文章编号:1671-4229(2021)04-0001-15

区块链隐私保护技术研究综述

谭作文[1]，唐春明[2]
(1. 江西财经大学 信息管理学院，江西 南昌　330032；2. 广州大学 数学与信息科学学院，广东 广州　510006)

摘　要：区块链技术综合了非对称加密体系、分布式计算范式和共识算法以及智能合约等多种技术，是一种“去中心化”的分布式账本，受到了人们的广泛关注。然而，由于其交易记录可以公开访问，分布式账本面临着严重的隐私泄露问题。文章旨在对区块链隐私威胁和保护机制进行全面研究，介绍区块链技术中身份隐私和交易隐私的概念，对区块链现有隐私保护机制进行分类，分析各自的优缺点。此外，还展望了未来区块链隐私保护研究可能的发展方向。

关键词：比特币；区块链；共识算法；密码体制；隐私泄露
中图分类号：TP 311　　**文献标志码**：A

A survey on privacy protection techniques in blockchain system

TAN Zuo-wen[1]，*TANG Chun-ming*[2]
(1. School of Information Technology, Jiangxi University of Finance & Economics, Nanchang 330032, China;
2. School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China)

Abstract: Blockchain is a kind of ‘decentralized’ distributed ledger, which integrates asymmetric encryption algorithms, new distributed computing paradigms, consensus algorithms, smart contracts and other technologies. It has aroused extensive attention. However, since transaction records on the blockchain are publicly accessible to users, the ledger sharing mechanism is faced with serious privacy leaks. This paper aims to conduct comprehensive research on the privacy threats and protection mechanisms of blockchains. The concepts of identity privacy and transaction privacy in blockchain technology are introduced, the existing privacy protection mechanisms of the blockchain are classified, and their respective advantages and disadvantages are analyzed. In addition, some suggestions about future directions on blockchain privacy protection research are given.

Key words: bitcoin; blockchain; consensus mechanism; cryptographic system; privacy disclosure

2008 年 10 月 31 日，Nakamoto[1] 的文章《Bitcoin: A peer-to-peer electronic cash system》出现在密码朋克邮件列表中，这标志着比特币的诞生。起初，区块链技术被看作是支持和实现比特币的关键基础技术。随后，人们发现区块链是一种分布式账本，加密数字货币是底层区块链技术之上的一种激励手段或金融工具。从中本聪提出比特币区块链起，区块链的发展可以大致划分为 3 个阶段：数字货币区块链 1.0，如比特币；引入智能合约的数字金融区块链 2.0，如以太坊；数字社会区块链 3.0。区块链 3.0 阶段出现了许许多多区块链智能合约去中心化应用 DApps (Decentralized Application)。对比中心化系统存在的信任依赖、效率低下及数据存储安全威胁大等弱点，区块链具有分布式、透明、防篡改、交易可追溯和去信任化等明显特点和优势。区块链技术被认为是继移动互联网后的第五代互联网颠覆性技术，将引领信息互联网向价值互联网转变。节点之间通过区块链技术将不需要借助第三方可信机构就能够建立起可信任的价值传递。传统金融结算系统存在对账清算

基金项目：国家自然科学基金资助项目(61862028;61772147)
作者简介：谭作文(1967—)，男，教授，博士. E-mail: tanzyw@163.com
引文格式：谭作文，唐春明. 区块链隐私保护技术研究综述[J]. 广州大学学报(自然科学版)，2021，20(4)：1-15.

慢、需要很高的中心化数据维护成本等缺陷,尤其跨境结算时间长。区块链能够去除这些痛点,可以被广泛地应用到支付清算、保险理赔、供应链金融和能源互联网等领域[2]。据 Gartner[3] 预测,2022 年,全球以区块链交易预计将有 100 亿美元。2023 年,全球近 30% 的新闻和视频内容将使用区块链认证。2025 年,区块链交易额预计会达到1 760 亿美元。2030 年,全球区块链交易额预计会达到 3.1 万亿美元。

随着区块链技术的广泛应用,区块链面临的安全威胁和挑战也越来越多。区块链不依赖中心节点,交易记录,如参与用户的地址和交易金额等,常常在区块链上公开,便于节点验证、存储交易内容并达成共识。但是,区块链的这种公开透明性将可能导致用户隐私泄露。各个区块链节点的安全性能和对抗信息泄露的能力不一,这更增加了数据隐私泄露风险。区块链中各种程序的缺陷也将使得区块链系统面临巨大的安全风险。2014 年 3 月,日本最大的比特币交易平台 MTGOX 遭受分布式拒绝服务 DDoS 攻击(Distributed Denial of Service),交易所用户信息被泄露,85 万枚比特币被盗走,经济损失超过 4.8 亿美元[4]。2016 年 6 月,当时区块链业界最大的众筹项目 The DAO(以太坊智能合约组成分布式自治组织)因软件中存在的“递归调用漏洞”问题丢失价值超过 6 000 万美元的 360 万以太币[5]。2016 年,中国香港比特币交易所 Bitfinex 发生用户私钥泄漏事件,黑客总共盗走了高达 7 500 万美元的比特币。

隐私对于个人和企业都至关重要,将身份信息、交易金额等交易内容公开记录在区块链上,将给交易用户带来严重的隐私泄露问题。例如,通过对金融链或供应链上的金额和合约等交易信息及供应服务信息进行分析,竞争对手可以获取商业机密,直接损害交易用户的利益。有些敏感信息的泄露甚至可能对国家安全造成威胁。在比特币[1]白皮书中,作者专门用了一章的篇幅分析比特币存在的安全威胁。例如,比特币并未采用 CA 来管理用户,而对用户公钥进行了匿名处理。通过区块链交易记录,可以看到交易接受方地址和发送方地址以及交易金额,但用户身份仍然保持一定的隐私性,无法将交易参与方地址与现实中用户的身份关联起来。然而,这种方式仅仅增加了用户的匿名性。通过对比特币交易内容结合其他平台获得的信息进行综合分析,常常可以跟踪到交易参与方的多个交易数据,找到地址间的关联性,发现用户的交易规律,甚至推测出用户现实世界中的真实身份和其他隐私[6]。

传统中心化存储架构的主要隐私保护手段有 K-匿名[7]、同态加密[8]和密码共享以及差分隐私[9]等。区块链是一种分布式账本,中心化数据隐私保护方案并不适用于它。近年来,人们开展了区块链安全[10-11]和隐私保护方面的研究[12-16]。Bhushan 等[17]概括了区块链匿名化的必要性,Zaghloul 等[18]讨论了比特币的安全性和隐私保护,Andola 等[19]分析了基于区块链的电子现金的匿名性。本文将全面深入分析区块链隐私保护机制,尤其是对于设计匿名协议所需的密码结构细节进行了描述,还分析了不同区块链隐私保护方法的特点和局限性。此外,还提出了区块链隐私保护技术研究的未来发展趋势。

1 区块链技术架构

若干交易记录组成区块链的数据区块,区块按照时间顺序,借助区块哈希值产生一种链式数据结构,形成分布式数据库。按照功能特点,区块链 1.0 具有 5 层技术架构:网络层、数据层、共识层、应用层以及激励层。区块链 2.0 与区块链 3.0 增加了合约层。

区块链的数据层分布式存放着记录交易的区块。区块由区块头和区块体组成。其中,区块头存放父区块哈希、本区块默克尔根及区块生成的时间戳等。不同区块链的区块头也有所差别。例如,比特币的区块头还记录了区块链版本信息、当前区块链的难度值与随机数等。而以太坊的区块头还记录了布隆过滤器、叔块哈希以及手续费限制等。区块链的区块体记录交易内容,不同区块链的区块体的记录方式也有所差别。例如,比特币使用交易数据的哈希值构造默克尔树,而以太坊采用默克尔树与 MPT(Merkle Patricia Tree)相结合的方式存储交易内容。

区块链大体以链式结构为主,区块通过父块节点指针连接起来。近年来,也出现了以有向无环图(DAG)作为组织形式的区块链。

区块链有 2 种交易模型:UTXO 模型与账户模型。比特币与 Corda 等区块链采用 UTXO 模型,区块体记录交易金额的发起方与接受方。UTXO 模型的特点是支持快速追踪交易、验证交易,缺点是扩展性差。以太坊与 Hyperledger Fabric 等采用账户模型,区块体记录账户的状态,也就是交易结果。账户模型的特点是可扩展性强,适用于复杂业务逻辑场景。区块链数据存储主要有 2 种方式,一种是如比特币与 Hyperledger Fabric 将文本文件直接存储在区块链上,另一种是如以太坊将数据存储在数据库中。例如,索引和状态信息一般存储在键值型数据库如 Level DB 中,这样便于快速完成检索。

区块链的网络层功能是组网和传输有效数据。区

块链网络架构不是 C/S 或 B/S 中心化结构,而是 P2P 点对点对等网络。区块链的所有网络节点均对等地执行路由、传播、验证及引入新节点等操作,这样可以避免少部分节点出故障导致网络瘫痪和数据丢失。

区块链共识层主要解决分布式系统中的一致性问题。目前,主要有概率性证明类(如 PoW, PoS 等)和确定性拜占庭容错(Byzantine Fault Tolerance,BFT)类等 2 类区块链共识协议。其中,概率性证明类共识协议指某节点通过证明以一定概率赢得记账权。最经典的概率性证明类共识机制有工作量证明(PoW)和权益证明(PoS)。在 PoS 机制中,节点以币龄来计算其权益。概率性证明类共识协议常常应用在公链中。例如,以太坊采用"PoW + PoS"这种混合概率证明共识机制。

区块链激励层紧挨着共识层。引入激励层是为了实现区块链利益分配。激励机制让共识节点自觉地按照共识机制完成记账验证等任务,区块链系统才能够安全和可靠地运行下去。激励机制由发行机制和分配机制组成。激励机制常常依赖于共识机制。不同区块链的激励机制会有所差别。

区块链合约层主要功能是为区块链提供智能合约编写与执行环境。正是由于有了分布式账本之上的合约层,区块链才有高度可编程性,才有了极其丰富的应用场景。智能合约的实现方式主要有容器方式(如 Hyperledger Fabric)和虚拟机方式(如以太坊)。

区块链的应用层面向用户,通过调用合约层的智能合约实现各种场景下的区块链应用。比较典型的区块链应用方式如数字货币的轻钱包(客户端)。借助钱包,用户可以实现转账等交易,完成与区块链系统的各自交互。

2　区块链隐私及其威胁

为了实现达到去信任的分布式共识,常常需要进行公开区块链的交易数据,这无疑给交易参与方带来了严重的隐私泄露问题,如可能泄露不愿意被披露的敏感信息(用户财务状况,或者揭示区块链用户的真实身份)。在某些区块链应用场景,重要数据必须加以保护。例如,供应链金融的交易订单信息常常属于商业机密,不宜公开。

2.1　区块链隐私定义

区块链交易涉及发送方地址(账户)、交易金额和接受方地址(账户)等。若泄露交易接受方和发送方地址(账户)的身份隐私,则违反了区块链的匿名性。如果泄露了交易金额,则违反了区块链的机密性。区块链隐私保护的目的是既要保证区块链匿名性又要保障区块链的机密性。在对区块链进行保护的同时,必须保证区块链交易的正常验证与更新:如能够快速验证接受币的数量与发送币的数量相等;验证交易的确是从发起方转账,而不能从别的用户转账。交易过程中,钱不能凭空产生,也不能凭空消失。区块链数据隐私[12,19]包含身份隐私和交易隐私。由于区块链依赖于 P2P 网络,区块链隐私保护的内容还涉及用户(节点)IP 地址等的隐私性。

2.1.1　身份隐私

区块链身份隐私指交易参与者的现实身份信息和地址之间的对应关系。比特币地址由用户公钥的哈希值产生,但比特币系统并没有 CA 和 PKI 管理公钥,公钥由用户自己产生。因此,用户的地址与现实世界中用户的具体身份信息并没有对应关系。然而,比特币地址只能提供有限程度的匿名性。通过分析区块链上大量交易记录,攻击者可能揭示用户的身份信息或判断不同交易是否源于同一个用户。

2.1.2　交易隐私

区块链交易隐私是指区块链上的交易记录及其由此推断出来的信息。交易隐私分为交易内容隐私与账户地址隐私等[13]。其中,区块链上每笔交易参与方、交易金额等属于交易内容隐私信息,而区块链账户余额、交易数据以及不同地址间的交易关联等属于账户地址隐私信息。当交易记录是敏感信息,或者从交易记录可以推测出用户的敏感信息时,用户并不希望公开这些交易数据,如消费记录能够反映用户经济生活状况,金融系统和供应链系统中的交易数据属于企业商业机密。

2.2　区块链隐私威胁

区块链去中心化,采用 p2p 网络支持匿名交易,便于保护区块链数据隐私。例如,比特币系统中,各个参与方并不会使用现实世界中的真实身份,而使用公钥散列值作为输入或输出地址实现转账交易。用户的地址没有实名认证,因此,无法从用户地址发现其真实世界中的用户身份信息。由于交易者能够生成多个公钥,每笔交易的不同公私钥对都可以不相同,从而也无法将不同公钥对应的用户关联起来揭示用户的真实身份信息。因为一个用户的不同账号不存在直接关联性,所以无法计算该用户不同账号的总比特币余额。用户拥有多个公钥地址似乎增加了用户的身份隐私,但区块链存在着很多的隐私威胁,借助大数据分析手段可以获取交易隐私信息,泄露交易隐私。例如,比特币交易记录中常常存在找零或将比特币发送到多个自己新生账户的情况。找零地址是上一笔交易的输出地址和下一笔交易的输入地址。若能发现找零地址,便能将 2 笔交易中的输入地址相关联。Coinbase 地址也会暴露用户地址间的关

联性。例如,Coinbase 交易的多个输出地址属于同一个用户群,这是因为多个矿工加入同一矿池,挖矿成功后,各个矿工均会获得奖励。因此,比特币不能保证匿名性。

在比特币系统中,所有交易都是公开透明的,没有进行保护,上链即可以获取详细的交易内容。比特币的 UTXO 交易模式便于对交易进行追踪,实现交易的可溯源性,但这也带来隐私泄露风险。虽然比特币系统对同一用户使用多个假名使交易不可链接,但这并不意味着比特币可以提供完美的匿名性。在去匿名化推理攻击下,用户的交易仍然可以链接起来,甚至揭示出用户的真实身份信息[20]。可以使用统计方法挖掘交易地址和比特币交易流,将用户的当前交易链接到其他交易。一旦将用户的真实身份与比特币地址联系起来,则可能泄露该比特币地址相关的所有交易信息。

结合一些背景知识来分析交易数据常常可能获得交易者的身份信息或发现区块链交易之间的关联性,造成身份隐私、交易隐私泄漏。例如,根据用户在论坛、微博、TWITTER 和抖音等上发布的网络信息,利用深度学习等方法有可能从区块链上的交易数据找到与一个地址关联的一系列地址,揭示不同区块链地址之间的对应关系。攻击者通过追踪分析地址间的交易记录,结合线下用户信息,甚至可能揭示用户身份信息,把用户公钥与其真实身份关联起来,从而造成用户隐私泄露。例如,用户使用比特币网上购物时,网上商家可以获得用户的邮箱、收货地址,甚至得到用户的 IP 地址等。用户在比特币论坛等网站公开公钥等,也将带来身份隐私泄露问题。如结合区块链交易数据分析用户的收入情况、消费记录,可能推算用户的余额信息。Reid 等[21]使用聚类分析方法对2009年1月3日-2011年7月12日的所有比特币系统交易数据进行分析,构造了用户网络,发现了用户间资产的流动情况。此外,还发现存在多个输入最终汇聚到同一个地址的现象,这些交易一般都是同一用户发起的。

通过分析比特币系统中364笔大于50 000比特币交易,Ron 等[22]发现大额资金交易的模式主要分为自循环、储蓄账户长期交易链、分叉合并和二叉树等模式,大额资产常常发送到同一个交易方的不同账户中,很多都是“休眠”账户。通过分析215 399个区块数据,Ober 等[23]制作了用户比特币交易的拓扑结构图和交易关系图,揭示出比特币交易系统不同时期休眠比特币变化的数量关系,发现休眠比特币一般维持在60% 左右。

Möser 等[24]对基于环签名的数字货币门罗币进行分析,发现用户签名私钥泄露了交易发起方的隐私信息。2017年,Ermilov 等[25]利用自动聚类算法揭示了用户信息和比特币地址间的对应规则。

Meiklejohn 等[26]通过对用户地址使用聚类算法,分析出公钥与服务提供商类别的关联性,得到了用户地址关系结果,如图1所示。

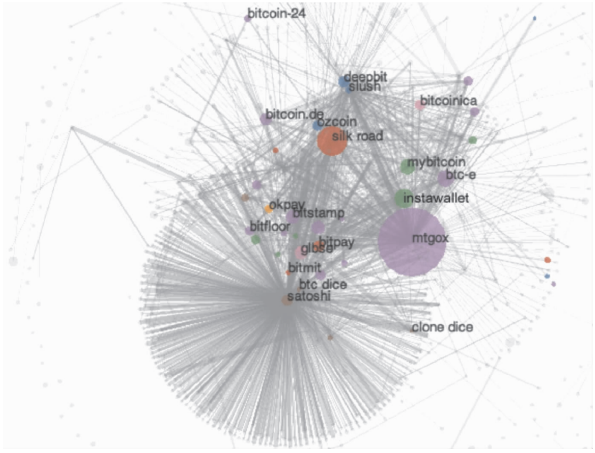

图1 用户可视化网络

Fig. 1 A visualization of user network

统计方法常常被用来分析区块链交易隐私。Fleder 等[27]运用信息流分析方法对用户的公开数据、交易特点、消费和查询特点以及交易记录等进行分析,揭示出用户的交易隐私。事实上,用户的交易特点可能泄露个人身份信息。Androulaki 等[28]的大学生比特币日常交易模拟实验证实了这一点。在实验中,每个交易用户都换用一个不同的公钥。但是,对交易行为采用聚类分析后,还是能够大概率地获得40% 比特币用户的身份信息。

区块链网络层存在隐私泄漏威胁,如恶意节点利用探针技术能够获得节点的 IP 地址,进而发现用户身份信息与节点之间的拓扑关系。如果区块链网络未采用加密的通讯协议,则通过分析区块链交易的 P2P 网络传输信息可以找出 IP 地址与比特币地址的对应关系,进而发现区块链地址对应的用户现实世界中的身份。Koshy 等[29]通过分析区块链交易中继转发模式,发现比特币地址与 IP 地址的映射关系。Puzis 等[30]的研究表明:通过监控通信信道就可能让用户失去匿名性。

区块链分布式账本结构特性更增加了数据隐私保护的难度,区块链应用面临比中心化系统更加严重的隐私问题。区块链网络中的节点更容易遭受女巫攻击。恶意节点假冒多个身份攻击系统,破坏区块链系统的匿名性,甚至泄漏用户现实世界中的身份[31]。

数据存储在各个区块链节点,但是各个节点的安全性能和隐私保护能力存在很大差异,攻击者很容易攻陷其中一些薄弱的节点造成整个区块链隐私泄露,攻击者可能伪装成合法节点直接获得区块链上存储的数据。

此外,区块链智能合约技术还属于刚刚发展的阶段,尚欠完善,远没有达到理论完备、高度智能化的程度,不能适应于大规模应用场景,智能合约也缺乏足够的透明性。区块链智能合约同样存在匿名、访问控制和链上信息等诸多隐私泄漏威胁。

3　现有区块链隐私保护技术与分析

近年来,人们对区块链隐私保护技术开展了深入广泛的研究。依照区块链交易模式,区块链隐私保护技术可以分为如下几类:一种是基于 UTXO 的区块链隐私保护技术,如 Mixcoin、Zcash 和 Monero 等;另一种是基于账户的区块链隐私保护技术,如 Zether[32] 和 AZTEC[33] 等。区块链基础架构的每一层如数据层、网络层、共识层、合约层和应用层等都有自身的隐私保护机制,如合约层的隐私保护技术有 Hawk 框架技术[34] 等,网络层的隐私保护技术有洋葱路由技术(Tor 网络)、大蒜路由技术(I2P 网络)和安全通道技术等。

本节将重点介绍区块链数据层、网络层与应用层相关的 3 种隐私保护技术:混币技术、基于密码学的技术和安全通道技术。其中,混币技术、盲签名、环签名[35] 和非交互零知识证明等属于身份隐私保护方法,零知识简洁非交互式知识论证(zk-SNARK)[36] 和保密交易(Confidential Transaction,CT)[37] 等属于交易隐私保护方法。这些技术常常结合在一起使用。因篇幅所限,其它隐私保护方法,如洋葱路由技术、限制发布等都将不作介绍[12-14]。

3.1　混币技术

由于交易记录存储在区块链上,攻击者直接对公开账本进行分析,能够确定交易发起方地址和接受方地址之间的对应关系,从而揭示用户的交易隐私,甚至发现用户的身份隐私。为了阻止这种攻击,常常把多个交易发起方的多笔交易混合成单笔多输入多输出的新交易,从而达到隐藏每个用户交易具体信息的目的。这种方法称为混币机制,其思想源自 Chaum[38] 于 1981 年发表的论文。混币机制隐藏了输入和输出账户与金额之间的逻辑关系,实现对交易规律的隐私保护。

依照混币执行者不同,混币方法可以分为中心化混币和去中心化混币 2 种。混币服务提供商协助用户完成混币操作,这是中心化混币方法。若混币操作由所有混币用户共同完成,而不是一个混币服务提供商单独完成,则称为去中心化混币方法。

3.1.1　中心化混币方法

在使用中心化混币方法时,混币服务提供商首先充当交易接受方完成与实际交易发起方的交易,随后对接收到的多笔资产进行随机混淆,最后将资产发送给实际交易接受方。所有参与混币服务的地址混在一起,打乱了交易地址关系,以达到难以分析单个用户资金真正流向的目的。中心化混币可以分为协商、输入和输出以及结束等几个阶段。在第一阶段,混币服务提供商和实际交易参与方关于发起方地址、接受方地址、中介地址、混币金额大小、操作时间和手续费等达成一致。在第二个阶段,交易实际发起方完成协商好的发起方地址与中介地址之间的交易。在第三个阶段,中心化混币服务提供商完成中介地址到交易实际接受方地址之间的交易,并扣除必要的手续费。在最后一个阶段,中心化混币服务商和交易参与方销毁所有的协商内容。这个方法借助中介完成,操作简单,技术难度不大,可以应用于比特币等。典型的中心化混币方法有:BitLaundry、Mixcoin、Blindcoin[39] 和 DASH 等。

目前,通过向用户收取混币费用提供混币服务的网站有:BitLaunder①、BitcoinFog② 和 Blockchain. info③。其中,BitLaundry 是第一个提供此种服务的平台。实际交易参与方把交易信息如交易发起方地址、交易接受方地址和金额以及交易时间提交给 BitLaundry 平台,完成与混币中介的交易。BitLaundry 在完成与多个交易发起方的交易后,汇总金额并完成与实际交易接受方的一对多交易,收取手续费。但是,BitLaundry 仍然存在隐私泄露问题。通过分析平台地址及其固定的手续费,攻击者可以把混币交易关联起来[40]。BitLaundry 方案也增加了用户费用,存在交易变慢的缺陷。交易费用占总金额的 1% ~3%,混币延迟交易常常达到 48 h。BitLaundry 方案还存在混币服务提供商盗窃资金和泄漏混币过程等风险。

为了克服 BitLaundry 方案的缺陷,Bonneau 等[41] 设计了 Mixcoin 方法。这种中心化混币方法具有审计功能。为了提高用户的匿名性,Mixcoin 要求各用户使用相同的金额进行混币。与 BitLaundry 方案不同,Mixcoin 中心化混币的第一阶段需要混币服务提供者产生关于

① http://app. bitlaundry. com

② http://bitcoinfog. com

③ https://blockchain. info/de/wallet/send-shared

协商内容的签名。交易参与者只有收到中心化混币服务提供商的这个承诺后才完成第二阶段的操作。若出现混币服务提供商违规操作的情况,交易参与方可以在系统中公开混币服务提供商的承诺,区块链节点通过验证签名来核实混币服务提供商的作弊行为,这样混币服务提供商将不能再提供混币服务。Mixcoin 协议对于手续费引入了随机化全有或全无(all-or-nothing)机制。混币服务提供参与商将一部分交易参与方的全部混币作为手续费,而全额返还其他交易参与方的混币。混币服务器对协商内容进行签名。对于交易参与方来说,该承诺机制提供了资产保护。然而,Mixcoin 还是存在服务提供商泄露用户隐私问题,无法提供内部隐私性。交易参与者似乎可以参与多个中心化混币平台来进行连续混币操作避免这一情况发生。事实上,这除了让用户付出更多的手续费外,也产生了更多的混币交易记录,存在更多的隐私泄露可能性。

为了降低上述中心化混币方法存在的内部隐私泄露风险, 2015 年,Valenta 等[42] 对 Mixcoin 进行了改进,提出了基于盲签名[43] 的 Blindcoin 协议。该协议仍然采用 MiXCoin 的审计机制,其主要改进在第一阶段。在公开账本中增加了混币服务提供商对于交易参与方地址的盲签名,形成时间戳认证标识。对盲签名进行去盲后,交易参与方得到混币服务提供商关于实际交易接受方地址的签名。这样服务商仅仅获得了用户的输入地址,接受方地址隐私获得了保护。在第三阶段,混币服务提供商使用实际的交易接受方地址,但是却不能将它与实际的交易发送方地址对应起来,避免了混币服务提供商获得每笔交易的双方地址信息。该机制增强了中心化混币方案的内部隐私性。然而,由于混合金额大小是不变的,混币服务提供商结合公共日志中的交易接受方地址信息还是可能分析出交易隐私。

2014 年,Duffield 等[44] 基于中心化混币方法设计了一种匿名数字货币——达世币(DASH)。所有打算参与混币操作的节点首先需要交纳 1 000 个达世币押金,成为具备混币操作权利的主节点。如果主节点在混币过程出现违规行为,则启动押金机制。在混币过程中,DASH 除了使用盲化技术外,还采用了链式混合方法。所谓链式混合方法,是交易发起方首先选择一个主节点环,其发起的交易将通过该环上的主节点逐个依次完成混币操作。第一个主节点是随机选择的,每步混币操作都进行盲化处理,减弱了地址间的关联性,降低了主节点作恶的风险。DASH 的一次混淆参与者人数必须多于 2 方。当混合链加长时,参与混淆的交易方会急剧增加,交易发起者和交易接受者的地址对应关系也减弱,混淆效果变好。恶意攻击者若要发现交易发起者和交易接受者的对应关系,则需要腐蚀混淆链上相当大比例的主节点。不过,中心化混币方法 DASH 仍然存在恶意主节点泄露用户隐私的风险。

综上所述,中心化混币是一种高效的区块链安全和用户隐私保护方法。但是,中心化混币方法中混币服务提供商的存在仍然可能带来区块链隐私泄露问题。

3.1.2 去中心化混币方法

针对中心化混币的缺陷,研究者提出了一系列去中心化混币协议。这种混币协议与中心化混币协议有所不同,其混币操作角色不再是单独的中心化混币服务器,而是多个混币参与方。这从根本上解决了中心化混币存在的信任问题和混币费用问题。去中心化混币可以分为协商、混淆和确认及结束 4 个阶段。在第一阶段,混币参与者关于混币输入和输出地址以及混币金额等达成一致。在第二阶段,混币参与者混淆输出地址。在第三阶段,混币参与者根据指定的输出地址执行混币交易。依据混币参与方人数不同,去中心化混币技术有多方混币与双方混币 2 种。

(1)多方混币技术

为了去除中心化混币服务提供商存在的潜在风险,混币过程由所有交易参与方自己完成。首先,所有交易参与者协商好等额混币的金额大小。接着,将多个交易整合为一个多对多的多签名交易。由于混币金额大小一样,其他人不能发现交易参与方地址之间的实际对应关系。典型的多方混币方案有:CoinJoin、CoinShuffle 和 CoinParty 等。

2013 年 8 月,Gmaxwall 在比特币论坛上提出 CoinJoin 协议[45]。CoinJoin 协议就是一种典型的多方混币方法,多个交易整合为一个多对多的交易。从交易记录无法找到原先的交易发起方地址和交易接受方地址的关联性,有效避免了攻击者获得具体的交易信息、追踪每笔输出资金的来源。CoinJoin 协议大体上分为协商、混淆和确认 3 个阶段。在第一阶段,混币参与方关于混币的输入地址、输出地址和混币金额大小等达成一致意见。在第二阶段,混币参与方将第一阶段协商好的全部交易发起者和接受者地址整合到一个交易中,其中混币大小相同。在第三阶段,混币参与方核实与自己相关联的接受方地址与总金额的正确性,当全体参与者确认后产生一个多重签名,全网广播该交易。CoinJoin 协议存在 3 个缺陷。首先,在协议的第一阶段,混币参与方知道该混币交易的所有接受方与发起方地址,通过合谋攻击等手段容易获得原本各自交易的发起方地址与接受方地址的对应关系。换句话说,CoinJoin 方法仍然存在

内部隐私泄露问题。即使每个参与者保持各自的独立性,其匿名程度也与参与者人数有关。其次,该协议遭受 DoS 攻击和女巫攻击。例如,在第三阶段,若部分混币参与者不参与多重签名,则混币操作会失败。恶意混币参与者也可能在第三阶段完成前就用掉自己参与混币的资产。此外,寻找参与混币参与方可能需要一个中心节点。这时候,CoinJoin 将面临着中心化混币类似的隐私泄漏威胁。

在 CoinJoin 方案的基础上,Ruffing 等[46]提出了一种新的去中心化混币方法 CoinShuffle。CoinShuffle 既能够像 CoinJoin 一样提供交易的外部隐私保护和用户的资金安全,还能够提供内部隐私保护。CoinShuffle 采用了 2 个关键技术:输出地址洗牌机制和多层加密方法。交易参与方用其他混币参与方的公钥对交易接受方地址加密。当依次对输出地址洗完牌后,广播输出地址表。CoinShuffle 使得交易参与方自己不依赖第三方就能够完成混币操作。任何一个混币参与方不能获得其他混币参与方相关的输入输出地址对应关系。其次,CoinShuffle 利用可审计的匿名群组消息传递协议 Dissent,对交易发起方和接受方地址的对应关系进行多层加密。多层加密方式解决了中心化混币服务中的内部地址可链接问题。但是,CoinShuffle 方案存在 2 个比较明显的缺陷:①在协议的第二个混淆阶段,所有参与者必须同时在线,而且计算成本较高,所花费的时间也较长。因此,CoinShuffle 存在 DoS 攻击风险;②在 CoinShuffle 中,一般都存在交易发起方地址个数为交易接受方地址个数的一半、50% 的输出金额相同的规律。根据这个规律,攻击者很容易就能够识别这些交易是否使用了 CoinShuffle 协议,并进一步发现与另一半找零地址对应的交易发起方地址。总之,CoinShuffle 协议构造的交易匿名性较低,具有可否认性。

2015 年,为了解决 CoinShuffle 协议混淆阶段存在的 DoS 攻击问题,Ziegeldorf 等[47]提出一个新的去中心化混币协议 CoinParty。该协议采用了基于安全多方计算技术,使用了阈值 ECDSA 签名,是一种基于混合网络的分布式混币技术。CoinParty 协议能够同时保证内部隐私性和外部隐私性。该协议包含协商阶段、混淆阶段和确认阶段 3 个阶段。在第一阶段,参与者一起执行伪随机秘密分享协议,生成临时托管地址,并将各自混币金额放入各自的临时托管地址,最后对这些承诺进行多重签名,形成一个全体参与者拥有的抵押。任何一个参与者都不能单独从该抵押中抽取自己的抵押资产。这种模式增加了攻击者在第二阶段发动 DoS 攻击的成本。CoinParty 的第二阶段与 CoinShuffle 协议的第二阶段相类似:均使用了多层加密模式。因此,CoinParty 也提供了交易的内部隐私性。相比 CoinShuffle 协议的第二阶段,CoinParty 协议的第二阶段也有不同:混淆结果的校验通过对比秘密分享的校验和与所有输出地址哈希值的和来完成。在第三阶段,所有参与方将各自存放在临时托管地址的资产发送到最终混淆结果中规定的各自输出地址。容易知道,当恶意攻击者人数没有达到总参与人数的 1/3 时,CoinParty 协议能够保证区块链的安全性。若 2/3 以上的恶意参与方发动合谋攻击,则其他参与者的资产将能够被盗走。此外,如果没有对参与方进行身份认证, CoinParty 协议将存在女巫攻击风险。因此,CoinParty 协议存在一定程度上的资产安全问题。

多方混币方案要求混币参与者必须在 3 个以上。当混币参与者增加时,交易发起方和交易接受方的直接对应关系变弱,外部用户获知交易双方关系的概率降低,方案能提供更强的外部隐私保护。混币参与方的增加还会减少各参与方交易费。然而,混币参与者越多,混入恶意参与者的可能性也越大。如果恶意参与者在混币过程中不遵守协议如广播错误消息甚至中途退出,则不能成功执行混币构造。恶意攻击者还可能监听分析出其他参与者发布的交易发起方地址与交易接受方地址的对应关系,造成内部隐私泄漏。

(2)双方混币技术

由上可知,参与者人数增加,也会带来一系列隐私泄露问题。如果将混币参与者限制为 2 人,则可以大大减少混入恶意参与者的可能性。这种混币协议称为双方混币。双方混币技术把多个混币参与者的一次混币交易构造改造为多轮混币,每轮混币由 2 个参与者执行。典型的双方混币方案有 CoinSwap[48]和 Xim[49]等。

2013 年, Maxwell[48] 在 Bitcointalk 论坛提出 CoinSwap 协议。CoinSwap 协议依赖第三方完成混币交易,打乱交易发起方与接受方地址之间的对应关系。假设用户 A 需要向用户 B 支付一个比特币,则由用户 A 向用户 C 发起交易,支付给中间人 C 一个比特币,然后由用户 C 向用户 B 发起交易,扣除费用后支付给 B。这样 A 与 B 用户的钱包地址没有直接关联起来。实质上,用户 A 和用户 B 可由同一用户扮演。该协议使用哈希时间锁定合约(Hashed timelock contract,简称 HTLC)防止中间人不把金额支付给 B 或者自己留下一部分金额。时间锁用于在发生异常的情况下,如其他用户离线,发起方一定时间后能够取回自己的资产。在 CoinSwap 协议中,参与方采用哈希 - 时间 - 签名锁定合约技术可以直接完成混币操作,不需要可信第三方参与混币。这减少了恶意参与者存在的可能性,增加了协议参与者的资

产安全,在一定程度上解决了攻击者监听和 DoS 攻击的问题。

在 CoinSwap 协议中,多次双方混币交易增加了交易手续费和交易时间,几次解锁增加了时间成本。CoinSwap 协议仍然有隐私泄露风险,如中间人知道 A 和 B 进行了交易,可以建立它们之间的联系。CoinSwap 协议也遭受女巫攻击,如多个恶意用户参与混币过程将破坏用户的隐私安全。

2014 年,为了降低恶意参与者参与混币的概率,Bissias 等[49]提出一个新的去中心化混币协议 Xim。在第一阶段,用户付费发布广告,愿意参与混币的用户付费回应广告。发布广告的用户从中随机挑选出参与混币的用户。正是由于这种广告匿名寻找混币同伴的机制,让 Xim 协议降低了女巫攻击的概率。攻击者要想成为混币参与者,必须付费回应广告。当混币用户增加时,恶意参与混币的攻击者付出的代价也会线性增加。在混淆阶段, FairExchange 协议[50]的使用增加了 Xim 方案抵抗 DoS 攻击的能力。若所有参与者都参与混币,则外部攻击者获知混币交易隐私的概率将大大降低。

双方混币方案中,虽然交易的外部隐私性获得了保护,但内部隐私存在很大的泄露风险。这是因为每轮混币仅有 2 个混币参与方。为了去除这个缺陷,用户将与不同参与方完成多轮的双方混币操作,以保证方案获得隐私保护。双方混币技术可以增强交易的隐私性,并且每轮混币操作都十分简单。但是,双方混币技术也存在不足,如多次混币构造意味着多次交易,这将大大增加交易成本。

综上所述,混币技术提供了用户交易的匿名,增强了用户资金安全。基于区块链的“数字货币”广泛应用了该技术。现有的混币协议主要依靠去信任的第三方平台对多个用户的交易集进行混合后输出到相应的地址,达到攻击者无法将交易的真正输入与输出地址链接起来的目的。然而,随着大数据分析算法的不断发展,攻击者仍然可能将交易地址进行关联。现有混币协议还存在一些其它弱点,如寻找诚实混币用户困难、难以阻止攻击者参与混币从而监听混币或发动 DOS 攻击。为了提高寻找混币同伴的效率,可以依赖第三方。但这种混币机制可能遭受中心化威胁,不可信第三方平台使得混币协议泄露交易信息或遭受 DoS 攻击。

3.2 基于密码学的技术

对于比特币区块链,交易数据以明文存储在链上。链上任何节点都可以下载这个区块链数据,参与交易验证和记账。这是区块链带来信任价值的关键。加密技术是隐私保护领域常用的解决方案之一。对敏感数据进行加密,只有持有相应私钥的用户才能查看数据内容,这样可以保证数据机密性。为了保护区块链隐私,需要加密交易信息,如交易来源、去向和交易内容。但是,区块链采用加密技术保护数据隐私,必须保证节点可以对加密数据进行验证并达成共识。

区块链隐私保护中常用的高级密码技术有:盲签名、群签名和可追踪的环签名等签名技术、zk-SNARKs[51]、zk-STARKs[52]和 Bulletproofs[53]等非交互式零知识证明技术、Pedersen 承诺[54]等同态加密技术。以密码技术构建的匿名“数字货币”系统非常多,如 Cryptonote、Monero、Zcoin 和 Zcash 等。其中,Zcoin 和 Zcash 需要进行可信初始化,而 Cryptonote 与 Monero 无需可信初始化。Mimblewimble 同时使用了多个密码技术和混币技术。

下面,对几种典型的基于加密技术区块链案例进行分析。

3.2.1 环签名与 Pedersen 承诺方案

2001 年,Rivest 等[35]提出环签名的概念。与群签名不同的是,环签名方案不需要管理员。若用户需要产生一个消息的环签名,则用户首先选择环签名成员。然后,用户使用私钥和环成员公钥签名。任何人都能够从签名中识别出所有环成员,并验证签名的有效性。虽然验证者能够证实该签名是其中一名参与者产生的,但是无法确定该签名的完成者。因此,环签名能够保证签名者的匿名隐私。

2013 年,Saberhagen 等[55]基于一次性可链接环签名和匿名地址技术设计了 CryptoNote 协议。CryptoNote 协议中,交易发起者选择若干个输出金额相等的交易,产生交易发起方作为环成员的环签名。该整合后的交易合法性可以通过环签名得到证实,但实际的交易发起人无法被识别出来。从零知识证明角度看,环签名相当于成员证明(membership proof)。为了能够防止恶意参与者通过签名陷害其他环成员,Rivest 等[35]引入了可链接环签名概念。可链接的环签名可以保护诚实的签名方。如果环签名被确定是由恶意参与方产生,则可以确定环签名的实际产生者,避免了其他无辜环成员被牵连,对他们提供了保护。区块链使用一次性可链接环签名能够有效抵御双花攻击。

为了满足交易的不可链接性,同一个交易发起方不同资产的不同输出地址可能对应同一个交易接受方。在传统区块链系统中,每次生成新地址时,接受方必须将新地址从私密通道传递给发送方。为了避免这个情况发生,CryptoNote 采用了一种称之为匿名地址的技术。匿名地址由匿名公钥加密产生。匿名地址产生后,交易接受者无需与交易发起方建立链下私密通道并把匿名

地址发送给交易发起方。匿名地址放在分布式账本上,只有指定的交易发起方可以从账本上解密对应的密文获得交易接受方的地址,其他交易方都无法解密发给未指定自己作为交易发起方的密文地址,也无法确定该密文的指定交易发起人是谁。其实现的具体技术方法如下:交易发起方通过交易接受方的长期公钥计算出一个临时公钥。只有该临时公钥指定的交易接收者能够由此计算出对应的临时私钥,任何其他参与者既不能计算出临时私钥,也不能找出该临时公钥指定的交易接受方是谁。匿名地址技术保证了交易接受方的匿名性。因此,CryptoNote 协议实现了交易的不可追踪性和不可链接性。但是,如果 CryptoNote 协议中其他所有环用户公开自己的资产使用情况,则攻击者能够分析出用户地址之间的关联性,导致隐私泄漏。

为了保护密码货币的隐私性,Maxwell[37] 提出保密交易(Confidential Transaction,CT)技术。CT 的核心思想是交易输出以 Pedersen 承诺[54] 这种非明文方式表示,然后通过 Pedersen 承诺的加法同态性质验证交易输入和与输出和是否一致。具体来说,在 Pedersen 承诺方案中,要承诺的数 v 和一个随机数 r 一起写成 $C = rG + vH$ 的形式,其中,G 和 H 分别是椭圆曲线群的 2 个生成元。容易知道,Pedersen 承诺具有加法同态性。分别把(v_1,r_1) 和(v_2,r_2)对应的 2 个承诺值按照椭圆曲线群的加法相加,得到的和是($v_1 + v_2$,$r_1 + r_2$)对应的承诺值。在整个过程中,不需要知道 v_1 与 v_2 的值。CT 方案使用上述方法将未花费交易输出 UTXO 转换为一个 Pedersen 承诺值。用户不能对加密承诺的余额值进行修改。在交易过程中,保密交易的接受者需要获得交易的具体金额值。承诺方案由承诺和显示 2 个阶段构成。在区块链中,为了避免出现金额为负数或者溢出的问题,范围证明(range proof)被引入到保密交易中。范围证明是一类知识证明密码技术,证明某个金额属于某个范围,但又不透露这个金额具体是什么。区块链采用保密交易技术将交易金额隐藏起来,提供了交易金额隐私。但是,运用该方法将耗费大量计算与存储资源。

2016 年,Noether 等[56] 结合环签名和保密交易技术提出了环保密交易(Ring Confidential Transaction,RingCT)。RingCT 的关键技术是多层可链接自发匿名群签名(Multilayered Linkable Spontaneous Anonymous Group Signature, MLSAGS)。MLSAGS 也使用了 Pedersen 承诺。RingCT 方案还利用了范围证明这种特殊的零知识证明技术。环签名和一次性密钥技术保证了 RingCT 交易发起方和接收方地址的隐私性。RingCT 还解决了 CryptoNote 协议存在的交易金额隐私性问题。

2014 年,一个匿名的数字加密货币门罗币(Monero)被推出[57]。Monero[57] 使用了 CryptoNote 和 MLSAGS 以及加法同态加密技术。交易发送方利用 Keccak 散列算法计算交易接受方公钥与随机数的哈希值。哈希值作为接受方的一次性公钥地址。该地址的形成使用了随机数,除了交易发起方,其他用户无法将该地址信息与接受方关联起来。随机数的使用也使得该地址不是静态地址,而是动态地址。同一个接受者在不同交易中的地址都会发生变化,从不同地址无法确定它是否属于同一个交易接收方,从而保证了交易接受方的匿名性。当发送方给接受方发送一笔金额时,发送方用自己的私钥对交易信息签名,交易信息包含随机选取的若干其他用户的公钥。发送方把一次性公钥和附加信息广播到区块链上。当接受方要花费这笔交易金额时,先要计算出一次性公钥相对应的私钥,使用该私钥产生交易的签名。这种隐蔽地址方式实现了接受方地址的外部不可见性。同时,环签名方案保护了发送方隐私,RingCT 隐藏了用户的交易信息如交易金额等。由于利用环签名机制实现混币过程,发起方不需要和其他用户进行交流,门罗币在一定程度上也解决了去中心化混币方案面临的 DoS 攻击和内部隐私性等问题。Monero 保障了交易发起方与接收方的匿名性,同时也保证了交易金额的隐私性。然而,同 CryptoNote 协议一样,当 Monero 中交易发起方选择的匿名集存在恶意用户时,一次性地址与接受方的对应关系可能被揭示出来。Monero 的匿名集合不会很大,攻击者结合交易信息很容易就能够将交易信息与用户身份关联起来。此外,Monero 方案中的交易签名都非常大,需要使用一个参数让交易接收方完成归属验证,这大大降低了方案的执行效率。

2016 年 8 月 1 日,Jedusor[58] 在 #bitcoin-wizards 聊天室频道中提出一个新区块链系统 Mimblewimble。后来,Poelstra[59] 证明了 Mimblewimble 的安全性。Mimblewimble 采用了保密交易 CT、Coin Join 和 Cut-through 等关键技术。其交易输出跟比特币交易输出有所不同。比特币的输出 UTXO 列表的每一项由一个地址和明文形式的金额组成,而 Mimblewimble 的输出由输出金额的 Pedersen 承诺和输出金额的范围证明组成。其中,Pedersen 承诺的随机数部分即盲化因子是交易签名的私有信息。最初的范围证明使用了环签名技术,证明所需的存储空间非常大。如证明范围是$(0,2^{64})$,则大约要 5 kB 左右的存储空间。后来,范围证明使用了 Bulletproof 零知识证明技术[53],则所需存储空间变得小于 1 kB。

在 Mimblewimble 中,每笔交易的输入地址、输出地址和金额用 Pedersen 承诺表示出来,保证了交易金额的

隐私性。这时,需要从以下几个方面来验证交易的合法性:交易的输入与输出金额是相同的,且交易得到了交易双方的授权。若输入是 $C_1 = r_1G + v_1H$ 和 $C_2 = r_2G + v_2H$,输出为 $C_3 = r_3G + v_3H$ 和 $C_4 = r_4G + v_4H$,f 是交易费,则当 $(C_1 + C_2) - (C_3 + C_4 + fH) = kG$,根据 Pedersen 承诺的加法同态性质得知验证通过。当且仅当 $v_1 + v_2 = v_3 + v_4 + f$ 成立时,点 H 的相关项加减后抵消,只剩下点 G 的相关项。右边项 kG 视为公钥,通过这个 excess value 获得交易方授权。交易合法性是通过交易手续费 f、excess value 和私钥 k 的签名来验证的,这 3 部分称之为交易的 kernel。显然,k 是 r_1、r_2、r_3 和 r_4 的一个线性组合,需要发送方和接受方合作产生以 k 为私钥的多重签名。因此,签名的有效性证实了交易得到双方的授权。由于采用 Pedersen 承诺作为输出值,交易合法性还需验证每个输出附带的范围证明是否保证输出金额是正值且在规定的范围以内。

Mimblewimble 也运用了类似比特币的 Coin Join 混币技术,将若干交易整合为一个大交易,形成区块。利用同态加密,可以验证这个构造的交易金额是否平衡。由于矿工并不对这笔交易进行签名,故其包含的全部原交易的 kernel 应该一同记录下来。

Mimblewimble 还把整个区块链历史上所有的区块放在一起进行一次裁剪操作 Cut-through。Cut-through 操作如下:从交易历史中删掉所有已经花掉的输出连同它们对应的范围证明。但是,需要保留从 Coinbase 到 UTXO 的交易,同时还要保留所有历史交易的 kernel,这些 kernel 可以用来验证上述保留交易的合法性。Cut-through 操作删除了整个区块链的历史数据,大大缩小了区块链的存储空间,系统扩容好。

跟 Monero 和比特币相比,Mimblewimble 将一个区块内的全部交易整合为一个区块级的交易,这样可将区块视为一个整体进行验证。Mimblewimble 提供了更高的可替代性和可扩展性。与 Zcash 相比,Mimblewimble 或 Monero 的安全性依赖于离散对数问题难假设与哈希抗碰撞假设,这跟比特币依赖的密码学原语同样简单。因此,Mimblewimble 比较适用于简单支付场景,是一种轻量级区块链。

Mimblewimble 也存在一些缺陷。比如,由于 Mimblewimble 没有地址的概念,发送方和接受者必须在将一笔交易发送到网络之前进行通信,并完成交易的签名。这与其他基于地址的区块链系统有很大不同。比如,比特币区块链中,每笔交易的接受方不必在线,双方也不需要隐私信道。其次,仅当交易方能够找到同时进行的交易,Mimblewimble 才能完成保密交易,实现交易金额的模糊化处理。而 Monero 和 Zcash 并不需要存在同时发生的相关交易。因此,Mimblewimble 的隐私保护性能并不比 Monero 和 Zcash 强。

3.2.2 非交互式零知识证明

在 20 世纪 80 年代,Goldwasser 等[60]提出零知识证明。借助零知识证明,证明者能够在不向验证者泄露任何额外信息的条件下提供论断的正确性证明,这是一种较强的隐私保护协议。零知识证明可以分为交互式零知识证明和非交互式零知识证明 2 类。在非交互式零知识证明协议中,证明者不需要与验证者进行交互。典型的基于零知识的区块链隐私保护方案有:零币(Zerocoin)、零钞(Zerocash)与 Aurora。

2013 年,Miers 等[61]基于零知识证明提出了比特币扩展协议,即 Zerocoin 或 Zcoin 协议,俗称“小零币”。Zerocoin 隐藏了交易输入地址与输出地址,在某种程度上可以抵抗区块链数据所面临的账本分析攻击。对货币的序列号产生 Pedersen 承诺,而用户对该资产的所有权关联到承诺方案中的随机数,以避免双花攻击。Zerocoin 的具体铸币过程如下:首先生成一个随机序列号 S 代表 Zerocoin,使用散列算法产生接受方公钥与随机数的承诺 C,并将承诺 C 广播至区块链上的铸币公告栏,用户自己操作混币过程。为了赎回 Zerocoin,用户通过零知识证明向矿工提供一个证明 π,证明自己的序列号是真实且没有 Zerocoin 被花费的,即表明自己在所有用户累加器资产集合中有一笔未曾花费的资产。用户将币的序列号 S 发布到注销币公告栏上。矿工验证 π,检查序列号 S 是否没有被使用过,完成兑换 Zerocoin 过程。

在 Zerocoin 中,聚合器(Accumulator)的使用也增强了货币的匿名性。聚合器将对所有货币的承诺压缩为一个群元素。用户需要证明他知道货币对应的随机数以表明其为该货币的所有人,还需要证明该货币的承诺是聚合器中的一个元素。聚合器提供“或证明”(Or proof),可视为一种零知识证明。因此,Zerocoin 解决了用户交易地址泄露问题。在 Zerocoin 协议中,除了交易方,任何其他人不能获得交易信息,不能关联用户的铸币地址和花费地址,但是可以验证货币是否属于该累加器和是否属于双花,即任何人都可以验证交易的合法性。因此,Zerocoin 能够提供交易的不可链接性。但是,Zerocoin 也存在一些缺陷:①Zerocoin 采用的零知识证明数据相对较大,所需存储空间及计算成本等都较高。这将使得区块链系统整体性能下降、账本容量变小;②Zerocoin 需要可信第三方来生成初始全局参数;③Zerocoin

金额不可分,铸造和兑换货币时只能使用固定大小的面值,从而无法隐藏交易金额大小,不能满足实际需求。最后,由于 Zerocoin 并未有提供交易金额的区间证明,Zerocoin 存在凭空造币隐患。

2014 年,Sasson 等[36]基于简洁非交互性零知识证明(zk-SNARK)提出一个比特币支付方案,简称零钞(Zerocash),俗称“大零币”。Zerocash 交易发起者将不同面值的币铸造成多个等值币,每个币有自己的序列号。铸币过程实质上是承诺生成过程。该承诺封装了交易来源、去向和金额。交易发起者用接受方的公钥对交易信息(交易金额、接受方地址)加密,将承诺添加到全网承诺列表。接受方用私钥检测到交易信息后,生成新币的序列号。矿工验证交易发起者的 zk-SNARK 证明的正确性,核实承诺是否在列表中、序列号是否在注销币序列中。验证过程不会泄露交易发送方、收款方与交易金额等信息,矿工也无法获取哪个承诺被使用过,从而保证了用户的匿名性。由于每一个币都有唯一的一次性序列号表示,可以有效避免双花。同 Zerocoin 一样,Zerocash 分为铸币交易和私密资产花费交易 2 个部分。从花费交易记录,外部用户不能发现其资产来源。Zerocash 协议与 Zerocoin 也有 3 个不同之处:①Zerocoin 的花费交易是公开资产,而 Zerocash 的花费交易资产仍然是私密资产;②Zerocoin 有固定大小的币值,而 Zerocash 比值大小不固定;③Zerocoin 公开交易金额,而 Zerocash 隐藏交易金额,提供了更强的用户隐私保护。Zerocash 是目前为止区块链 UTXO 模型中隐私性最强的数字货币。

Zerocash 保证了交易的匿名性,交易隐私性强。但是,其运算成本非常高,效率不高。如 zk-SNARK 证明生成过程非常缓慢,通常需要 1 min 才能完成。又如,初始化公共参数和私密参数是由可信第三方完成的,协议存在运行瓶颈和安全隐患。

2016 年 1 月 20 日,Zcash 项目作为 Zerocash 的应用①正式由首席执行官 Zooko Wilkox 宣布。Zcash 将 Sander 等[62]提出的审计匿名电子现金技术运用到区块链里,增加了系统的可审核性(auditability)和可追踪性(traceability),可以看作是 Zcoin 的改进版。与 Zerocash 不同,Zcash 通过多方计算分布式初始化参数。Zcash 的地址分为透明资金地址 taddr 和私有资金地址 zaddr。透明资金地址与比特币地址相似。当 Zcash 交易涉及到私有资金时,采用零知识证明 zk-SNARK 生成证明,同时将交易发起方、接受方和交易金额隐藏起来。Zcash 交易的可审计性由参与者控制。其中,私有资金的交易是保密不可查的。虽然 Zcash 可以对交易和地址进行隐私保护,但是,由于 Zcash 总量被隐藏了,是否有漏洞被利用或者在其信任机制中是否存在问题难检测。相比于 Zerocash,Zcash 方案的计算成本更高。例如,Zcash 使用零知识证明技术来验证哈希计算的正确性,使用 Merkle tree 的承诺 membership proof 验证货币合法性。当货币发行加大时,Merkle tree 规模加大,电路变大。

随着量子计算理论的快速发展,为了让区块链能够更好地抵御量子计算的破解技术,Ben-Sasson 等[52]构建了量子安全的高效零知识、可扩展和透明的知识论证(zero-knowledge scalable transparent argument of knowledge,zk-STARK)方案,将计算完整性(computational integrity)归约为 Reed-Solomon 编码问题,计算电路(arithmetic circuit)使用类似快速傅立叶变换方式减少了验证复杂度。zk-STARK 具有 4 个优势:①使用零知识证明保护数据隐私;非交互方式减少了参与双方的通信复杂度;②无第三可信方的存在增强了系统透明性;③交易者的时间复杂度相对较低,系统可扩展强;④zk-STARK 没有使用公私钥对映射,仅依赖 hash 抗碰撞性和随机谕示模型,能够抵御量子攻击。这些特性使得 zk-STARK 非常适合那些需要互信同时又存在很多欺诈动机的应用场景,例如,区块链出块验证、安全信息验证和投票系统等。

2019 年,Ben-Sasson 等[63]在此基础上构造了 Aurora 方案,不需要可信第三方来初始化全局参数。Aurora 方案把对计算结果的验证问题转化为多项式相等验证。zk-STARK 采用“快速里德—所罗门码接近性交互预言证明”(fast reed—Solomon interactive oracle proof of proximity)实现多项式的简洁验证,以抵御高阶多项式伪造攻击。由于 Aurora 方案的参数初始化不再需要可信第三方,协议具有很好的扩展性,验证效率也提高了。但是,Aurora 方案中的证明生成过程仍需要较大的存储空间。

3.3　安全通道技术

通道隔离机制从网络层完成数据隔离。节点仅能存储和访问自己所在通道的数据,避免了数据的非法访问,对账本进行隔离,提供了用户隐私保护。通道隔离机制可以分为链下通道隔离和多链通道隔离 2 类。使用链下通道隔离机制首先在区块链上记录起始状态,完

① https://z.cash/

成通道的创建,在链下执行交易。中止交易时,仅将最新的结束状态公布到区块链上而不记录中间结果。链下通道隔离技术适用于高频小额交易,其又可细分为比特币闪电网络与以太坊雷电网络等技术。

比特币闪电网络技术是 Poon 等[64]于 2016 年提出的。通过闪光网络交易合约之 RSMC 序列到期可撤销合约(revocable sequence maturity contract)建立双方安全支付通道,通过哈希时间锁合约 HTLC 进一步建立支付网络,保障双方可以通过中间人完成交易。HTLC 的运用减少了 RSMC 的数量,扩展了闪电网络的适用性,也提高了用户的支付效率。因为交易信息并不会直接出现在区块链账本上,所以不会发生账本分析攻击,这将较好地保护用户隐私。但是闪电网络也存在一些缺陷,如仅限于比特币的小额支付等。

以太坊采用雷电网络技术来构建链下支付通道[65]。因此,雷电网络是基于账户余额状态模型的"状态通道技术"。不同于闪电网络,雷电网络基于以太坊的智能合约机制,对序列到期可撤销合约 RSMC 和哈希时间锁定合约 HTLC 的执行方式进行了简化。雷电网络支持双方支付通道和多方支付网络的构建,但是,雷电网络存在离线问题和路径查找问题。

多链通道隔离机制在多个节点之间通过他们自己的一个账本和一个通道建立一条链,从而达到节点通信隔离、保护隐私信息的目的。一个通道维护一个账本,同一区块链系统将存在多个区块链账本。一个节点可以加入多个通道,维护多套账本。通道内的节点才能访问属于自己通道的区块链,不同通道之间不进行通信,这种访问控制机制保证了区块链的数据隐私安全。HyperLedger Fabric 项目①就采用了这种多链通道技术。

2016 年,Heilman 等[66]提出一种依赖可信第三方的链下匿名支付方案,后来将该方案改进为匿名支付通道方案 TumbleBit[67]。交易参与方在链下交易通道利用不受信任的中介实现快速匿名的链下支付。Tumbler 基于 RSA 和 ECDSA 密码学技术验证交易真实性,但是它不能得到用户的交易信息,用户交易具有不可链接性,从而保障了用户隐私。

为了增强链下安全通道交易的隐私性,Green 等[68]提出了新的匿名支付通道技术 Blot。Blot 可以构建单向支付通道、双向支付通道和第三方支付通道。用户使用盲签名及零知识证明技术借助不可信第三方完成交易。在整个交易执行过程中,第三方不会获得用户交易信息,保证了用户的隐私性。

安全通道技术也存在一定的缺陷,如创建通道的代价高,节点创建和进出通道时都要进行网络配置,导致系统灵活性不强,还有当出现交易错误时,需要公开验证用户的交易信息,并不能真正实现不泄露用户隐私的情况下交易的公平性。

4 结束语

本文从区块链技术的发展现状和基本技术架构出发,探索了区块链隐私保护机制。重点阐述了区块链面临的数据隐私威胁,分析了区块链数据层与应用层的身份隐私与交易隐私,对区块链隐私保护技术进行了全面的分析与总结。

目前,人们对区块链巨大应用价值的认识已经达成一致。然而,区块链技术仍然处于发展的初期阶段,区块链还存在着数据存储瓶颈、拓展性不强和功能不全等问题。区块链的公开透明特性严重影响用户的隐私安全。至今为止,虽然已经存在很多区块链隐私保护方案,但是,现有方案都存在一些不足。为此,本文提出几个未来区块链隐私保护技术研究可能的方向。

区块链隐私保护主要采用了哈希函数、数字签名、同态加密和零知识证明等密码技术。需要进一步研究基于加密技术的混币协议的安全性和匿名性。随机选择一定数量的用户对交易进行环签名,将真实交易隐藏在一个匿名集中。需要进一步研究区块链匿名技术存在的隐私保护强度不够的问题。Zcash 方案中,全局初始化参数没有依赖可信第三方生成,而是由 6 个人生成。任何一方都能够随意生成货币。因此,这种初始化参数方法存在安全缺陷:初始化参数集可信度不高。为了克服这个不足,可以利用多方密码共享等 MPC 技术。零知识证明在区块链隐私保护中起到重要作用,如验证计算、身份认证和数据存储以及共识机制等确保身份隐私。但是,现有零知识证明方法存在计算资源消耗大、占用内存较大、时间长等特点,影响了系统运行效率,导致交易吞吐量变小。SNARK 是一类密码证明系统,它使证明者能够通过简短证明和简洁验证向验证者证明数学陈述,而递归 SNARK(Recursive SNARKS)能够产生关于先前证明的陈述证明[69-70]。进一步开展递归 SNARK 等区块链密码技术研究,改善区块链性能,保持

① https://www.hyperledger.org/

区块链大小固定,满足不同隐私保护需求。

参考文献:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2008-10-31)[2009-12-10]. https://bitcoin.org/bitcoin.pdf.

[2] 王继业,高灵超,董爱强,等. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展,2017,54(4):742-749.

[3] Gartner. Top 10 strategic technology trends for 2017[EB/OL]. (2017-03-21)[2020-06-10]. http:// www. gartner. com/technology/ topics/trends. jsp.

[4] Adelstein J, Stucky N. Behind the biggest bitcoin heist in history: Inside the implosion of mt gox[EB/OL]. (2016-05-19)[2020-05-19]. https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.

[5] Vitalik B. Critical update re:Dao vulnerability[EB/OL]. (2016-06-17)[2020-01-12]. https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

[6] Au M H, Liu J K, Fang J, et al. A new payment system for enhancing location privacy of electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2014,63(1):3-18.

[7] Bayardo R J, Agrawal R. Data privacy through optimal k-anonymization[C]//Proceedings of the 21st International Conference on Data Engineering. Piscataway:IEEE, 2005:12.

[8] Gentry C. Fully homomorphic encryption using ideal lattices[C]// STOC'09. New York: ACM, 2009:169-178.

[9] Dwork C. Differential privacy: A survey of results[C]//International Conference on Theory and Applications of Models of Computation. Berlin, Heidelberg: Springer, 2008:1-19.

[10] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[11] Zheng Z, Xie S, Dai H, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[12] 祝烈煌,高峰,沈蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展,2017,54(10):2170-2186.

[13] 张奥, 白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020,31(5):1406-1434.

[14] 王宗慧, 张胜利, 金石,等. 区块链数据隐私保护研究[J]. 物联网学报, 2018,2(3):71-81.

[15] Khan N, Nassar M. A look into privacy-preserving blockchains[C]//2019 IEEE/ACS 16th International Conference on Computer Systems and Applications. Piscataway:IEEE, 2019: 1-6.

[16] Feng Q, He D, Zeadally S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[17] Bhushan B, Sinha P, Sagayam M, et al. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions[J]. Computers and Electrical Engineering, 2021, 90(9):1-13.

[18] Zaghloul E, Li T, Mutka M, et al. Bitcoin and blockchain: Security and privacy[J]. IEEE Internet of Things Journal, 2020,7(10): 10288-10313.

[19] Andola N, Raghav, Yadav V, et al. Anonymity on blockchain based e-cash protocols—a survey[J]. Computer Science Review, 2021, 40(2):1-18.

[20] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and cryptocurrency technologies: A comprehensive introduction[M]. New Jersey: Princeton University Press, 2016.

[21] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system[C]//2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. Piscataway: IEEE, 2011:1318-1326.

[22] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph[C]//17th International Conference on Financial Cryptography and Data Security. Heidelberg: Springer, 2013: 6-24.

[23] Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the bitcoin transaction graph[J]. Future Internet, 2013, 5(2): 237-250.

[24] Möser M, Soska K, Heihnan E, et al. An empirical analysis of traceability in the Monero blockchain[J]. Proceedings on Privacy Enhancing Technologies,2018,2018(3):143-163.

[25] Ermilov D,Panov M,Yanovich Y. Automatic bitcoin address clustering[C]//Proceedings of the 16th IEEE International Conference on Machine Learning and Applications (ICMLA). Piscataway:IEEE, 2017:461-466.

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

[27] Fleder M, Kester M S, Pillai S. Bitcoin transaction graph analysis[EB/OL]. (2015-02-06)[2021-12-17]. https://arxiv.org/pdf/1502.01657.pdf.

[28] Androulaki E, Karame G O, Roeschlin M, et al. Evaluating user privacy in bitcoin[C]//International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2013: 34-51.

[29] Koshy P, Koshy D, Mcdaniel P. An analysis of anonymity in bitcoin using P2P network traffic[C]//International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014: 469-485.

[30] Puzis R, Yagil D, Elovici Y, et al. Collaborative attack on internet users' anonymity[J]. Internet Research, 2009, 19(1): 60-77.

[31] Bissias G,Ozisik A P,Levine B N,et al. Sybil-resistant mixing for bitcoin the 13th workshop on privacy in the electronic society[M]. New York: ACM, 2014: 149-158.

[32] Bünz B, Agrawal S, Zamani M, et al. Zether: Towards privacy in a smart contract world[C]//International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2020:423-443.

[33] Williamson Z J. The aztec protocol[EB/OL]. (2000-01-23)[2020-12-03]. https://github.com/AztecProtocol/AZTEC.

[34] Kosba A,Miller A,Shi E,et al. Hawk:The blockchain model of cryptography and privacy—preserving smart contracts[C]// 2016 IEEE Symposium on Security and Privacy. Piscataway:IEEE,2016:839-858.

[35] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Berlin, Heidelberg: Springer, 2001: 552-565.

[36] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP). Piscataway:IEEE, 2014: 459-474.

[37] Maxwell G. Confidential transactions[EB/OL]. (2015-06-01)[2020-06-01]. https://people.xiph.org/~greg/confidential_values.txt.

[38] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2):84-90.

[39] Jan H Z, Roman M, Martin H, et al. Secure and anonymous decentralized Bitcoin mixing[J]. Future Generation Computer Systems,2018,80:448-466.

[40] Möser M, Böhme R, Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem[C]//Proceedings of the 2013 APWG eCrime Researchers Summit. Piscataway: IEEE,2013:1-14.

[41] Bonneau J, Narayanan A, Miller A, et al. Mixcoin: Anonymity for bitcoin with accountable mixes[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014: 486-504.

[42] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2015: 112-126.

[43] Chaum D. Blind signatures for untraceable payments[C]//Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer, 1983:199-203.

[44] Duffield E, Daniel D. Dash: A privacy centric crypto currency[EB/OL]. (2015-07-15)[2020-08-10]. https://pic.nanjilian.com/20180716/343445b5bc4-b5e0cba4589 3a083b480d.pdf.

[45] Maxwell G. CoinJoin: Bitcoin privacy for the real world[EB/OL]. (2013-05-20)[2020-05-11]. https://bitcointalk.org/index.php?topic=279249.0.

[46] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for Bitcoin[C]//European Symposium on Research in Computer Security. Berlin, Heidelberg: Springer, 2014: 345-364.

[47] Ziegeldorf J H, Grossmann F, Henze M, et al. Coinparty: Secure multi-party mixing of Bitcoins[C]//Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. New York: ACM, 2015:75-86.

[48] Maxwell G. CoinSwap: Transaction graph disjoint trustless trading[EB/OL]. (2013-07-11)[2020-08-09]. https://bitcointalk.org/index.php? topic=321228.0.

[49] Bissias G, Ozisik A P, Levine B N, et al. Sybil-resistant mixing for Bitcoin[C]//Proceedings of the 13th Workshop on Privacy in the Electronic Society. New York: ACM, 2014:149-158.

[50] Barber S, Boyen X, Shi E, et al. Bitter to better how to make bitcoin a better currency[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2012: 399-414.

[51] Parno B, Howell J, Gentry C, et al. Pinocchio: Nearly practical verifiable computation[C]//2013 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2013: 238-252.

[52] Ben-Sasson E, Bentov I, Horesh Y, et al. Scalable, transparent, and post-quantum secure computational integrity[EB/OL]. (2018-03-17)[2018-04-17]. https://eprint.iacr.org/2018/046.

[53] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more[C]//2018 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2018: 315-334.

[54] Pedersen T. Non-interactive and information-theoretic secure verifiable secret sharing[C]// Advances in cryptology-CRYPTO'91. Heidelberg: Springer, 1991: 129-140.

[55] Saberhagen V N. Cryptonote v 2.0[EB/OL]. (2013-10-17)[2020-04-24]. https://cryptonote.org/whitepaper.pdf.

[56] Noether S, Mackenzie A, Team M C. Ring confidential transactions[J]. Ledger, 2016,1: 1-18.

[57] Monero. About monero[EB/OL]. (2014-01-02)[2020-06-10]. https://getmonero.org/knowledge-base/about.

[58] Jedusor T E. Mimblewimble[EB/OL]. (2016-07-19)[2020-08-20]. https://scalingbitcoin.org/papers/mimblewimble.txt.

[59] Poelstra A. Mimblewimble[EB/OL]. (2016-10-06)[2020-10-16]. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf.

[60] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989,18(1): 186-208.

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

[62] Sander T, Ta-Shma A. Auditable, anonymous electronic cash[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 1999: 555-572.

[63] Ben-Sasson E, Chiesa A, Riabzev M, et al. Aurora: Transparent succinct arguments for R1CS[C]//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2019:103-128.

[64] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments[EB/OL]. (2015-07-17)[2020-09-08]. https://blog.bitmex.com/wp-content/ uploads/2018/01/lightning-network-paper.pdf.

[65] Raiden Network. What is the raiden network? [EB/OL]. (2018-02-26)[2020-12-06]. https://raiden.network/101.html.

[66] Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions[C]//International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2016: 43-60.

[67] Heilman E, AlShenibr L, Baldimtsi F, et al. TumbleBit: An untrusted bitcoin-compatible anonymous payment hub[C]// 24th Annual Network and Distributed System Security Symposium, NDSS 2017. Diego:Internet Society,2017:15.

[68] Green M, Miers I. Bolt: Anonymous payment channels for decentralized currencies[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 473-489.

[69] Nir B,Ran C,Alessandro C,et al. Recursive composition and bootstrapping for SNARKs and proof-carrying data[C]//Proceedings of the forty-fifth annual ACM symposium on Theory of Computing. New York: ACM, 2013:111-120.

[70] Abhiram K, Srinath S, Ioanna T. Nova: Recursive zero-knowledge arguments from folding schemes[EB/OL]. (2021-03-18)[2021-03-20]. https://eprint.iacr.org/2021/370.pdf.

【责任编辑: 周　全】