



Top Player :

Analysis of Global Virtual Currency Assets Extortion under the U.S. Technological Hegemony

National Computer Virus Emergency Response Center
National Engineering Laboratory for Computer Virus Prevention Technology
360 Digital Security Group
Antiy Labs

Feb 26th, 2026

Executive summary

In the digital era, blockchain, virtual currencies, and virtual reality are regarded by tech enthusiasts as key elements in constructing so-called "cyber utopias". Particularly, virtual currencies, driven by widespread adoption, have exerted systemic and structural influence on the international financial and monetary systems. However, due to their technical characteristics and regulatory gaps, they have also become a hotspot for international cybercrime and a new arena for global financial hegemony. Leveraging its technological advantages, industrial clustering, robust legal frameworks, and strong law enforcement capabilities, the United States has established a triangular system of "Technological superiority — Regulation blockade — Enforcement actions". Using virtual assets as a key lever, the U.S. employs tactics such as cyberattacks, rule-based containment, feigned retreats, targeted and long-range harvesting to conduct precise and large-scale digital plundering, severely infringing on the technological sovereignty, economic interests, and political security of nations worldwide. This report examines typical cases like the Chen Zhi and Zhao Changpeng cases, analyzing the technological background and security risks of blockchain. It systematically decodes the logic and technical details behind the U.S.'s use of technological hegemony to harvest global virtual currency assets, while deeply dissecting its state-sponsored cyberattack methods and underlying political motives, providing insights for nations to counter digital hegemony threats.

I. From "Money Laundering Tools" to "Digital Gold"

Blockchain technology, characterized by decentralization, distributed ledgers, and cryptographic verification, has shattered the monopoly of traditional centralized institutions over data and value circulation. This has spawned virtual currencies like Bitcoin and ETH, along with various virtual assets, posing a tangible challenge to the traditional international financial and monetary systems based on sovereign endorsement and centralization. According to statistics from CoinGecko, a renowned digital currency tracking agency, as of January 2026, the total market value of global digital currency assets reached approximately \$2.73 trillion, with Bitcoin accounting for about \$1.57 trillion. During the same period, central banks' gold reserves

stood at around \$5.83 trillion. This indicates that the market value of virtual currency assets has already reached approximately 47% of the total value of global official gold reserves—nearly half—making them a significant new financial asset. Some countries have even listed Bitcoin as legal tender.

Meanwhile, the rapid development and dramatic price fluctuations of virtual currencies have drawn significant attention from governments worldwide. Virtual currency policies across nations are continuously evolving, influenced by global political and economic landscapes. Taking the U.S. government as an example, its policy evolution toward virtual currencies has progressed from initial neglect to gradual regulation, culminating in comprehensive legislation by 2025. Early policies primarily relied on regulatory agencies issuing guidelines and directing enforcement actions, focusing on anti-money laundering, fraud prevention, taxation, and securities classification. Particularly in anti-money laundering efforts, stringent enforcement targeted the use of virtual currencies as "money laundering tools" to evade financial and economic sanctions. After 2022, amid market volatility and shifting political climates, policies shifted toward more proactive regulatory innovations. Notably during Trump's second term, the U.S. government implemented major adjustments to its virtual currency regulatory system and policies. On March 6, 2025, the U.S. government issued an executive order announcing the establishment of a Bitcoin Strategic Reserve. In its introduction to Bitcoin, the White House lavished praise, claiming "Bitcoin protocol has never been hacked" and referring to it as "digital gold".

While the United States is not the only country adopting an active stance on virtual currencies, its sudden 'acceleration' in virtual currency governance policies, as a key defender of the traditional financial hegemony centered on the US dollar, reveals underlying logic that warrants careful examination.

II. The "God's Eye View" of The " Top Player"

As is widely recognized, regardless of changes in the ruling party of the U.S. government, the essence of U.S. hegemony and power politics remains unchanged. Political-military hegemony, economic-financial hegemony, and technological-cultural hegemony form the three pillars of American hegemony, with "monetary hegemony" and "technological hegemony" serving as foundational elements. Clearly, the technical characteristics of blockchain and virtual currencies align perfectly with America's aspirations for "monetary hegemony" and "technological hegemony." Consequently, the U.S. has naturally become the "top player" in the international virtual currency "bet" maintaining its position as the "banker" for the long term. The specific pathways through which the U.S. government leverages its "God's eye view" to achieve "banker dominance" in this game include:

Technological Monopoly

Leveraging its first-mover advantages in blockchain infrastructure, artificial intelligence, cyber defense, and big data analytics, the United States has built a multi-layered technological monopoly. In the virtual currency sector, it controls core R&D of mainstream blockchain protocols, maintains dominance over critical nodes, and holds technological superiority in on-chain data analytics. Leading blockchain firms like Chainalysis and Elliptic are U.S.-led, capturing over 90% of the global on-chain traceability market. Through its "small yard, high fence" strategy, the U.S. restricts the outflow of advanced technologies, integrates core technology of crypto into military-civilian dual-use systems, and bans the export of blockchain security tools to specific nations, thereby stifling other countries' digital innovation capabilities at the source.

Forming Clique

The United States has deeply intertwined technological hegemony with geopolitical objectives, using virtual currency asset regulation and cybersecurity as pretexts to interfere in other nations' internal affairs and suppress strategic rivals. By linking virtual asset transactions to political agendas like "anti-money laundering", "counter-terrorism financing", and "sanctions compliance", the U.S. has forged a global virtual asset regulatory alliance, imposing technological blockades and financial sanctions on countries that defy its rules. Simultaneously, it employs state-sponsored cyberattacks to steal sensitive political and economic data, leveraging digital cognitive warfare to shape favorable international narratives and maintain its global political dominance.

The Aggressive Extortion

As a new form of wealth in the digital era, virtual currency assets has become a key target for the U.S. economic plunder. Leveraging its technological superiority and regulatory authority, the United States, with the cooperation of allied nations, has incorporated global virtual currency transactions into its regulatory framework and cross-border enforcement system based on "long-arm jurisdiction". Through criminal prosecution, confiscations and fine, the U.S. has systematically seized overseas virtual currency assets on a massive scale. According to incomplete statistics, between 2022 and 2025, the U.S. confiscated virtual currency assets worth over \$30 billion through various cases worldwide. Notably, the Chen Zhi case alone accounted for \$15 billion in confiscated assets, representing 50% of the total. This unilateral seizure not only disrupts international law enforcement efforts and causes secondary losses to victims, but also interferes with the global circulation of virtual currency assets, destabilizes emerging market economies, and ultimately aims to consolidate the U.S. dollar's hegemony in the digital finance sector.

Regulation Blockade

The United States has enacted a series of policies and regulations to deeply integrate the cryptocurrency ecosystem with the US dollar system, transforming it into an "on-chain extension" of dollar hegemony. This initiative creates new demand for US Treasury bonds, attempting to establish a digital Bretton Woods system that extends the seigniorage privileges

of dollar dominance into the blockchain domain, thereby constructing a "Digital Dollar Hegemony 2.0". In 2025, the GENIUS Act (full name: Guiding and Establishing National Innovation for U.S. Stablecoins Act, commonly known as the Genius Act) requires stablecoin issuers to allocate over 80% of their reserve assets to purchase U.S. Treasury Securities. This effectively creates a mandatory and sustained demand source for the US bond market, serving dual purposes: transferring debt pressure while simultaneously harvesting global virtual currency assets.

III. "Thieves Falling Out" and "Long-arm Jurisdiction"

The Chen Zhi and Zhao Changpeng cases exemplify America's use of technological hegemony to harvest global virtual assets. These cases fully demonstrate the U.S. closed-loop strategy of "technological intrusion—regulatory coordination—enforcement action" with processes and technical details exhibiting distinct hegemonic characteristics. The Garantex case further illustrates how the U.S. weaponizes virtual asset regulation and exercises "long-arm jurisdiction" to achieve geopolitical objectives. This case highlights how the U.S. combines regulatory frameworks with sanctions to create transnational regulatory constraints, enabling targeted strikes against foreign exchanges.

Chen Zhi Case: A Model of "Thieves Falling Out" Virtual Asset Extortion Supported by Cyber Attacks

In October 2025, the U.S. District Attorney's Office for the Eastern District of New York announced criminal charges against Chen Zhi, founder of Cambodia's Prince Holding Group, involving online scams and money laundering. The office also publicly declared the confiscation of approximately 127,000 bitcoins under his control, valued at around \$15 billion at the time's market price, setting a record for the largest virtual asset seizure in U.S. judicial history. Under the pretext of "combating transnational online scam and money laundering," the U.S. Department of Justice hastily assembled so-called evidence and avoid the original source, "legalized" and confiscated the Prince Holding Group's bitcoins stolen through state-sponsored hacking in 2020. This case exemplifies America's typical "thieves falling out" approach of exploiting technological vulnerabilities to conduct cross-border plunder and impose cyber hegemony. In November 2025, China's National Computer Virus Emergency Response Center (CVERC) issued a report, "Technical Analysis of the LuBian Mining Pool Hacking Incident", revealed through technical evidence that U.S. state-sponsored hackers precisely exploited underlying encryption vulnerabilities to attack the cold crypto wallet of the LuBian mining pool and transfer assets, demonstrating America's mature technical capabilities in virtual currency asset theft. This starkly contradicts the U.S. government's claim that "Bitcoin has never been hacked", or more accurately, that "Bitcoin has never been hacked by hackers outside the U.S.

government".

Zhao Changpeng Case: Compliance Accountability Under Regulatory Blockade and Cyber Surveillance

From 2023 to 2025, the United States initiated a dual-track legal action (civil and criminal) against Binance, a globally renowned cryptocurrency exchange, and its founder Zhao Changpeng. The case culminated in Binance paying a \$4.35 billion fine, including \$2.7 billion in confiscated illicit gains, \$1.35 billion in civil penalties, and \$150 million in personal fines, while Zhao Changpeng was granted a pardon after signing a plea agreement. This case exemplifies how the U.S. leverages judicial hegemony and cyber surveillance to compel global virtual asset exchange to comply with its regulatory rules, thereby enabling economic exploitation and rule imposition.

During the investigation, the United States employed comprehensive cyber surveillance methods to thoroughly analyze and collect evidence from Binance's operational, user, and transactional data, demonstrating its technological edge in monitoring virtual asset exchange platforms.

Firstly, cross-border data theft and internal information acquisition. The U.S. utilized hacking techniques to infiltrate Binance's internal servers, obtaining core operational data and executive communication records. This confirmed that Binance executives were fully aware of U.S. regulatory rules but deliberately circumvented compliance requirements. For instance, internal communication records revealed that Zhao Changpeng instructed employees to use encrypted communication tools like Signal to destroy evidence, replaced "U.S." labels in internal databases with "UNKWN" to conceal U.S. user presence, and even issued "VPN usage guidelines" to help U.S. users bypass IP blockchains. Secondly, comprehensive monitoring and analysis of transaction data. By connecting to global blockchain nodes and collaborating with on-chain data analytics firms, the U.S. achieved real-time monitoring of Binance's transaction data, accurately tracking U.S. user activities and fund flows in sanctioned regions. Data showed that while U.S. users accounted for nearly 20% of Binance's total, only 30% to 40% completed KYC (Know Your Customer) verification, exposing vulnerabilities like "no KYC required for 2 BTC withdrawal limits." These findings were used by the U.S. as key evidence of non-compliance. Thirdly, technical tracing of compliance loopholes. U.S. technical teams conducted penetration tests on Binance's KYC system and anti-money laundering monitoring systems, identifying systemic flaws in compliance mechanisms. Issues included IP blockchains appearing as pop-up notifications and sub-accounts bypassing KYC reviews, further supporting allegations that Binance "deliberately maintained invalid compliance procedures".

The enforcement logic of this case exhibits a distinct pattern of "rule presupposition—technical evidence collection — penalty harvesting": The U.S. first incorporates global virtual asset exchange platforms into its "long-arm jurisdiction" through domestic regulations, then employs technical means to secure evidence of platform violations, and ultimately achieves economic gains through hefty fines. Simultaneously, it compels platforms to undergo U.S. compliance

reforms, thereby reinforcing America's rule dominance in the virtual currency asset sector.

The Garantex Case: Control the virtual asset Ecosystem by "Inter-agency Coordination" and "Long-arm Jurisdiction" .

The United States has adopted cryptocurrencies as a geopolitical tool in its toolkit, viewing platforms like Garantex as funding channels for sanctioned nations to circumvent sanctions. Through a multi-pronged approach — administrative sanctions, judicial accountability, technological blockades, and international collaboration—the U.S. systematically severs these platforms' links with the global financial system.

In 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) placed Garantex and its affiliates on the Specially Designated Nationals And Blocked Persons List (SDN), compelling stablecoin issuer Tether to freeze its wallet assets and paralyzing its liquidity through dollar-dominated settlement systems. The U.S. Department of Justice subsequently prosecuted executives and dismantled the operational team via international arrests (including India's capture of co-founders), while seizing domain names and servers to physically destroy its infrastructure. The U.S. also employed technical means to identify circumvention tactics—when Garantex attempted to transfer assets by rebranding Grinex or issuing the ruble stablecoin A7A5, OFAC immediately expanded sanctions to include alternative channels. This demonstrates how the U.S. leverages "digital traces" and "financial touchpoints" as jurisdictional connection points, combining on-chain tracking with traditional judicial procedures to extend domestic law to foreign jurisdictions, achieving comprehensive suppression of its virtual asset ecosystem.

The United States' aggressive stance in the Garantex case stems from its strategic needs to maintain financial hegemony, counter geopolitical rivals, and dominate emerging digital domains.

While the aforementioned typical cases differ in their targets and enforcement methods, they fundamentally follow a unified digital harvest logic: leveraging technological superiority as the core support, legal regulations as binding tools, and specialized agencies as execution vehicles to form a closed-loop system. Technologically, core technologies such as on-chain traceability, data monitoring, and vulnerability exploitation enable precise positioning and evidence fixation of global virtual assets. Legally, institutional innovations like extended jurisdiction through local regulations and civil confiscation allow cross-border jurisdiction expansion. Institutionally, a collaborative law enforcement network spanning multiple departments and allies ensures the implementation of harvesting operations. Throughout this process, for numerous fraud victims, it's akin to a mantis catching a cicada while an oriole lurks behind. The U.S. government's tolerance of telecom fraud and its massive profits derived from technological hegemony have largely failed to compensate victims, effectively constituting indirect plunder of foreign assets. In reality, this model not only applies to the virtual currency asset sector but also represents a universal paradigm through which the U.S. has long exploited technological dominance to infringe upon global interests. Clearly, the successful practices of cases like Chen Zhi, Zhao

Changpeng, and Garantex have bolstered the U.S. government's confidence in fully controlling the global virtual currency market, serving as a key driver for establishing a national strategic reserve of virtual currency assets represented by Bitcoin.

IV. The Global Expansion and Underlying Motives of U.S. Technological Hegemony

As the well-known "Empire of Hacking", the United States maintains the world's largest state-sponsored hacking capabilities. Between 2023 and 2025, U.S.-backed hacker groups conducted targeted attacks on over 20 major cryptocurrency exchanges globally. Their tactics included backdoor implantation, spear-phishing, and supply chain infiltration, primarily stealing users' wallet private keys, transaction records, and regulatory compliance data. The attacks targeted platforms across multiple countries and regions in Asia, Europe, and Africa. Timeline analysis reveals that some of these attacks were linked to U.S. law enforcement actions by the Department of Justice and OFAC in the virtual asset sector.

The United States leverages technological hegemony to harvest global virtual assets, fundamentally aiming to maintain its economic dominance and the status of the US dollar. On one hand, it directly plunders global wealth through confiscations and fines to bolster domestic economic strength. On the other hand, by controlling regulatory rules and transaction flows of virtual assets, it integrates the digital financial system into the US dollar-dominated global financial framework, curbing attempts by other countries to bypass dollar settlements via virtual currency assets. For illegally acquired Bitcoin, the US government monetizes assets through public auctions, generating substantial profits. The Bitcoin seized during the 2013 case where the FBI shut down the dark web trading platform "Silk Road" alone saw auction proceeds exceeding \$10 billion over a decade from 2014 to January 2025. According to the US "Equitable Sharing Program", part of the revenue becomes "dividends" for law enforcement agencies, while the majority goes into federal coffers. The data from U.S. Department of Treasury shows that law enforcement actions in the virtual asset sector generate hundreds of billions of dollars in annual fiscal revenue, while simultaneously reinforcing global reliance on dollar-denominated virtual currency transactions and further consolidating the dollar's international monetary status. Moreover, the auctioned Bitcoin represents merely a drop in the bucket of its aggressive acquisitions, with the bulk serving as Bitcoin strategic reserves. The Trump administration redefined "judicial forfeiture" as a "zero-cost strategy" to build national strategic assets. This move was not merely a fiscal maneuver but also a response to the dollar hegemony crisis, aiming to counter the global de-dollarization trend by controlling "digital gold".

It must be emphasized that the extortion in the virtual asset sector is merely a microcosm of America's global technological hegemony. Leveraging the world's largest cyber arsenal, elite state-sponsored hacker groups, and a sophisticated high-tech industrial ecosystem, the U.S. has

extended its technological dominance to critical infrastructure, scientific research, and political spheres. Through state-sponsored cyberattacks, weaponized technical standards, and digital cognitive warfare, it serves its global expansion of political and economic interests while maintaining global hegemony. More crucially, the true underlying motive of American hegemony lies in sustaining the deep-rooted operation of its "Tech-Politics-Military Complex" which epitomizes the dual pursuit of capital appreciation and power expansion.

The U.S. "Tech-Politics-Military Complex" centers around Silicon Valley tech titans, political elites, and Wall Street financial oligarchs, forming an interconnected power network through mechanisms like political donations, secret defense budgets, and revolving doors between government and business. By leveraging technological hegemony for digital extortion and cyberattacks, the U.S. essentially sustains this complex's self-reinforcing cycle. Tech giants secure lucrative government contracts, tax breaks, and regulatory relaxations by providing technical support (e.g., blockchain analytics, cyberattack tools) to politically controlled governments. Meanwhile, political elites advance hegemonic strategies through these tech giants while benefiting from their technological capital. Wall Street oligarchs lobby politicians to push unilateral cryptocurrency regulations and harvest sanctioned assets for capital gains. This self-reinforcing cycle makes technological hegemony the core pursuit of the "Tech-Politics-Military Complex," driving the U.S. to continuously strengthen its digital harvesting and cyberattack capabilities while maintaining its privileged status.

V. Conclusion

This article systematically exposes the sinister schemes of the U.S. government, which relies on technological hegemony, uses financial innovation as a cover, employs virtual currency assets as a vehicle, aims to maintain and upgrade the dollar hegemony system, and fundamentally seeks to continue exploiting the world. Regarding virtual currencies, the People's Bank of China has explicitly stated that virtual currencies do not possess legal status equivalent to legal tender, lack legal tender status, and should not be used as currency in market circulation. virtual currency-related business activities are classified as illegal financial activities. Even so-called "stablecoins" pegged to legal tender remain subject to cautious scrutiny from international financial organizations and central banks, as they still carry significant financial risks. We also urge global holders of virtual currency assets to carefully assess the security of their holdings. In the face of the powerful U.S. state apparatus, so-called "digital gold" could be "vanished into thin air" at any moment.