第 4 卷◆第 4 期◆版本 1.0◆2021 年
文章类型：论文|刊号（ISSN）：2630-4759 /（中图刊号）：270GL018

区块链时代数字货币匿名与追踪技术研究——以门罗币为例

刘泽雨[1] 魏晓光[1] 张倩[2] 王雨寒[1] 路毅[1]
1 河北金融学院 2 河北软件职业技术学院
DOI:10.12238/ej.v4i4.746

[摘 要] 虚拟数字货币的存在为非法融资、洗钱行为等犯罪活动开辟了捷径,而门罗币是数字货币的典型代表,本文从门罗币追踪技术进行分析,为有效解决以数字货币为基础的犯罪活动提供技术支撑。本文首先叙述了门罗币环签名、不可链接性、不可追溯性等匿名技术；其次,根据匿名技术的特征,介绍了输出合并攻击、最新猜测攻击、恶意远程节点攻击、o-mixin攻击等追踪技术；最后笔者对以门罗币为代表的数字货币的追踪和监管进行了展望。
[关键词] 数字货币；门罗币；匿名技术；追踪技术
中图分类号：F49 文献标识码：A

Research on Anonymity and Tracking Technology of Digital Currency in the Era of Blockchain--Taking Monero as an Example

Zeyu Liu[1] Xiaoguang Wei[1] Qian Zhang[2] Yuhan Wang[1] Yi Lu[1]
1 Hebei Finance University 2 Hebei Software Institute

[Abstract] The existence of virtual digital currency opens up shortcuts for illegal financing, money laundering and other criminal activities. Monero is a typical representative of digital currency. This paper analyzes Monroe coins tracking technology to provide technical support for effectively solving criminal activities based on digital currency. Firstly, this paper describes the anonymous technologies such as Monroe coin ring signature, unlinkability and traceability. Secondly, according to the characteristics of anonymous technology, the tracking technologies such as output merge attack, latest guess attack, malicious remote node attack and o-mixin attack are introduced. Finally, the author looks forward to the tracking and supervision of digital currency, represented by Monroe coins.
[Key words] Digital currency; Monero; anonymous technology; tracking technology

引言

区块链时代金融全球化、数据共享化程度的提高,促使世界各地之间距离的逐步缩小,而犯罪人员时常运用数字货币为交易手段,来逃避有关部门的监管。例如：运用加密货币,实现了跨国的违法交易、提高了违法行为的匿名程度,为洗钱行为、网络袭击提供了便利。而根据匿名技术特征衍生出来的追踪技术,可使以门罗币为代表的数字货币提高可追踪性并对其进行有效监管。本文通过分析门罗币的匿名和追踪技术,研究数字货币的监管,为有效解决以数字货币为基础的犯罪活动提供技术支撑。

1 门罗币的匿名技术

1.1门罗币匿名技术核心——环签名。环签名加密技术是门罗币匿名技术的核心技术。结合加密理论,我们将环签名进行了定义,指可以由具有单独性密钥的交易主体组中的任一成员来执行数字化签名。因此,具有环签名的信息可被特定持有对象组中的某位成员认可,但生成的签名在计算过程中无法具体确定所属于哪位成员,也就是说,如果发生信息泄露,攻击者也无法掌握签名者信息,因此增加了其安全程度。

环签名是基于椭圆曲线离散对数问题的EDDSA算法生成的。一次环签名由四种算法组成：

(1)密钥生成算法：签名者可以随机选择一个秘钥a,计算公钥A=aX和密钥镜像I=H(A),H为确定性哈希函数。(2)签名生成算法：签名者获取一个信息1,存在一组公钥D'的$\{A_x\}$,后输出一个签名α和一个密钥集S。(3)签名验证算法：验证者检验签名。(4)链接性验证算法：验证者检验其是否在过去的签名中使用过。

1.2门罗币匿名技术的不可链接性。门罗币的不可链接性,根本上来说是因为运用一次性的随机地址,而这与比特币模型运用的内容恰好相反。私钥对应了地址,具有私密性；公钥则具有唯一性。对于门罗币而言,发出者靠接受人地址随机生成一个一次性的公钥,因此即使发送给同一接受人,每笔交易也是由不同的一次性公钥接受,地址不唯一且不确定,仅仅接受人可以收回一次性私钥。

门罗币一次性随机地址代码于github

上公开,当交易的一方希望另一方进行付款时,此交易主体会获得一个另一方的长期公钥,进而生成一个一次性公钥,而长期公钥只有初始持有者知道且得到。接受者会创建一个交易和一个一次性公钥,并将此公钥交给交易的另一方。付款方一次性使用的支付地址包含在了一次性秘钥中。因为支付地址具有一次使用性且随机生成,因此除接受方和方以外的任何人都很难将两个交易地址链接到同一个用户。

1.3门罗币匿名技术的不可追溯性。以门罗币为基础的数字货币交易,其不可追溯性主要涉及到了交易主体的签名密钥以及密钥所代表的签名信息。在签署信息过程结束后,签署者会将所有用户的公钥提交给验证者,进而使得验证者可以凭借公钥验证部分信息用户。但验证者仍无法仅通过个人公钥就确定被验证者的身份信息,从而提高了不可追溯性。

2 门罗币追踪技术

目前将门罗币追踪技术分为四类：(1)基于大量0-mixin交易进行攻击：0-mixin攻击；(2)基于选择不同交易输出进行追踪：输出合并攻击等；(3)基于历史统计数据进行追踪：最新猜测性攻击；(4)利用门罗币安全机制漏洞进行攻击：恶意远程节点攻击。

2.1 0-mixin攻击。比特币明确地标识了交易中使用了哪枚币,而门罗币允许用户通过被称为“mixin”的交易输入来模糊交易的真正输入。在0-mixin攻击中,其所包含的输入均未使用mixin进行混合,形成可追踪输入。在任意一个输入中真实输入就是唯一的密钥。而由于此种攻击存在大量的了0-mixin交易,因此会获得许多干扰的密钥。当唯一性密钥与真实输入相等时,就可以在出现其他冗杂输入时进行剔除此密钥,降低了匿名性,提高了可追踪性。

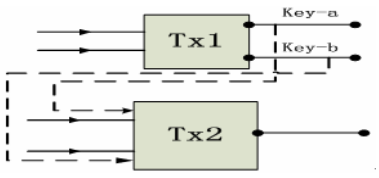

图1 输出合并攻击示意图

2.2输出合并攻击。输出合并攻击方法成立具有一定的前提假设,假设内容为选择同一个交易mixin时,设计算法不会选择同一个交易的输出。其攻击示意图如图1所示。

由图可知,Tx1使用了多个mixin输入,有key-a和key-b两个输出。Tx2有两个存在着多个mixin输入的输入端,并且每个输入端包含了TX1的输出。如若均满足以上条件,就可得出TX2中使用的真正密钥为虚线所对应的输入秘钥key-a和key-b,即TX2中的真实输入。但这种攻击方法必须以选择同一个交易的mixin为前提,如果没有选择同一个交易的输出,则极大概率会降低门罗币的匿名性。

2.3最新猜测攻击。如图2所示,最新猜测攻击会给定一组用于创建环签名的输入密钥,而实际使用的密钥是最具有高度的,并且其显示未花费TXO。换句话说,此算法并未选择最新的输入内容,而是选择的mixin大多来自更早之前的输入内容进而进行计算。此处所论述的更早的输入内容一定程度上指存储于100000之前的区块之中的内容,因此,旧的输入内容更容易被作为mixin。在之后的研究中,由于使用三角分布中抽取混合样本的方法,打破了均匀采样,给予更新的TXO更大的权重,使得最新猜测攻击的准确性下降。当同时有是个混合式输入时,会影响到最新猜测攻击的准确性,进而更大程度保护匿名性。

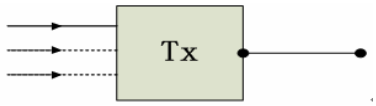

图2 最新猜测攻击示意图

2.4恶意远程节点攻击。门罗币客户端和远程节点在相互关联时,远程节点中包含了有关链的信息内容,而包含在内的最大索引又可以被钱包用来确定包含了mixin,钱包按全局索引进行了筛选,从而确定运用哪个mixin。为了保障不可追溯性,隐藏真实输入,客户端将索引与真正输入一同包含在请求中,多余的数据信息仍包含在钱包中。而输出通过API端点发送到远程节点,然后每个请求对应的密钥则发送到端点上。当收到端点响应时,客户端会进行部分验证过程;如若密钥未包含在客户端发出的响应中,则终止相关过程并报错。如若确认有关交易内容,则输出信息请求标记为已花费状态,并且将信息传输到远程节点。

客户端会在远程节点返回无效响应时显示异常状态,后客户端会终止交易过程并发出有关回应。而当用户再次尝试启动同样交易时,客户端会重新处理发出来的信息。最终将两次查询信息同时发送到远程节点,而查询请求的内涵密钥中相交的一个则为真实输入。因为未使用加密性的信息传递过程,恶意远程节点攻击可以根据自己意愿获取信息,从而推断出真实输入,这些问题应受到有关人员的重视。

3 总结与展望

区块链时代,数字货币的匿名技术和追踪技术互相促进,就目前形势来说,从门罗币等数字货币本身机制出发,而研究其追踪探索方面的仍属于少数,结合密码学角度进行科学追踪方法的探索,是未来数字货币领域一个新的角度和突破方向,将更有效地揭露数字货币匿名技术对于追踪技术的促进。

[基金项目]

2021年度大中学生科技创新能力培育专项《基于区块链的数字货币资金流追溯及监管研究》(编号2021H060404);2020年河北金融学院大学生科学研究项目《数字货币时代资金流追溯及监管体系研究》(编号DXSKYY2020020)。

[参考文献]

[1]林定康,颜嘉麒,巴·楠登,符朕皓,姜皓晨.门罗币匿名及追踪技术综述[J/OL].计算机应用:1-10[2021-11-6].http://kns.cnki.net/kcms/detail/51.1307.tp.20210428.1027.004.html.

[2]潘宁,胥苗苗.区块链与数字货币匿名技术的演化[J].生产力研究,2020(12):13-15+154.

[3]张启飞.论数字货币犯罪的刑法规制[J/OL].法治研究:1-11[2021-11-06].https://doi.org/10.16224/j.cnki.cn33-1343/d.20211022.009.

作者简介：

刘泽雨(2000--),女,汉族,河北石家庄人,河北金融学院金融科技学院2019级本科在读。