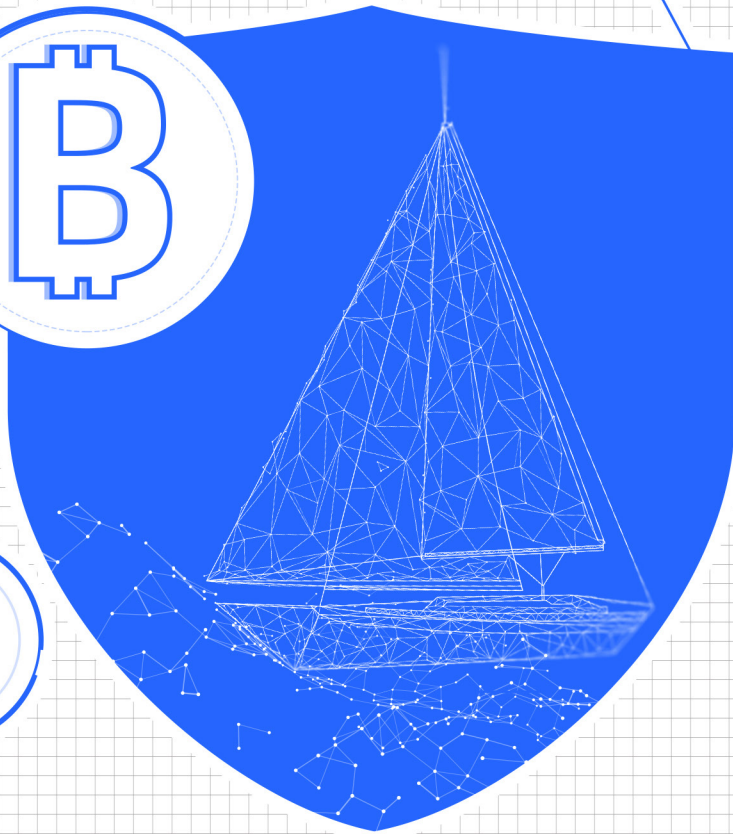
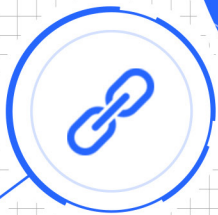
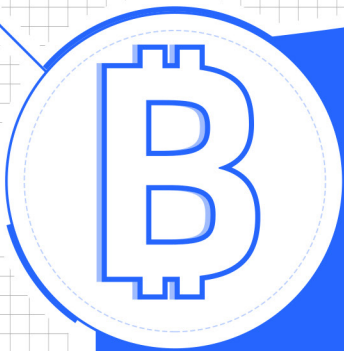
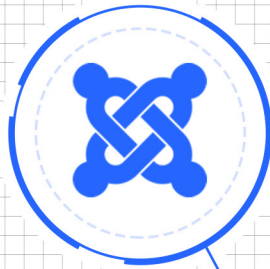


区块链与虚拟货币 犯罪趋势研究报告

CHAINDIGG

区块链大数据分析专家

2022
年度



 知帆科技
CHAINDIGG

 知帆学院
ZHIFAN ACADEMY

摘要

在本报告中，知帆安全团队从 2021 年至 2022 年虚拟货币犯罪案件、2022 年虚拟货币传销和赌博项目、近五年涉虚拟货币刑事文书的主要类型、数量、金额、币种等维度，结合 2021 年至 2022 年虚拟货币跨境资金分析、2022 年区块链安全事件和典型案例揭示了 2022 年区块链和虚拟货币犯罪的发展现状和发展趋势。总结出 2022 年区块链安全领域十大关键词、2022 年 NFT 相关非法活动分析、2022 年网络赌博的新形态和难点和 2022 年虚拟货币诈骗“八宗最”。

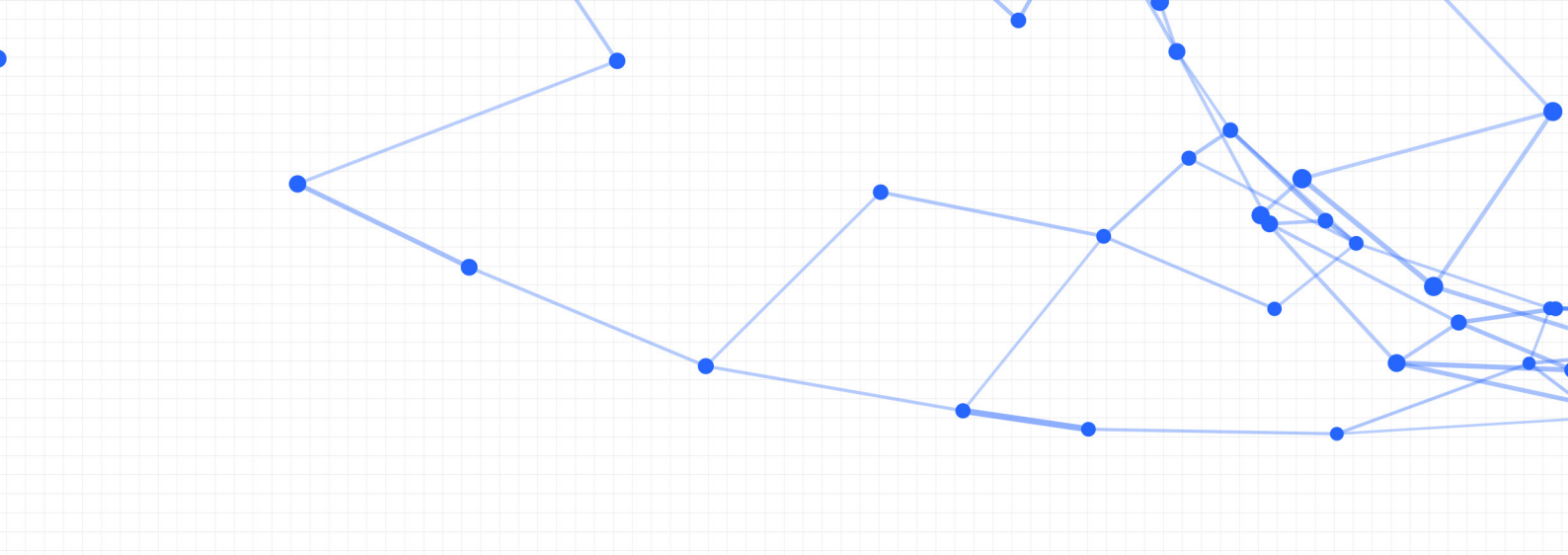
- ◆ 虚拟货币诈骗洗钱类和网赌结算类是主要的虚拟货币犯罪类型。2022 年，诈骗洗钱类案件数量占比 30.5%，位居首位；涉案金额占比 22.5%，排名第二。网赌结算类案件数量占比 12.3%，排名第二；涉案金额占比 66.1%，位居首位。
- ◆ 虚拟货币网赌结算类案件平均涉案金额最高。2022 年，网赌结算类案件的平均涉案金额最高，达到 8.71 亿元。
- ◆ 虚拟货币传销类案件数量和涉案金额下降。传销类案件数量占比从 2021 年的 29.2% 下降至 2022 年的 11.8%，同比下降 59.5%。2022 年，传销案件涉案金额占比仅为 8.6%，相比 2021 年（67.8%）大幅下降。
- ◆ 涉案比例最高币种：TRC20-USDT。2022 年，USDT（泰达币）是最主要的涉案币种，主要是波场区块链上的 TRC20-USDT 和以太坊区块链上的 ERC20-USDT。其中 TRC20-USDT 位居首位，占比高达 84.6%。
- ◆ 虚拟货币传销项目偏爱 BSC。2022 年，超过八成的传销项目部署在 BSC 上，这主要因为 BSC 是目前最受欢迎的公链之一，生态发展比较好，用户和项目基数明显高于其他公链。其中私募空投模式最多，占比 26.5%。
- ◆ 虚拟货币传销项目周期缩短，整体资金规模下降。2022 年，传销项目往去中心化方向转换，运营周期缩短，资金规模下降明显，大多数都在百万级跑路。
- ◆ 虚拟货币赌博项目更爱 TRON。2022 年，超过七成的赌博项目部署在 TRON 上，主要由于波场链上的 TRC20-USDT 在转账速度、拥堵情况、手续费等方面有明显优势。其中哈希竞猜模式项目成为新型赌博模式，占比 14%。
- ◆ 虚拟货币刑事文书数量逐年上升。2017 年至 2021 年（因裁判文书公开有延迟性，本报告统计时间为 2017-2021），虚拟货币相关的刑事文书的数量呈逐年上升趋势。其中 BTC（比特币）相关的刑事文书总数量最多，其次是 USDT（泰达币）相关的刑事文书，2021 年，USDT 刑事文书数量已超过 BTC。
- ◆ 虚拟货币刑事文书中，案由较多的是：帮信罪、诈骗罪和掩隐罪。从案由分布上看，2017 年至 2021 年，帮助信息网络犯罪活动罪最多，占比为 21%；诈骗罪排名第二，占比为 20%。掩饰、隐瞒犯罪所得、犯罪所得收益罪则排在第三位，占比为 19%。

- ◆ 诈骗类是打击最多的虚拟货币犯罪类型。根据不完全统计，2022年全国公安机关破获各类虚拟货币相关案件190余起，诈骗类型最多，其中有部分案件公布了涉案金额，此部分已破获虚拟货币案件总涉案资金流水达1064亿元。
- ◆ 虚拟货币跨境资金整体资金规模下降。2022年，虚拟货币跨境流入资金1755亿美元，较2021年下降44.3%；虚拟货币跨境流出资金1842亿美元，较2021年下降40.1%。
- ◆ 区块链安全事件数量整体呈上升趋势。近五年，区块链安全事件数量整体呈上升趋势，2022年，Q2季度季度区块链安全事件数量最高。
- ◆ 区块链安全事件损失金额明显下降。由于整个市场虚拟货币价值下跌，2022年全年区块链安全事件损失累计金额为33.27亿美元，只占2021年的30%左右。其中Q1季度季度损失金额最高，达到12.8亿美元。
- ◆ 合约漏洞类是最主要的区块链安全事件类型。2022年，合约漏洞类安全事件数量最多（占比33.6%），累计损失金额最高（17.62亿美元）。另外，诈骗类虽然数量较多，但是整体损失金额偏低。
- ◆ 2022年区块链安全与犯罪领域十大关键词。分别是：百日行动、反洗钱、惩治电诈、FTX破产、Luna崩盘、行业监管、跨链攻击、Rug Pull、哈希赌博和数藏遇冷。
- ◆ 众公链纷纷入场NFT，以太坊独占鳌头。根据NFTScan数据显示，以太坊NFT交易量高达340亿美元，位居第一，远高于其他公链。

目录

第一章 2022 年虚拟货币犯罪案件综合分析	01
一、2022 年虚拟货币犯罪主要类型及平均涉案金额	02
二、2022 年虚拟货币犯罪主要类型累计涉案金额	03
三、2022 年虚拟货币犯罪主要涉案币种分布	04
第二章 2021 年至 2022 年虚拟货币犯罪案件发展趋势	05
一、2021 年至 2022 年虚拟货币犯罪主要类型数量发展趋势	06
二、2021 年至 2022 年虚拟货币犯罪主要类型累计涉案金额发展趋势	07
三、2021 年至 2022 年虚拟货币犯罪主要涉案币种发展趋势	08
第三章 2022 年虚拟货币传销和赌博项目分析	09
一、2022 年虚拟货币传销项目所属公链和模式分布	10
二、2022 年虚拟货币传销发展趋势	11
三、2022 年虚拟货币赌博项目所属公链和模式分布	12
四、2022 年虚拟货币赌博发展趋势	13
第四章 2017 年至 2021 年虚拟货币刑事文书综合分析	14
一、2017 年至 2021 年虚拟货币相关刑事裁判文书发展趋势	15
二、2017 年至 2021 年虚拟货币相关刑事文书案由分布	16
三、2017 年至 2021 年虚拟货币相关刑事文书主要涉及币种发展趋势	17
四、2017 年至 2021 年虚拟货币相关刑事文书分布省份 TOP10	18
第五章 2022 年全国破获虚拟货币案件和典型案例盘点	19
一、2022 年全国破获虚拟货币案件整体情况	20
二、2022 年已破获虚拟货币典型案例盘点	21
第六章 2021 年至 2022 年虚拟货币跨境资金分析	25
一、2022 年虚拟货币跨境资金各季度流动情况	27
二、2021 年至 2022 年虚拟货币跨境资金流动情况	28
第七章 2022 年区块链安全事件综合分析	29
一、2018 年至 2022 年区块链安全事件发展趋势	30
二、2022 年区块链安全事件季度数量及损失金额	31
三、2022 年区块链安全事件各类型数量及损失金额	32
四、2022 年区块链安全事件被攻击项目损失金额 TOP10	34
五、2023 年展望	37

第八章 2022 年区块链安全与犯罪领域关键词	38
一、百日行动	39
二、反洗钱	39
三、惩治电诈	40
四、FTX 破产	40
五、Luna 崩盘	40
六、行业监管	41
七、跨链攻击	41
八、Rug Pull	41
九、哈希赌博	42
十、数藏遇冷	42
第九章 2022 年 NFT 相关非法活动分析	43
一、各区块链 NFT 相关数据	44
二、NFT 相关非法活动类型	46
三、监管现状和 NFT 链上溯源分析工具	48
第十章 2022 年网络赌博的新形态和难点	49
一、区块链在网络赌博中的应用	50
二、区块链应用带来的问题和难点	53
三、网络赌博生态趋势	55
第十一章 2022 年虚拟货币诈骗“八宗最”	58
一、最“屡试不爽”——投资	59
二、最“以假乱真”——虚假 APP	59
三、最“言听计从”——老年人	59
四、最“老调重弹”——杀猪盘与杀洋盘	59
五、最“笑里藏刀”——熟人	60
六、最“巧立名目”——智能合约	60
七、最“呼群结党”——Telegram	60
八、最“单刀直入”——OTC 诈骗	60
第十二章 2022 年国内虚拟货币监管情况	61
一、2022 年国内虚拟货币相关监管政策	62
二、2022 年国内虚拟货币“挖矿”相关监管政策	64
附录：关于知帆科技和知帆学院	66



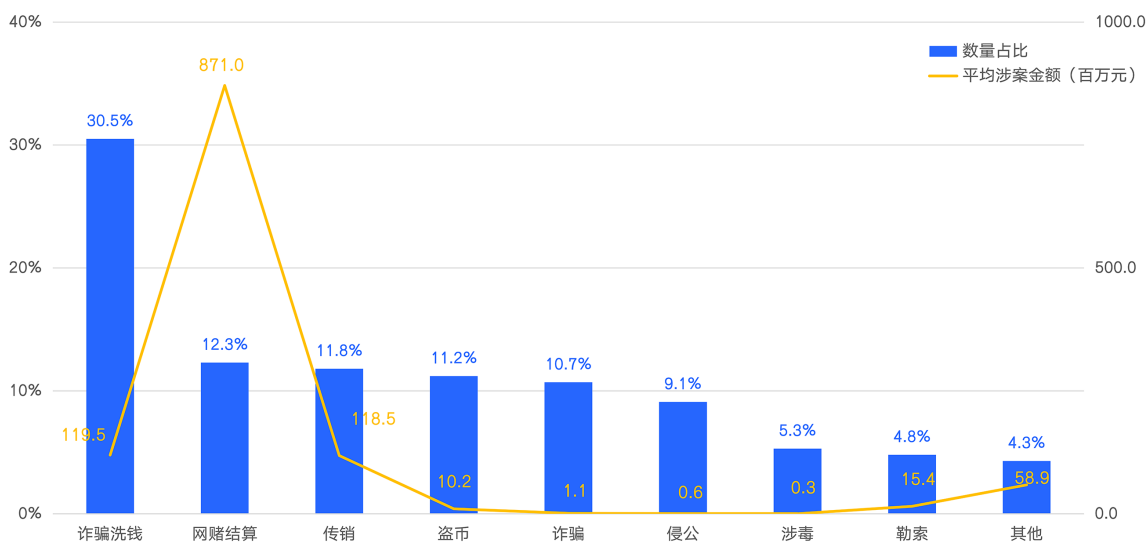
第一章

2022年虚拟货币犯罪案件 综合分析

本章中，根据知帆科技 2022 年服务全国执法机关的数百条有效案件数据进行了调研和分析，从案件数量、类型分布、涉案金额、币种分布等维度，揭示了利用虚拟货币犯罪的发展现状。

一、2022 年虚拟货币犯罪主要类型及平均涉案金额

2022年虚拟货币犯罪主要类型及平均涉案金额



知帆科技

本章中的诈骗洗钱类指的是上游犯罪为各类型网络诈骗，下游关联到利用虚拟货币为交易媒介的洗钱平台的案件；诈骗类型则为直接诈骗虚拟货币的案件；网赌结算类指的是与网络赌博平台相关联的结算平台利用虚拟货币为交易媒介为其提供非法资金流转的案件，该结算平台通常为多个犯罪团伙提供服务。

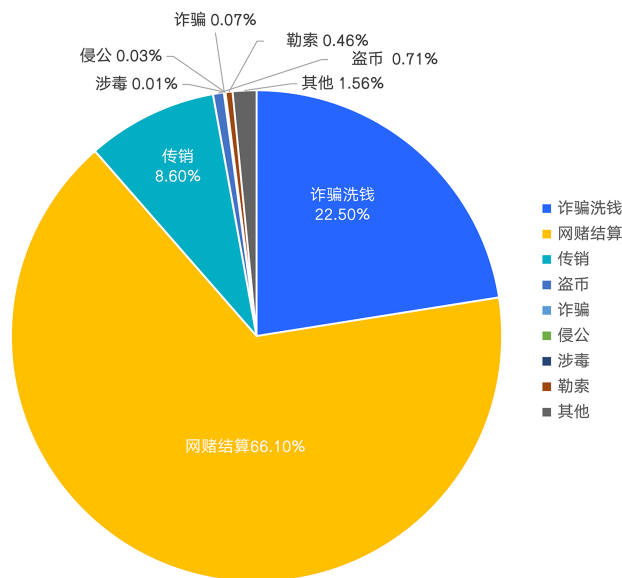
2022 年，诈骗洗钱类案件数量位居首位，占总数量的 30.5%，远高于其他类型。其次为网赌结算类案件，占总数量的 12.3%。传销类案件，排在第三位，占总数量的 11.8%。

从主要类型的平均涉案金额看，网赌结算类案件的平均涉案金额最高，达到 8.71 亿元。主要因为该类型涉案金额统计的是结算平台中整个的资金流水，不仅包含该网赌的资金还包含了该结算平台相关的其他黑灰产资金。

诈骗洗钱类案件在数量和涉案金额上都相对较高，平均涉案金额排在第二位，为 1.19 亿元。传销类案件平均涉案金额排在第三位，为 1.18 亿元。

二、2022 年虚拟货币犯罪主要类型累计涉案金额

2022年虚拟货币犯罪主要类型累计涉案金额



知帆科技

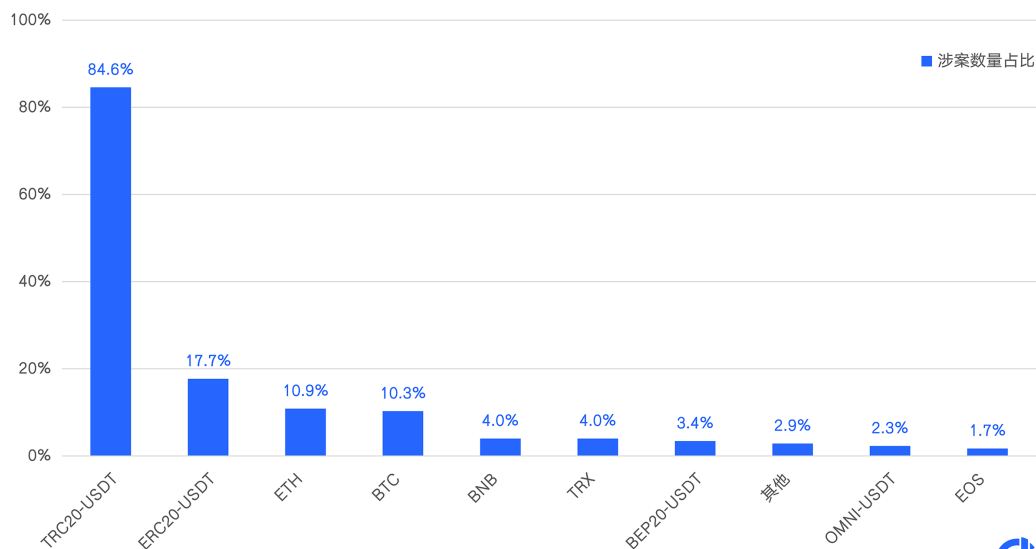
从主要类型的累计涉案金额看，主要为网赌结算类案件和诈骗洗钱类案件，这两类占比超过 88%，其中，网赌结算类案件的累计金额位居首位，占有虚拟货币犯罪案件总涉案金额的 66.1%。其次为诈骗洗钱类案件，占比 22.5%。

由此可见，无论是从数量上还是涉案金额上，网赌结算类都是最主要的虚拟货币犯罪类型。虚拟货币由于存在匿名性、去中心化、追踪难、全球流通性、交易便捷性、交易模式的复杂性、交易之后的不可撤销性、持有方式的多样性、价值认定标准存在争议性等一些特点，因此具有较高的洗钱风险。

我国虽是禁止了虚拟货币，但国际上许多地区和国家还是默许虚拟货币流通的，虚拟货币可以自由兑换成全球货币，犯罪分子加以利用也让虚拟货币逐渐沦为新的洗钱工具。另外，国家有关部门近年来不断加大打击网络犯罪的力度，传统洗钱渠道遭遇沉重打击，也让虚拟货币洗钱的现象加剧。

三、2022 年虚拟货币犯罪主要涉案币种分布

2022年虚拟货币犯罪主要涉案币种分布



知帆科技

从2022年虚拟货币犯罪案件涉案币种分布看，有一部分案件涉及了多个币种，USDT（泰达币）涉案比例最高，占据了绝对主力位置。

USDT（泰达币）是Tether公司推出的一种将加密货币与法定货币美元挂钩的虚拟货币，是稳定币的一种，它与美元稳定在1:1的比值，并且它能和所有的虚拟货币自由兑换，这样稳定币就成了虚拟货币世界与法币之间的桥梁。USDT作为使用最为广泛的稳定币，一方面起到了法币入金媒介作用，涉案人会使用法币购买USDT，然后再兑换为其他虚拟货币；另一方面，由于其价值相对稳定，也被不法分子用于洗钱或转移非法收入等用途。

USDT是在一系列不同的区块链中发行的，如：OMNI-USDT是基于BTC（比特币）网络的OMNI协议、ERC20-USDT是基于ETH（以太坊）网络的ERC-20协议、TRC20-USDT是基于TRON（波场）网络的TRC-20协议。

具体来看，由于波场区块链上的TRC20-USDT在转账速度、拥堵情况、手续费等方面有明显优势，因此被越来越多的虚拟货币犯罪使用，位居首位，占比高达84.6%，超过八成的案件都涉及TRC20-USDT。以太坊区块链上的ERC20-USDT占比则为17.7%，排在第二位。ETH和BTC占比相对偏低，分别为10.9%和10.3%，排在第三位和第四位。

2022年4月14日，公安部刑事侦查局相关领导在国新办新闻发布会上表示，从资金通道看，传统的三方支付、对公账户洗钱占比已减少，大量利用跑分平台加数字货币洗钱，尤其是利用USDT（泰达币）危害最为严重。从上图的币种分布趋势来看也印证了这一点。



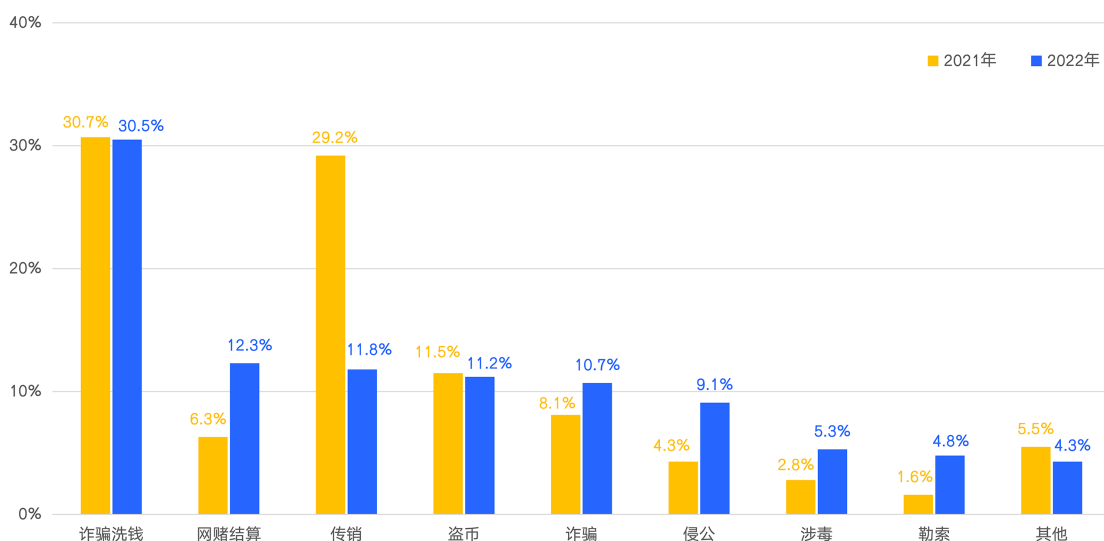
第二章

2021年至2022年虚拟货币 犯罪案件发展趋势

本章中，将知帆科技 2021 和 2022 年服务全国司法机关有效案件数据进行对比分析，从案件数量、类型分布、涉案金额、币种分布等维度，以此透视利用虚拟货币犯罪的发展趋势。

一、2021 年至 2022 年虚拟货币犯罪主要类型数量发展趋势

2021-2022年虚拟货币犯罪主要类型数量



知帆科技

2021 年和 2022 年对比来看，数量上的趋势主要为：诈骗洗钱类依然最多，传销类变少，网赌结算类变多。具体来看，诈骗洗钱类案件数量都为 30% 左右，保持持平，并且都位居首位。这与电诈案件数量多以及电诈案件在洗钱环节绝大部分都利用到虚拟货币不无关系。

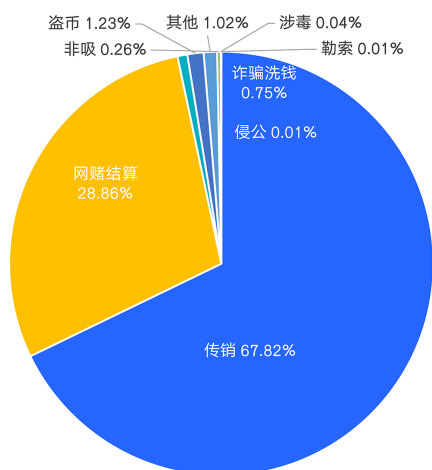
网赌结算类案件数量从 2021 年的 6.3% 增至 2022 年的 12.3%，同比增长 95%。此类犯罪通常与电诈、暗网、洗钱、赌博网站、非法游戏等黑产相互交织。犯罪团伙分工明确，有的负责推广为其提供赌博服务，有的则负责推广 USDT 跑分平台，为境外网络赌博网站提供非法支付结算服务。

传销类案件数量从 2021 年的 29.2% 下降至 2022 年的 11.8%，同比下降 59.5%。主要是因为 2021 年 9 月 24 日，央行、银保监会、网信办、外汇局等十部委发布了《关于进一步防范和处置虚拟货币交易炒作风险的通知》，《通知》明确了虚拟货币不具有与法定货币等同的法律地位，相关业务活动属于非法金融活动，参与虚拟货币投资交易活动存在法律风险。一方面，受此最强监管影响，多个交易所、钱包等服务商开始清退中国大陆用户，暂停了中国大陆新用户的注册，网民购买虚拟货币难度大幅增加，网民参与虚拟货币交易活动变少。另一方面，受《通知》和国家大力反诈宣传的影响，网民防范意识有所提高，对以区块链和虚拟货币为噱头的投资有所防范，不再盲目轻信。

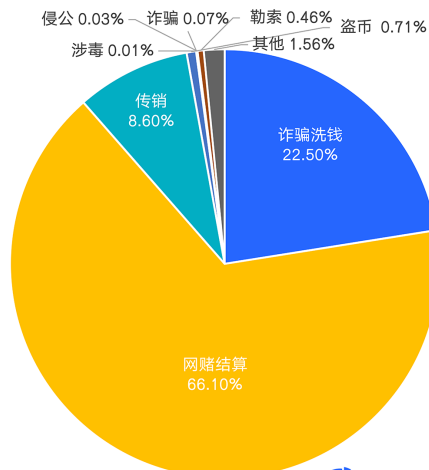
二、2021年至2022年虚拟货币犯罪主要类型累计涉案金额发展趋势

2021-2022年虚拟货币犯罪主要类型累计涉案金额

2021年主要类型涉案金额占比



2022年主要类型涉案金额占比



知帆科技

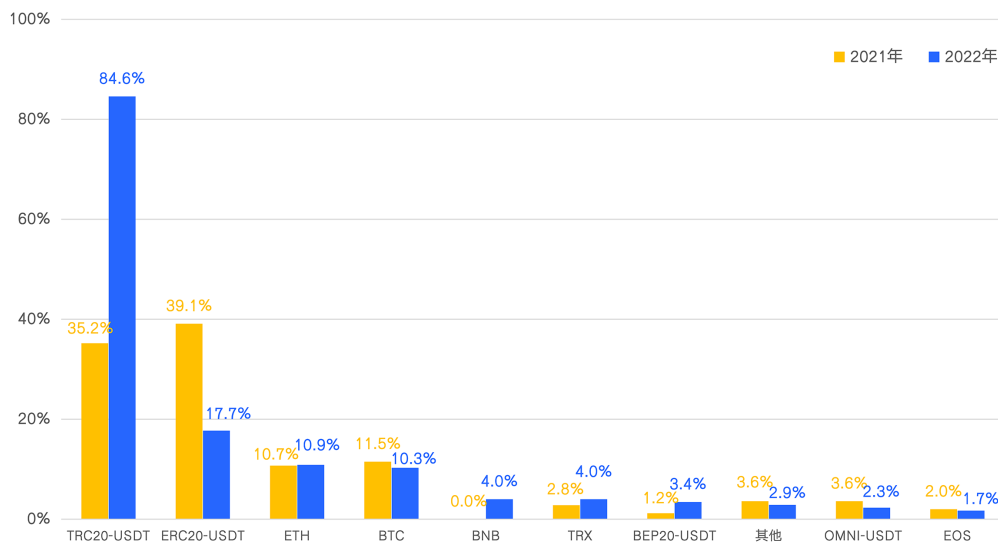
从近两年的主要类型总涉案金额看，主要为传销类案件和网赌结算类案件，2022年最大的变化有两点，一是传销类总涉案金额大幅降低；二是网赌结算类总涉案金额大幅上升。

2021年，传销类位居第一，占有虚拟货币犯罪案件总涉案金额的67.82%。网赌结算类排在第二，占比28.86%。2022年，网赌结算类跃居首位，占有虚拟货币犯罪案件总涉案金额的66.10%。其次为诈骗洗钱类，占比22.50%。传销类则排在第三，仅占8.60%。

另外，数据显示2022年诈骗洗钱类总涉案金额也有明显上升，这种趋势再次表明了诈骗洗钱类和网赌结算类是当前主要的虚拟货币犯罪类型。

三、2021年至2022年虚拟货币犯罪主要涉案币种发展趋势

2021-2022年虚拟货币犯罪主要涉案币种分布



知帆科技

在2021年和2022年的主要涉案币种中，USDT都是最主要的涉案币种，主要为以太坊区块链上的ERC20-USDT和波场区块链上的TRC20-USDT。

2021年，ERC20-USDT位居首位，占比39.1%；TRC20-USDT则排在第二，占比35.2%。2022年，ERC20-USDT下降至17.7%，同比下降约55%，跌落至第二位；TRC20-USDT跃居首位，增至84.6%，同比增长约140%，远高于其他币种。

由于波场链上的TRC20-USDT在转账速度、拥堵情况、手续费等方面有明显优势，从2020年开始，越来越多的虚拟货币犯罪使用到TRC20-USDT，这一趋势在2022年变得更加明显，表明波场链上的TRC20-USDT已经成为当前虚拟货币犯罪中使用频率最高的币种。



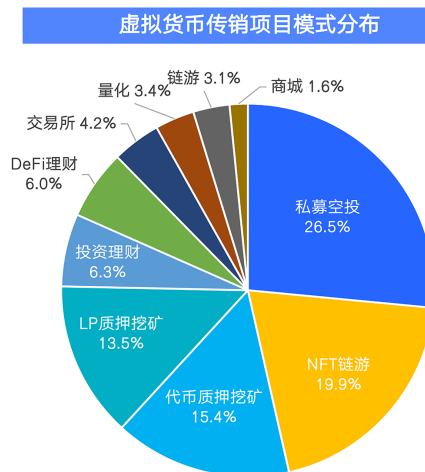
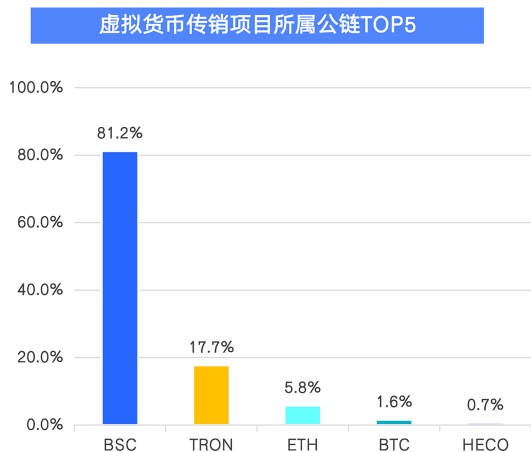
第三章

2022 年虚拟货币传销和 赌博项目分析

本章中，根据知帆科技安全团队获取到的 2022 年近两千个疑似有传销风险和赌博行为的虚拟货币项目数据进行了调研分析，从所属公链、模式、类型、趋势等维度，揭露了 2022 年虚拟货币传销和赌博项目的发展现状。

一、2022 年虚拟货币传销项目所属公链和模式分布

2022年虚拟货币传销项目所属公链和模式分布



知帆科技

从所属公链分布看，部分虚拟货币传销项目涉及多个公链，主要为 BSC（币安智能链）和 TRON（波场链），占比分别为 81.2% 和 17.7%。其他链占比都相对较少。2022 年，虚拟货币传销项目偏爱 BSC，超过八成的传销项目部署在 BSC 上，这主要因为 BSC 是目前最受欢迎的公链之一，生态发展比较好，用户和项目基数明显高于其他公链。

从项目模式分布看，2022 年，私募空投模式的虚拟货币传销项目位居首位，占总数量的 26.5%。其次为 NFT 链游模式，占总数量的 19.9%。代币质押挖矿和 LP 质押挖矿，排在第三位和第四位，分别占比 15.4% 和 13.5%。

二、2022 年虚拟货币传销发展趋势

知帆安全团队结合数据并调研分析后，总结出 2022 年的虚拟货币传销的发展趋势：

① 发布代币的公链以 BSC 为主

近两年，BSC 发展迅速，公链生态较好，已经成为最受欢迎的公链，用户、项目和 DAPP 数量明显高于其他公链，受基数影响，在 BSC 上的传销项目也随之上升。由于 BSC 兼容性相对较好、钱包关联相对便捷、本身的 Gas Fee（矿工手续费）相对低廉，吸引大量用户的同时也促进了智能合约的交互，使得 DeFi 市场更加活跃。据公开数据显示，截至 2022 年 12 月底，BSC 上 DAPP 数量高达 4500 余个，位居首位，高于 ETH（3600 余个）和 TRON（1400 余个），BSC 在 2022 年新增地址数超过 1 亿个。

② 向去中心化模式发展

随着 DEX（去中心化交易所）的快速发展、DAPP（去中心化应用程序）技术逐渐成熟，越来越多的传销项目选择 DEX+DAPP 的方式。一方面，上线去中心化交易所没有门槛，人人都可以发行代币并上线去中心化交易所；另一方面，还可以利用去中心化交易所的机制，通过 LP 质押来收割主流币。

③ 私募空投项目兴起

基于前文所述之因由，发币几乎没有门槛，导致空气币泛滥，私募空投项目数量大幅上升，其中很大一部分代币智能合约中就自带传销机制。炒作的噱头天花乱坠，一会儿元宇宙、一会儿 DAO、一会儿 IDO，其实最后都是新瓶装旧酒，拉人头就有奖励的传销项目。

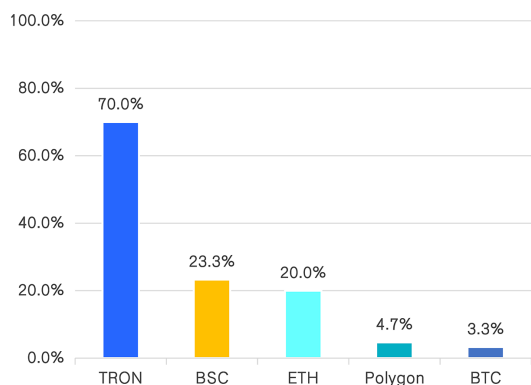
④ 资金规模下降

对比前些年传销项目的资金规模，2022 年单个项目资金规模下降明显，大多数都在百万级跑路，借助去中心化交易所实现“短平快”。

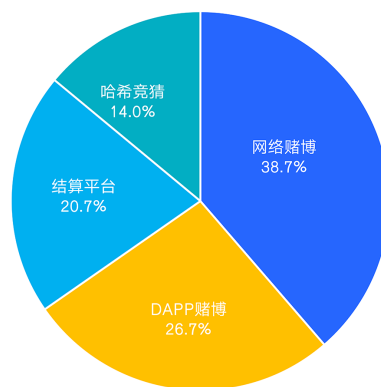
三、2022 年虚拟货币赌博项目所属公链和模式分布

2022年虚拟货币赌博项目所属公链和模式分布

虚拟货币赌博项目所属公链TOP5



虚拟货币赌博项目模式分布



知帆科技

从所属公链分布看，部分虚拟货币赌博项目涉及多个公链，TRON（波场链）位居第一，占比70.0%。BSC（币安智能链）和ETH（以太坊），排在第二和第三位，占比分别为23.3%和20.0%。2022年，虚拟货币赌博项目偏爱TRON，超过七成的赌博项目部署在TRON上。

2022年，基于区块链智能合约开发的网络赌博平台的数量和使用人数继续增加。从项目模式分布看，网络赌博模式的虚拟货币赌博项目位居首位，占总数量的38.7%。其次为DAPP赌博模式，占总数量的26.7%。结算平台和哈希竞猜，排在第三位和第四位，分别占比20.7%和14.0%。

四、2022 年虚拟货币赌博发展趋势

知帆安全团队结合数据并调研分析后，总结出 2022 年的虚拟货币赌博的发展趋势：

① TRC20-USDT 为主要支付通道

虚拟货币已发展为重要的网络赌博平台出入金通道，波场链上的 TRC20-USDT 转账速度快、转账手续费低，在国外认可度高，已形成固定市场，变现通道多。

② 网络赌博同虚拟货币洗钱、非法支付等活动之间的联系更加紧密

赌博项目通常与多种黑灰产业链相关交织，为最大程度洗钱，各种中心化和去中心化结算平台应运而生，这些平台支持 OTC 功能、无限生成新地址、具备 C2C 交易模块等，为各大网赌平台提供各式各样的支付通道，使得洗钱更加隐蔽。

③ 哈希竞猜模式项目成为新型赌博模式

此模式开发难度低，只需要静态网页即可，无须注册和实名，玩家有钱包地址即可参与。哈希竞猜模式就是玩家通过给赌博网站提供的地址进行转币作为投注，该笔转账交易随机生成的交易哈希值最后几位作为开奖结果，如满足此前设定的规则，从而确定游戏输赢，若玩家赢了则自动将所赢虚拟货币转入玩家地址。

④ 追逐热点赛事

如 2022 年卡塔尔世界杯、电子竞技相关赛事等。



第四章

2017年至2021年 虚拟货币刑事文书综合分析

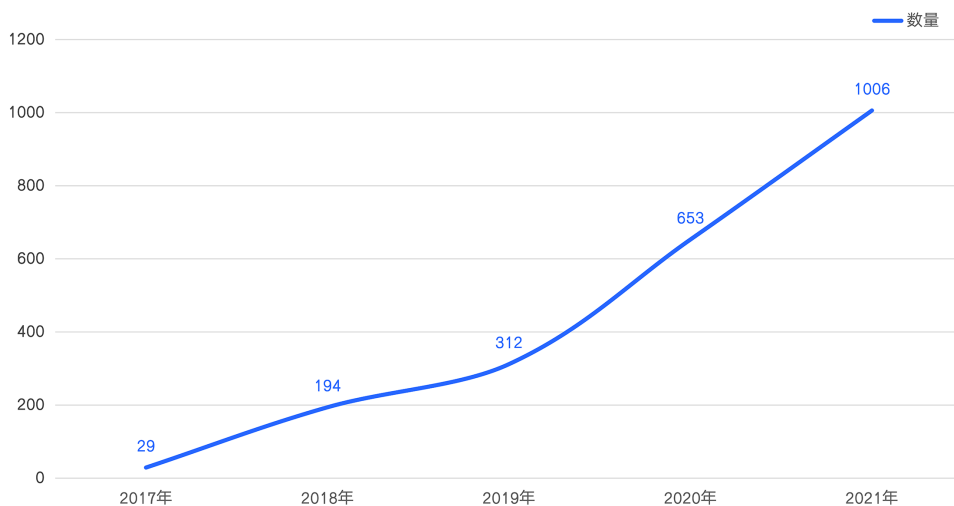
本章中，基于对知帆科技虚拟货币案例信息库收录的 2300 余篇虚拟货币相关的刑事裁判文书进行检索、统计和分析，以此来揭示 2017 年至 2021 年涉虚拟货币相关犯罪案件的发展趋势（因为裁判文书公开有延迟性，部分裁判年份为 2022 年的文书还未公开，防止对真实数据造成干扰，故本次统计时间为 2017 年至 2021 年）。

知帆安全团队认为，数据的意义在于精准，统计方法不当将造成统计数据失真：虚拟货币这一词相对广义，不仅包含比特币、以太币等去中心化加密货币还包含了很多种市场上用于社区内各种虚拟商品交易的虚拟货币，如网络积分、游戏币、社交网站发行的各类“代币”（如 Q 币）。所以在裁判文书网检索“虚拟货币”关键词后的统计结果将远大于真实数据，此时需要对检索后的文书进行逐篇审核才能保证数据的真实性。另外，检索多个关键词后直接对数据做求和的方法也是不当的统计方法，此种统计方法会导致极大部分的文书被重复统计，对数据的真实性造成极大的干扰。

知帆安全团队在源头上确保数据真实性，在收录前对文书进行逐篇审核、清洗、去重和归类等操作。为防虚拟货币文书有遗漏，还选择了“BTC（比特币）”、“USDT（USTD、泰达币、U 币）”、“以太币（ETH、以太坊）”、“加密货币”等更有针对性的关键词进行检索。

一、2017 年至 2021 年虚拟货币相关刑事裁判文书发展趋势

2017-2021年虚拟货币相关刑事文书数量

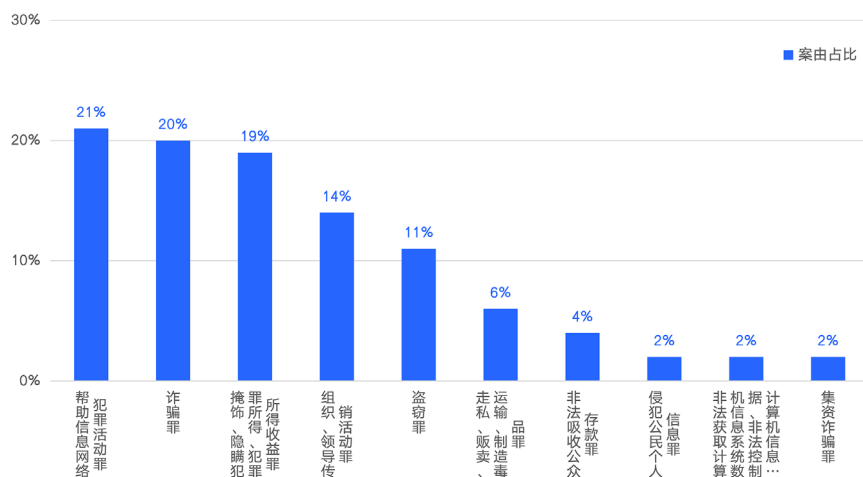


知帆科技

从整体数量上看，2017 年至 2021 年之间，随着利用虚拟货币犯罪愈演愈烈，虚拟货币相关的刑事文书的数量呈逐年上升趋势。从 2017 年的 29 篇连续递增至 2021 年的 1006 篇。

二、2017年至2021年虚拟货币相关刑事文书案由分布

2017-2021年虚拟货币相关刑事文书案由分布

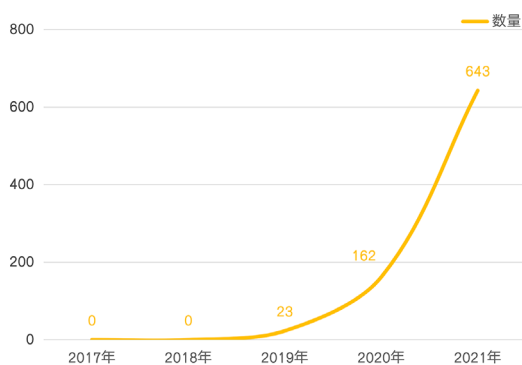


知帆科技

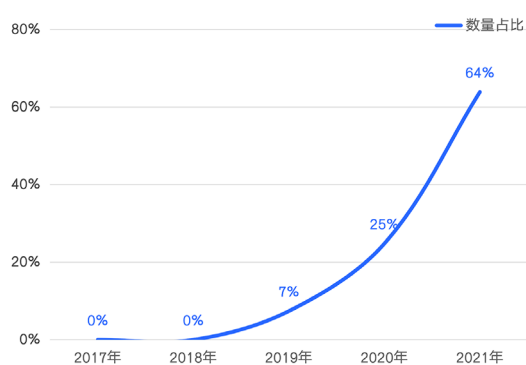
从所有虚拟货币相关刑事文书的案由分布上看，在2017年至2021年之间，案由占比最多的是帮助信息网络犯罪活动罪，占比为21%。诈骗罪排名第二，占比为20%。掩饰、隐瞒犯罪所得、犯罪所得收益罪则占比为19%，排在第三位。

2017-2021年虚拟货币洗钱类刑事文书数量

虚拟货币洗钱类刑事文书数量



洗钱类占有所有虚拟货币刑事文书比例

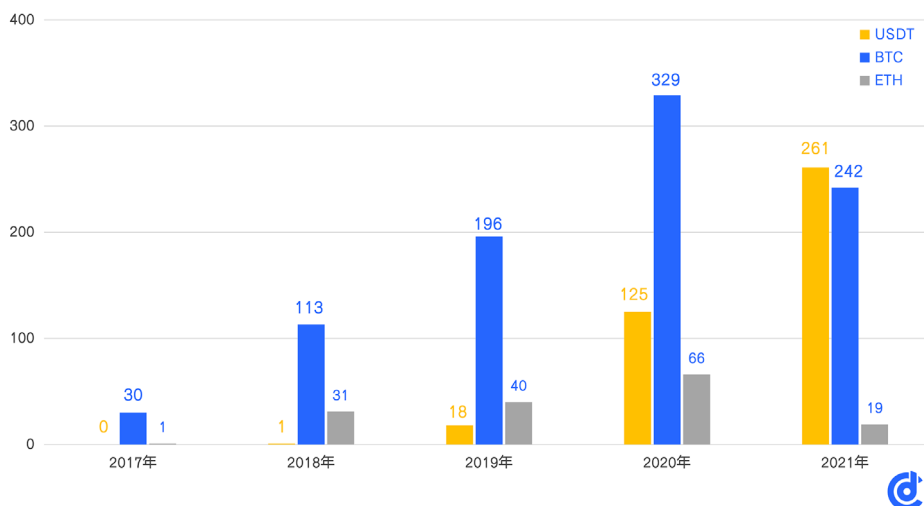


知帆科技

我们将判为帮助信息网络犯罪活动罪，掩饰、隐瞒犯罪所得、犯罪所得收益罪和洗钱罪的判决书归为虚拟货币洗钱类刑事文书，这三种案由基本都是表现形式为洗钱的违法犯罪活动。根据上图显示，虚拟货币洗钱类刑事文书呈逐年上升的趋势，尤其在2021年，较2020年同比上升297%，占比也从2020年的25%增至2021年的64%，由此可见，近些年，虚拟货币已经逐渐沦为洗钱新工具。

三、2017年至2021年虚拟货币相关刑事文书主要涉及币种发展趋势

2017-2021年主要币种相关的刑事文书数量

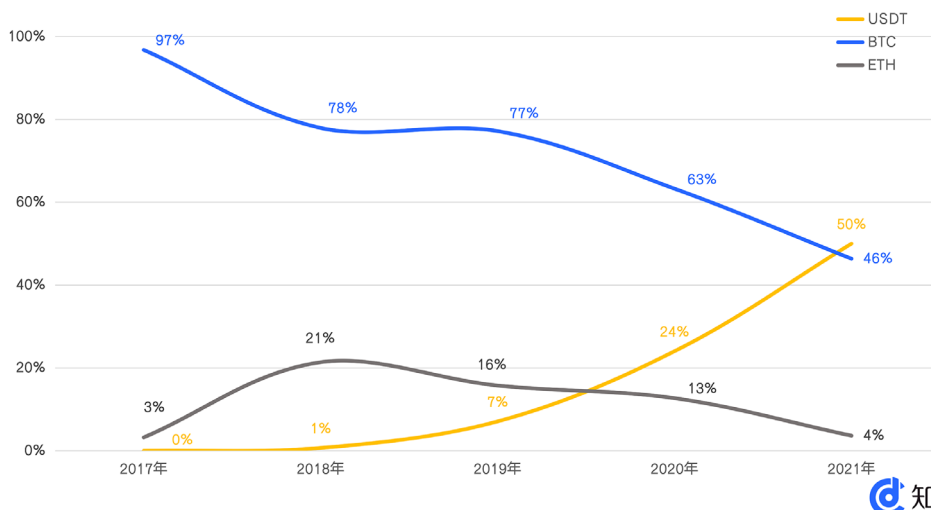


在公开的虚拟货币相关刑事文书中，只有部分文书提及了涉案虚拟货币币种，知帆安全团队对所有文书进行币种关键词组检索和去重处理，统计出每年的币种相关联文书数据，在保证数据真实性的前提下，以此来揭示虚拟货币相关刑事文书主要涉及币种发展趋势。

根据上图数据显示，2017年至2021年，BTC（比特币）相关的刑事文书总数量最多，为910篇。其次是USDT（泰达币）相关的刑事文书，总数量为405篇。最后是ETH（以太币）相关的刑事文书，总数量为157篇。

其中，BTC相关的刑事文书数量在前四年呈上升的趋势，在2020年达到峰值，到2021年时有所下降。USDT相关文书则在五年间，都呈现上升趋势，在2021年达到峰值，超过BTC的数量，跃居第一。ETH相关文书数量偏少，其在2020年达到峰值之后急剧下降。

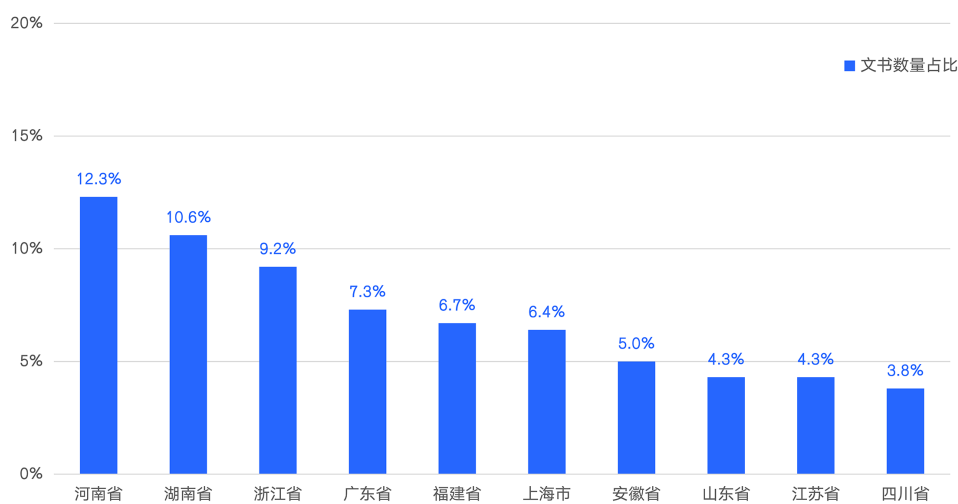
2017-2021年虚拟货币相关刑事文书的币种占比



2017年至2021年，BTC相关刑事文书占比呈现逐年下降的趋势，此消彼长，USDT相关刑事文书占比呈现逐年上升的趋势。2017年至2020年，BTC相关刑事文书占比都是排在第一位，并且占比都在六成以上，这一趋势在2021年发生变化，BTC相关刑事文书下降至46%；USDT相关刑事文书上升至50%，超过BTC相关刑事文书。

四、2017年至2021年虚拟货币相关刑事文书分布省份TOP10

虚拟货币相关刑事文书分布省份TOP10



知帆科技

2017年至2021年，虚拟货币相关刑事文书数量最多的是河南省（12.3%），其次是湖南省（10.6%）、浙江省（9.2%）。



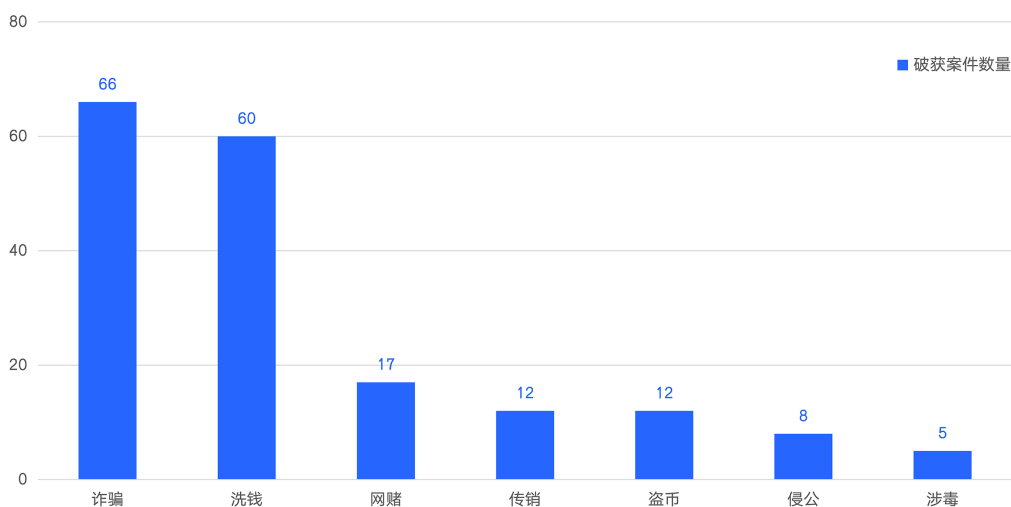
第五章

2022 年全国破获虚拟货币 案件和典型案例盘点

本章中，基于知帆安全团队收集的媒体公开披露的 2022 年已破获虚拟货币案件进行统计和分析，并且对 2022 年已破获的虚拟货币典型案例做了盘点。

一、2022 年全国破获虚拟货币案件整体情况

2022年全国破获虚拟货币案件类型分布



知帆科技

根据不完全统计，2022 年全国公安机关破获各类虚拟货币相关案件 190 余起，其中有部分案件公布了涉案金额，此部分已破获虚拟货币案件总涉案资金流水达 1064 亿元。福建、湖南、浙江报道的涉虚拟货币案件最多。

从案件类型分布看，2022 年全国破获的虚拟货币案件中，诈骗类型数量有 66 起，位居首位，成为打击最多的虚拟货币犯罪类型。其次是洗钱类型，有 60 起。网赌则排在第三位，数量 17 起。这与电信诈骗案件在洗钱环节绝大部分都利用到虚拟货币、我国打击治理电信网络诈骗新型违法犯罪持续保持高压打击态势有关。

从省份分布看，浙江、湖南、福建、江苏、广东等省破获虚拟货币案件的报道比较多。2022 年 6 月 22 日，公安部在全国开展为期 100 天的夏季治安打击整治行动——百日行动，各地公安机关攻坚克难，大力整治社会治安乱象，侦破了众多重点案件，打掉了一大批犯罪团伙。从百日行动公开的报道看，全国大部分省份都有破获涉虚拟货币案件，据不完全统计，破获的涉虚拟货币案件总计 40 余起，主要类型同样是诈骗和洗钱，诈骗类中养老诈骗、“杀洋盘”案件尤为突出。

二、2022 年已破获虚拟货币典型案例盘点

(一) 虚拟货币诈骗

近年来电信诈骗案件高发，特别是区块链、虚拟货币概念的火热，给了更多犯罪分子可乘之机。

许多犯罪分子利用受害者对于虚拟货币认识不足，骗取受害者信任，引导投资并进行资金诈骗。另外，近年来随着国内反诈宣传和对虚拟货币诈骗打击力度的加大，一些犯罪分子将目光转向了海外，操作专门针对外国人的新型诈骗“杀洋盘”。

2022 年虚拟货币诈骗相关典型案例：

1、2022 年 1 月 18 日，池州市警方破获利用区块链技术非法获取计算机系统虚拟货币数据案，涉案价值约 5000 万元人民币，并依法冻结 600 万元的虚拟赃款。2021 年 6 月，受害人王某用手机上网时发现某款数字钱包首页上新发布了一个项目，觉得有利可图，便投资了价值约 59 万元人民币的虚拟货币。次日凌晨发现自己质押的虚拟货币全部被项目方转走，另外还卷走了其他投资者质押的近 800 万美元数字资产，并关闭了网站访问，失联跑路。据统计，该项目受害人达数百人。

2、2022 年 6 月 14 日，琼山警方接到张某报警称其遭遇养老诈骗，被骗数百万元，琼山警方立即抽调精干警力成立专案组进行侦办。经过半个多月的缜密侦查，一伙以刘某为首，组织严密、分工明确、专门针对中老年人实施诈骗的犯罪团伙逐渐浮出水面。7 月 8 日，专案组集中收网，一举抓获刘某等 9 名涉案人员。经调查，犯罪嫌疑人专门以中老年人作为诈骗目标，经常对其嘘寒问暖以取得信任，随后向其灌输投资虚拟货币维卡币赚钱的思想，而该虚拟货币为典型的互联网金融骗局，无论货币如何增值，一经购买便无法兑现。该案涉案金额高达 2000 余万元，受害人 100 余名。

(二) 虚拟货币洗钱

由于虚拟货币本身具有匿名性，不利于监控和追踪，这些特性受到了从事地下钱庄以及洗钱业务的犯罪分子的热衷。

犯罪分子利用虚拟货币的去中心化和匿名性，代替了传统法币洗钱，形成了更加严谨成熟的黑灰产产业链。这类案件上下线层级较多，并且大多都是单线联系，导致案件分析追踪上存在很多困难。

2022 年虚拟货币洗钱相关典型案例：

1、衡阳县公安局“2021.9.15”专案组从刘某被诈骗 780 万入手，深度研判，缜密侦查，2021 年 12 月、2022 年 7 月分别在海南、广东、福建、江西等地多次开展收网行动，全链条捣毁了以洪某某为首的洗钱犯罪集团，抓获犯罪嫌疑人 93 人，捣毁洗钱、跑分窝点 10 余个，

缴获涉案手机、电脑 100 余台，查封冻结涉案资金 3 亿元，为受害人挽回经济损失 780 万元。该犯罪集团利用虚拟货币交易的方式洗钱金额高达 400 亿元。

2、2022 年 7 月，内蒙古自治区公安厅经侦总队联勤中心向通辽市公安局科尔沁分局下发人民银行呼和浩特支行预警：发现犯罪嫌疑人石某园在我局辖区办理的建设银行卡内资金流水异常，月流水交易量 1000 余万元，涉嫌洗钱犯罪。经过前期研判发现，该犯罪团伙利用区块链兑换虚拟货币帮助上游犯罪集团进行涉案资金清洗。2022 年 12 月，通辽市公安局科尔沁分局在内蒙古自治区公安厅经侦总队和通辽市公安局经侦支队的全力指导下，抽调 200 余名警力赴 17 省、自治区、直辖市，分线出击、锐力攻坚，历时三个月，一举打掉一特大利用网络区块链兑换数字虚拟货币洗钱团伙，抓捕犯罪嫌疑人 63 名，扣押涉案现金 3200 万元，涉案固定资产价值 1800 余万元，扣押并转出区块链数字货币价值人民币 7500 余万元，冻结涉案资金 500 余万元，共计收缴违法所得约 1.3 亿元。

（三）虚拟货币传销

随着去中心化金融（DeFi）技术的发展，越来越多的传销项目开始通过智能合约的形式运行，将合约代码上传后自动执行，传销的参与者通过数字钱包参与，传销项目也不再需要财务、技术、维护等人员，大大增加了打击难度。

2022 年虚拟货币传销相关典型案例：

1、2021 年 5 月，重庆沙坪坝警方接群众张某报警，称妻子王某在家休产假期间，无心照料小孩，整天邀约亲朋好友加入某网络组织，参加网上刷单，并缴纳会费、发展下线，疑似陷入传销组织。经民警初查，确认王某陷入新型网络传销，民警循线深挖，一个网络传销组织浮出水面。在市公安局经侦总队统筹指导下，沙坪坝警方成立专案组，全力侦办。2022 年 3 月，专案组奔赴浙江、安徽等地开展集中收网行动，抓获犯罪嫌疑人 7 名，涉案资金 8.6 亿余元，涉及传销会员 22 万余名，遍布全国 21 个省市。

2、2022 年 5 月，昆明市公安局呈贡分局经侦大队接到上级公安机关有关“526 某平台”“530 某平台”涉嫌犯罪的两条线索。呈贡分局立即成立专案组开展研判、侦查工作。2022 年 5 月 31 日前，云南省昆明市公安局呈贡分局经侦大队警方兵分多路，分别在义乌、深圳、昆明、文山、曲靖等地发起收网行动，成功捣毁两个跨多省区市作案的网络传销平台和团伙，抓获主要犯罪嫌疑人 20 名。现场查获现金、微信、支付宝资金 120 余万元，冻结价值 1700 万元的虚拟货币，查获涉案手机 30 余部、车辆 1 辆、电脑 4 台、银行卡 30 余张。目前，4 名犯罪嫌疑人被依法刑事拘留，16 人被监视居住。自 2021 年 3 月以来，平台发展会员 1 万余人，会员分布全国 20 多个省区市，吸纳资金 4.5 亿元。

（四）虚拟货币盗窃

随着虚拟货币市场规模的扩大和价值的飞升，虚拟货币本身也成了不法分子的犯罪目标。

犯罪分子利用植入木马病毒等黑客手段，侵入受害者电脑，盗窃受害者的钱包私钥、助记词等钱包相关信息，进行盗窃。这种新型犯罪，主要针对一些刚接触虚拟货币的新人，他们在下载相关软件时误点击木马链接，下载安装了带有病毒的软件，导致自己的虚拟货币被黑客盗取。

2022 年虚拟货币盗窃相关典型案件：

1、2022 年 2 月 28 日，浙江省温州市公安局瓯海区分局网安大队接到受害人报警，称其在 TG 群里，被人盗走 25 万泰达币，价值人民币 160 余万元。瓯海警方立即开展侦查，成功锁定一个以张某祥为首，包含上游盗币、木马制作和下游洗币在内的全链条黑客团伙。6 月 22 日，瓯海警方组织警力分赴黑龙江齐齐哈尔和广东广州、廉江等地开展收网，抓获犯罪嫌疑人 9 名，扣押电脑 11 台、手机 15 部，冻结房产 13 处、查获豪华轿车 3 辆，涉案金额超 1 亿元。

2、2022 年 2 月 26 日，南昌市市民黄某报案称，在 2 月 23 日晚上 18 点左右，手机号码被人莫名挂失，然后他发现自己手机号绑定的某外域账号中的区块链货币，包括雷达币和比特币被人全部转走，失窃的这些虚拟货币价值上千万元。专案组奔袭上千公里到达江苏连云港，在当地转战 10 天，将 4 名犯罪嫌疑人抓获，其中邓某、张某丽和王某苗是女子，而张某 1 是男子，警方从邓某家中缴获了 140 余万现金，以及大量用于作案的手机、电脑和各种伪造的证件。

（五）虚拟货币赌博

虚拟货币发展的同时也使各类线上赌场更加猖獗，网络赌博案件大多为跨境赌博，这类案件追踪难度大，资金难以监控追回，侦破难度高。

目前，虚拟货币已发展为重要的网络赌博平台出入金通道，网络赌博同虚拟货币洗钱、非法支付等活动之间的联系更加紧密。基于区块链上哈希数据的随机性进行的哈希赌博正在发展为新的赌博模式。

2022 年虚拟货币赌博相关典型案件：

1、2022 年 3 月，安徽省池州市东至县公安局破获一起跨境赌博案件，抓获犯罪嫌疑人 14 名，依法冻结涉案资金 5000 余万元，涉案资金流水近 100 亿元。警方调查发现，国内互联网上多个赌博网站的线索均指向同一个赌博集团。该赌博集团旗下共运营有 5 个赌博网站，实际运营地点在菲律宾，网站会员人数总计高达 20 余万人。近 3 年的赌资充值款接近 100 亿元人民币。赌客将赌博资金充入上分卡后，一部分资金流入到下分卡，也就是赌客进行提现的卡。大部分的资金流入了跑分平台。赌博集团依托跑分平台进行跑分，之后大部分资金再流入三方支付的通道。三方支付，再通过撮合交易、虚假交易，虚拟货币的买卖，再进行大量资金的一个洗白。

2、2022 年 5 月，内蒙古自治区鄂尔多斯市东胜区警方接到线索称，当地多人参与境外

网络赌博。经过两个多月侦查，专案组查明该赌博平台共发展境内参赌人员 3780 人，境内代理人员 511 人，关联账户交易流水金额 64 亿余元。9 月，专案组抽调 300 名警力划分 25 个抓捕小组迅速奔赴广东、福建、河北、黑龙江等 20 余个省区市展开抓捕。截至目前，警方共抓获涉案人员 151 人，打掉“洗钱”团伙 4 个，彻底斩断了这起特大跨境网络赌博案的组织链条。



第六章

2021 年至 2022 年 虚拟货币跨境资金分析

近两年，区块链上的非法活动情况依然活跃，虚拟货币交易本身有着跨国性的特点，在强监管、严监管下，所有境内虚拟货币交易所无法在境内运营，并停止对境内用户提供服务。然而随着境内交易所纷纷选择出海，一批服务器设在境外、但能够在境内登录的虚拟货币交易所依然被大众使用，仅凭境内禁止平台交易已无法有效阻止虚拟货币交易市场的运行。

本章内容基于知帆科技自主研发的虚拟货币地址标注模型系统，对已标注数据进行分析，以此来揭示虚拟货币跨境资金流动情况。以下为数据说明：

一方面，严格意义上讲，境内已经没有合法的虚拟货币交易所；另一方面，虚拟货币交易所的服务，不仅面向境内交易者还面向全球的虚拟货币交易者。所以，很难完全准确地界定哪些资金来源境内和境外，但是各大交易所的创立背景和主要面向的客户群体还是有境内外之分。

中国背景的交易所：在国内创立，主要为中国用户提供服务的交易所。比如：Binance（币安）、Huobi（火必）、OKX（欧易）等。

非中国背景的交易所：在国外创立，主要为非中国用户提供服务的交易所。比如：Coinbase、FTX 等。

流入资金：非中国背景交易所流向中国背景交易所的虚拟货币资金总额。

流出资金：中国背景交易所流向非中国背景交易所的虚拟货币资金总额。

虚拟货币价格：虚拟货币本身作为一种投资商品，价格是浮动的，币种价格取的是该币种在当月的月平均价格。

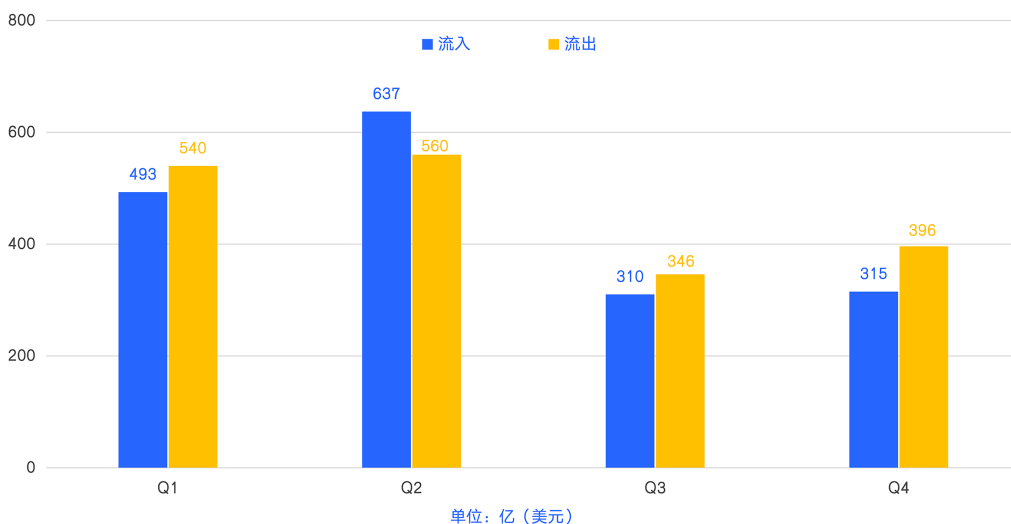
金额单位：因为资金量级较大，为了便于统计和展示，单位为：亿（美元）。

数据来源：知帆科技自主研发的虚拟货币地址标注模型系统对已标注数据的分析。

误差说明：在界定交易所是否为中国背景存在一些主观性，此处可能会造成一些误差；虚拟货币地址量级过大，存在标注不全的情况，此处可能会造成一些误差；有些币种的价格浮动较大，取的是月平均值，此处可能会造成一些误差。

一、2022 年虚拟货币跨境资金各季度流动情况

2022年虚拟货币跨境资金各季度流动情况

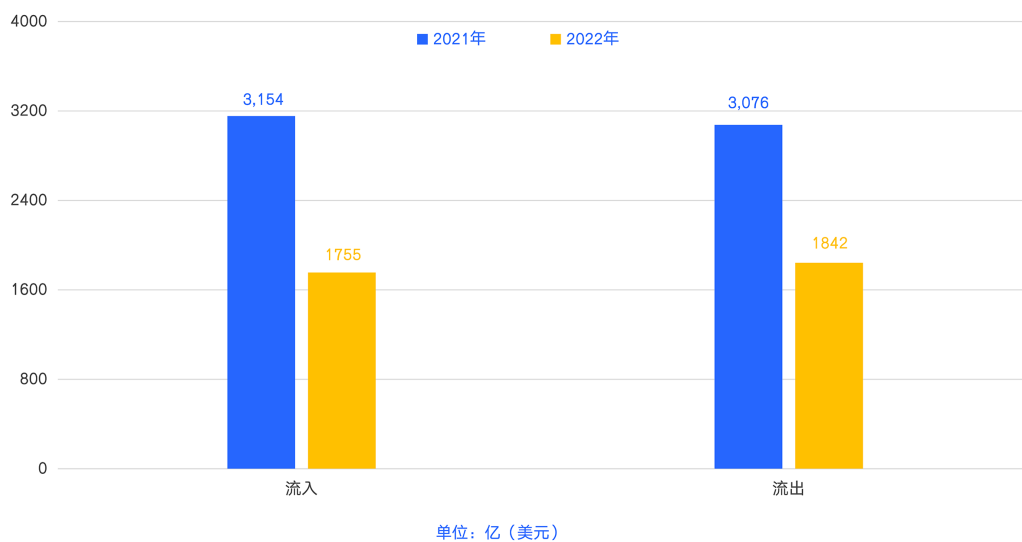


知帆科技

2022 年虚拟货币跨境资金总流入 1755 亿美元，总流出 1842 亿美元，Q2 季度虚拟货币跨境资金流动最为活跃，流入和流出金额均为最高，流入 637 亿美元，流出 560 亿美元。相较 2022 年上半年，2022 年下半年资金流动有所下降，Q3 季度的流入金额和流出金额均为最低，流入 310 亿美元，流出 346 亿美元。

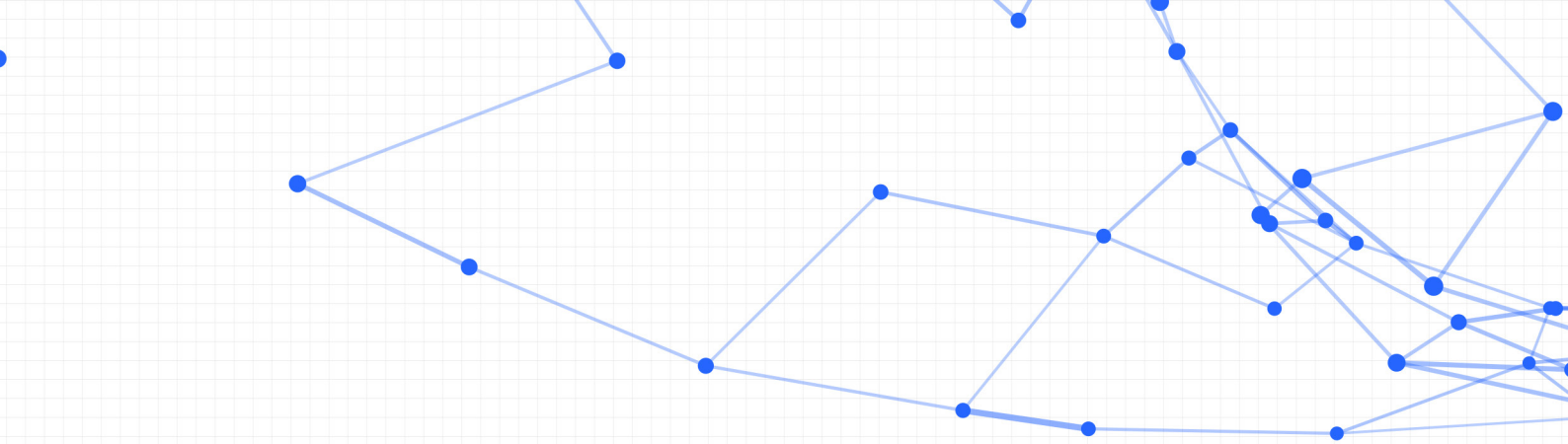
二、2021 至 2022 年虚拟货币跨境资金流动情况

2021-2022年虚拟货币跨境资金流动情况



根据数据显示，虚拟货币跨境流入资金从 2021 年的 3154 亿美元下降至 1755 亿美元，同比下降 44.3%。虚拟货币跨境流出资金从 2021 年的 3076 亿美元下降至 1842 亿美元，同比下降 40.1%。

由此可见，无论是流入还是流出，2022 年虚拟货币跨境资金整体资金规模相比 2021 年都有所下降。



第七章

2022 年区块链安全事件 综合分析

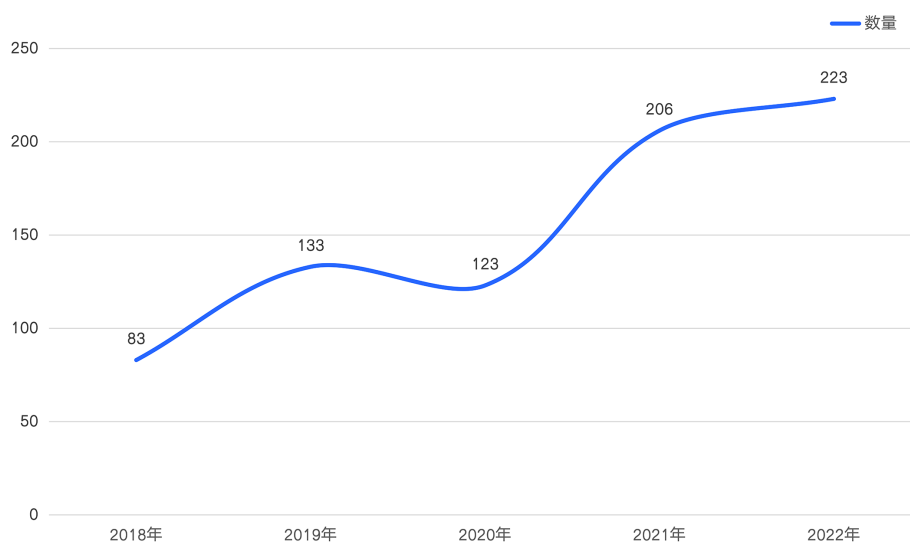
2022年，区块链和虚拟货币行业未能延续2021年的高速发展。一方面，推动上一轮虚拟货币行业发展的DeFi、NFT、GameFi等热点概念不同程度的遇冷，行业内部没有新的概念和引擎出现；另一方面，虚拟货币市场内部高杠杆、资金挪用等情况积累的系统化风险在熊市爆发，由Luna、三箭资本、FTX交易所等项目或机构爆雷影响了行业内的投资者和参与者的信心。

虽然如此，2022年里区块链和虚拟货币行业在部分领域也取得了一些可喜的进步。第二大公链以太坊终于完成了The Merge进入了PoS时代，在提高区块链可扩展性方面二层网络蓬勃发展，在一些细分赛道中仍然有新的模式在不断涌现。

本章中，基于收集的2022年区块链安全事件进行统计和调研，通过数量趋势、类型分布、损失资金等维度，对区块链安全事件发展趋势进行综合分析。区块链安全事件包括：规模偏大的诈骗、私钥泄漏、闪电贷攻击、合约漏洞以及其他类型的攻击。其中诈骗指的是Rug Pull、钓鱼攻击、钓鱼邮件等形式的国外诈骗事件。

一、2018年至2022年区块链安全事件发展趋势

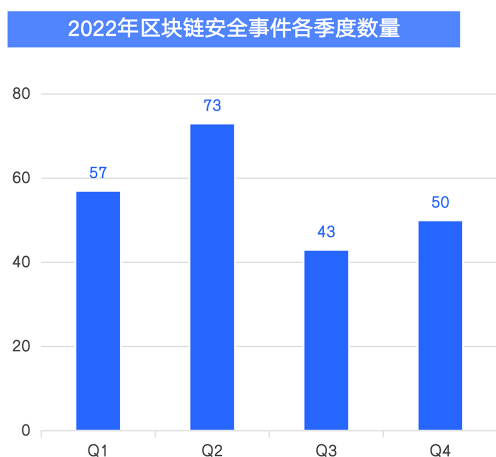
2018年至2022年区块链安全事件数量



据不完全统计，2022年发生了223起安全事件，相比较2021年（206起）上升8.3%。在过去五年中，区块链安全事件数量整体呈上升趋势。很大程度上可以归因于从DeFi协议中窃取资金的持续增长。DeFi协议由于代码开源可以被网络犯罪分子研究寻找漏洞，特别容易受到攻击遭受损失。自2020年开始，DeFi类项目被盗资金所占比例稳步上升，DeFi成为黑客攫取资金的摇篮。

二、2022 年区块链安全事件季度数量及损失金额

2022年区块链安全事件各季度数量及损失金额



知帆科技

2022 年 Q2 季度区块链安全事件数量最高，为 73 起，其次是 Q1 季度，为 57 起。Q3 季度数量最低，为 43 起。

在损失金额方面，由于 2022 年虚拟货币市场受到熊市的影响，整个市场虚拟货币价值下跌，2022 年全年区块链安全事件损失累计金额为 33.27 亿美元，只占 2021 年的 30% 左右。需要注意的是，损失金额中并不包括 Luna、FTT 等因市场动荡而崩盘损失的资产。其中 Q1 季度季度损失金额最高，达到 12.8 亿美元，Q3 季度损失金额最低，为 4.88 亿美元。

具体来看，今年开年，被盗资金、数量“稳步上升”，在 3 月份 Ronin Network 爆出惊天大雷后震惊整个市场，也一举将该月被盗资金推向顶峰。

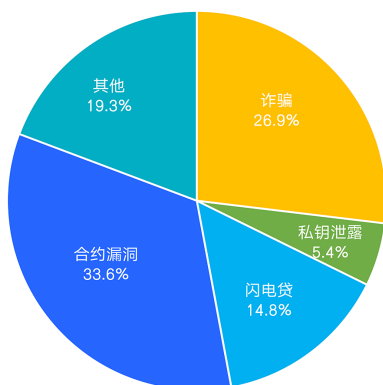
2022 年 5 月，Luna 发生死亡螺旋后，安全事件被盗资金呈断崖式下跌。在整个市场处于低迷的情况下，2022 年 Q3 季度虚拟货币损失了 4 亿余美元。

2022 年 10 月，情况发生了变化，整个虚拟货币市场好像沦为了黑客的提款机，BNBChain、Mango 被攻击，涉及资金均逾上亿美元。值得注意的是，包括 Mango 在内一天里有 5 个虚拟货币平台遭受攻击，其余 4 家分别为：RabbySwap、ParaSwap、TempleDAO 和 QANplatform，累计损失近 1.2 亿美元。10 月成为有史以来黑客活动量最大的一个月。紧随其后的两月并没有像 10 月份这么疯狂，可能由于市场动荡，有利可图的机会大大减少，所以案件数量、金额都下降很多。

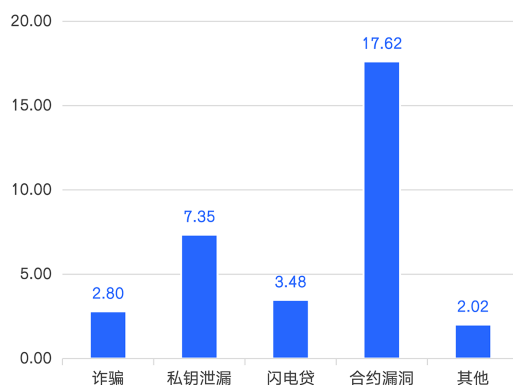
三、2022 年区块链安全事件各类型数量及损失金额

2022年区块链安全事件各类型数量及损失金额

2022年区块链安全事件各类型数量



2022年区块链安全事件各类型损失金额（亿美元）



知帆科技

2022 年合约漏洞类型的区块链安全事件数量占比最高，占比 33.6%，诈骗事件数量占比 26.9%，排在第二，合约漏洞和诈骗成为最主要的区块链安全事件类型。

2022 年损失金额最高的区块链安全事件是合约漏洞类型，高达 17.62 亿美元。其次是私钥泄露类型，为 7.35 亿美元，诈骗类虽然数量较多，但是整体损失金额偏低。

2022 年损失资金主要在 BSC 和 ETH 上，一方面因为这两个链很受欢迎，其用户基数大、转账速度快、协议丰富，成为黑客攻击的主要目标；另一方面，混币平台是黑客转移资金时的首选，小到几十万美元大到上亿的虚拟货币被盗后，都会有黑客将资金转入混币平台混币，而许多混币平台都在这两个链上运行。

诈骗包括 Rug Pull、钓鱼攻击等其他诈骗的案件，目前 Rug Pull 类案件数量占诈骗类的 80%。Rug Pull 也被称为“欺诈 Token”或“DeFi 诈骗”，是一种常见的虚拟货币骗局，往往发生于 DeFi 领域，通常是指项目方突然放弃某一个项目或撤出流动性池子，卷走用户投资资金的诈骗行为，通俗地讲就是卷款跑路。Rug Pull 相关项目方会在智能合约中精心设计代码，将一些不合规矩的代码脚本隐藏在代币里，之后通过包装自己来吸引他人投资，当资金池内价值代币达到一定数量时，他们就会恶意抛售代币或者直接取走池内资金从而让自己获利。在今年 10 月 Freeway 项目方宣布停止服务、删除了官方名单并且实施了 Rug Pull，涉及金额或超 1 亿美元。这是目前为止该类事件中被骗金额较大的一起事件。

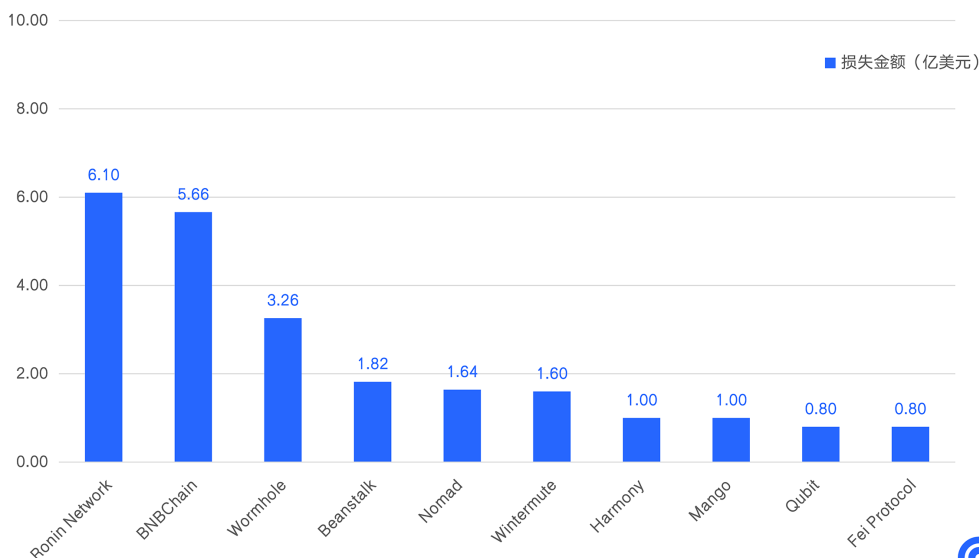
反观合约漏洞类案件，黑客瞄准的都是热度高、资金量大的项目，这类项目在发展过程中很容易在合约代码层面产生一些漏洞从而被黑客利用。震惊行业的 Nomad 被攻击事件，就是由于项目方合约存在漏洞，导致全民都加入了这场抢钱狂欢。

除此之外，已发生 30 余起闪电贷攻击事件，虽然被盗资金只占整体的 10% 左右，但是其与诈骗类案件都是近年来常见的安全问题。Elephant Money 可以说是今年典型的闪电贷攻击受害者，其未经验证的合约 (0xd520a3b) 使用 Uniswap pair 池作为价格预言机，因此为预言机被攻击埋下伏笔，酿成损失。

私钥泄漏类事件虽然数量不多，但是被盗金额不低。私钥可以简单理解为一串长字符串，拥有这串字符串的人可以轻易地将我们地址内资金任意使用。只要黑客掌握了项目方的私钥，那么存在地址上的资产将会全部被转移。2022 年发生的 Ronin Bridge 和 Harmony 被盗事件都是由私钥泄漏引发的骇人听闻的大事件。

四、2022 年区块链安全事件被攻击项目损失金额 TOP10

2022年区块链安全事件被攻击项目损失金额TOP10



知帆科技

在被攻击项目损失金额 TOP10 中，前 8 个被攻击项目涉及资金都超过 1 亿美元，Ronin Network、Wormhole、Nomad、Harmony、BNBChain 均是跨链桥项目。

近年来，区块链公链越来越多，却因缺乏主流虚拟货币资产，需要使用跨链桥从以太坊等公链上获取资产，导致市场对跨链桥的需求越来越大、各个跨链桥上存有大量资金。另外跨链桥项目自身合约会存在意想不到的漏洞，容易被黑客利用。所以黑客将目标瞄准了跨链桥，盗取了大量的资金。

值得注意的是朝鲜黑客组织 Lazarus 对跨链桥情有独钟，今年发生在 Ronin Network、Harmony、deBridge 等项目的被攻击事件中均可以看到该组织的影子。

简单介绍这 10 起被攻击事件的过程：

① Ronin Network

基于以太坊的 Ronin Bridge 被黑客入侵并盗取了 173600 枚以太坊和价值 2500 万美元的 USDC，总价值超过了 6 亿美元。这一攻击已经成为了 DeFi 史上最大的攻击，超过了 Poly Network 黑客事件。该起事件可以追溯到 2021 年 11 月，当时 Sky Mavis 请求 Axie DAO 帮助分发免费交易，因为用户负载巨大。Axie DAO 允许 Sky Mavis 代表其签署各种交易。这已于 2021 年 12 月停止，但未撤销许可名单访问权限。一旦攻击者获得了 Sky Mavis 系统的访问权限，他们就能够通过使用无 gas RPC 从 Axie DAO 验证器获取签名。黑客也正是通过这点，获取了 Ronin Bridge 的私钥，然后将虚拟币全部转移出来。在资金方面，黑客已经将

盗窃所得通过跨链桥全部转化为 BTC。

② BNBChain

此次 BSC 链攻击涉及多个跨链，并且金额庞大，成为历史最高的黑客攻击之一。黑客于区块高度 21955968 通过调用系统 RelayerHub 合约 0x1006 缴纳 100 BNB 注册成为 Relayer，然后对系统 CrossChain 合约 0x2000 发起攻击。黑客对 BSC 跨链桥发起攻击，利用币安跨链桥 BSC Token Hub 的漏洞，两次攻击共获取了 200 万枚 BNB，并转入钱包 0x489...79BEc。随后黑客通过 Venus 的借贷服务，抵押了 90 万个 BNB，并从该平台贷出 6250 万枚 BUSD、5000 万枚 USDT 和 3500 万枚 USDC。币安立即采取措施暂停所有通过 BNB 链的存取款，直到有进一步的更新。

③ Wormhole

专门桥接各种 DeFi 的 Wormhole 遭到黑客入侵，被盗走 120,000 个 wETH，市价约 3.2 亿美元。具体经过为黑客通过一次很小金额来测试之前被披露过的漏洞。轻而易举就获得了一个函数，并通过外部的合约绕过 Wormhole 的协议验证进而骗取了 120,000 个 wETH，并成功转走了 93,750 ETH，剩下的 wETH 被紧急锁定在了 Solana 中。

④ Beanstalk

去中心化稳定协议 Beanstalk 受到闪电贷攻击，损失了大约 1.82 亿美元的加密货币，攻击者从中获利近 8000 万美元。在本轮攻击中，黑客使用了“闪电贷”（flash loan）的方式利用协议的治理机制，并将资金发送到黑客所控制的钱包。黑客借了 8000 万美元价值的加密货币，并将其存放在项目的筒仓中，从而获得了足够的投票权，并换取能够通过任何提案。有了这个权力，他投票决定将 Beanstalk 库内的虚拟资产转移给自己，然后再归还投票权，提走存放的资金，并立即偿还了贷款——这一切都在几秒钟内完成。

⑤ Nomad

这次 Nomad 漏洞是为数不多的，即便是普通人不懂技术和代码也有机会可以实现的攻击，其甚至演变成 DeFi 史上最大规模、最混乱的“去中心化”抢劫案。Nomad 跨链桥升级合约时有个低级错误，导致普通人也可参与 hack，找到过往成功的交易，然后改下地址重新广播。不过金额是改不掉的，所以黑客也要一笔一笔偷，这给其他人可乘之机，都去哄抢 Nomad 剩余资产，这次被盗案非常特殊的一点在于，这可能是 DeFi 史上最规模、最混乱的去中心化抢劫案，它并非由单个或者数个黑客发起，而是在最初的攻击者发起攻击后，数百个不同的账户发现了这个方式并复制了他们的方式来获取被盗资金，链上资金记录也反映出这一状况。

⑥ Wintermute

与此前“漏洞”、“闪电贷”、“价格操纵”等常见的攻击方式不同，此次黑客盗窃的方式更为冷门——暴力破解。攻击者频繁地利用 0x0000000fe6a... 地址调用 0x0000000ae34... 合约的 0x178979ae 函数向 0x0248 地址（攻击者合约）转账，通过反编译合约，发现调用 0x178979ae 函数需要权限校验，通过函数查询，确认 0x0000000fe6a... 地址拥有

setCommonAdmin 权限，并且该地址在攻击之前和该合约有正常的交互，那么可以确认 0x0000000fe6a... 的私钥被泄露。仅在 Wintermute 被盗数日前，Profanity 的安全风险就已被业界所注意。Wintermute 官方称在上周得知 Profanity 存在漏洞后，加速弃用旧密钥，但由于内部（人为）错误，调用了错误的函数，因此 Wintermute 没有删除受感染地址的签名和执行操作。

⑦ Mango

黑客利用两个拥有 500 万 USDC 的账号 A 和 B，通过铸造 MNGO 的永续合约来操纵 Mango 现货市场价格，将 MNGO 价格从 0.03 美元推高至 0.91 美元，4.83 亿份 MNGO 的价值便达到了 4.23 亿美元，随后又利用账号 B 的 MNGO 作为抵押品，借出 1.16 亿美元的贷款，此时 Mango 的流动性被耗尽，USDC、MSOL、SOL、BTC、USDT、SRM 和 MNGO 等资产均被抽空，黑客获利 1 亿美元。本来一个常见的闪电贷攻击，但出乎意料的是，或许是为了让自己免于刑事调查或资产冻结，黑客再次现身发起了 DAO 治理攻击。对于被盗走的 1 亿美元，黑客发起提案要求用国库来偿还用户损失，并用盗取的大量治理代币操控投票，让支持率近乎 100%。

⑧ Harmony

由 Layer1 公链 Harmony 开发的以太坊与 Harmony 间的资产跨链桥 Horizon 遭到攻击，损失约为 1 亿美元。Harmony Bridge 是一个跨链桥项目，由五个验证者节点进行操作验证，本次攻击主要原因是由于两个验证者节点的私钥疑似泄露，导致合约的 confirmTransaction 函数被成功调用。本次攻击事件以太坊上损失了 85,867 个 ETH，990 个 AAVE 和 78,500,000 个 AAG，BSC 上损失了 5,000 个 BNB 和 640,000 个 BUSD，共计约 100,428,116 美元。这种项目方因为验证节点较少被攻击的情况在之前就发生过，但是 Harmony 并没有重视。

⑨ Qubit

Qubit 项目的 QBridge 遭受攻击损失约 8000 万美金。本次攻击的主要原因在于在充值普通代币与 native 代币分开实现的情况下，在对白名单内的代币进行转账操作时未对其是否是 0 地址再次进行检查，导致本该通过 native 充值函数进行充值的操作却能顺利走通普通代币充值逻辑，导致本次损失。

⑩ Fei Protocol

Fei Protocol 遭受重入攻击，损失超 28380 ETH，约 8000 万美元，攻击者地址 0x6162759eDAd730152F0dF8115c698a42E666157F。攻击者先从 Balancer: Vault 中进行闪电贷。将闪电贷的资金用于 Rari Capital 中进行抵押借贷，由于 Rari Capital 的 cEther 实现合约存在重入漏洞，攻击者通过攻击合约中构造的攻击函数回调，提取出受协议影响的池子中所有的代币。

五、2023 年展望

2023 年，根据虚拟货币市场四年左右的牛熊周期，市场的寒冬可能会在这一年终结，2023 年可能会成为新的牛市的起点。

然而，过去的经验并不是未来成功的保障。虚拟货币行业需要发展，还需要宏观经济、技术、监管、生态、资本等各个方面都具备相应的条件。

可以预见的是，Web3.0 的需求将越来越被关注，NFT、GameFi、DeFi 和智能合约应用将延续增长趋势，并在 2023 年继续寻找合适的市场产品契合点，努力来提高其可扩展性。更多主流人群将通过各种不同的入口进入这一领域。

公链将仍然是区块链项目争夺的重点，以太坊仍然在保持进化，MEV 将成为新的关注点，新的竞争公链仍然在努力蚕食以太坊的市场占有率和用户数量，二层网络将在公链之争中找到自己的立足之地。2023 年，将有新的公链以“以太坊杀手”的姿态出现，而决定它能否成功的，是能否有基于它的杀手级应用出现。

2023 年，监管机构已经对虚拟货币行业足够了解，针对虚拟资产的监管框架将以更加成熟的形式适时地推出，对于虚拟货币行业的参与者来说，合规意味着虚拟资产真正被主流金融世界认可，从而迎来进入更多主流人群和传统企业资产负债表中的机会。

与区块链技术和虚拟货币生态一同“进化”的还有那些永不疲倦的黑客和攻击者们，他们不会放弃任何一个利用代码漏洞的机会，在新技术的学习赛道上同开发者赛跑。区块链项目的开发者虽然在过去几年中已经交了足够多的学费，但是与黑客之间的这场攻防战是一场永无休止的战争。

对于投资者和项目的参与者来说，在自身财产安全方面需要慎之又慎，谨慎投资，面对各类网络诈骗、网络钓鱼、盗窃等违法活动需要有一定的认知，虽然监管政策也在不断完善，但只有提高自身“防御”能力才能让犯罪分子更加无机可乘。



第八章

2022 年区块链安全与犯罪 领域关键词

2022年，虚拟货币市场持续下行，整体市值缩水2万亿美元，比特币和以太坊两大龙头的价格相较于年初都跌超60%。在种种市场影响因素中，产生决定性影响的，还是全球的宏观金融因素，美联储持续加息，全球流动性紧缩，虚拟货币市场也难逃冲击。

市场的不景气也是整个行业在2022年发展低迷的缩影，在熊市中，行业中一些在高速发展时被忽略的安全问题被暴露，甚至成为了致命的顽疾。

对于虚拟货币和区块链安全行业来说，2022年是监管和执法机构主动出击，大力打击虚拟货币相关犯罪活动的一年。

在公安部等多部门发起的多个专项行动中，大量涉虚拟货币的非法犯罪活动被打击，保护了人民群众的资产安全，维护了社会经济秩序的稳定。

本章中，知帆科技根据2022年度热点事件的分析和统计，结合专家评议，梳理出2022年区块链安全与犯罪领域十大关键词，以此来回顾和盘点2022年的虚拟货币和区块链安全行业。

一、百日行动

2022年夏季，全国各地公安展开“百日行动”，打击突出违法犯罪，大力整治社会治安问题，攻坚化解各类安全隐患，坚决维护社会稳定、保障人民安宁。

在“百日行动”中，多起大型虚拟币相关案件被侦破，如广西来宾破获2.3亿的虚拟币传销案件、湖南衡阳县破获的特大型洗钱犯罪团伙，涉案资金达400亿。

警方的一系列行动，加之2020年至2022年持续在全国开展的“断卡行动”，2022年夏季公安部等多个部门联合开展打击惩治涉网黑恶犯罪的“净网2022”行动，有效遏制和打击了虚拟币犯罪活动。

二、反洗钱

2022年初，公安部等多部门联合制定实施《打击治理洗钱违法犯罪三年行动计划（2022—2024年）》，对加大洗钱犯罪惩治力度作出系统部署安排。

反洗钱是维护国家政治安全、金融安全和积极参与全球金融治理体系建设的重大国家战略，而虚拟货币也正在被越来越多地用于洗钱活动当中，因此也是反洗钱工作的重点之一。

公开数据显示，1月至9月，全国检察机关以洗钱罪提起公诉共计1462人，同比上升142.5%。11月3日，最高检发布5件检察机关惩治洗钱犯罪典型案例，其中包括一件“自洗钱”案件，这是“自洗钱”案件首次入选最高检典型案例。

三、惩治电诈

近几年，电信网络诈骗及其关联犯罪呈多发态势。2022年9月2日，十三届全国人大常委会第三十六次会议表决通过了《中华人民共和国反电信网络诈骗法》，自2022年12月1日起施行。

《中华人民共和国反电信网络诈骗法》共七章50条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任、附则等，坚持以人民为中心，统筹发展和安全，立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑。

在第25条中，明确说明任何单位和个人不得“帮助他人通过虚拟货币交易等方式洗钱”。

四、FTX 破产

2022年虚拟货币行业最大的事件莫过于中心化交易所FTX突然倒闭，数百亿估值从几天内跌至破产，FTX创始人兼首席执行官Sam Bankman-Fried被捕，他将面临美国检察官提出的一系列欺诈指控。

FTX的崩溃暴露了中心化金融的风险管理不善、治理不充分、审计不完整和潜在欺诈等问题，使虚拟行业重新受到严格审查，中心化交易所（CEX）人人自危，争相证明交易所内部资金储备的安全性。

此事件过后，大量用户将自己的资金撤出中心化交易所，存放于非托管钱包，尽管各大交易所纷纷出具审计报告或是出示储备金地址证明，但市场对于中心化交易所的信任流失是不可避免的，中心化机构面临的信任危机不可逆转。

五、Luna 崩盘

Terraform Labs成立于2018年，旨在使用旨在创建去中心化金融网络的区块链技术。区块链使用TerraUSD及其姊妹代币Luna创建算法稳定币系统。

Luna代币的市值一度进入到虚拟货币市值排行榜前十名，但就在2022年5月的几天内，Terra网络分崩离析。

5月7日，当时价值180亿美元的算法稳定币TerraUSD的价格开始波动，并在5月9日跌至35美分。Luna代币价格，在5月12日则从80美元跌至几美分，给虚拟货币市场造成超过4000亿美元的损失，也对方兴未艾的算法稳定币领域造成了致命打击。

六、行业监管

2022 年虚拟货币行业频繁的“爆雷”事件引发了各国监管机构对行业监管的关注。

FTX 事件之后，美国多个监管机构对 SBF 等公司高管提起诉讼，FTX 发行的虚拟货币 FTT 很可能被认定为证券。无论这一事件最终如何发展，这都将完善监管机构对虚拟货币行业的监管法规和合规管理框架。

此外，国外监管机构还加强了对混币洗钱行为的打击，以太坊链上最有影响力的混币平台 Tornado Cash 就被美国财政部列入 SDN 制裁名单。

七、跨链攻击

黑客发起攻击从来不估计牛市还是熊市，哪里聚集了大量的虚拟货币资金，哪里就是他们的攻击目标，2020 年是中心化交易所，2021 年是 DeFi 项目，2022 年则是跨链平台。

2022 年，随着更多高性能公链生态的蓬勃发展，虚拟货币资产跨链的需求也与日俱增，相对应的，不同跨链项目都在多条公链上维护着资金规模庞大的资金池，以支持其客户的跨链需求。跨链桥还结合了多种结构，例如托管人、债务发行人和预言机，这使得跨链桥有些脆弱，黑客可以利用多种方式进行攻击。

从年初的 Ronin Network 开始，到之后的 Wormhole、Nomad、Harmony、BNB chain 等近 20 个跨链项目，黑客通过对跨链项目攻击获取了近 20 亿美元的非法收入。这也使用户对跨链桥的安全问题提出质疑，跨链服务应该加大投入进行代码审计，加强资产安全。

八、Rug Pull

通俗地说，Rug Pull 就是指项目方卷款跑路，是典型的割韭菜的行为。

Rug Pull 通常发生在 DeFi 领域。由于在区块链上创建新代币既便宜又简单，而且无需代码审计，就可以在去中心化交易所（DEX）上发行，这使得 Rug Pull 的犯罪成本相当低廉。

2022 年是较为动荡的一年，据统计，有超过 10 万个用于诈骗的代币被部署，比 2021 年全年增长了超过 40%，这些项目背后的部署者创建代币后，为资金池提供流动性，开始大规模进行宣传，吸引韭菜进场，当代币上涨到一定程度后，项目方又立刻从流动性池中提取所有主流代币，使项目代币价格一落千丈。

九、哈希赌博

2022 年，随着区块链技术和虚拟货币使用的增多，网络赌博也同这些新兴技术结合出现了新的形态，其中最有代表性的就是哈希赌博。

由于每一个区块被开采之前不能明确其区块的哈希值，赌博平台的运营者便利用这个特点制定出诸多针对区块哈希的赌博游戏。

由于区块链透明去中心化等特点，参赌者可以在区块浏览器中自己查询是否中奖，所以这类赌博平台基本不存在作弊的情况，使得这类赌博平台深受赌徒的喜爱，这也助长了这些平台的发展。

十、数藏遇冷

数字藏品，作为 NFT（非同质化代币）在国内的合规形态，一度成为 2022 年我国区块链界最为瞩目的应用，但最终热度过后，仍然没有摆脱成为弃子的命运。

2022 年上半年，在元宇宙、Web3 概念的推动下，数字藏品将公链上风生水起的 NFT 本土化改造移植到了联盟链上，头部科技大厂纷纷入局，一众官方机构扎堆发行数字藏品，一度引发主流媒体的热议。

但是数字藏品本身二级市场方面的监管限制，以及本身商业模式的不完善，使得用户权益难以保证，最终大厂退出，平台清退，虚假繁荣过后，只剩下一地鸡毛。



第九章

2022 年 NFT 相关非法活动分析

NFT（非同质化代币）是过去一年来区块链领域最新出现的概念，其在艺术品、收藏品、区块链游戏、虚拟地产、元宇宙、金融和数字收藏领域都有应用场景，但是同虚拟货币一样，非同质化代币也可以被用于洗钱、诈骗、恐怖主义融资、非法集资、非法意识形态宣传等非法犯罪活动当中。

本章中，基于收集的 NFT 相关数据和安全事件进行统计和调研，通过攻击事件数量、非法活动类型、监管现状等维度对 NFT 相关非法活动进行分析。

一、各区块链 NFT 相关数据

（一）众公链纷纷入场，以太坊独占鳌头

各区块链NFT相关数据

区块链	NFT资产数	NFT合约数	NFT转移次数	持有NFT钱包地址数	NFT交易量
以太坊	119,052,145	182,018	201,069,864	7,432,799	27,812,417ETH 340亿美元
币安链	139,707,286	48,978	347,949,012	16,415,087	1,095,312BNB 2.66亿美元
Polygon	321,459,657	489,816	808,744,299	44,656,731	355,856,672MATIC 2.88亿美元
Solana	30,327,113	93,613	106,788,975	7,452,119	41,965,250 SOL 4.74亿美元
Arbitrum	5,769,352	3,925	19,645,047	1,134,418	15,097ETH 1841万美元
Optimism	4,918,695	17,442	6,578,469	819,681	2,670ETH 325万美元
Avalanche	6,592,163	18,667	15,395,445	592,054	2,268,836AVAX 2656万美元

知帆科技

根据 NFTScan 数据显示（截至 2022 年 12 月底），以太坊 NFT 交易量高达 340 亿美元，位居第一，远高于其他公链。

在 2022 年中，众多公链将 NFT 作为自身发展用户生态、扩展使用场景、与以太坊进行竞争的重要方式，但是无论是交易量还是品牌的认可度，以太坊仍然是毫无疑问的 NFT 第一公链。

(二) 上半年高潮迭起，下半年走势低迷

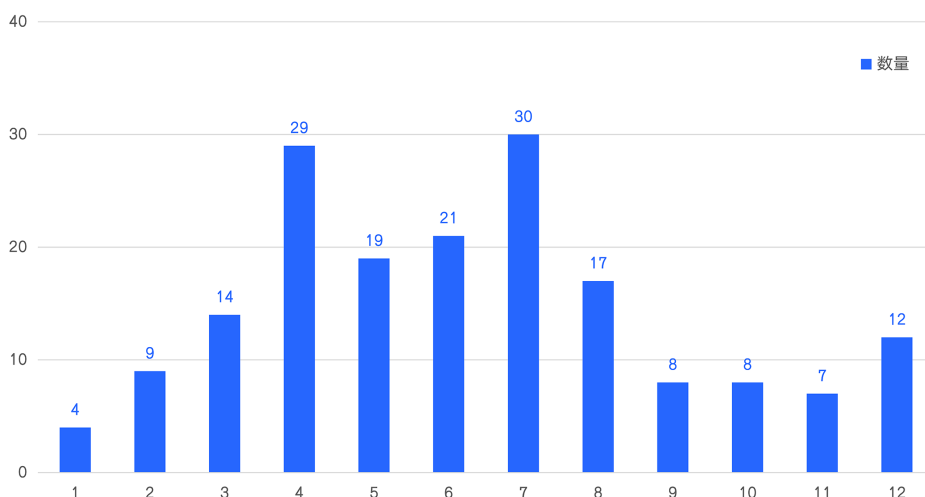
Market Cap & Volume



根据链上 NFT 交易数据可以看到，NFT 交易额在今年 1 月份和 5 月份出现两次高峰，而进入下半年之后，NFT 交易额整体走低。

(三) NFT 相关安全事件激增，Discord 成钓鱼攻击重灾区

2022年NFT相关安全事件月度分布



2022 年，在 NFT 市场蓬勃发展的同时，NFT 相关安全事件频发，特别是很多 NFT 项目使用的社区工具 Discord，频频成为黑客进行钓鱼攻击的工具。在 2022 年中，4 月到 8 月是 NFT 安全事件发生最多的几个月。其中，对 NFT 项目的 Discord 服务器进行攻击占到所有攻击类型中的 44.38%。

二、NFT 相关非法活动类型

(一) 涉政、涉恐等非法活动宣传和融资

虚拟货币自出现以来，由于其去中心化、匿名性的特点，就一直被一些涉政、涉恐等非法组织用作融资渠道。而在 NFT 出现之后，由于其易于和艺术品和收藏品结合的特性，除了被用来融资之外，还在某种程度上起到了意识形态宣传的作用。

以目前全球最大的 NFT 交易平台 Opensea 为例，平台对 NFT 作品的发布者没有有效的审核机制，因此一些涉政、涉恐势力会利用该平台上传、发布宣传非法内容的 NFT 作品，以达到宣传和融资的目的。

(二) 非法集资和投资诈骗

在某些高价 NFT 的带动下，NFT 投资逐渐成为虚拟货币领域最新的投资热点。随着而来的，则是越来越多的非法集资和诈骗项目的出现。

这些 NFT 项目同虚拟货币非法集资和诈骗项目并无本质区别，不同之处无非是，此前的虚拟货币投资诈骗项目使用的是同质化代币，而 NFT 诈骗项目使用的是非同质化代币。

NFT 投资诈骗项目往往会首先发布部分作品图片，这些图片往往是在众包网站中低价请一些设计师设计，或者直接抄袭、剽窃自某个不知名的艺术家，然后通过 Telegram、Discord、Twitter 等社交媒体或聊天软件发布消息、建立社区，有些还会在媒体上付费发文或邀请行业内的意见领袖站台。

在时机成熟时该项目就会开始预售，也就是以相对低的价格小规模发售，预售之后则是规模更大的公开发售。不管是在预售阶段还是在公开发售阶段，诈骗项目都有可能会卷款跑路，这时投资者手中拿到的只有一个一文不值的 NFT 代币。

(三) 洗钱

任何有价值的商品都有可能被用于洗钱活动，非同质化代币也不例外。目前一方面 NFT 的市场规模已经相对较大，很多 NFT 系列作品的价格相对较高；另一方面 NFT 领域目前没有形成合理的定价体系和标准，任何人都有可能创造出天价的 NFT 作品。

据 Chainalysis 公司统计，2021 年下半年开始，进入 NFT 平台的非法资金数量猛增，第四季度进入 NFT 平台的资金接近 150 万美元。其中大部分都是诈骗资金，此外还有来自恶意软件、被制裁实体的资金流入。

使用 NFT 进行洗钱的模式其实和传统的使用艺术品进行洗钱非常相似的，只是过程中增加了虚拟货币兑换法定货币的过程。在传统的艺术品洗钱流程中，洗钱者先是低价购入艺术品，

然后通过市场炒作或自买自卖抬高价格，最终让一个不知情的买家购入该艺术品；NFT 代币也可以这样被用于洗钱，洗钱者不仅可以买入其他人发行的流动性好的 NFT 用于洗钱，还可以自己创建 NFT 洗钱，洗钱手段更加多样，也更加隐蔽。

(四) 钓鱼攻击

但是据知帆安全团队统计，2022 年上半年，在虚拟货币领域涉及 NFT 的安全事件中占比最大的，是 NFT 钓鱼攻击相关事件。

NFT 项目通常都会使用 Discord 软件建立社区维护与收藏者和支持者的关系，这一点也被一些不法分子和黑客所利用。攻击者首先对 NFT 项目在 Discord 上建立的服务器进行攻击，在获得管理员权限之后在相应群组或频道中发布虚假的钓鱼链接，诱骗受害者前往虚假网站按照相应提示进行钱包授权或者将助记词透露给攻击者。

攻击者在控制了受害者的虚拟货币钱包之后，便会将其钱包中的所有 NFT 以及其他虚拟货币转移走，进而完成攻击。

(五) 资金盘或传销盘

NFT 也可以被一些资金盘和传销盘作为推广和运营工具。资金盘项目往往都会向投资者许诺高额收益，操盘手在运营过程中需要想方设法让投资者的钱一直停留在盘内，让他们在获得了一定的收益之后仍然不退出或者继续加大投资。

传统的虚拟货币资金盘往往会使用多种虚拟货币挖矿的方式诱导参与者继续投资，而 NFT 出现之后，资金盘和传销盘则鼓励投资者将前期收益兑换为项目方发行的 NFT，最大限度地让投资者的资金留在盘内。

(六) 侵犯著作权等

很多 NFT 相关的艺术品和收藏品其实还涉及著作权、许可权等方面的问题。

最典型的就是侵犯著作权的问题，据杭州互联网法院消息，该院审理了奇策公司与被告某科技公司侵害作品信息网络传播权纠纷一案，被告将奇策公司创作的漫画“胖虎打疫苗”作为 NFT 数字藏品发布，法院判决被告立即删除涉案平台上发布的“胖虎打疫苗”NFT 作品，同时赔偿奇策公司经济损失及合理费用合计 4000 元。

另外一种侵权的行为是 NFT 购买者将其购买的 NFT 作品用于商业行为，如果该 NFT 在发行时未说明包含相关权益的转让，那么这种行为也是不合法的。

三、监管现状和 NFT 链上溯源分析工具

（一）监管现状

目前在全球范围内都没有有效的 NFT 监管框架，在国内除了此前发布的一些和虚拟货币相关的规定之外，和 NFT 以及数藏有关的主要有以下两个文件。

1、《关于防范 NFT 相关金融风险的倡议》

该倡议由中国互联网金融协会、中国银行业协会、中国证券业协会联合发布，倡议呼吁要坚决遏制 NFT 金融化证券化倾向，从严防范非法金融活动风险”，具体包括不变相发行交易金融产品、不变相开展代币发行融资、不变相违规设立交易场所、不以虚拟货币作为 NFT 发行交易的计价和结算工具等。

2、《数字藏品合规评价准则》（团体标准）

该团体标准对数字藏品的定义、合规发行及流转进行规范。《标准》还明确提出，数字藏品仅限于使用目的流转，不可开展炒作、洗钱、代币化、金融化、证券化等挂牌或私下非法交易流转。

在国际上也没有专门针对 NFT 的监管措施或框架，对 NFT 领域的监管主要集中在某几个领域，具体包括：许可权和著作权领域、NFT 相关的金融风险、NFT 内幕交易、NFT 在洗钱方面的应用等。

（二）链上分析工具

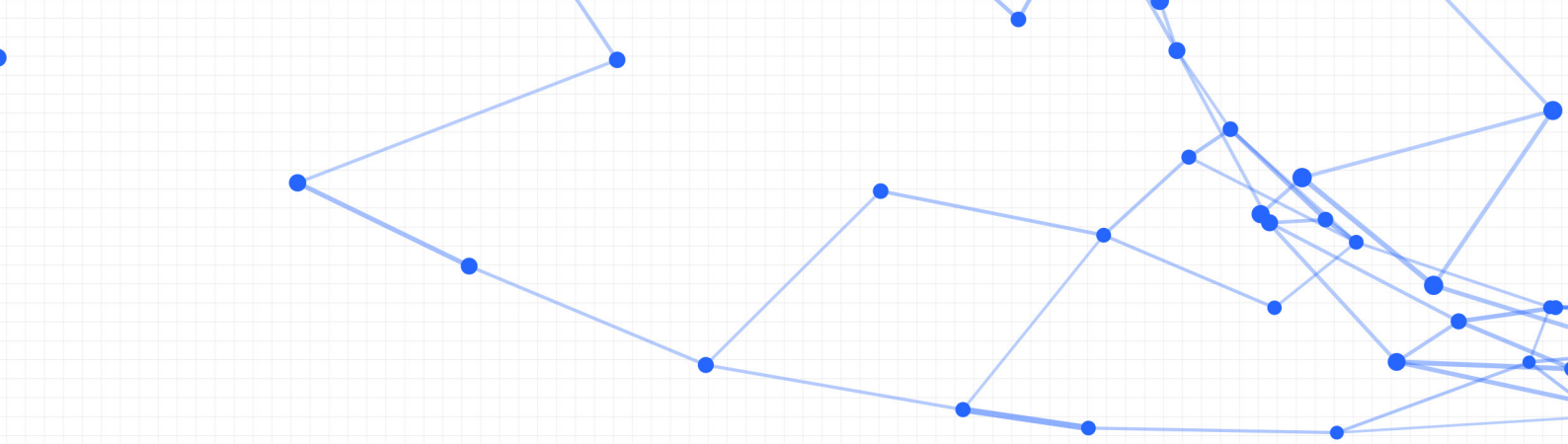
在 NFT 相关案件的分析研判过程中，往往需要对 NFT 的铸造、购买、交易、转移情况进行溯源和追踪。由于 NFT 的所有交易都是在区块链上记录的，所以可以通过链上数据追踪发现 NFT 和非法资金的关联。

1、通过 NFT 交易平台

以全球最大的 NFT 交易平台 Opensea 为例，在每个 NFT 作品的页面下方，都会显示出这个 NFT 相关的历史活动信息，比如转移、出售等。点击右侧的箭头就可以直接通过 Etherscan 等区块浏览器查看具体的交易情况。

2、通过区块浏览器

通过 Etherscan 区块浏览器，可以查看任何一个地址的 NFT 交易情况。目前的 NFT 代币主要通过 ERC721 协议和 ERC1155 协议发行的，所以点击区块浏览器相应地址页面的 ERC721 Token 和 ERC1155 Token 标签，就可以看到和这个地址有关的所有 NFT 交易记录。在特定的交易页面，也可以看到 NFT 代币的转移情况。页面中可以看到交易双方的地址信息、NFT 的转移情况、其他代币的转移情况、交易的手续费等重要信息。



第十章

2022 年网络赌博的新形态 和难点

本报告第三章提到，2022 年网络赌博项目发展趋势：虚拟货币交易已发展为重要的网络赌博平台出入金通道，其中主要为 TRC20-USDT，网络赌博同虚拟货币洗钱、非法支付等活动之间的联系更加紧密；基于区块链智能合约开发的网络赌博平台的数量和使用人数继续增加；基于区块链上哈希数据的随机性进行的哈希赌博正在发展为新的赌博模式。

随着区块链技术的发展和虚拟货币使用的增多，网络赌博也同这些新兴技术结合出现了新的形态。在本章中，结合上述趋势展开论述。

一、区块链在网络赌博中的应用

（一）参与者使用虚拟货币出入金

进入 21 世纪以来，随着互联网的发展，网络赌博活动也在一直发展壮大，但是作为网络赌博的核心环节，收款和提现一直是其发展的瓶颈。

在虚拟货币出现之后，由于其支付去中心化、匿名化的特点，很快就被网络赌博平台用来作为参赌者的出入金通道，成为网络赌博平台收款和提现的新工具。之前曾占据支付通道主要地位的微信、支付宝等第三方支付工具，逐渐被虚拟货币所取代。最受欢迎的虚拟货币包括比特币（BTC）、以太坊（ETH）、泰达币（USDT）和波场币（TRX）等。

比特币（BTC）和以太坊（ETH）是目前市值排名前两位的虚拟货币，其价值相对较高并且被市场普遍认可。锚定美元的泰达币（USDT）价值稳定且支持多个不同的区块链网络。波场币（TRX）则是由于波场链上有较多的赌博应用，因此被很多参赌者使用。

使用虚拟货币可以随时随地进行转账操作，参赌者可以直接使用虚拟货币充值赌资，网络赌博平台也可以将虚拟货币用于自身运营或盈利资金转移。

从网络赌博平台提供的虚拟货币通道来看，主要包含以下两种方式：

虚拟货币钱包：主要针对当前不持有虚拟货币的用户。网络赌博平台常用的虚拟货币钱包一方面支持储存泰达币（USDT）、以太坊（ETH）、比特币（BTC）等主流虚拟货币，另一方面还提供 P2P 交易服务，用户可以直接交易相关赌博平台自己发行的、仅在内部使用的虚拟货币。

虚拟货币直转：主要针对当前持有虚拟货币的用户。如果参赌者本身持有泰达币（USDT）等虚拟货币，那么他可以在充值页面选择充值泰达币（USDT），通过扫码或者向赌博平台的地址直接转账充值赌资。

（二）通过智能合约开发去中心化赌博应用

传统的网络赌博平台主要依托于中心化的服务器进行开发，所有赌博相关程序都运行在中心化的服务器上。随着区块链特别是智能合约技术的出现，网络赌博平台的运营者可以将其平台部署在区块链上。

基于区块链技术的赌博方式，因为相关数据存储链上，相关数据具有不可篡改、公开透明等特征，使得相关“赌博行为”更具“公平性”和“可信赖性”等，这也进一步增加了对于参赌人员或者潜在参赌人员的吸引力。

使用智能合约开发网络赌博平台，可以降低平台的运营成本，减少在运营、财务、客服、网站维护方面的人力投入。参赌者可以直接通过数字货币钱包接入赌博平台中，在平台中，参赌者在区块链上的地址就是他在平台的账户，他可以直接通过与使用智能合约开发的去中心化应用交互完成投注和参与赌博的过程。

这种方式减少了参赌者与赌博平台之间的中间环节，参赌者的资金管理在自己的钱包中，减少了某些赌博平台跑路或限制提现的风险，因此在出现之后吸引了很多参赌者参与。

（三）运营者通过虚拟货币转移盈利或支付运营费用

对于非使用虚拟货币入金或基于智能合约开发的传统网络赌博平台，其运营者同样可以利用虚拟货币为自己提供便利。

一方面，赌博平台的运营者可以使用虚拟货币转移自己的平台盈利，将虚拟货币作为一种洗钱工具，将自己的非法资金“洗白”为合法资金。

另一方面，赌博平台还可以使用虚拟货币作为自己支付平台运营费用的工具，比如平台开发维护费用、客服费用、各级代理费用等。特别是在代理方面，目前的网络赌博平台主要都设置在境外，主要依靠各级代理在国内发展用户、吸引参赌者，使用虚拟货币支付代理费用则使得代理和平台之间的资金关联更为隐蔽，增加了查处打击的难度。

（四）运用区块哈希的随机性来制定赌博规则

由于每一个区块被开采之前不能明确其区块的哈希值，赌博平台的运营者便利用这个特点制定出诸多针对区块哈希的赌博游戏。

这类赌博的游戏一般有以下几种玩法：

哈希单双：参赌者将赌资转入平台指定地址，若赌资的个位数字与交易所在区块哈希的最后一位数字单双一致为赢，否则为输。

哈希幸运：参赌投注交易所在区块哈希的最后两位分别为数字和字母为赢，否则为输。

哈希大小：以交易所在区块哈希的最后一个数字为开奖结果，0 ~ 4 为小、5 ~ 9 为大。以押注金额个位数字判定押注类型，0 ~ 4 为小、5 ~ 9 为大，押对中奖，否则失败。

哈希牛牛：以转账所在区块哈希的最后 5 位为牌面（字母当 10 算），前三位为平台所有，后三位为参赌者所有。双方将自己的牌相加后用各位数字进行比较，大的一方胜出。

以上仅列举了此类赌博比较常见的几种玩法，由于区块链透明去中心化等特点，参赌者可以在区块浏览器中自己查询是否中奖，所以这类赌博平台基本不存在作弊的情况，使得这类赌博平台深受赌徒的喜爱，这也助长了这些平台的发展。

二、区块链应用带来的问题和难点

（一）平台运营者和参与者匿名

由于区块链技术和虚拟货币交易的匿名性，使用智能合约技术开发的网络赌博平台的运营者和参与者的身份难以确定，需要对平台相关的链上地址进行分析、通过链上链下信息数据碰撞才能够落地平台运营者和参与者的身份。

对于使用虚拟货币用作出入金手段的赌博平台也是如此，由于该资金通道从某种程度上可以不依赖银行等传统的法定货币通道，因此参与者的身份具有一定的匿名性，需要投入大量人并使用高科技工具才能够对参与者的现实身份进行确认。

（二）资金流转方式复杂

为了逃避金融监管和公安打击，许多网络赌博网站与非法结算黑产相互勾结、依附，进行赌资洗白。通过非法结算黑产的平台，网络赌博的赌资依靠电商平台、第三方支付平台、跑分平台等形式来进行结算和流转。

在虚拟货币出现之后，赌博平台的资金流转方式更为复杂，除了传统网络赌博的基于法定货币的资金流之外，用户以及支付平台可以使用虚拟货币在赌博平台进行出入金操作，在资金链上还涉及用户或者跑分平台人员在交易所或场外交易平台进行虚拟货币兑换、买卖等操作。

使用虚拟货币，还可以通过区块链上的混币等去中心化应用切断资金链路，使得侦查人员无法对某些交易中的虚拟货币来源或去向进行追踪。

（三）赌资计算难

使用虚拟货币参与的网络赌博平台，很多情况下出入金和投注都是以虚拟货币的形式进行的。除了泰达币（USDT）等稳定币，很多虚拟货币的价格波动大，不同的时间点同样数额的虚拟货币金额差别可能会在几倍到十几倍，因此在赌资计算时需要考虑不同时间的虚拟货币价格变化情况。

基于智能合约开发的网络赌博平台，链上交易数据巨大，需要从中提取、计算出平台和参与者涉及的赌资情况，需要对数据进行清洗等大量的分析工作。

（四）资金冻结难

虚拟货币相关网络赌博平台的主要赌资都是以虚拟货币的形式存在的，因此在资金的冻

结和查缴方面也同传统网络赌博有很大不同。想要对相应地址中的虚拟货币进行冻结或者查缴，需要控制嫌疑人的数字钱包的私钥，进而才能进行相关操作。

虚拟货币交易在我国目前并不合法，而查缴资金需要转换为人民币才能够进行后续操作。

（五）取证关停难

涉及虚拟货币和智能合约的网络赌博平台相关的电子证据数量庞大且时刻变化，要审查和判断调查的数据与案件之间的关联性的任务繁重，并且数据分析具有一定的技术性，对侦查人员的技术水平要求很高。

此类赌博平台往往还利用各个国家、地区的不同政策的规定，实施跨国犯罪。平台运营者和赌博活动参与者关系网络复杂，平台实控人、运营者、参与者、网站服务器都有可能分布在不同的国家、地区，难以根据电子证据与现实人员进行确实、有效的同一认定。

对于基于智能合约的赌博平台，还存在关停难的问题。传统的网络赌博平台只需要关闭服务器就可以停止服务，但是区块链上的赌博平台，智能合约一经部署就自动执行，需要获得部署合约的地址权限以及使用相应的技术手段才能够对其进行关停。

三、网络赌博生态趋势

(一) 运营方

虚拟货币的出现和流行对网络赌博平台的运营方式产生了很大影响。

最明显之处在于大多数网络赌博平台都支持了使用虚拟货币进行支付，根据来自 ARF 的报告，有 780 个赌博网站支持使用比特币（BTC）、以太坊（ETH）、泰达币（USDT）、瑞波币（XRP）和比特币现金（BCH）进行支付，约占知名赌博网站数据库 Casino City 中收录网站的 19%。这些网站大多面向一些所在司法管辖区赌博并不合法的用户。

赌博网站的运营方要么在充值页面增加了虚拟货币地址，要么网站中集成了支持虚拟货币支付功能的 API 接口，使得参赌者充值更为便捷。

另一方面，智能合约的出现也使得赌博类去中心化应用蓬勃发展。相比于传统网络赌博平台只将虚拟货币作为出入金的入口，基于智能合约的网络赌博平台将区块链技术应用得更彻底和娴熟。区块链技术已经成为此类网络赌博平台的重要底层基础架构，而不仅仅是一个出入金的支付通道。

在以太坊、波场、EOS 等支持智能合约的区块链上，赌博类去中心化应用的数量一度接近半壁江山，主要原因是赌博类应用的开发部署成本相对较低，而应用上线之后很快就能够带来回报。运营方在宣传上会称自己基于区块链的赌博平台具有“完全透明公开”、“用户匿名参与”等优势，用来吸引参赌者参与。

(二) 参赌者

互联网特别是移动互联网的普及，使得网络赌博行为迅速向主流人群渗透。在虚拟货币出现之后，用户参与网络赌博的门槛再次降低，只需要在手机上安装一个数字钱包软件，就可以参与网络赌博活动。

虚拟货币支付通道的出现使得一些担心使用法定货币支付导致自身信息泄露的参赌者自认为找到了一种“更加安全”的支付渠道，他们也更加频繁地参加网络赌博活动。

(三) 代理

目前主要的网络赌博平台的运营者或服务器均在境外，但是其主要用户群体仍然是国内用户，这就需要有不同级别的赌博平台代理人或代理机构，专门负责在国内为相应的赌博平台进行推广宣传、招徕新用户相关的工作。

网络赌博代理的主要模式包括：通过平台生成的自己的二维码和推广链接拉新绑定自己的下级，获得下级的部分流水抽成；通过帮助他人开设账号供他人进行赌博，他人通过代理

账号充值之后，代理可以获得部分流水抽成。

这些代理方可以是个人，也可以是类似于“赌博工作室”之类的团队，他们在国内为境外网络赌博平台吸引用户，同时拿到相应的返佣。虚拟货币在广泛应用之后，也迅速成为网络赌博平台支付返佣费用的主要方式。

（四）资金链

在网络赌博平台资金链的上游，虚拟货币的出现改变了传统的以法定货币为中心的赌资流动路线，在主要网络赌博平台纷纷接受比特币（BTC）、以太坊（ETH）、泰达币（USDT）等虚拟货币作为入金手段之后，已经初步形成了一条新的资金流动路径：用户将法定货币从银行等传统金融机构转入虚拟货币交易平台，在虚拟交易平台中兑换为网络赌博平台接受的虚拟货币，然后将虚拟货币转移到自己的数字钱包中，再通过数字钱包向网络赌博平台充值赌资。

在这条路径中，虚拟货币交易平台和数字钱包作为虚拟货币兑换和存储的节点，是最为关键的部分。需要注意的是，不一定所有资金链路上都会有交易平台或者数字钱包。

一方面，很多数字钱包本身就支持或兼容虚拟货币交易和法定货币兑换的功能，用户只需要使用特定的数字钱包就可以完成法定货币到虚拟货币的兑换，因此不需要通过交易平台获得虚拟货币。

另一方面，用户在交易平台中购买虚拟货币之后，也可以直接把虚拟货币提现至网络赌博平台，这时就不需要通过数字钱包。

由于目前包括我国在内的一些司法管辖区内虚拟货币交易并不合法，很多参赌者往往通过币商、场外交易平台等方式获取虚拟货币。

在网络赌博平台资金链的下游，虚拟货币成为网络赌博平台洗钱的重要手段。平台要么直接将参赌者以虚拟货币形式充值的赌资转移，要么通过一些“跑分”平台，将法定货币形式的赌资转换为虚拟货币，再进行分配和转移。

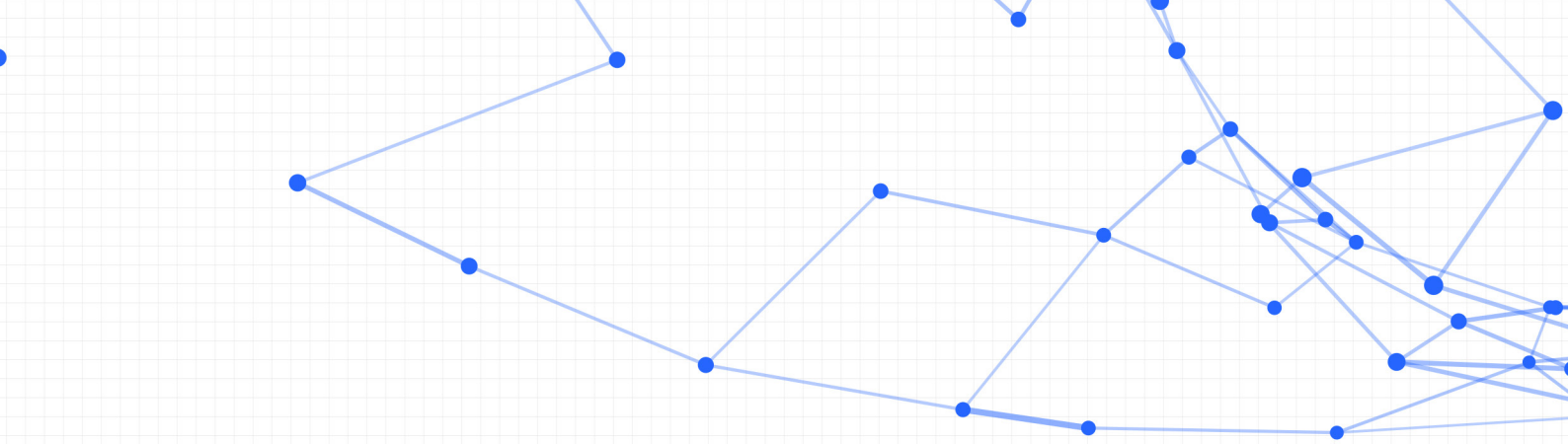
（五）新技术

虽然目前区块链技术在网络赌博中的应用主要体现在虚拟货币作为出入金支付通道、使用智能合约开发赌博去中心化应用以及通过虚拟货币转移平台利润，但是区块链技术仍然在不断发展，这一领域的一些新的技术发展仍然有可能被继续用于网络赌博领域，比如非同质化代币（NFT）、链游、元宇宙等。

非同质化代币（NFT）是近年来区块链领域比较热门的名词之一，其可以代表区块链上独一无二的数字资产的所有权。随着非同质化代币的价值被越来越多的人承认，其也有可能被网络赌博平台用作赌博的奖励物。此外，赌博平台也可以使用非同质代币将自己部分去中

心化，也就是发行一定代表本平台所有权的非同质化代币，使代币所有者可以分享一部分平台的利润。

链游和元宇宙也是近期区块链领域的热点概念。链游是将区块链和传统网络游戏相结合，元宇宙则是一个虚拟的网络空间的概念。通过披上链游或元宇宙的外衣，网络赌博平台可以使自己的非法行为更加隐蔽。



第十一章

2022 年虚拟货币诈骗 “八宗最”

在本章中，根据 2022 年高发的典型案例中，选取诈骗者常用套路总结为 2022 年虚拟货币诈骗“八宗最”。

一、最“屡试不爽”——投资

知帆安全团队对虚拟货币案例信息库中 2300 余篇刑事文书做关键词检索，“投资”成为最高频的词，由此可见，虚拟货币相关的骗局几乎都和投资相关。

不管是“一夜暴富 XX 币”，还是“跟着专家财富自由”，不法分子利用投机者的投机心理，施行违法犯罪活动。以各种各样的形式引导受害者进入陷阱，不管是投资矿机、还是跟着专家投资虚拟货币，都是利用了受害人想暴富的心理。

二、最“以假乱真”——虚假 APP

犯罪团伙自行开发可随意操纵后台数据的虚假 APP 或网站，通常都模仿真实平台的样子。在虚拟货币投资骗局中，不法分子往往一边鼓吹投资的升值前景，一边引导受害者下载、使用虚假 APP，并在后台操纵数据，诱骗受害者充值，最后携款跑路。

三、最“言听计从”——老年人

不法分子利用区块链、虚拟货币等噱头，声称有国家背书，能轻松赚钱，诱骗老年人。大多数老年人由于网络安全意识较差，很容易陷入不法分子精心打造的骗局。投资虚拟货币、投资矿机和参与虚拟货币传销，是 2022 年最常见的针对老年人的虚拟货币骗局。

老年人对网络诈骗的防范意识相对薄弱，他们很容易深陷骗局，甚至卷入传销，这不仅会让一个家庭蒙受大量经济损失，也让老年人自身身心遭受伤害。

四、最“老调重弹”——杀猪盘与杀洋盘

杀猪盘是大众熟悉的一种传统电信诈骗方式，指诈骗分子利用网络交友，诱导受害人投资、赌博等。2022 年“杀猪盘”出现新变化，诈骗分子故技重施，将骗局瞄准了外国人，此类诈骗也被称为：杀洋盘。

诈骗分子往往假扮白富美、高富帅，利用翻译软件和 Telegram、WhatsApp 等国外社交软件，和外国网友聊天“交友”，一步步引导受害者走入陷阱，除诈骗钱财外还会诱骗受害者参与境外跑分洗钱。

五、最“笑里藏刀”——熟人

熟人作案经常出现在虚拟货币盗窃类案件中，受害者由于面对熟人掉以轻心，或无意间泄露了自己的私钥或助记词，更有甚者将虚拟货币账号信息主动交予熟人代为保管、交易和投资，最终导致虚拟货币资产被盗。

除了盗币类案件，洗钱跑分、传销、投资类诈骗也常涉及熟人推荐。

知帆安全团队提醒：保管好私钥和助记词等重要账号信息，即使面对熟人，也须提高安全意识。

六、最“巧立名目”——智能合约

智能合约是一项基于区块链的技术，它可以在区块链上运行特定的合约程序。前些年智能合约作为一种复杂的技术鲜为人知，但随着网络信息的高度共享，近年来智能合约的搭建已经变得容易很多。这给资金盘、诈骗盘提供了便利，诈骗团伙自行搭建未经严格审计的智能合约，其中藏有难以被人发现的漏洞，他们吸收受害者资金后，再利用漏洞轻松跑路。

更有一些诈骗分子，实际并未运用到区块链技术，只是打着“智能合约”的幌子实施诈骗。

七、最“呼群结党”——Telegram

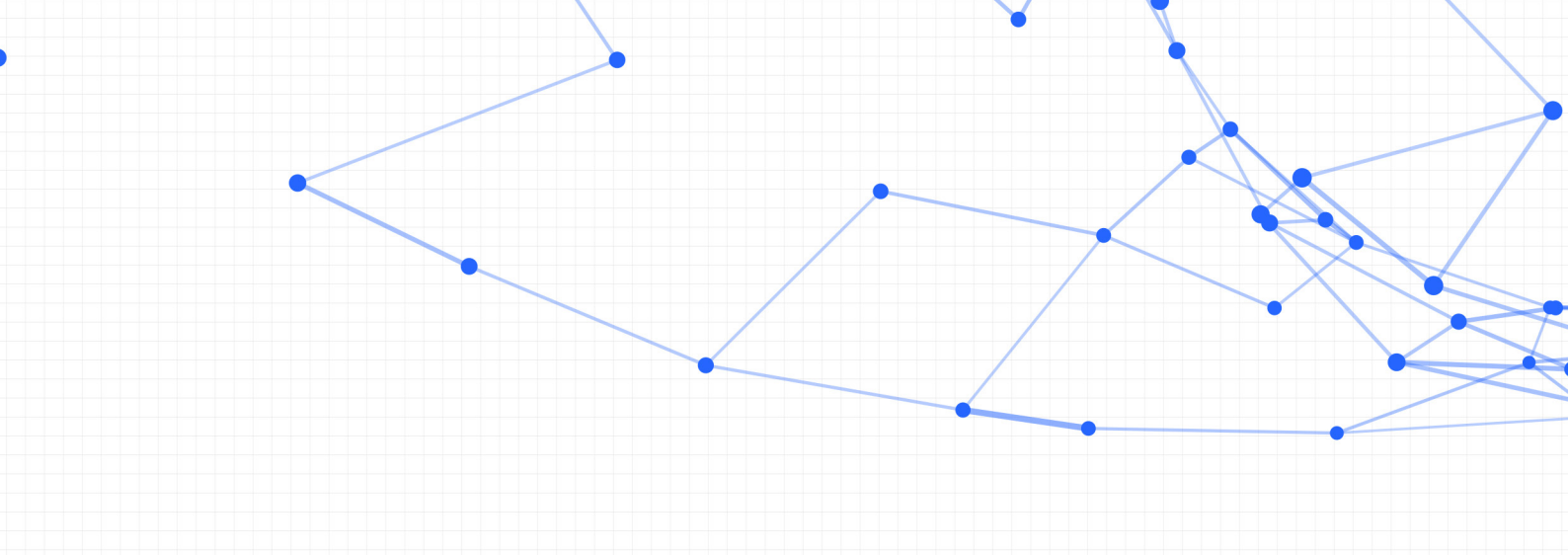
Telegram 是一款跨平台的即时通讯软件，又称 TG 或电报，因其匿名聊天、阅后即焚等功能，成为加密领域最受欢迎的通讯软件之一。同时 Telegram 只需要手机号就能注册，不需要实名，这也使其成了涉虚拟货币犯罪的高发地。

在近年的多起案件中，犯罪分子利用 Telegram 作为实施违法犯罪活动的主要引流推广渠道。其中，诈骗虚拟货币、虚拟货币传销、利用虚拟货币洗钱、买卖违禁品和买卖公民信息是常见的利用 Telegram 作为推广、交流渠道的犯罪类型。

八、最“单刀直入”——OTC 诈骗

2021年下半年，国内严格打击虚拟货币 OTC 场外交易，各大交易所清退中国大陆用户。一些交易虚拟货币的需求无处落实，这催生出许多没有保障的 OTC 场外交易，一些受害者因贪小便宜，企图用更低的价格购买虚拟货币，最终落入不正规 OTC 的陷阱。

伪造交易明细、收款后拉黑跑路都是常见的 OTC 骗局套路。而这类诈骗往往也非常直接，没有花里胡哨的铺垫和技术，受害者掉以轻心，主动将资产转移给诈骗分子。



第十二章

2022 年国内虚拟货币监管情况

为了防范金融风险，维持金融秩序稳定，近年来，我国相关监管部门接连发声，释放了从严监管的信号，始终保持对虚拟货币交易炒作活动的高压打击态势，以下为 2022 年发布的相关内容。

一、2022 年国内虚拟货币相关监管政策

（一）《关于防范以“元宇宙”名义进行非法集资的风险提示》

2 月 18 日，银保监会发布《关于防范以“元宇宙”名义进行非法集资的风险提示》。

银保监会指出，一些不法分子蹭热点，以“元宇宙投资项目”“元宇宙链游”等名目吸收资金，涉嫌非法集资、诈骗等违法犯罪活动，提示社会公众增强风险防范意识和识别能力，注意防范编造虚假元宇宙投资项目、打着元宇宙区块链游戏旗号诈骗、恶意炒作元宇宙房地产圈钱、变相从事元宇宙虚拟币非法牟利等诱惑力大、欺骗性强的违法犯罪活动，谨防上当受骗。

（二）《关于修改〈最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释〉的决定》

2 月 24 日，最高人民法院发布《关于修改〈最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释〉的决定》，对原司法解释中有关非法吸收公众存款罪、集资诈骗罪的定罪处罚标准进行修改完善，明确相关法律适用问题，自 2022 年 3 月 1 日起施行。

修改后《解释》保留认定非法吸收公众存款罪的四个特征要件不变，即非法性、公开性、利诱性、社会性。结合司法新实践和犯罪新形式，增加网络借贷、虚拟币交易、融资租赁等新型非法吸收资金的行为方式。同时，针对养老领域非法集资突出问题，增加“以提供‘养老服务’、投资‘养老项目’、销售‘老年产品’等方式非法吸收资金”的情形，为依法惩治 P2P、虚拟币交易、养老领域等非法集资犯罪提供依据。

（三）2022 年金融市场工作电视会议：持续保持对虚拟货币交易炒作高压打击态势

3 月 1 日，人民银行召开 2022 年金融市场工作电视会议。会议深入学习党的十九大、十九届历次全会和中央经济工作会议精神，贯彻落实 2022 年人民银行工作会议要求，总结 2021 年人民银行金融市场和信贷政策工作，部署 2022 年重点工作。其中，会议要求，联合有关部门继续推进互联网平台企业金融业务的自查整改工作，持续保持对虚拟货币交易炒作的高压打击态势。

（四）《关于防范 NFT 相关金融风险的倡议》

4月13日，为防范金融风险、保护消费者合法权益、维护行业健康生态，中国互联网金融协会、中国银行业协会、中国证券业协会发布《关于防范 NFT 相关金融风险的倡议》。倡议指出，近年来，我国 NFT（Non-FungibleToken，非同质化通证）市场持续升温。

NFT 作为一项区块链技术创新应用，在丰富数字经济模式、促进文创产业发展等方面显现出一定的潜在价值，但同时也存在炒作、洗钱、非法金融活动等风险隐患。倡议提出，坚决遏制 NFT 金融化证券化倾向，从严防范非法金融活动风险，自觉遵守多项行为规范。

（五）《中华人民共和国反电信网络诈骗法》

9月2日，最高人民检察院发布《中华人民共和国反电信网络诈骗法》，第四章“互联网治理”中第二十五条规定，任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助：（一）出售、提供个人信息；（二）帮助他人通过虚拟货币交易等方式洗钱；（三）其他为电信网络诈骗活动提供支持或者帮助的行为。第七章“附则”中第五十条显示，本法自2022年12月1日起施行。

二、2022 年国内虚拟货币“挖矿”相关监管政策

自 2021 年 9 月 24 日，国家发改委、财政部、央行、税务总局、银保监会等 11 部门联合发布《关于整治虚拟货币“挖矿”活动的通知》后，全国各地积极推进落实整治虚拟货币“挖矿”行为。2021 年，海南省率先发布了对虚拟货币“挖矿”项目实行差别电价的通知。今年以来，国内对虚拟币“挖矿”的监管持续升级，内蒙古、浙江、山东、山西、四川、陕西、贵州等地区也先后发布了实行差别电价的通知。

（一）内蒙古发改委：对虚拟货币“挖矿”项目用电实行差别电价

1 月 20 日，内蒙古发改委发布《关于虚拟货币“挖矿”用电实行差别电价政策的通知》，对虚拟货币“挖矿”项目用电实行差别电价，加价标准为每千瓦时 1 元；禁止虚拟货币“挖矿”项目参与电力市场交易；禁止擅自接入电价低的供电线路进行虚拟货币“挖矿”。

（二）浙江宣布对虚拟货币挖矿用电实行差别电价，每度电加价 0.5 元

2 月 14 日，浙江省发改委发布《关于虚拟货币挖矿用电实行差别电价政策有关事项的通知》。据通知内容显示，为整治虚拟货币挖矿活动，深入推进节能减排，助力如期实现碳达峰、碳中和目标，浙江省内虚拟货币挖矿用电将实行差别电价，加价标准为每千瓦时 0.50 元。

（三）山东拟对虚拟货币“挖矿”实行差别电价，每千瓦时加 2 元

2 月 25 日，山东省发改委发布《关于虚拟货币“挖矿”用电差别电价政策有关事项的通知（征求意见稿）》（以下简称“通知”）。通知显示，山东省拟对虚拟货币“挖矿”用电执行差别电价，加价标准为每千瓦时 2 元（含税）。

（四）山西对虚拟货币“挖矿”用电执行差别电价政策

4 月 8 日，山西省发改委发出《关于虚拟货币挖矿用电实行差别电价政策有关事项的通知》，决定自 5 月 10 日起对虚拟货币“挖矿”用电执行差别电价政策。

（五）四川发改委：加大整治力度，对关停虚拟货币“挖矿”项目实用电量执行差别电价

4 月 15 日，四川省发改委发布了《四川省发展和改革委员会关于加大整治力度对关停虚拟货币“挖矿”项目实用电量执行差别电价的通知（川发改价格规〔2022〕186 号）》，决定对虚拟货币“挖矿”活动的各类用电量执行差别电价，加价标准为每千瓦时 2 元。

(六) 陕西对“挖矿”实行差别电价，每度加 1 元

4 月 26 日，陕西省发改委发布关于虚拟货币“挖矿”用电实行差别电价的通知，决定对虚拟货币“挖矿”用电实行差别电价，每度加 1 元。

(七) 贵州省发改委：虚拟货币“挖矿”项目执行“淘汰类”企业电价，加价标准提至每千瓦时 2 元

6 月 20 日，贵州省发改委发布了《关于虚拟货币“挖矿”用电实行差别电价政策有关问题的通知（黔发改价格〔2022〕462 号）》，将虚拟货币“挖矿”项目纳入差别电价政策实施范围，执行“淘汰类”企业电价，该类项目加价标准提高为每千瓦时 2 元。

(八) 天津对虚拟货币“挖矿”用电实行差别电价

10 月 10 日，天津市发改委发布《市发展改革委关于虚拟货币“挖矿”用电实行差别电价政策的通知》，对虚拟货币“挖矿”用电实行差别电价，执行“淘汰类”企业电价，加价标准为每千瓦时 0.5 元。



附录

关于知帆科技和知帆学院



知帆科技成立于 2017 年 7 月，是国内最早专注于区块链大数据分析的安全公司之一，也是最早提供虚拟货币追踪服务的专业公司，截至目前，知帆科技已与全国数百余家公安机关建立合作，利用核心技术能力对区块链数据进行分析挖掘，帮助公安等监管机构解决涉虚拟货币相关案件查证难题，提供技术服务达到上千余次，协助侦破数十起具有影响力的重大涉虚拟货币案件，总涉案金额超一千亿元。

“逐迹”虚拟货币追踪查证平台由知帆科技（CHAINDIGG）安全团队研发，独创资金分析层级图结构和关联图结构切换功能，作为面向公安机关的虚拟货币侦查服务平台，“逐迹”从虚拟货币地址账户分析、追踪溯源、线索扩线、实战工具等方面，为监管部门日常研判虚拟货币案件提供了工具支持，解决由虚拟货币匿名性带来的无法追踪资产流向的问题。主要模块包含：态势感知、资金分析、通用工具。

知帆学院由公安情报与大数据应用研究中心指导北京知帆科技有限公司创立，致力于应对犯罪升级，服务情报信息技术。



知帆科技
CHAINDIGG



微信公众号

官网：www.chaindigg.com

官方微信：知帆科技