区块链和虚拟货币犯罪趋势研究报告

2021 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 年虚拟货币犯罪案件、涉虚拟货币裁判文书的主要涉案类型、数量、金额、币种、领域等维度，结合区块链安全事件和典型案例揭示了 2021 年区块链和虚拟货币犯罪的发展现状和发展趋势，总结出 2021 年区块链安全领域十大关键词、2021 年八大虚拟货币典型骗局、2021 年十大虚拟货币诈骗话术和十种虚拟货币传销的典型模式。

- **虚拟货币诈骗洗钱类案件数量最多，虚拟货币网赌类案件平均涉案金额最高。**2021 年，诈骗洗钱类案件数量位居首位，占总数量的 38.8%，平均涉案金额较低，为 0.09 亿元。网赌类案件数量排在第四位，占总数量的 6.3%，平均涉案金额最高，达到 21.49 亿元。

- **虚拟货币传销是最主要的犯罪类型。**2021 年，虚拟货币传销类案件占总数量的 29.2%，排名第二，累计涉案金额位居首位，占所有虚拟货币犯罪案件总涉案金额的 67.82%。无论是从数量上还是金额上，虚拟货币传销都是主要的虚拟货币犯罪类型。

- **稳定币成主力，USDT 的涉案占比最高。**从 2021 年虚拟货币犯罪案件涉案币种分布看，USDT 涉案比例最高，占据了绝对主力位置，四种不同链上的 USDT 总占比接近 80%。

- **传销犯罪分子偏爱波场，诈骗洗钱更爱以太坊。**在 2021 年的虚拟货币传销案件中，波场链上的 TRX 和 USDT-TRC20 案件数量占比明显增多，分别为 9.1%和 31.5%。而在虚拟货币诈骗洗钱案件中，USDT-ERC20 的案件数量占比接近半数，达到 47.9%。

- **境内流出资金达到 2230 亿元。**2021 年，境内交易所与美国交易所之间的资金流动最为频繁，从境内流出的 USDT 和 BTC 均大于流入境内的量，其中 USDT 流出 23 亿枚，BTC 流出 83 万枚。

- **虚拟货币犯罪案件数量逐年上升。**2021 年，与比特币和以太坊相关的案件数量有减少的趋势，而与 USDT 相关的案件数量继续快速增长。

- **涉虚拟货币裁判文书中，案由较多的是：诈骗罪、盗窃罪、帮信罪。**2014 至 2021 年，涉虚拟货币裁判文书数量呈逐年上升趋势。2021 年，与比特币和以太坊相关案件的案由中占比最多的是诈骗罪和盗窃罪，与 USDT 相关的案件占比最多则是帮信罪。

- **区块链安全事件数量整体呈上升趋势。**在过去几年中，区块链安全事件数量整体呈上升趋势。2021 年，DeFi 应用的发展加之 NFT、元宇宙等新概念的出现，使得区块链安全事件的数量猛增，相较于 2020 年增长 67%。

- **DeFi 成区块链安全领域重灾区。**从安全事件主要领域分布上看，DeFi 领域是 2021 年区块链安全领域的重灾区，占比高达 54%；从主要类型分布上看，漏洞类问题最严重；从损失情况上看，诈骗项目和跑路项目造成的损失最大。其中 7 月安全事件的数量最多。

- **闪电贷攻击成 DeFi 噩梦。**随着更多资金流入 DeFi 领域，黑客运用闪电贷攻击的频率增多，在 2021 年 5 月开始明显上升。整体数量上，2021 年较 2020 年也呈现上升趋势。

- **三大典型区块链安全事件：项目跑路和砸盘骗局、合约漏洞、私钥被盗。**前两个都是区块链行业特别常见的安全事件，私钥被盗导致的虚拟货币资产失窃事件占比虽然不高，但是一旦某个项目或交易所的钱包私钥失窃，将造成非常严重的损失。

- **2021 年区块链安全与犯罪领域十大关键词。**分别是：NFT、DeFi、交易所、Meme 币、元宇宙、Play To Earn、“土狗”项目、挖矿、DAO、数字人民币。

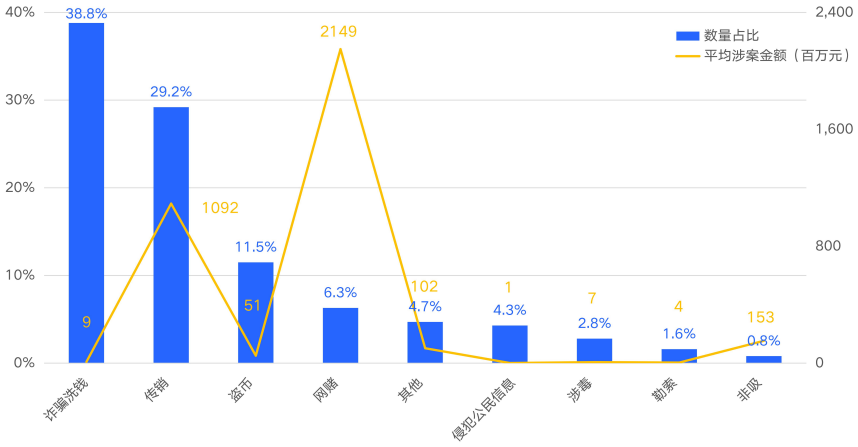
目 录

第一章 2021 年虚拟货币犯罪案件综合分析

本章中，根据知帆科技 2021 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、2021 年虚拟货币犯罪主要类型及平均涉案金额

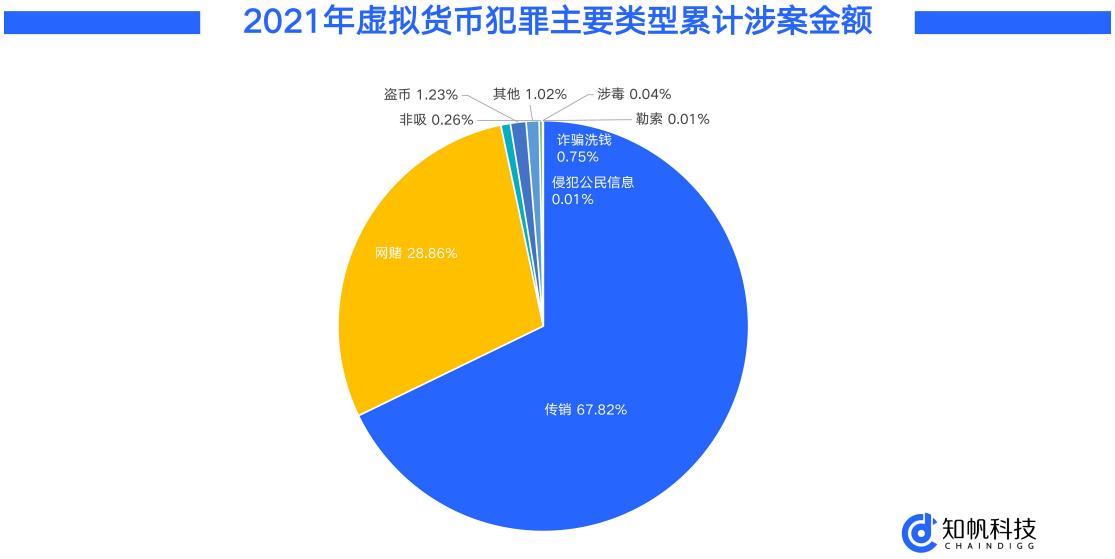
2021年虚拟货币犯罪主要类型及平均涉案金额



2021 年，诈骗洗钱类案件数量位居首位，占总数量的 38.8%，本章中的诈骗洗钱类指的是：前期犯罪手段为各类型网络诈骗，然后利用虚拟货币进行洗钱的案件，此类型包含了诈骗虚拟货币和诈骗人民币。其次为虚拟货币传销案件，占总数量的 29.2%。盗币类案件，排在第三位，占总数量的 11.5%。

从主要类型的平均涉案金额看，网赌类案件的平均涉案金额最高，达到 21.49 亿元。传销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 10.92 亿元。诈骗洗钱类案件虽然数量最多，但平均涉案金额较低，为 0.09 亿元。

二、2021 年虚拟货币犯罪主要类型累计涉案金额

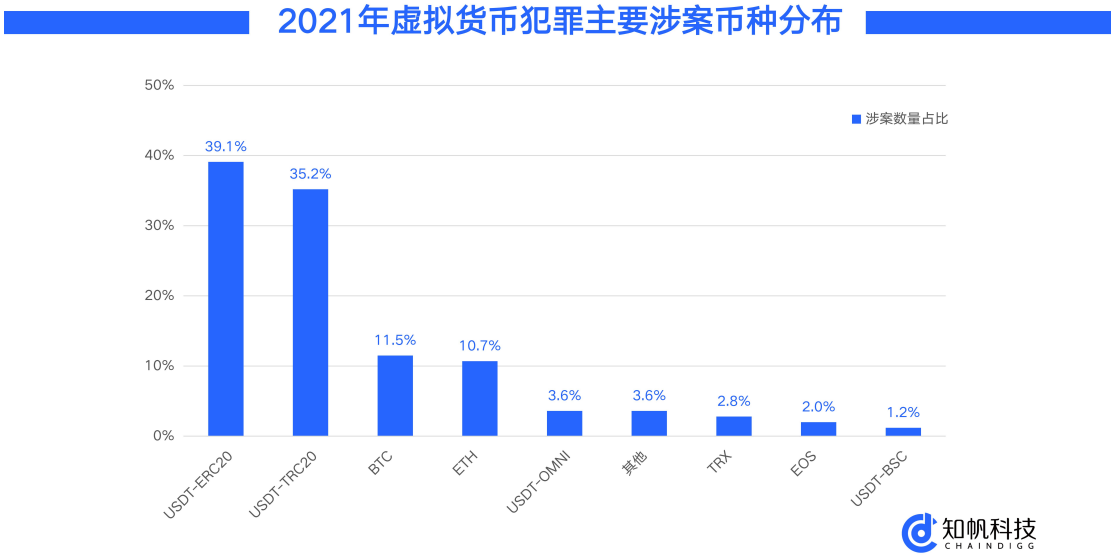


从主要类型的累计涉案金额看，主要为虚拟货币传销类案件和网赌类案件，这两类占比超过 96%，其中，传销类案件的累计金额位居首位，占所有虚拟货币犯罪案件总涉案金额的 67.82%。其次为网赌类案件，占比 28.86%。排在第三位的则是盗币类案件，占比 1.23%。

由此可见，无论是从数量上还是金额上，虚拟货币传销类犯罪都是主要的虚拟货币犯罪类型，此类犯罪参与人多、金额大、传播快，通过发展下线维持资金流，以达到侵占公众存款的目的。虚拟货币传销通常具备以下特征：1.利用区块链的噱头来包装和炒作，从而诱骗投资者；2.交纳一定数额的虚拟货币作为入门费；3.犯罪组织化、专业化、隐蔽化；4.拉人头模式、层级深、采用层级团队计酬；5.发展速度快，可复制性强。

值得注意的是，网赌类案件平均涉案金额和累计涉案金额都很巨大，此类犯罪与电诈、暗网、洗钱、赌博网站、非法游戏等黑产相互交织。为了最大程度“洗钱”，犯罪团伙越来越热衷于利用虚拟货币进行结算跑分，参与者到 USDT 跑分平台购入 USDT 作为保证金，参与跑分抢单。跑分参与者提供购入 USDT 币的充值码给跑分平台，跑分平台汇聚各种充值额度的 USDT 充值码，整合成一个 USDT 充值码池，并以充值接口方式提供给赌博平台。赌客充值赌资需扫描 USDT 充值码进行充值，也就是使用人民币向跑分平台购入 USDT，最终致使人民币流转至跑分平台。

三、2021 年虚拟货币犯罪主要涉案币种分布



从 2021 年虚拟货币犯罪案件涉案币种分布看，部分案件涉及了多个币种，USDT 涉案比例最高，占据了绝对主力位置，四种不同链上的 USDT 总占比接近 80%。其中以太坊区块链上的 USDT-ERC20 位居首位，占比高达 39.1%；波场区块链上的 USDT-TRC20 占比则为 35.2%，排在第二位；比特币区块链上的 USDT-OMNI 占比为 3.6%。BTC 和 ETH 占比相对偏低，分别为 11.5%和 10.7%，排在第三位和第四位。

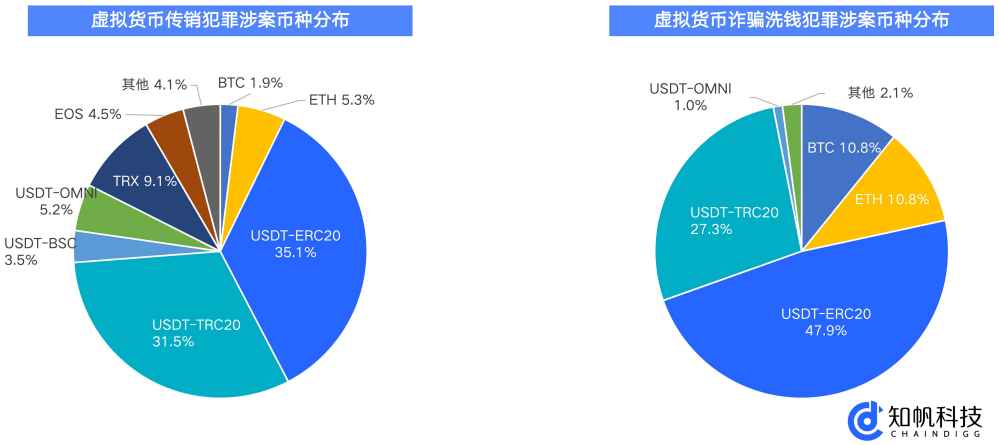
这种趋势表明了稳定币在区块链生态中的关键作用，USDT 作为使用最为广泛的稳定币，一方面起到了法币入金媒介作用，涉案人会使用法币购买 USDT 稳定币，然后再兑换为其他虚拟货币；另一方面，由于其价值相对稳定，也被不法分子用于洗钱或转移非法收入等用途。

值得注意的是，由于波场链上的 USDT-TRC20 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 USDT-TRC20，上图数据显示，占比已经和 USDT-ERC20 基本持平。

此外，知帆安全团队发现，随着 BSC（币安智能链）和 HECO（火币生态链）的崛起，在其链上发行的 USDT 也逐渐出现在相关虚拟货币犯罪中，上图数据也显示 USDT-BSC 占比 1.2%。

四、2021 年虚拟货币传销及诈骗洗钱涉案币种分布

2021年虚拟货币传销及诈骗洗钱涉案币种分布



在不同类型的犯罪中，涉案币种的使用情况也有所不同，上图选取了传销和诈骗洗钱两种最为高发的犯罪类型的数据分别做分析。

在虚拟货币传销案件中，USDT-ERC20 的案件数量占比下降至 35.1%，BTC 和 ETH 的案件数量占比也大幅减少至 1.9%和 5.3%。此消彼长，波场链上的 TRX 和 USDT-TRC20 案件数量占比都有明显增多，分别为 9.1%和 31.5%，这表明波场链已成为传销犯罪分子最常利用的区块链。

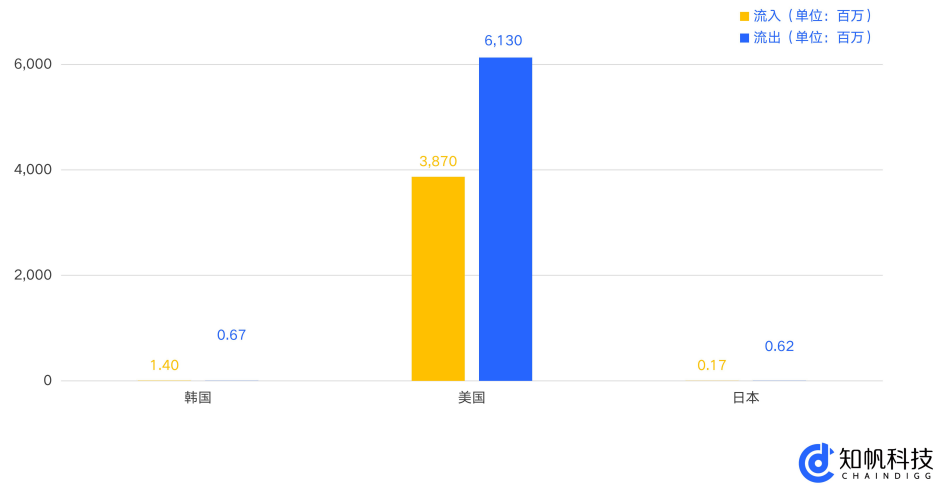
在虚拟货币诈骗洗钱案件中，USDT-ERC20 的案件数量占比接近半数，达到 47.9%，USDT-TRC20 的案件数量占比则为 27.3%，BTC 和 ETH 的案件数量占比均为 10.8%。

五、2021 年跨境资金流动分析

2021 年，区块链上的非法活动情况依然活跃，本节对知帆科技地址标注数据库的已标注数据进行分析，以此来揭示跨境资金流动情况。虽然分析的十余个主要虚拟货币交易所现阶段都是面向全球的虚拟货币交易者，但是为了更好的分析，创建时主要面对境内用户的交易所，我们把其资产认为是境内资产，同理主要面对境外用户的交易所的资产则为境外资产。

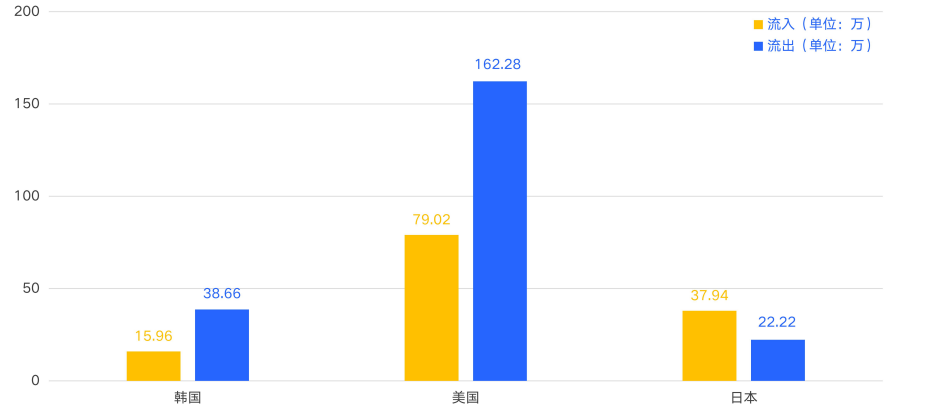
通过对各大交易所间的资金流向分析可以看到，境内交易所与美国交易所之间的资金流动最为频繁，从境内流出的 USDT 和 BTC 均大于流入境内的量，其中 USDT 的流出量比流入量多近 23 亿枚，BTC 的流出量比流入量多 83 万枚。BTC 按 4 万美元价格计算，据知帆科技不完全统计，2021 年虚拟货币资产从境内流出资金达到 2230 亿元。

境内外USDT资金流动情况



知帆科技 CHAINDIGG

境内外BTC资金流动情况



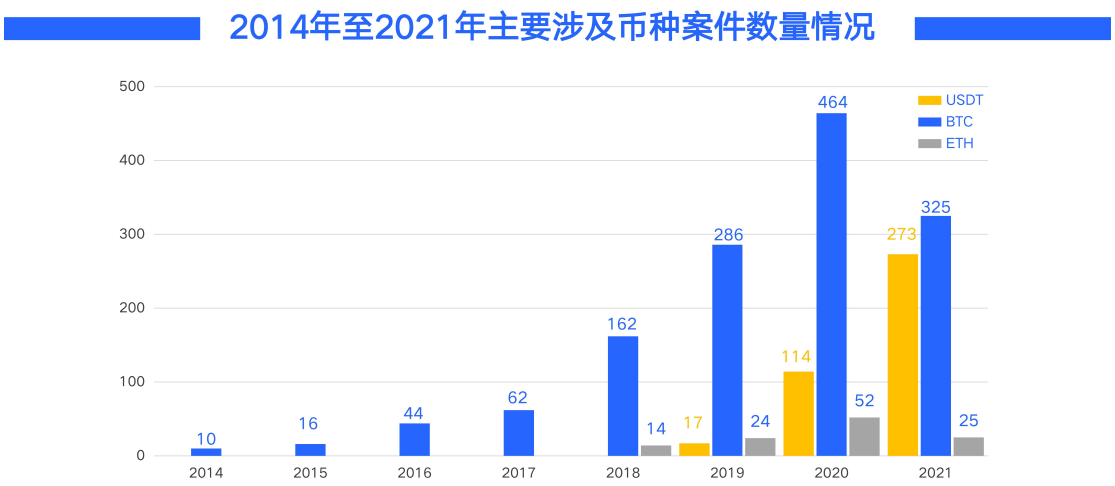
知帆科技 CHAINDIGG

第二章 涉虚拟货币裁判文书综合分析和典型案例盘点

本章中，基于中国裁判文书网已经公开的裁判文书进行了检索、统计和分析，也对 2021 年已破获的虚拟货币典型案例做了盘点。以此来揭示过去几年涉虚拟货币相关犯罪案件的发展趋势。

知帆安全团队认为，数据的意义在于精准，虽然自 2009 年比特币正式出现以来，一般提到虚拟货币通常指以比特币、以太币等为首的去中心化加密货币，但是虚拟货币这一词相对广义，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），所以在对裁判文书网进行关键词检索时，没有选择“虚拟货币”关键词，而是选择了“BTC”、“USDT（泰达币）”、“以太坊（ETH）”、“加密货币”等更有针对性的关键词。

一、2014 年至 2021 年主要涉及币种案件数量情况

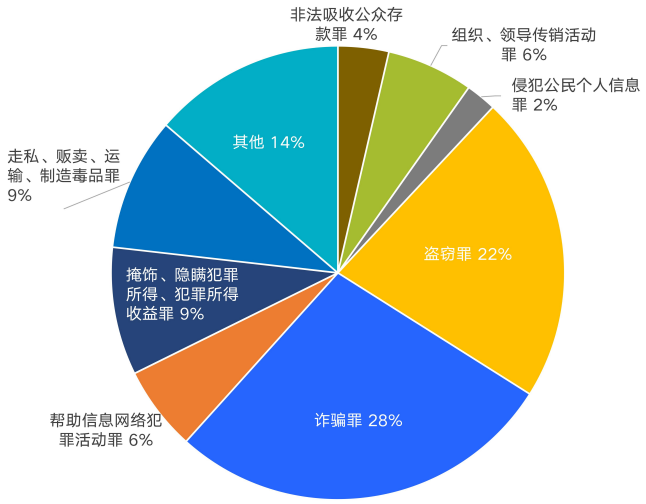


从整体数量上看，在 2014 年至 2021 年之间，随着区块链技术的发展和虚拟货币发币、交易流程的简化、交易所和钱包的普及，虚拟货币犯罪的数量呈逐年上升趋势。

从各个主要虚拟货币涉及的案件数量上看，在 2021 年，与比特币和以太坊相关的案件数量有减少的趋势，而与 USDT 相关的案件数量继续快速增长，这反映了 DeFi（去中心化金融）技术的发展对虚拟货币犯罪趋势的影响，因为在 DeFi 相关犯罪活动中，不法分子往往借助自身创建的虚拟货币实施犯罪，受害人往往需要使用 USDT 去购买这些虚拟货币。

二、2021 年 BTC、ETH、USDT 相关案件的案由分布

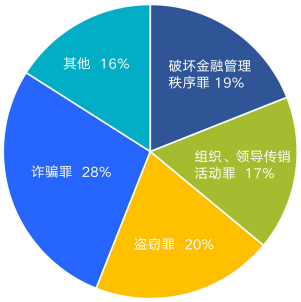
2021年BTC相关案件的案由分布



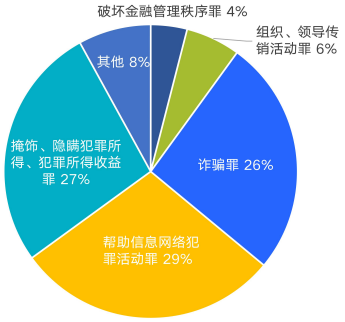
从比特币相关案件的案由上看，案由占比最多的是诈骗罪，占比为 28%。盗窃罪占比为 22%，排在第二位。

2021年ETH及USDT相关案件的案由分布

ETH相关案件的案由分布



USDT相关案件的案由分布



与以太坊相关的案件占比最多的也是诈骗罪和盗窃罪，占比分别为 28%和 20%。与 USDT 相关的案件占比最多的是帮助信息网络犯罪活动罪，占比为 29%。其次是掩饰、隐瞒犯罪所得、犯罪所得收益罪，占比为 27%。诈骗罪则占比为 26%，排在第三位。

从以上两张统计表可以看出，2021 年涉虚拟货币裁判文书中，案由是诈骗罪、盗窃罪、帮助信息网络犯罪活动罪的裁判文书比较多。

三、2021 年已破获虚拟货币典型案例盘点

（一）洗钱

由于虚拟货币的匿名性以及便于跨境转移的特性，虚拟货币在洗钱犯罪中的使用自其出现以来就有增加的趋势。传统的反洗钱监管措施往往依赖于银行等金融中介机构，而点对点支付的虚拟货币可以通过一些没有实施 KYC 和 AML 等合规措施的中心化交易所或者去中心化交易所进行交易，这增加了对其进行监管和打击的难度。

根据公安部发布的数据，2021 年共打击虚拟货币洗钱相关案件 259 起，收缴虚拟货币价值 110 亿余元。

2021 年虚拟货币洗钱相关的典型案例：

1、遵义市公安局成功打掉一特大虚拟货币洗钱犯罪团伙，共计抓获涉案嫌疑人近百人，破获发生在全国各地的电信诈骗案件 332 起,认定掩饰隐瞒涉案金额 956 万元,查扣涉案资产价值 300 余万元、作案手机 51 部、电脑 15 台、银行卡 511 张，涉及转账洗钱流水达 8 亿元。

2、西昌市公安局在强化打击电信网络诈骗犯罪过程中，深挖线索，首次打掉利用虚拟货币为电信网络诈骗犯罪“洗钱”的团伙。该团伙利用交易虚拟货币的方式为上游犯罪转移赃款，致使上游犯罪无法被及时查处，并造成公私财物重大损失，其犯罪程度已严重影响公安机关正常查明犯罪上游团伙成员、追缴犯罪所得及收益。

（二）传销

虚拟货币由于其本身技术复杂、概念新颖，并且与区块链技术结合紧密，所以经常被一些传销分子用来作为噱头进行传销相关活动。一些犯罪分子通过鼓吹虚拟货币投资的静态收益以及拉人头的动态收益诱骗投资人发展下线，还有一些项目通过和“质押挖矿”等区块链概念相结合，使得传销行为更加隐蔽，增加了打击的难度。

此外，随着去中心化金融（DeFi）技术的发展，一些传销项目更是通过智能合约的形式运行，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，传销项目不再需要财务、技术、维护等人员，这进一步增加了对虚拟货币传销项目调查、取证的难度。

2021 年虚拟货币传销相关的典型案件：

1、徐州睢宁警方破获“BBGO”虚拟货币质押挖矿平台特大传销案，犯罪嫌疑人通过搭建一款名叫“BBGO”的虚拟货币质押挖矿平台，诱骗投资人加入。嫌疑人利用自己搭建的没有任何市场价值的虚拟货币平台，并以高额回报和高返利为诱饵，逐级发展下线进行组织、领导传销活动。徐州警方共抓获全链条犯罪嫌疑人 8 名，案件涉及全国约 11 万人，涉案资金达 10 亿元。

2、徐州市公安机关组织在 11 月 2 日 20 时至 11 月 4 日 20 时展开 2021 汉风行动 3 号行动，以严厉打击整治秋冬季突出违法犯罪和治安问题。其中，丰县县局先后在上海、武汉、深圳等地抓获星际联盟网络（IPFS）传销犯罪团伙成员 31 人，查获以太坊、泰达币、FIL 币等约 4 亿元的虚拟货币。

（三）诈骗

诈骗案件在所有涉及虚拟货币的案件中占比例最大，犯罪分子往往利用了投资者对虚拟货币不够了解的弱点，将一些完全没有价值的“空气币”甚至并非虚拟货币的“虚拟货币”进行包装，并将其同一些热点概念进行捆绑，诱骗投资者进行投资。

在 2021 年，NFT（非同质代币）、元宇宙、链游、Web3.0 等概念都曾火爆一时，这些概念也都被不法分子利用，成为虚拟货币诈骗活动的高发区。

在诈骗手法上，除了兜售没有任何价值的“空气币”外，犯罪分子还采用了一些新的手段，比如在去中心化交易所中先拉盘再抛售，以及通过设置合约使某些虚拟货币无法卖出的“貔貅盘”，这些新的诈骗手段都为执法部门的调查、取证工作带来了新的挑战。

2021 年虚拟货币诈骗相关的典型案例：

1、上海市公安局闵行分局破获“EEE 虚拟货币”诈骗案件，犯罪嫌疑人宣传其发行的 EEE 虚拟货币不仅是国家支持的项目还可以在国外虚拟货币平台兑现。闵行公安分局刑侦支队反诈中心会同属地派出所开展集中行动，共抓捕违法犯罪嫌疑人 7 人。经初步调查，该案件涉及被害人 600 多人，涉案资金 2800 余万元。

2、公安部挂牌督办、四川省公安厅提级侦办的特大电信网络诈骗案件“509”专案已一审审结。犯罪嫌疑人通过在直播过程故意露出赚取巨额利润的虚拟货币账户等手段，诱使被害人投资虚拟货币，共计骗取 500 余名被害人的金额逾 1.4 亿元。该案是近年来四川法院系统审理的被告人数最多、犯罪链条最为完整的投资理财类电信网络诈骗案件。

（四）盗窃

虚拟货币盗窃类案件主要是以虚拟货币为对象，不法分子通过获取受害人持有的虚拟货币的公钥和私钥、虚拟货币交易所登录密码等非法获取虚拟货币。

虚拟货币盗窃案件的作案手法相对较为多样，不法分子会通过使用钓鱼网站、对受害人的电子邮箱进行攻击、伪造受害人身份证挂失并办理手机卡等方式获得受害者的交易所密码等重要信息，然后转移受害者持有的虚拟货币。

另外，由于受害人自身密码或私钥管理不慎导致泄露也给了一些别有用心的不法分子可乘之机。

2021 年虚拟货币盗窃相关的典型案例：

1、南昌警方成功破获全省首例利用黑客网络技术盗取区块链货币的新型网络犯罪案件。报案人黄某发现自己的手机号码被人莫名挂失，继而发现与手机号码捆绑登录的“雷达网”账户中市值近 1450 万元人民币的虚拟货币被人转走。民警研判发现，案发前曾有 5 名江苏连云港籍人员开车窜至南昌，持伪造的受害人身份证件挂失、补办受害人手机卡的犯罪踪迹。3 月 8 日，南昌警方抓获 4 名犯罪嫌疑人，并于 15 日赴广东抓获 2 名犯罪嫌疑人。

2、江苏省徐州市铜山区公安局打掉一个盗窃虚拟货币犯罪团伙。该团伙通过搭建钓鱼网站盗取他人登录交易网站的账号和密码，短短两个月的时间，共获利 500 余万元，受害民众 30 多人。

（五）支付非法活动

由于虚拟货币的“价值”仍被很多人接受，所以其在现实生活的很大范围内可以充当一般等价物，特别是犯罪分子愿意接受虚拟货币作为犯罪中的支付工具，尤其是在涉及到毒品、赌博、枪支、色情服务业、游戏外挂等黑灰产业链犯罪中。

此外，由于虚拟货币的匿名属性，其也被不法分子用于转移非法活动所得、进行计算机勒索活动等。

2021 年虚拟货币用于支付非法活动的典型案例：

1、江苏昆山警方破获一起全球最大的游戏外挂案件，涉案人员遍布全球，经营国内外多个游戏外挂，流水达数亿元。该挂组织全球财务负责人王某某表示，负责把卖外挂销售利润，根据上线要求，每隔十天需要给成员发放薪酬，只使用比特币进行分发。

2、盐城建湖警方破获 EOS 公链“Biggame”赌博平台，该平台交易量长期高居 EOS 公链日交易额榜首，日均投注金额折合人民币达 1000 余万元，最高峰时日活跃参赌人员达 1 万余人，近一半赌客为国内人员。公安机关已查明，该平台参赌人员高达 7.3 万余人，涉及境内外 17 个国家和地区，涉案资金达 80 亿元，违法所得 6000 余万元，抓获位于广州、上海、安徽滁州等地的藏匿窝点的犯罪嫌疑人 25 名，查扣涉案虚拟货币 130 余万个，价值人民币 2600 余万元。

（六）挖矿

2021 年，虚拟货币挖矿活动遭受重大打击。9 月，国家发改委等 11 部门发布《关于整治虚拟货币“挖矿”活动的通知》，全国各省市都加大了对虚拟货币挖矿活动的整治。

虚拟货币挖矿由于能源消耗和碳排放量大，其盲目无序发展与我国碳达峰碳中和和高质量发展目标背道而驰，发改委也在《产业结构调整指导目录(2019 年本)》中将“虚拟货币‘挖矿’活动”列入淘汰类产业清单。

与虚拟货币挖矿相关的案件主要集中在判定比特币等虚拟货币相关的挖矿交易合同无效，以及盗用电力进行比特币挖矿等。

2021 年虚拟货币挖矿相关的典型案例：

1、鞍山市公安局铁东分局破获一起为获取比特币使用“挖矿机”从而盗电近百万元的特大盗电案件，该盗电团伙自年初以来在该地区租下一个平房进行比特币挖矿，并利用窃电装置盗取某公司厂房内的电，累计盗电价值达 120 余万元。铁东公安组织 20 余名警力，分成 3 个抓捕组，在查明的“挖矿”设备放置点和犯罪嫌疑人居住地，同时展开抓捕行动。当场抓获涉案人员 3 人，查封“挖矿”设备 161 台，并现场查获了盗电设施。

2、北京朝阳法院公开开庭审理并宣判了一起因比特币挖矿迟迟未见收益而引发的服务合同纠纷。法院一审认定合同无效，判决驳回原告要求支付巨额比特币收益的诉讼请求。该案系北京法院首例认定比特币挖矿合同无效案。案件宣判后，朝阳法院反馈案件中涉及的虚拟货币“挖矿”活动线索，建议有关部门进行清理整治。

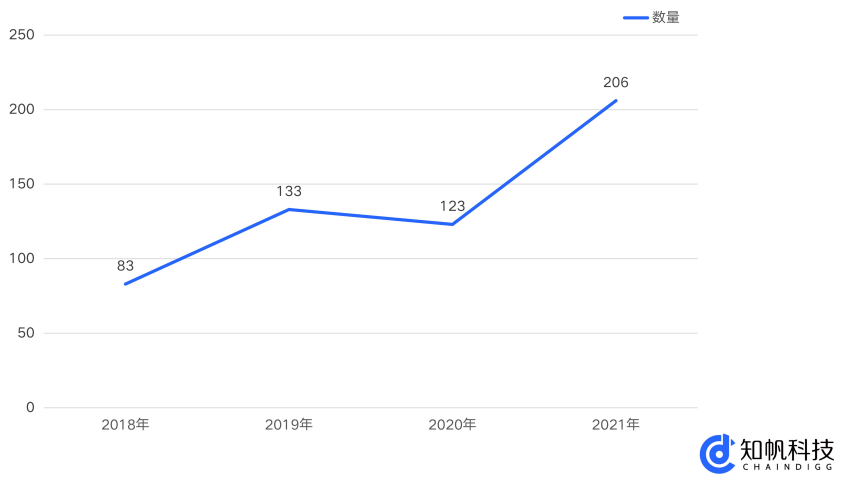
3、11 月 13 日，江西省政协原党组成员、副主席肖毅被“双开”。原因是“滥用职权引进和支持企业从事不符合国家产业政策要求的虚拟货币‘挖矿’活动，违规举债上项目、搞建设，造成恶劣影响”。

第三章 2021 年区块链安全事件综合分析

本章中，基于收集的区块链安全事件进行统计和调研，通过数量趋势、领域分布、时间分布、典型安全事件盘点等维度，对区块链安全事件发展趋势进行综合分析，并对 2022 年作出展望。

一、2018 年至 2021 年区块链安全事件数量呈上升趋势

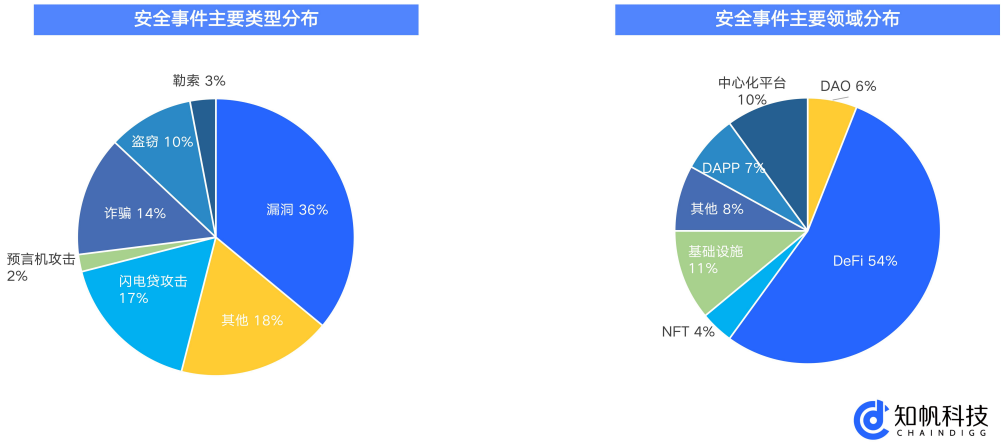
2018年至2021年区块链安全事件数量



在过去几年中，区块链安全事件数量整体呈上升趋势。数据显示，2019 年，随着虚拟货币市场复苏走出熊市，区块链安全事件数量急剧增多，相较于前一年增长超 60%；2020 年，DeFi 领域在下半年的发展推动虚拟货币市场规模达到了前所未有的高度，但区块链安全事件数量整体上同 2019 年保持持平；2021 年，DeFi 的应用发展加之 NFT、元宇宙等新概念的出现，使得区块链安全事件的数量再次猛增，相较于 2020 年增长 67%。

二、2021 年区块链安全事件主要类型及领域分布

2021年区块链安全事件主要类型及领域分布



从安全事件主要领域分布上看，DeFi 领域是 2021 年区块链安全领域的重灾区，占比高达 54%，位居首位，2020 年下半年开始的 DeFi 热潮吸引了大量投资者进入这一领域，这也吸引了黑客的关注，未审核的代码以及不严谨的治理模式都为黑客留下了攻击的机会，闪电贷攻击更是成为了很多 DeFi 项目的噩梦。

从安全事件主要类型分布上看，漏洞占比 36%位居首位，然后是其他类型和闪电贷攻击，分别占比 18%和 17%。

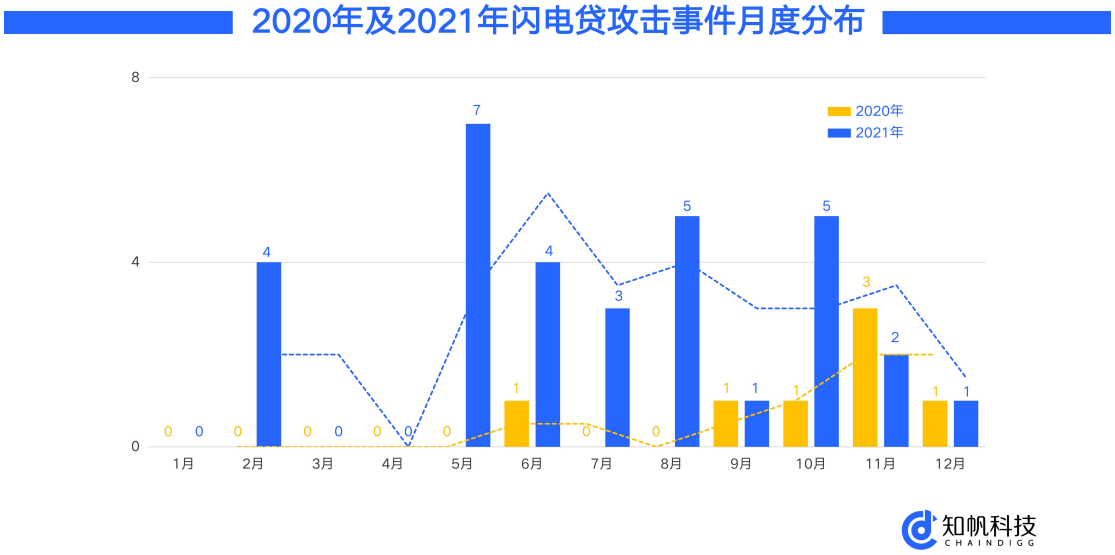
从损失情况上看，诈骗项目和跑路项目带来了更多的经济损失，特别是在 2021 年随着 NFT、链游、元宇宙等概念的火热，大量不法分子借用这些概念大肆炒作空气币，然后通过砸盘、限制卖出等方式进行收割。

此外，世界各国的执法机构也加强了对区块链和虚拟货币相关犯罪活动的打击力度，大量涉及虚拟货币的洗钱、传销、诈骗、盗窃等的不法分子被抓获，有力的监管保证了行业的健康有序发展，同时也保护了国家和广大人民群众的利益不受侵犯。

三、2021 年区块链安全事件月度分布

从 2021 年链上安全事件发生的时间来看，1 月至 3 月链上安全事件数量明显呈上升走势，这与整个虚拟货币市场的走势基本保持同步，此后链上安全事件数量居高不下，并在 7 月份达到顶峰。

四、2020 年及 2021 年闪电贷攻击事件月度分布



在 2021 年发生的链上安全事件中，发生在 DeFi 领域的超过半数，其中最典型的就是闪电贷攻击。闪电贷攻击在 2020 年夏天的 DeFi 热潮中崭露头角，在 2021 年，随着更多资金

流入 DeFi 领域，闪电贷攻击这一攻击手段也被黑客运用的越来越多，在 2021 年 5 月开始明显上升。整体数量上，2021 年较 2020 年也呈现上升趋势。

2021 年发生的重要的闪电贷攻击事件：

1、DeFi 借贷协议 Cream Finance 在 2021 年 2 月、8 月和 10 月三次遭到闪电贷攻击，总损失约 1.7 亿美元。被盗的资金主要是 Cream LP 代币和其他 ERC-20 代币。

2、2021 年 10 月，币安智能链上的 DeFi 收益聚合器 PancakeBunny 遭遇闪电贷攻击，损失 114,631.5421WBNB 和 697,245.5699BUNNY，合计约 4500 万美元。

3、2021 年 2 月，Yearn v1 yDAI vault 遭到闪电贷攻击，攻击者获得 280 万美元，而 vault 则损失 1100 万美元。

4、2021 年 12 月，Fantom 链上复合收益平台 GrimFinance 遭遇闪电贷攻击，损失超过 3000 万美元。

五、部分典型区块链安全事件盘点

（一）项目跑路/砸盘骗局

项目跑路和砸盘骗局一直以来都是区块链行业无法摆脱的顽疾，特别是每当行业迎来高速发展的繁荣期时，各种打着区块链相关概念幌子的骗局也如雨后春笋般出现，对跟风进入的投资者进行收割。

2021 年区块链行业迎来了前所未有的发展，行业中的 NFT、元宇宙、链游等概念频频出圈，吸引了一些投资者的入场，不法分子通过引诱投资人购买空气币、投资貔貅盘、跑路砸盘等方式获取了大量的非法资产。

2021 年发生的重要项目跑路/砸盘骗局：

1、2021 年 5 月，SEC 对 5 名 BitConnect 项目的推广者提起诉讼，该项目从散户投资者处筹集了超过 20 亿美元的资产。BitConnect 是在 2017 年推出具备庞氏骗局特征的一项虚拟货币投资计划，其代币 BCC 是当时价值最高 20 种虚拟货币之一，市值超过 26 亿美元。

2、2021 年 6 月，虚拟货币投资平台 Africrypt 创始人失联，平台上 6.9 万枚比特币（当前价值约为 23 亿美元）被转移。投资者的律师调查发现，Africrypt 平台的资金已经从其账户和客户钱包中转移，并进入比特币混币器进行混币。

3、2021 年 3 月，币安智能链项目 Meerkat Finance 疑似跑路卷走约 3100 万美元，其中包括 1400 万 BUSD 和 7.3 万个 BNB。项目方则自称是受到黑客攻击盗走了所有资产。

4、2021 年 5 月，币安智能链 DeFi 协议 DeFi100 官方网站无法访问，约有 3200 万美元的用户资金被团队卷走跑路。

5、OHM 仿盘项目 AnubisDAO 上线一天后撤走流动性池卷款跑路，共逾 13556 枚 ETH 被转移，价值约 5830 万美元。

（二）合约漏洞

从技术的角度上看，很多区块链安全事件都是可以避免的。合约中的代码和逻辑漏洞要么直接导致项目异常，要么被黑客利用，导致项目资产遭受严重损失。由于合约一经部署自动运行且涉及大量虚拟货币资产相关的操作，这也再次凸显了代码安全审查等合约质量保障工作的重要性。

2021 年由合约漏洞导致的典型安全事件：

1、2021 年 8 月，跨链互操作协议 Poly Network 遭到攻击，共计超 6.1 亿美元转出。该项目被攻击的原因在于由于代码漏洞，其 EthCrossChainData 合约的 keeper 被黑客修改。

2、去中心化借贷协议 Compound 在执行 062 号提案后，流动性挖矿出现 COMP 代币分发异常情况。问题原因是根据 062 号提案进行 COMP 代币分发的速率初始设定出错，导致过多 COMP 代币被分发。修改相应代码必须通过治理，最少需要 7 天时间。

3、2021 年 5 月，DeFi 协议 ValueDeFi 连续遭到黑客攻击，由于合约漏洞，项目中所有非 50/50 的交易池都被黑客利用。经确认，两次攻击造成的总损失达 1500 万美元。

4、2021 年 5 月，链上期权协议 FinNexus 的代币 FNX 在短时间内在被大量铸造、转出或售出，涉及 BSC 和以太坊上超过 3 亿个 FNX 代币（约 700 万美元），原因在于合约所有者的权限被修改。

（三）私钥被盗

虽然从事件发生的数量和金额总和上看，私钥被盗导致的虚拟货币资产失窃事件在所有区块链安全事件中占据的比例并不高，但是一旦某个项目或交易所的钱包私钥失窃，其势必会导致大量自身或者客户资产的损失。

2021 年由私钥被盗导致的安全事件包括：

1、2021 年 12 月，虚拟货币交易平台 Bitmart 遭黑客窃取 1.96 亿美元，其中约 1 亿美元来自以太坊区块链的各种虚拟货币，9600 万美元来自币安智能链上的货币，资产失窃主要是由于两个热钱包被盗私钥造成的。

2、2021 年 12 月，Vulcan Forged 的 148 个持有 PYR 的钱包遭到入侵，超过 450 万 PYR 已被盗，价值达 1.45 亿美元。

3、2021 年 12 月，交易所 AscendEX 热钱包异常，发生了一些未经授权的转账。损失高达 7770 万美元。

4、2021 年 4 月，黑客将大量 EASY 代币从 EasyFi 官方钱包转移到以太坊网络和 Polygon 网络上未知钱包，涉及资产 4690 万美元，本次事件为助记词破解安全事件，EasyFi 智能合约未被黑客利用，只是 MetaMask 的助记词短语或管理员密钥遭到远程攻击。

5、2021 年 11 月，黑客通过网络钓鱼攻击获得了 bZx 平台上用于与 Polygon 和币安智能链区块链集成的两把私钥，通过私钥发起无限制消费操作，成功盗取 bZx 平台价值约 5500 万美元的虚拟货币资产。

六、2022 展望

2022 年的区块链和虚拟货币行业，仍将在过去十几年的发展基础上高速迭代，一方面寻求探索解决自身的顽疾，一方面新的项目优胜劣汰不断更新演进。区块链和其他技术的融合将真正打造能够进入主流人群的杀手级应用，这也是所有行业从业人员的期待。

展望 2022 年，区块链行业整体上仍然会保持发展的趋势，但是也会受到行业自身的发展周期的影响；监管将成为整个行业在进入主流人群之前无法逃避的一个问题；行业中会出现新的热点概念和项目，以及随之而来的新的泡沫；DeFi 和 NFT 等领域内的细分赛道将会有充分发展的机会，DAO 则可能会改变人们的工作方式。

在区块链安全领域，DeFi 仍然是业内人士同不法分子交战的主阵地，随着 DeFi 应用中资产金额的继续增加，各种新的 DeFi 玩法的出现，黑客会更加积极的寻找合约代码和机制中的漏洞进行攻击，而项目方则需要在代码审计、业务模型设计、治理流程上做好安全防御工作，避免自己成为黑客的提款机。执法机构也需要提前为此做好准备，增加对 DeFi 领域的重视程度和投入力度，为这一领域可能发生的安全事件设计好预案，在调查、取证等方面部署好相应的工具。

随着资产规模的增大，NFT 和 DAO 领域将成为黑客攻击的新热点，黑客会对 NFT 项目和 DAO 项目发起攻击，攻击方式可能是链上的，也可能是链下通过攻击获取治理社区的管理账号或权限。

在区块链行业中的新概念仍将层出不穷，不管是 NFT 或 DeFi 等现有模式的细分领域的延伸，还是元宇宙或 Web3.0 等宏大的愿景，或是 DAO 或 XXX To Earn 的新的模式，都可

以被不法分子用来作为噱头进行诈骗，投资者仍需擦亮眼睛，做好功课，谨慎进行虚拟货币投资。

对于行业中的参与者和投资者来说，管理好自己的私钥仍然是重中之重，在过去几年中，很多大的项目或者交易所因为私钥被盗导致了巨额的资金损失，在 2022 年，此类虚拟货币盗窃事件仍然会大量发生。

虚拟货币仍将被不法分子用作转移非法资产、洗钱、勒索、赌博、暗网交易等活动，他们会通过使用隐私币、混币等方式逃避追踪，不过随着全球范围内的虚拟货币监管政策的完善，以及大量合法实体部署 KYC 和 AML 等合规流程，不法分子在虚拟货币领域中的空间将越来越小。

第四章 2021 年区块链安全与犯罪领域关键词

本章中，知帆科技根据 2021 年度热点事件的分析和统计，结合专家评议，盘点出 2021 年区块链安全与犯罪领域十大关键词，以此来回顾 2021 年该领域的事态发展。

一、NFT

NFT 是 Non-Fungible Token（非同质化代币）缩写，定义了一种不可分割的、具有唯一性的代币交互和流通的接口规范。每个 NFT 代币都是独一无二的，可以用来作为独一无二的数字资产的所有权证明。

2021 年被称为是“NFT 元年”，艺术家 Beeple 创作的 NFT 作品《Everydays - The First 5000 Days》在佳士得拍卖行以超过 6000 万美元的价格成交，使得 NFT 概念迅速走红，在区块链行业内部，大量 NFT 平台和 NFT 项目上线或获得融资，在行业外部，艺术家和明星名人争相发布 NFT 作品，各个行业的公司都纷纷跨界涉足 NFT。

在区块链安全和犯罪方面，不法分子也利用了投资者对 NFT 市场和技术的不了解，通过多种方式实施诈骗和犯罪行动，其中主要可以分为四种手段：

（一）投资骗局

打着 NFT 的幌子诱骗投资者对某些没有价值的虚拟货币或 NFT 代币进行购买或投资，特别是在“无聊猿”和“加密朋克”等头部 NFT 收藏品爆火之后，不法分子在市场上推出了大量仿盘，吸引大量没有经验和判别能力的投资者购买。

（二）项目攻击

通常 NFT 项目在代币分发之前都会先在 Discord 等社交媒体上建立收藏者社区，在社区中公布项目相关的进展和分发计划，不法分子会利用 Discord 的安全漏洞获得该社群的管理员权限，发布假的铸币地址信息骗取参与者的资金。

（三）NFT 盗窃

随着某些收藏品的 NFT 价值的持续上涨，一些不法分子也会直接以 NFT 代币为作案对象进行盗窃，然后再到 OpenSea 等 NFT 交易市场上转售变现。

（四）伪造 NFT

虽然 NFT 藏品在链上是唯一且不可复制的，但是由于 NFT 的内容载体是公开的，不法分子可以伪造或剽窃知名的 NFT 作品图片，将其另行铸造 NFT 代币，进而售卖给不知情的

收藏者。另外仿冒 NFT 平台也是常见的诈骗手段，用户看起来该网站与官方平台网站一样，诈骗者会试图盗取用户的个人信息。

二、DeFi

DeFi 和 NFT 一样，都是区块链领域的原生概念，其在 2020 年夏天成为行业热点，在经历了高潮和泡沫之后，在 2021 年进入平稳发展阶段，DeFi 应用也从最早的 DEX（去中心化交易所）、流动性挖矿、数字资产质押等扩展进入了更多领域。

在区块链安全和犯罪方面，随着 DeFi 领域的发展，不法分子也将一些犯罪行为转为通过智能合约实现，或是对一些 DeFi 项目进行攻击，其中主要的手段和方式包括：

（一）使用智能合约进行传销

犯罪分子利用了 DAPP（去中心化应用）智能合约一经部署自动执行、参与者更加匿名的特性，将传销规则使用智能合约代码实现，使得其犯罪行为更加隐蔽，并增加了执法机构调查和取证的难度。

（二）通过去中心化交易所进行诈骗

在去中心化交易所上，不法分子可以为其发行的“空气币”建立流动性池，然后诱骗投资者在该去中心化交易所上购买，可以再通过抛售砸盘的方式攫取投资者的资金。

（三）闪电贷攻击

闪电贷是一种区块链上的无担保贷款，不过借款者需要在一个区块内归还贷款，如果贷款未被归还，则借款行为也无效。闪电贷攻击是 2021 年针对 DeFi 项目的最主要的攻击类型，攻击者往往通过将借出的大量资金转入去中心化交易所或借贷协议，使得某些虚拟货币的价格大幅上涨或下跌然后从中获利。

（四）漏洞攻击

随着越来越多的应用通过智能合约实现，智能合约设计本身的一些漏洞也会被黑客用来发起攻击，其中主要的漏洞包括合约机制漏洞、代码漏洞、治理漏洞等。

（五）预言机攻击

预言机是区块链的基础设施，是将区块链外的信息导入区块链的一种方式。使用去中心化预言机获取虚拟货币的价格数据常被用来作为应对闪电贷攻击的一种手段，不过不法分子仍然有机会通过对预言机进行攻击导致 DeFi 项目的价格出现异常进而获利。

三、交易所

中心化虚拟货币交易所一度在区块链行业中处于中心位置，在 2021 年，一方面加密市场的蓬勃发展使得交易所的交易量、用户量和收入大幅增加，另一方面它们也迎来了更有活力的去中心化交易所的冲击，面临着被后来者超越的风险。在区块链安全和犯罪方面，不同的交易所在 2021 年也经历了不同的挑战。

（一）合规上市

美国的虚拟货币交易所 Coinbase 在 2021 年成功上市，这被认为是虚拟货币行业被主流接受的关键一步，Coinbase 的合规以及同相关监管部门的积极合作对其上市起到了关键作用，随着各个司法管辖区中虚拟货币监管政策的逐渐明确，合规将成为交易所必须要重视的问题。

（二）资金被盗

同以往一样，中心化交易所的钱包中由于存储了大量用户的虚拟货币，仍然是黑客重点攻击的对象，在 2021 年，Bitmart、AscendEX 等多家中心化交易所遭遇盗币行为，资产安全仍然是中心化交易所需要解决的问题。

（三）〝清退〞

2021 年 9 月，中国人民银行等 10 部门发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》，明确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。这使得 Huobi、OKEx、Binance 等三大交易所开始彻底“清退”中国大陆地区的用户。

四、Meme 币

Meme 币也称为模因币，来源于互联网的模因文化，主要指由互联网和社交媒体上的模因文化或笑话激发产生的虚拟货币。第一个也是最有代表性的 Meme 币是狗狗币，灵感来源于 2013 年网络上流行的一个日本柴犬表情图片。在 2021 年上半年，狗狗币的价格在马斯克等有影响力的名人的推动下节节走高，引来了众多模仿狗狗币的虚拟货币，这些 Meme 币多以动物命名，因此也有很多人将其称为动物币。

Meme 币的供应量往往很大，并且没有销毁机制，这使得这些虚拟货币的价格极低，可能只需几美元就能买到上万或百万个 Meme 币；此外，这也导致了 Meme 币的价格高度波动，由于其价格主要都是由社区主导的，所以可能会由于知名人士的力挺一夜之间价格飙涨，也可能会由于社区成员的离开而价格暴跌。2021 年，最受欢迎的 Meme 币是狗狗币和柴犬币。

（一）狗狗币 Dogecoin（DOGE）

狗狗币由软件工程师 Billy Markus 和 Jackson Palmer 于 2013 年创建。作为莱特币的分叉，狗狗币采用了工作量证明（POW）机制，并且没有最大供应量的限制。

（二）柴犬币 Shiba Inus（SHIB）

柴犬币是 DOGE 的竞争对手，通常被称为“Dogecoin 杀手”。SHIB 也是以日本的一个狗种命名的。它是由一个名叫 Ryoshi 的匿名开发者在 2020 年 8 月创建的。DOGE 和 SHIB 的主要区别是，后者的供应量有限，只有 1000 万亿个代币，其中 50%被烧毁并捐赠给慈善机构。SHIB 的生态系统还包括去中心化的交易所，NFT、一个 NFT 艺术孵化器和一个 NFT 游戏。

五、元宇宙

元宇宙（Metaverse）是 2021 年区块链领域最火的一个概念，虽然定义尚无共识，但业内基本都认可其为一个与现实有某种联系的虚拟数字空间，用户可以通过有沉浸感的交互方式在其中进行社交和协作。

元宇宙的概念符合全球疫情的大背景下人们生活由实转虚的潮流，也为互联网行业和科技巨头提供了宏大的愿景，社交巨头 Facebook 的强势入场更是把这场元宇宙狂欢推向高潮，一时间其他大公司也纷纷跟进。

在区块链安全和犯罪方面，由于元宇宙仍处于概念阶段，并没有真正意义上落地的场景，因此不法分子主要是打着元宇宙的幌子进行犯罪活动，将其发布的无价值的虚拟货币通过包装，诱骗不明真相的投资者购买，骗取投资者的资金。

六、Play To Earn

Play To Earn（“玩赚”）是区块链游戏领域的概念，指游戏的玩家在区块链游戏中，不再是付费玩游戏，而是可以通过玩游戏赚取虚拟物品或虚拟货币，并可以将这些虚拟资产变现。

这种模式也被称作 GameFi（Game Finance，游戏化金融），即在 Game 中引入 DeFi 以及 NFT 质押，并且将玩家的资产转化成游戏内资产或代币资产等，通过流动性挖矿提升玩家收益。

链游成为热点一方面是受元宇宙概念的影响，因为区块链游戏是目前最为接近元宇宙概念的产业，或者说是元宇宙的雏形；另一方面，头部链游项目 Axie Infinity 在全球范围内走红，吸引了大量玩家加入打金，日收入一度超过传统头部游戏《王者荣耀》。

不过在链游概念火热的背后，仍然存在着明显的安全问题，目前链游的可玩性还比较差，不管是哪种类型的链游，玩家的收入从某种意义上说都是来自新玩家投入的资金，有着资金盘的嫌疑。目前链游的主要类型包括：

（一）收藏类链游

最早的“加密猫”就属于这一类型的链游，游戏参与者可以收集不同类型的虚拟动物 NFT，不同的 NFT 有不同的属性，并且游戏中的繁殖机制使得这些 NFT 可以为玩家产生新的 NFT。

（二）经营类链游

玩家在游戏中通过战斗、挖矿、种地等形式获取虚拟道具或虚拟货币，但是获取这些虚拟资产之前需要质押一定的虚拟货币或者投入资产购买相应的生产资料或道具。

（三）虚拟地产类链游

这类链游高度自由化，玩家可以在开放的虚拟世界中进行探索，也可以在其中投资购买虚拟地产，在没有明显的市场需求的情况下，这种投资虚拟地产的行为很可能因为市场炒作成为泡沫而崩盘。

七、“土狗”项目

“土狗”项目是 2021 年区块链投资领域的一个新生词汇，主要是指无白皮书、无创始团队信息、没有代码审计的项目方发行的没有任何价值的虚拟货币，项目方的目的就是借助行业内的热点，骗取想要一夜暴富的投资者的资金。

“土狗”项目反映了区块链安全和犯罪领域的监管真空，投资者的权益难以被保护，虚拟货币的匿名性、发行代币和建立资金池的便捷性、投资者的盲目跟进都造成了如今“土狗”项目猖獗的现状。

“土狗”项目对投资者进行“收割”的主要方式包括：

（一）砸盘跑路

也被称为 Rug Pull，指项目方突然抛售大量代币或者撤出流动性池的资金导致投资者蒙受损失的情况，在“土狗”项目中，从上线到跑路的时间周期长则不到一个月，短则不到一日。

（二）貔貅盘

也被称为 Honeypot，指项目代币的合约通过某些代码设置了代币的交易行为，比如只能买入不能卖出等，使得投资者蒙受损失。

八、挖矿

挖矿是指区块链上的节点通过计算或其他方式增加区块链区块并获取奖励的过程。很长时间以来，中国大陆地区的虚拟货币“矿工”提供了区块链行业中相当比例的算力，但是以比特币为代表的工作量证明类代币在挖矿过程中造成的大量能源浪费也饱受诟病。

2021 年 9 月，国家发改委等 11 部门发布《关于整治虚拟货币“挖矿”活动的通知》，宣布虚拟货币“挖矿”活动将被正式列为淘汰类产业。全国各地对挖矿行为采取“清零”政策，严厉打击非法挖矿活动，大量矿工将矿机转移海外。

整体来看，中国治理挖矿的措施并未对全球区块链行业产生重大影响。从区块链安全和犯罪的角度上看，涉及挖矿的主要方面包括：

（一）盗窃电力挖矿

在全国大范围内整治虚拟货币挖矿行为之前，盗窃电力挖矿的犯罪活动就一直存在，随着相关部门打击挖矿活动力度的加大，此类犯罪活动将逐渐减少。

（二）挖矿木马

不法分子通过外挂程序、漏洞利用、网页挂马、弱口令等传播途径植入挖矿木马，控制受害者的计算资源来挖矿，从而赚取虚拟货币。挖矿木马会潜伏在用户的电脑中，定时启动挖矿程序进行计算，大量消耗用户电脑资源。在利益的驱使下，近些年此类犯罪持续出现，随着挖矿木马的升级和变种，未来挖矿木马的热度也会持续下去。

（三）挖矿合同纠纷

此类案件的数量在整治挖矿活动之后开始增加，虚拟货币的生产交易环节被认为威胁国家金融安全，社会稳定衍生风险突出，违反公序良俗，因此相关虚拟货币挖矿合同应属于无效合同。挖矿活动中出现的政策风险、技术风险及由此引发的投资损失风险，应由投资者自行负担。

（四）FIL 挖矿

虽然名为挖矿，但是 FIL 矿机挖矿和比特币挖矿并不相同。FIL 挖矿指存储挖矿，是基于分布式存储 IPFS 挖矿，主要依靠存储能力来挖矿：矿机的存储内存越大，挖矿能力就越强，获得相应的 Filecoin 奖励就越多。FIL 挖矿的机制是存币生息模式，表面上矿工可以购

买不同公司的矿机来挖矿获得报酬，根本上却是一个个资金盘。在 2021 年，随着星际联盟等主要 FIL 矿机公司都因涉嫌传销被查，Filecoin 这一在中国活跃多年的项目也被定性。

九、DAO

DAO 是 Decentralized Autonomous Organization（去中心化自治组织）的缩写，通过事先约定的议事规则来协调成员的行动和资源，允许投资者从世界任何地方匿名汇款，然后向这些贡献者提供代币，让他们拥有对议案的投票权，这一过程完全通过智能合约实现。

发生在 11 月中旬的 Constitution DAO 参与美国宪法拍卖使 DAO 成为区块链领域的热点。DAO 在加密社区中的火热也吸引了大批的投机者和不法分子，很多 DAO 项目被他们当作牟取暴利的工具，特别是一些在短时间内通过社区炒作、营销、拉盘来博人眼球的项目。

从区块链安全和犯罪的角度上看，参与 DAO 项目可能涉及的风险包括:

（一）项目代币集中

很多项目本身手中都掌握了超过总量 50%的代币，一般以 DAO 治理、流动性激励等名义持有。随着其治理代币价格的短期上涨，项目方套利砸盘的风险增大。

（二）钱包私钥泄漏

DAO 项目大多未经专业审计机构审计，用户在申领代币时需要向智能合约授权，这可能导致用户钱包私钥泄露，进而导致资产被盗。

（三）诈骗风险

一些不法的 DAO 项目可能会故意往加密 KOL 的合约地址转币伪造大佬买入的假象诱骗普通用户购买，但当用户买入后，却发现这些代币无法卖出，最终产生损失。

（四）监管问题

由于 DAO 的去中心化和无国界的性质，如何对其进行监管仍然是一个空白领域。现实世界的法律系统还没有承认 DAO 系统的合法性。

十、数字人民币

数字人民币是由中国人民银行发行的数字形式的法定货币，由指定运营机构参与运营并向公众兑换，以广义账户体系为基础，支持银行账户松耦合功能，与纸钞硬币等价，具有价值特征和法偿性，支持可控匿名。虽然数字人民币同虚拟货币一样都属于数字资产，但是二者有本质上的不同，数字人民币是法定货币，并且在技术上，并非依赖于区块链技术。

在2021年下半年，随着中国政府推广数字人民币力度的加大，中国的多个试点城市和机构都开始大范围使用数字人民币，数字人民币也被用于人们吃穿住行用等各个不同的使用场景，这也引起了不法分子的注意。

（一）利用于洗钱

由于数字人民币具有支付更便捷、无需经过第三方网络、支持可控匿名等特点，数字人民币被一部分不法分子利用于洗钱犯罪方面，帮助藏匿在国外的犯罪分子处理诈骗等非法收入。

（二）衍生出的相关诈骗

不法分子将数字人民币结合到电信诈骗的老套路当中，衍生出了一些新型诈骗套路，例如：数字人民币短信诈骗，以“抢先体验数字人民币”“数字人民币预约中签”等为噱头的诈骗套路；假借推广高收益“数字人民币”项目，诱使受害人充值，甚至是参与传销；冒充公检法诈骗中要求受害者开通数字人民币钱包。

第五章 2021 年八大虚拟货币典型骗局

近年来，虚拟货币相关的骗局不断更新迭代，新一代骗局往往更具欺骗性与危害性。在本章中，总结提炼出 2021 年的一些典型骗局并对其进行分析，以期引起广大网民注意。

一、云算力挖矿 萌新韭菜的〝盛宴〞？

比特币、以太坊等虚拟货币价格的高涨带动了全球“挖矿”热潮，各种高端显卡、笔记本更是供不应求，价格一路飙涨。此时，一种号称可以租赁代替购买、矿机由矿场统一管理、低投入高收益低风险的“云算力挖矿”引得不少跟风的投资者争先恐后加入“挖矿”这门生财之道。

国内知名 FIL 矿商“人人矿场”以“联合挖矿”的名义宣传，将矿机租赁给客户，并承诺高额的年化回报率，还拥有大量的真实矿机和实体矿场。然而，人人矿场的高收益并不完全是通过挖矿产生，其所谓的“挖矿”占比为 20%，剩下的 80%则是挖的“空气”。人人矿场对外宣称矿机数量达到 15000 台，实际情况却是只有 3000 台左右。每一个去实地矿场考察的人都会确实看到矿机在工作运转，但所见的四川甘孜的矿机数量，是远小于全网矿工租赁总量的。

2021 年 12 月 17 日，人人矿场因涉嫌违法犯罪，公司高层包括吴某在内的 21 人全部被警方在办公场地带走调查，人人矿场也正式走向崩盘。

分析：

我国已正式将虚拟货币“挖矿”纳入淘汰类产业，虚拟货币“挖矿”看似一本万利，背后却隐藏着经营失败、投资炒作、卷款跑路等众多风险，有损社会公共利益。

随着比特币投机热潮的褪去，不少矿商的“真面目”也显露无疑。人人矿场的操盘手吴某早期通过核心成员拉拢熟人的方式，诱以高年化回报率，获取种子客户。并以套现购买比特币炒币获利的方法，发放矿工收益。后通过出租“空气矿机”，拉人头填坑，不断扩大资金盘，来维持盘面运转，是典型的庞氏骗局。

二、蹭热点割韭菜〝鱿鱼币〞暴涨后 5 分钟跌零

2021 年 11 月 1 日，与热播网剧《鱿鱼游戏》同名的虚拟货币“SQUID（鱿鱼币）”价格突然一路飙升，疯涨几十万倍达到 2861.8 美元顶点。币价的上涨引发不少“嗅觉敏锐”的投资者跟风入场。

然而令人没想到的是，鱿鱼币在达到顶点后的 5 分钟内突然“闪崩”，迅速跌至 0.0007 美元，几乎为零，令投资者们血本无归，损失了数百万美元。

据悉，10 月 26 日鱿鱼币发行价仅为 1 美分，闪崩之前，有关平台就多次收到情报称用户无法在去中心化交易所 PancakeSwap 出售鱿鱼币。

分析：

这是一个典型的“Rug Pull（拉地毯）”骗局，即开发者推出虚拟货币吸引买家，然后突然停止交易并卷走交易所得，仿佛猝不及防地拉走别人脚下地毯。与传统的成熟的投资市场不同，虚拟货币的价格波动剧烈，具有更大的不稳定性和不可预测性。

分析显示，该项目的创始人使用 Tornado Cash 协议隐藏交易细节，从而转移资金，并兑现了等值的币安币（BNB），目前，该地址已经被注记为“涉及骗局”。

三、币安英雄（BNBH）一夜闪崩 链游是游戏还是投机？

火遍全球的元宇宙带动了虚拟货币市场 GameFi 的热潮。由于政策对虚拟货币挖矿的禁止，市场急需挖矿概念的代替品，主打“边玩边赚”（Play to Earn）的 GameFi，也叫做区块链游戏，即链游，吸引了无数人入场。

2021 年 12 月 6 日，一度十分火爆的链游项目币安英雄 (BNBH) 币价狂跌，PancakeSwap 的 BNBH/WBNB 流动性池的流动性在 2021 年 12 月 5 日至 2021 年 12 月 7 日期间断崖式下跌。

从宣传，到上线交易所，再到崩盘，币安英雄（BNBH）只花了 15 天。最高点时炒得多火热，崩盘时亏得就有多狠，一夜之间，无数人血本无归。

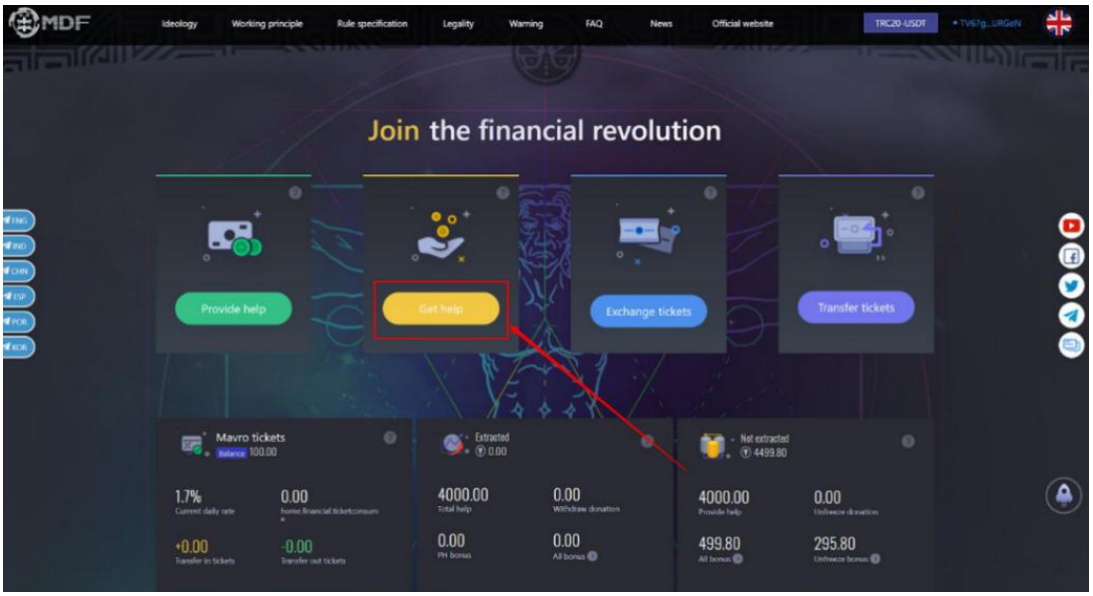
分析：

添加了金融属性的“游戏”不再是单纯的游戏，链游一直都是套了游戏外壳，具有投资、投机、套利属性的“金钱游戏”。如今市面上的链游鱼龙混杂、良莠不齐，不少链游的可玩性并不高，项目方的核心工作不是提高游戏性，而是维持游戏的经济体系，必须不断有新人涌入才能维持项目经济体系不破坏。然而仍有许多投资者明知其中利害，却仍抱着“零撸不亏”、“第一批入场稳赚”的想法一头扎入，都认为自己不会是最后一批韭菜，结果基本都是亏损的。

四、名为〝智能合约互助〞 实为〝虚拟货币传销〞!

2021 年 2 月，一个名为“MMMDeFi”的平台，利用区块链智能合约技术，让传销规则的逻辑代码能在链上自动执行。该组织成员通过聊天软件对该项目进行宣传推广，进而发展了 5 万余名会员，层级达 100 多层，涉案金额 10 亿余元。

4 月 23 日，办案民警赴北京、郑州、成都等地开展集中收网，一举捣毁了这一打着区块链旗号的传销犯罪团伙，并抓获犯罪嫌疑人 16 名。



分析：

MMMDeFi 是 MMM 去中心化互助金融的简称。该项目想通过“标题党”来吸引原来参与过“互联网第一大互助盘骗局”MMM 项目的会员，从而快速吸引“投资人”注意。其本身并没有盈利能力，而是利用人们对智能合约的不了解，诱以高额回报，来刺激参与者疯狂充钱和发展下线，一旦没有新鲜血液加入，项目随时面临崩盘。因此，MMMDeFi 的本质还是 MMM 的仿盘，是一场“庞氏骗局”。

为了方便行骗，此类项目通常把自己包装成有世界知名区块链项目、金融机构或者经济学家、技术专家的加入，且在网络大肆宣传，以骗取公众信任。还有不少参与者明知其必定崩盘的事实，仍冒险投资，最后加入这场“击鼓传花”游戏的人，必将成为最大受害者。

五、交易所清退潮下 冒充平台客服电诈案频起

2021 年 5 月，国务院金融委发布《打击比特币挖矿和交易行为》，2021 年 9 月，中国人民银行等多个部门发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》，多记监管重拳落地，虚拟货币交易所也开启了停新清退的模式。

在这样的背景下，市民黄先生接到一个境外电话，对方自称是火币平台客服，发送钓鱼邮件（如下图），要求配合清退，要求黄先生将虚拟货币平台资金转到指定软件以备资金查验。对方不但套取了黄先生的交易账号密码，转走黄先生价值四万元人民币的虚拟货币，还以“账户异常，需要资金进行流水对冲”的理由，骗走黄先生两万元人民币。

分析：

一直以来，我国对虚拟货币采取严监管模式，从打击比特币挖矿到切断虚拟货币炒作资金链条，一系列监管“组合拳”呈现出多维度、多层次、全覆盖态势。

在这类案件中，骗子通常会使用境外电话，冒充虚拟货币交易所客服或安全部门人员，准确说出受害人的真实姓名、交易账号等，甚至具体到交易时间、金额，以此获取受害者信任。再要求受害人转移资金到指定软件、填写个人信息、开启屏幕共享功能等，最后利用受害人信息转走赃款。

如今电诈案件层出不穷，变化极快，涉猎面极广，除了冒充交易所客服，还有冒充公检法、要求配合提供交易流水自证清白等多种套路。但是归根到底，电诈手法都是换汤不换药。

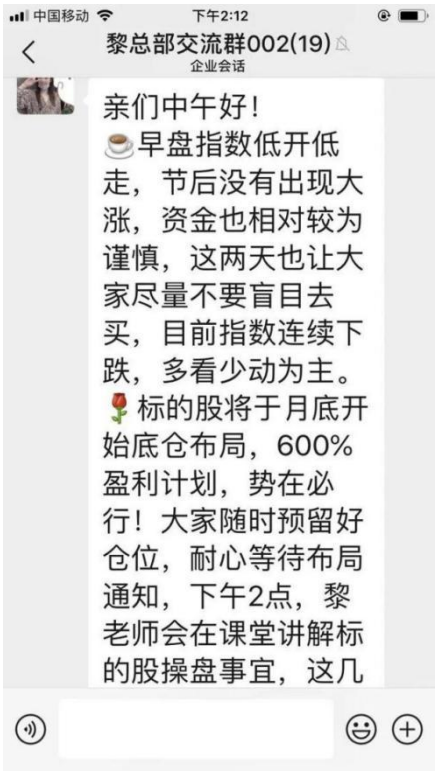
知帆安全团队提醒，务必警惕一切要求提供视频、录屏、共享屏幕、远程操控、引导提现到“安全地址”、“安全账户”等的诈骗手法。

六、利好虚拟货币 专家授课解秘密?

近年来，虚拟货币的热潮引发了投资者们的极大关注。2021 年 8 月，深圳市民张女士经他人介绍，认识到了一名“资深投资专家”黎某，随后加入了黎设立的微信股票交流群。微信群内定期会有直播课程，由黎和几位授课老师及助教授课。通过这些“老师们”的授课和经验分享，张女士不仅学习到了股票知识，还了解到了时下热门的“虚拟货币”。

一次，在老师们所说的“600%收益标的股计划”的吸引下，张女士开始尝试跟进投资。随后，对方以资金征集不足为由，引导张女士在对方的币利 APP 上投资虚拟货币，并约定

一周后收益 35%脱手，转投标的股。于是张女士陆续在币利 APP 平台投入 30 万元本金的虚拟货币。然而到了约定的清仓提现时间 10 月 28 日，她却发现不仅资金无法到账，币利 APP 也无法打开，联系平台客服等相关人员，也相继被拉黑。



分析：

疫情之下，各种直播课、网课盛行，不少不法分子利用人们想要赚钱的焦虑心理，精心包装，团伙作案进行诈骗。相较于个人欺诈，团伙欺诈的波及范围更广、社会危害性更高。

在本案例中，诈骗分子正是团伙作案，利用隐蔽的私域直播，内外勾结，对被害人进行有组织、有计划的诈骗。诈骗分子通过自导自演，将被害人引诱到由对方操纵的虚假虚拟货币平台上投资，投资人看到的余额与收益，不过是对方动动手就能生成的数据。一旦钱财到手，对方就会关闭平台、删好友、拉黑，然后用同样的手法另起炉灶，再骗下一个人。

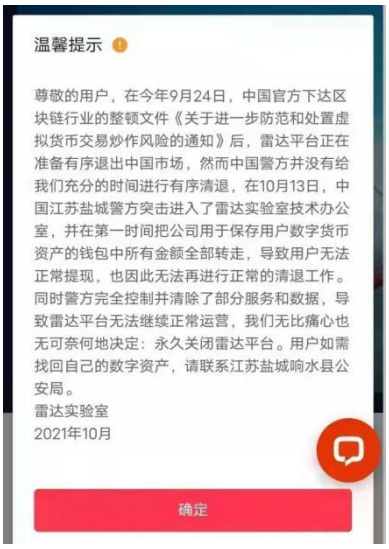
知帆安全团队提醒，投资者在面对不熟悉的领域切莫急功近利，轻信他人承诺的高额收益。

七、“国内第一神盘”雷达币崩盘 警方定性为传销

2021 年 10 月 19 日，历时 7 年、会员众多、涉及资金庞大的“神盘”雷达币落下帷幕，雷达官网宣布永久关闭雷达币，雷达网技术人员已被盐城警方带走调查。

雷达币的前身是 Vpal（V 宝币），宣称其去中心化、开源、长期持有无风险，是一种能解决通货膨胀和金融危机的国际通用型货币。与比特币不同，雷达币的挖矿方式由“持币算

力”和“推广算力”组成——用户只需要持有雷达币，即可每日生息，同时推广的下线持有的雷达币越多，收益也就越高，而且没有层级限制。



分析：

雷达币虽然声称是基于区块链、完全去中心化的，但是它本质上却是彻头彻尾的拉人头、后人为前人买单的庞氏骗局，一旦没有新人加入，它就会崩盘。

为了完成这场击鼓传花的游戏，推广人员甚至采用极端方法刺激投资者：“必涨”“稳赚”，即使倾家荡产也要持有雷达币。由于涉及面甚广，层级多且复杂，雷达币已被警方定性为传销。

2021 年 9 月，人民银行等十部门发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》中明确表示，虚拟货币不具有与法定货币等同的法律地位，虚拟货币相关业务活动属于非法金融活动。

八、数字人民币推广进行时 冒充公检法诈骗异军突起

2021 年 11 月 8 日，黑龙江的王女士接到一个陌生电话，对方自称“黑龙江省公安警务人员”，以受害人涉嫌贩卖身份证、参与诈骗为由，要求受害人下载某 APP，并提供个人信息、银行卡号、手机号及自拍照片等“自证清白”。随后，诈骗分子利用受害人的个人信息和手机号注册数字人民币钱包，通过 APP 的会议模式共享屏幕的功能，获取受害人手机上的注册验证码。在指示受害人办理银行卡、转移存款到新卡的过程中，诈骗分子又获取受害人的账户信息及密码，并将银行卡的存款全部充入受害人名下的数字人民币钱包，然后转至其他数字人民币钱包，最终导致受害人损失共计 7.6 万元。

无独有偶，山西的宋女士接到一自称是太原市公安局工作人员的电话，对方以宋女士涉及洗黑钱为由，要求其提供存款证明清白，并通过同样的手法，最终导致受害人被骗 20 万元。

分析：

2021 年，随着央行大力推行数字人民币，电诈分子的诈骗套路也不断“更新迭代”。不法分子正是利用人们对数字人民币认知的模糊，和对公检法人员的信任，从而一步步骗取受害者钱财。

经查，山西一案中的犯罪团伙诈骗得手后，利用境外聊天软件同上游犯罪人员取得联系，按照对方要求，通过数字人民币的形式帮助转移赃款，最后通过境外虚拟货币 APP 平台再次洗钱获利。正是由于数字人民币具有一定匿名性，其中四类钱包通过手机号即可注册，不法分子利用买卖、租赁、盗窃来的手机卡开通数字人民币钱包，从而达到洗钱目的。

知帆安全团队提醒，“断卡”行动与每个人息息相关，一定要保护好个人的银行卡、电话卡等信息，切勿出售、出租、出借本人银行卡、电话卡，一旦出现个人信息泄漏情况，应及时挂失与报警。

第六章 2021 年十大虚拟货币诈骗话术

对于虚拟货币领域而言，2021 年可被称之为是“跌宕起伏”的一年，从比特币的暴涨暴跌，到动物币的疯狂，再到有关部门发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》、《关于整治虚拟货币“挖矿”活动的通知》，最后到元宇宙的全球火热，这个领域时刻都有新的监管动态与新技术出现。元宇宙、NFT、链游、DeFi 等区块链领域“新概念”频频爆火，为网民展示了一个个互联网“新风口”，不法分子也跟风转换套路，利用新兴概念的噱头行骗。

在本章中，报告从 2021 年高发的典型案例中，选取行骗者常用话术或关键话术，梳理、总结为“2021 年十大虚拟货币诈骗话术”，当网民看到、听到以下类似话语时，要格外注意，谨防被骗子“套路”。

一、稳赚不赔 xx 币，一夜暴富不是梦

不法分子利用人们“一夜暴富”的心理，以“低风险高收益”作为诱饵，声称可以低买高卖虚拟货币“搬砖套利”、租赁矿机挖矿“躺赚”收益、投资 xx 币“稳赚不赔”，其实质都是操作虚假后台，控制价值涨幅，最终圈钱跑路。

二、钱包空投糖果，亲测收到 xxxx

不法分子通过网络钓鱼，发送空投信息实施诈骗。空投骗局一般分为两种，一种是在空投活动时引导受害者填写钱包私钥，目的是盗取受害者钱包中的币。另一种是虚假空投，一般是为了聚集用户，再用聚集的用户变现。

三、云养 xx 就可以获得巨额回报

不法分子打着“云养 xx”的旗号，设置典型的“躺赚”陷阱，其本质就是“互助盘”的庞氏骗局模式，受害者用虚拟货币购买饲料等虚拟资产云养宠物，等待“虚拟宠物”升值，当项目平台突然关闭时，投资者的资金将无法提现。

四、共享经济，DeFi 革命，颠覆未来

DeFi，即去中心化金融，通常是指使用基于区块链上的智能合约创建的 DAPP（去中心化应用）来实现传统的金融功能，比如交易、借贷、抵押、保险等。有不法分子发行空气项目，再为项目披上 DeFi 的外衣，实行诈骗。

五、这是 100%去中心化的项目，生态收益 100%分配

去中心化本是区块链的特征之一，原意为“消除垄断，人人都可以成为中心”。然而一些不法分子假借“去中心化”的概念，喊着“金融革命”“人人都有机会”“分众时代到来”的口号，实施表面去中心化项目，实则是传销。

六、比特币暴富机会没把握住，这次的 NFT 一定不能错过

2021 年 3 月，佳士得以 4.5 亿元拍出 Beeple 的 NFT 艺术作品《每一天：前 5000 天》后，NFT 艺术在国内被火爆地炒作起来。有不法分子打着 NFT 的幌子，引诱投资者入局，以此实施诈骗，或利用 NFT 传销、伪造 NFT 等方式，进行非法犯罪活动。

七、元宇宙，互联网的下一个风口

2021 年被看作“元宇宙元年”，10 月末 Facebook 宣布改名“Meta”并宣布布局元宇宙业务，元宇宙概念被热炒。“元宇宙课程”“元宇宙炒房”“元宇宙链游”层出不穷，不法分子借机打着元宇宙的旗号，实施击鼓传花式的金融骗局。

八、月收益 100%，边玩游戏边赚钱

随着元宇宙成为市场热点，不法分子借机炒作“元宇宙链游”，扬言“玩游戏就能赚钱”，然而许多区块链游戏的本质就是网页游戏，开发成本很低，其实质为披着链游外衣的庞氏骗局。由于涉及虚拟货币结算，其本身或已涉嫌非法集资或金融诈骗。

九、交易平台正在清退大陆账户，请您配合我们操作

2021 年底，各大虚拟货币交易平台全面清退。有不法分子假冒交易所平台客服、公检法等机关工作人员，以“交易所清退大陆账户”或“账户异常操作”等名义，要求受害者配合“查验资金”，实则转移受害者资产，实施诈骗。

十、你涉嫌洗黑钱，需要开通数字人民币账户

2021 年下半年，数字人民币逐渐走进大众视野，然而其支付隐私性强、钱包转账金额大等特点却被不法分子利用。有不法分子假冒“公检法”，通过打电话等方式告知受害者涉嫌洗钱等违法行为，诱导其开通数字人民币账户，最终转移受害者资金。

第七章 十种虚拟货币传销的典型模式

近年来，虚拟货币传销犯罪越来越多，此类犯罪规模大、受害人众多、涉案资金多，对社会和金融秩序稳定带来严重危害。在本章中，知帆科技对虚拟货币传销类犯罪的十种典型模式做梳理总结，以利于读者能识别犯罪和了解虚拟货币传销的发展现状。

一、交易所模式

交易所模式就是犯罪团伙建立山寨交易平台并发行对应的平台币作为手续费，表面上提供 BTC、ETH 等主流虚拟货币交易服务，实际上却以“公链”概念为幌子、高额的持币生息收益为诱饵，吸引投资人开设高额账户。同时还利用高比例的推广收益，诱导投资人发展线下，建立层级，参与传销而不自觉。明为“高收益”，实则瞄准投资人的本金，犯罪团伙非法敛财后，通常会以黑客攻击、发行新代币结算等方式软跑路。

二、钱包模式

除了发行各种空气币、山寨币，犯罪团伙还将目光瞄准了主流公链。通过拷贝公开的公链代码，犯罪团伙能开发自己的公链项目、发行公链代币，还可以打造自己的钱包、去中心化虚拟货币交易平台和 APP。这些所谓的钱包和交易平台，不仅支持各种主流币种如 BTC、USDT 的充值，还可以通过平台内部交易所，将主流币兑换为平台代币。

但是，用户想要注册钱包，必须有推荐人的邀请码，绑定成层级关系，还必须持有一定量的平台代币才能使用。同时，平台鼓励用户质押平台代币来获得平台矿池的算力进行“挖矿”，算力越多，获得奖励平台币越多。项目方称可以通过持币收益和推广收益，让用户避免躺赚、保持全网推广动力，不断分钱包，复利生息。实际上，所有这些都是包装成“去中心化”的中心化项目，平台代币的发行、交易平台上虚拟货币价格的变化等，都是项目方后台控制调节的。

三、虚假“智能合约”模式

随着以太坊、波场链的发展，区块链智能合约的出现，一些犯罪团伙打着“智能合约”的名义，开发所谓的“去中心化金融理财游戏”，能以小搏大，获得高额收益，并且有完整的商业逻辑协议(奖金制度)，宣称项目低门槛、低风险、透明公平、完全去中心化，能根据智能合约自动运行，一旦上链就永远无法改变“游戏规则”、无法停止。但实际上，平台上所有的充值、返利、提币等业务，都由犯罪团伙在后台操作。而投资者投入的主流币其实都被转移到了犯罪团伙的地址上，最后，犯罪团伙携币关网跑路。

四、智能合约模式

DeFi 是“去中心化金融”的英文简称，是一种依赖区块链技术，以去中心化的方式开发和运营的金融产品。而 DeFi 中的关键就是智能合约，在智能合约模式中，犯罪团伙需要一个虚拟货币地址，将用于犯罪的智能合约部署到区块链上，然后包装成理财项目，并在各种社群中以高额收益为由大肆推广传播。

项目方不仅在 ETH、TRX 公链发行智能合约、上线 DAPP，还为项目设置了一系列丰富的“奖励机制”：捐赠奖励、推荐奖励、领导奖励……这些奖励机制又和项目的主玩法形成体系，一并运行在智能合约上。即用户除了可以通过平台方的 DAPP 投入主流币，冻结一定天数后根据本金数量获取静态收益，还可以通过发展线下、获取各个层级的动态收益，以及参与平台的各种游戏活动获取收益。这些项目的确是运行在智能合约上，但是一旦合约内积累了一定数量的资金，项目方可通过之前设置好的合约后门直接把资金转移到其他地址，从而崩盘跑路。

五、矿机租赁模式

矿机租赁模式的项目方一般通过承诺“零风险、高回报、能产出高收益的虚拟货币”，向公众宣传投资虚拟货币矿机。缴纳一定 USDT、BTC、ETH 等主流币作为租金即可成为承租人，再根据承租人投入的资金数额，选择不同档次、组合的矿机，以获得不同层次的算力，平台最后根据算力占比来发放平台虚拟货币作为收益。

而这部分挖矿的收益往往只占一小部分，真正能获得更多收益的是推广下线。不断往下推广，就能获得更多下线投资矿机的收益提成。事实上，矿机往往只是噱头，项目方主要通过用户购买矿机的费用来维持用户收益，不断发展新人入局，来填补前人窟窿，直到崩盘。

六、云矿机模式

不同于传统挖矿需要购买实体矿机，云矿机模式只需要购买平台的虚拟矿机，加入平台的矿池，就可以产生算力、获得收益。这种模式前期投入小，通过推荐码、推荐链接实名注册后，还会获赠初级矿机，因此很容易吸引投资人加入。由于不同等级的矿机算力不同，投资人除了可以用主流币兑换平台币来购买更高算力的矿机，还可以通过发展下线来提升用户等级，也就是通过下线的投资来获得收益提成。最终下线投资的越多，获得的奖励提成就越多。就这样，犯罪团伙打着云挖矿赚钱的旗号，通过各类社交软件，利用资金盘的金钱效应及分裂模式吸引流量，不断诱导投资人入局。而这类项目的结局无疑都是崩盘、收割。

七、量化机器人模式

2021 年币圈迎来大牛市，市面上也出现了很多炒币机器人、量化跟单系统和高频交易量化平台。它们通过宣称用户可随时提币、无限制、不跑路、有交易所背书，还有老师跟单授课、分析 K 线、追踪趋势，来迷惑投资人、取得他们的信赖。除了这些“成熟”的模式，平台们还以高收益引诱用户入局，从而忽略平台需要保证金和“伪量化”的本质。

其实，这些平台和项目方、资本方以及交易所的关系暧昧不清，一方面能为后者们提供交易量，一方面又利用被蒙骗的用户，拉更多人下水：推广拉新可以提高“等级”，获得更高的团队代理奖励和动态收益。在高额佣金的诱惑下，越来越多的用户加入进来。天下没有免费的午餐，当用户参与进来的时候，其实就已经进入了平台设置的陷阱。

八、短视频模式

短视频的兴起也给币圈犯罪团伙带来了新思路。开发者们根据短视频热潮，开发了可以看视频获取收益的项目。项目方发行自己平台代币作为支付通证，利用平台代币链接广告主和流量个体，而用户，则通过点击观看这些短视频广告来获取收益。

不同等级的用户观看短视频广告的收益不同，等级越高，收益比例越高，想要提高会员等级，则需要充值 USDT 或者在其指定的交易所购买平台代币。观看短视频广告的静态收益每日固定，更高、无封顶的动态收益来自于邀请的下线——发展下线越多，收益越多；下线收益越高，提成收益越高。实际上，这就是披着刷短视频赚收益外衣的“拉人头”模式。

九、矩阵 DAPP 模式

矩阵滑落机制是一种常见的传销玩法模式，具体机制是参与人按照上下级关系形成类金字塔模式的层级关系，矩阵的顶端是推荐人，下面的成员都是该推荐人的下线，下线在平台内的充值都会有一定比例分给推荐人。常见矩阵内总共有三名或六名成员，同时矩阵内的最后一名成员的门槛费会作为整个平台内的滑落奖励，分配给矩阵等级较高的上级。

一部分为所谓的动态收益，即源于自己直接推荐用户的奖励，需要投入大量精力拓展下线；另一部分则是所谓的静态收益，只要用户开通的矩阵级别够高并发展了一定数量的下线，可能会出现其下线在进一步发展下线时，矩阵级别低于更低下线的情况，那么就可以享受到这些下线的“滑落”收益。自己拉的人头、上下级溢出的伙伴、超过上级的伙伴都在对应等级的矩阵内，该用户的金字塔层级会纵向拓展；若有高等级的伙伴进入该用户的矩阵，那该用户的金字塔层级会横向拓展。在这样“烧伤机制”的加持下，用户为了维持自己的收益，只能不断复投，去做推广布道，最终深陷其中，成为项目方的取款机，直到最后没有新成员加入，项目崩盘。

十、链游元宇宙模式

“玩游戏就能赚钱”，这样的宣传难免不让人动容。在元宇宙概念的加持下，各种 NFT 链游项目蓬勃发展，犯罪团伙们也紧跟风口，开发自己的链游项目、发行游戏代币并上线去中心化交易所。用户使用主流币兑换游戏代币，然后通过购买游戏装备、升级人物等完成一系列游戏任务，来获取相应的收益。除了获取这部分静态收益，用户还可以享受推广带来的额外动态收益。用户在游戏内的充值购买行为可以提高用户等级，等级越高的用户，可以获得更多层级的下线节点投资收益，得到的游戏内奖金池的分红也就越多。

项目方通过蹭热点、挂靠知名项目等手法对自己的链游大肆宣传，吸引投资人入场，不断拉升游戏代币价值，又靠动静结合的高额收益来吸引更多投机者加入，其本质仍是靠用户兑换平台币消耗的主流币来扩大资金池，项目方趁机套现跑路。

第八章 2021 年国内虚拟货币监管情况及影响

2021 年以来，虚拟货币行情异常火爆，各种虚拟货币投资的造富神话刺激了市场敏感神经，大量投资者跟风进场。随之而来的则是泡沫化加剧，虚拟货币市场盛行炒作毫无价值的空气币，暴涨暴跌成为常态，越来越多投资者被吸引参与高杠杆交易，爆仓频发，风险巨大。

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 2021 年发布的相关内容。

一、518 公告

5 月 18 日晚间，中国互联网金融协会、中国银行业协会、中国支付清算协会联合发布了《关于防范虚拟货币交易炒作风险的联合公告》，强调虚拟货币是一种特定的虚拟商品，不由货币当局发行，不具有法偿性与强制性等货币属性，不是真正的货币，不应且不能作为货币在市场上流通使用，要求金融机构、支付机构等会员单位不得开展与虚拟货币相关的业务，提醒防范虚拟货币交易存在的风险。

同日，内蒙古发改委发布了《关于受理虚拟货币“挖矿”企业、个人问题信访举报的公告》，指出目前内蒙古自治区已设立虚拟货币“挖矿”的企业举报平台，并将全面清理关停虚拟货币“挖矿”项目。

5 月 19 日晚，虚拟货币市场出现恐慌式崩盘，多家虚拟货币交易平台上演“拔网线”操作。

二、521 金融委会议

5 月 21 日，国务院金融稳定发展委员会（以下简称“金融委”）在第五十一次会议中指出，“打击比特币挖矿和交易行为，坚决防范个体风险向社会领域传递”。此次会议重申防范金融风险，强调“坚决防范个体风险向社会领域传递”，维护金融秩序稳定。同时，这也是金融委首次点名比特币挖矿，金融委的重磅发声，再次阐明了金融监管部门对于比特币等虚拟货币的严监管态度。

受此影响，5 月 21 日，虚拟货币全线暴跌，美股区块链股也直线跳水。

三、924 通知

9 月 24 日，中国人民银行、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、公安部、市场监管总局、银保监会、证监会、外汇局联名发布了《关于进一步防范和处置虚拟货币交易炒作风险的通知》(以下简称《通知》)，明确了虚拟货币和相关业务活动的本质属性：虚拟货币不具有与法定货币等同的法律地位；虚拟货币相关业务活动属于非法金融活动；境外虚拟货币交易所通过互联网向我国境内居民提供服务同样属于非法金融活动；参与虚拟货币投资交易活动存在法律风险。

《通知》强调，依法严厉打击虚拟货币相关业务活动中的非法经营、金融诈骗等犯罪活动，利用虚拟货币实施的洗钱、赌博等犯罪活动和以虚拟货币为噱头的非法集资、传销等犯罪活动。

《通知》再次强调，具有非货币当局发行、使用加密技术、分布式账户或类似技术、以数字化形式存在等特点的虚拟货币，如比特币、以太币等，包括泰达币等所谓稳定币，均不具有与法定货币等同的法律地位，不能作为货币在市场上流通。《通知》明确指出，虚拟货币兑换、作为中央对手方买卖虚拟货币、为虚拟货币交易提供撮合服务、代币发行融资以及虚拟货币衍生品交易等虚拟货币相关业务全部属于非法金融活动，一律严格禁止，坚决依法取缔。

《通知》指出，我国将建立健全应对虚拟货币交易炒作风险的工作机制，多部门协同联动，强化属地落实，积极预防、妥善处理虚拟货币交易炒作有关问题。

由此，虚拟货币行业全链条打击已成趋势。受“924 通知”影响，虚拟货币市场迅速下挫，多家交易所、机构、项目纷纷响应和落实通知规定，对外宣布限制和清退大陆用户。

四、《关于整治虚拟货币〝挖矿〞活动的通知》

9 月 24 日，国家发改委等 11 部门发布《关于整治虚拟货币“挖矿”活动的通知》(以下简称《通知》) 称，严禁投资建设“挖矿”新项目，加快存量项目退出。同时，《通知》也将虚拟货币“挖矿”活动列为淘汰类产业，对不按期淘汰的企业，要依据国家有关法律法规责令其停产或予以关闭。

《通知》指出，虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对推动经济社会高质量发展和节能减排带来不利影响。

《通知》要求，要区分虚拟货币“挖矿”增量和存量项目。严禁投资建设增量项目，禁止以任何名义发展虚拟货币“挖矿”项目；加快有序退出存量项目，在保证平稳过渡的前提下，结合各地实际情况科学确定退出时间表和实施路径。

在严禁增量项目方面，《通知》将虚拟货币“挖矿”活动列为淘汰类产业。将“虚拟货币‘挖矿’活动”增补列入《产业结构调整指导目录（2019 年本）》“淘汰类”，根据相关规定禁止投资。

2021 年以来，国内对虚拟货币“挖矿”的监管持续升级。从 3 月份起，内蒙古率先开展清理虚拟货币“挖矿”项目，5 月份，又先后设立虚拟货币“挖矿”企业举报平台、制定八项惩戒措施；到新疆、青海、四川、云南等省份紧跟步伐，开展虚拟货币“挖矿”活动清理整顿；再到“924 通知”出台后，江苏、浙江、福建、江西等省份也抓紧开始行动。截止 2021 年 12 月 15 日，为了全面实现虚拟货币挖矿“清零”目标，全国已有 15 个省份开展针对虚拟货币“挖矿”的专项整治。

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，知帆科技已与全国五百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，提供技术服务达到七百余次，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，是一个服务于公安等监管机构的虚拟货币侦查服务平台，为办案人员日常研判虚拟货币案件提供工具支持，一站式解决虚拟货币案件的各种查证难题。依托全球领先的人工智能技术、全网海量的地址数据库、精准的溯源分析能力、多年的案件支撑实战经验，打造了集态势、查询、追踪、分析、监控等为一体的实战工具，适用于研判涉虚拟货币的各种类型犯罪，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。

扫码关注公众号了解更多信息

知帆科技 CHAINDIGG

知帆学院 ZHIFAN ACADEMY