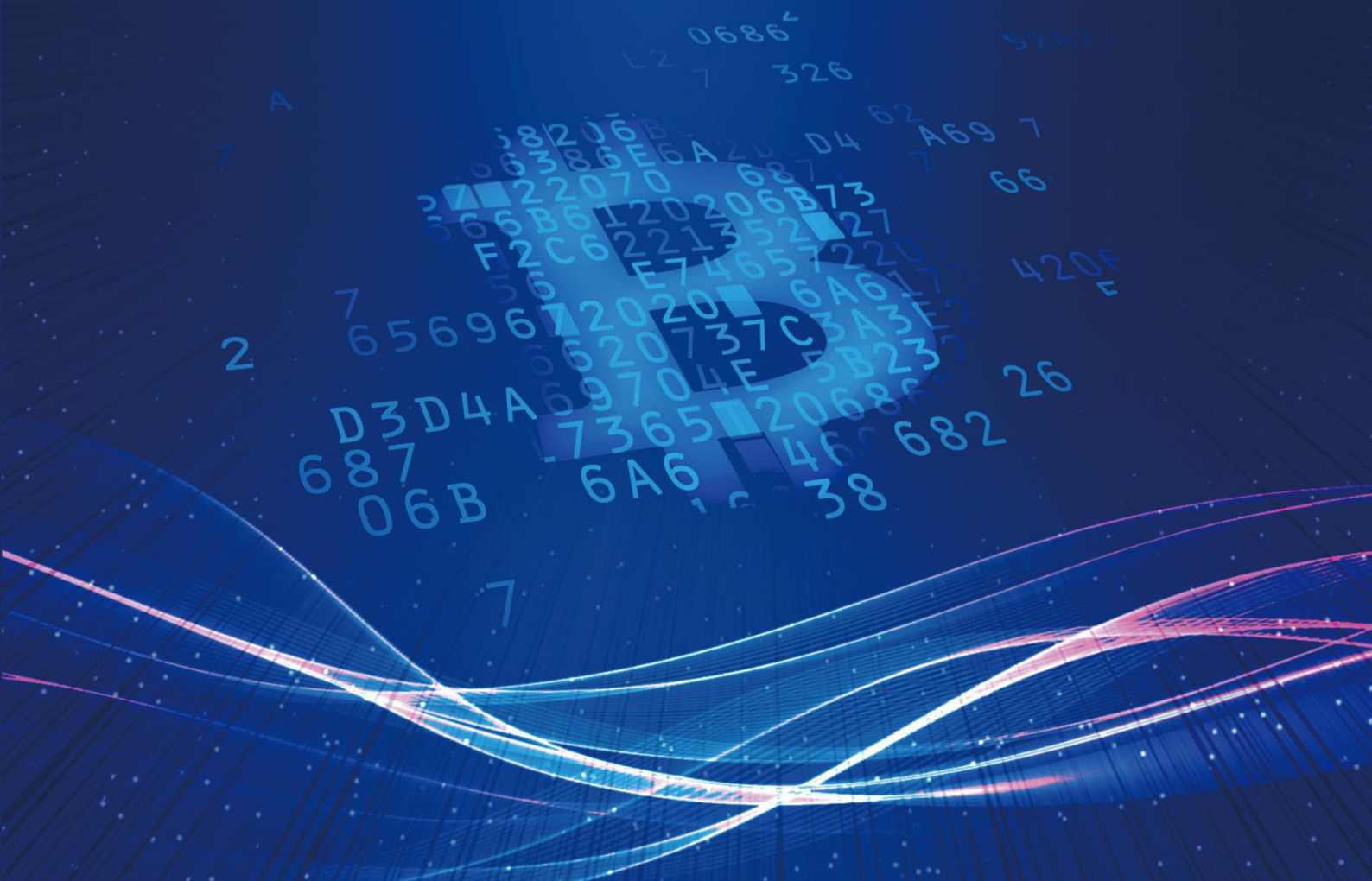
CSA GCR cloud security alliance®
GREATER CHINA REGION

数字货币溯源技术白皮书



致谢

云安全联盟大中华区（简称：CSA GCR）区块链安全工作组在 2020 年 2 月份成立。由黄连金担任工作组组长，9 位领军人分别担任 9 个项目小组组长，分别有：知道创宇创始人&CEO 赵伟领衔数字钱包安全小组，北大信息科学技术学院区块链研究中心主任陈钟领衔共识算法安全小组，赛博英杰创始人&董事长谭晓生领衔交易所安全小组，安比实验室创始人郭宇领衔智能合约安全小组，世界银行首席信息安全架构师张志军领衔 Dapp 安全小组，元界 DNA 创始人兼 CEO 初夏虎领衔去中心化数字身份安全小组，北理工教授祝烈煌领衔网络层安全小组，武汉大学教授陈晶领衔数据层安全小组，零时科技 CEO 邓永凯领衔 AML 技术与安全小组。

区块链安全工作组现有 100 多位安全专家们，分别来自中国电子学会、耶鲁大学、北京大学、北京理工大学、世界银行、中国金融认证中心、华为、腾讯、知道创宇、慢雾科技、启明星辰、天融信、联想、OPPO、零时科技、普华永道、安永、阿斯利康等六十多家单位。

本白皮书主要由 AML 技术与安全小组专家撰写，感谢以下专家的贡献：

原创作者：邓永凯、黄连金、刘林炫

审核专家：石瑞生

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/）上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

序言

反洗钱是政府动用立法、司法力量，调动有关组织和商业机构对可能的洗钱活动予以识别，对有关款项予以处置，对相关机构和人士予以惩罚，从而达到阻止犯罪活动目的的一项系统工程。从全球来看，反洗钱是金融监管中非常重要的工作。

随着区块链技术的广泛应用，以比特币为主的数字货币，以及越来越多基于区块链技术的数字资产开始出现。而类似于比特币这样的数字货币，尽管绝大多数国家都没有将其视为法定货币，但是的确已经在全球中获得越来越多的使用场景，并且由于其设计的架构具有一定的匿名性，经常被认为可能会与违法犯罪行为相关。

如何能够使得区块链技术在符合监管的情况下大规模落地应用数字货币溯源技术对于链上和链下的数据进行分析、跟踪、监管等等处理，对于区块链技术发展具有重要的意义。数字货币溯源技术并不会破坏区块链的“去中心化”的特点。相反，它将通过激发对网络的更大信心从而鼓励更加多的区块链技术的参与者。

云安全联盟大中华区对于 AML 技术和应用进行分析总结了这本白皮书，希望抛砖引玉与行业专家一起在白皮书的基础上结合新的创新和安全风险，为有关从业者提供一些指导。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

相关术语解释

AML：即 Anti Money Laundering ，反洗钱。是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪等犯罪所得及其收益的来源和性质的洗钱活动，是一系列旨在防止将非法收入转化为合法收入、维护市场经济秩序的政策及法律体系。

VASP：即 Virtual Asset Service Providers，虚拟资产服务供应商。提供虚拟资产交易服务的相关机构。

UTXO：即 Unspent Transaction Outputs，未花费交易输出。比特币的交易由交易输入和交易输出组成，每一笔交易都要花费（spend）一笔输入，产生一笔输出（output），而其所产生的输出，就是“未花费过的交易输出”，也就是 UTXO。

KYC：即 Know Your Customer，了解你的客户。 交易平台获取客户相关识别信息的过程，需要客户提供相关的身份证明信息。例如：身份证、护照等。它的目的主要是为未来的调查中为执法机构提供调查依据。

目录

一、资金来源安全

AML（Anti Money Laundering，反洗钱）中第一个环节就是保障资金来源安全，也就是说当数字货币交易中的收款方收到一笔数字货币时，需要知道这笔资金来源是否合法、合规。这就需要进行资金来源的溯源。

资金溯源就是追踪交易中输入的数字资产的来源。在区块链上，由于数据均是公开可查的。且由于区块链系统的特性，我们可以将链上的交易关联起来。简单的来讲，我们可以根据链上公开的数据分析某一地址中的数字资产“从哪来、到哪去”。例如，在比特币网络中，采用了 UTXO（Unspent Transaction Output，未花费输出）模型，可以通过分析资金对应钱包地址的 UTXO 数据来找出资金的来源。从而判断资金来源是否合法、合规。

二、交易风险识别

交易风险识别，就是识别正在进行的每一笔交易的风险。由于链上的数据有限，且每笔交易针对观察者来说均是大体相同的，因此我们需要引入其他的情报来针对交易进行评分。也就是针对交易中的地址进行评分，从而识别交易的风险。如果参与区块链中某笔交易中的地址评分过低，则说明该笔交易存在一些风险。

针对地址的评分可以有以下维度：

1、地址背后的实体：例如，若地址属于大型数字货币交易所，则该地址就有很高的可信度；若地址属于勒索软件、挖矿木马中的数字货币地址，则该地址的可信度就较低。

2、地址的相关情报：数字货币地址在互联网上的情报（例如，互联网上的用户或新闻等对于某一数字货币地址的评价、描述等）。若互联网中的情报大多为正面消息，则该地址的可信度就较高，否则可信度就偏低。

3、地址的历史交易记录：基于数字货币历史的交易状况（历史交易笔数、历史交易金额等）。例如，一个经常进行数字货币交易，资金量很多的地址可信度就大于一个没有任何交易的地址。

4、地址的行为特征：若地址进行过风险交易，则该地址的风险程度比较高。类似参考《人民币大额和可疑支付交易报告管理办法》，例如短期内资金分散转入、集中转出或集中转入、分散转出。[7]

三、风险控制

VASP（Virtual Asset Service Providers，虚拟资产服务供应商）避免资产损失，需要针对风险交易进行风险控制，保证风险资产不会通过 VASP 被承兑。针对风险交易，VASP 可以采取冻结资金、深入调查、联合监管部门和执法机构调查等方法。

针对 VASP，当用户将数字资产转移到风险地址时，可以也采取相应的措施，例如冻结资金等。

四、数字货币溯源技术面临的挑战

数字货币溯源技术包括两个方面：一是利用数字货币交易中输入和输出地址的映射关系查询数字货币的来源和流向；二是利用大数据分析技术分析出数字资产地址对应的背后实体。

由于区块链的特性，所有数据均公开可查。例如，在比特币网络中，我们可以很轻易的获取一个比特币地址的所有交易、资金数量等。虽然，使用传统方法很难将比特币网络中的地址与现实世界中的实体对应，但是，通过大数据分析等数据处理技术，很有可能还原出比特币地址对应的实体。于是，衍生出多种方法用来阻止第三方通过利用大数据技术还原数字资产地址背后的实体和对数字货币进行追溯。

其中，在比特币网络中有一种经典的方法——混币。

混币原理就是由多人参与交易，将大量的不同用户的资金放入一个池子中，当某一用户从资金池取出时，输入和输出已经被割裂，很难在输入和输出中找到一一对应的映射关系。割裂后便切断了分析人员进行数字资产来源、流向追踪的途径。

通常，使用混币服务的人群大多有两种目的：一是单纯为了提升比特币系统的匿名性；二是违法犯罪集团用来进行洗钱并且逃避司法系统的打击。

且经过小额、多次混币后提升现阶段数字货币溯源的难度，使得传统的方法很难溯

源，但是也并非不可能。若混币服务器上留存用户相关信息，则通过留存的信息对混币前后的资金流进行关联。不过，目前绝大多数的混币服务都声明未留存用户相关信息，且在明网和暗网均可使用该服务。即使如服务商宣称的一样不保存用户信息，也可以使用混币算法逻辑的漏洞进行追踪。[1][2]

零知识证明(zk-SNARK)

零知识证明是一种在无需泄露数据本身的情况下证明某些数据运算的密码学技术。允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了“它是真实的”之外的任何信息。

以太坊中的 Tornado Cash 采用了此类方法（zk-SNARK）。Tornado Cash 为一家提供以太币隐私保护的机构，Tornado Cash 合约提供转入转出交易隔离，利用零知识验证来实现转入转出交易的隔离。例如，用户可以使用 A 账户向资金池中转入一笔以太币，并生成一个秘密（Secret）。用户可以使用 B 账户并提供一个与存入资金池中的秘密对应的证明（Commitment），可将资金池中同等数额的资金取出。上述认证通过零知识证明实现，因此不用泄露具体的秘密内容。这样第三方便无法找到 A 账户到 B 账户的映射关系。

ZCash 同样采取了零知识证明(zk-SNARK)的方法，Zcash 地址分为隐蔽地址(z-addresses) 和透明地址 (t-addresses)。隐蔽地址（z-addresses）之间发生的交易交易的地址、资金、备注均经过加密，观察者无法看到；透明地址（t-addresses）之间发生的交易和传统的比特网网络类似，发送者、接收者、交易金额等信息均为明文信息且公开在链上。

隐蔽地址之间的交易也会出现在公有区块链上，所以大家都知道有一笔隐蔽交易发生，手续费也会支付给矿工，但交易的地址、资金的数额以及备注字段都被加密过，公众是看不见的。

地址的拥有者可以选择向可信第三方公开隐蔽地址和交易细节。比如，要符合审计和监管需要——通过观察密钥（view key）以及支付信息公开（payment disclosure）。

而两个透明地址之间的交易则与比特币交易没有区别：发送者、接收者以及交易金额都是公开可见的。虽然当前许多钱包和交易所都只能使用透明地址，但许多人已经开

始转向隐蔽地址，以更好地保护隐私。

两种 ZCash 地址之间也是可以交互的。资金可以在隐蔽地址和透明地址之间转移。资金一旦转入隐蔽地址则变得无法追溯。

环签名

环中一个成员利用他的私钥和其他成员的公钥进行签名，但却不需要征得其他成员的允许，而验证者只知道签名来自这个环，而不知到谁是真正的签名者。这个方式实现了对签名者的完全匿名，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。门罗币可以通过在交易中添加大量虚假交易，通常称之为 mixins，再利用环签名技术进行交易签名。第三方无法获取实际发起发起交易的公钥，从而隐藏了交易发送方的信息。因此从技术角度来讲，门罗币几乎无法进行溯源。[1]上述做法的原理同样是将一笔交易中的输入和输出割裂，达到资金无法溯源的目的。

但是，随着技术的发展，即使交易中使用了随机添加的 mixins，也可以通过分析其属性判断是否为交易中真正的花费。这些技术使得对门罗币的溯源成为了可能。[3][4]

五、数字货币溯源技术安全

在数字资产交易过程中，由于需要进行交易、资产安全评估，因此需要收集大量的链上数据（首次交易时间、总交易笔数、总转出笔数、总转入笔数等）、链下数据（地址相关情报、地址背后实体、交易时地理位置、交易时 IP 地址、用户 KYC 信息等）。但是收集、处理和存储的信息越多则信息系统中的环节也越多，可能被攻击的风险也就越大。且由于数据的特殊性，被攻击后造成数据泄露的影响也就越大。

另一方面，若数字货币溯源技术遭到滥用，便会导致数字资产交易毫无隐私，任何机构和个人均可以任意的查询地址背后的实体信息，个人用户私密的转账信息等。

因此，VASP 等相关机构在收集、存储相关用户信息时，需要做好对应的安全措施。例如，针对数据进行加密，针对存储数据的服务器进行加固，部署相关安全防护设备等。针对员工进行信息安全意识培训，防止人为的数据泄露。

[1] 据统计，64.04%的门罗币交易没有添加 mixins，即不包含任何迷惑分析者的 UTXO，可以清晰的定位到 UTXO 的花费情况

六、反洗钱案例分析

根据 Peckshield 分析[5][6]，7 月 16 日，包括 奥巴马（Barack Obama）、拜登（Joe Biden）、坎耶·韦斯特（Kanye West）、埃隆·马斯克（Elon Musk）、杰夫·贝佐斯（Jeff Bezos）及比尔·盖茨（Bill Gates）在内，多名美国知名人士推特账户遭到黑客攻击。

截止 08 月 02 日，涉案的两个地址一共收到 13 枚 BTC，黑客动用了超过 100 个中转地址进行洗钱。

7 月 19 日有其中少量的 BTC 流入了 Coinbase 交易所，如图二所示。而根据媒体得到的消息，FBI 正是根据 Coinbase 提供的 KYC 信息最终锁定了嫌疑犯。由此可见，严格的交易所 KYC 信息对于打击违法犯罪案件十分重要。

七、对行业的建议

1.对于政府部门、监管机构的建议

加快区块链链上数字资产的合规进程，建立相关监管部门。既可以保护合规的数字资产不受非法侵害，又可以处置区块链中基于数字资产的乱象。

2.对于区块链项目的建议

做好项目安全，防止黑客攻击造成项目方及用户相关资产的损失；项目方可与 AML 技术专业公司合作实现安全和合规。

3.对于 VASP 的建议

各大交易所进行实时情报共享，联合安全公司严格控制异常地址的转入、转出、承兑的交易。对经过综合分析研判为高风险交易做延迟处理，无法研判的建议上报监管部门协助处理。

交易所应注意符合针对数字货币反洗钱的合规需求，防止不良资产进入 VASP 造成相关资金损失和法律风险，美国已经有多家数字货币交易所因为合规问题受到处罚。

4.对于区块链个人用户的建议

谨慎进行 OTC（Over-the-counter，场外交易市场）交易，避免来历不明的数字货币；在进行数字货币交易时尽量在大型的数字货币交易所进行交易。

增强个人信息安全意识。例如，不在互联网上泄漏自己的数字钱包地址，不要安装来历不明的软件、APP 等，不要使用简单的密码，防止黑客通过网络攻击盗取用户的数字资产，造成个人用户的财产损失。

参考资料

[1]. T. de Balthasar and J. Hernandez-Castro, “An Analysis of Bitcoin Laundry Services,” in Secure IT Systems, ser. Lecture Notes in Computer Science, H. Lipmaa, A. Mitrokotsa, and R. Matulevicius, Eds. Springer ˇ International Publishing, 2017, pp. 297 – 312

[2]. M. Moser, R. B ¨ ohme, and D. Breuker, “An inquiry into money launde
ing tools in the Bitcoin ecosystem,” in 2013 APWG eCrime Researchers Summit, Sep. 2013, pp. 1 – 14.

[3]. A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of monero’s blockchain. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, ESORICS 2017

[4]. Möser, Malte, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan et al. "An empirical analysis of traceability in the monero blockchain." Proceedings on Privacy Enhancing Technologies 2018, no. 3 (2018): 143-163.

[5]. https://mp.weixin.qq.com/s/MQ8AOq7gbMfNP_CZzdpwhA

[6]. https://medium.com/@peckshield/2019%E5%85%A8%E7%90%83%E6%95%B0%E5%AD%97%E8%B5%84%E4%BA%A7%E5%8F%8D%E6%B4%97%E9%92%B1-aml-%E7%A0%94%E7%A9%B6%E6%8A%A5%E5%91%8A-150da50756b9

[7].人民币大额和可疑支付交易报告管理办法[EB/OL].http://www.gov.cn/gongbao/content/2003/content_62302.htm,2013 年 1 月 3 日

关于云安全联盟大中华区

云安全联盟 CSA （Cloud Security Alliance）是全球中立权威的非营利产业组织，致力于国际云计算安全和下一代 IT 安全的全面发展，聚焦在网络安全领域的基础标准研究和产业最佳实践。云安全联盟大中华区是在香港注册的独立、中立、专业的第三方非营利组织，与 CSA 美洲区、亚太区、欧非区共享 CSA 品牌与研究成果。

企业会员主要包括：世界大部分科技公司与网络安全公司如 Amazon、Microsoft、Google、Facebook、IBM、Intel、Oracle、VMWare、华为、中兴、腾讯、阿里、百度、奇安信、360、OPPO、启明星辰、天融信、深信服、安恒信息、浪潮、海尔集团、龙湖集团、格尔软件、Ucloud、数字认证、工商银行等。

云安全联盟大中华区欢迎各个单位加入，与联盟一起携手共进，共建网络安全生态。

邮箱：info@c-csa.cn
官网：https://c-csa.cn