WNS
Part of Capgemini

The Crypto Investigation Gap
A New Mandate for Blockchain Intelligence

Sandeep Chakravadhanula
Practice and Capability Lead – Financial Crimes, Banking & Financial Services

The cryptocurrency revolution has fundamentally transformed how value moves across borders. What began as an experimental technology has evolved into a multi-trillion-dollar ecosystem.

McKinsey estimates tokenized assets alone will total between USD 1-4 Trillion by 2030, encompassing everything from stablecoins and Non-Fungible Tokens (NFTs) to Decentralized Finance (DeFi) tokens and tokenized real-world assets.[1]

Yet this transformation has brought a troubling reality, with traditional financial crime investigation methods proving inadequate for the crypto era.

For organizations operating in the cryptoasset space, the pressure is on. The Financial Action Task Force (FATF) reports that there was a total of USD 51 Billion in illicit crypto activity tied to fraud and scams in 2024 alone.[2] Regulators worldwide are tightening compliance requirements, while sophisticated criminals exploit blockchain's unique characteristics to mask illicit activity. The result is a widening gap between regulatory expectations and operational capabilities, putting organizations at serious risk.

Promisingly, this pressure is fueling innovation, with a new generation of Artificial Intelligence (AI)-powered blockchain analytics, real-time monitoring systems and specialized expertise emerging to bridge this gap. Leading institutions are also re-imagining their financial crime operating models to embed blockchain intelligence into core compliance workflows. In doing so, these organizations are proving that sophisticated blockchain investigation capabilities can deliver both regulatory confidence and operational efficiency, transforming what was once an insurmountable compliance burden into a strategic advantage.

[1]From Ripples to Waves: The Transformational Power of Tokenizing Assets | McKinsey & Company
[2]FAFT Urges Stronger Global Action to Address Illicit Finance Risks in Virtual Assets | The FATF

A Critical Inflection Point for Blockchain Intelligence

At present, several factors are converging to create a perfect storm for those operating in the cryptoasset space when it comes to financial crime, including exploding transaction volumes, evolving global regulations and increasingly sophisticated criminal activity.

In 2025, Anti-Money Laundering (AML) and compliance penalties topped USD 1.1 Billion globally, with crypto exchanges being fined USD 927.5 Million.[3] Recent research, meanwhile, shows that despite 99 jurisdictions having enacted Travel Rule frameworks requiring businesses to collect, verify and share information about cryptoasset transfers, over 70 percent remain only partially compliant with full FATF requirements.[4]

Unlike banking transactions tied to verified identities, crypto transactions are linked to pseudonymous wallet addresses that shield participants' identities. Although traditional transaction monitoring systems can detect trigger events, they fall short on the investigative heavy lifting required in crypto contexts, demanding specialized knowledge of blockchain technology, transaction tracing methodologies and attribution techniques that most institutions simply don't possess in-house.

The compliance challenge alone is immense. **The financial industry detects only about 2 percent of global financial crime flows despite banks commonly assigning 10 to 15 percent of their full-time equivalents to Know Your Customer (KYC) / AML activities alone.**[5] The gap between effort and effectiveness reflects the sophistication of modern money laundering, which increasingly exploits digital payment rails and blockchain networks that require specialized forensic analysis to trace effectively.

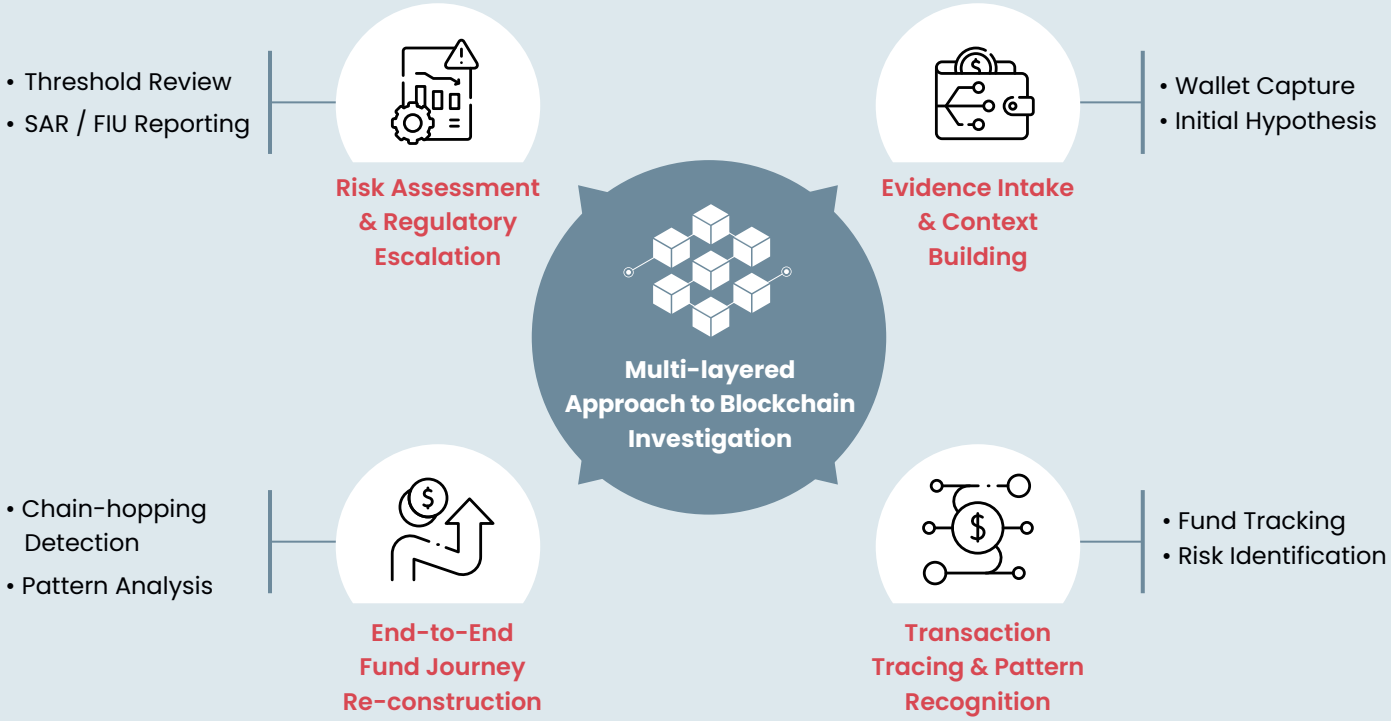
However, challenges extend far beyond technical capabilities. Investigators face inherent ecosystem limitations, from the non-existence of unified global laws and regulations to the proliferation of mixers and tumblers designed to obscure transaction trails, chain-hopping across multiple blockchains to evade detection and the persistence of unregulated exchanges operating in high-risk jurisdictions. Even the most sophisticated blockchain intelligence tools have coverage gaps, and many investigations remain inconclusive due to these structural barriers.

[3]AML/CFT and Sanctions Enforcement Actions in 2025 |Institute for Financial Integrity
[4]Global Crypto Regulation Report 2026 | PwC
[5]How Agentic AI Can Change the Way Banks Fight Financial Crime | McKinsey & Company

Re-imagining Blockchain Investigations Through a Multi-layered Approach

So, how can organizations successfully overcome these challenges and re-imagine their investigation capabilities?

First and foremost, a multi-layered approach that combines technology, process expertise and specialized domain knowledge is required. Firms need more than software and digital tools; they need analysts who understand both technology and the criminal methodologies that exploit them.



Advanced Blockchain Technology

- AI-powered Analytics
- Cross-chain Visibility
- Risk Scoring Models

Process & Governance Controls

- Standardized Workflows
- Case Documentation
- Audit Readiness

Specialized Domain Expertise

- Certified Crypto Investigators
- Financial Crime Methodology

This balance between human expertise and digital tools can ensure blockchain investigations follow a rigorous process. Analysts gather initial datasets from known crypto addresses, whether they belong to scammers or victims, and collect comprehensive evidence documenting *who, what, when, where and why*. Next come transaction tracing and pattern recognition, which require mastery of blockchain intelligence platforms to track fund movements and identify high-risk exchanges.

Transaction analysts then trace the complete journey of funds from origin to destination. Throughout this process, investigators build detailed, chronological case notes that document red flags and suspicious patterns. Finally, if evidence meets regulatory thresholds, reports are filed with the relevant country's Financial Intelligence Unit (FIU).

Building Investigations That Are Crypto-Intelligent by Design

Such multi-layered models can be built through capabilities that align directly with the investigative lifecycle. Customer onboarding and due diligence services, for example, establish strong foundations for risk control through KYC, Customer Identification Programs (CIP) and sanctions screening. Transaction monitoring can facilitate ongoing investigations and support the preparation of Suspicious Activity Reports (SARs).

For more complex cases, advanced tracing capabilities that leverage blockchain analytics, cross-chain investigations, risk-scoring models and transaction tracing methodologies to surface hidden flows will be required. Critically, rigorous documentation and standardized workflows throughout this process strengthen both audit readiness and cross-border compliance, providing the regulatory defensibility that institutions need when operating across multiple jurisdictions.

Together, these capabilities allow institutions to run comprehensive, well documented and crypto intelligent investigations from the start. However, finding the right blend of financial crimes expertise, crypto asset investigation certifications, premium blockchain intelligence platforms and operational capacity represents a challenge in and of itself. Change, however, is coming fast.

Emerging technologies, for instance, are already demonstrating impact, with 64 percent of organizations using compliance technology reporting better visibility of risks and risk management activities, and 53 percent achieving faster identification and response to compliance issues.[6]

On the regulatory front, meanwhile, we see organizations like the Monetary Authority of Singapore driving innovation by introducing clear, practical frameworks for assessment that mark a critical evolution in how financial institutions approach cryptoassets.[7]

[6]Global Compliance Survey 2025 | PwC
[7]Industry Perspectives on Best Practices for Source of Wealth Due Diligence | Monetary Authority of Singapore

Accelerating Capability Through Strategic Partnerships

The blockchain investigation landscape will only grow more complex as the crypto ecosystem matures and regulators intensify their scrutiny. Organizations that fail to develop robust capabilities risk regulatory sanctions, reputational damage and unwitting involvement in financial crime. Those that succeed will do so by combining strategic vision with operational excellence, whether built internally or accessed through partnership.

The right partnerships can enable instant access to battle-tested frameworks and deep experience. Effective partnerships combine certified crypto investigators with proven expertise, global delivery capabilities to support operations across time zones and jurisdictions, integrated risk-scoring frameworks that enhance detection accuracy and optimized case management systems that streamline workflows.

It also means access to enterprise-grade blockchain intelligence platforms and end-to-end support.

Firms, whether crypto exchanges, FinTechs or Virtual Asset Service Providers (VASPs), can work with partners to co-create investigation models and future-ready frameworks that combine human expertise with advanced analytics, enabling faster case resolution, sharper detection of illicit behavior and stronger oversight across jurisdictions. This combination of advanced technology and hands-on experience can deliver striking efficiency gains and empower organizations to embrace a new era for blockchain-based investigations.

It's a future that is rapidly taking shape, with innovative collaborations proving that compliance and efficiency are not mutually exclusive. HSBC's Tokenised Deposit Service is one such example, using distributed ledger technology to support instant settlement for remittance and payments.[8]

[8]Ant International is the First to Use Our Tokenised Deposit Service | HSBC

From Compliance Burden to Strategic Advantage

The question is no longer whether to invest in sophisticated blockchain investigation capabilities, but how quickly organizations can close the gap between regulatory expectations and operational reality. The future belongs to intelligence-driven, scalable and AI-enabled investigation models that combine advanced analytics with deep domain expertise. In this high-stakes environment, those who thrive will recognize the unique demands of blockchain investigations and harness the specialized expertise, technology and processes needed to meet them head-on.

Re-imagine your blockchain investigation operating model. Explore how leading institutions can embed AI, governance and domain expertise to scale crypto-intelligent compliance.

About WNS

WNS, part of Capgemini, is an Agentic AI-powered intelligent operations and transformation company. We combine deep domain expertise with talent, technology, and AI to co-create innovative solutions for over 700 clients across various industries. WNS delivers an entire spectrum of solutions, including industry-specific offerings, customer experience services, finance and accounting, human resources, procurement, and research and analytics to re-imagine the digital future of businesses. WNS has 66,085 professionals across 65 delivery centers worldwide, including facilities in Canada, China, Costa Rica, India, Malaysia, the Philippines, Poland, Romania, South Africa, Sri Lanka, Turkey, the United Kingdom, and the United States.

To know more, write to us at **marketing@wns.com** or visit us at **www.wns.com**

WNS
Part of Capgemini