

新型跨境洗钱犯罪分析及防治措施

■ 褚洪泉

摘要 近年来，电信诈骗、网络赌博等各种电信网络犯罪猖獗，黑灰产资金的跨境洗钱与转移需求不断增加，一批专门从事为黑灰产资金提供跨境汇兑、支付、转移服务的跨境洗钱犯罪集团应运而生。笔者在侦办一起跨境洗钱犯罪后，通过对犯罪复盘总结，尝试就跨境洗钱犯罪的交易模式、通联方式、资金通道及防控治理对策做全面梳理，希望能有针对性地打击相关犯罪。

关键词 跨境洗钱犯罪 交易模式 防治措施

洗钱通常是指运用各种手法，掩饰或隐瞒非法资金的来源和性质，使其变成貌似合法资金的行为和过程。跨境洗钱即运用金融工具以及网络科技为上游黑灰产犯罪资金提供跨境转移、隐匿、换汇、虚实币种转换等服务。新型跨境洗钱新生态中以汇旺、七喜、坦克等平台为代表，平台公司均藏匿于境外，公然面向全球开展业务，主要辐射东南亚，重点针对我国开展犯罪活动，撮合的是网赌、电诈、贩毒、贩卖人口等恶性犯罪黑灰产交易，越来越呈现出专业化、集团化、国际化的特点。

新型跨境洗钱犯罪所涉上下游犯罪团伙之间一般使用具有加密及阅后即焚功能的 Telegram、WhatsApp 等 IM 平台作为通

联方式，达成犯罪合意，以担保平台为背书，交付一定保证金，在零信任基础上实现不同团伙间的犯罪勾连，犯罪所得通过非法买卖外汇、黄金交易、直播平台充值、网赌跑分、第三方支付、虚拟币兑换等途径清洗，以对敲和错配的形式跨境转移。客户以黑灰产犯罪团伙为主，也包括为逃避外汇监管跨境转移资金的高净值人群。跨境洗钱犯罪会导致资本外流，破坏国家外汇管理秩序，对国家经济安全造成威胁，影响国家的外汇储备和国际收支平衡。1.25”专案成功侦破后，通过对犯罪复盘总结，尝试就跨境洗钱犯罪的交易模式、通联方式、资金通道及防控治理对策做全面梳理，希望能有针对性地打击相关犯罪。

作者：山东省济南市公安局经侦支队政委

一、交易模式

跨境洗钱犯罪集团面向全球广泛开展各类货币的跨境汇兑业务。以“1.25”专案为例，汇旺集团建立了独特结算系统，客户通过汇旺支付公群交易，或者通过汇旺支付 APP 操作均能完成跨境货币汇兑业务，两种方式在目标客户群体上各有侧重，同时互有交织。其中汇旺支付公群交易一般涉及交易金额较大，汇旺支付 APP 则金额较小。

在汇旺跨境汇兑中，以泰达币为中间媒介，开展人民币与外币的跨境兑换，具体的交易手法上又有所不同。

（一）公群交易模式

汇旺支付工作人员一方面在电报公群中招揽有换汇需求的客户，另一方面在其他电报公群中联系境内资金通道完成汇兑业务，从中赚取汇率差价。具体分两个步骤：第一步是汇旺工作人员收取换汇客户的外币（泰达币），并收集换汇客户在境内的收款人民币账号。第二步是汇旺工作人员向境内资金通道支付泰达币，并要求境内资金通道按照换汇客户提供的境内收款人人民币账号支付人民币。

根据获取的公链交易数据分析，2023 年 9 月至今，汇旺收 U 地址和汇旺付 U 地址存在大量交易，收 U 地址向付 U 地址单向转账累计约 4 亿泰达币，在此期间，汇旺支付通过上述方式累计为客户兑换人民币 3000 余万元。

（二）APP 交易模式

客户先在手机上下载并安装汇旺支付 APP，开通汇旺账户，之后在柬埔寨汇旺银行柜台网点存入美元至汇旺账户，也可以由打款方通过汇旺支付 APP 转账至客户汇

旺账户。然后在汇旺支付 APP 上输入国内银行账户，进行“提现”操作，等待收款。客户在汇旺支付 APP 进行“提现”操作后，汇旺支付 APP 后台系统就会生成订单数据并存储至专门的数据库，再联系境内资金通道进行转款操作。

二、通联方式

通常对于犯罪分子来说，具有匿名基本特性的暗网，是进行秘密通信的绝佳工具。暗网中的地下网络黑市才是网络犯罪分子的主要交易场所，但是网络犯罪分子越来越多地使用 Telegram、WhatsApp 等 IM 平台作为犯罪通联工具。为什么 Telegram 正在取代暗网论坛以及黑客社区，成为不法分子买卖数据、实施互联网犯罪、跨境洗钱的首要平台工具，原因有以下三点：

（一）暗网作为一种匿名通信工具可以被监管

暗网多被用于违法犯罪、恐怖主义等非法目的。随着网络技术的进步，美国执法部门摧毁 SilkRoad、AlphaBay 等大型暗网秘密市场后，一系列小型暗网交易网站也主动关闭，这表明监管活动有助于遏制暗网非法活动的发展。同时也可以看出，虽然暗网具有匿名特点，随着对暗网监管力度的加大，执法部门仍然可以对非法活动进行管控，导致犯罪分子感到不安全，遂加入到电报平台。

（二）Telegram（电报）平台自身的技术原因

高度加密。安全性极高的大众化即时沟通软件，使用独有的网络传输协议 MTProto，给犯罪分子安全感。

没有审查。不用担心被封号，除非执法

调查单位能证明用户是恐怖分子，这导致犯罪分子可以在平台上任意发布犯罪信息而无人监管。

云端同步。聊天历史无缝同步到所有的设备上（Cloud Storage）。纵使设备损坏，但数据固若金汤（Secret Chat 除外），犯罪分子不用担心数据的丢失。

不占内存。不必在设备上存储所有的聊天记录，因为数据一直保存在云端，你随时可以取回来，你也可以完全删除。

超大群聊。封顶 20 万人，配合各种管理工具（例如限制发言间隔），让大型申请群的交流井井有条，这样有助于犯罪分子在平台上做广告，推广其非法活动信息。

正是由于这些原因，Telegram 逐渐成为非法商品交易商与客户沟通的理想平台，而无需冒被执法机构监听的风险。

（三）Telegram（电报）平台注册使用方便没有任何限制

Telegram 之所以会受到不法分子的青睐，是因为它的平台注册方法非常简单：Telegram 用户往往只需要一个手机号即可完成注册，并且在使用时，这个号码会对群聊的其他用户隐藏，只有 Telegram 官方能够获取到这一号码的讯息，这意味着对于使用者而言，它能够实现全程匿名化的操作。此外，Telegram 创建群聊和频道也异常的简单，不法分子们完全可以通过 Telegram 平台实现信息的共享和传递，不必担心自建暗网服务器和域名被执法机构查处。同时，Telegram 的“频道”功能也缺乏相应的内容审核机制，相较于其他社交平台，用户可以轻松利用它来传播犯罪信息。它是一个加密的社交软件，支持秘密聊天、阅后即焚、账户定期删除等功能，令政府难以监视用户。

三、跨境洗钱犯罪的 11 种资金通道

（一）卡农账户三级连转直洗型资金通道

跨境洗钱犯罪是一个复杂的跨境金融犯罪生态，由一系列不同犯罪组合而成。其犯罪分工越来越细，卡农账户三级连转直洗型资金通道中，由卡商实现招募卡农指导卡农开立多张银行卡，并向洗钱车队提供卡农银行卡，卡农须按照洗钱方的要求开户、刷脸转账。卡农须提供银行卡三张，第一张用于直接接受上游黑灰产犯罪资金，上游犯罪资金到账后，立即刷卡汇入由第二张卡绑定的第三方支付账户中，而后迅速通过面部识别，将资金归集、混杂后转入第三张卡，随后使用第三张卡转移或派发。

（二）中介机构担保交易型资金通道

此种模式中跨境洗钱组织一般作为中介机构出现，其主要依托 telegram 软件（又称电报，是一款国外的聊天软件）作为联络方式。为网络赌博、电信诈骗等黑灰产各业务环节提供交易担保和撮合服务，为各类违法犯罪、黑灰产交易的顺利进行提供资源配置、担保交易、纠纷处理等服务，有效避免犯罪团伙间“黑吃黑”。因使用虚拟货币作为交易和通道媒介，成为黑灰产交易的“安全阀”。此种类型重塑了黑灰产交易模式，重构了非法资金转移通道生态，是全国各地警方公认“知名度”最高、规模最大的担保平台。同时，因其长期盘踞在境外，团伙核心骨干和核心关键数据极难调查获取，依法打击面临严重困难，导致其短时间内做大成势，成为电诈、网赌、传销、洗钱等犯罪屡打不绝的根源，严重危害国家政治安全、经济金融安全和社会大局稳定。

此种模式交易分专群交易、公群交易两种。专群交易指交易双方根据需求自行进入

大群，发布供需信息，建立联系后即另行搭建担保管理员和供需双方参与的三方聊天私群进一步勾连。交易双方达成交易意向后，向担保平台提交保证金，交易成功后，担保平台根据资金性质收取 0.1% 到 3% 的手续费后扣佣退费。公群交易指客户方自行或者按照大群推荐与担保平台的合作公群开展交易，担保平台收取合作公群押金，并收取诸如开群费、推广费、月租费等费用。担保平台收取开群费 500U、月租费 200U，转账手续费（每笔 2U），另外还要抽取该团伙洗钱业务量 2‰ 作为佣金。公群交易又分为以下三种交易类型：

代收一道赃款，错配泰达币。公群方系洗钱车队方，客户系电信诈骗方。公群方在担保平台上押资金，直接给客户id提供接收诈骗资金的一道资金账户，代收诈骗款，并按照约定汇率（约 12 元 /USDT）向客户回泰达币。

持一道赃款，兑换泰达币。公群方系一道赃款资金持有方，客户系虚拟币洗钱方。公群方在担保平台上押资金，客户向公群指定的虚拟币钱包地址转账虚拟币，公群方按照约定汇率（约 12 元 /USDT）向客户指定的银行账户转账一道资金。

持二道赃款，兑换泰达币。公群方系二道赃款资金持有方，客户系虚拟币洗钱方。公群方在担保平台上押，客户向公群指定的虚拟币钱包地址转账虚拟币，公群方按照约定汇率（约 9 元 /USDT）向客户指定银行账户转账二道资金。

（三）“换汇门店资金错配”型通道

该类资金通道手法特点是在跨境洗钱集团境外资金流向境内环节中，换汇实体店将收取的境内换汇人员的刷卡资金，按照跨境洗钱集团指示向其指定的境内人民币账

户转账，跨境洗钱集团按照约定的汇率或价格将等值的外汇或虚拟币支付给换汇门店。

（四）“黄金交易资金错配”型通道

当下黄金价格节节攀升，黄金市场交投活跃，投资黄金保值、升值，容易变现，一时间黄金产品供不应求，黄金回收业异常繁荣。黄金市场及黄金珠宝商成了洗钱的又一资金通道。该类资金通道手法特点是跨境洗钱犯罪集团在境外资金流向境内环节中，跨境洗钱犯罪集团指定的境内收款人民币账户的资金来源于大型大型黄金加工企业购买黄金珠宝商手中黄金应支付的“白资”，而黄金珠宝商手里的黄金来自于电信诈骗等黑灰产犯罪团伙，通过车手购买的大量黄金实物，车手用电诈资金购买黄金后转手卖给异地黄金珠宝商（以深圳水贝市场为主），再由黄金珠宝商层层批发转售与大型黄金加工企业，大型黄金企业将购金款按指令向洗钱犯罪集团指定的境内人民币账户转账，洗白资金。

（五）“同业票据贴现期限错配资金错配型”通道

该通道的特点是跨境洗钱犯罪集团指定的境内账户收到的资金是银行同业票据贴现期限错配后的正规金融资金。受各种因素影响，各金融机构比较热衷于做同业票据业务。银行采用票据过桥模式，卖出票据资产，并以回购的形式向同业融资，这样一来票据资产由表内转向了表外，表内的信贷资产置换成了同业资产。银行同业之间票据转贴现的期限错配更是监管盲区，容易被不法分子利用，存在着巨大风险。该资金通道为专门从事票据业务的票据中介持有，他们租用村镇银行同业账户，利用同业户开展票据转贴现以及卖出票据资产，并以回购的形式向同业融资等业务。银行同业间票据转贴现

以及票据售后回购的同业融资业务的交易对手往往不是同业银行，而是票据中介冒用的村镇银行，他们利诱一些城商行，做同业之间资金融通通道，以票据转贴现售后回购名义，向“资金行”短期融资，后利用期限错配方式，截留银行承兑汇票远期利息。并利用这些截留的远期利息形成的资金池，向跨境洗钱犯罪集团指定的境内人民币账户转账，将跨境洗钱犯罪集团支付的等价黑灰产资金用于收购票据。

（六）“车队跑分资金错配”型通道

不法分子搭建“跑分平台”并通过推广招募“码商”在跑分平台缴纳一定保证金，利用“码商”的微信或者支付宝收款码，收取上游犯罪资金，并依照洗钱方指令进行转移，“码商”赚取佣金。该类资金通道手法特点是“跑分车队”犯罪团伙为网络赌博、电信诈骗犯罪团伙等上游犯罪代收赌资等黑灰产资金在境内形成资金池，并将缴纳的保证金依照洗钱犯罪团伙指令转移，或兑换成虚拟币，向在境外的赌博网站等上游犯罪实控人虚拟币账户支付等价虚拟币，协助其资金转出，或在根据约定汇率收取等值外汇或虚拟币后，将境内资金池中的资金按照其他钱庄或跨境支付平台要求向其境内客户的境内人民币账户转账。这种模式的特点是通过缴纳“保证金”的方式，实现了资金错配和资金流向的改变。

（七）“抖音币充值打赏”型资金通道

该类资金通道手法特点是，大量黑灰产涉案资金，为了在实际变现过程中规避风险，在经过前述手法清洗后仍不放心，仍害怕被追踪，往往会将经过前述几种手法清洗后的资金在非法支付平台撮合下，向专门代充抖音币的网络科技公司支付，由网络科技公司代为购买抖音币，代为向非法支付平

台指定并与其有合作关系参与洗钱犯罪的MCN或网红打赏，MCN或网红将打赏变现扣除佣金后交予洗钱资金方。

（八）“第三方支付型”资金通道

该类资金通道手法特点是犯罪团伙利用购买或使用虚假身份骗取的第三方支付端口非法搭建第三方支付平台，利用为网赌、电诈等上游黑灰产资金提供代收代付、赌资派发等业务形成的资金池非法从事资金错配跨境资金支付结算业务。

（九）“虚拟币交易型”资金通道

虚拟币洗钱的主要方式：一是借助交易平台或OTC（虚拟币场外交易商），将赃款兑换成虚拟币，并利用虚拟币可全球兑换的特性，快速跨境转移，最后在境外兑现提现。二是借助中心化平台混淆资金。根据技术手段不同，可分为虚拟币跑分平台（搭建平台，招募社会人员以“代收代付”“先付后收”的形式批量分拆、清洗资金）、混币平台（利用混币器建立资金池，切断交易中发送方于接收方的联系）、匿名币（将资金兑换成不可追踪记录的门罗币、达世币等匿名币转移）等。

当前利用虚拟币从事跨境洗钱犯罪已经具有明显的组织化运行特点，以汇旺集团控制汇旺担保、汇旺支付为代表的虚拟币担保平台出现后，改变了跨境支付犯罪交易模式，彻底解决了黑灰资产上、下游信任难题，极大提高了黑灰资产交易效率，形成了一个高度集成、循环流转的跨境支付犯罪生态。

随着全国范围内开展的“断卡”“歼击”专项行动给各类违法犯罪资金通道以沉重打击，传统交易模式遭受重创，更多不法分子把目光聚焦到利用虚拟币洗钱模式上，由银行卡，三方、四方支付账户两种交易通道进化为银行、支付账户加虚拟币钱包“三驾

马车”密切使用阶段，无形中加大了查证涉案资金难度。

以“1.25”专案位列，汇旺集团控制的汇旺担保、汇旺支付利用互联网电报群（Telegarm）与境外不法分子、境内地下钱庄、虚拟币承兑商、“卡农”、“币农”利益共同、深度绑定、各司其职、各获其利，催生出一个利用虚拟币从事跨境支付犯罪生态系统。

其中，平台在生态中是处于统筹地位的组织者、领导者。组成要素包括互联网、在短视频中寻找、对接客户的引流员；电报群里承担撮合交易的客服员，负责管理资金账户、虚拟币钱包，资金对账的财务员；负责维护资金、数据安全，开发通信工具的技术员等。

境内地下钱庄的功能是接受平台指令向国内账户收、付资金。虚拟币承兑商则为平台源源不断的供给、变现虚拟币，是维持平台运转的“永动机”。

（十）“NFT 交易型”资金通道

2021 年，元宇宙（Metaverse）元年开启，自此元宇宙热潮居高不下，国内外产业巨头相继在元宇宙产业链条布局。在虚拟与现实交互的同时，NFT 的出现打破了以“虚拟数字”为核心的虚实平衡。NFT 是基于区块链技术的数字资产，与现实世界相隔离，且具有可转让性、双向隐匿性、不可篡改性等特性，深受洗钱分子青睐，逐渐沦为一种新型洗钱工具。

NFT（Non-FungibleToken）是“非同质化代币”的英文缩写。著有“数字艺术品”之称的 NFT，以其匿名性、全球流通、高溢价等特征沦为洗钱的工具，其表现方式主要为：一是不法分子使用赃款兑换虚拟币购买 NFT，然后直接转卖给他人或通过多次交易炒高价卖给他人，实现资金洗白；二是

在 NFT 交易平台自己铸造发布一款 NFT 作品，通过大肆宣传、引流等手段将作品炒热，后用赃款购买自己发布的 NFT 再转卖给他人将赃款洗白。

（十一）Defi 洗钱通道

Defi 是“去中心化金融（Dencentralized Finance）”的英文缩写，主要指以太坊等可编程的公有区块链网络上搭建的，以加密货币价值锚定、借贷、互换等类金融活动为功能目标、由系列智能合约和应用程序共同构成的区块链应用项目，目前主要以去中心化交易所加密货币借贷等项目为主。大多数 Defi 协议中，允许客户将一种虚拟货币换成另外一种新的虚拟货币，而在这些协议上追踪资产转移存在困难，且缺乏 KYC（“Know Your Custome”，客户认证）要求，造成 Defi 洗钱犯罪活动快速增长。其方式主要表现为：一是通过去中心化交易所洗钱。不法分子将非法获得的赃款发送到诸如 Uniswap、MDEX、Justswap、Sushiswap、DOTC 等去中心化交易所，然后通过去中心化交易所的资金池兑换成新虚拟货币，达到混淆资金流转路径，洗白赃款的目的。2020 年 Kucoin（库币）交易所被黑客入侵，被盗资金中的 1700 万美元通过去中心化交易所洗白而失去了追索路径。二是通过 Defi 借贷协议洗钱。不法分子将非法获得的赃款发送到 Defi 上提供接待服务的项目中，通过借贷项目资金池换成新的虚拟货币，以达到混淆资金流转路径，将赃款洗白的目的。三是创建一个 Defi 项目进行洗钱。不法分子自己创建一个 Defi 项目，将非法获得的赃款投入到项目中，然后通过“监守自盗”（设置后门，自己伪装黑客盗币等）等方式将项目资金转移，或者将吸收的用户资金和赃款混淆，以达到洗钱的目的。四是通过 Defi 质

押或流动性挖矿洗钱（相当于银行存款获取高额利息的项目）。不法分子将非法获得的赃款投入到 Defi 质押挖矿或 Defi 流动性挖矿项目中，并从中获得收益，以收益覆盖赃款达到洗钱目的。

四、防控治理措施

跨境洗钱犯罪团伙为逃避打击，主服务器设在境外且物理安防，数据获取难；客户上押保证金、黑灰交易均使用虚拟货币，资金追踪难；境内外上下游犯罪间的勾连均使用 telegram、WhatsApp 等通联工具，嫌疑人身份落地难；各种资金通道呈现职业化特点且多次错配，反侦查意识强，锁定打击难；境内外、上下游各团伙之间错综复杂，全链条打击难；核心打击目标团伙均藏匿于境外，境外缉捕难；跨境洗钱犯罪涉及多个行业、多个监管职能部门、数以万计的嫌疑人，生态治理难；为克服以上困难我们采取了以下措施：

（一）对利用 Telegram 通联实施犯罪的防范措施

由于程序具有随意复制和传播的特性，不易被控制和封堵，所以只能从源头进行扼制才能达到效果。Telegram 是一个移动通联工具，通常被安装在手机端使用，目前手机主流的两大操作系统是安卓和苹果的 IOS 系统，这两大操作系统是支持 Telegram 程序运行的，由于 Telegram 程序在我国被列为非法软件，自从我国华为公司自主研发的手机操作系统鸿蒙上市以来，所有安装鸿蒙操作系统的手机是不能安装 Telegram 的，安装时会提示这是非法软件禁止安装，国内品牌的其他手机如：小米、VIVO，OPPO 等使用的是安卓系统是可以安装 Telegram 的，

建议国内品牌的手机全部使用鸿蒙系统或者工信部要求这些国内品牌的手机安装的操作对 Telegram 程序进行屏蔽，这样就能很大程度上控制住此软件在境内的传播速度和范围，减少犯罪的发生。

（二）搭建“信息断点续传 deep 模型”

应对传统经济犯罪，我们一般采用资金穿透就可以了！而跨境洗钱犯罪平台一方面采取利用 Telegram 通联，割裂勾连信息；另一方面通过“卡接回 U”、“码接回 U”、承兑、“收 U 代付”、“同城换 U”等多种手段割裂资金链路。我们总体的侦查思路是“信息流爆破，资金流穿透”。我们一方面需要通过以下措施提升动态感知线索断点续传能力：一是建立虚拟币热钱包交易数据库，1.25 专案入库数据 570 余万条。二是研发可疑交易模型，筛选可疑交易线索。三是通过腾讯、阿里等企业及时查控涉嫌利用虚拟币犯罪的议价聊天、资金转账记录等信息。另一方面通过搭建电子证据链条续传资金断点。专案组通过向钱包企业，币安、欧易、火币等交易所通过电子邮件发送调证函件，获取涉案地址的资产信息、用户注册信息、交易数据等证据，以接续资金断点。犯罪集团为了切断与自身的联系，在资金流、信息流等方面制造了诸多断点。我们的任务就是搭建一款模型，将这些被切断的信息断点接续起来。

信息断点续传 deep 模型，开发理念为“深度”即深度搜集线索，并将异构化特色数据整理入库，系统及时自动分析后，列出标签数据，并向侦查员提供数据调取建议及策略。资金方面提供资金透视分析、账户报告、应调账户等需求；虚拟币方面提供应调地址及调证策略；网站数据、电报类数据根据系统字段提供 python 爬取代码，侦查员

复制到互联网即可爬取数据，导入公安网入库分析。

1.25 专案中，我们从碎片化的开源信息入手，通过技侦、网警、特情等途径，获取了汇旺担保平台“纠纷群数据”、汇旺支付平台换汇群聊天数据、汇旺 APP 注册数据，从出入境部门获取了近 5 年来出入境柬埔寨的中国公民数据，并调取人民银行反洗钱数据和虚拟币交易链上公开数据，特别是技术手段获取了汇旺自主开发通联工具“密言”聊天数据、水房沟通群数据、客户咨询业务汇总表等数据，构建了总量 1.7 亿条的专案数据库，通过“信息断点续传模型”比对、碰撞、分析，将不同形式、互不关联的数据信息通过研判形成一条完整、延续的侦查思路，梳理出境内嫌疑银行账户。

（三）搭建类罪多流爆破 seek 模型

类罪多流爆破 seek 模型，开发理念为探索数据关联，对现实货币资金流、虚拟币资金流、交易信息对接流、人员轨迹流等多维度进行关联碰撞爆破，进而锁定嫌疑类案、嫌疑人、嫌疑账户、嫌疑资产，开展专案打击；结合公安部云搜数据碰撞出重点参与群体，向行业监管部门、群体监管部门提出两书一单治理建议。

我们针对嫌疑账户落地身份开展“双链路资金穿透”，一方面依托“类罪多流爆破模型”对嫌疑账户资金流水进行“追踪—识别—调取—穿透—归析”五步战法研判，明确资金与与账户实控人员的关联，追踪涉案资金去向，绘制出资金流向图。另一方面，使用“无匿”“链上云眼”等虚拟币分析工具，查询犯罪集团的公链地址交易，虚拟

币钱包首笔 gas 费的缴纳，关联与信息流研判出的交易时间、数额对应的虚拟币流水，印证并拓展嫌疑账户，锁定目标团伙骨干人员，进而追踪锁定涉案资产。在虚实两种货币“双链路资金穿透”的基础上，根据不同类罪所呈现出的虚实两种货币的类罪资金交易特征，开展针对性的类案专项打击。

（四）搭建指挥调度生态治理 TDCS 模型

该模型开发理念为生态治理，侧重指挥调度；在侦查侧对取证、打击、查扣等各项行为进行全链条提供侦查建议、监督并提出整改补充建议，起到 ai 法制员效能；在指挥侧实现全程监控案件进度、办案质量、执法行为监督等各项功能。确保案件高效能高质量的同时，做到打击不漏人、挽损不漏赃、生态治理全覆盖，起到 ai 小参谋效能。

该模型依托经侦法库、专家注释为基础知识库，对接 python、mysql、Powerlink、云镜、360 锋刃各项工具，汇聚 1.25 专案案调取的 200 万条人民银行反洗钱数据、1 千万条虚拟币数据、5 千万条资金查控平台数据以及三方、外汇、出入境、app 注册等 1.7 亿量级数据对 deepseekR1 满血版 32b 模型进行驯化，实现数据的自动关联分析、数据报告的自动生成、案件线索自动生成、两书一单自动生成等各项功能。通过该模型针对跨境洗钱犯罪十种通道类型我们分别形成了对应的净化治理措施，分别向国家外汇管理局、中国人民银行、山东黄金集团、抖音公司等部门和企业推送“两书一单”，协同刑警、网安等警种建立常态化监测和预警机制。

责任编辑 马煜童