# 2020 年加密货币犯罪和反洗钱报告

—2021 年 2 月



本报告由云安全联盟大中华区（CSA GCR）区块链安全工作组专家于乐、刘洁、姚凯、吴潇、杨喜龙翻译，工作组组长黄连金审核。希望读者通过这篇文章了解加密货币犯罪和反洗钱的最近全球情况，若有翻译不当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

# 序言

加密货币 Cryptocurrency 是由控制交易方以密码学原理保障交易安全而创造的交易媒介，当前众多种类的加密货币在国际市场上流通交易，其中最知名的比特币市值已达到美元、欧元、人民币、日元之后的世界第五大货币规模，被特斯拉等大批企业认可为支付手段。然而，加密货币存在着巨大的金融与安全风险，比如币值不稳定性，监管不透明性，技术产品安全性等等，加密货币领域的各种犯罪和洗钱活动在规模和频率上均呈严重局面，对加密货币的发展与数字经济的发展造成负面影响。

CSA 大中华区专家们对各国相关的威胁风险、攻击诈骗、入侵事件等持续分析研究，通过本白皮书首次将中文翻译版《2020 年加密货币犯罪和反洗钱报告》呈现给读者们，希望从业人员和用户通过这篇文章了解加密货币犯罪和反洗钱的国际最新情况，以利对加密货币的知识学习和风险管控。

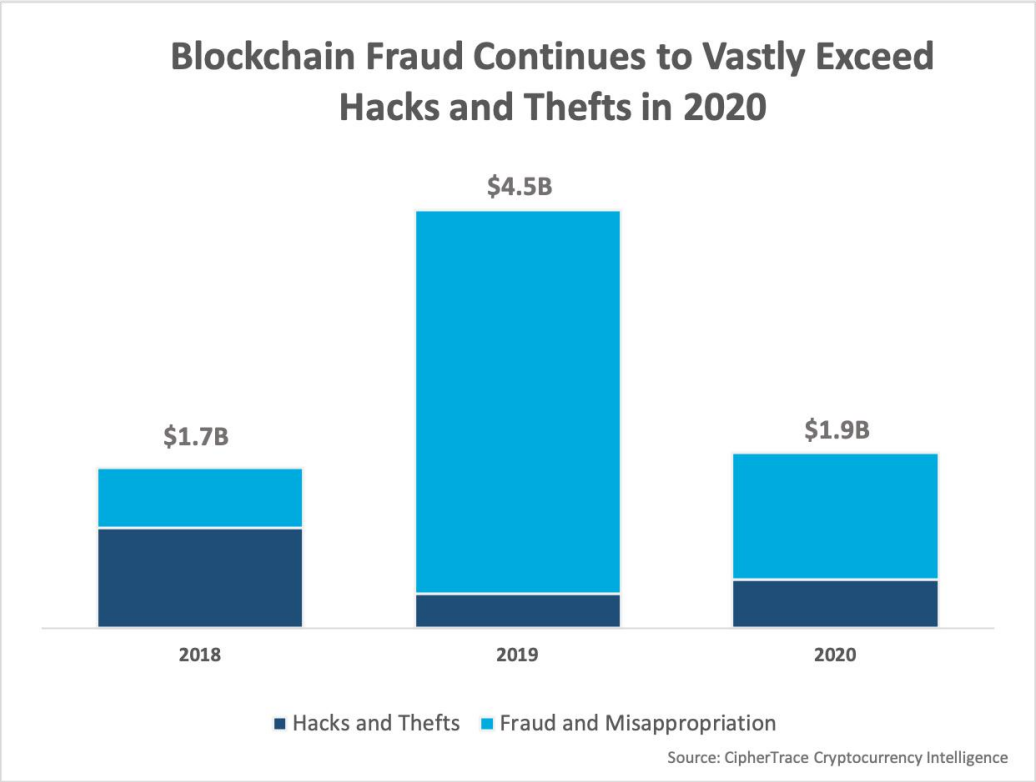
李雨航 Yale Li

CSA 大中华区主席兼研究院院长

# 目录：

# 一、摘　要

美国加密货币情报公司 CipherTrace 的 2020 年加密货币犯罪和反洗钱报告显示，2020 年，重大的加密货币盗窃，黑客攻击和欺诈总额达到 19 亿美元，是有史以来加密货币犯罪犯罪诈取金额的第二高年度。




在过去的两年中，大规模的退出骗局（exit scams）在加密货币犯罪中占大多数。2019 年，庞氏骗局 PlusToken 通过其退出骗局净赚了 29 亿美元，占该年度主要犯罪诈取金额的 64%。到 2020 年，WoToken（与 PlusToken 相同的人员实施的一项类似计划）在退出骗局中诈骗了投资者 11 亿美元，占 2020 年主要犯罪诈取金额的 58%。尽管重大欺诈案件数量大幅减少，但仍占 2020 年犯罪总数的 73%。

尽管在 2019 年和 2020 年发生的盗窃，黑客攻击和欺诈事件数量相似，但案件的平均价值在 2019 年比 2020 年高 160%，这表明随着实体机构继续加固系统并采取预防行动对抗内部和外部威胁，加密货币领域的成熟度有所提升。2020 年确实发生了 2.81 亿美元的加密货币交易所 KuCoin 遭黑客入侵的情况，但该交易所声称已追回了 84%的被盗资金，这在前几年几乎是闻所未闻的。

导致这种差异的另一个因素是，2020 年被数十个 DeFi 相关的黑客和骗局所淹没，这些黑客和骗局的规模要小得多。2020 年所有加密黑客中有一半是采用 DeFi 协议（这种模式在以前的年份中几乎可以忽略不计），而 2020 年下半年，将近 99%的主要欺诈行为源于 DeFi 协议在互联网上执行了“地毯式拉出（rug pulls）”和其他退出欺诈行为，这让人联想到 2017 年 ICO 热潮。在类似于抽空交易的地毯式拉出中，一些投资者将整个 DeFi 池清算退出，从而使剩余的代币持有者没有流动性且无法交易，从而抹去了剩余价值。在监管方面，随着监管和政策制定机构对空间的运作方式进行权衡，加密货币领域已受到新的法律关注。在美国，FinCEN(Financial Crimes Enforcement Network, FinCEN, 金融犯罪执法网络)对银行和虚拟资产服务提供商（Virtual Asset Service Providers：VASP）在进行某些虚拟货币交易时面临的监管义务提出了两项主要规则变更。

10 月发布的拟议规则通知（NPRM - Notice of Proposed Rulemaking：法规制定通知是在美国政府的独立机构希望在法规制定过程中添加，删除或更改法规或规章时由法律发布的公告。该通知是美国行政法的重要组成部分）试图修订法规，要求以更低的门槛保存记录和‘旅行规则’（Travel Rule），收集、保留和传输有关国际支付的转移信息。目前，金融机构会传输任何超过 3000 美元的转帐记录。新规则将在相同的要求下，适用于较小的转账（超过 250 美元的转账），如果资金转移在美国境外开始或结束。该规则特别将加密货币转移作为提案适用的一类交易。

如果交易的对手方使用无托管服务（非托管）或“其他方式覆盖”的钱包，则在 12 月发布的另一项 NPRM 中将要求银行和 VASP 验证其客户的身份，保存超过 3,000 美元的虚拟货币交易记录，并提交超过 10,000 美元的虚拟货币交易的类似 CTR（Currency Transaction Report：货币交易报告）的报告，NPRM 将“其他方式覆盖”的钱包定义为不受 BSA 约束且位于 FinCEN 认定为主要洗钱问题的外国司法管辖区的金融机构中持有的钱包，例如缅甸，伊朗和朝鲜。

拜登政府于 2021 年 1 月上任后，宣布冻结所有政府机构的新规则制定，尚待总统任命或指定的政府部门或机构负责人进行审查。虽然特朗普政府已经将关于无托管钱包 NPRM 的 1 万美元门槛的规则公开讨论期限延长了 15 天，而其余规则又延长了 45 天，但 FinCEN 之后将这两个截止日期都延长和合并到 60 天。尚无迹象表明‘旅行规则’ NPRM 将获得类似的重新审理或者延长。

这些规则或类似的规则很可能在 2021 年上半年生效，从而产生了重要的新的加密货币合规性要求，并大大增加了银行和 VASP 提交加密货币 CTR 报告和 SAR 报告 (Suspicious Activity Report，SAR 可疑活动报告）的紧迫感。

在全球范围内，FATF（Financial Action Task Force, FATF 反洗钱金融行动特别工作组 )于 6 月份发布了针对虚拟资产和虚拟资产服务提供商的修订版 FATF 标准的 12 个月审查。在其中，FATF 决定不修改先前有关虚拟资产或 VASP 的建议，但已记录了未来继续指导的必要性。计划在 2021 年 6 月进行下一次为期 12 个月的审核，以重新评估‘旅行规则’解决方案的进度和进一步的指南。

# 二、几个重点

主要发现的重点如下：

1．随着合法加密货币使用量的上升，加密犯罪的百分比下降。2020 年加密货币犯罪比 2019 年下降了 57%，从 45 亿美元下降到 2020 年的 19 亿美元。

2．去中心化金融（DeFi）是欺诈和洗钱的下一个主要威胁媒介：2020 年所有盗窃中的一半（总计 1.29 亿美元）是与 DeFi 相关的黑客攻击，并且一些集中式交易所（例如 Shapeshift）正在转变为去中心化交易所（DEX）以避免 KYC（know-your-customer）要求。

3．交易所主管面临逮捕，引渡和巨额罚款，因为个人要对洗钱负责。

4．欺诈是主要的加密货币犯罪，其次是盗窃和勒索软件。

5．2020 年，美国交易所直接向犯罪分子发送了价值 4,120 万美元的 BTC。

6．交易所之间交换的比特币中有 84%是跨境转移的。

7．三分之一的跨境比特币交易量被发送到与 KYC 表现不佳的交易所进行交易。

8．从美国 VASP 发送的跨境 BTC 总量的 41%流向了 KYC 明显较弱的 VASP。美国 VASP 收到的跨境交易量的 50%来自与明显弱势的 KYC 的交易所。

9．来自韩国 VASP 的 BTC 交易量的 78%来自与明显弱势的 KYC 的交易所。

10．FinCEN 建议更改‘旅行规则'门槛将是美国 VASP 需要发送的‘旅行规则'消息数量的两倍以上。

11．到 2020 年，将 BTC 付款量的 52%发送到交易所; 40%寄给了私人钱包。

12．美国在接收比特币方面处于世界领先地位，其中有 19.3%全球交易所中接收到的 BTC 发送到美国境内的 VASP。所有 BTC 付款的 10%已发送到美国注册的 VASP。

13．发送到高风险交易所的全球 BTC 交易量的历史最低水平，比 2019 年下降了 59%。

# 三、主要趋势与发展

匿名的和流动的现金一直以来都是犯罪分子的工具。2020 年，尽管非法交易仅占比特币年交易量的 0.5%，具有类似特征的加密货币可能同样难以彻底摆脱其不良声誉。虚拟资产服务提供商（VASP）是预防金融犯罪和确定不良行为者的前线。但是，VASP 的反洗钱控制不足会最终难于阻止全球犯罪资金的流动。随着 VASP 的不断成熟和采取更强大的安全措施，CipherTrace 发现，犯罪分子开始将目光投向比集中式对等服务防护更弱的分散式金融服务。

## （一）2020 年从 BTC 犯罪地址发送的 35 亿美元

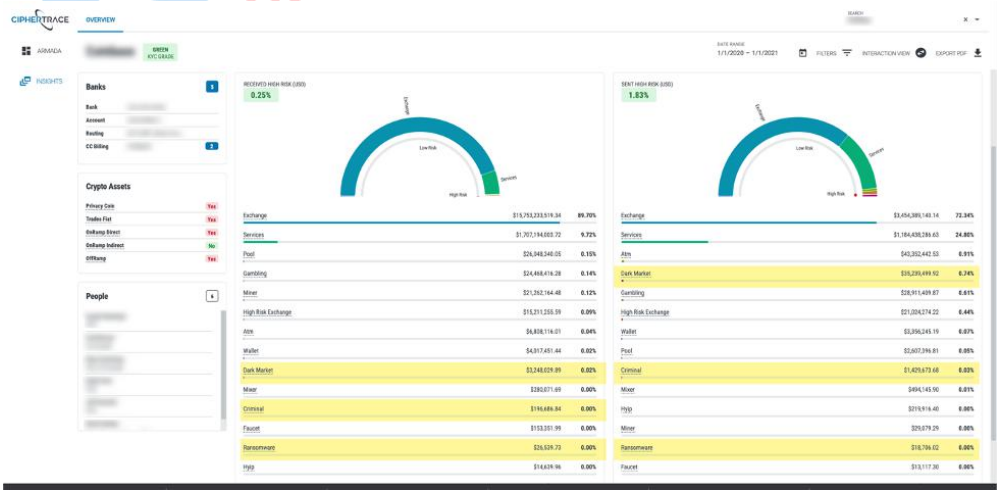
与犯罪相关的比特币地址在 2020 年发送了价值超过 35 亿美元的比特币。该数字包括受黑市，勒索软件参与者，黑客和欺诈者控制的 BTC 地址。这些比特币的大部分最终需要由这些犯罪分子洗钱，这意味着它将进入交易所，在交易所可以将其转换成法定货币并转移到银行。

## （二）一家美国交易所在 2020 年直接向罪犯发送了超过 3670 万美元

通过使用包括 CipherTrace Armada 在内的加密货币情报工具，分析人员能够确定，尽管 KYC 表现出色，但一家著名的美国交易所在 2020 年仍直接从犯罪来源获得了价值超过 350 万美元的比特币。但是，这个数字只是实际流入交易所的犯罪资金来源的一小部分。精明的犯罪分子通常会在其非法资金来源与他们选择的法定出口之间建立距离。值得注意的是，尽管交易所直接从与犯罪相关的地址接收了价值 350 万美元的 BTC，但交易所在收到资金之前无法拒绝任何资金。即使交易所退还了这些资金，互动仍将记录在区块链上。

然而，该交易所还直接发送了价值 3670 万美元的比特币与犯罪相关的地址。适当的 AML 软件可以并且应该停止这些事务。这些直接发送给犯罪来源的交易突出了准确的区块链分析数据的重要性。在与受监管的交易所进行交易时，许多罪犯通常不会直接从其与犯罪链接的地址发送邮件，这使 3670 万美元成为通过交易所流向罪犯口袋的资金的保守估计。绝大多数不良行为者至少会转移他们的资金一次。实际上，CipherTrace 分析师发现，典型的加密货币交易所的黑市敞口通常会在两跳后翻倍（交易一旦从交易所中删除）。在这家美国加密货币交易所，黑市敞口的两跳交易在三倍以上。

## （三）美国交易所直接向犯罪分子发送了 4,120 万美元

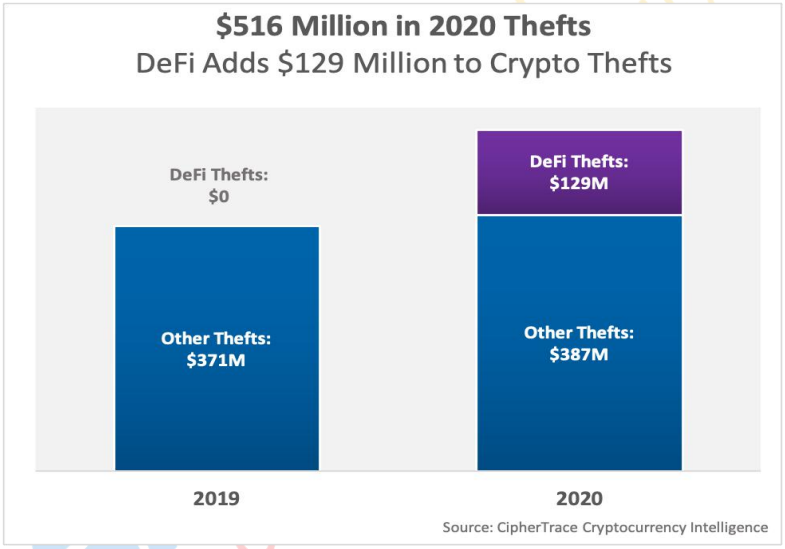



资料来源：CipherTrace Armada

整个美国交易所直接从犯罪地址获得了价值 840 万美元的比特币，并直接向犯罪相关地址发送了价值 4,120 万美元的比特币。

## （四）2020 年一半以上的加密黑客来自 DeFi 协议

锁定在 DeFi 中的美元价值在 2020 年呈指数增长，由于在 DeFi 协议被黑客窃取的 2020 年构成了大部分加密货币盗窃，因此产生了潜在的新洗钱风险。根据 CoinGecko 的数据，到 2020 年 12 月，DeFi 已锁定 198 亿美元—以太坊总市值的 23%。这个数字比 2020 年初在 DeFi 所持有的 17 亿美元增长了 1000%以上。这种指数式的繁荣超过了从 2019 年初（当时 DeFi 市值仅为 10 亿美元）到 2020 年初的 70%增长。就像之前的山寨币热潮一样，资本的爆炸性增长和缺乏监管的明确性吸引了犯罪分子加入 DeFi，最终导致了迄今为止一年以来最多的 DeFi 黑客入侵。




总计，在 2020 年所有盗窃案中，有超过 50%是 DeFi 黑客，相当于约 1.29 亿美元，略超全年被盗数量的 25%以上。相反，在 2019 年，DeFi 黑客数量几乎可以忽略不计。各个 DeFi 盗窃案范围广泛，从几十万到数千万美元的加密代币。CipherTrace 估计，2020 年平均 DeFi 黑客攻击价值约为 600 万美元。

即使是 2020 年最大的盗窃案，集中式交易所 KuCoin 的 2.81 亿美元被黑客入侵，最终也涉及 DeFi，因为犯罪分子试图通过世界上最大的去中心化交易所之一 Uniswap 洗钱。显然，DeFi 已成为加密行业增长最快的趋势之一。因此，必须警惕其洗钱风险。分散式交易所通常不收集有关其用户的 KYC 信息，也无法像集中式交易所那样冻结资金。有时，这种能力取决于各个 DeFi 项目本身。

2020 年著名的 DeFi 黑客入侵包括：

- bZx
- Akropolis
- Axion Network
- Balancer
- Bancor DEX
- Bisq
- Cheese Bank
- COVER
- Finance
- Harvest Finance
- Lendf.Me
- Opyn
- OUSD
- Pickle Finance
- Uniswap
- Value DeFi
- WarpFinance
- wLEO

## （五）DeFi 地毯式拉出（Rug Pulls）成为顶部退出骗局

自 2020 年第一季度以来，尽管 DeFi 黑客数量一直在上升，但随着地毯式拉出和退出骗局的激增，今年年底对 DeFi 带来了新的挑战，这使许多加密货币老手想起了在加密货币时代流行的“ pump and dump”（拉盘，砸盘）计划，也是 ICO 繁荣的高度。在 2020 年下半年，将近 99％的重大欺诈和盗用行为源于 DeFi 协议执行的地毯式拉出和退出骗局。

地毯式拉出类似于退出骗局。两者都涉及内部人将用户的大部分（如果不是全部）资金拿走。尽管退出骗局经常互换使用，但它们往往与已建立的实体或项目意外关闭（“退出”）相关联，从而占用了用户资金。例如，在 2020 年 11 月，DeFi 项目 SharkTron 似乎利用 1000 万美元的用户资金进行了一次退出骗局，关闭了其网站，使用户陷入困境。

另一方面，地毯式拉出是一种特定类型的退出骗局，涉及通过出售大部分 DeFi 池，从投资者（用户）下方“拉出地毯”，从而消耗特定代币的流动性。地毯式拉出通常是通过将后门写入智能合约来完成的。就 DeFi 项目 Compounder.Finance 而言，写入智能合约的一个隐藏后门使开发人员可以在 2020 年 11 月从该项目的流动资金池中提取 1,080 万美元。DeFi 项目 Unicats 在 10 月进行了类似的地毯式撤资，耗尽了全部用户资金。

在我们的研究中，CipherTrace 在 2020 年发现了几起 DeFi 地毯式拉出和退出骗局事件。不幸的是，由于缺乏确定的数据，我们无法验证每起事件。未经验证的事件不包括在我们的整体数据库中以进行分析。

2020 年 DeFi 地毯式拉出和退出骗局的著名例子包括：

- Lv.Finance
- Emerald Mine
- Yfdexf.Finance
- SharkTron
- Unicats
- Compounder.Finance
- Amplifi.money (未经验证)
- Burn Vault Finance (未经验证)
- Minions Farm (未经验证)
- Unirocket (未经验证)

如果没有对智能合约进行适当的审计，对投资者进行持续的教育以及对这些新的风险监管的相关规定，这种趋势很可能会持续到 2021 年。

## （六）DeFi 黑客，诈骗和监管的未来

DeFi 协议在设计上是无需许可的，这意味着它们通常缺乏监管监督，并且任何国家的任何人都几乎不需要 KYC 即可访问它们。结果，我们已经看到 DeFi 在 2020 年的最后几个月成为洗钱者的天堂。

*“ [DeFi 项目]应该已经适用于各种法律，包括证券法，潜在的银行业和贷款法 – 当然包括 AML / CTF（反洗钱及反恐怖主义融资）法。”*

*美国证券会 SEC 的 Valerie Szczepanik*

监管机构似乎开始更加关注 DeFi 及其相关合规性要求。许多 DeFi 项目所依赖的未经审核的智能合约通常具有漏洞，不良行为者可以利用这些漏洞。正如 Polychain Capital 的创始人兼首席执行官 Olaf Carlson-Wee 在 9 月 8 日发布的 Unchained 节目中所说：“我的确认为，这让我有点担心，这么多钱被注入到未经审计的合同中。我认为，总体上讲，进行安全审核是使这些系统中的任何一个成熟

的重要部分。”随着 DeFi 的持续增长，可以预期 DeFi 项目可能会落入全球监管机构的范围之内。FATF 已经将去中心化交易所（DEX）视为 VASP，FinCEN 对 DEX 采取了与对比特币 ATM 相同的监管要求。

美国证券交易委员会的工作人员已经注意到 DeFi 项目受到漏洞，黑客，攻击，欺诈和操纵的影响。在 9 月 18 日并行峰会上，美国证券交易委员会（SEC）的 Crypto Czar Valerie Szczepanik 说：“当您在代码上运行[Defi]逻辑并将其直接发布时，您可能会错过测试代码的关键一步。这样非常危险。您应该审核代码，需要对代码进行一些同行审查。如果没有这些保护措施，立即将其实时发送出去是有风险的。”

Val 警告说：“不要陷入围绕 ICO 市场的炒作。”“炒作会导致欺诈；它可能导致错误的代码实现和不足的测试。如果该行业花时间将其做好，并与监管机构合作以帮助他们做到这一点，那么所有好的东西都将浮现出来，您将获得分布式账本技术所带来的好处。”

Val 说：“我们看到的结构旨在使用户能够放款，赚取利息，借钱，兑换，持仓；这些都是金融活动，它们应该已经受制于各种法律，包括证券法，潜在的银行业和贷款法 – 当然包括 AML / CTF 法。”

同时，欧盟引入了加密资产市场（MiCA），这项拟议法规如果获得通过，如果去中心化交易（DEX）所未作为法人实体注册并在欧盟一个会员国有注册的办公室，将禁止这个去中心化交易所与欧盟公民进行交易。

## （七）FinCEN 拟议的规则为针对托管钱包的交易创建了新的报告和记录保留要求

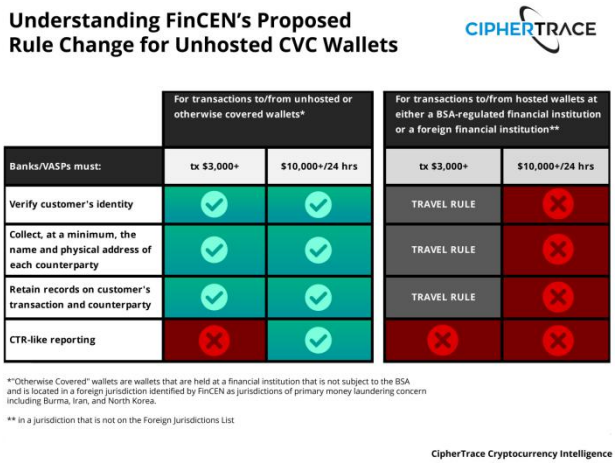
2020 年 12 月 18 日，美国财政部发布了拟议规则（NPRM）通知，该通知将要求受 BSA 约束的金融机构验证其客户身份，保留超过 3,000 美元的可转换虚拟货币（CVC）交易记录，如果交易的交易对手使用了无托管（非托管）或“以其他方式覆盖”的钱包，则提交超过 10,000 美元的 CVC 交易的类似 CTR 的报告。NPRM 将“其他方式覆盖”的钱包定义为在不受 BSA 约束且位于 FinCEN 认定为主要洗钱关注点的外国司法管辖区的金融机构中持有的那些钱包，此列表包括伊朗，缅甸和朝鲜。

这些规则是特朗普政府提出的。2021 年 1 月，即将上任的拜登政府宣布冻结机构规则制定，其中包括这些拟议的变更。但是，冻结只是暂时的，有待拜登总统任命或指定的部门或机构负责人审查。特朗普政府已经将无托管钱包 NPRM 的 1 万美元门槛规则公开讨论延长了 15 天，其余规则的时间延长了 45 天，但 FinCEN 之后将这两个截止日期都延长和合并到 60 天。尚无迹象表明‘旅行规则 ' NPRM 将获得类似的重新开放讨论和时间延长。

许多 BSA 官员认为，对无托管钱包的监管是不可避免的，并且拟议的规则是对当前和未来由无托管钱包流入和流出的可能不受监管的资金流动所造成的洗钱风险的合理反应。拟议的规则实施起来将很昂贵，并且预计这些费用将转嫁给用户。

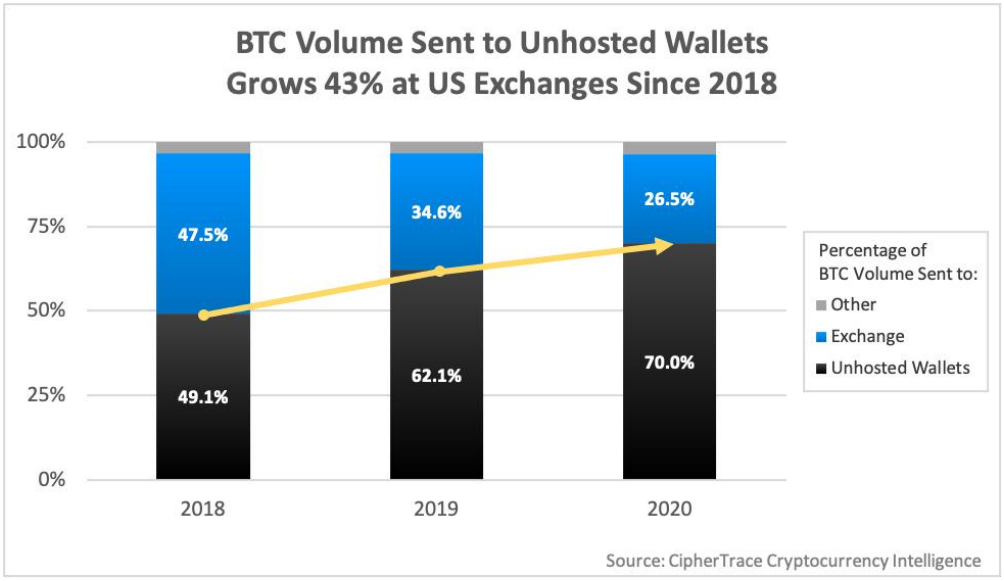
如果被采纳，新规则将进一步强制要求 VASP 以及从事加密交易的银行能够识别交易对手是否是另一个 VASP，如果是，则确定该 VASP 的住所。当前的法规已经根据‘旅行规则’对 VASP 施加了这种负担，现在针对未托管的钱包和其他覆盖的司法管辖区的某些交易设置了附加规则，从而弥补了‘旅行规则’法规未涵盖的 AML 漏洞。CipherTrace 区块链分析工具可以帮助您的机构确定交易对手地址是否属于托管，非托管或“其他方式覆盖”的钱包，这是新提议规则的关键。

新规则还要求 VASP 在 24 小时内汇总加密货币交易，以报告超过 1 万美元的交易并识别任何结构化迹象。汇总时，无需将加密交易和现金交易合并在一起。CipherTrace 具有独特的功能，可以帮助 VASP 和银行汇总多链汇总付款并利用预测分析来识别结构。



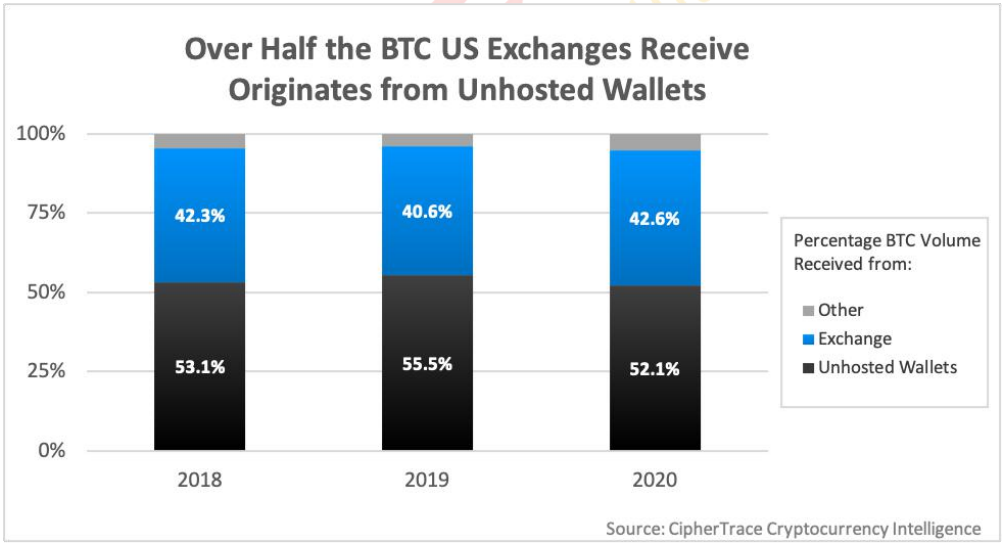

## 1. 无托管钱包主导往返美国交易所的 BTC 交易量

2020 年，美国交易所的流出比特币量的 70％被发送到了无托管的钱包；BTC 接收量的 52.1％来自非托管钱包。




资料来源：CipherTrace 加密货币情报

相比之下，美国交易所发送的比特币交易量中只有约 26.5%流向了其他交易所，而传入的交易量中约有 42.6%来自其他交易所。




资料来源：CipherTrace 加密货币情报

## 2. 拟议规则的潜在含义

区块链分析解决方案帮助加密交易所识别涉及无托管钱包的风险交易。VASP 可以通过无托管钱包的地址追踪资金，从而获得与高风险地址和交易对手相关的洞察。这种透明性使人们能够洞悉与无托管型加密资产钱包相关的风险，而在交易法定货币或现金时无法获悉这些风险。

这些拟议的要求基本上只是金融机构长期遵守的现金（现金和电子资金转账）规则的应用，这些规则已应用于某些虚拟资产交易。但是，从调查的角度看，拟议的规则可能会将犯罪活动延伸到区块链的更多隐蔽角落，将严重阻碍调查的成功。犯罪分子可能会使用未注册的 P2P 交换而不是交易所，以免引起关注。当加密货币达到受监管的交易所时，大多数调查都会获得成功。将犯罪活动排除在交易之外，调查人员将失去他们用于跟踪、追踪和识别犯罪分子及其活动的最强大工具之一。

## （八）美国“旅行规则”所制定的较低阈值可能会使触发 VASP 合规性的数量加倍

2020 年 10 月 23 日，金融犯罪执法网络（Financial Crimes Enforcement Network, FinCEN）和联邦储备委员会提出了一项规则变更，要求包括银行和加密货币交易所在内的金融机构以较低阈值收集、存储和转移有关国际支付的信息。

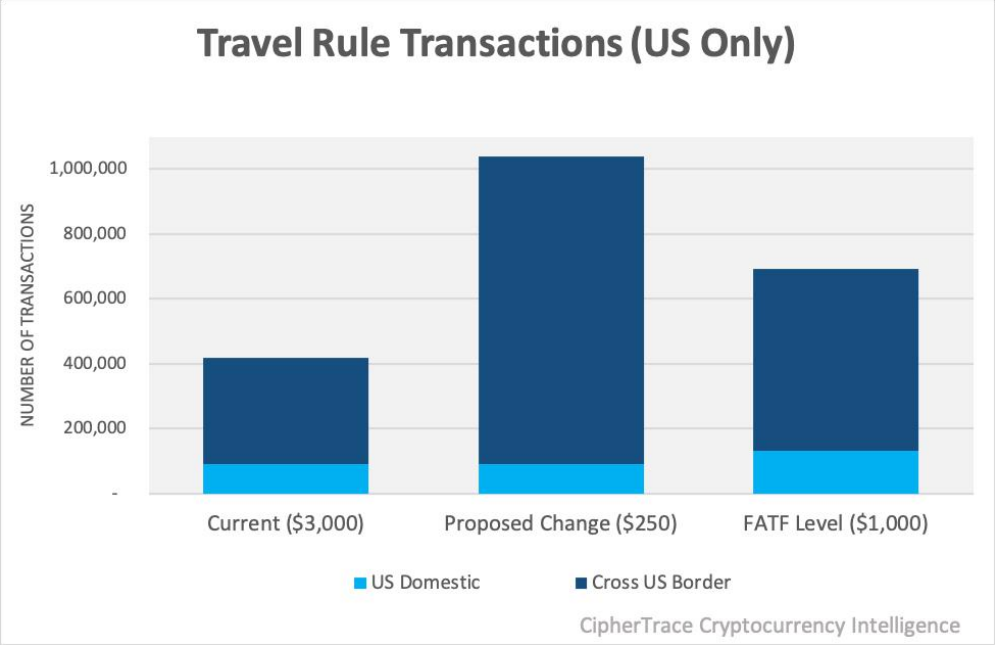
目前，财务机构必须存储和转发超过 3000 美元的国外资金转移记录。根据新规定，在相同要求下，转账金额降低到超过 250 美元。值得注意的是，该规则特别将加密货币转移列为提案适用的一类交易。

根据 CipherTrace 的分析，降低收集、保留和传递有关“开始或结束于美国境外”的资金转移信息的阈值后，每年触发旅行规则阈值的交易数量至少增加 2.5 倍。

| | Monthly US Transactions | | | Number of "Travel Rule" Messages Required by US VASPs | | Transactions at FATF Threshold ($1,000) | |
|---|---|---|---|---|---|---|---|
| Region | txs over $250 | txs over $1,000 | txs over $3,000 | Current | Proposed Change | US | Other |
| US Domestic | 15,921 | 11,016 | 7,510 | 7,510 | 7,510 | 11,016 | |
| US Cross-Border | 79,011 | 46,780 | 27,295 | 27,295 | **79,011** | 46,780 | |
| International (Non-US) | 392,952 | 260,439 | 178,664 | | | | 260,439 |
| Global | 487,884 | 318,235 | 213,469 | | | | |
| Monthly Travel Rule Messages | | | | **34,805** | **86,521** | 57,796 | 260,439 |
| Annual Travel Rule Messages | | | | 417,660 | 1,038,252 | 693,552 | 3,125,268 |

Source: CipherTrace Cryptocurrency Intelligence

资料来源：CipherTrace 加密货币情报




资料来源：CipherTrace 加密货币情报

根据 CipherTrace 的数据，为了符合当前“美国旅行规则”的 3,000 美元阈值，美国 VASP 在 2020 年 10 月期间必须发送超过 34,000 条消息。这些消息中有 27,000 多条（约占 78%）本质上是跨境的，意味着发送或接收 VASP 的地址位于美国境外。按照目前的阈值，每年将有超过 417,000 条消息。

将阈值降低到 250 美元，每年共享和存储的'旅行规则' 所要求的消息数量将超过一百万条。在这个较低的阈值下，跨境交易占所有美国 VASP 旅行规则触发数量的 83%。

如果美国仅将其阈值降低至 FATF 最低标准的 1000 美元，那么每年触发合规性的交易数量将增加 1.7 倍。中介银行或金融机构也要求将该信息传输到支付链中的其他银行或非银行金融机构。拟议的规则变更承认，加密货币的转让无需第三方银行的介入，但实际上许多用户的交易依赖托管钱包和交易所。

## 1. 在虚拟资产世界中难以确定“跨境支付”

FinCEN 建议的规则更改基于“在美国境外开始或结束”的交易。这些交易是由金融机构是否“知道或有理由知道，转让人、转让人的金融机构、收款人或收款人的金融机构是否位于美国或美国境内的司法管辖区以外的其他司法管辖区、或根据美国或美国境内的司法管辖区以外的其他司法管辖区的法律组建。”

由于虚拟资产和 VASP 的跨境性质和全球范围，因此很难强制执行此定义。鉴于许多 VASP 在全球多个司法管辖区注册，更是如此。金融机构只有在接收传输命令或从传输者那里收集信息时根据

共享的这些信息“有理由知道”一项交易在美国境外开始或结束，前提是机构甚至知道交易的跨国性质。

*“根据建议 16（INR. 16）的解释性说明，各国应根据虚拟资产活动和 VASP 运营的跨境性质，将所有虚拟资产转账视为跨境电汇而不是国内电汇。”*

*-FATF 金融行动工作组*

出于这个原因，FATF 在其 2019 年 6 月的虚拟资产指南中决定“根据建议 16 的解释性说明（INR.16），基于虚拟资产活动和 VASP 操作的跨国性质，各国应将所有虚拟资产转账视为跨境电汇而不是国内电汇。”

## （九）超过三分之一的跨境比特币交易量以明显薄弱的 KYC 形式发送给交易所

2020 年，跨境比特币交易占全球 VASP 流出量的 84%。跨境比特币交易量的三分之一（36%）流向了 KYC 程序薄弱或漏洞百出的 VASP。

### 1. 美国聚焦

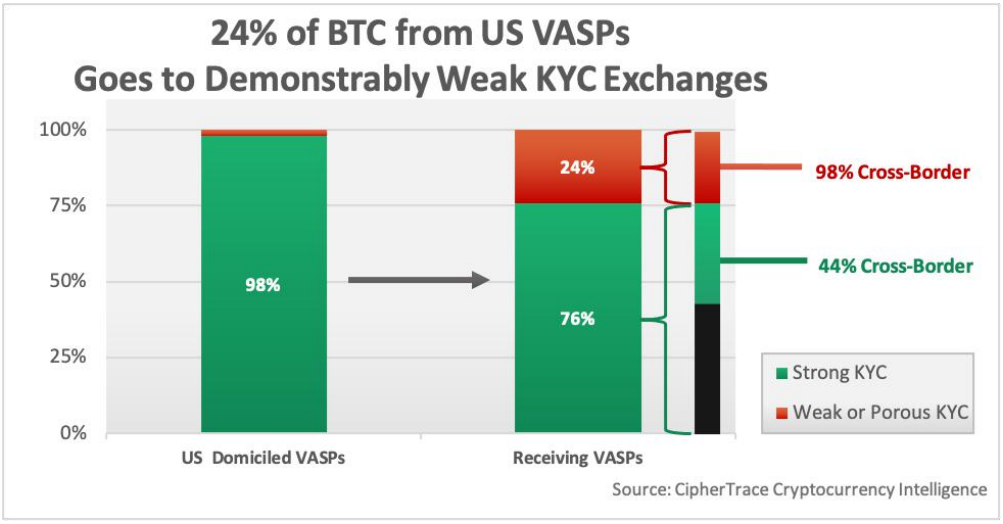
按管辖区更深入地研究 VASP 的流入和流出，发现 98%的美国 VASP 流出的比特币交易量来自具有强大 KYC 程序的交易所。在分析 2020 年美国 VASP 的对外交易量时，CipherTrace 研究人员发现，发送给虚拟资产服务提供商的比特币交易量中有 24%流向了 KYC 薄弱或漏洞百出的 VASP。在 24%的交易所间交易量中，有 98%是跨境交易。相比之下，与实力雄厚的 KYC 进行交易的交易所间交易量中，只有 44%是跨境交易。

*“…… CipherTrace 发现交易所间跨境交易量中有 41%发送到 KYC 薄弱或漏洞百出的 VASP。”*

总体而言，当查看美国 VASPS 的流出量时，CipherTrace 发现**交易所间比特币交易量的 58%是跨境的，其中 41%的跨境交易量发送到 KYC 薄弱的 VASP**。

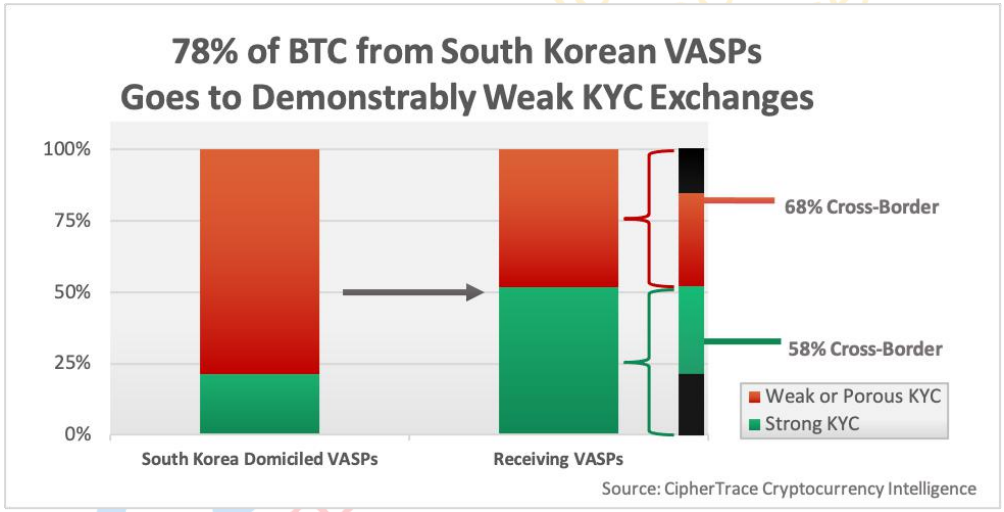
相反，当查看美国 VASP 的流入量时，**入境的交易所间比特币交易量的 74%是跨境的**。在这一跨境交易量中，**有 50%来自于 KYC 行为薄弱或漏洞百出的加密货币交易所**。

进入或来自脆弱或漏洞百出的 VASP 的跨境交易所占的高比例使“旅行规则”法规的目的严重复杂化。这些缺乏 KYC 的 VASP 可能不会收集或保留执法部门所要求的可行情报所需的信息。



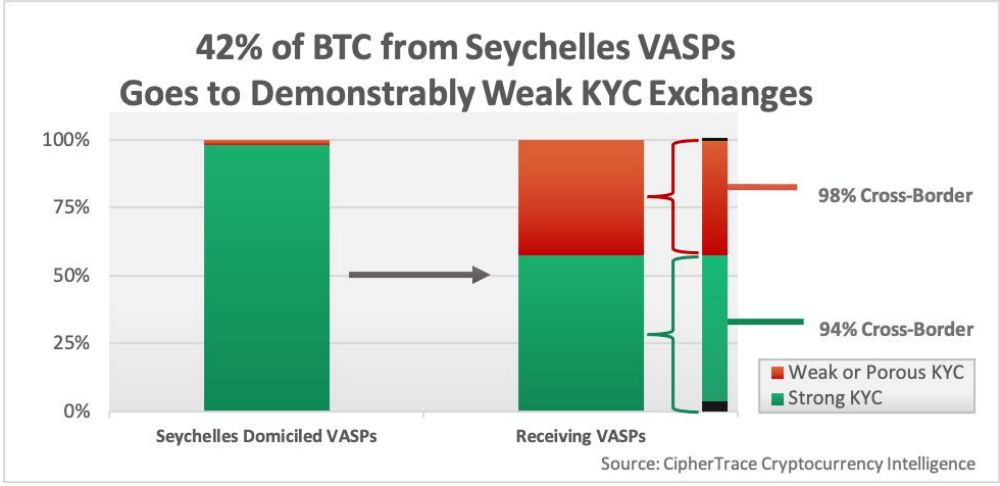

资料来源：CipherTrace 加密货币情报

## 2. 全球跨境比特币交易量



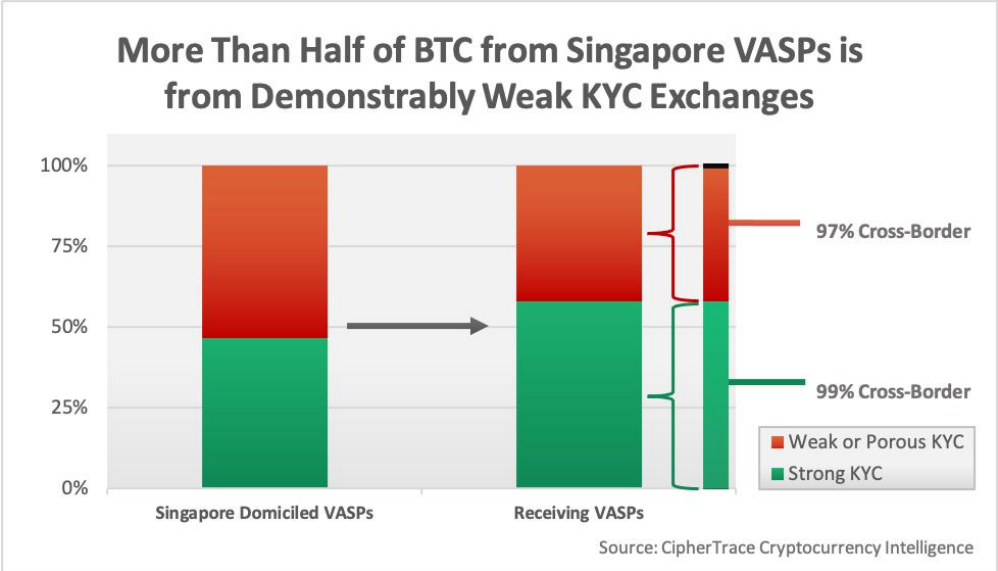

资料来源：CipherTrace 加密货币情报

*查看在韩国注册的 VASPS 的流出量时，CipherTrace 发现 63％的交易所间的比特币交易量是跨境的，其中 53％的跨境交易量发送到 KYC 明显脆弱的 VASP。*



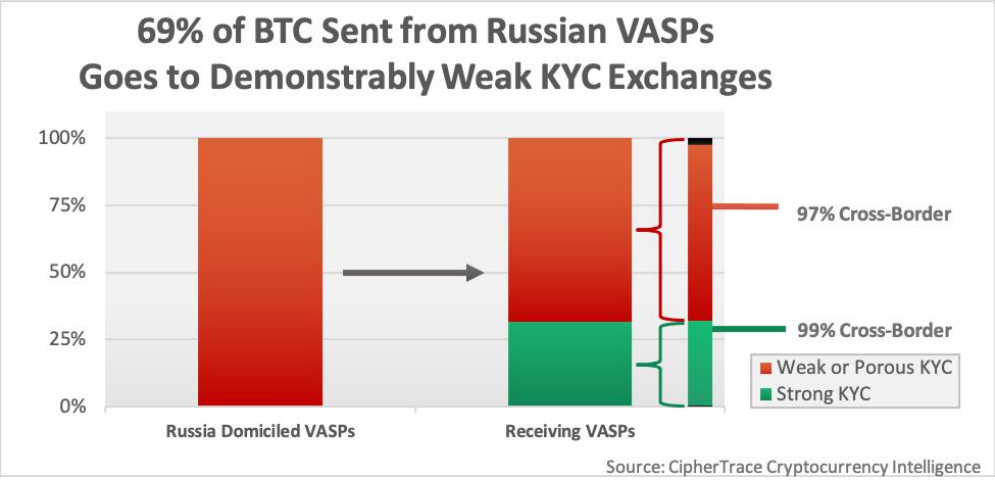

资料来源：CipherTrace 加密货币情报

*查看在塞舌尔注册的 VASPS 的流出量时，CipherTrace 发现 96％的交易所间比特币交易量是跨境的，其中 51％的跨境交易量发送到 KYC 明显脆弱的 VASP。*




资料来源：CipherTrace 加密货币情报

*查看新加坡注册的 VASPS 的流出量时，CipherTrace 发现，98％的交易所间比特币交易量是跨境的，其中 49％的跨境交易量发送到 KYC 明显脆弱的 VASP。*




*查看韩国 VASPS 的流出量时，CipherTrace 发现，98％的交易所间比特币交易量是跨境的，其中 49％的跨境交易量发送给 KYC 明显脆弱的 VASP。*

有效的 KYC 协议是 AML 计划的重要组成部分。了解交易对手机构的 KYC 流程可以帮助金融机构更好地理解和管理风险并防止洗钱。但是，在纸上拥有强有力的 KYC 准则是一回事，而要实施这些准则却是另一回事。通过分析和探究 80 多个国家/地区的 800 多个 VASP 的 KYC 流程，CipherTrace 能够在地理位置上定位洗钱者、罪犯和极端分子可以利用的薄弱且漏洞百出的 KYC。

要了解关于按地区 KYC 平均得分的更多信息，请查看我们的 *2020 年地理风险报告：按管辖区划分的 VASP KYC*：https：//ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/

## （十）交易所在 2020 年收到超过一半的比特币付款

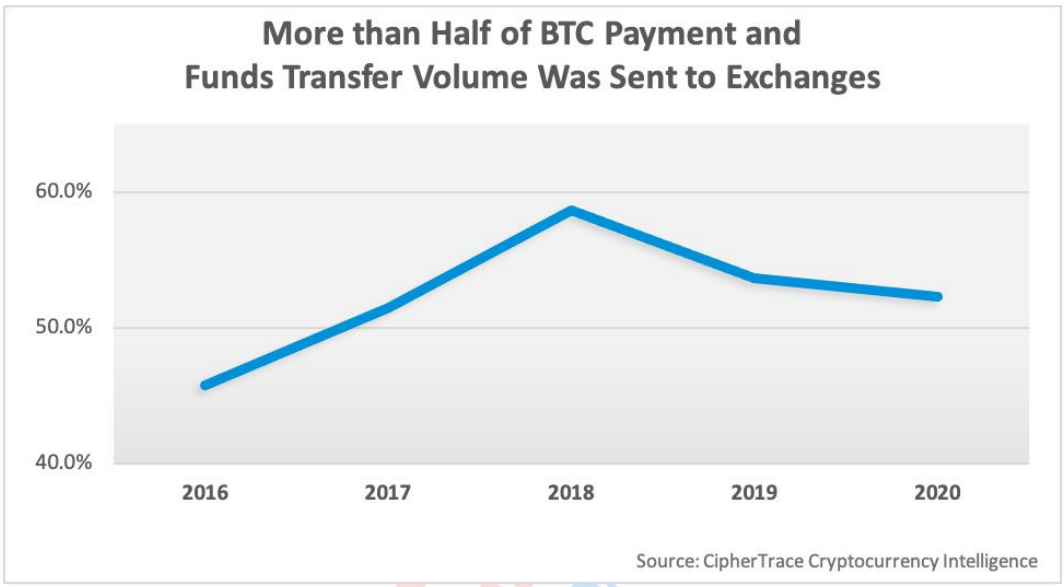
到 2020 年，超过一半（52.3％）的比特币付款和转账交易量发送到交易发送到私人钱包。

对于此分析，CipherTrace 通过过滤同一实体内的区块链数据（例如，从 Binance 到 Binance 的交易）识别支付和资金转移。这种过滤消除了代表虚拟资产实体内部交易的大量区块链数据，因为这些内部交易歪曲了加密资金流动的总体情况。通过删除这些数据，分析师可以更好地了解区块链上的支付流程，而不是分析整个未经过滤的区块链数据池。

同样，CipherTrace 还过滤掉了将资金返还给自己（例如剥离链 Peel-Chains，https://www.bitcoininsider.org/category/peel-chains）以及私人钱包间交易的犯罪分子，因为这些交易

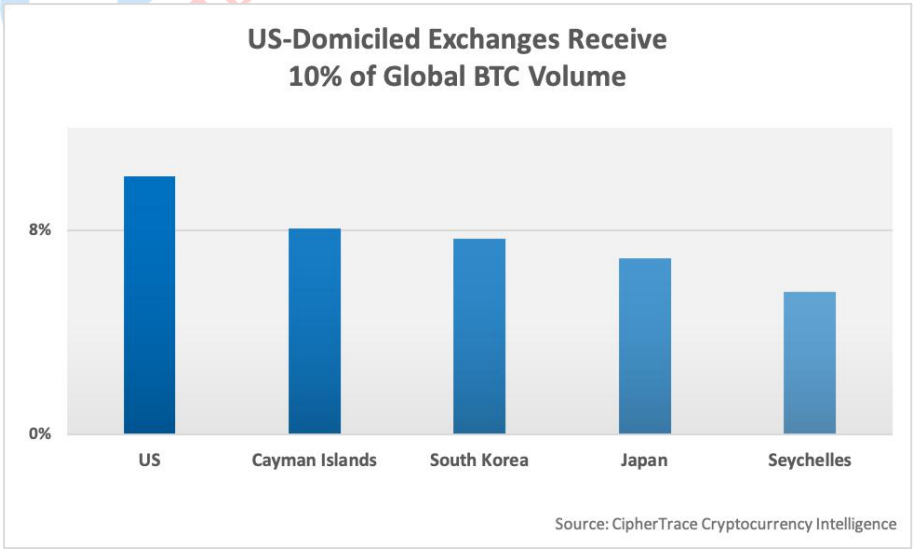
也可以人为地使数据膨胀。在私人钱包间交易中，无法知道个人何时将资金转移到他们控制下的不同帐户中、或进行 P2P 交易。

然而，尽管交易所接收的比特币在全球范围内的总体百分比似乎正在下降，但发送给交易所的比特币的实际数量在 2019 年至 2020 年之间增加了 630 万个，价值约 1500 亿美元。总之，这些趋势可能意味着，尽管交易所继续变得越来越流行，但比特币开始在交易所以外更广泛地使用。




资料来源：CipherTrace 加密货币情报

尽管 2020 年超过一半的比特币付款量用于交易所，但其中大部分来自五个国家/地区的交易所：美国、开曼群岛、韩国、日本和塞舌尔。美国交易所获得的收益最多，占全球比特币总量的 10%，或交易所获得的比特币总量的 19%。




资料来源：CipherTrace 加密货币情报

## （十一）发送到高风险交易所的比特币交易量占比创历史新低

到 2020 年，高风险交易所在全球比特币交易量中所占百分比下降了 59%。有几种因素可以确定何时将实体归类为“高风险交易所”，这些因素包括但不限于以下因素：

- 众所周知的不良行为者
- 有意设法规避 AML 和 KYC 措施
- 与众所周知，经常不与执法和监管机构合作

高风险的交易所以洗钱而闻名。尽管犯罪分子继续将高风险交易所用作许可途径，但 CipherTrace 调查人员继续在犯罪资金的接收端看到更集中、主流的交易所。通常犯罪分子在试图通过使用果皮链、混合器或其他混淆技术混淆资金并将其与犯罪来源隔离后再使用这些交易所。

# 四、2020 年恐怖分子对加密货币的使用

恐怖主义组织及其支持者和同情者一直在寻找新的方法筹集和转移资金，避免被执法机构发现或追踪。像加密货币这样的资产必定引起他们的注意，该资产无需进行尽职调查或保存记录就可以在世界范围内即时进行假名化价值传输。幸运的是，区块链分析以及执法机构的勤奋调查已导致 2020 年恐怖分子融资网络的重大挫败。

## （一）司法部没收加密货币捐款，致使恐怖主义资金损失了 200 万美元

2020 年 8 月 13 日，美国司法部宣布从基地组织、伊斯兰国和哈马斯等著名恐怖组织手中没收 200 万美元的加密货币。这些资金来自这些团体通过社交媒体和自己的网站在线募集的加密货币捐赠。

*“我们的敌人使用现代技术、社交媒体平台和加密货币促进他们的邪恶和暴力的议程，这不会让任何人感到惊讶……”*

*–美国前司法部长威廉·巴尔*

这些恐怖组织使用加密货币购买武器，训练特工并支付国际运输费用。时任司法部长的威廉·巴尔（William Barr）说：“我们的敌人使用现代技术、社交媒体平台和加密货币促进其邪恶和暴力的议程，这不会让人感到惊讶。”

当局与秘密行动者共同进行了调查。根据 IRS 的 Don Fort 的说法，恐怖分子除了捐款外，还通过假冒的慈善机构和诈骗活动筹集资金。这些诈骗活动涉及与冠状病毒大流行有关的防护用品的销售。

美国司法部的报告中重点介绍了哈马斯通过其称为“卡桑旅”（Tassam Brigades）的军事部门的电报频道使用比特币捐款的情况。CipherTrace 先前已在 2019 年第三季度的报告中报告了这一确切的方案。尽管这次行动似乎仅给恐怖组织带来了相当于 5000 美元的收入，但重要的是要记住，进行恐怖袭击的成本可能非常低。

美国国务院反恐怖主义局前反恐金融和指定办公室主任，现恐怖主义、极端主义和反恐怖主义中心主任杰森·布拉扎基斯（Jason Blazakis）解释说：“恐怖分子不必筹集大量的加密货币或现金维持庇护所，或者更糟的是装备可以杀害无辜平民的弹药、枪支和炸弹。 虽然一千美元看起来不算是很多钱，但在错误的人手中，可以完成以上所有工作，甚至更多。”

### （二）法国警方在加密货币恐怖主义融资计划中逮捕了 29 个人

2020 年 9 月 30 日，执法部门逮捕了 29 名与恐怖主义融资活动有关的在法国的特工，这些特工使用加密货币“优惠券”掩盖资金的来源和流向。据信这些在法国的特工隶属于基地组织的下属的 Hayay Tahrir Al-Sham 组织。

法国行动人员从法国的持牌烟草商店购买了价值“数十万欧元”的加密货币“优惠券”，并将优惠券上的凭证发送给叙利亚的圣战分子。圣战分子在那里可以在线兑换比特币。法国金融情报部门 Tracfin 能够检测到从法国流向叙利亚的资金，原因是该组织不断受到监视，导致当局对数十名居住在法国的人进行了调查，这些人“在过去几个月中多次到访了全国的烟草店。国家反恐怖主义检察官办公室说：“他们会匿名购买价值 10 到 150 欧元的优惠券，然后将这些优惠券存入圣战分子在国外开设的帐户。”

## 五、2020 年主要执法行动

2020 年是加密货币广泛采用和价格上涨的一年，这使加密货币欺诈者和不遵守法规的人成为执法行动的主要目标。VASP 与公民开展业务时必须遵守当地法律。除了高额罚款外，那些故意无视许多司法管辖区反洗钱法的人还可能面临个人责任和潜在的牢狱之灾。

### （一）BitMEX 高管被指控非法运营和反洗钱

10 月 1 日，美国司法部（DoJ）宣布起诉四位 BitMEX 高管，指控该组织违反《银行保密法》（BSA），并密谋违反了 BSA，“故意不建立、实施和维持适当的反洗钱（AML）计划。”当天，美国商品期货交易委员会（CFTC）提起民事诉讼，指控拥有和运营 BitMEX 交易平台的五个实体和三个个人，其中包括 BitMEX 首席执行官 Arthur Hayes。

这些指控包括操作未注册的交易平台和违反多项 CFTC 法规，例如在产生 10 亿美元的交易费用时未能实施 AML 程序。被告人每人将面临长达 10 年的监禁，CFTC 的禁令可能高达 13 亿美元，这使其成为金融机构有史以来支付的最昂贵的反洗钱（AML）罚款之一。

自 2019 年初以来，美国商品期货交易委员会（CFTC）一直在调查 BitMEX 是否允许美国人在其交易所进行交易。尽管该平台声称已经改进了他们的客户身份识别程序，有效地将美国人排除在外，但 CFTC 的投诉却声称并非如此。根据投诉，BitMEX 是由同一个人所有和控制，由同一人经营的错综复杂的公司实体。这些业务包括：HDR Global Trading Limited，100x Holdings，ABS Global Trading，Shine Effort 和 HDR Services。（注释：这些是 BitMEX 的母公司，信息来自互联网搜索）

根据 CFTC 的说法，HDR Global Trading Limited 运营着 BitMEX 交易平台。尽管在塞舌尔注册成立了 HDR，但“HDR 在塞舌尔没有，也从未有过任何业务或员工。”尽管注册在塞舌尔，但 Arthur Hayes 通过特拉华州的一家有限责任公司持有 BitMEX 实体的所有权权益，该公司在美国的金融机构拥有银行账户。尽管 BitMEX 为至少 8.5 万名美国客户提供服务，并在美国境内管理其很大一部分交易基础设施--一半的员工在旧金山或纽约办事处工作--但 BitMEX 从未在 CFTC 注册。

## 1. AML 缺陷和未举报可疑活动

起诉书还声称，BitMEX 不仅没有遵守保存记录的义务，而且该公司还积极删除了关键的客户身份信息。在某些情况下，这些记录被删除“显然是因为发现用户位于美国或其他受限制的司法管辖区”。美国司法部的起诉书补充称，自 2014 年末 BitMEX 推出以来，至少在 2020 年 9 月左右，该交易所没有提交任何 SARS 申请，没有报告平台上的可疑非法活动。

针对美国司法部的起诉书，美国曼哈顿代理检察官奥黛丽·施特劳斯（Audrey Strauss）说，“随着在美国经营金融机构的机会和优势，这些企业有义务尽自己的一份力量，帮助驱逐犯罪和腐败。据称，这些被告藐视这一义务，并承诺经营据称是“离岸”的加密交易所，而故意不执行和维持甚至基本的反洗钱政策。据称，他们这样做是为了让 BitMEX 在金融市场的阴影下作为一个平台运作。今天的起诉是本办公室和我们在联邦调查局的合作伙伴为揭露洗钱平台而进行的又一次努力。”

BitMEX 在其网站上回应了这些指控，称“我们强烈反对美国政府提出这些指控的高压决定，并打算积极为这些指控辩护。从我们作为一家初创公司的早期开始，我们一直寻求遵守适用的美国法律，因为这些法律在当时是被理解的，并且是基于现有的指导。”

### 2. 提高 AML 合规性的步骤

为了提高合规性，BitMEX 已经采取措施增加他们的 AML 程序。自被起诉以来，BitMEX 已聘请英国皇家联合军种研究所(Royal United Services Institute)金融犯罪和安全研究中心副研究员马尔科姆 •赖特(Malcolm Wright)担任公司首席合规官。赖特将监督交易所的全球合规活动，并直接向 BitMEX 代理临时首席执行官兼首席运营官 Vivien Khoo 汇报工作。目前仍不清楚 BitMEX 在赖特之前是否有 CCO。

在重新评估 BitMEX 的 KYC 后，CipherTrace 发现该交易所已经改进了其做法，自本月早些时候我们的地理风险报告发布以来，该交易所的 KYC 评分已从“漏洞百出”(黄色)转为“强劲”(绿色)KYC 评分。这进一步证实了 BitMEX 加强合规程序的立场，证明聘用新 CCO 的努力没有白费。

## （二）Ripple，高管面临 SEC 诉讼

美国证券交易委员会于 12 月 22 日对 Ripple，Ripple 首席执行官 Brad Garlinghouse 和该公司的联合创始人 Chris Larsen 提起诉讼，指控该公司出售 XRP 构成发行未注册证券。

Ripple 在一份富国银行(Wells)提交的文件中回应了这起诉讼-在这份文件中，面临执法行动的个人或企业有机会提出事实和法律论点，以说服 SEC 不应提起诉讼。在提交给富国银行的文件中，Ripple 声称：“委员会声称 Ripple 发行的 XRP 是投资合同，同时坚称比特币和以太币不是证券，这是在挑选虚拟货币的赢家和输家，在这过程中破坏了基于美国的、对消费者友好的创新。”然而，比特币和以太币的去中心化特性使它们免于 SEC 的强制执行。另一方面，XRP 更加集中。

在 SEC 诉讼结果公布之前，许多交易所已将 XRP 暂停或除牌。该列表包括：Binance.US，Coinbase，eToro 和 Bittrex。一些拥有 XRP 头寸的投资公司，例如 Greyscale 和 Bitwise Asset Management，也已经清算了所持股份。

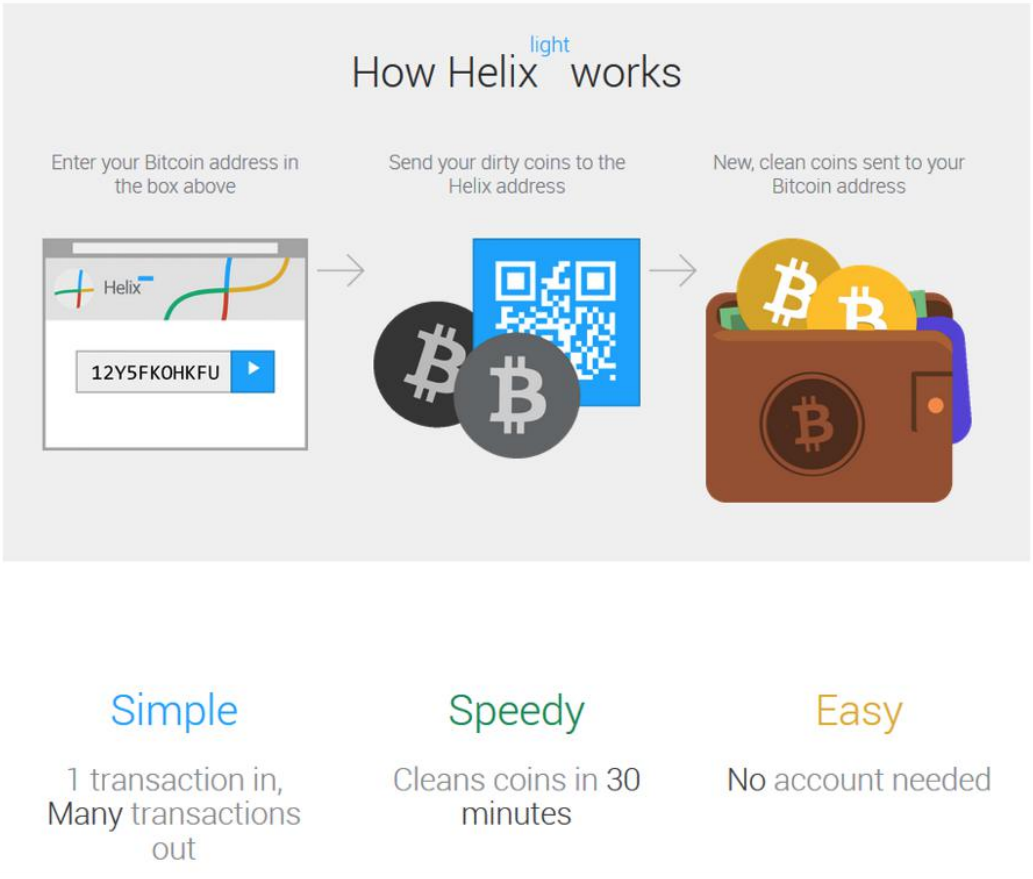
Garlinghouse 在 SEC 做出决定前一个月的 PompPodcast 节目中表示，他相信，在 XRP 被宣布为证券的“假设情景”下，他的公司仍将蓬勃发展。加林豪斯后来补充说，“超过 90%的 RippleNet 客户不在美国。”然而，这起诉讼和随后的退市导致 XRP 价格暴跌，而大多数硬币仍然看涨，影响了无数与 Ripple 或美国没有联系的 XRP 零售持有人。

虚拟预审定于 2021 年 2 月 22 日进行。

## （三）FinCEN 因 Helix Mixer 运营商与臭名昭著的黑市有关的比特币洗钱计划处以 6000 万美元罚款

今年 2 月，联邦执法部门以洗钱罪逮捕了俄亥俄州阿克伦市的拉里·迪恩·哈蒙，这是加密货币匿名服务最重要的一次行动。哈蒙的螺旋“暴跌”操作移动了大约 3 亿美元的比特币。司法部指称，Helix 曾与现已停业的地下市场 AlphaBay 合作，该市场以毒品交易和其他非法活动闻名，直到 2017 年被执法部门关闭。

根据起诉书，Helix 使客户能够以一种旨在隐藏交易和比特币所有者的方式发送比特币。把一个玻璃杯或“搅拌机”想象成一个类似于搅拌机的东西，你可以把各种各样的水果放进搅拌机里做成冰沙。一旦叶片旋转，几乎不可能区分香蕉和草莓。同样，一旦匿名服务将干净的加密货币与被盗或用于贩毒等犯罪活动的加密货币混合，就很难追查不良资金的来源。美国国税局刑事调查处处长唐福特（donfort）表示：“Helix 的厚颜无耻应该是这次行动对普通市民最可怕的一面。“有坏人，也有罪犯为数百起其他犯罪提供便利。哈蒙行动的唯一目的是对执法机关隐瞒犯罪交易。



八个月后的 10 月 19 日，芬森宣布对 Harmon 处以 6000 万美元的民事罚款，罪名是违反《银行保密法》（BSA）及其实施条例。Harmon 通过各种方式接受和传输比特币，充当了可兑换虚拟货币的交换者。FinCEN 发现，Harmon 故意违反 BSA 的注册、计划和报告要求，未注册为 MSB，未实施和维护有效的反洗钱计划，未报告可疑活动。

## （四）BitGo 与美国财政部就多次违反加密制裁的行为达成 98,830 美元的和解协议

根据美国财政部海外资产控制办公室（Office of Foreign Asset Controls）12 月 30 日发布的一份执法公告，机构加密托管服务和钱包运营商 BitGo 未能阻止明显位于受制裁司法管辖区的人士通过其平台开立账户和发送数字货币。

该新闻稿指出，向乌克兰，古巴，伊朗，苏丹和叙利亚的克里米亚地区发送的交易中有 183 起明显违规，总计超过 9,000 美元。财政部声称，BitGo 有理由根据用户登录平台时收集的 IP 数据知道这些用户位于受制裁的辖区中，但是 BitGo 缺乏任何阻止受制裁辖区中的用户访问其服务的控件。

虽然适用于这些事项的法定最高民事罚款为 53051675 美元，但外国资产管制处认定，这些明显的违规行为构成“不严重的案件”，双方达成了 93 830 美元的和解。事实上，BitGo 是一家小公司，配合 OFAC 对违规行为的调查，并投资采取重大补救措施应对违规行为，这些都是导致结算金额降低的缓解因素。

OFAC 在执法行动中强调，制裁遵守义务适用于所有美国人，包括那些参与提供数字货币服务的人。两个月前，OFAC 发布了一项警告，警告称允许客户支付勒索软件的赎金可能违反了制裁规定。

## （五）联邦调查局和德国警方指控 movie2k.to 的运营商并没收 3000 万美元的加密货币

由于联邦调查局和德国当局的联合调查，8 月 6 日从非法电影流媒体网站 movie2k.to 的涉案人员手中缴获了价值 2500 多万欧元的加密货币——价值 2960 万美元的比特币（BTC）和比特币现金（BCH）。

据德国《明镜》周刊报道，movie2k.to 是分享盗版电影的最大平台之一。由于版权侵权问题，该网站于 2013 年春季正式关闭；在关闭之前，该网站的运营商据称能够发行 88 万部盗版电影。movie2k.to 的一名运营商曾担任该网站的程序员，自 2019 年 11 月以来一直被警方拘留。这名程序员目前已全面供认了指控，据报道，他正在协助当局继续调查第二名主要运营商，该运营商仍在逃。

## （六）美国检察官办公室指控男子无照经营自动取款机网络

美国检察官办公室发表声明，详细说明约尔巴·琳达（Yorba Linda）男子凯斯·穆罕默德（Kais Mohammad）参与 Herocoin 非法加密货币业务的认罪过程。Herocoin 通过当面交易和比特币 ATM 机网络交换了高达 2500 万美元的资金。

根据他的认罪协议，穆罕默德亲自提供比特币现金兑换服务，每一笔金额高达 25000 美元。在一个典型的比特币现金兑换交易中，穆罕默德通常不询问客户资金的来源，而且在许多情况下，他知道资金来源于犯罪活动。

Mohammad 还拥有一个比特币 ATM 型售货亭网络，位于整个洛杉矶地区的购物中心、加油站和便利店网络中。这些信息亭允许顾客用现金购买比特币，或者用现金出售比特币。

根据认罪协议，穆罕默德在知情的情况下决定不在美国财政部金融犯罪执法网(FinCEN)注册希罗币（Herocoin）。据报道，他还拒绝制定有效的反洗钱计划，也没有为可疑交易提交货币交易报告。

尽管比特币自动取款机过去曾为犯罪分子和骗子提供服务，但全球监管环境正在收紧对加密自动取款机运营商的监管。世界各国都制定了新的立法，专门监管将密码兑换成现金的企业，要求它们获得超过一定门槛的所有交易的 KYC 信息。这次 KYC 信息收集和记录保存也是遵守加密自动取款机运营商必须遵守的‘旅行规则’规定的关键一步。这些规定对于各国政府起诉和阻止那些使用比特币洗钱的人至关重要。

## （七）涉嫌国际加密犯罪圈中的十五人认罪

6 月 16 日，加密交换公司 CoinFlux 的所有者弗拉德·克林·尼斯特（Vlad-Călin Nistor）和他的 14 名同伙因参与一项国际加密货币骗局而认罪。根据美国司法部的说法，这个犯罪团伙负责欺诈性的网上拍卖，这些拍卖用于通过尼斯特的加密货币交易所洗钱，他们将加密货币兑换成菲亚特，然后以 CoinFlux 员工和家庭成员的名义将资金存入银行账户。

关于调查，司法部刑事司助理司法部长 Brian Benczkowski 评论说：“今天的现代网络罪犯依靠越来越先进的技术来欺骗受害者，往往伪装成合法的生意。”，“这些认罪证明，美国将追究外国和国内犯罪企业及其推动者的责任，包括欺骗美国公众的不正当比特币交易。”

不过，真正的危险可能来自其他民族国家行为者，他们试图通过使用加密货币交易所来掩盖自己的踪迹来复制这种行为。司法部长本兹科夫斯基(Benczkowski)在他的新闻稿中强调了这一危险，他

说，“这一次(加密货币交易所)被犯罪欺诈者使用，但我们从民族国家行为者那里看到的情况肯定有相似之处。”

这个案例展示了加密货币交易所如何被滥用来洗钱，突出了旅行规则的重要性。与较差的 KYC 或反洗钱控制薄弱的地区进行交流，使得信任和分享这些证据变得更加困难。

## （八）美国司法部指控“AML 比特币”创始人洗钱

6 月 22 日，美国司法部指控 NAC 基金会首席执行官、AML 比特币创始人马库斯·安德拉德(Marcus Andrade)犯有电信欺诈和洗钱罪。美国证券交易委员会(SEC)宣布对安德拉德采取类似的刑事行动，原因是安德拉德进行了欺诈性、未注册的 AML 比特币发行，并欺骗了投资者。

SEC 称，NAC 基金会通过出售代币从 2400 多名投资者那里筹集了近 560 万美元，这些代币后来可能会转换成 AML 比特币。《反洗钱比特币白皮书》将该代币描述为优于原始比特币，因为据称该代币内置了反洗钱、反恐和防盗技术，这些技术将驻留在 NAC 自己的“私人监管的公共区块链”上。然而，美国证交会的起诉书称，这些能力实际上都不存在。

美国证券交易委员会(SEC)执行部网络部门负责人克里斯蒂娜·利特曼(Kristina Littman)表示，安德拉德“一再误导投资者，让他们为不存在的技术提供资金，错误地声称该技术将使数字资产交易更加安全”，并补充说，“投资者有权获得真实信息，这样他们就可以在充分知情的情况下做出投资决策。”

## （九）SEC 命令 Telegram 向投资者返还 12 亿美元，支付 1850 万美元的罚款以解决指控

6 月 26 日，SEC 获得法院批准与 Telegram 达成和解，以了结有关其未注册的 ICO“gram”违反联邦证券法的指控。根据和解协议，在不承认或否认指控的情况下，被告同意向投资者返还超过 12 亿美元，并支付 1850 万美元的民事罚款。

SEC 执法部门网络部门负责人 Kristina Littman 指出，“欢迎新兴和创新企业加入我们的资本市场，但不能违反联邦证券法的注册要求。”她补充说：“这项和解协议要求 Telegram 将资金退还给投资者，并处以巨额罚款，并要求 Telegram 通知未来的数字产品。”

美国证交会于 2019 年 10 月首次对 Telegram 提起诉讼，原因是该公司未能登记其提前出售的 17 亿美元“Grams”代币。

## （十）中国当局逮捕 100 多名参与 PlusToken 庞氏骗局的人。

7 月 31 日，中国当局逮捕了涉嫌参与 PlusToken 加密货币欺诈圈的 109 人。PlusToken 的庞氏骗局用广告宣传加密货币的高收益投资，该公司声称投资者将获得 9%至 18%的月收益。

成员们被鼓励让其他人加入，以换取一个奖励，创造了一个庞大的庞氏骗局。去年，PlusToken 的运营商实施了一次可疑的退出骗局，从多达 400 万用户的账户中提取了大约 30 亿美元，这些用户突然发现自己无法获得资金。中国公安部说，他们有 27 名“主要犯罪嫌疑人”和另外 82 名“关键”成员被警方拘留。

随着这起案件的不断展开，经济损失的真实范围不断暴露出来。最初估计被盗金额为 30 亿美元，但中国的媒体新闻（chainnews）现在显示，投资者被盗 60 亿美元。此前，英国也发生了类似事件，当局最近关闭了加密货币诈骗平台 GPay 有限公司。英国高等法院下令 GPay 赔偿投资者资金 150 万英镑（约合 180 万美元）的损失。

## （十一）美国检察官试图向庞氏骗局的受害者返还 650 万美元的加密货币

美国检察官正试图返还从“ Banana.Fund”众筹项目的受害人那里获得的 650 万美元的加密货币，这是一个所谓的庞氏骗局。

官方报告未按名称标识 Banana.Fund 的运营方。但是，几名涉嫌诈骗的受害者证明该基金由英国人理查德·马修·约翰·奥尼尔（Richard Matthew John O'Neill）（又名“乔·库克”）经营。

联邦检察官指控香蕉基金的管理人向投资者承认他的项目失败了，承诺返还 170 万美元，但后来又没有兑现。检察官声称，这位行政官员随后秘密开始了一项洗钱和退款计划，导致美国特勤局（USSS）扣押了 482 比特币（BTC）和 1721868Tether（USDT）。

该诉讼于 7 月 29 日在美国哥伦比亚特区地方法院提起，旨在使联邦政府拥有资产的所有权，以便将其归还受害者。

司法系统对待加密货币的方式可以揭示法律对待加密货币的前进方向。随着各国政府想方设法将被盗或被骗的资金归还其合法所有者，其影响将远远超出这一特定案件的范围。

## （十二）Centra Tech Inc.联合创始人涉嫌 2500 万美元骗局

7 月 13 日，Centra Tech Inc.的联合创始人 Sohrab“Sam”Sharma 正式认罪，因为他参与了一场骗局，通过首次公开募股(ICO)从投资者那里窃取了超过 2500 万美元。他的公司在包括拳击手弗洛伊德·梅威瑟(Floyd Mayweet)和音乐家 DJ 哈立德(DJ Khaled)在内的名人的帮助下推动了首次公开募股(ICO)。

Centra Tech 的其他联合创始人罗伯特·法卡斯(Robert Farkas)和雷蒙德·特拉帕尼(Raymond Trapani)已经承认，他们在开发“Centra Card”和万事达卡(Mastercard)支持的购物方面向投资者撒谎。Centra Card 据称是一种借记卡，客户可以使用密码进行 Visa 支付。

这三人还被指控谎称他们有一位毕业于哈佛大学的首席执行官，拥有 20 多年的商业经验，与万事达卡(MasterCard)和 Visa 等大公司建立了合作伙伴关系，并在超过 38 个州持有执照。检察官声称，他们兜售这些谎言是为了诱使投资者向欺诈性的 Centra 代币骗局投入更多资金。

## （十三）中国警方破获套利诈骗案，价值 1500 万美元的加密货币和超级跑车

7 月 9 日，中国公安部宣布，他们从涉嫌销售假币的新型诈骗运营商手中查获了 1500 万美元的密码和价值 200 万美元的超级跑车。这次行动拘捕十名涉嫌操控诈骗计划的人。

根据该部的说法，这是中国第一例举报的刑事案件，据称受害者是使用区块链智能合约诈骗受害者以产生假加密货币的。此案最早于 2020 年 4 月由一名被称为李的受害者向警方报告，他加入了一个名为“火币全球套利 HT 华人社区”的 Telegram 组织。

根据 Li 的说法，该组织宣传了一个区块链智能合约，该合约据称产生了 Huobi Tokens（HT），可以产生套利机会，回报率为 8%。Li 解释了智能合约的工作原理：“简单来说，您将一个 ETH 单位发送到指定地址，您将收到 60 HT。然后您可以出售它以获取差价。”但是，在 Li 向 Telegram 组管理员提供的以太坊地址发送了 10 ETH 之后，他获得的 600 HT 是伪造的代币，无法存入出售。

## （十四）警方逮捕了 BitGrail 老板，因为他参与了意大利最大的网络金融攻击

运营意大利加密货币交易所 BitGrail 的男子涉嫌诈骗超过 23 万人共计 1.2 亿欧元（1.46 亿美元），被捕。BitGrail 老板被视为“意大利最大的网络金融攻击，也是世界上最大的攻击之一”，面临着计算机欺诈，欺诈性破产和洗钱的指控。

2018 年，同一名男子向警方通报了一起纳米硬币黑客攻击事件，称损失“一笔巨款”。意大利国家网络犯罪中心负责人伊万诺·加布里埃尔（Ivano Gabrielli）说，当他们的团队开始调查

时，很明显，这名男子实际上是 BitGrail 的头目“[而且]现在还不清楚他是否积极参与了盗窃，或者他只是在发现后决定不增加安全措施。”

警方进一步称，这名 34 岁的男子被称为“F.F.”，他进行了干预，以阻止他们阻止继续盗窃。

## （十五）澳大利亚加密货币借贷计划发起人被判入狱 20 年。

澳大利亚男子 John Bigatton 曾担任加密货币贷款计划 BitConnect 的发起人，他被澳大利亚证券和投资委员会(ASIC)起诉，并被判处最高两个十年监禁。比加顿被发现经营着一项未经注册的管理投资计划，该计划提供无照金融服务，并通过提供误导性财务报表来欺骗客户。在 ICO 狂热的高峰期，BitConnect 传销计划的估值一度超过 25 亿美元。

在 Bigatton 被判刑之前，ASIC 在 9 月份禁止 Bigatton 提供金融服务。除了被判刑外，Bigatton 还必须赔偿至少 8 万澳元的澳大利亚货币（合 5850 万美元）。

在 2017 年加密货币牛市的巅峰时期，像 BitConnect 这样的投资计划非常猖獗，这可能会为新生的 Defi 行业提供经验教训。截至 2019 年底，Defi 的总锁定价值不到 10 亿美元。截至 2020 年底，总锁定价值超过 198 亿美元，令人振奋地将其与 2017 年的加密货币泡沫相提并论。那些希望通过启动 Defi 协议而不采取适当的安全审计措施来“快速致富”的人不应该忘记 2017 年。正如 BitConnect 案所表明的那样，欺诈和玩忽职守的肇事者仍在受到指控。。

## （十六）美国司法部从巴西一项加密货币投资计划中查获 2400 万美元

11 月 4 日，美国司法部（DOJ）宣布，“美军行动”（Operation Egypto）是美巴西共同努力追回从加密货币欺诈计划中窃取的资金所使用的代号，导致查获 2400 万美元。巴西向美国调查提供帮助，因为该计划针对美国居民，其中包括鼓励他们投资于伪造投资机会，其中包括将巴西货币或加密货币存入犯罪者控制的账户。

根据司法部的新闻稿，该计划的幕后策划者马科斯·安东尼奥·法冈德斯被控“非法经营金融机构、欺诈性管理金融机构、挪用公款、违反证券法和洗钱”。巴西调查人员说，已经追回的钱将被送回受害者手中。

瑞士人工智能在线保护项目 Immuniweb 的创始人伊利亚·科洛琴科（Ilia Kolochenko）提到，对于这样的犯罪，多个国家参与进来是至关重要的，这样这个计划就不会产生病毒效应，在网络上大行其道。

## （十七）美国国税局将乌克兰国民判刑称为美国首例比特币税收欺诈案

11 月 9 日，美国司法部(DoJ)宣布，一名居住在华盛顿的 26 岁乌克兰人被判处 9 年监禁，美国国税局(IRS)称这是美国“第一起含有税收成分的比特币案件”。

Volodymr Kvashuk 曾是微软的一名员工，据称他从微软窃取了 1000 多万美元的数字礼品卡等货币储值（CSV）。据 Cointelegraph 报道，Kvashuk“利用同事的账户和身份窃取并出售 CSV——让人觉得他的同事对欺诈负有责任。”

Kvashuk 试图通过使用比特币混合服务来隐藏被盗价值的来源，然后与美国国税局(IRS)沟通，称标记为通过他账户的 280 万美元密码资产是一位亲戚送给他的礼物。他提交了一份假税单来支持虚假申报。

## （十八）OKEx 创始人徐明星被警方拘留

10 月 16 日，中国新闻媒体报道 OKEx 创始人徐明星被警方带走。徐的加密货币交易所总部位于香港，但在马耳他拥有执照，在逮捕发生地上产生了一些歧义。

此前，有报道称，由于交易所的一名私钥持有人（可能是徐）缺席，OKEx 暂停了加密货币的取款——不过，来自火星金融（Mars Finance）的一份报告显示，情况并非如此。火星财经的报道认为，徐可能被警方带走以协助调查 OK 集团借壳上市一事，与交易所停止退市完全无关。OKEx 首席执行官兼联合创始人杰伊·郝（Jay Hao）表示：“这个问题是个人问题，不会影响业务。”OKEx 的声明试图向用户保证徐与 OKEx 的距离，声称他的参与最近集中在 OK Group 和 OK Coin 的独立实体上。（译者注：OKEx 已经恢复所有业务）

透明度差和管辖权购买合谋增加了交易者的风险，超出了基础虚拟资产的波动性。OKEx 似乎位于马耳他，这是一个管理良好的司法管辖区，但根据其服务条款，非马耳他和非意大利客户通过塞舌尔子公司 Aux Cayes 提供服务。除了马耳他和意大利以外，Aux Cayes 还提供风险更高的金融产品，包括保证金贷款、点对点匹配、现货服务以及与 VFA 或指数相关的衍生产品。

## （十九）全球加密货币洗钱卡特尔交易-20 人被捕

来自 16 个国家/地区的执法机构在 10 月进行了一次重大镇压合作，逮捕了 33 名涉嫌加密货币洗钱的犯罪分子。其中有 20 人被怀疑是 QQAAZZ 犯罪网络的成员，据称自 2016 年以来，该网络已为网络犯罪分子洗劫了数千万美元。

据 Cointelegraph 称，“(这些)资金据称是通过国际银行账户、位于波兰和保加利亚的空壳公司以及加密货币混合服务转移的。”为了逮捕这些人，当局搜查了欧洲 40 多个家庭，并在保加利亚缴获了比特币开采设备。

同一天，在另一起案件中，一名新西兰男子因涉嫌洗钱 200 万美元的加密货币而被捕，部分原因是他购买了一辆兰博基尼(Lamborghini)和一辆梅赛德斯 G63(Mercedes G63)等豪华汽车。

10 月 15 日，美国司法部(US Department Of Justice)公布了一份替代起诉书，其中详细列出了一起针对 6 名个人的案件，他们被控合谋“代表外国卡特尔洗钱数百万美元的毒品收益”。赌场、幌子公司、现金走私和银行账户都被用来洗钱，其中一人使用加密货币贿赂一名美国国务院官员，试图获得欺诈性的美国护照。

洗钱和货币本身一样古老。随着犯罪分子越来越多地寻求加密货币来隐藏非法资金的来源，执法和调查机构利用加密货币跟踪服务和区块链分析将变得更加重要。“跟着钱走”通常会引出源头。

10 月 15 日，美国司法部发布了一项替代起诉书，其中详细描述了一起针对 6 个人的阴谋，该阴谋共谋“国外联盟集团洗钱了数百万美元的毒品”。赌场、前台公司、走私现金和银行账户都被用来洗钱，一个人用加密货币贿赂美国国务院的官员，以试图获取欺诈性的美国护照。

**洗钱的历史与货币本身一样悠久。随着犯罪分子越来越多地使用加密货币来隐藏非法资金的来源，执法和调查机构利用加密货币追踪服务和区块链分析将变得更加重要。“追踪资金”通常会找到资金来源。**

## （二十）比特币托管公司首席执行官承认欺诈和挪用公款

10 月 1 日，纽约比特币托管公司 Volantis 的负责人乔恩·巴里·汤普森（Jon Barry Thompson）承认欺诈和挪用投资者资金超过 700 万美元。在 CoinDesk 获得的法庭文件中，汤普森承认对 Volantis 的比特币保管、控制、购买行为以及风险敞口进行了虚假陈述，为确保投资者资金安全。汤普森可能面临最高 60 年的监禁。他的判决定于 2021 年 1 月 7 日。

汤普森还与美国商品期货交易委员会（CFTC）达成和解，同意支付 740 万美元的赔偿金，并被禁止在未来从事比特币交易，并承诺在未来的 CFTC 调查中进行全面合作。

## （二十一）加密交易员被指控欺诈并被要求向投资者偿还超过 600 万美元

托马斯·吉蒂（Thomas J. Gity）是佛罗里达州一名男子，经营着一家数字资产交易公司，他被指控欺诈和从投资者那里挪用了 600 多万美元。SEC 于 9 月 29 日提起的诉讼称，Gity 在 2018 年 1 月至 2019 年 1 月期间，通过宣传“他是一名高利润的数字资产交易员，从未在交易日中亏损”的虚假陈述，骗取了投资者 680 万美元。

吉蒂（Gity）利用这一谎言以及巨额回报的承诺，吸引了超过 18 位投资者加入他的公司。他还声称自己管理着 1 亿美元的资产。SEC 称，吉蒂使用了大部分投资者资金来延续他的庞氏骗局计划，同时为儿子筹集了约 180 万美元。

## （二十二）Coincheck 黑客盗取的加密数字货币在日本首次正式没收

8 月 19 日，东京地方法院发布了一项命令，扣押从东京的加密货币交易所 Coincheck 窃取的部分挪用资金。2018 年，Coincheck 被黑客攻击，攻击者盗窃了超过 5 亿美元的新经币 NEM（XEM）。当时，它是迄今为止最大规模的加密黑客攻击之一。但是，此后，XEM 代币的价值下降了 93%。最初的价值现在估计约为 3,900 万美元。

据报道，法院对大博市医生井居隆（Takayoshi Doi）下达了没收令。Doi 不涉嫌参与 2018 年黑客攻击; 但是，他被指控从黑客那里购买了 XEM。

这是日本法院首次下令没收加密货币。涉及的 XEM 和比特币的资金总额约为 480 万日元（约合 45,000 美元）。在做出正式裁决之前，Doi 有望确保资金安全。

## （二十三）司法部以加密货币挖矿欺诈罪指控 Airbit 创始人

8 月 18 日，美国司法部发布了一项起诉书，指控 AirBit 运营商进行国际欺诈、洗钱和通过一家所谓的加密货币公司欺诈个人。

AirBit Club 的五位创始人-Pablo Rodriguez，Gutemberg Dos Santos，Scott Hughes，Cecilia Millan 和 Jackie Aguilar 自 2015 年初以来一直运营该公司。根据美国司法部的说法，Airbit 被广告宣传为一家加密货币采矿和贸易公司。

接受采访的受害人证明了他们在 Airbit 网站上查看帐户时获利的印象。但是，这些利润实际上是不存在的。相反，Airbit 的运营商将这些资金用于支付他们过分奢侈的生活方式。美国司法部称，该团伙还参与了至少 2,000 万美元的洗钱活动。

## （二十四）马来西亚当局逮捕了窃取了超过 60 万美元电力的加密矿工

9 月 1 日，马来西亚国家官员结束了历时三年的加密挖矿行动，该行动窃取了价值逾 60 万美元的电力。

该国能源委员会区域主任纳兹林·阿利姆·萨迪基（Nazlin Alim Sadikhi）表示：“我们发现安装了非法线路，以便直接供电，而不是通过 TNB 电表供电。”

萨迪基（Sadikhi）解释说，该集团最大的加密采矿设备包括 100 多个单独的采矿设备，并且已经不间断地运行了三年。该计划的实施者每月只需支付 7 至 14 美元的电费，但每月消耗的电力价值超过 20,000 美元。

## （二十五）美国货币监理署 OCC 首次对一家总部位于纽约的银行采取执法行动，指控其缺乏加密货币“反洗钱”合规

2020 年 1 月 30 日，美国货币监理署（OCC）对纽约的 M.Y. Safra 银行（MYSB）发起了首个与加密货币相关的执法行动，这是美国首次对银行采取执法行动。OCC 称，两年多来，MYSB 未能完全审查其高风险辖区中的加密货币客户和交易。

该命令完全集中在银行数字资产客户(DACs)合规和监控方面缺陷的反洗钱(AML)实践。报告中提到的缺乏反洗钱控制措施包括在没有足够的客户尽职调查（CDD）的情况下为 DAC 开立账户，以及缺乏对与这些客户相关的可疑交易的充分监控和调查。这些实体包括加密货币交易所、比特币 ATM 运营商、ICO、孵化器和虚拟 OTC 以及其他与加密相关的业务。

在 CipherTrace 博客上阅读更多详细信息：
https://ciphertrace.com/occ-hits-new-york-based-bank-with-first-ever-enforcement-action-for-lack-of-crypto-aml-compliance/

# 六、重大盗窃、诈骗和欺诈

在过去的两年中，大规模的退出骗局已成为加密货币犯罪的主导。2020 年，与 2019 年的 PlusToken HYIP 类似的 WoToken 在退出骗局中骗取了 11 亿美元。由于这些巨额诈骗，欺诈行为占 2020 年犯罪

总量的 73%。但是，数据还表明，2020 年的黑客攻击数量少于前一年，随着实体继续强化系统并采取防范内部和外部威胁的措施，加密领域的成熟度不断提高。以下是重大盗窃、诈骗和欺诈的摘要。

## （一）社交媒体巨头推特遭到内部人士的攻击

7 月 15 日，多个备受关注的加密货币交易所、公众人物以及各种实体的 Twitter 账号被黑客入侵，这些黑客发起了比特币替身骗局。骗子不久后就开始将资金转移到加密货币交易所和混合服务中。

7 月 30 日，Twitter 发布了一份最新调查报告，声称此次黑客攻击是针对其员工的“电话鱼叉式网络钓鱼攻击”的结果，超过 130 个经过验证的 Twitter 帐户受被攻破。黑客成功地在 130 个被盗帐户中的 45 个发布了比特币钓鱼诈骗推文，其中包括巴拉克·奥巴马（Barack Obama），埃隆·马斯克（Elon Musk），比尔·盖茨（Bill Gates）和乔·拜登（Joe Biden）。

电话鱼叉式网络钓鱼是一种复杂的网络钓鱼形式，其中恶意行为者使用电话针对特定企业或个人。在这些电话中，Twitter 黑客可能已经说服受害者提供了用于访问 Twitter 内部工具的密码或其他信息。

Twitter 在一条推文中说：“ 2020 年 7 月 15 日的攻击是通过电话鱼叉式网络钓鱼攻击了一小部分员工”，并补充说：“这次攻击是依赖于一次重大的、协调一致的尝试，误导某些员工，利用人类的弱点来访问我们的内部系统。”

我们的研究表明，大多数比特币在被黑客攻击后存放在未知地址中-最有可能是私人钱包。我们还能够将比特币的某些部分追踪到交易所和其他钱包服务中，特别是那些具有隐私增强功能的服务。

在黑客攻击之后，Twitter 缺乏安全协议的细节被严厉披露。根据 Decrypt 的说法，“超过 1,000 名 Twitter 员工甚至外部承包商都可以访问该平台的所谓“上帝模式”管理面板。彭博社（Bloomberg）在 2017 年和 2018 年透露，那些有权使用该管理工具的承包商曾滥用该工具来窥探碧昂丝（Beyonce）等人的信息，跟踪音乐家的地理位置数据并查看私人信息。

在博客中阅读我们对黑客行为的完整分析：https：//ciphertrace.com/twitter-hacked-insiders-compromise-social-media-giant/

## （二）加密货币交易所 KuCoin 的热门钱包被黑客攻击

9 月 26 日，总部位于新加坡的数字资产交易所 KuCoin 宣布，它检测到比特币（BTC）和以太坊（ETH）代币在前一天 UTC 时间 19:05 开始向一个未知的钱包提款，影响了大约 1.5 亿美元的用户资金。

KuCoin 首席执行官 Johnny Lyu 在直播中表示，渗透到其系统的组织已获得 KuCoin 的以太坊热钱包的私钥。然后，黑客将两个热钱包的大部分内容发送到外部以太坊地址。总共，攻击者总共代购了 11,480 ETH。

在被黑客攻击后，KuCoin 将其剩余的热钱包转移到了新的安全钱包中，并冻结了所有客户的存款和取款。大多数被盗的加密货币是 ERC20 代币，可以通过 DeFi 协议轻松对其进行清洗。该案例标志着 DEX 的第一个高调实例，在这个案例中，Uniswap 被用作货币混合器。与集中式交易所不同，DEX 不能冻结资金--只有特定项目才能冻结。

10 月 3 日，Lyu 宣布该交易所已经确认了黑客嫌疑人，并正式将执法部门参与调查。

## （三）DeFi 黑客使用复杂攻击从 Balancer 盗取 50 万美元

6 月 29 日，去中心化金融（DeFi）流动性提供平台 Balancer 被黑客盗取以 50 万美元的加密货币。在几篇在线报告之后， Balancer 确认发生了一个事件，该事件影响了两个包含转账费用的池，即所谓的通货紧缩代币。

Balancer 描述了攻击者如何从非托管交易所 dYdX 中获得以太坊（ETH）的快速贷款，如何将这些 ETH 转换为 WETH（包裹的以太坊），执行随后的 STA 代币交易，并最终从池中耗尽了 STA 余额。根据该平台，一旦池中的余额接近零，“它相对于其他代币的价格将非常高，而攻击者（使用）STA 将以极低的价格交换池中的其他资产。”

CryptoNews 指出，此攻击与今年早些时候发生的其他攻击具有相似之处。今年 2 月，代币化的保证金交易和借贷平台 bZx 遭受了两次攻击，这些攻击被定义不是甲骨文攻击，而是“巧妙的套利执行”。

不幸的是，这种攻击只是对 DeFi 行业的一连串打击。今年 2 月，黑客还针对 ERC777 回调机制中的一个已知漏洞，该漏洞使黑客能够劫持交易并多次出售同一批代币。这些情况强调了增强安全机制和审计的必要性，以及早发现攻击并在理想情况下完全阻止攻击。

## （四）Instagram 网红“ Hushpuppi”隐藏了 1400 万美元的比特币被盗资金

联邦调查局（Federal Bureau of Investigation）认为，两名尼日利亚公民可能隐藏了他们通过网络钓鱼计划在获得的 1700 万美元中的很大一部分。据报道，这些骗子被确定为雷蒙德·阿巴斯（Raymond Abbas），他在 Instagram 上的 240 万粉丝将其称为“ Hushpuppi”，而 Olalekan Jakob Ponle 被称为“伍德伯里先生”

据称，两人伪装成两家总部位于芝加哥的公司的会计师，这是大规模网络钓鱼计划的一部分。据报道，一家公司以这种方式损失了 1520 万美元，而另一家公司的雇员向嫌疑人转移了 230 万美元。

美国伊利诺伊州北区检察官和联邦调查局芝加哥办事处的特别负责人提起的刑事诉讼说：“这些电子邮件几乎与以前通过该公司的电子邮件帐户发送的合法电子邮件相同，但是欺诈性电子邮件指示受害者将资金汇入指定的银行帐户。”

迪拜刑事调查部主任贾马尔·萨利姆·贾拉夫准将（Brigadier Jamal Salem Al Jallaf）表示，当地警察还没收了“涉嫌在全球范围内策划欺诈的文件，总价值达 16 亿迪拉姆（4.35 亿美元）。”

## （五）新西兰警方在调查 BTC-e 交易中扣押 9000 万美元

6 月 22 日，新西兰资产回收部门宣布冻结 9000 万纽币，这是对比特币交易所 BTC-e 的全球调查的一部分。警察专员安德鲁·科斯特（Andrew Coster）表示：“新西兰警方已与美国国税局紧密合作，以解决这一非常严重的罪行。”

Vinnik 被指控为网络罪犯洗钱、勒索软件诈骗、身份盗用计划、腐败的公职人员的行为、税收欺诈和贩毒集团提供便利。美国司法部表示，他臭名昭著的交易所 BTC-e 是世界上最大的交易所之一，以“高度匿名”交易了至少价值 40 亿美元的比特币。BTC-e 通过不要求用户验证其身份来促进犯罪活动，并被指控匿名交易和资金来源。

纽西兰警察局局长安德鲁·科斯特（Andrew Coster）在没收资产的话题上说：“这些资金很可能反映了全球成千上万（甚至数十万）受害人口的利益网络犯罪和有组织犯罪的结果。”

## （六）Nexus Mutual 首席执行官被窃取了超过 800 万美元的 NXM 代币

12 月 14 日，DeFi 保险公司 Nexus Mutual 的首席执行官休·卡普（Hugh Karp）在一场由项目成员发起的针对性攻击中损失了相当于 800 万美元的 NXM 代币。黑客通过完成 Nexus Mutual 的 KYC 流

程成为会员来执行攻击；后来，攻击者切换到新地址，并获得了对 Karp 计算机的远程访问权，并修改了 Karp 的 MetaMask 钱包扩展名。

幸运的是，没有其他成员受到攻击，据 Nexus Mutual 推文称："资金池和所有系统都是安全的。"但是，在攻击曝光后，Nexus Mutual 包装代币在加密货币交易所火币（Huobi）上的价格下跌了 14%。一部分被盗资金转移到 1inch.exchange，这是一个去中心化的交易聚合商。

## （七）爱尔兰人通过黑 SIM 卡窃取了 250 万美元的加密货币

11 月 17 日，来自爱尔兰都柏林的二十一岁的 Conor Freeman 因盗窃超过 200 万美元的加密货币而被判有期徒刑三年。尽管他的律师声称他是单独行动，但检方发现，弗里曼是其六人小组的成员之一，他们在 2018 年为期三天的抢劫中入侵了加密货币账户。

该组织通过社交媒体找到了受害者，获得了受害者的电子邮件地址和电话号码，并将其放在 SIM 卡上。Conor Freeman 的主要工作是浏览受害者的电子邮件以找到其加密货币帐户。被盗的 250 万美元资金是从三名受害者身上被抢走的。

爱尔兰国家警察部队最终抓获 Freeman 时，他们发现 Freeman 已经花费了超过 13 万美元的赃款，但是在被捕时，他提供了数字钱包和访问密钥，以便警察可以取回剩余的余额。

## （八）勒索软件集团（Ransomware Group）入侵了阿根廷国家移民局

据 Cointelegraph 报道，阿根廷政府官员拒绝与对其国家移民局进行勒索软件攻击的组织进行谈判。

一群 Netwalker 勒索软件黑客攻击了阿根廷的移民局 DirecciónNacional de Migraciones（DNM）。遭到黑客入侵后，DNM 收到了一张赎金通知，内容是"您的文件已加密"。该说明详细说明，解锁文件的唯一方法是以 200 万美元的价格从黑客那里购买解密程序。

当天晚些时候，勒索软件组织发布了一小部分敏感数据，以证明黑客攻击的有效性。在政府拒绝支付赎金之后，该组织将赎金增加到 400 万美元。

阿根廷新闻媒体 Infobae 报道称，当局将移民官员使用的所有计算机网络都下线，黑客入侵将所有边境口岸关闭了四个多小时。阿根廷政府官员对此作出回应，称"他们不会与黑客进行谈判，也不关心找回被盗的数据。"

## （九）斯洛伐克加密交易所 Eterbase 在热钱包黑客攻击中损失了 160 万美元

Eterbase 是斯洛伐克的一家小型加密货币交易所，在 9 月 7 日晚上被一群黑客入侵，闯入他们的热钱包并偷走了大约 160 万美元的各种加密货币。

黑客侵入 Eterbase 的系统，偷走了价值近 160 万美元的比特币、以太币、XRP、tezos、algorand 和 TRON。第二天早晨，Eterbase 从其 Telegram 频道宣布，交易所中列出的六种加密货币的热钱包已被盗。

在公告中，Eterbase 分享了黑客将资金转至的钱包地址，但在完成对攻击的调查之前，它没有透露更多细节。

## （十）Wotoken 庞氏骗局骗取投资者价值超过 10 亿美元的加密货币

5 月 14 日，在盐城市滨海县人民法院对负责组织和领导 Wotoken 传销活动的 6 家核心运营商展开审判。根据公开听证会，此庞氏骗局于 2018 年 7 月至 2019 年 10 月期间活跃，拥有 715,249 名注册用户。该计划在运营仅一年多的时间里，为 Wotoken 骗子提供了超过 77 亿元人民币（约合 10.9 亿美元）的加密货币。

您可以在我们《2020 年春季加密货币犯罪和反洗钱报告》中找到更多详细信息：https：//ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/

# 七、2020 技术入侵事件

尽管 2020 年可能还没有像前几年那样饱和，但针对区块链协议和未经审计的智能合约的较小攻击继续激增。以下是发生在 2020 年的著名黑客事件。

1．12 月 28 日，Cover Protocol 被利用。黑客将 LP(Liquidity Provider: LP, 流动性提供者代币）代币存入其 shield mining contract（盾牌挖矿合同），撤回了几乎所有代币以充实“accRewardsPerToken”，再次存入 LP 代币，然后索取覆盖奖励并欺骗了该合同制造了五百亿个代币。Grap Finance 归还了大约 300 万美元的代币，并附有一条消息。阅读我们的完整分析：https://ciphertrace.com/infinite-minting-exploit-nets-attacker-4-4m/

2．12 月 19 日，bitcoin.org 网站因 DDoS 攻击而短暂宕机。开发人员迅速开始通过 BitTorrent 共享有关 Bitcoin Core v0.20.1 的文件，以允许其他人播种该文件并使新节点保持最新状态。

3．12 月 17 日，Warp Finance 中的一个 Oracle 操作漏洞被利用，导致 WarpVaultSC 损失了大约 780 万美元的 USDC 和 DAI。攻击是通过 Uniswap 和 dYdX 进行的 1.8 亿美元的快速交换进行的，然后将其用于清空 Warp。

4．12 月 21 日，从 2020 年 6 月开始的 Ledger 数据泄露事件被转交给 RaidForum。此次入侵包括超过一百万个电子邮件地址以及超过 25 万个物理邮寄地址和电话号码，这些地址和号码现在正用于活跃的网络钓鱼活动中。

5．12 月 21 日，EXMO 提醒用户可疑的取款活动以及热钱包中近 5％的总资产受到损害。

6．11 月 27 日，对 BCHA 的攻击达到了 51％。一个名为 voluntarism.dev 的矿工暗示他们已经链接了币库规则，因此所有矿工都需要将至少 100％的区块奖励发送到 IFP 地址。更改将使整个 BCHA（ABC）链失效，直至其起源（2020 年 11 月 15 日），然后从那里重新增长。

7．11 月 21 日，Pickle Finance 的 pDAI PickleJar 被黑，造成损失 1,976 万。该损失由 COVER 赔偿。

8．11 月 18 日，在 GoDaddy 托管的针对加密货币项目的最新系列攻击之后，攻击者接管了 NiceHash 的 DNS 记录。

9．11 月 17 日，在 88mph 的项目中发现了两个漏洞，导致被利用并累积了 10 万美元的损失。幸运的是，Uniswap 的资金池中挽救了一些资金。

10．11 月 16 日，Origin Protocol 对他们的 Origin Dollar（OUSD）进行了重新进入攻击，造成大约 700 万美元的损失。攻击是通过闪贷发起的，随后进行了几次稳定币掉期和重入攻击，并伴随着赎回和进一步的代币掉期。

11．11 月 14 日，由于攻击者通过借贷平台 Aave 借入 80,000 ETH 进行的快速贷款攻击，DeFi 协议 Value DeFi 被利用，价值约 600 万美元。

12．11 月 13 日，DeFi 平台 Akropolis 通过衍生品平台 dYdX 的快速贷款再次进入攻击，遭受了大约 200 万美元的损失。这次攻击遵循了 2016 年 DAO 黑客采取的相同步骤，但增加了 DeFi 流动资金池。

13．11 月 13 日，管理 Liquid Exchange 核心域名之一的域名托管服务提供商错误地将对帐户和域的控制权转移给了恶意行为者。该错误导致参与者可以更改 DNS 记录并控制内部电子邮件帐户。

14．11 月 10 日，Monero 的前首席维护者和 Tari 的共同创始人 Riccardo Spagni（又名 fluffypony）分享了有关攻击者的信息，该攻击者通过对 Monero 的 51％攻击而大跌眼镜，试图将交易与交易的 IP 地址关联起来。广播它的节点。这种徒劳无功的努力对 Monero 的链上机制没有影响，并且被 Tor、I2P 和 Dandelion ++减轻了。

15．11 月 8 日，基于 Mimblewimble 的区块链 GRiN 遭受了 51％的攻击。该攻击最有可能使用了 NiceHash 的可租用哈希功能。事件发生时，单个攻击矿工控制了 58.1％的网络。

16．11 月 7 日，利用了 BSV 区块链中的 multisig 错误，并利用了大约 600 个 BSV 资金。该利用源自 BSV，它删除了使用最广泛的基于比特币的 multisig 脚本 Pay-to-Script-Hash（P2SH），并替换为使用错误的不等式符号的阈值。

17．8 月 29 日，ETC 遭受了 51％的攻击，导致 7,000 多个区块重组，相当于大约两天的采矿时间。

18．7 月 31 日，2together 遭受了网络攻击，其中约 120 万欧元的加密货币从用户帐户中被盗。

19．7 月 10 日，黑客尝试对 BitcoinGoldnetwork 发起 51％的攻击。攻击者从 7 月 1 日开始秘密在 Nicehash 上开采了 1300 个区块，然后秘密地为矿工提供了更新的节点软件，以在块 640650 激活，从而导致大量公共合法节点块被丢弃。攻击每小时仅花费 297 美元。

20．7 月 11 日，黑客从 Cashaa 柜台交易柜台（OTC）窃取了 336 个比特币，当时价值约 310 万美元。据该公司称，黑客能够渗透到印度东德里的 OTC 交易经理的个人计算机，从而使他的设备受到恶意软件的感染。

21．7 月 2 日，注意到有关 Tendermint v0.33.0 的 Tendermint DoS 漏洞，该漏洞将允许阻止提议者包括针对错误阻止的签名，并允许恶意验证程序终止整个网络。

22．6 月 30 日，Vether（VETH）的整个 Uniswap 池耗尽了，约 919,299（VETH）相当于 90 万美元，而价格仅为 0.9 ETH（200 美元）。

23．6 月 29 日，黑客利用 Ravencoin 漏洞，允许在通常创建的每个块 5000 RVN 之外铸造额外的（RVN）令牌。Ravencoin 认为该漏洞是有意从特定的 GitHub 帐户 WindowsCryptoDev 引入的。

24．6 月 28 日，两个 Balancer 多令牌池被利用，造成大约 50 万美元的损失。攻击者使用快速借贷来利用 Balancer 处理通货紧缩令牌的方式利用漏洞。Balancer 指出，该错误是通过他们的 Bug Bounty 程序报告给他们的，但已被消除。

25．6 月 24 日，Palo Alto Networks 发布了来自众多 CVE-2019-9081 利用事件的两种新的加密劫持和 DDoS 混合恶意软件的信息。密码劫持恶意软件 Lucifer 能够通过利用多个漏洞和凭证暴力破解来丢弃 XMRig 以便对 Monero 进行密码劫持以及命令和控制 C2 操作以及自我传播。

26．6 月 25 日，Palo Alto Networks 发布了一份有关 Docker 容器内使用密码劫持并使用 Docker Hub 分发这些图像的报告。恶意的 Docker Hub 帐户“ azurenql”托管着六个旨在开采 Monero 的恶意映像。

27．6 月 1 日，Netwalker 团伙袭击了 UCSF。UCSF 最终支付了大约 114 万美元的赎金。

28．5 月 14 日，BlockFi 遭受了数据泄露。

29．2 月 15 日，DeFi 借贷协议 bZx 被利用，使攻击者获得了 35 万美元的利润。

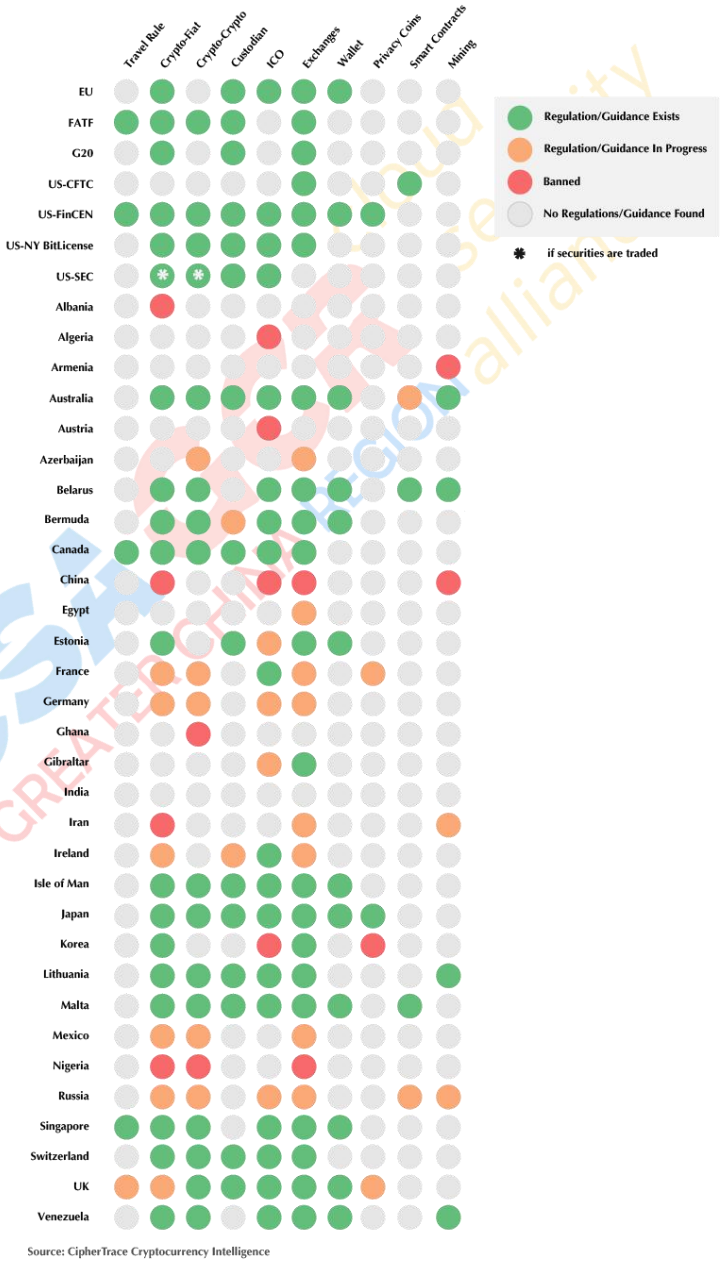
30．在 bZx 攻击之后，bZx 宣布他们将 Kyber 用作 oracle。两天后，攻击者通过 Kyber 操纵了 sUSD。bZx ETH 池损失了约 180 万美元，而 sUSD 池则损失了 110 万美元。攻击者赚了大约 64 万美元。

31．1 月 23 日，BitcoinGold 遭受了 51％的攻击。BTG 的两个深度重组组织检测到了这次攻击，其中包含双花。

# 八、全球监管环境的变化

2020 年出现了大量新的加密法规，以及针对 vasp 及其高管缺乏监管合规的全面执法行动。下表显示了全球“反洗钱”/“全面反洗钱”(CTF)制度的成熟度和复杂程度差异很大。这些法规中的空白提供了洗钱者和恐怖组织可以利用的途径。具体来说，试图根据法定货币的物理特性监管数字资产的立法者并没有很好地解决加密货币对加密货币交易所和加密货币的洗钱潜力。

## （一）当前全球反洗钱/反洗钱条例的实施情况



## （二）FATF-修订后的虚拟资产标准 12 个月审查

2020 年 6 月 24 日，金融行动工作组举行了一次虚拟会议，以审查在实施针对虚拟资产和 VASP 的新反洗钱指南方面的全球进展。FATF 报告中发布的会议细节为 VASP 和更大的加密货币社区提供了希望的前景。

审查范围突出了三个主要评估领域：新兴市场趋势和洗钱风险，公共部门对修订后标准的实施和执行，以及私营部门所开发和采用的‘旅行规则’合规机制。

根据该报告，在 54 个做出回应的 FATF 及 FSRM（FATF-Style Regional Body）成员辖区中，有 32 个辖区报告了针对虚拟资产服务提供商的现有 AML / CFT 法规，有 13 个辖区报告了正在制定法规，还有 5 个辖区表示禁止或即将禁止 VASP。

报告中关于 CipherTrace 的完整书面简介可在以下位置找到：
https : //ciphertrace.com/revised-fatf-standards-on-virtual-assets-12-month-review/

## （三）FATF-虚拟资产洗钱和恐怖融资的红旗指标

9 月 14 日，FATF 发布了有关虚拟资产红旗指标的报告。该报告旨在协助报告实体，例如银行，指定的非金融企业和专业（DNFBP）和 VASP。

虽然焦点是 VASP，但该报告的确表明银行在非法资金的进出过程中发挥的关键作用，并强调在两端对金钱规则的利用。

为了使银行遵守报告中说明的任何红旗指标，它们必须能够准确识别和监视所有与加密有关的交易。这样做将使他们能够识别红旗指标，例如：

- 客户将大量法定货币转换为 VA（Virtual Asset：虚拟资产），而没有合理的业务解释。
- 在点对点（P2P）交换网站上作为未注册/未授权 VASP 进行操作的客户，使用银行帐户来促成这些 P2P 交易。
- 客户使用链接到 VA 钱包的一张或多张信用卡和/或借记卡提取大量法定货币（crypto-to-plastic ），或用于购买从现金存款中提取的 VA 到信用卡的资金。
- 潜在的加密钱骡（money mule，是在不知不觉或自愿的情况下代表犯罪分子转移非法所得款项的人）或骗局受害者的客户。

## （四）欧盟—加密业务面临 AMLD5 法规

自 2020 年 1 月 10 日起，为了让加密交易更加透明，欧盟的第五个反洗钱指令，也称为 5AMLD 或 AMLD 5，开始生效。在一定程度上受法国恐怖袭击的推动，新指令旨在打击恐怖主义融资和洗钱活动，同时使欧洲金融监管机构更容易获得信息。该指令还包括针对虚拟资产服务提供商（VASP）的严格的新条款，例如虚拟到法定交易所和托管钱包提供商。不合规的加密服务提供商可能会面临最高 200,000 欧元的罚款。

许多欧洲加密资产企业无法满足新的监管准则。当 AMLD 5 实施时引用了大量的 KYC 和 AML 要求，现在已有多家公司因此而停止运营。不过，可以快速且经济高效地使 VASP 满足合规要求的所有技术都是现成的。

并非所有的欧洲 VASP 都在投资以更新其合规性制度以满足新的 AMLD5 要求。例如，荷兰加密衍生品平台 Deribit 宣布计划在 2020 年 2 月上旬搬去巴拿马，以避开这些规定。尽管有些人认为合规成本不会显著提高，但 Deribit 声称新法规将给大多数交易者造成太多障碍。

## （五）美国—FinCEN 发布了旨在消除无托管钱包 AML 漏洞的新建议规则

12 月 18 日，金融犯罪执法网络（FinCEN）发布了有关使用无托管钱包进行虚拟货币交易的拟议规则更改。根据拟议的规则，将要求银行和货币服务业务（MSB）验证其客户的身份及对超过 10,000 美元的 CVC 交易提交报告，并在交易对方使用无托管钱包或其他隐藏式钱包时，保持对超过 3,000 美元的 CVC 交易记录。“其他隐藏式”钱包是指不受 BSA 约束的金融机构持有的钱包，该金融机构位于被 FinCEN 认定为主要洗钱问题管辖的外国司法管辖区，例如缅甸，伊朗和朝鲜。

然而，拜登政府于 2021 年 1 月掌管了美国政府的行政部门，宣布冻结机构规则制定，其中可能包括最近提议的降低‘旅行规则’阈值的更改以及对未托管钱包的加密货币交易的新的记录和报告要求。该冻结规则只是临时的，有待拜登总统任命或指定的部门或机构负责人进行审查。

值得注意的是，在管理和预算办公室（OMB）主任的批准下，对于“财政或国家安全事项”的冻结是有例外的。目前尚不清楚是否将这些提议的加密规则包括在这一例外情况中。所有其他已在《联邦公报》中发布但尚未生效的规则变更，包括拟议规则通知（NPRM），应推迟 60 天，并开放一个新的 30 天评论期以便进行进一步评估。

## （六）美国-FinCEN，OFAC 警告 VASP，允许客户向勒索软件付款可能会违反制裁规定

10 月 1 日，美国财政部恐怖主义与金融情报办公室发布了两份咨询报告，以协助美国个人和企业打击勒索软件诈骗和攻击。

财政部的金融犯罪执法网络（FinCEN）发布了一份报告，提供了有关金融中介机构在支付中的角色信息，勒索软件趋势和类型，以及相关金融红旗指标。FinCEN 的顾问强调指出，检测和报告勒索软件支付是防范勒索软件的重要组成部分。

美国财政部外国资产控制办公室（OFAC）发出了一项报告来警告那些与勒索软件攻击的受害人打交道的公司，为勒索软件支付提供便利的潜在制裁风险。VASP 的制裁合规程序应考虑到勒索软件支付可能涉及 SDN 或被封锁的人，或被全面封锁的司法管辖区的风险。

## （七）美国— 2021 财年国防授权法案（HR6395）

12 月 11 日，美国国会向时任总统唐纳德·特朗普（Donald Trump）提交了《2021 财年国防授权法案》（NDAA），供其进行最终审批。特朗普总统于 12 月 23 日否决了该法案，但参议院于 2021 年 1 月 1 日以较大的优势在两党中推翻了特朗普的否决。

对于加密货币社区而言，最引人注目的是，今年的 NDAA 的语言扩大了“替代货币的价值”的法律定义，将虚拟货币等新兴支付方式也包括进来。

NDAA 还通过将通用术语“资金”替换为“货币，资金或替代货币的价值”来阐明转账业务和服务的定义。

为了加强财政部的金融情报、反洗钱和打击资助恐怖主义项目，该法案还确立了国家审查和监督的优先事项，增加了对国际合作的技术援助，并寻求解决与受益所有权和公司缺乏透明度有关的金融犯罪问题

## （八）美国—OCC 发布声明，允许银行为客户持有加密资产

7 月 22 日，货币审计长办公室（OCC）发表声明，批准银行为其客户持有加密资产。新的指导意见指明，包括持有数字资产在内的银行托管服务可以扩展到加密密钥和其他加密相关资产。

高级副审计长兼首席顾问乔纳森·古尔德（Jonathan Gould）写道：“我们的结论是，一家国家银行可以代表客户提供这些加密货币托管服务，包括持有与加密货币相关的唯一加密密钥。”他还重申了 OCC 的立场，即“国家银行可以向他们选择的任何合法业务提供允许的银行服务，包括加密货币业务，只要他们有效管理风险并遵守适用的法律。”

随着金融技术领域的进步，银行必须适应不断变化的形势，以提供客户所需的必要服务。根据OCC的说法，“随着金融市场变得越来越技术化，银行和其他服务提供商可能会越来越需要利用新技术和创新方式为客户提供传统服务。通过提供这些服务，银行可以继续履行其在提供支付，贷款和存款服务方面历来发挥的金融中介职能。”

## （九）美国上诉法院称，美国第四修正案不能保护比特币数据

6月30日，由第五巡回法院(Fifth Circuit court)的三名法官组成的小组裁定，美国政府的《第四修正案》不适用于犯罪行为中使用的比特币交易数据，如果这些交易数据来自虚拟货币交易所。美国法院驳回了被告理查德·格拉特科夫斯基（Richard Gratkowski）的上诉，他试图利用《第四修正案》禁止不合理搜查和没收私人财产的规定。

Gratkowski被控涉嫌向儿童色情网站付款，并通过他的Coinbase帐户将比特币支付给该网站。在调查过程中，联邦调查局（FBI）传唤了Coinbase以获取Gratkowski的交易记录。但是，Gratkowski对此案提起上诉，并表示他的比特币交易记录应该收到《第四修正案》的保护。

Haynes法官投票否决了这一上诉，他解释说：“Coinbase是一家金融机构，是一家虚拟货币交易所，为比特币用户提供了一种转移比特币的方法。Coinbase与传统银行之间的主要区别在于，Coinbase处理虚拟货币，而传统银行处理的是实体货币。”

## （十）美国司法部发布了加密货币执行框架

10月8日，美国司法部发布了加密货币执行框架。该框架分为三个部分：与加密货币相关的威胁概述，应对这些威胁作的法律和法规，当前的挑战和加密货币实施的未来战略。

该框架将非法使用加密货币分为三个主要的类别：1）直接使用加密货币进行犯罪或支持恐怖主义；2）使用加密货币来隐藏金融活动，例如逃税或经营未注册的MSB；或3）在加密货币市场内犯罪。在讨论司法部在应对这些威胁方面面临的挑战时，该框架承诺司法部将继续积极的调查和起诉那些使用加密货币进行犯罪，促成或掩盖犯罪的人员，司法部强调了这一事实“已经起诉了一些从事P2P交易的个人，罪名是从事洗钱和违反BSA。”

## （十一）英国-FCA成为英国加密资产经营活动的AML和CTF监管

2020年1月10日，英国金融行为监管局（FCA）成为反洗钱和反恐怖主义融资（AML / CTF）监管机构，负责根据修订后的《反洗钱、反恐怖主义融资和资金转移条例》对企业开展加密资产经营活动监管。该修正案是将AMLD5纳入英国国家立法的结果。根据新的法规，除了整合传统的反洗钱

要求，如进行客户尽职调查、增强的尽职调查、报告和监控之外，在英国运营的加密资产企业现在必须先向 FCA 注册，然后才能在英国国内提供服务。

## （十二）英国—FCA 向英国加密资产企业发出通知

根据金融行为监管局（FCA）的加密货币反洗钱法规，现有企业必须在 2020 年 6 月 30 日之前向 FCA 注册并申请对其业务进行优先审核。未在该日期之前申请的公司被警告可能遇到注册处理延迟的情况。任何未在 FCA 注册的公司都必须在 2021 年 1 月 10 日停止交易。

在 2020 年 1 月 10 日之后开始运营的任何新的英国加密资产企业，现在都必须在 FCA 注册后才能开展业务。

## （十三）英国-新的洗钱和恐怖主义融资国家风险评估

12 月 17 日，财政部和内政部联合发布了英国第三次洗钱和恐怖主义融资的国家风险评估（NRA）。该评估更新了先前于 2017 年发布的 NRA 调查结果。最值得注意的是，2020 年 NRA 将加密资产的洗钱和恐怖主义融资风险从“低级”提高到“中级”。评估指出，加密资产生态系统在过去三年已经经历了成熟、发展和快速扩张。然而，根据他们的分析，这种成熟性也为滥用提供了更多机会，从而导致“洗钱风险增加，犯罪分子越来越多地使用加密资产生态系统并将其纳为洗钱方法。NRA 还指出，自 2020 年 1 月起将 VASP 纳入《反洗钱条例》(MLR)将有助于随着时间的推移减轻脆弱性。

## （十四）法国-适用于所有加密货币交易的强制性 KYC 规则

12 月 8 日，法国宣布了计划对所有加密货币交易实施严格的 KYC 规则，并对加密货币之间的交易施加更严格的要求。由加密货币资助的恐怖袭击被认为是这些变化背后的主要驱动力，在 9 月逮捕了 29 名涉嫌参与加密货币恐怖注意融资的人员。这一事件促使法国财政部长 Bruno Le Maire 宣布，将提出“加强对财政资金控制”的建议。

该法令的细节表明，任何价值超过 0 欧元的加密货币交易都将通过 KYC 流程，并需要两种形式的政府身份证明。同样，所有加密货币交易所都需要注册并获得许可证后才能运营。截至目前，KYC 支票的最高限额为 1,000 欧元，仅适用于加密货币到法定货币。未能在截止日期前注册的交易所可能会面临罚款或监禁。

这些严格的规定将使法国交易所的用户入门费用从每位用户大约 1 欧元增加到大约 5 欧元。数字服务集团（Digital Service Group）首席技术官 Pierre-Guy Bareges 指出，KYC 规则的更改“是“法国所有参与者”的顾虑因为客户可能会去监管没有那么严格的外汇交易所。”

这些措施目前处于条例阶段，预计将在 2021 年初成为法令。在法国，法令在成为法律之前不需要议会批准。一旦成为法律，所有加密货币公司将有 6 个月的时间来遵从。

### （十五）韩国—新税收目标加密货币交易者

7 月 22 日，韩国政府公布了新的加密货币税收提案。根据该提案，年收入超过 2100 美元的交易者将为其收入缴纳 20%的税，这一门槛远低于对股票交易者征收的税率，后者投资 KOSDAQ 上市公司的收入不超过 42,000 美元，无需缴纳所得税。

税务机关还向可能试图通过在海外交易所交易而绕过税收措施的人发出警告。未申报的交易者将面临未披露交易的额外 20%税单。

### （十六）韩国—计划禁止使用隐私货币

11 月 3 日，韩国宣布将在 2021 年在全国范围内禁止使用隐私货币，同时对加密货币用户实施更严格的 KYC 要求。作为该国《特别支付法案》的更新，新法规将取缔被认为难以追踪的所谓“暗币”。交易所有 6 个月的时间来证明其遵守了 KYC 条款。

2019 年 9 月，OKEx 新加坡分公司和新加坡交易所 Upbit 根据对 FATF 准则的解释，将隐私币退市。2020 年 11 月，总部位于科罗拉多州的 ShapeShift 也将隐私币 Zcash，Dash 和 Monero 摘牌。

### （十七）吉尔吉斯斯坦-国家银行制定新的加密货币法律

11 月 13 日，吉尔吉斯共和国国家银行（National Bank of Kyrgyz Republic）宣布正在制定一项法律草案，该草案将赋予他们监管加密货币买卖的管辖权，以便更好地跟踪欺诈行为并保护消费者权益。

### （十八）巴基斯坦—正在创建加密框架

11 月 6 日，巴基斯坦安全与交易委员会（SECP）宣布正在努力创建该国加密货币监管框架。巴基斯坦认为采用数字货币是一个机会，可以提出一个“与世界同等的强有力的监管制度来监管数字资产。”该国希望拥有自己的中央银行。

## 九、中央银行数字货币

随着中央银行数字货币（CBDC）从试点阶段向到零售使用过渡，优先遵守 AML 和 CFT 法规将变得至关重要。正如法定货币经常跨境转移一样，我们应该预料到 CBDC 也是如此，因此也应考虑‘旅行规则’。

CBDC 对全球经济产生的最终影响尚无定论。不同国家以不同的速度发展 CBDC 导致了有关全球采用和互操作性的问题。尽管在 2020 年以下国家在 CBDC 发展方面取得了长足进步，但仍有许多国家缺乏涵盖 CBDC 的法律结构。

## （一）BIS-中央银行拒绝有关 CBDC 发行动机的热门叙述

6 月 24 日，国际清算银行（BIS）发表了一份声明，在声明中他们驳斥了这样的假设，即私营部门稳定币提案（如天秤座）刺激了中央银行数字货币（CBDC）的发行。

BIS 解释了对 CBDC 产生的新兴趣是因为认识到数字货币提供了一个可以塑造未来支付方式的渠道。该报告指出：“CBDC 的发行与其说是对加密货币和私营部门“稳定币”提案的回应，不如说是中央银行为同时实现若干公共政策目标而进行的一项集中技术努力。”

该报告为过去一年中突然增加的 CBDC 测试、招聘和研究提供了另一种解释。不管 CBDC 兴趣激增背后的原因是什么，BIS 都清楚地表明，数字货币可能是具有革命性的，并且“ CBDC 有可能成为货币演变的下一步。”

## （二）美国-OCC 表示，美国国家银行可以使用稳定币来促进支付

1 月 4 日，美国货币监察长办公室（OCC）发出了一封解释性信，允许国家银行和联邦储蓄协会使用稳定币和独立节点验证，作为美国金融系统内的结算基础设施，来参与和促进支付活动。

根据这封信件，银行现在可以通过充当独立节点验证网络（INVN）上的节点来验证，存储和记录支付交易。同样，银行可以使用 INVN 和相关的稳定币进行其他允许的支付活动。但是，任何稳定币安排“都应具有获取和验证所有交易方身份的能力，包括使用无托管钱包的交易方的身份。”

OCC 的指南是使美国银行能够通过稳定币网络提供金融服务的关键的第一步。但是，这封信件警告说，考虑从事与 INVN 相关活动的银行也必须意识到对其机构构成的潜在风险，包括运营风险，合规风险和欺诈。新技术需要足够的技术专业知识，以确保银行可以安全，合理地管理这些风险。

该解释性信还指出，尽管银行应进行尽职调查并确保评估与任何稳定比发行人的银行业务相关的 AML 及合规风险，但它们还应确保对加密货币的总体风险有所了解。

美国证券交易委员会（SEC）回应了 OCC 解释性信，指出某些稳定币可能不符合联邦法律规定的证券。根据这份声明，SEC 愿意就与某些稳定币有关的活动是否援引联邦证券法的适用行 d 提供“不采取行的动”立场。

## （三）美国-联邦储备委员会行长宣布与麻省理工合作研究数字货币

8 月 13 日，美国联邦储备委员会行长 Lael Brainard 表示，美国中央银行一直在测试数字化账本技术，以了解数字货币对现有支付生态系统，货币政策，金融稳定性和银行业的影响。Brainard 说：“考虑到这些重要问题，美联储积极开展与分布式账本技术和数字货币潜在用例有关的研究和实验。”

Brainard 解释说，COVID-19 大流行加剧了对“立即且可信地使用资金”的需求。她观察到 COVID-19 刺激资金的接受者很快就花了他们，这表明了需求的紧急程度。

Brainard 说：“为了增强美联储对数字货币的理解，波士顿联邦储备银行正在与麻省理工学院的研究人员合作，以期通过多年的努力来建立和测试一种针对中央银行用途的虚拟数字货币。”

Brainard 在讲话中提到，其他 CBDC 和私人加密货币的兴起凸显了美国必须认真追求数字货币解决方案的必要性。Brainard 认为，鉴于美元在全球经济中的作用，美国政府需要“保持研究和政策制定的前沿”。

## （四）巴哈马群岛-沙币被零售使用

10 月 20 日，巴哈马正式成为第一个推出央行数字货币（CBDC）的国家。该国近 40 万居民可以通过手机将“沙币”转移到央行批准的电子钱包中，商家也可以接受。。

到 12 月，巴哈马沙币已开始零售使用，这是世界上第一个在试点项目之外的中央银行数字货币（CBDC）。一家保健食品咖啡馆是最早接受用沙币支付的机构之一；目前有 130,000 沙币在流通。

那第一笔交易是什么物品呢？据路透社报道，是一杯绿色奶昔和一个鲷鱼汉堡。

## （五）中国—央行数字货币向前迈进了一大步

10 月 12 日，中国人民银行副行长范一飞宣布了数字人民币试点的结果。他分享说：“银行开设了 113,300 个消费者数字钱包和 8,859 个企业数字钱包。”最令人印象深刻的是，“在 4 月至 8 月的试点启动和结束期间，数字钱包处理了 310 万笔数字人民币交易，共计 11 亿元人民币（1.62 亿美元）”。这些数字使数字人民币成为商业环境中最常用的 CBDC。

## （六）瑞典-进入 CBDC 发展的下一个阶段

2020 年 2 月，瑞典宣布启动其 CBDC，即 e- krona 的测试阶段，该阶段由瑞典国家银行 Riksbank 和 Accenture 使用区块链技术开发。将近一年之后，现在它已进入下一阶段，由瑞典银行财务委员会前主席 Anna Kinberg Batra 领导进行可行性审查。预计审查将于 2021 年 11 月左右完成。

尽管瑞典央行行长 Stefan Ingves 对向发行数字货币的过渡充满激情，但他仍然需要说服瑞典议会将此举动成为永久性的。这应该不太困难，因为瑞典在 2018 年被国际清算银行（Bank of International Settlements）评为全球最无现金的地区。尽管如此，但仍有一些人担心老年人和农村地区仍依赖现金进行基本交易的人会被这一转变抛在后面。

## （七）澳大利亚-CBDC 竞赛升温

11 月 1 日，澳大利亚储备银行宣布了有意探索一种中央银行数字货币。储备银行正在与联邦银行，澳大利亚国民银行，Perpetual 和 ConsenSys Software 合作开展该项目。

## （八）巴西-中央银行行长视 CBDC 为金融的未来

9 月 2 日，巴西中央银行行长 Roberto Campos Neto 表示，巴西可能准备最早于 2022 年发行中央银行数字货币。

Neto 说："要拥有数字货币，您需要一个高效且可互操作的即时支付系统；一个开放的系统，您可以在其中创建竞争； 一种具有信誉的，可兑换的和国际化的货币。"

中央银行于 2020 年 11 月试行推出即时支付系统 PIX。预计巴西议会将在本月底前就该国汇率制度现代化的提案进行投票。

巴西的 CBDC 工作组正在研究一种国家数字货币的潜在影响，并将在 6 到 12 个月后公布其研究成果。

## （九）私营部门—花旗集团与世界各国政府合作建立 CBDC

彭博社在 2020 年 12 月的一次活动上引用花旗集团首席执行官 Michael Corbat 的话称，花旗集团正在与世界各地的政府合作，协助他们建立自己的 CBDC。尽管 Corbat 没有提及该公司正在与哪些特定政府合作，但他确实表示他们正在致力于这些 CBDC 的开发和商业化。

就在三年前，Corbat 预测政府将推出 CBDC 计划来应对比特币。自 2014 年以来，他所在的花旗银行一直在研究加密货币。

花旗集团是最新加入 CBDC 开发的私营金融部门，因为 Visa 和万事达卡也推出了 CBDC 计划。正如 Corbat 在彭博盛活动上所说，CBDC 是未来货币是“不可避免的”发展趋势。

### （十）IOSCO-全球稳定币可能受证券监管

3 月 23 日，国际证监会组织（IOSCO）董事会发布了《全球稳定币计划》（Global Stablecoin Initiatives）-一份研究全球稳定币举措对证券市场监管机构可能产生的影响以及现有 IOSCO 原则和标准如何适用的报告。该报告采用了一个稳定币的假设案例研究，该稳定币集将通过储备基金和治理委员会用于国内和跨境支付。该报告的结论是，根据其结构，全球稳定币可以而且很可能属于证券市场监管框架之内。

## 十、被美国制裁的国家或者个人的加密货币情况

### （一）俄国

#### 1. 俄罗斯法院裁定盗窃比特币不是犯罪

6 月 30 日，俄罗斯法院驳回了一项要求对绑架和比特币盗窃受害人进行赔偿的动议。法官裁定，这起盗窃不属于重罪，因为虚拟货币比特币不享有与实物资产相同的财产保护。

该案要追溯到 2018 年，当时两名男子冒充联邦安全局（FSB）特工绑架了受害者，并强迫他交出 500 万卢布（约合 9 万美元）的现金和 99.7 BTC-当时价值约 90 万美元。绑架者分别被判处八年和十年监禁。

作为刑事诉讼的一部分，受害人要求法院裁定迫使窃贼偿还从他那里偷走的资金。法院做出了部分有利于受害人的裁决，要求窃贼必须偿还现金。但是当涉及到加密货币时，法院宣布它无法满足索赔要求，因为虚拟货币没有被俄罗斯法律上认可为法定货币或替代货币。

#### 2. 新的 Russian 加密相关指示

9 月 10 日，四人因试图影响美国选举进程而被添加到 OFAC 的 SDN 名单。其中被选定的三人与与支持互联网研究机构（IRA）的加密货币帐户有关联，IRA 是俄罗斯的“巨魔农场”，与代表俄罗斯政治利益影响国外运作有关。根据 OFAC 的说法，“ IRA 使用加密货币为其在世界各地持续进行恶意影响活动提供资金。”这些指定对象包括 BTC，LTC，ZEC 和 BSV 地址。

9 月 16 日，两名俄罗斯公民被列入 OFAC 的 SDN 名单，原因是他们参与了一场复杂的网络钓鱼活动，该活动在 2017 年和 2018 年的目标分别是两家美国虚拟资产服务提供商（VASP）的客户和一家外国虚拟资产服务提供商（VASP）的客户。这场攻击导致的损失合计至少为 1,680 万美元。选定对象包括 Bitcoin, Bitcoin Gold, Litecoin, Ethereum, Ethereum Classic, DASH and ZCash 虚拟货币地址和一个 Monero 支付 ID。这是 OFAC 首次在其称号中列出 Monero（XMR）。

为了实施其计划，欺诈者之一 Potekhin 欺骗了许多合法虚拟货币交易所的网站，以收集用户的登录凭据并获得对其真实帐户的访问权限。根据 OFAC 的说法，两人采取了多种方法将合法资金从用户帐户中移出，包括创建带有伪造或被盗 ID 的交易所帐户；交换到不同的虚拟货币，例如 Monero；以及通过多个中间地址移动虚拟货币。

一旦他们获得了资金，第二个欺诈者 Karasavidi 就将所有攻击收益洗劫到了他的名字下。尽管试图通过通过多个账户和多个虚拟货币区块链对存款进行分层来掩盖资金的真实性质，但区块链分析仍然能够将被盗资金追踪到他的账户。美国特勤局没收了 Karasavidi 帐户中的数百万美元虚拟货币和美元。

## （二）伊朗

### 在经济不景气的情况下，伊朗修订法规，允许以加密货币资助的进口商品

10 月 25 日，《伊朗日报》报道说，伊朗政府已修改了先前颁布的加密货币法规，以允许合法开采的加密货币在用于资助从其他国家进口时可以互换。CoinDesk 对此消息的报道表明，做出此修正是为了满足该国需要大量国际货币以帮助其经济的需求。

《伊朗日报》援引 IRNA 的报告说："矿工应该在[伊朗中央银行]引入的渠道的授权限制内直接提供原始加密货币。"《伊朗日报》建议："使用加密货币为进口提供资金可能有助于 CBI 逃避美国对伊朗使用美元体系施加的限制。"

## （三）北朝鲜

### 1. 据美国陆军备忘录，有 6,000 多名朝鲜黑客为自己的国家服务

2020 年 7 月，美国陆军发表了一份关于朝鲜战术的报告，其中揭示了有关隐士王国臭名昭著的由政府批准的黑客网络的信息。根据该报告，朝鲜在世界上有 6,000 多个黑客，其中包括白俄罗斯，中国，印度，马来西亚和俄罗斯。

该报告建议该小组受朝鲜网络战指导单位 121 局的监督。人们认为，黑客通常不会直接从朝鲜发起网络攻击，因为该国缺乏实现这一目标所必需的 IT 基础架构。

朝鲜黑客已经对金融机构和国际业务进行了多次备受瞩目的黑客攻击。臭名昭著的拉撒路集团（Lazarus Group）已成功从数个加密货币交易所盗窃了数百万美元，在网络上释放了 WannaCry 勒索软件，并闯入了 Sony Pictures，并泄漏了未发行的内容和其他私人信息。根据美国陆军的备忘录，该组织的任务是“通过武器化敌方网络漏洞并在政权指示下提供有效载荷来制造社会混乱”。人们还认为，在将资金转换为现金时，黑客使用隐私币来掩盖自己的踪迹。该报告表明，需要继续开发通过隐私币追踪非法资金流的方法。

## 2. 两个人被 OFAC SDN 列入名单，并被美国司法部指控为洗钱 1 亿美元被朝鲜盗用的加密货币

3 月 2 日，美国财政部外国资产控制办公室（OFAC）将两个人列入特别指定国民名单（SDN），以表彰他们在洗钱 2018 年交易所黑客入侵的加密货币中的作用。据称，这两家人分别是田寅音和李家栋，与拉撒路集团有关。拉撒路集团是朝鲜政府资助的网络犯罪分子，被认为是索尼漏洞和 WannaCry 恶意软件攻击的幕后推手，并从银行和加密货币交易所盗窃了 20 亿美元。

根据美国财政部的新闻稿，Tian 和 Li 从朝鲜控制账户收到了价值约 1.005 亿美元的被盗加密货币。田最终通过与他的加密货币兑换账户相关联的银行账户最终转移了价值超过 3400 万美元的这些非法资金。李还通过 9 家不同银行的关联账户又转移了 3300 万美元。

由于这些制裁，所有在美国境内或由美国个人和实体拥有或控制的田和李所有财产必须被封锁并报告给 OFAC。此外，与 Tian 或 Li 进行交易或与他们的受制裁地址进行交易的人可能会因违反制裁而受到惩罚或被列入 SDN 名单。

同时，美国哥伦比亚特区检察官针对与盗窃和洗钱过程相关的 113 个虚拟货币帐户，在雷姆（Rem）提出了“没收已验证的投诉”。司法部刑事司助理检察长本奇科夫斯基说：“今天的行动表明，国防部将揭开加密货币提供的匿名面纱，以追究罪犯，无论他们身在何处。”

尽管虚拟货币地址所有者的身份是匿名的，但这些制裁表明，执法部门可以通过应用高级区块链分析（例如 CipherTrace 加密货币智能）来识别特定加密货币地址的所有者。使用具有高质量归因的准确工具，不仅可以揭示由同一个人或实体控制的其他地址，而且可以确保金融机构或其客户不与受制裁实体进行交易。Tian 和 Li 使用与他们的加密货币交换帐户关联的银行帐户的行为也证明了银行能够检测其支付网络中与加密货币相关的交易的重要性。

在此处阅读我们的完整分析：

https：//ciphertrace.com/chinese-linked-dprk-laundering-analysis/

## （四）委内瑞拉

### 美国指责委内瑞拉总统使用加密技术掩盖非法毒品交易

3 月 26 日，司法部起诉委内瑞拉总统尼古拉斯·马杜罗（NicolásMaduro）和其他 14 名官员，他们操纵了一个由毒贩，哥伦比亚革命者和毒品恐怖主义组织的毒品团伙。在相关的新闻稿中，国土安全调查局（HSI）指控密谋者使用加密货币来掩饰其罪行。

在一次新闻发布会上，时任美国总检察长威廉·巴尔（William Barr）以及毒品执法管理局局长以及曼哈顿和迈阿密的最高联邦检察官一起，指控马杜罗（Maduro）与哥伦比亚革命武装力量（FARC）反叛派别共谋小组“用可卡因淹没美国”和“摧毁美国社区”。

恒生指数代理执行副总监艾丽莎·D·埃里希斯（Alysa D. Erichs 解释说：“今天的公告凸显了 HSI 在全球范围内的决心和决心，积极识别，瞄准和调查违反美国法律，利用金融系统并躲藏在加密货币背后的个人，以进一步开展非法犯罪活动。”“让这一起诉提醒人们，没有人超越法律，包括权利很大的政治官员。”