



“头号玩家”

—— 美国技术霸权下的全球虚拟货币资产收割行动深层解析

“头号玩家”——美国技术霸权下的全球虚拟货币资产收割行动深层解析

〔内容摘要：在数字时代，区块链、虚拟货币、虚拟现实等被技术狂热分子视为构建所谓“赛博乌托邦”的关键核心要素。尤其是虚拟货币，在多方追捧下，已经对国际金融体系和货币体系构成了系统性和结构性影响。然而，因其技术特性与监管空白，也成为国际网络犯罪活动的重灾区和国际金融霸权收割的新场域。美国凭借先发技术优势、产业聚集优势、完善法规体系与强大执法能力，构建“技术优势—法规绑定—机构执行”的三位一体体系，以虚拟资产领域为重要抓手，通过网络攻击、规则围堵、欲擒故纵、定向收割、远洋捕捞等手段，实施精准化、规模化的数字掠夺，严重侵害全球各国技术主权、经济利益与政治安全。本报告结合陈志案、赵长鹏案等典型案例，从区块链技术背景与安全风险切入，系统剖析美国利用技术霸权收割全球虚拟货币资产的过程逻辑、技术细节，深入解构其国家级网络攻击手段与深层政治动机，为全球各国应对数字霸权威胁提供参考。〕

一、从“洗钱工具”到“数字黄金”

区块链技术以去中心化、分布式账本、加密验证为核心特征，打破了传统中心化机构对数据与价值流转的垄断，催生了

比特币、以太币等虚拟货币及各类虚拟资产，对传统的基于主权背书和中心化的国际金融体系和货币体系造成了现实冲击。据著名虚拟货币跟踪调查机构 CoinGecko 的统计数据，截至 2026 年 1 月底，全球虚拟货币资产总市值约为 2.73 万亿美元，其中比特币总市值达到约 1.57 万亿美元。而同期，各国央行的黄金储备价值约为 5.83 万亿美元，这意味着虚拟货币资产市值已达到全球官方黄金储备总市值的 47% 左右，已经接近一半，成为不可忽视的新型金融资产，甚至已有少数国家将比特币列为法定货币。

与此同时，虚拟货币的迅猛发展和价格的剧烈波动，也引发了全球各国政府的高度关注，全球各国的虚拟货币政策也在不断调整变化，并受到国际政治经济局势的影响。以美国政府为例，美国政府对虚拟货币的政策演变经历了从初期忽略到逐步监管，再到 2025 年全面立法的过程。早期政策主要通过监管机构发布并指导执法行动，焦点在反洗钱、反欺诈、税收和证券分类上。尤其是反洗钱方面，重点针对使用虚拟货币作为“洗钱工具”逃避金融和经济制裁的行为进行严厉执法。2022 年后随着市场波动和政治局势变化，政策转向更加积极的监管创新，尤其是在特朗普第二任期，美国政府对虚拟货币的监管体系和政策进行了重大调整。2025 年 3 月 6 日，美国政府发布行政令宣布将建立比特币战略储备。在介绍比特币时，白宫

极尽溢美之词，声称“比特币从未被黑客攻破”，并将比特币称为“数字黄金”。

虽然美国并非唯一在虚拟货币政策上采取积极态度的国家，但是美国作为以美元为核心的传统金融霸权体系的主要维护者，其在虚拟货币相关治理政策上的突然“加速”，背后的深层逻辑值得仔细揣摩。

二、“头号玩家”的“上帝视角”

众所周知，无论美国政府执政党如何更迭，美国霸权主义和强权政治的本质都不会变化。政治军事霸权、经济金融霸权和科技文化霸权是美国霸权主义的三大支柱，而“货币霸权”和“技术霸权”又在其中发挥着基础性要素作用。显然，区块链与虚拟货币的技术特性，与美国的“货币霸权”和“技术霸权”诉求高度契合，美国自然而然地成为国际虚拟货币这场大型“赌局”的“头号玩家”，并且长期霸占“庄家”席位。美国政府在这场赌局中利用“上帝视角”实现“庄家通吃”的具体路径包括：

（一）垄断技术

美国凭借在区块链底层技术、人工智能、网络攻防、大数据分析等领域的先发优势，构建起层层递进的技术垄断壁垒。在虚拟货币资产领域，美国掌控着全球主流区块链协议的核心

研发权、关键节点控制权及链上数据分析技术优势，头部区块链企业（如 Chainalysis、Elliptic）均由美国主导，占据全球链上溯源市场 90% 以上的份额。同时，美国通过“小院高墙”策略限制高端技术外流，将加密资产核心技术纳入军民融合体系，禁止向特定国家出口区块链安全技术与工具，从源头遏制其他国家数字技术自主创新能力。

（二）拉帮结派

美国将技术霸权与地缘政治目标深度绑定，以虚拟货币资产监管、网络安全为借口，干涉他国内政，打压战略竞争对手。通过将虚拟货币资产交易与“反洗钱”“反恐融资”“制裁合规”等政治议题挂钩，美国构建起全球范围的数字资产监管同盟，对不服从其规则的国家实施技术封锁与金融制裁。同时，利用国家级网络攻击力量窃取他国政治与经济敏感数据，通过数字认知战塑造有利于自身的国际叙事，维护其全球政治主导地位。

（三）强取豪夺

虚拟货币资产作为数字时代的新型财富载体，已成为美国经济收割的重要目标。美国利用技术优势与规则制定权，并在盟友国家的配合下，将全球虚拟货币资产交易纳入自身监管与基于长臂管辖的跨境执法体系，通过民事没收、刑事追责、罚

款追缴等方式，大规模侵占境外虚拟货币资产。据不完全统计，2022-2025年，美国通过各类案件累计没收全球虚拟货币资产价值超300亿美元，其中仅陈志案单案没收资产规模就达150亿美元，占比达50%。这种单方面收割行为不仅破坏他国的执法活动，导致受害者的二次损失，还干扰了虚拟货币资产全球流动，破坏新兴市场国家金融稳定，最终目的则是巩固美元在数字金融领域的霸权地位。

（四）法规绑定

美国通过炮制系列政策法规将加密货币生态与美元体系深度绑定，使其成为美元霸权的“链上延伸”，并为美国国债提供新需求，试图建立数字经济的布雷顿森林体系，将美元霸权的铸币税特权延伸至区块链领域，构建“数字美元霸权2.0”。2025年，《GENIUS法案》（Guiding and Establishing National Innovation for U.S. Stablecoins Act，全称《指导与建立美国稳定币国家创新法案》，俗称《天才法案》），要求稳定币发行商将80%以上储备资产购买美国国债。这相当于为美债市场创造了一个强制性的、持续的需求来源。一方面转嫁其债务压力，另一方面收割全球虚拟货币资产。

三、“黑吃黑”与“长臂管辖”

陈志案与赵长鹏案是美国运用技术霸权收割全球虚拟资

产的两大典型样本。两起案件完整呈现了美国“技术突破—法规配套—机构执行”的收割闭环，其过程逻辑与技术细节具有鲜明的霸权主义特征。**Garantex** 案则是美国将虚拟资产监管武器化、实施长臂管辖以实现地缘政治目标的又一典型样本。该案例凸显美国如何利用法规与制裁机制相结合，构建跨国管制枷锁，对外国交易所实施精准打击。

（一）陈志案：网络攻击支撑下的“黑吃黑”式资产收割范本

2025年10月，美国纽约东区联邦检察官办公室宣布对柬埔寨太子集团创始人陈志发起刑事指控，罪名涉及电信网络诈骗、洗钱等，同时高调宣布没收其控制的约12.7万枚比特币，按当时市场价格计算价值约150亿美元，创下美国司法部门历史上最大规模的虚拟资产没收纪录。美国司法部以“打击跨国电诈洗钱”为名义，临时拼凑所谓证据，回避最初来源，将2020年通过国家级黑客手段窃取的太子集团比特币“合法化”没收，是美国利用技术漏洞实施跨境资产掠夺、施加技术霸凌的典型“黑吃黑”案例。国家计算机病毒应急处理中心2025年11月发布的《**LuBian** 矿池遭黑客攻击被窃取巨额比特币事件技术溯源分析报告》，已通过技术实证揭露这一核心真相，即：美国国家级黑客组织通过底层加密漏洞实现精准破解，攻击**LuBian** 矿池冷钱包并转移资产，展现了美国成熟的国家级

虚拟货币资产窃取技术能力。这显然与美国政府关于“比特币从未被黑客攻破”的说法大相径庭，或者其真实含义是“比特币从未被美国政府以外的黑客攻破”。

（二）赵长鹏案：法规绑定与技术监控下的平台合规追责

2023年至2025年，美国针对国际著名虚拟货币交易所“币安”及其创始人赵长鹏发起“民事+刑事”双重追责，最终以币安支付43.5亿美元罚款（含27亿美元非法所得追缴、13.5亿美元民事罚款、1.5亿美元个人罚款）、赵长鹏签署认罪协议后被特赦告终。该案是美国利用司法霸权与技术监控手段，逼迫全球虚拟资产平台服从其监管规则、实现经济收割与规则输出的另一典型案例。

美国在案件调查过程中，运用了全方位的技术监控手段，实现对币安运营数据、用户数据、交易数据的全面渗透与取证，展现了其在数字资产平台监控领域的技术优势。

一是跨境数据窃取与内部信息获取。美国通过黑客技术渗透币安内部服务器，获取了核心运营数据与高管通讯记录，证实币安高管明知美国监管规则，却故意规避合规要求。例如，获取的内部沟通记录显示，赵长鹏指示员工使用 Signal 等加密通讯工具销毁证据，将内部数据库中的“U.S.”标签替换为“UNKWN”以掩盖美国用户存在，甚至发布“VPN使用指

南”指导美国用户规避 IP 封锁。二是交易数据全量监控与分析。通过接入全球区块链节点、与链上数据分析企业合作，美国实现对币安平台交易数据的实时监控，精准定位美国用户交易行为、受制裁地区资金流向。数据显示，币安美国用户曾占比近 20%，但仅 30%-40%的用户完成 KYC（Know Your Customer,即：实名认证机制）验证，存在“2 BTC 提现限额无需 KYC”的漏洞，这些数据均被美国作为核心违规证据。三是合规漏洞技术溯源。美国技术团队针对币安的 KYC 系统、反洗钱监控系统进行渗透测试，发现其合规机制存在系统性缺陷，如 IP 封锁仅为弹窗提示、子账户可绕过 KYC 审核等，进而论证币安“故意维持无效合规程序”的指控。

该案执法逻辑呈现鲜明的“规则预设—技术取证—罚款收割”特征，即：美国先通过国内法规将全球虚拟资产平台纳入长臂管辖的监管范围，再利用技术手段固定平台违规证据，最终以巨额罚款实现经济收割，同时强制平台接受美国的合规改造，强化美在虚拟货币资产领域的规则主导权。

（三）Garantex 案：“全政府协同+长臂管辖”手段控制数字资产生态链

美国将打击加密货币作为地缘政治博弈工具箱选项。美认为 Garantex 等加密货币平台为受制裁国家提供了规避制裁的

资金通道。美国通过行政制裁、司法追责、技术封堵与国际协作的多维联动，系统性切割其与全球金融体系的连接。

2025年，美国财政部外国资产控制办公室（OFAC）将Garantex及其关联实体列入SDN（特别指定国民清单）名单，强制稳定币发行商Tether冻结其钱包资产，利用美元清算霸权直接瘫痪其流动性；继而司法部起诉高管并通过国际抓捕（如印度逮捕联合创始人）瓦解运营团队，同时查封域名与服务器，从物理层面摧毁其基础设施。此外，美国还利用技术手段识别其规避手法——当Garantex试图通过更名Grinex或发行卢布稳定币A7A5转移资产时，OFAC立即扩展制裁范围，将替代通道一并纳入打击网络。此举凸显美国以“数字痕迹”和“金融触点”为管辖权连接点，通过链上追踪与传统司法程序结合，将国内法域外适用，实现对其数字资产生态的全链条绞杀。

美国在Garantex案中采取如此强硬的手段，正是其维护金融霸权、打击地缘政治对手、以及控制新兴数字领域的战略需求相互交织的结果。

上述典型案例虽攻击对象、执法手段不同，但本质上遵循统一的数字收割逻辑，即：以技术优势为核心支撑，以法规规则为绑定工具，以专门机构为执行载体，形成“技术破局—法规确权—机构收割”的闭环体系。技术层面，依托链上溯源、数据监控、漏洞利用等核心技术，实现对全球虚拟资产的精准

定位与证据固定；法规层面，通过本土法规长臂管辖、民事没收等制度创新，突破国界限制实现管辖扩张；机构层面，构建跨部门、跨盟友的协同执法网络，确保收割行动落地。在整个过程中，对于大量诈骗受害者而言，相当于螳螂捕蝉，黄雀在后，美方放纵电信诈骗，通过技术霸权攫取的巨额收益的大部分并没有返还受害人，事实上构成了对他国财产的间接掠夺。实际上，这种模式不仅适用于虚拟货币资产领域，也是美国运用技术霸权长期侵害全球利益的通用范式。显然，陈志、赵长鹏和 **Garantex** 等相关案例的成功实践也给予了美国政府全面掌控全球虚拟货币市场的充足信心，也成为美国政府建立以比特币为代表的虚拟货币资产国家战略储备的重要推动因素。

四、美国技术霸权的全域扩张及深层动机

众所周知，作为名副其实的“黑客帝国”，美国拥有全球最庞大的国家级黑客力量，2023年至2025年，具有美国政府支持背景的黑客组织针对全球20余家主流虚拟货币资产交易所发起定向攻击，攻击手段包括植入后门、鱼叉钓鱼、供应链渗透等，重点窃取用户钱包私钥、平台交易流水及合规监管信息，攻击目标覆盖亚洲、欧洲、非洲多个国家和地区的平台。从时间线比对来看，部分攻击行动与美国司法部、OFAC等部门针对虚拟资产领域的执法行动存在关联性。

美国通过技术霸权收割全球虚拟资产，本质是为了维护其

经济霸权与美元地位。一方面，通过没收、罚款等方式直接掠夺全球财富，补充国内经济实力；另一方面，通过掌控虚拟资产监管规则与交易流向，将数字金融体系纳入美元主导的全球金融框架，遏制其他国家通过虚拟货币资产绕开美元结算的尝试。对于非法攫取的比特币，美国政府通过公开拍卖来变现资产，获利巨大。仅对 2013 年美国联邦调查局（FBI）关闭暗网交易平台“丝绸之路”一案收缴的比特币，从 2014 年至 2025 年 1 月历时 10 多年陆续拍卖完毕，收益就超过了 100 亿美元。根据美国国内《资产没收激励计划》（Equitable Sharing Program），其部分收入成为执法部门的“红利”，而大部分则纳入联邦财政收入。美国财政部数据显示，通过虚拟资产领域的执法行动，每年可增加数百亿美元的财政收入，同时强化了全球虚拟货币资产交易对美元的依赖，进一步巩固了美元的国际货币地位。而且，事实上拍卖变现的比特币只是其强取豪夺来的九牛一毛，更多的成为战略比特币储备。特朗普政府将“司法罚没”重新定义为“零成本构建国家战略资产”，这不仅是财政操作，更是对美元霸权危机的回应，企图通过掌控“数字黄金”来对冲全球去美元化趋势。

同时必须强调的是，虚拟资产领域的数字收割，仅是美国技术霸权全域扩张的一个缩影。依托全球最庞大的网络武器库、最专业的国家级黑客组织、最完善的高科技产业供应链和生态

链，美国已经将技术霸权延伸至关键基础设施、科研领域、政治领域等各个层面，通过国家级网络攻击、技术标准武器化、数字认知战等手段，服务于其全球政治与经济利益扩张目标，维护全球霸权。而必须进一步指出的是，美国霸权的真正深层动机则是维持美国“科技—政治—军工复合体”的深度运作，并充分体现了资本增值与权力扩张的双重诉求。

美国“科技—政治—军工复合体”以硅谷科技巨头、政治贵族、华尔街金融寡头为核心，通过政治献金、秘密国防预算、政商旋转门等机制，形成利益互锁的权力网络。美国利用技术霸权开展数字收割与网络攻击，本质是为了维护这一复合体的利益循环。科技巨头通过为政治贵族控制的政府提供技术支持（如链上分析、网络攻击工具），获取巨额政府合同、税收优惠与监管松绑；政治贵族则通过科技巨头的技术能力推进霸权战略，同时回馈科技资本利益；华尔街寡头资本则通过游说政客推动出台单边主义的虚拟货币资产监管政策、收割被制裁资产，实现资本增值。这种利益循环使得技术霸权扩张成为“科技—政治—军工复合体”的内在诉求，推动美国不断强化数字收割与网络攻击能力，维护自身特权地位。

五、总结

本文系统性揭示了美国政府以技术霸权为依托，以金融创新为掩护，以虚拟货币资产为载体，以维系和升级美元霸权体

系为目标，以继续收割全世界为根本目的的险恶图谋。对于虚拟货币，中国人民银行明确指出，虚拟货币不具有与法定货币等同的法律地位，不具有法偿性，不应且不能作为货币在市场上流通使用，虚拟货币相关业务活动属于非法金融活动。即使是所谓与法定货币进行锚定的“稳定币”，国际金融组织和中央银行等金融管理部门也普遍持审慎态度，仍然存在较高的金融风险。我们也在呼吁全球虚拟货币资产的持有者应谨慎评估所持有虚拟资产的安全性。在强大的美国国家机器面前，所谓的“数字黄金”随时可能被“隔空取物”。

国家计算机病毒应急处理中心
计算机病毒防治技术国家工程实验室

360 数字安全集团

安天科技集团股份有限公司

2026 年 2 月 26 日