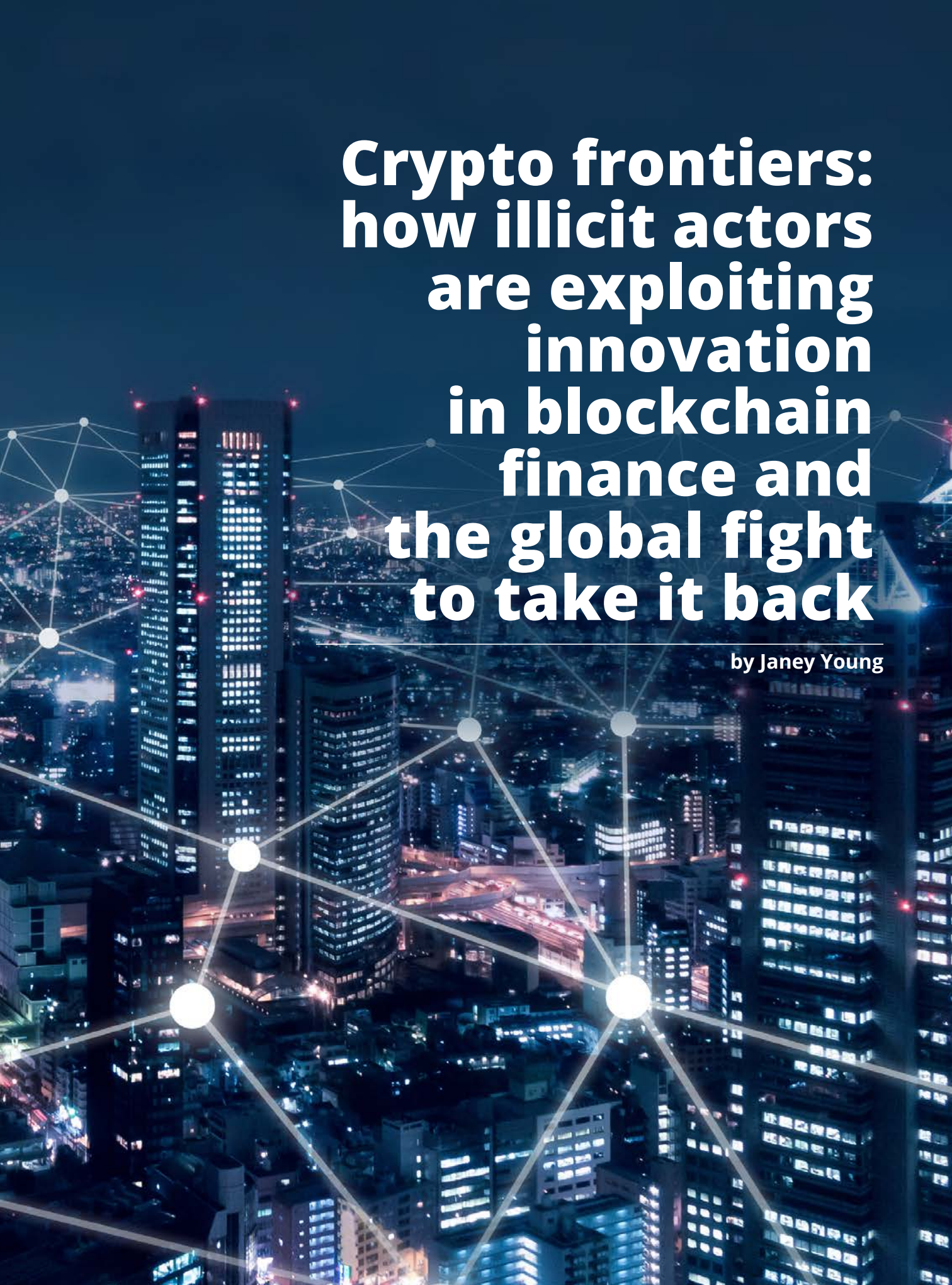
Crypto frontiers: how illicit actors are exploiting innovation in blockchain finance and the global fight to take it back

by Janey Young



The rise of blockchain technology has unlocked unprecedented opportunities in global finance. What began with Bitcoin has now evolved into a diverse digital ecosystem powered by decentralized networks like Ethereum, Polygon, Solana, and others. These platforms have laid the foundation for a wave of innovation — from decentralized finance (DeFi) to non-fungible tokens (NFTs) — promising more accessible, transparent, and efficient financial systems.

But as with many transformative technologies, the same features that drive progress can also invite abuse. Criminal groups are rapidly adapting, exploiting blockchain's decentralized and pseudonymous architecture to commit fraud, launder money, and evade law enforcement — presenting new and complex challenges to global security and governance.

Decentralization's double-edged sword

At its core, blockchain offers transparency and immutability. Every transaction is recorded on a public ledger, visible to anyone with Internet access. However, the decentralization that makes blockchain powerful also makes it difficult to regulate. Without intermediaries like banks or payment processors, there are fewer gatekeepers to monitor activity or flag suspicious behaviour. This appeals not only to technology enthusiasts but also to money launderers, cybercriminals, and fraudsters.

In particular, DeFi — blockchain-based financial services that operate without intermediaries and enable activities such as trading, borrowing, and lending, among others — has emerged as fertile ground for exploitation. Many operate without full know-your-customer (KYC) verifications, allowing users to interact anonymously or pseudonymously. The result is an ecosystem where significant funds can move at pace and across borders with limited oversight.

Vulnerabilities in decentralized finance: innovation meets exploitation

While DeFi's open-source ethos drives innovation, it also creates serious vulnerabilities. Weaknesses include poorly audited smart contracts, flawed governance mechanisms, and the manipulation of price oracles and liquidity pools. The ability to launch rapid, high-impact attacks has become a defining risk within the DeFi ecosystem. Exploits such as reentrancy attacks — where funds are repeatedly withdrawn from a smart contract before balances can update — or the distortion of data feeds to falsify asset

values illustrate the systemic risks. Inadequately secured platforms further expose users to malicious actors who may seize control of operations, leading to financial losses, service disruptions, or outright theft.

Among the most concerning methods exploiting these vulnerabilities are flash loan attacks. Flash loans enable users to borrow vast sums without collateral, provided the loan is repaid within the same transaction. Because these attacks can unfold in seconds, bypassing conventional fraud detection, criminals have used them to manipulate asset prices or drain liquidity pools. In some instances, attackers have even leveraged flash loans to gain temporary control of governance tokens, allowing them to force through malicious proposals — such as transferring treasury funds to their own wallets — before the broader community can respond.

Non-fungible tokens: digital art or digital laundering?

NFTs have captured popular imagination as digital collectibles and artworks, from meme coins to celebrity-endorsed avatars. But beneath the surface, they also present new opportunities for abuse. Criminals can mint NFTs, then engage in 'wash trading' — selling them to themselves using illicit funds. They can then offload them to unsuspecting buyers, effectively laundering money through digital art. This risk is compounded as many NFT marketplaces lack strong identity verification or compliance mechanisms.

Furthermore, 'rug pulls' have become a recurring threat, where developers of 'meme' tokens — a type of cryptocurrency created largely as a joke or Internet trend, whose value is driven by online hype rather than real-world use — vanish after securing investor funds. A high-profile example is the 2021 Squid Game (SQUID) token scam, in which the creators drained all liquidity and disappeared, leaving

investors with worthless tokens.[1]

Obscuring the trail: mixers, tumblers, and privacy coins

To further mask their tracks, illicit actors often turn to transaction-obfuscating services known as mixers or tumblers. These tools blend different users' transactions, making it harder to trace individual fund flows. Others rely on privacy-focused cryptocurrencies like Monero, which are designed to resist tracking altogether. While all these tools have legitimate privacy use cases, they are increasingly flagged by regulators as high-risk, and several cryptocurrency mixers have been sanctioned or dismantled in global efforts to stem illicit activity.

The myth of the untraceable blockchain

Despite these challenges, the belief that crypto transactions are untraceable is a misconception. Public blockchains, by design, maintain a transparent record of all activity, allowing investigators to follow the digital money trail with growing sophistication.

> **Despite these challenges, the belief that crypto transactions are untraceable is a misconception**

Blockchain forensics tools have become essential in modern law enforcement, enabling agencies to trace complex transaction chains across networks. As these tools evolve, they are helping expose criminal networks and recover stolen funds.

A united front: international and industry collaboration

Addressing the dark side of crypto requires global coordination. Initiatives such as the Egmont Group's information-sharing among Financial Intelligence Units (FIUs)[2] and INTERPOL's Global Complex for Innovation[3] are strengthening cross-border efforts to investigate and disrupt criminal activity. Meanwhile, the Financial Action Task Force (FATF) continues to refine its guidance on virtual assets, urging Member States to adopt clear and robust regulatory frameworks.[4] In response, many jurisdictions are integrating these standards into national legislation, clarifying compliance obligations and boosting their capacity to monitor digital financial crime. Building on these efforts, the private sector plays a vital role in countering crypto crime. Blockchain analytics firms are evolving their technologies to keep pace with threats, deploying tools to trace illicit transactions across decentralized and often opaque networks. Through close cooperation with law enforcement, cryptocurrency exchanges — platforms where digital assets are bought, sold, and traded — and other industry stakeholders are helping to secure vulnerabilities and identify, investigate, and disrupt suspicious activity in real time. Furthermore, many exchanges are now proactively freezing wallets tied to criminal activity and reinforcing compliance to align with international standards, contributing to a more secure digital asset ecosystem.

1 Chris Stokel-Walker, "How a Squid Game Crypto Scam Got Away With Millions", Wired, November 2021.
2 "The Egmont Group of Financial Intelligence Units", Financial Crimes Enforcement Network.
3 "INTERPOL Innovation Centre".
4 "FATF Urges Stronger Global Action to Address Illicit Finance Risks in Virtual Assets", FATF, June 2025.

Striking the balance: innovation without impunity

Policymakers face a delicate balancing act: how to foster innovation without opening the floodgates to exploitation. Overregulation could stifle progress and push activity underground. Underregulation and criminal misuse become inevitable.

Ongoing dialogue is critical between governments, industry leaders, technologists, and civil society. So is public education. Many users remain unaware of the risks associated with DeFi platforms and NFTs. Promoting digital literacy, responsible platform design, and stronger consumer protection can empower individuals and reduce the impact of fraud.

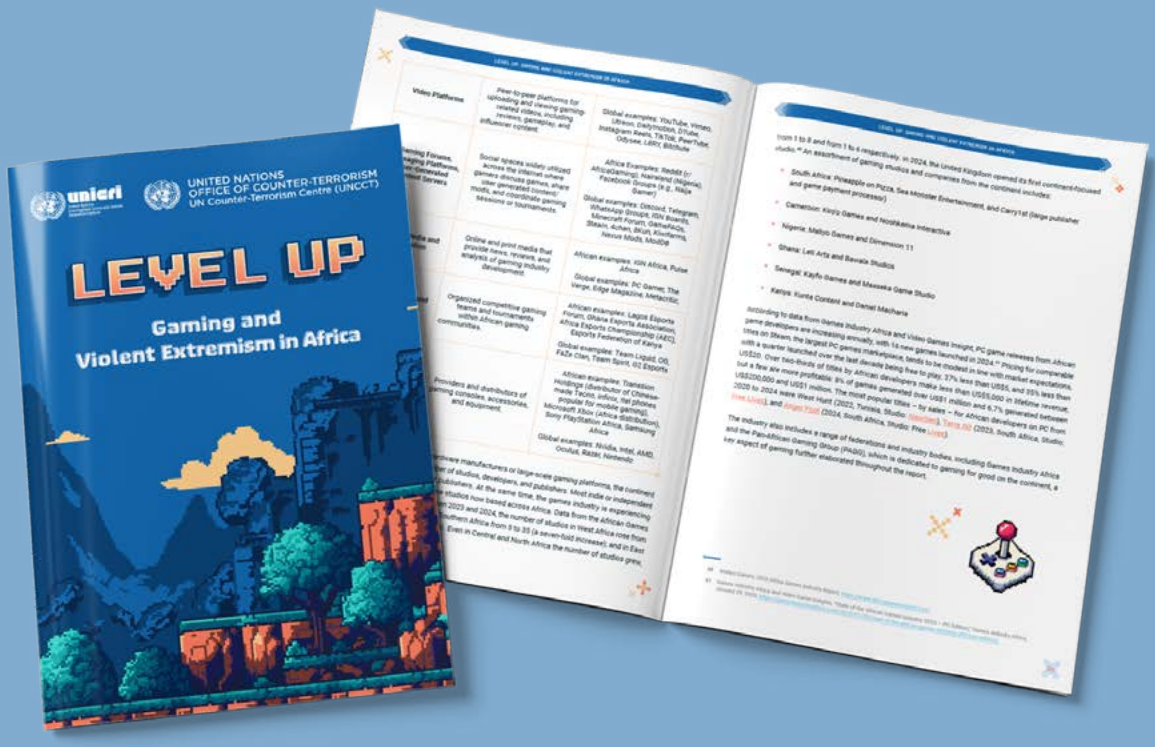
Looking forward: a safer digital finance future

The frontier of blockchain finance is expanding rapidly, and so is its misuse. As decentralized systems continue to reshape global finance, the international community must act decisively to secure this space.

The international community must stay ahead of the curve. Through agile regulation, shared intelligence, and continued investment in investigative tools, we can disrupt illicit activity while preserving the transformative potential of blockchain. Only then can we ensure that this technology serves the cause of global peace, economic resilience, and inclusive development.

ABOUT THE AUTHOR

Janey Young is the Founder and Principal Consultant of Safe Digital Futures, advising organizations on cybercrime, risk management, and responsible innovation. Her career includes leading cybercrime investigations at the UK's National Crime Agency and Europol's European Cybercrime Centre, where she pioneered strategies against threats like NotPetya and dark web activity. Most recently, as Head of Global Investigations at Chainalysis, she built internationally recognized capabilities using blockchain, AI, and advanced analytics to strengthen compliance and investigative solutions worldwide.



Download UNICRI publications