Crypto Loopholes Are Powering America's Adversaries

Last week, the Treasury Department froze $344 million in cryptocurrency tied to Iran's regime, sanctioning digital wallets giving Tehran a financial lifeline. The fact that these funds could move at scale underscores a troubling reality: digital finance is emerging as a powerful tool for America's adversaries to evade sanctions. As it considers the CLARITY Act, the Senate has a chance to respond to this challenge by closing the cryptocurrency loopholes that empower Iran's regime and other anti-American actors. Congress must ensure digital assets are subject to robust anti-money laundering (AML) and counter-terror financing regulations so they no longer serve as a weapon in the hands of adversaries.

America's Adversaries Are Weaponizing Crypto

- **Tehran's effort to turn Hormuz into a crypto tollbooth is just the tip of the iceberg.** China, Iran, Russia, North Korea and their proxy networks are using digital assets to evade sanctions, launder money, and finance their militaries. This is not just moving money–it is giving enemies the tools to threaten U.S. troops, strike allies, and damage our interests.
- **State adversaries and their terrorist proxies are the most direct threat:**
    - Iran's Islamic Revolutionary Guard Corps, a designated terrorist organization, used the world's largest crypto exchange to sell military equipment and procure drone components from Chinese suppliers. $1.7 billion in crypto was allegedly transferred to Iranian entities via Binance, which is under DOJ investigation.
    - The CCP is directly abetting this activity. Chinese companies serve as key payment hubs for IRGC drone and missile procurement, helping terrorist actors operate outside the dollar system.
    - Pro-Russian paramilitary groups have raised more than $8.3 million in crypto since Russia's invasion of Ukraine, including purchases of battlefield drones.
    - North Korea regularly uses cryptocurrency theft to bankroll the Kim regime. In 2025 alone, it stole an estimated $2.02 billion in digital assets as part of a campaign of intrusions targeting crypto firms and software supply chains.
- **These same regulatory gaps are also being exploited by criminal networks:**
    - China-linked money laundering networks processed roughly $16.1 billion in illicit crypto funds last year alone.
    - Chinese nationals have pleaded guilty to directly targeting American citizens in crypto scams: a June 2025 scheme laundered more than $36.9 million stolen from 174 U.S. victims; another case produced the world's largest crypto seizure–roughly 61,000 Bitcoin tied to an alleged $6.7 billion scam.
    - Chinese and Iranian hackers targeting U.S. hospitals, pipelines, and critical infrastructure use crypto to collect and launder ransom payments beyond the reach of law enforcement.
    - Cartels, traffickers, and black-market networks use cryptocurrency to launder proceeds, pay smugglers, procure weapons and drugs, and finance human trafficking.

- These threats are connected. **State adversaries and criminal networks exploit the same unregulated channels for the same reason**: digital asset platforms are not required to screen customers, report suspicious activity, or comply with sanctions lists. That vulnerability is a problem Congress can fix.

Weak Rules Enable Enemies

- **Lightly governing digital finance markets is a security vulnerability**, especially with rising foreign cyber aggression against critical U.S. systems. Every dollar routed to a sanctioned regime, terror-linked network, or proxy force can help finance drones, missiles, cyberattacks, and other tools aimed at Americans and U.S. allies.
- **Crypto loopholes are a homeland security threat.** Ransomware attackers use crypto to extort hospitals, pipelines, utilities, and other critical infrastructure–and digital finance is the mechanism that makes their coercion and payoff possible.
- **Our adversaries are turning to crypto because it has gaps in federal oversight**, and digital asset platforms operate under weaker standards than the rest of the financial system. That gap hands our adversaries exactly what they want: a fast, opaque, and hard-to-police channel for moving money across borders in minutes, routing around traditional chokepoints, and reaching weak jurisdictions.
- **The fix is not complicated.** Customer identification, suspicious activity reporting, sanctions compliance, recordkeeping, and risk-based controls are the frontline defenses that have locked criminals and terrorists out of the global financial system for decades. There is no national security justification to exempt crypto from the same standards.

Clearer Rules From Congress Would Strengthen Security

- As Treasury Secretary Scott Bessent recently argued, **proper rule-making will not weaken digital finance**–it will provide safety, resilience, and credibility. It will also equip the Treasury, law enforcement officials, and the Intelligence Community with enhanced tools to trace, flag, freeze, and disrupt illicit flows before the consequences become grave. The backbone of America's national security is our economic security.
- **The right foundation already exists**. The Senate Banking Committee's version of the CLARITY Act–championed by Chairman Tim Scott–adds important Bank Secrecy Act (BSA) and AML requirements for crypto intermediaries, including customer identification, suspicious activity reporting, and sanctions screening.
- However, **the current framework does not go far enough to fully close the sanctions evasion pathways** adversaries like Iran can exploit through crypto. It should be strengthened before passage. Failing to address these shortcomings would be an own-goal for national security, especially with adversaries exploiting lax oversight.

Policy Recommendations:

1. **Strengthen BSA and AML requirements** for digital asset intermediaries, including customer identification, suspicious activity reporting, and sanctions screening.
2. **Expand enforcement mechanisms** to reduce sanctions evasion risks and strengthen oversight on U.S. adversaries and malign actors.

3. **Close regulatory gaps** allowing offshore or lightly regulated platforms to facilitate illicit finance.
4. **Do not delay urgent national security safeguards** in digital asset legislation as a result of market structure debates, including over stablecoin policy.
5. **Require the same baseline financial crime standards** for digital asset firms moving money in the U.S. as banks have, ensuring parity across the financial system.

Bottom Line: Congress must put national security first by holding digital asset firms to the same standards as every other financial institution in America—and closing the crypto loopholes our adversaries exploit.