Tornado Cash Trial: Is Code Speech or Crime? **Roman Storm**'s Case Challenges Crypto Freedom

Excerpt

Roman Storm, co-founder of **Tornado Cash**, faces trial in New York for allegedly facilitating over $1 billion in money laundering, including funds tied to North Korea's **Lazarus Group**. The case raises critical questions about whether developers of decentralized, open-source software can be held criminally liable for its misuse. With a parallel conviction in the Netherlands setting a chilling precedent, Storm's trial could redefine the boundaries of financial privacy and software development. As the U.S. pushes to regulate crypto, is this a justified crackdown on cybercrime or an overreach threatening innovation?

Introduction

The trial of **Roman Storm**, a co-founder of **Tornado Cash**, began on July 14, 2025, in the Southern District of New York, marking a pivotal moment for the cryptocurrency industry and the broader debate over developer liability. Storm faces charges of conspiracy to commit money laundering, conspiracy to violate U.S. sanctions, and conspiracy to operate an unlicensed money-transmitting business, with a potential sentence of up to 45 years if convicted.

These charges stem from his role in developing **Tornado Cash**, a decentralized protocol designed to anonymize cryptocurrency transactions on the Ethereum blockchain. The case echoes a similar prosecution in the Netherlands, where **Tornado Cash** co-founder **Alexey Pertsev** was convicted of money laundering in 2024, raising alarms about the global crackdown on crypto privacy tools. This report critically examines the charges, the connections between the cases, and their implications for decentralized finance (DeFi) and free speech.

Background: **Tornado Cash** and Its Role

Launched in 2019, **Tornado Cash** is a non-custodial cryptocurrency mixer that allows users to deposit Ethereum into shared pools, mixing their funds with others to obscure transaction histories. Users receive a cryptographic code to withdraw funds to a new wallet, making it difficult to trace the origin or destination of the crypto. Promoted as a privacy tool, **Tornado Cash** has been lauded by advocates like Ethereum co-founder Vitalik Buterin, who used it to anonymize donations to Ukraine, and criticized by authorities for enabling illicit activities. The U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned **Tornado Cash** in August 2022, alleging it facilitated over $7 billion in transactions, including $455 million laundered by North Korea's **Lazarus Group**, a state-sponsored hacking syndicate.

The protocol's decentralized nature—running on immutable smart contracts—means developers like Storm, Pertsev, and **Roman Semenov** (the third co-founder, currently at large) do not control user

funds or transactions. This raises a central question: can developers be held liable for how others use their open-source code?

Charges Against **Roman Storm**

Storm, a 34-year-old U.S. resident, was arrested in August 2023 in Washington state and released on $2 million bail. The *U.S. Department of Justice (DOJ)* alleges that Storm and Semenov knowingly operated **Tornado Cash** to facilitate over $1 billion in money laundering, including hundreds of millions for the **Lazarus Group**, in violation of U.S. sanctions under the *International Emergency Economic Powers Act (IEEPA)*. The indictment also charges them with operating an unlicensed money-transmitting business, claiming **Tornado Cash** should have registered with the *Financial Crimes Enforcement Network (FinCEN)* and implemented anti-money laundering (AML) measures.

Prosecutors argue that Storm and Semenov were aware of illicit uses, citing private chats where they acknowledged the platform's exploitation by hackers but failed to implement effective controls. For instance, after the **Lazarus Group** used **Tornado Cash** to launder funds in 2022, the developers made a public claim of sanctions compliance, but privately admitted the changes were ineffective. The DOJ further contends that Storm profited significantly, allegedly selling $12 million in TORN tokens, the protocol's governance token.

Storm's defense, led by attorneys **Brian Klein** and **David Patton**, argues that he merely wrote open-source code and cannot be held responsible for third-party actions. They cite a 2019 *FinCEN* guidance stating that developers of anonymizing software are not money transmitters, as they do not control user funds. The defense also invokes First Amendment protections, asserting that code is a form of expressive speech. Industry groups like the *Blockchain Association* and *Coin Center* have filed amicus briefs, warning that a guilty verdict could criminalize software development and stifle DeFi innovation.

The Netherlands Connection: Alexey Pertsev's Conviction

The case of **Alexey Pertsev**, another **Tornado Cash** co-founder, provides a troubling precedent. Arrested in the Netherlands in August 2022, Pertsev was convicted of money laundering in May 2024 by the 's-Hertogenbosch Court of Appeal and sentenced to 64 months in prison. Dutch prosecutors argued that **Tornado Cash** laundered $1.2 billion in stolen cryptocurrency, including funds from high-profile hacks like the $600 million Axie Infinity theft by the **Lazarus Group**.

The court rejected Pertsev's defense that the protocol's decentralization absolved him of responsibility, stating that **Tornado Cash** "executed concealing and disguising activities" and was not merely a neutral tool. Evidence from group chats showed that Pertsev and his co-founders were aware of illicit uses but took no action to curb them.

Pertsev, released under electronic monitoring in February 2025 to prepare his appeal, has garnered support from crypto advocates who argue that holding developers liable for decentralized protocols sets a dangerous precedent. The Dutch verdict has been criticized for its broad interpretation of money laundering laws, which could extend liability to any software developer whose tools are misused.

Connections and Contrasts Between the Cases

The U.S. and Dutch cases share striking similarities but differ in legal context. Both Storm and Pertsev are charged with money laundering tied to **Tornado Cash**'s use by the **Lazarus Group**, and both prosecutions rely on evidence of the developers' knowledge of illicit activities. However, the U.S. case includes additional charges of sanctions violations and unlicensed money transmission, reflecting America's stricter regulatory framework.

The DOJ's partial dismissal of one charge against Storm in May 2025—related to failing to register as a money transmitter under 18 U.S.C. § 1960(b)(1)(B)—suggests a slight shift in prosecutorial strategy, possibly influenced by the Trump administration's crypto-friendly policies and the April 2025 Blanche Memo, which discourages regulatory charges without clear criminal intent.

The Dutch case, by contrast, focused solely on money laundering and applied a broader liability standard, holding Pertsev accountable for the protocol's automated actions. U.S. law, with its First Amendment protections and *FinCEN* guidance, may offer Storm a stronger defense, particularly if the court accepts that code is protected speech or that **Tornado Cash**'s non-custodial nature exempts it from money transmitter status. The U.S. Court of Appeals for the Fifth Circuit's ruling in Van Loon v. Department of the Treasury (2024), which found that **Tornado Cash**'s smart contracts are not sanctionable property, bolsters this argument, though Judge **Katherine Polk Failla** barred mention of this case in Storm's trial to avoid jury confusion.

Critical Analysis: A Clash of Principles

The **Tornado Cash** cases pit financial privacy against law enforcement's need to combat cybercrime. On one hand, **Tornado Cash**'s ability to anonymize transactions serves legitimate purposes, such as protecting dissidents in authoritarian regimes or enabling private donations, as demonstrated by Buterin's use. On the other, its exploitation by groups like the **Lazarus Group**, linked to North Korea's nuclear program, underscores the risks of untraceable transactions. The DOJ's narrative—that Storm and his co-founders knowingly facilitated crime—relies on their failure to implement AML controls, but this assumes developers can or should police decentralized systems, a notion at odds with the ethos of DeFi.

The prosecution's case raises troubling questions. If developers are liable for misuse of their code, could creators of operating systems like Linux or messaging platforms like WhatsApp face similar charges? The Dutch court's ruling against Pertsev suggests a slippery slope, where any tool enabling anonymity could expose its creator to criminal liability. Yet, the DOJ's evidence of private chats and profit-taking by Storm complicates the narrative of a purely idealistic developer. The government's decision to drop part of the money transmitter charge indicates uncertainty about applying traditional financial regulations to decentralized protocols, especially after the Van Loon ruling.

Judge Failla's skepticism of Storm's free speech defense and her rejection of his motion to dismiss suggest a narrow interpretation of First Amendment protections for code. Her ruling that **Tornado Cash** is not "meaningfully different" from other money-transmitting businesses could set a precedent that chills DeFi development. However, the crypto community's robust support, including $2.11 million raised for Storm's legal defense and backing from figures like Buterin, highlights the case's broader stakes. A guilty verdict could deter innovation, while an acquittal might embolden developers to create privacy tools without fear of prosecution.

Implications and Unanswered Questions

Storm's trial, expected to last a month, will test whether U.S. courts view decentralized protocols as neutral tools or criminal enterprises. The outcome could influence Pertsev's appeal in the Netherlands and shape global approaches to crypto regulation. If Storm is convicted, developers may hesitate to build privacy-focused tools, fearing liability for third-party actions. Conversely, an acquittal could affirm the right to code as protected speech, encouraging innovation but potentially complicating law enforcement efforts against cybercrime.Key questions remain: Should developers be obligated to prevent misuse of open-source software? Does the DOJ's case align with its own guidance under the Blanche Memo? And how will courts balance privacy rights with national security concerns? The exclusion of the Van Loon verdict from Storm's trial limits the defense's ability to leverage favorable precedent, raising concerns about judicial fairness.

Conclusion

The trial of **Roman Storm** is more than a legal battle; it's a referendum on the future of decentralized finance and the right to create privacy-preserving software. As governments worldwide grapple with regulating cryptocurrency, the **Tornado Cash** cases highlight the tension between innovation and accountability. The Dutch conviction of **Alexey Pertsev** serves as a warning, but the U.S. legal system's unique protections may yield a different outcome. The crypto community watches closely, knowing the verdict could redefine the boundaries of code, crime, and freedom.Call to Action: If you have information on cybercrime cases, including those involving cryptocurrency mixers like **Tornado Cash**, we urge you to share it securely through our whistleblower platform, Whistle42. Your insights could expose illicit activities or protect innovators from overreach. Visit Whistle42 to submit tips anonymously and help shape a fairer digital future.