

New Report: Real World Harms of Failing to Properly Regulate Crypto

Ahead of a Senate vote on the CLARITY Act, Transparency International U.S. warns of a wide range of corrupt and criminal activity if the bill isn't amended

WASHINGTON, D.C. — Transparency International U.S. released a new report today, **Crypto's Dirty Money Problem: What Congress Must Fix**, warning that fast-moving legislation that fails to properly regulate the cryptocurrency industry will leave law enforcement unequipped to fight scammers and fraudsters, drug cartels, terrorist financing, sanctions evasion, and corruption, among many other kinds of crime.

This report is released as the Senate actively debates the CLARITY Act — a bill that seeks to regulate the crypto industry but leaves significant gaps that a wide range of criminal actors could exploit — and rushes to vote on it before the August congressional recess.

The report identifies three core concerns: cryptocurrency facilitating serious, real-world illicit finance, stablecoins are emerging as a preferred vehicle for moving that dirty money, and Congress is nevertheless prepared to pass legislation that leaves major gaps through which a wide range of criminal activity could continue unchecked. Digital assets have become attractive to illicit actors due to their speed, pseudonymity, borderless access, regulatory arbitrage, and obfuscation tools, which are dangerous when unmet with compliance obligations.

"Congress is writing the rules for the next frontier of money. The choice is whether that new system becomes a Wild West for criminals using crypto or includes basic safeguards to protect Americans from scammers, fraudsters, drug cartels, terrorist networks, and other criminals," said **Scott Greytak**, co-author of the report, attorney, and Deputy Executive Director for TI US. "Clear rules of the road for the crypto industry cannot come at the expense of the tools law enforcement needs to keep Americans safe. If Congress gives the

industry what it wants without giving law enforcement what it needs, it will hand criminals a roadmap for staying one step ahead.”

The report details real-world examples of harm, such as Iran's recent use of exchanges and front-company networks. In June, the U.S. Department of the Treasury sanctioned Nobitex, Iran's largest digital asset exchange, for alleged terror finance and sanctions evasion activity.

This is not a hypothetical or emerging threat. Terrorist organizations have used cryptocurrency to raise and move funds for years. In 2020, the Department of Justice disrupted three major cyber-enabled terrorist-financing campaigns:

- Hamas conducted cryptocurrency fundraising campaigns.
- Al-Qaeda used sham charities and Telegram channels to solicit cryptocurrency donations for weapons procurement.
- ISIS used cryptocurrency—including privacy-enhancing assets and online donation campaigns—to raise funds.

“Crypto policy cannot be built around what companies call themselves. The rules must follow the financial function, the risks involved, and the people who control or profit from the activity,” said **Annalise Burkhart**, co-author of the report and U.S. Global Programs Lead at Transparency International U.S. “Congress should close the gaps involving offshore platforms, stablecoins, DeFi services, mixers, unhosted wallets, and other parts of the market that illicit actors can exploit. A regulatory framework is only as strong as the activity it actually covers.”

The risks extend beyond illicit finance: Public officials and their immediate family members create serious conflicts of interest when they are permitted to own, promote, sponsor, or profit from digital-asset ventures. Officials who write or enforce the rules governing the industry should not have a personal financial stake in the outcome; otherwise, they have a direct incentive to shape policy in ways that increase the value of their holdings rather than protect the public.

TI US calls on Congress to ensure that any digital asset legislation includes the bare minimum of:

- Applying AML/CFT obligations based on financial function and risk, not industry labels

- Closing offshore loopholes that allow crypto firms and illicit actors to evade U.S. law
- Requiring stablecoin issuers to monitor and address risks across their ecosystems
- Covering decentralized finance (DeFi) businesses and interfaces where identifiable persons control, influence, or materially benefit from the services
- Clarifying regulatory authority over mixers and anonymizing services
- Imposing risk-based obligations for exposure to unhosted wallets
- Requiring effective fraud prevention, evidence preservation, and victim-recovery measures
- Preserving sanctions authorities and requiring operational sanctions compliance
- Strengthening information sharing and converting existing recommendations into concrete action
- Providing adequate resources for enforcement and requiring meaningful public reporting
- Establishing a clear ethics rule that bars public officials and their immediate family members from owning, promoting, sponsoring, or profiting from digital-asset ventures while those officials write or enforce the rules governing the industry

###

About Transparency International U.S.

Transparency International U.S. is part of the world's largest coalition against corruption. In collaboration with national chapters in more than 100 countries, we are leading the fight to turn our vision of a world free from corruption into reality.