Cointel

Investment Club

Crypto's Legal Crossroads:

The Tornado Cash Case And the Crypto Privacy Paradox

What the battle between privacy protocols and global regulators reveals about crypto's evolving identity.

August 2025

Few events have crystallized the philosophical and legal tensions at the heart of crypto as sharply as the Tornado Cash case. At its center lies a simple but polarizing question: should individuals have the right to transact privately on public blockchains, or should the state's imperative to combat money laundering and terrorism financing take precedence?

Tornado Cash was built as a decentralized, non-custodial privacy protocol on Ethereum. It uses zero-knowledge proofs (zk-SNARKs) to obscure the on-chain link between sender and receiver addresses. Instead of tracing funds directly, users deposit assets into a pool and later withdraw them to a different address, breaking the visible chain of custody. Importantly, no single entity controls this system. Once deployed, the smart contracts are immutable and operate independently of their creators.

The philosophy behind Tornado Cash was straightforward: public blockchains expose all financial activity, and in such a transparent environment, privacy tools aren't just useful for criminals—they're necessary for everyone. Anonymous charitable donations, shielding competitive business activity, and protecting personal financial information are all legitimate applications. For privacy advocates, Tornado Cash represented a natural extension of a fundamental right into the digital economy.

But that vision collided with an opposing one: the regulatory mandate to prevent illicit finance. And it collided hard.

A Whirlwind of Sanctions and Prosecutions

The conflict erupted on August 8, 2022, when the U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash. The agency alleged that over $7 billion had been laundered through the protocol since 2019, including funds linked to North Korea's Lazarus Group. For the first time in history, the U.S. government placed open-source software itself—immutable code—on its Specially Designated Nationals (SDN) sanctions list.

This was only the beginning. The U.S. Department of Justice later indicted two Tornado Cash co-founders, Roman Storm and Roman Semenov, on charges including conspiracy to commit money laundering and operating an unlicensed money transmitting business. Meanwhile, Dutch authorities prosecuted developer Alexey Pertsev, ultimately convicting him of money laundering.

The resulting legal battles became a watershed moment for crypto. They raised unprecedented questions: Can code itself be sanctioned as a "person" under the law? Are developers criminally liable for how decentralized protocols are used after launch? And where does the line fall between expression, innovation, and complicity?

Privacy as a Right vs. AML as a Duty

The heart of the Tornado Cash debate is the clash between privacy and anti-money laundering (AML) enforcement.

Supporters argue that financial privacy is not just a perk but a necessity. Salaries, medical reimbursements, donations, and personal purchases shouldn't be open to anyone with a block explorer. Tools like Tornado Cash, they contend, enable ordinary users to protect themselves from surveillance, discrimination, or retaliation. The principle that "code is speech" further bolsters this argument: publishing open-source code, like writing encryption software, is an act of expression protected under law.

Critics, however, point to the darker side of privacy protocols. They obscure funds for ransomware operators, cybercriminals, sanctions evaders, and state-backed hackers. From a regulatory perspective, such tools frustrate AML and Know Your Customer (KYC) rules that underpin global financial security. For governments, allowing these systems unchecked means enabling the very actors AML laws are designed to stop.

The dual-use nature of Tornado Cash mirrors debates around encryption itself: technology that protects dissidents also shields criminals. And the law is still struggling to reconcile the two.

Divergent Trials, Divergent Philosophies

In the wake of these cases, the crypto community has been forced to adapt. Rather than focusing solely on "uncensorable" systems, developers are now exploring ways to reconcile privacy with compliance.

One promising path is the use of zero-knowledge proofs not just for anonymity, but for selective transparency. In theory, ZKPs could allow users to prove they are not on a sanctions list or have passed KYC checks—without revealing any personal data. This "compliance without surveillance" model could offer regulators the assurances they need while preserving privacy for ordinary users.

At the governance level, the Tornado Cash DAO itself became a cautionary tale. Prosecutors used Roman Storm's TORN token holdings as evidence of control, undermining the argument that the system was truly decentralized. A subsequent governance attack in 2023, where an exploiter seized control of the DAO's voting power, further exposed the fragility of such models. These episodes have forced projects to reconsider what "decentralization" means in practice, and whether their governance structures are legally defensible.

At the policy level, industry groups like Coin Center, the Electronic Frontier Foundation, and the Blockchain Association have called for clearer boundaries. They argue that distinguishing between code publication and active facilitation of crime is essential for innovation. Internationally, frameworks like Europe's MiCA regulation may set new baselines by demanding operational resilience and clearer compliance obligations, but at least offering predictability.

The Crypto Community's Response

In the wake of these cases, the crypto community has been forced to adapt. Rather than focusing solely on "uncensorable" systems, developers are now exploring ways to reconcile privacy with compliance.

One promising path is the use of zero-knowledge proofs not just for anonymity, but for selective transparency. In theory, ZKPs could allow users to prove they are not on a sanctions list or have passed KYC checks—without revealing any personal data. This "compliance without surveillance" model could offer regulators the assurances they need while preserving privacy for ordinary users.

At the governance level, the Tornado Cash DAO itself became a cautionary tale. Prosecutors used Roman Storm's TORN token holdings as evidence of control, undermining the argument that the system was truly decentralized. A subsequent governance attack in 2023, where an exploiter seized control of the DAO's voting power, further exposed the fragility of such models. These episodes have forced projects to reconsider what "decentralization" means in practice, and whether their governance structures are legally defensible.

At the policy level, industry groups like Coin Center, the Electronic Frontier Foundation, and the Blockchain Association have called for clearer boundaries. They argue that distinguishing between code publication and active facilitation of crime is essential for innovation. Internationally, frameworks like Europe's MiCA regulation may set new baselines by demanding operational resilience and clearer compliance obligations, but at least offering predictability.

A New Digital Frontier

The Tornado Cash case is far from the last word on privacy in decentralized finance. But it has already left a lasting mark.

The long-term impact will likely be twofold. On one side, developers may face a chilling effect, wary of building privacy protocols under the shadow of potential prosecution. On the other, regulators are beginning to clarify boundaries, and that clarity—while restrictive—may help stabilize the industry and attract more institutional adoption.

At its core, the saga underscores that privacy and AML enforcement are not mutually exclusive absolutes, but competing principles that must coexist. Tornado Cash revealed both the necessity of financial privacy in a transparent digital economy and the dangers of untraceable flows exploited by malicious actors.

Rather than resolving the tension, the case has illuminated it. The future of DeFi will depend on whether developers, regulators, and users can chart a middle ground.

Market conditions in digital assets are subject to rapid change. The analysis contained herein reflects our understanding as of the publication date.

Cointel Global Research Center

Cointel.io
Follow us for the latest insights:

- Twitter/X: @Cointel_io
- linktr.ee/Cointel_io
- Telegram: https://t.me/CointelOfficial

This article is intended for informational purposes only and does not constitute financial advice. Investing in blockchain assets involves inherent risks, including the possibility of losing some or all of your investment. We encourage you to make informed decisions and consult a qualified professional if necessary.