
(c) Explanation of symbols

图 3 Zerocash 结构图
Figure 3 Structure of Zerocash

(2) 匿名传输. Zerocash 修改地址密钥对的结构, 如图 4 所示, 其中箭头指示密钥推导过程. Zerocash 地址密钥对包括两个公钥: 与接收地址的币承诺匹配的接收密钥 a_{pk} 和用于 key-private 非对称加密方案的传输密钥 $\mathrm{pk}_{\mathrm{enc}}$. "key-private" 意味着除了相应的私钥 (查看密钥 $\mathrm{sk}_{\mathrm{enc}}$) 的持有者, 密文不会泄露关于它们被加密的密钥的信息. 地址密钥对用于将区块链上的加密币承诺传送给目的接收方, 接收方可以使用查看密钥 $\mathrm{sk}_{\mathrm{enc}}$ 扫描区块链中的币承诺, 然后解密.

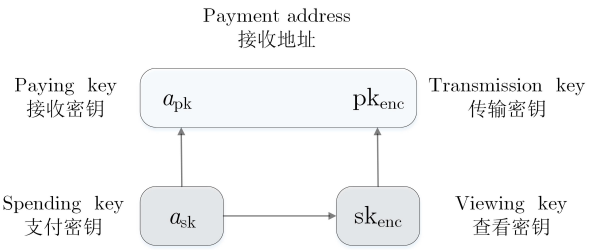


图 4 Zerocash 地址密钥对结构
Figure 4 Structure of address key-pair of Zerocash

用户在 $\mathrm{pk}_{\mathrm{enc}}^{\mathrm{new}}$ 下计算明文 $(v^{\mathrm{new}}, \rho^{\mathrm{new}}, r^{\mathrm{new}}, s^{\mathrm{new}})$ 的加密密文 C, 并将 C 包含在花费交易中 ($\mathrm{addr}_{\mathrm{pk}}^{\mathrm{new}}$ 是用户新的公钥地址). 通过扫描公开帐本上的花费交易来查找和解密该消息 (使用私钥 $\mathrm{sk}_{\mathrm{enc}}^{\mathrm{new}}$). 由于加密方案的密钥私有属性, 将 C 添加到花费交易中, 既不泄露支付金额, 也不会泄露目标地址.

(3) 验证效率. Zerocash 通过对 (增长的) 列表 CMList 维护一个高效可更新的基于抗碰撞函数 CRH 的 Merkle-tree: Tree, 并使 rt 表示 Tree 的根. 插入新的叶节点时, rt 被更新的时间和空间复杂度与树的深度成比例. 因此, 运算成本从 CMList 的线性级降至对数级, 也增加了列表空间 (深度为 64 的树可以支持存储 2^{64} 个币).

Zerocash 将 NP 语句修改为: "我知道 r, 使得 $\mathrm{COMM}_r(\mathrm{sn})$ 作为叶节点出现在基于 CRH 的 Merkle-tree 中." 与初始数据结构相比, 该修改指数增加了给定的 zk-SNARKs 实现可以支持的 CMList 的大小.

4.4 同态加密

同态加密最初在 1978 年由 Rivest 等 [50] 提出: "是否可以无需密钥就能够对密文进行计算"? 同态加密也称为隐私同态, 实现无需解密信息数据即可对加密数据进行运算. 这种技术允许在保留对数据和交易隐私的同时还能对其进行运算, 只有使用解密秘钥才能访问这些数据和交易的详细信息. 区块链上的数据

将会被加密, 保护了公有区块链的隐私. 使用同态加密技术在区块链上加密存储数据, 不会对其公有链属性造成改变. 同态加密技术使公有区块链具有私有区块链的隐私效果.

为了保护交易数据的私密性, 通常需要将交易数据进行加密, 但同时还需要保障交易的合法性和可验证性. 在很多场景下, 交易合法性表现为交易的输入总和等于输出总和, 交易中的每一个金额都大于 0, 小于一个上界.

2014 年, França [51] 改进了微型区块链 [52], 使之更加私密, 更具可扩展性. França 通过使用同态加密对交易金额和账户余额进行加密来实现这一目的, 允许用户对加密值执行加法和减法而不会泄露明文. 随后在 2015 年, França 设计了一个新的基于微型区块链 [52] 和同态承诺的加密货币 [53] 以实现更好的隐私保护, 分析表明能有效防御区块链分析攻击.

机密交易 (confidential transactions) 最初由 Adam 在 2013 年比特币论坛中提出, 并由比特币核心开发人员 Maxwell 开发 [54]. 机密交易希望通过隐藏交易的金额提高比特币区块链的隐私, 基本思想是加密明文交易脚本, 使用 Pedersen 承诺 [55] 作为同态工具来操作密文, 保证转账交易数量只对参与者可见. 但是, 机密交易容量相对较大, 标准交易需要大概 200 字节的空间, 机密交易所需空间是普通交易的 60 倍. 即使通过软分叉部署在比特币区块链上, 也会对现有区块链容量造成极大负担. 机密交易目前部署在了 Blockstream 的 Element 侧链上.

2017 年, 研究人员提出基于加法同态加密技术隐藏区块链上的交易金额和用户余额 [56], 解决了传统区块链交易中暴露了真实的转账金额的问题, 实现了区块链上的隐私保护功能. 但是需要利用到可信任第三方信息机构. 同年, Wang 等 [57] 通过使用同态 Paillier 加密系统 [58] 来实现交易金额的隐藏, 以及用承诺证明方案来实现密文交易金额的验证过程, 保证: (1) 账号余额非负; (2) 输入总和与输出总和相等. 分析显示, 该系统不仅提高了匿名性, 也能有效抵抗主动攻击和被动攻击.

同态加密对于区块链的意义非常重大. 目前, 从安全的角度讲, 用户并不愿意将敏感信息直接放到区块链上进行运算, 如果有足够实用的同态加密技术, 用户就可以放心地使用区块链服务而不用担心信息泄露. 尽管当前的同态加密尤其全同态加密技术需要消耗大量的计算时间, 还远达不到大规模应用的水平, 但对于数据规模较小且需求较迫切的业务场景, 如智能合约层面的实现依然具有极强的现实意义.

5 总结与展望

表 2 分别从技术特点、匿名性、优缺点等方面, 总结了混币技术、离链支付协议、隐蔽地址、环签名、零知识证明、同态加密几类最新区块链隐私保护技术.

表 **2** 区块链隐私保护技术对比

Table 2 Comparison of Blockchain privacy protection technology

名称	技术特点	匿名性	优点	缺点	典型应用
中心化混合	可信第三方	弱	混合时间短	资金失窃风险	BitLaundry
去中心化混合	多签名交易, 哈希锁定	一般	安全, 无交易费	混合时间长	CoinJoin, CoinShuffle
离链支付协议	链下交易	弱	快速交易	匿名性弱	闪电网络, Bolt
隐蔽地址	一次性中间地址	弱	接收方匿名	发送方未匿名	Todd 方案, CryptoNote
环签名	无条件匿名性	一般	内部不可链接性, 双花检测	开销大, 可扩展性差	CryptoNote
零知识证明	零知识性, 承诺	强	隐藏交易细节, 抗交易图分析	计算、存储开销大	Zerocoin, Zerocash
同态加密	密文计算, 承诺	强	抗交易图分析	计算、存储开销大	机密交易

随着以比特币为代表的区块链技术的快速发展以及其在金融、物联网、通信、大数据等各个领域的广泛应用, 其隐私保护与性能问题也越来越突出. 现有的匿名技术方案还不够完善, 需要设计更加安全、高

效的隐私保护方案. 其中最具有代表性的方案是结合区块链和可信计算技术 (如 Intel SGX) 提供信任机制和隐私保护, 也已经成为该研究领域的新方向.

References

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. http://bitcoin.org/bitcoin.pdf. 2008.

[2] PFITZMANN A, HANSEN M. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management[OL]. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. 2010.

[3] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]. In: Proceedings of 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. IEEE, 2011: 1318–1326. [DOI: 10.1109/PASSAT/SocialCom.2011.79]

[4] AWAN M K, COREST A. Blockchain transaction analysis using dominant sets[C]. In: Computer Information Systems and Industrial Management—CISIM 2017. Springer Cham, 2017: 229–239. [DOI: 10.1007/978-3-319-59105-6_20]

[5] MAESA D D F, MARINA A, RICCI L. Uncovering the Bitcoin Blockchain: An analysis of the full users graph[C]. In: IEEE International Conference on Data Science and Advanced Analytics. IEEE, 2016: 537–546. [DOI: 10.1109/DSAA.2016.52]

[6] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of Bitcoins: Characterizing payments among men with no names[C]. In: Internet Measurement Conference 2013. ACM, 2013: 127–140. [DOI: 10.1145/2504730.25047]

[7] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]. In: Financial Cryptography and Data Security—FC 2013. Springer Berlin Heidelberg, 2013: 34–51. [DOI: 10.1007/978-3-642-39884-1_4]

[8] GOLDFEDER S, KALODNEEER H, REISMAN D, et al. When the cookie meets the Blockchain: Privacy risks of web payments via cryptocurrencies[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(4): 179–199. [DOI: 10.1515/popets-2018-0038]

[9] DOUCEUR J R. The Sybil attack[C]. In: Peer-to-Peer Systems—IPTPS 2002. Springer Berlin Heidelberg, 2002: 251–260. [DOI: 10.1007/3-540-45748-8_24]

[10] KAMINSKY D. Black ops of TCP/IP[J]. Black Hat USA, 2011: 44.

[11] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in Bitcoin using P2P network traffic[C]. In: Financial Cryptography and Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 469–485. [DOI: 10.1007/978-3-662-45472-5_30]

[12] LISCHKE M, FABIAN B. Analyzing the Bitcoin network: The first four years[J]. Future Internet, 2016, 8(4): 7. [DOI: 10.3390/fi8010007]

[13] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: The second-generation onion router[C]. In: Proceedings of the 13th Conference on USENIX Security Symposium. USENIX Association, 2004: 303–320.

[14] BIRYUKOV A, KHOVRATOVICH D, PUSTOGAROV I. Deanonymisation of clients in Bitcoin P2P network[C]. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 15–29. [DOI: 10.1145/2660267.2660379]

[15] BIRYUKOV A, PUSTOGAROV I. Bitcoin over Tor isn't a good idea[C]. In: Proceedings of 2015 IEEE Symposium on Security and Privacy. IEEE, 2015: 122–134. [DOI: 10.1109/SP.2015.15]

[16] KARAME G, AUDROULAKI E. Bitcoin and Blockchain Security[M]. Artech House, 2016: 93–97.

[17] WOOD A D, STANKOVIC J A. Denial of service in sensor networks[J]. Computer, 2002, 35(10): 54–62. [DOI: 10.1109/mc.2002.1039518]

[18] BOJJA V S, FANTI G, VISWANATH P. Dandelion: Redesigning the Bitcoin network for anonymity[OL]. https://arxiv.org/abs/1701.04439v1. [DOI: 10.1145/1235]

[19] FRANCO P. Understanding Bitcoin: Cryptography, Engineering and Economics[M]. John Wiley & Sons, 2014: 123–142.

[20] TENG J K, WU C K. An identity-based group key agreement protocol for low power mobile devices[J]. Chinese Journal of Electronics, 2016, 25(4): 726–733. [DOI: 10.1049/cje.2016.06.038]

[21] SINGH S, SHARMA P K, MOON S Y, et al. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions[J]. Journal of Ambient Intelligence and Humanized Computing, 2017: 1–18. [DOI: 10.1007/s12652-017-0494-4]

[22] HEARN M, SCHILDBACH A. BitcoinJ[EB/OL]. https://bitcoinj.github.io.

[23] BLOOM B H. Space/time trade-offs in Hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422–426. [DOI: 10.1145/362686.362692]

[24] GERVAIS A, CAPKUN S, KARAME G O, et al. On the privacy provisions of bloom filters in lightweight Bitcoin clients[C]. In: Proceedings of the 30th Annual Computer Security Applications Conference. ACM, 2014: 326–335. [DOI: 10.1145/2664243.2664267]

[25] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for Bitcoin with accountable mixes[C]. In: Financial Cryptography and Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 486–504. [DOI: 10.1007/978-3-662-45472-5_31]

[26] VALENTA L, ROWAN B. Blindcoin: Blinded, accountable mixes for Bitcoin[C]. In: Financial Cryptography and Data Security—FC 2015. Springer Berlin Heidelberg, 2015: 112–126. [DOI: 10.1007/978-3-662-48051-9_9]

[27] WU W D. Bitcoin mix system design based on blind signature[D]. Shenzhen University, 2015. [DOI: CNKI:CDMD:2.1015.412641]
吴文栋. 基于盲签名技术的比特币混币系统设计与实现 [D]. 深圳大学, 2015. [DOI: CNKI:CDMD:2.1015.412641]

[28] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[OL]. arXiv:1510.05833. https://arxiv.org/ftp/arxiv/papers/1510/1510.05833.pdf. 2015.

[29] MAXWELL G. CoinJoin: Bitcoin privacy for the real world[EB/OL]. https://bitcointalk.org/index.php?topic=279249. 2013.

[30] BARBER S, BOYEN X, SHI E, et al. Bitter to better—How to make Bitcoin a better currency[C]. In: Financial Cryptography and Data Security—FC 2012. Springer Berlin Heidelberg, 2012: 399–414. [DOI: 10.1007/978-3-642-32946-3_29]

[31] MAXWELL G. CoinSwap: Transaction graph disjoint trustless trading[EB/OL]. https://bitcointalk.org/index.php?topic=321228.0. 2013.

[32] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for Bitcoin[C]. In: The Workshop on Privacy in the Electronic Society. ACM, 2014: 149–158. [DOI: 10.1145/2665943.2665955]

[33] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: Practical decentralized coin mixing for Bitcoin[C]. In: Computer Security—ESORICS 2014, Part II. Springer Cham, 2014: 345–364. [DOI: 10.1007/978-3-319-11212-1_20]

[34] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub[C]. In: 2017 Network and Distributed System Security Symposium. San Diego, CA, USA, 2017. [DOI: 10.14722/ndss.2017.23086]

[35] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: Secure multi-party mixing of Bitcoins[C]. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. ACM, 2015: 75–86. [DOI: 10.1145/2699026.2699100]

[36] DANEZIS G, SERJANTOV A. Statistical disclosure or intersection attacks on anonymity systems[C]. In: Information Hiding—IH 2004. Springer Berlin Heidelberg, 2004: 293–308. [DOI: 10.1007/978-3-540-30114-1_21]

[37] GEISLER M, NIELSEN J B. Asynchronous multiparty computation: Theory and implementation[C]. In: Public Key Cryptography—PKC 2009. Springer Berlin Heidelberg, 2009: 160–179. [DOI: 10.1007/978-3-642-00468-1_10]

[38] POON J, DRYJA T. The Bitcoin lightning network: Scalable off-chain instant payments[EB/OL]. https://lightning.network/lightning-network-paper.pdf. 2015.

[39] DECKER C, WATTENHOFER R. A fast and scalable payment network with Bitcoin duplex micropayment channels[C]. In: Stabilization, Safety, and Security of Distributed Systems—SSS 2015. Springer Cham, 2015: 3–18. [DOI: 10.1007/978-3-319-21741-3_1]

[40] MILLER A, BENTOV I, KUMARESAN R, et al. Sprites: Payment channels that go faster than lightning[OL]. https://arxiv.org/abs/1702.05812v1, 2017.

[41] GREEN M, MIERS I. Bolt: Anonymous payment channels for decentralized currencies[C]. In: 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017: 473–489. [DOI: 10.1145/3133956.3134093]

[42] TODD P. Stealth addresses[EB/OL]. 2014. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html

[43] SABERHAGEN N V. CryptoNote v 2.0[R/OL]. https://cryptonote.org/whitepaper.pdf. 2013.

[44] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[C]. In: Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 552–565. [DOI: 10.1007/3-540-45682-1_32]

[45] NOETHER S, MACKENZIE A. Ring confidential transactions[J]. Ledger, 2016, 1: 1–18. [DOI: 10.5195/LEDGER.2016.34]

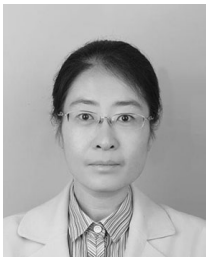
[46] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[EB/OL]. https://gavwood.com/paper.pdf. 2014.

[47] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof-systems[C]. In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. ACM, 1985: 291–304. [DOI:10.1145/22145.22178]
[48] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: Anonymous distributed E-cash from Bitcoin[C]. In: 2013 IEEE Symposium on Security and Privacy. IEEE, 2013: 397–411. [DOI: 10.1109/SP.2013.34]
[49] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized anonymous payments from Bitcoin[C]. In: 2014 IEEE Symposium on Security and Privacy. IEEE, 2014: 459–474. [DOI: 10.1109/SP.2014.36]
[50] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169–180.
[51] FRANÇA B F. Privacy and pruning in the mini-blockchain[EB/OL]. https://cryptonite.info/files/Anonymity_account_tree.pdf. 2014.
[52] BRUCE J D. The mini-blockchain scheme[EB/OL]. https://cryptonite.info/files/mbc-scheme-rev3.pdf. 2017.
[53] FRANÇA B F. Homomorphic mini-blockchain scheme[EB/OL]. http://cryptonite.info/files/HMBC.pdf. 2015.
[54] MAXWELL G. Confidential transactions[EB/OL]. https://people.xiph.org/∼greg/confidential_values.txt. 2015.
[55] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]. In: Advances in Cryptology—CRYPTO'91. Springer Berlin Heidelberg, 1991: 129–140. [DOI: 10.1007/3-540-46766-1_9]
[56] LIANG X B, LI Q L, YIN K T, et al. A Blockchain privacy protection method based on additive homomorphic encryption[P]. China. CN106549749A. 2017-03-29.
梁秀波, 李启雷, 尹可挺, 等. 一种基于加法同态加密的区块链隐私保护方法 [P]. 中国. CN106549749A. 2017-03-29.
[57] WANG Q, QIN B, HU J, et al. Preserving transaction privacy in Bitcoin[J]. Future Generation Computer Systems, 2017, In Press. [DOI: 10.1016/j.future.2017.08.026]
[58] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in Cryptology—EUROCRYPT'99. Springer Berlin Heidelberg, 1999: 223–238. [DOI: 10.1007/3-540-48910-X_16]

作者信息

李旭东 (1993–), 安徽无为人, 博士生在读. 主要研究领域为区块链、信息安全.
xudongli@mail.ustc.edu.cn

牛玉坤 (1989–), 河南周口人, 博士生在读. 主要研究领域为应用密码学.
xiaoniu@mail.ustc.edu.cn



魏凌波 (1979–), 陕西周至人, 博士, 副研究员. 主要研究领域为应用密码学.
lbw@ustc.edu.cn

张驰 (1977–), 湖北武汉人, 博士, 副教授. 主要研究领域为无线网络、网络安全.
chizhang@ustc.edu.cn

俞能海 (1964–), 安徽无为人, 教授. 主要研究领域为多媒体数据处理与分析、数字内容安全.
ynh@ustc.edu.cn