计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300025

大零币匿名技术及追踪技术综述

符朕皓　林定康　姜皓晨　颜嘉麒
南京大学信息管理学院　南京 210023
(191820045@smail.nju.edu.cn)

摘　要　近年来,依托于区块链技术的研究取得了重大突破且发展快速,各种数字货币正在不断兴起并涌入市场。大零币作为到目前为止区块链UTXO模型中隐私性最强的币种,其匿名技术除了为用户自身隐私提供了有力保障之外,同样具有很高的科研价值和广泛的应用前景。因此,为了规范数字货币的合法使用,探寻数字货币匿名技术更广泛的应用前景,各界学者也都在大零币匿名与反匿名技术方面进行了不同角度的研究。聚焦于大零币这一新型数字货币,首先介绍了大零币这一币种的大体框架;其次对大零币采用的匿名技术——zk-SNARKs和屏蔽池交易技术进行了梳理;然后总结并分析了目前各界学者在大零币追踪技术方面的研究;最后对大零币匿名技术和追踪技术的发展进行了展望。

关键词:区块链;大零币;加密货币;数字货币;追踪技术;匿名技术;零知识证明;文献综述
中图法分类号　TP311

Survey of Anonymous and Tracking Technology in Zerocash

FU Zhen-hao, LIN Ding-kang, JIANG Hao-chen and YAN Jia-qi
School of Information Management, Nanjing University, Nanjing 210023, China

Abstract　In recent years, relying on the research breakthrough and rapid development of blockchain technology, a variety of digital currencies are rising and flooding into the market. As the currency with the strongest privacy in the UTXO model of blockchain so far, the anonymity technology of Zcash not only provides a strong guarantee for users' privacy, but also has high scientific research value and a wide range of application prospects. Therefore, in order to standardize the legal use of digital currency and explore the wider application prospect of digital currency anonymity technology, scholars from all walks oflife have also conducted research on the anonymity and anti-anonymity technology of Zcash from different angles. Focusing on Zcash, a new digital currency, we first introduce thegeneral framework of Zcash. Secondly, the anonymous technology adopted by Zcash: zk-SNARKs and shielded pool transaction technology, are sorted out. Then we summarize and analyzethe research on Zcash tracking technology by scholars from all walks of life. In the end, anonymous technology and tracking technology development of Zcash are prospected.

Keywords　Blockchain, Zcash, Cryptocurrency, Digital currency, Tracking technology, Anonymity technology, Zero-Knowledge proof, Literature review

1　引言

大零币(Zerocash or Zcash)[1]等许多数字货币具有安全、匿名、便利、持久等优势,但也正是由于数字货币去中心化[2]、可编程[3]、易于跨国转账、匿名性强的特点,对数字货币的监管、跟踪难度也相应增大。越来越多的不法分子开始利用这一新生事物来进行洗钱、盗窃、欺诈、非法集资等违法犯罪活动。因此,重视研究数字货币反匿名追踪技术,实现数字货币交易的可链接性对于促进经济健康发展、维护社会秩序十分重要。

现阶段,以比特币(Bitcoin)[4]为代表的数字货币主要是通过假名技术[5],即通过地址而非实际账户作为媒介标识买卖双方来实现匿名性。根据Zhu等[6]的总结来看,目前针对假名技术来实现数字货币追溯的方法可以概括为如下几类:1)追溯方于网络层面捕捉交易相关信息,并与交易发起方的IP地址关联,实现交易溯源技术[7-9];2)追溯方基于UTXO模型对交易进行向上追溯,通过聚类分析等方法来跟踪特殊交易[10]、发现交易规律[11];3)追溯方通过寻找数字货币用户不规范行为导致的隐私泄露,来获取用户敏感信息,从而将区块链全局账本中的匿名地址和真实用户相关联,实现反匿名[12]。

由此可见,随着数字货币反匿名技术的不断发展,比特币

到稿日期:2021-03-02　返修日期:2021-05-23　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金青年项目(71701091);教育部人文社科青年项目(17YJC870020)
This work was supported by the National Natural Science Foundation of China(71701091) and Ministry of Education of Humanities and Social Science Project(17YJC870020).
通信作者:颜嘉麒(jiaqiyan@nju.edu.cn)

的匿名性在日益降低，针对数字货币的追溯方法也在不断丰富，51%攻击、双花攻击、日蚀攻击、权益窃取攻击等追溯技术层出不穷[7,13-16]。因此，在各种利益的驱动下，诸多改进匿名技术的加密货币不断诞生，其中最典型的代表为大零币。

大零币是一种隐私保护加密货币，于 2016 年 10 月 28 日推出，至今已经过数次迭代升级。与比特币采用的假名技术相比，大零币的不同点是在假名技术的基础上追加了名为 zk-SNARKs(zero knowledge Succinct Non-interactive Argument of Knowledge)[1]的实用零知识证明技术，以实现对指定交易的屏蔽，从而达到提高匿名性的目的。

在大零币中，大多数屏蔽交易都与矿池[17]相关。矿工们通过寻找各自需证明问题(一种基于加密哈希函数寻找部分预图像的数学问题)的解决方案，在矿池中开采大零币。而所有的交易集合称为资金池，资金池通常由一个实体来管理，该实体根据工作量证明(PoW)[18]规则向矿工支付大零币。而在解决需证明问题之前，矿工必须先将该问题转移到屏蔽地址，以匿名化通过解决问题而获得的大零币[19]。因为大零币的原始版本计划本身就是作为比特币协议的扩展，所以大零币的结构与比特币相似，同样也基于未使用的交易输出(Unspent Transaction Output，UTXO)[20]。大零币中的货币称为 ZEC，而最小的可能值是 1 Zatoshi，ZEC 的总供应量将略低于 2100 万，这与比特币的供应量相同。因此，总体上来看，大零币具有和比特币十分相似的框架。

本文主要对大零币的匿名技术和追踪技术进行了整理和评价。本文第 2 节为大零币匿名技术综述，该部分主要对大零币采用的零知识证明技术 zk-SNARKs 和屏蔽池交易进行介绍；第 3 节为大零币追踪技术综述，介绍了基于价值指纹的达南礼物攻击、粉尘攻击、侧信道攻击、往返交易攻击、用户行为分析、隐蔽信道攻击等攻击方法；第 4 节基于现有的研究进行了总结与展望；最后总结全文。

2 大零币匿名技术

大零币高匿名性的实现，主要由零知识简洁非交互式知识论证技术(即 zk-SNARKs 技术的应用)，以及依托其实现的屏蔽池交易机制两部分构成。本节主要介绍了 zk-SNARKs 这一技术的关键性作用，并对其从生成到使用过程中的工作机制进行了梳理，最后介绍了屏蔽池交易包含的 4 种不同交易类型。

2.1 zk-SNARKs

2.1.1 零知识证明的新形式——zk-SNARKs

零知识证明(Zero-Knowledge Proof)[21]，最早由 Goldwasser 等于 20 世纪 80 年代初提出。它早于区块链[22]诞生，但因区块链中对零知识证明技术的应用，才使得它被大家熟知。零知识证明指证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。

zk-SNARKs 就是零知识证明的一种新形式，它在大零币中的广泛应用既使得被屏蔽的交易可以在区块链上完全加密，又使得交易能够在网络共识规则下被验证为有效[23]。具体而言，zk-SNARKs 实际上指的是一种涉及两方甚至更多方的协议，或者可以说是双方或者多方为了完成具体的一项任务所需要采取的一系列步骤[24]。在 zk-SNARKs 的作用下，交易的证明方能够以不暴露具体交易内容的方式向交易的验证方证明自己的身份。例如，给定一个有关交易的随机生成的数列，证明者能够利用 zk-SNARKs，采取一定的方式向验证者证明该数列确实存在，而无须透露该数列的具体数值。

2.1.2 zk-SNARKs 的生成

简单来说，为了生成 zk-SNARKs，首先要将计算机可识别的代码转换为代数电路[19]，再将代数电路转换为一级约束系统(R1CS)，然后将 R1CS 转换为二次算术程序(QAP)[25]/二次跨度程序(QSP)，最后生成 zk-SNARKs。具体来说，需要经过以下步骤：

(1)采用 C 或 Python 等编程语言编写表示需证明问题的高级代码。将证明式子转换为对应编程语言的代码，进而可以得到多项式方程函数定义的代码片段[26]。

(2)将高级代码转换为一系列语句，语句包含以下形式的表达式：$x = y$ 或者 $x = y(op)z$。op 代表加减乘除等运算符，y 和 z 可以是变量或数字，甚至是更长的子表达式。处理结束后每个语句都可以看作代数电路中的门。随后增加行数和运算符的数量，以形成代数门。最终可以将上面的扁平代码表示为一个门系统[27]。

(3)把代数电路转换成一级约束系统(R1CS)。R1CS 是由 3 个向量组($\boldsymbol{v},\boldsymbol{w},\boldsymbol{k}$)组成的序列，其中 R1CS 的解是向量 $\boldsymbol{t}$，满足下列方程：$\boldsymbol{t}.\boldsymbol{v} * \boldsymbol{t}.\boldsymbol{w} - \boldsymbol{t}.\boldsymbol{k} = 0$[28]。其中，(.)表示向量的点积。

(4)将 R1CS 转换成二次算术程序(QAP)，此算术程序的目标任务是找到一个多项式 H，使方程 $\boldsymbol{t}.\boldsymbol{v} * \boldsymbol{t}.\boldsymbol{w} - \boldsymbol{t}.\boldsymbol{k} = H * Z(x)$。在此式中，$Z(x)$定义为最小简单多项式，使得对应于代数门的所有点都等于零。例如，在 4 个代数门的 R1CS 中，$Z(x)$即为$(x-1) * (x-2) * (x-3) * (x-4)$。

通过以上 4 个步骤，便生成了一个 zk-SNARKs，接下来就是利用 zk-SNARKs 进行交易的处理与验证。

2.1.3 zk-SNARKs 的工作机制

zk-SNARKs 在大零币交易中的工作机制主要包含以下 6 个部分[29-31]：

(1)zk-SNARKs 的草样通常产生于浇注硬币阶段。首先，系统规定一个安全参数 λ，它可以被看作是安全比特数和通用电路 C(通常是 100 万门控电路)。在系统设置阶段，利用 C 和 λ 的值，调用 KeyGen 函数对验证密钥(加密验证多项式)进行采样并存储为输出(由可信的第三方使用 RSA 协议[32]完成)。由于大零币使用了 zk-SNARKs 来构建它的知识结构，这意味着 zk-SNARKs 本质上是一个公开可验证的机制，因此任何人都可以成为验证者。

(2)创建支付地址阶段。在本阶段，系统会使用公共加密方案(ECIES 加密[33])为单个用户创建一个公钥和一个密钥。这些密钥依次与伪随机函数带有种子值的 PRF 一起使用，以生成公钥/私钥地址对。

(3)铸造硬币阶段。顾名思义，就是从已知硬币地址铸造新硬币。

(4)注值阶段。这个阶段基本上是将旧币的价值注入新

币，以确保旧币得到使用。在此阶段，验证方执行证明功能和生成 zk-SNARKs 证明。

(5)验证事务阶段。验证者可以验证铸币交易分类账，或者验证倾注交易分类账。

(6)接收硬币阶段。此阶段，接收方是具有地址对(公钥和私钥)的用户，该地址希望接收要发送到公钥地址的付款。若要做到这一点，首先要扫描当前账本。对于公钥地址的每次付款，接收方都会收到序列号不会出现在当前分类帐上的硬币(也就是说，这确保了接收方只收到未使用的硬币)。要花掉收到的硬币，就必须使用 POUR 算法，因此需要形成一个 zk-SNARKs 证明，随后需要验证证明，以确保用户不会重复使用旧的(已经花掉的)大零币。

2.2 屏蔽池交易

一般来说，大零币中有两种类型的交易事务。第一种是透明的交易。这些交易与比特币交易的工作方式相同，以一些以前未使用的输出作为输入，而新的未使用的输出作为交易的输出，此时投入和产出的总价值之差就是交易费用。但是，用户只能在公共地址或透明地址(t-address)[1]之间传输硬币，在本文中这种地址称为 t 地址，此类交易也称为 t-to-t 交易，目前为默认交易[1]。

第二种类型的交易是向隐藏地址(z-addresses)[1]发送或接收大零币的交易。在本文中这种地址称为 z 地址。一个交易可以同时使用 t 地址和 z 地址，但是 z 地址不会显示在链上，它的作用只是证明有一个有效的 z 地址进行了发送或接收未知数量的硬币这一项操作。本文将把涉及 z 地址的所有事务称为屏蔽事务或者屏蔽交易。

屏蔽交易由若干称为 joinsplit[34]的底层零知识证明组成。joinsplit 有两个公共参数，一个是以前公开发行的硬币数量，称为“vpub old”[35]，另一个是新公开发行的新硬币数量，称为“vpub new”[35]。事务中的每个 joinsplit 都有一对这样的值。如果我们将每个被屏蔽事务的每个“vpub old”值加总到一个区块中，然后对每个“vpub new”值也做同样的操作，那么将二者相减的剩余值，就是此时该区块的隐藏地址中存在的大零币的数量。屏蔽池交易通常涉及以下 4 种不同的交易类型，如图 1 所示。

(1)z-to-z 交易：在这种交易类型中没有透明可见的输入和输出，即这笔交易的传输只在 z 地址之间进行，“vpub new”字段中唯一透明可见的新金额只可能是交易费。这种交易类型通常被称为“公开交易”。

(2)z-to-t 交易：在这些交易中，没有透明可见的输入，但至少有一个透明可见的输出，其中输出之和必须小于或等于披露出的新 ZEC 的总和，而剩余部分则是交易费用。这种交易类型通常被称为“解蔽交易”。

(3)t-to-z 交易：在这种情况下，事务中没有透明可见的输出，只有透明可见的输入。并且输入的总和必须大于或等于新的被隐藏起来的 ZEC 的数量，而剩余部分是交易费用。这种交易类型通常被称为“入蔽交易”。

(4)t-to-t 交易：涉及 z-SNARKs，但事务中也有公共输入和输出。在这种情况下，交易费用是 zk-SNARKs 新发现的硬币与公共产出之和之间的差额。这种交易类型通常被称为“完全私密交易”。

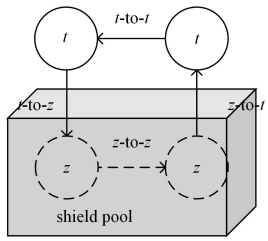

图 1 屏蔽池交易示意图

Fig. 1 Schematic diagram of shielded pool transaction

3 大零币追踪技术

如上文所述，大零币通过 zk-SNARKs 技术和屏蔽池交易机制的有效结合，使得交易的匿名性得到大大提高，针对比特币等较为传统的数字货币的追踪方法已经不能适用。如何实现大零币的可追踪，实现大零币交易双方的可链接成为了相关领域的研究热点。本节汇总介绍了最新的 6 种大零币追踪技术：达南礼物攻击、粉尘攻击、远程侧信道攻击、往返交易攻击、用户行为分析、隐蔽信道攻击。

3.1 基于价值指纹的达南礼物攻击

3.1.1 价值指纹

2018 年，Biryukov 等[36]首次在大零币领域提出了价值指纹(Fingerprinted Value)这一概念，并立足于价值指纹组织进行了达南礼物攻击(Danaan-Gift Attack)来达到反匿名的目的。

由于大零币采用了基于 UTXO(未使用的交易输出)的分类账本，每一笔交易中的大零币都源自上一个交易，形成了有效的溯源机制。因此利用 UTXO 一直向上溯源，其最初的交易即为大零币矿工因挖矿而获得奖励的创币交易，并且在大零币中，矿工由挖矿得到的大零币必须先转化为屏蔽地址之后才能进行流通。在 Biryukov 等[36]的定义中，所谓价值指纹即每笔交易中交易金额的 zatoshi 的后 7 位。并且在一般情况下，以 zatoshi 的最后 4 位做价值指纹十分稳定可靠，原因在于现阶段一般大零币交易的手续费均在 10000zatoshi(其价值低于 1 美分)以上，因此其没有进行交易的实际的经济意义，指纹也不会因为交易多次而失效。简而言之，价值指纹可以理解为交易独特性的一种标识。

对于价值指纹而言，如果两个价值指纹最后 7 位数字中有 5 位是相同的，或者最后 4 位数字是完全相同的，那么就可以认为该对价值指纹匹配成功，或者说该价值指纹在经过多长时间之后并没有被改变。文献[37]通过进一步统计分析区块数量与价值指纹匹配数量，最终确定交易价值指纹的寿命在 2～6 周左右，而后价值指纹的标识作用将大打折扣。

3.1.2 达南礼物攻击

价值指纹为链接屏蔽性交易的隐蔽 ZEC 金额和公开 ZEC 金额提供了可能性，因此 Feher 等[37]立足于价值指纹，于 2018 年设计了达南礼物攻击，其攻击步骤如下。

(1)攻击者可以将非常少量的精心选择的 zatoshis 以捐赠或购买服务的方式转移到被攻击者的特定地址，并希望被

攻击者在将其转换为隐藏地址或从隐藏地址中转换出来时留下指纹痕迹。

(2)攻击者只需监控在区块中公开的交易信息，并获取这些交易信息，从而构成指纹集。

(3)攻击者通过先前输出的 zatoshis 与指纹集中的各条指纹进行一一对比，最终匹配确认被攻击者的地址。

需要强调的是，达南礼物攻击成功的前提是被攻击者需要接收攻击者发送的 zatoshis，因此这种反匿名方式通常针对的是接收公共捐赠的实体，因为对他们来说，从一个未知的来源收到 ZEC 看起来不那么可疑。此外，攻击者可以持续监视被攻击者的地址并重新发送指纹，从而防止另一项或多项捐赠抹去原有的指纹。

3.1.3 达南礼物攻击技术总结

基于价值指纹的达南礼物攻击利用大零币交易金额的特点实现了对指定节点的标记。其优点在于：可操作性强，攻击者能够自由选择拟追踪节点，控制交易金额；可重复性高，攻击者可以多次进行攻击操作以保证指纹的有效性。然而，其缺点也十分明显：指纹集收集与指纹对比的工作量大，导致该攻击方法的性能较低；攻击能否成功取决于被攻击者的安全意识与行为规范程度，一旦被攻击者拒绝交易，后续攻击步骤将无法展开。

3.2 粉尘攻击(DUST ATTACK)

3.2.1 技术简介

2013 年，Bradbury 在“The problem with Bitcoin”[38]中提及并介绍了比特币中的粉尘攻击。粉尘攻击是一种较为传统的反匿名方式，在比特币诞生初期就已经产生，近年来随着各种匿名数字货币的不断涌现，各匿名数字货币领域均出现了粉尘攻击的现象，大零币也不例外。

在数字货币领域，“粉尘”通常指那些可以将其忽略的极少数量的货币额。以比特币为例，比特币的最小单位是 1 satoshi(也就是 0.00000001 比特币)，通常我们将 3 位数及以下 satoshis 的数量视为粉尘。换句话说，粉尘就是很小部分的交易或金额，通常这部分金额都不值得交易，因为它们的交易费用常常都高于其本身价值。而粉尘攻击，顾名思义，即利用“粉尘”，通过向目标地址多次发送极少量的数字货币，以将多个地址连接到一个所有者，最终达到采用极少量的虚拟货币来达到反匿名的目的。

2019 年，Vitto 等[37]对传统的粉尘攻击进行改进后，在大零币领域尝试并成功实现了粉尘攻击(见图 2)，其设计思路大致如下：

(1)攻击者通过购买服务或者向其捐献匿名大零币来获取被攻击者的隐蔽地址。

(2)攻击者将 ZEC 转成众多的极小额支票(如 1 zatoshis)，同时支付给被攻击者。

(3)因为支票数额极小，甚至交易费往往已经超过其本身的价值，所以很多用户根本不会在意这些微小金额的“粉尘”。一旦用户使用这些“粉尘”，这些微小金额就和用户未使用的交易输出(UTXO)混合在一起，就可以在区块链上通过这些极小的粉尘的组合来确定使用者，从而追踪用户的钱包地址，获得用户的真实身份。

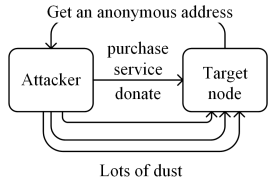

图 2 粉尘攻击流程图

Fig. 2 Flow chart of dust attack

3.2.2 粉尘攻击技术总结

粉尘攻击作为一种传统的反匿名攻击方式，其主要思想与达南礼物攻击类似，即通过对加密货币交易过程中的金额进行价值分析来实现交易的追踪，其简单易行，实现难度不高，但很容易被识别，成功率较低。目前已经有许多策略可以应对粉尘攻击，其中尤以“隔离”和“混币”两大策略最为有效。隔离，就是将那些来路不明和已经受到污染的粉尘金额与钱包中的其他金额隔离开，并且永久不使用，这样就从用户行为这一层面瓦解了粉尘攻击。而混币机制最早来源于 Chaum 于 1981 年发表的文章[39]，最简单的实现方式就是为每笔交易使用不同的地址。每个大零币钱包可以创建多个地址，而钱包上的余额就是输入和 UTXO(未使用的交易输出)的总和，这就意味着，使用者的 1ZEC 可以分割成多块进行使用(如 0.2ZEC+0.3ZEC+0.5ZEC)，从而割裂了 ZEC 输入和输出之间的一对一的对应关系，避免了粉尘攻击。此外，现阶段已有 Bitlaunder[40]等第三方提供混币服务，由此可见混币这一策略应用的广泛程度。

3.3 侧信道攻击(SIDE-CHANNEL ATTACK)

3.3.1 大零币匿名交易中的侧信道

在密码学中，侧信道攻击又称旁道攻击、边信道攻击，它的实现基于从密码系统的物理实现中获取的信息，而非直接寻找算法中的理论性弱点或对密码系统进行暴力破解[41]。例如，时间信息、反馈信息、功率消耗等可以提供额外的信息来源，并且这些信息可以被用于对系统进行进一步的破解。许多卓有成效的侧信道攻击都基于由保罗·科切开拓的统计学方法[42]。

Tramèr 等[43]于 2020 年对匿名交易整个生命周期中可能存在的侧信道进行研究后，最终发现了两个可以利用的侧信道。第一个侧信道存在于匿名交易的生成期。由于匿名交易的生成途径有两种，一种为交易用户创建，另一种为外包第三方创建。如果交易用户委托远程服务第三方创建匿名交易，那么在交易创建期间，攻击者便可以对外包证明的生成进行计时，以建立侧信道，从而获取可以利用的隐私信息。第二个侧信道存在于匿名交易的实际作用期。对于交易双方已链接起来的匿名交易，攻击者可以采取某些方法隐蔽地观察交易双方钱包与连接节点之间的信息传输模式或者内容，或者直接控制远程节点以获取信息。

在大零币中，用户的钱包和 P2P 节点在一个进程中运行。钱包通过尝试使用个人私钥解密交易来检查本钱包所有者是否是每个传入交易的收款人。这导致了两个侧信道泄漏源：1)如果解密成功，解密的事务格式正确，那么钱包将会进一步执行 Pedersen 承诺(Pedersen commitment)检查；2)如果

解密成功，但是解密的事务格式不正确，钱包将抛出一个异常信息，该异常信息将传播到节点的 P2P 层。

在第一种情况下，执行额外的 Pedersen 承诺检查所需的时间会导致 P2P 节点对后续网络消息的响应延迟。因此，Boneh 等设计了一种称为延迟攻击(PING ATTACK)[44]的反匿名追踪方式。在第二种情况下，可以利用拒绝消息攻击(REJECT ATTACK)[44]实现反匿名。

3.3.2 延迟攻击(PING ATTACK)

早在 2005 年，Brumley 等[45]提出并说明了针对 OpenSSL 的定时攻击(timing attack)，并且在文献[46]中进一步论证了定时攻击的可能性与实用性。延迟攻击可以说是在定时攻击的基础上发展而来的变种。

在大零币的交易模式中，当用户接收到一个新的屏蔽交易时，大零币客户端将会自动尝试解密相关的 Note 密文[1]。如果解密成功，则证明此客户端是事务的接收方，而后客户端将尝试解析 Note 明文[1]，并接收交易中的大零币。需要注意的是，大零币屏蔽交易的解密过程一般涉及到较为复杂的数学运算，由于这些加密操作十分复杂，调用解密算法解密成功花费的时间比解密失败花费的时间长，这一时间差便造成了隐私信息的泄露。延迟攻击的流程如图 3 所示，其具体攻击步骤如下：

(1)攻击者通过向拟追踪节点多次发送错误的屏蔽交易信息(后文统称为 ping 信息)来构建定时基线，即明确目标节点对于错误屏蔽交易解密失败所需的一般时长。

(2)每当区块链中出现新的匿名交易信息时，攻击者立即将该匿名交易与自己新生成的 ping 信息同时中继转移到目标节点，记录目标节点接收 ping 消息并在响应之前经过的时间，将其与先前构建的时间基线进行对比。如果此次响应时间比原先时间基线测量的时间长，则说明目标节点很有可能是此屏蔽交易的真正接收方，因为其为了解密成功而花费了更长的时间。

(3)立足于上述攻击步骤，攻击者可以在多个节点之间同时构建定时基线、中继屏蔽交易，从而可以扩大加密货币追踪的范围，提高追踪的效率。

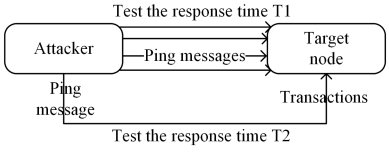

图 3 延迟攻击流程图

Fig. 3 Flow chart of ping attack

3.3.3 拒绝消息攻击(REJECT ATTACK)

根据大零币匿名交易的规则，客户端在接收到一笔新的匿名交易后会自动尝试解密该笔交易的相关密文，如果解密成功将进一步尝试解析交易事务中的明文，这样才能完成整笔交易。一般情况下，有效明文的第一个字节表示编码版本(Sprout 为 0x00，Sapling 为 0x01[19])。那么如果第一个字节是一个不正确的值，如在 Sprout 下第一个字节不是 0x00，则客户端会显式地抛出拒绝消息，并且将该消息反馈给交易发起方。

因此，如图 4 所示，假设有已知但匿名的交易地址(G, P)，攻击者有意采用错误首字节创建交易明文，并且使用匿名交易地址(G, P)的公钥加密该明文，创建一个匿名交易，进而将其发送至 P2P 网络中尽可能多的节点，回应拒绝消息的节点即为匿名交易地址(G, P)的真实所有者，由此实现了反匿名。

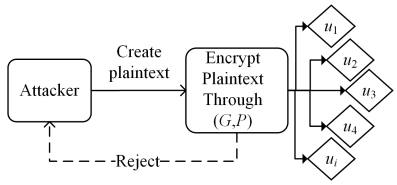

图 4 拒绝消息攻击流程图

Fig. 4 Flow chart of reject attack

3.3.4 侧信道攻击技术总结

延迟攻击与拒绝消息攻击均捕捉了大零币交易过程中存在的侧信道，本质上是利用了大零币密码系统在执行相关密码操作时产生的侧面信息，区别是前者利用了时间信息，而后者利用了回复消息信息。

就延迟攻击而言，其优点在于：1)隐蔽性高，被攻击者往往在无意间透露了有关自身身份的真实信息；2)效率高，理论上攻击者仅需两次操作即可实现反匿名，一次为构建时间基线，一次为中继交易信息并发送 ping 消息；3)成功率高且难以反制，延迟攻击与大零币交易的加密与解密机制密切相关，被攻击者很难在不改变自身硬件条件的情况下干扰时间基线的构建。而其缺点在于：延迟攻击的实现依赖于向目标节点中继正常的交易信息，如果目标节点的活跃度较低，持续的监控将会耗费大量资源；延迟攻击中产生的时间差往往短于 1 ms，对时间测量精度的高要求给硬件设备带来了一定的挑战。

就拒绝消息攻击而言，其优点在于：1)隐蔽性高且难以反制，拒绝消息的生成与反馈属于大零币客户端存在的缺陷，被攻击者很难察觉并进行反制；2)成功率高，回复拒绝消息的节点必然为公钥所有者。然而，其缺点同样十分明显：拒绝消息攻击成功的关键在于攻击者创建的匿名交易采用的公钥的所有者存在于被攻击节点范围中，为保证攻击成功率而采取“全面撒网”的方式会给硬件设备带来巨大负担，属于以效率换成功率的妥协之策。

3.4 往返交易攻击

往返交易在 Quesnelle 的论文中首次提出，实验数据采集到的区块数量为 196 304。2017 年 10 月 4 日，Biryukov 等[37]再次提到了这一方法。往返交易指如果一笔入蔽交易和一笔解蔽交易的金额完全相同，金额的数值在观察到的区块范围内是唯一的，并且入蔽所在的交易处于比解蔽所在交易更早的区块中，那么就可以认为这两个地址是链接的，交易双方的真实身份也就随之确定。也就是说，这笔金额在入蔽和解蔽之间没有经过变化，经历了多次转移后仍然保持了原始的值。

Quesnelle 通过统计分析发现，入蔽交易中的往返交易占比达到了 31.5%。针对这一性质，衍生了两种不同的大零币追踪方法，本文分别概括为考虑奖励费的往返交易攻击和考

虑拆分金额的往返交易攻击。

3.4.1 考虑奖励费的往返交易攻击

在大零币中,在隐蔽池内进行的交易需要支付给矿工一定的费用作为奖励,而费用往往是固定数额。那么在这样的情况下,入蔽的金额和解蔽的金额的差值往往是少量奖励金额的组合。由此,Quesnelle 提出了考虑奖励费的往返交易攻击,即如果入蔽和解蔽的差额刚好等于少量奖励费的组合,金额的数值在观察到的区块范围内是唯一的,并且入蔽所在的交易处于比解蔽所在交易更早的区块中,那么这两个地址被认为是链接的。Quesnelle 在实验中只发现了 388 个考虑奖励费的往返交易,而 Biryukov 等的研究中也采用了这个方法,但是只采用了奖励费为 0.0001 的情况,也只发现了少量的含有奖励费的往返交易。

3.4.2 考虑拆分金额的往返交易攻击

Biryukov 等[37]进一步提出,如果解蔽的金额中两笔的值相加等于入蔽时的值,或者是仅差少量奖励金额的组合,金额的数值在观察到的区块范围内是唯一的,并且入蔽所在的交易处于比解蔽所在交易更早的区块中,那么这几个地址同样可以被认为是链接的。即,用户很有可能在隐蔽池中将一笔金额拆成了多笔金额。例如,对于一个输入为 3.541 563 25ZEC 的交易和金额为 0.40002ZEC 和 3.141 543 25ZEC3 的两个输出,在相邻几个区块中,3.541 563 25ZEC 的交易区块先出现,而且 3.54156325ZEC 金额的数值在这几个区块中唯一。如果满足上述条件,则可以认为这 3 个地址是链接的。

3.4.3 往返交易攻击技术总结

总的来看,往返交易攻击从交易金额数值本身出发进行追踪,攻击者不再以链上的节点而是以旁观者的身份开展统计分析工作,隐蔽性高。但是,这种攻击基于用户本身的行为,而非大零币的内在机制,容易随用户行为的变更被瓦解。在 2017 年,大零币的使用者很多还没有养成设置数额提高隐蔽性的意识,很多用户在对交易入蔽后直接进行了解蔽,认为这样就可以提高隐蔽性。然而,随着大零币交易设置的规范化和用户行为的不断养成,这种攻击的效率与成功率并不突出。

3.5 用户行为分析

对大零币的追踪不仅可以立足于匿名交易金额信息,还可以立足于匿名用户的一些行为习惯。Kappos 等[47]统计分析了不同的交易参与者的行为,并将具有某些特征的交易进行了归类和验证,最终证实了他们的假设。他们采集的数据截止时间为 2018 年 1 月 21 日,当时已经开采了 258 472 个区块。

3.5.1 不同参与者的行为

大零币创始人在每个区块开采出来时会自动获得 2.5ZEC 的奖励,而在创始人的所有公开地址中,同一时间仅允许使用一个公开地址,因此创始人将使用该公开地址获取的所有奖励全部通过该地址存入屏蔽池中。如果利用该地址存放的 ZEC 数量达到了 44272.5ZEC 的限制,下一个地址就会取代这个地址。Kappos 等对创始人行为的统计显示,创始人每笔交易存放的金额数量绝大多数是相同的,正好是 249.9999ZEC,约为开采 100 个区块的奖励。而创始人取出的金额也具有高度规律性,其金额为固定的 250.0001ZEC,并且在 1953 次提款中,1943 次提款的间隔接近 6～10 个区块。因此,可以将任何价值为 250.0001ZEC 的 z-to-t 交易和 249.9999ZEC 的 t-to-z 交易标记为创始人行为。

大零币协议规定,所有新生成的硬币都必须放入屏蔽池中才能进一步使用。因此,对于矿工而言,其挖矿的奖励通常会被支付到一个固定的地址中,并由矿池的操作员控制。矿池操作员首先会将这些奖励存入屏蔽池,取出后再将每个人对应的奖励支付给每个矿工,这便会导致 z-to-t 交易的大量输出。因此,Kappos 等经过标记发现,对于可检测到的 z-to-t 类型的交易,如果该笔交易有超过 100 个输出的 t 地址,其中一个属于已知的矿池,那么这笔交易就可以被标记为挖矿支付,并将所有非矿池输出的 t 地址标记为属于矿工。根据这个特征,Kappos 等最终将区块链中的 110 918 个地址标记为属于矿工。

3.5.2 后续研究改进

Biryukov 等[37]离实现矿工地址的跟踪更近了一步,他们采集到了 416 062 个区块,发现了两种模式。为方便表述,后续将这两种模式称为模式 T 和模式 Z。在模式 T 的情况下,在找到固定的公共地址后,奖励直接转移到由同一实体控制的一组地址。根据每一笔接收到的金额,可以链接到矿池的特定输入,并且可以直接链接解蔽和入蔽交易。在模式 Z 的情况下,隐藏交易和公开交易之间的链接不是通过一个固定的地址,而是通过数百数千个地址。矿工地址将定期出现在池奖励交易中,其频率取决于其挖掘硬件的效率和池支付的频率。因此,扫描每个屏蔽交易,以找到具有矿池支付结构的交易(即上一段阐述的方法)。一旦找到模式 Z 交易,将进一步检查它的输出,并查找与已经存在的矿工地址集重叠的地址。如果重叠次数超过某一阈值(例如大于等于 40),便可以认为交易是由同一个采矿池发送的。

Biryukov 的工作揭示出了更多的地址,涉及了更多的矿池,使得 66.5%的屏蔽交易被挖掘出来,如果考虑整个链,那么他们链接了 88.4%的矿池奖励支付的屏蔽地址。但是,T 模式跟踪方法的缺点在于:很难将只挖掘了少数块的小型采矿池连接起来。因为在这些情况下,总是有多个匹配的显示值。而 Z 模式的缺点在于:由于矿工不一定一直在同一个矿池,因此这种方法只适用于较短的时间,一般约为 2000 个区块生成期。

3.5.3 用户行为分析技术总结

用户行为分析与往返交易攻击类似,攻击者均从第三人称视角通过对大零币交易的统计分析来进行追踪。而其特点在于:用户行为分析的最终追踪结果并非精确到具体节点,而是通过数学推理得出参与某笔匿名交易的节点集,因此其往往不是以单独的反匿名方式存在,而是与其他攻击方式相结合,作为缩小待攻击节点范围的一种有效手段,以减小原有攻击方式的工作量。

3.6 隐蔽信道攻击(SUBLIMINAL CHANNELS ATTACK)

3.6.1 技术简介

在密码学中,隐蔽信道(Subliminal Channel)可以理解为正常外观修饰下进行秘密通信的渠道。1984 年,Simmons 在

文献[48]中首次提出了采用签名技术进行隐蔽信道传输(Subliminal Channel Communication)的思路,并在文献[49]中成功构建了囚徒困境中的隐蔽信道。2019 年,Biryukov 等[37]提出了隐蔽信道攻击的方法。

在大零币中,Sapling 交易的输入由一系列支出描述和输入金额组成,而其输出由一系列输出描述和输出金额组成。由用户创建的完全屏蔽的交易事务,仅由支出和输出描述、完全透明的事务或导致它们组合的事务组成。Sapling 协议允许在可信环境中执行一个简化的签名步骤,同时允许另一台计算机构造证明,不需要支出秘钥的信任。硬件钱包也支持屏蔽地址,允许连接的计算机构造证明,而不将支出密钥暴露给该机器。

利用 Sapling 的新特性,Biryukov 等改造了钱包的证明和验证机制,以达到如下功能:证明机制和验证机制可以共享一些秘密辅助信息(aux)[37],允许验证器将带有 aux 的证明与生成的真正随机证明区分开来。将 aux 嵌入要发送的证明信息中,唯有知道 aux 的接收者可以解密,由此便可建立隐蔽信道,传递一些额外的信息用作交易的标记。这种标记便成为了后续追溯大零币去向的依据。

利用隐蔽信道,攻击者可以使用最初不是用来交换此类信息的系统参数,在密码系统中嵌入 n 位任意信息。这意味着隐蔽信道会成为密码系统中隐藏的部分,因此攻击者可以自由地决定是否发送秘密消息,也可以利用隐蔽信道来显示密钥或用户 ID。此外,攻击者能够很轻易地使用加密来保证隐蔽信道的机密性,仅允许提前知晓 aux 的接收者检索隐蔽消息,从而提高隐蔽信道攻击的成功率。

3.6.2 隐蔽信道攻击技术总结

传统隐蔽信息传输方法大多是定向发送、显式接收的,也就是说信息传输是点对点的,这种隐蔽传输方式易被其他恶意节点监听,恶意节点可以通过监听网络、分析网络流量的方式检测出隐蔽信道[50]。而大零币去中心化、交易数据复杂的特点恰好使得隐蔽信道难以被检测到,因此隐蔽信道攻击具有极高的隐蔽性;秘密辅助信息的构建与传递使得该技术能够精确地锁定目标节点,在效率、成功率、反制难度方面的表现都十分突出。

然而,需要注意的是,隐蔽信道攻击的实现需要攻击者在满足相关脚本标准的前提下对大零币钱包的证明和验证机制进行修改。与前文中提及的其他攻击技术相比,其对攻击者的技术能力提出了更高程度的要求。

4 总结与展望

4.1 总结

总的来说,大零币的高匿名性得益于 zk-SNARKs 技术和屏蔽池交易机制的有效结合。并且在大零币的历次版本更新中,完成一次 zk-SNARKs 证明的成本越来越低,所耗时间越来越短,这使得大零币的隐私保护日臻完善。但是,目前为止,大零币仍然存在着一定的缺陷,如大零币始终由一个中性化的公司进行管理,其权力太大,大零币也因此一直被质疑非中心化;大零币创始者始终持有总币量的 10%,并且收取挖矿奖励作为开发费用,高额的矿税屡遭诟病等。因此,在大零币的基础之上也产生了诸如 Zclassic[51],ZenCash[52] 等分叉币,它们尝试从不同的角度完善大零币的不足,甚至超越大零币本身。

综合第 3 节的内容,对不同大零币追踪技术的优劣进行对比,结果如表 1 所列。

表 1 追踪技术对比

Table 1 Comparison of different tracking technologies

追踪技术	隐蔽性	效率	成功率	反制难度
达南礼物攻击	中	低	中	低
粉尘攻击	低	低	低	低
延迟攻击	高	高	高	高
拒绝消息攻击	高	中	高	高
往返交易攻击	高	中	中	低
用户行为分析 隐蔽信道攻击	极高	高	高	高

由表 1 得出如下结论:

(1)隐蔽信道攻击为现阶段大零币追踪技术的最优解,其在隐蔽性、效率、成功率、反制难度 4 个方面的表现均十分优秀,然而实现起来的难度较高,如何绕过大零币钱包的安全检测机制是关键。

(2)粉尘攻击作为传统的加密货币追踪技术,其原理简单且普及度高,相比之下在隐蔽性、效率、成功率、反制难度方面已经不具备显著的优势。

(3)用户行为分析往往并不作为单独的追踪技术出现,而是充当其他追踪技术的补强方案。

(4)达南礼物攻击与粉尘攻击具有类似的技术思路,隐蔽性与成功率略高于粉尘攻击,可以通过重复攻击操作的方式来保证指纹的有效性。

(5)同属于侧信道攻击的延迟攻击和拒绝消息攻击的表现都十分可观,但由于延迟攻击可以进行点对点的针对性攻击,其效率略胜一筹。

(6)往返交易攻击采取统计分析的方式来链接匿名交易,规避了攻击者被检测为恶意节点的风险,但严重依赖用户行为的特点也导致其在其他 3 个方面存在短板。

不难发现,现阶段各界学者对于大零币反匿名和追踪技术的研究更多侧重于基于大零币交易规则、交易过程、交易主体寻找可能存在的漏洞,而并非实际寻找大零币底层算法上的弱点,从算法上实现大零币的反匿名。基于价值指纹的达南礼物攻击、粉尘攻击、往返交易攻击都是通过交易金额来寻找交易之间耦合的可能性,属于“价值分析层”;侧信道攻击(拒绝消息攻击、延迟攻击)和隐蔽信道攻击则立足于大零币交易信息传播过程中的漏洞,属于“信息传播层”;用户行为分析则是通过对用户行为进行统计分析后发现的普遍规律来对其他追踪技术进行补强,属于“应用统计层”。

4.2 展望

为对大零币匿名与追踪技术的发展进行展望,帮助各界学者探索发现更多包括大零币在内的加密货币领域的研究思路与方法,本文最后对基于区块链技术的加密货币相关的学术成果进行了引文分析。分析范围包括:Web of Science 核心合集收录的相关文章 1 971 篇,中国科学引文数据库收录的相关文章 129 篇,共计 2100 篇。

Web of Science 核心合集收录的 1 971 篇文章中共计有 68 篇文章围绕大零币展开研究。其中,文献[7]于 2014 年首次集中讨论了比特币这一匿名币种采用的匿名技术与可能的反匿名技术,随后大量相关研究于 2015—2020 年间展开,文献[16,53-54]等高引用论文均对加密货币的属性、匿名技术、溯源技术等进行了讨论与研究。而针对大零币这一匿名币种的研究从 2014 年大零币白皮书"Zerocash: Decentralized Anonymous Payments from Bitcoin"[1] 发布开始,文献[35,55]等针对大零币采用的匿名技术和可能的追踪技术进行了较为深入的研究。

在中国科学引文数据库收录的 129 篇相关文章中,文献[56]于 2003 年首次系统地分析了数字货币应用系统安全中的加密算法,文献[6,57-58]也聚焦于加密货币的匿名性质进行了不同角度的分析与研究。值得注意的是,由于针对大零币的研究在近年来处于初始阶段,中国国内的相关学术课题仍处于萌芽阶段,相关文献并未形成明晰的引文网络,大零币等加密货币领域的研究亟待各界学者开拓探索。

最后,基于全文内容及前人的研究经验,本文针对大零币匿名与追踪技术的研究提出了以下 3 点建议:

(1)机器学习作为近年来较为热门的数据挖掘与分析手段,可以尝试将其与大零币相关的研究结合,通过相关数学模型的构建来分析大零币匿名特点,寻找可能的突破口。

(2)以往的加密货币交易过程中往往只涉及交易发起方与接收方,然而近年来随着加密货币的兴起,""Bitcoin Fog"等许多针对加密货币的第三方服务平台不断涌现,因此接下来针对大零币等加密货币追踪技术的研究,可以尝试以第三方服务平台为切入点,实现交易的可链接性。

(3)目前针对大零币反匿名技术的研究主要基于大零币交易过程、交易规则、交易主体中的漏洞,而真正试图从算法层面逆匿名的操作尚未出现,因此相关学者可以基于密码学的视角分析大零币加密机制的缺陷,研究可能的大零币反匿名技术。

结束语 本文聚焦于大零币这一新兴数字货币,介绍了大零币的大体框架,并对大零币匿名技术的核心——zk-SNARKs 技术和屏蔽池交易机制进行了梳理,而后整理总结了现阶段不同学者针对大零币追踪技术的研究思路和实现方法,并给后续的研究提出了一些建议。大零币的匿名与反匿名技术在信息安全、隐私保护领域都有十分重要的科研意义和实践价值,值得各界学者进行进一步的深入研究。

参 考 文 献

[1] SASSON E B,CHIESA A,GARMAN C,et al. Zerocash:Decentralized anonymous payments from bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. IEEE,2014:459-474.

[2] GUO S T,WANG R J,ZHANG F L. Summary of Principle and Application of Blockchain[J]. Computer Science,2021,48(2):271-281.

[3] YUAN Y,WANG F Y. Current Status and Prospects of Blockchain Technology Development[J]. Acta Automatica Sinica,2016,42(4):481-494.

[4] NAKAMOTO S. Bitcoin:A peer-to-peer electronic cash system[R]. Manubot,2019.

[5] LI X D,NIU Y K,WEI L B,et al. Overview on Privacy Protection in Bitcoin[J]. Journal of Cryptologic Research,2019,6(2):133-149.

[6] ZHU L H,GAO F,FENG M,et al. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. Journal of Computer Research and Development,2017,54(10):2170-2186.

[7] 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. Springer,2014.

[8] BIRYUKOV A,KHOVRATOVICH D,PUSTOGAROV I. Deanonymisation of clients in Bitcoin P2P network[C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

[9] ANDROULAKI E,KARAME G O,ROESCHLIN M,et al. Evaluating user privacy in bitcoin[C]// International Conference on Financial Cryptography and Data Security. Springer,2013.

[10] LIAO K,ZHAO Z,DOUPÉ A,et al. Behind closed doors:measurement and analysis of CryptoLocker ransoms in Bitcoin[C]// 2016 APWG Symposium on Electronic Crime Research(eCrime). IEEE,2016.

[11] RON D,SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]// International Conference on Financial Cryptography and Data Security. Springer,2013.

[12] 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. 2013.

[13] HERRERA-JOANCOMARTÍ J. Research and challenges on bitcoin anonymity[M]// Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer,2014,3-16.

[14] BONNEAU J,NARAYANAN A,MILLER A,et al. Mixcoin:Anonymity for bitcoin with accountable mixes[C]// International Conference on Financial Cryptography and Data Security. Springer,2014.

[15] KENDLER E A,ZOHAR A,GOLDBERG S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C]// 24th USENIX Security Symposium (USENIX Security 15). 2015.

[16] CONTI M,KUMAR E S,LAL C,et al. A survey on security and privacy issues of bitcoin[J]. IEEE Communications Surveys & Tutorials. 2018,20(4):3416-3452.

[17] SCHRIJVERS O,BONNEAU J,BONEH D,et al. Incentive compatibility of bitcoin mining pool reward functions[C]// International Conference on Financial Cryptography and Data Security. Springer,2016:477-498.

[18] GERVAIS A,KARAME G O,WÜST K,et al. On the security and performance of proof of work blockchains[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.

[19] BIRYUKOV A,TIKHOMIROV S. Security and privacy of mo-

bile wallet users in Bitcoin, Dash, Monero, and Zcash[J]. Pervasive and Mobile Computing, 2019, 59: 101030.
[20] DELGADO-SEGURA S, PÉREZ-SOLA C, NAVARRO-ARRIBAS G, et al. Analysis of the bitcoin utxo set[C]// International Conference on Financial Cryptography and Data Security. Springer, 2018.
[21] DE SANTIS A, MICALI S, PERSIANO G. Non-interactive zero-knowledge proof systems[C]// Conference on the Theory and Application of Cryptographic Techniques. Springer, 1987.
[22] PILKINGTON M. Blockchain technology: principles and applications[M]// Research Handbook on Digital Transformations. Edward Elgar Publishing, 2016.
[23] PINTO A M. An Introduction to the Use of zk-SNARKs in Blockchains[M]// Mathematical Research for Blockchain Economy. Springer, 2020: 233-249.
[24] WAHBY R S, TZIALLA I, SHELAT A, et al. Doubly-efficient zkSNARKs without trusted setup[C]// 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.
[25] BUTERIN V. Quadratic arithmetic programs: from zero to hero [OL]. https://medium. com/@ VitalikButerin/quadratic …, 2016.
[26] BEN-SASSON E, CHIESA A, GENKIN D, et al. SNARKs for C: Verifying program executions succinctly and in zero knowledge[C]// Annual Cryptology Conference. Springer, 2013.
[27] BANERJEE A, CLEAR M, TEWARI H. Demystifying the Role of zk-SNARKs in Zcash[C]// 2020 IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2020.
[28] BEN-SASSON E, CHIESA A, RIABZEV M, et al. Aurora: Transparent succinct arguments for R1CS[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2019.
[29] BOWE S, GABIZON A, GREEN M D. A multi-party protocol for constructing the public parameters of the Pinocchio zk-SNARK[C]// International Conference on Financial Cryptography and Data Security. Springer, 2018.
[30] PETKUS M. Why and how zk-snark works[J]. arXiv: 1906. 07221. 2019.
[31] MAYER H. zk-SNARK explained: Basic Principles [OL]. https://blog. coinfabrik. com/wp-content/uploads/2017/03/zk-SNARK-explained_basic_principles. pdf. 2016.
[32] ZHOU X, TANG X. Research and implementation of RSA algorithm for encryption and decryption[C]// Proceedings of 2011 6th International Forum on Strategic Technology. IEEE, 2011.
[33] SMART N P. The exact security of ECIES in the generic group model[C]// IMA International Conference on Cryptography and Coding. Springer, 2001: 73-84.
[34] QUESNELLE J. On the linkability of Zcash transactions [J]. arXiv: 1712. 01210, 2017.
[35] BIRYUKOV A, FEHER D. Privacy and linkability of mining in zcash[C]// 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019.
[36] BIRYUKOV A, FEHER D. Deanonymization of hidden transactions in zcash[OL]. https://cryptolux. org/images/d/d9/Zcash. pdf?via=indexdotco.
[37] BIRYUKOV A, FEHER D, VITTO G. Privacy aspects and subliminal channels in Zcash[C]// Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019.
[38] BRADBURY D. The problem with Bitcoin [J]. Computer Fraud & Security, 2013, 2013(11): 5-8.
[39] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.
[40] DE BALTHASAR T, HERNANDEZ-CASTRO J. An analysis of bitcoin laundry services[C]// Nordic Conference on Secure IT Systems. Springer, 2017.
[41] STANDAERT F. Introduction to side-channel attacks[M]// Secure Integrated Circuits and Systems. Springer, 2010: 27-42.
[42] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Annual International Cryptology Conference. Springer, 1999.
[43] TRAMÈR F, BONEH D, PATERSON K. Remote side-channel attacks on anonymous transactions[C]// 29th {USENIX} Security Symposium ({USENIX} Security 20). 2020.
[44] TRAMER F, BONEH D, PATERSON K G. PING and REJECT: The Impact of Side-Channels on Zcash Privacy [OL]. https://crypto. stanford. edu/timings/.
[45] BRUMLEY D, BONEH D. Remote timing attacks are practical [J]. Computer Networks, 2005, 48(5): 701-716.
[46] BRUMLEY B B, TUVERI N. Remote timing attacks are still practical[C]// European Symposium on Research in Computer Security. Springer, 2011.
[47] KAPPOS G, YOUSAF H, MALLER M, et al. An empirical analysis of anonymity in zcash[C]// 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018.
[48] SIMMONS G J. The prisoners' problem and the subliminal channel[C]// Advances in Cryptology. Springer, 1984.
[49] SIMMONS G J. The subliminal channel and digital signatures [C]// Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1984.
[50] ZHANG T, WU Q H, TANG Z X. Bitcoin blockchain based information convert transmission[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 84-92.
[51] LI T R, CHAMRAJNAGAR A S, FONG X R, et al. Sentiment-based prediction of alternative cryptocurrency price fluctuations using gradient boosting tree model[J]. Frontiers in Physics, 2019, 7: 98.
[52] AVERIN A, SAMARTSEV A, SACHENKO N. Review of Methods for Ensuring Anonymity and De-Anonymization in Blockchain[C]// 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). IEEE, 2020.
[53] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[C]// International conference on financial cryptography and data security. Springer, 2014.
[54] PHILLIP A, CHAN J S, PEIRIS S. A new look at cryptocurrencies[J]. Economics Letters, 2018, 163: 6-9.

[55] BEN-SASSON E,CHIESA A,TROMER E,et al. Succinct non-interactive zero knowledge for a von Neumann architecture [C]// 23rd {USENIX} Secu-rity Symposium ({USENIX} Security 14). 2014.

[56] LV L T,CUI D W,HEI X H,et al. Three Mechanisms of Key Encryption Algorithm in Network System[J]. Computer Engineering,2003(14):114-116.

[57] HAN X,YUAN Y,WANG F Y. Security Problems on Blockchain:The State of the Art and Future Trends[J]. Acta Automatica Sinica. 2019,45(1):206-225.

[58] WANG H,SONG X F,KE J M,et al. Blockchain and Privacy Preserving Mechanisms in Cryptocurrency[J]. Netinfo Security, 2017(7):32-39.

FU Zhen-hao, born in 2001, postgraduate. His main research interests include blockchain, digital currency and information system.

YAN Jia-qi, born in 1983, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include blockchain, information systems, data analysis, and information science.