Crypto Loopholes Are Powering America's Adversaries

Last week, Tehran demanded that oil tankers pay cryptocurrency tolls to transit the Strait of Hormuz, underscoring a troubling reality: digital finance has quickly become a tool for America's adversaries to evade sanctions at scale. 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 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.
- **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.

Clear Rules From Congress Would Strengthen Security

- As Treasury Secretary Scott Bessent argued last week, **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 foundation 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 and anti-money laundering requirements for crypto intermediaries, including customer identification, suspicious activity reporting, and sanctions screening.
- The current framework does not go far enough to fully close the sanctions evasion pathways adversaries like Iran can exploit through crypto. **Before passage, this framework should be strengthened** even further with tougher Bank Secrecy Act and anti-money laundering provisions, alongside robust enforcement mechanisms to reduce sanctions evasion risks and ensure parity with other banks.
- Lawmakers should require digital asset firms moving money in the U.S. to **meet the same baseline standards as other financial institutions** and close loopholes allowing our adversaries to exploit offshore or lightly-regulated platforms.
- **The security dimensions of digital asset policy must come first.** Congress cannot let disputes over stablecoin interest rates or other market structure questions stall solutions to close vulnerabilities America's adversaries are actively exploiting.
- **Digital asset companies should be held to the same financial crime standards as every bank in America.** Doing otherwise would be an own-goal for national security, especially while adversaries are using lax oversight to their advantage.