FINANCIAL INTEGRITY HUB INSIGHTS

Virtual Assets & Virtual Asset Service Providers

June Issue 2025

FINANCIAL INTEGRITY HUB

MACQUARIE University
SYDNEY·AUSTRALIA

ISSN: 2982-3188

LEADERSHIP

Patron
Honourable Patricia Bergin AO SC

Director
Associate Professor Doron Goldbarsht

Associate Director
Isabelle Nicolas

Advisory Board
Armina Antoniou
Professor Louis De Koker
Paul Jevtovic APM OAM
Professor Elizabeth Sheedy
Michael Tooma
Stuart Clark AM (d. June 2025)

Reference Group
Sue Bradford
Jeremy Moller
Tony Prior

Research Fellows
Dr Mirella Atherton
Dr Daley Birkett
Dr Derwent Coshott
Dr Jamie Ferrill
Dr Hannah Harris

Researchers
Giang Nguyen
Ben Scott

Interns
Soha Khan
Benjamin Mensah
Jade Reuveny
Dana Schmidt

Citing reference: Financial Integrity Hub 'FIH Insights' (2025) 1(2) FIH, Sydney
<https://www.mq.edu.au/research/research-centres-groups-and-facilities/groups/financial-integrity-hub/engagement>.

ABOUT US

The Financial Integrity Hub (FIH) is a leading research center dedicated to financial crime prevention and mitigation. Our mission is to foster collaborative partnerships that strengthen research, policy, and practice, ensuring a robust and resilient financial system.

At FIH, we actively engage with academia, government, and industry to develop innovative, evidence-based solutions that address the complexities of financial crime. Our research is designed not only to advance academic understanding but also to influence regulatory frameworks, enhance enforcement strategies, and shape industry best practices.

By bridging the gap between theory and real-world application, we contribute meaningfully to financial integrity, compliance effectiveness, and policy reform. Through thought leadership and collaborative dialogue, we strive to create a more transparent, accountable, and secure financial landscape.

We extend our appreciation to our authors and contributors, whose expert insights and analyses allow us to deliver timely updates, valuable perspectives, and thought-provoking content to our readers.

Together, we can drive progress in the fight against financial crime and work towards a stronger, more resilient financial system.

CONTACT US
Financial Integrity Hub
Michael Kirby Building Macquarie University
NSW 2109, Australia
E: fih@mq.edu.au T: +61 (2) 9850 7074

Follow us here:

We thank our partner, WhiteLight AML, for their support. Since 2019, WhiteLight AML has been Australia's trusted partner in navigating the complexities of AML and CTF. Specialising in risk assessments and tailored AML/CTF programs, they ensure comprehensive compliance. With fully outsourced AML/CTF operations, they take the burden off your shoulders, allowing you to focus on what you do best!

TABLE OF CONTENTS

THE ANNUAL FINANCIAL INTEGRITY HUB FINANCIAL CRIME SYMPOSIUM

Image: ASUTRAC CEO Brendan Thomas delivering a key note speech at the 2025 Financial Integrity Hub Financial Crime Symposium

The 2025 Financial Integrity Hub Financial Crime Symposium opened with a powerful keynote by AUSTRAC CEO Brendan Thomas, who highlighted AUSTRAC's strategic leadership in combating money laundering, terrorism financing, and proliferation financing.

Throughout the day, leading experts shared insights across key panels:

- **The Impact of Financial Crime on Society:** A compelling discussion with Colm Gannon, Dr Hannah Harris, Holly Miller, Paul Jevtovic APM OAM, and Timothy Goodrick, exploring how financial crime erodes public trust and impacts everyday lives.
- **Tranche 2 Reforms:** Featuring Dan Mossop, Neil Russ, Alice Bexson, Albert van Zy, and Jeremy Moller, this panel addressed regulatory changes and the critical role of gatekeeper professions in AML/CTF frameworks.
- **Emerging Risks and Reputational Impact:** Armina Antoniou, Christopher Kerrigan, and Prof. Elizabeth Sheedy examined evolving threats and the growing need for organisations to manage reputational risk proactively.
- **Financial Crime, Fraud, Scams, and Technology:** Experts, including John Fogarty, David O'Mahony, Ben Scott, Tim Dalgleish, and Sue Bradford, analysed how technology is both a tool for criminals and a key to prevention.
- **Navigating Proliferation Financing:** David Shannon, Claudine Lamond., and Prof. Louis De Koker provided in-depth analyses of PF threats, highlighting global obligations and compliance challenges.
- **Terrorism Financing:** With Stephen Dametto, Prof. Dotan Rouso, Prof. Julian Droogan, and Simone Abel, this panel provided perspectives on how terrorist groups fund operations and how law enforcement can respond.

A big thank-you to all speakers, the Crown Resorts for our ongoing partnership, and attendees for a day full of passionate dialogue, expert insights, and meaningful engagement in the fight against financial crime.

VIRTUAL ASSET SERVICE PROVIDERS UNDER AUSTRALIA'S REFORMED AML/CTF REGIME

On 29 November 2024, the Parliament of Australia passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill* 2024 (the Bill), amending the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (AML/CTF Act). The Bill received Royal Assent on 10 December 2024 and became the *AML/CTF Amendment Act* 2024 (Amendment Act).

The new laws modernise and strengthen Australia's AML/CTF regime to ensure it continues to effectively deter, detect, and disrupt money laundering, terrorism financing, and proliferation financing. As part of this reform, the terms "digital currency" and "digital currency exchange" have been replaced with "virtual asset" and "virtual asset service provider" (VASP), aligning with the terminology used by the Financial Action Task Force (FATF) and reflecting developments in the digital asset sector. The updated definition of virtual asset now encompasses emerging forms of assets, such as non-fungible tokens (NFTs) that function as a medium of exchange or investment, as well as governance tokens used to regulate participation in decentralised autonomous organisations.

The reformed regulatory framework expands coverage beyond traditional exchanges between virtual assets and fiat currency. It now also captures transactions involving the exchange of one virtual asset for another (including those of the same kind), the transfer of virtual assets between individuals, the safekeeping or custodianship of virtual assets and private keys, and financial services offered in connection with the issuance or sale of virtual assets. This includes services such as accepting funds or purchase orders, underwriting, market-making, and acting as a placement agent in relation to initial coin offerings and similar arrangements.

These changes ensure that Australia's AML/CTF regime remains responsive to the risks associated with a rapidly evolving and increasingly mainstream financial sector. They also bring the Australian legal framework into closer alignment with international standards, particularly those developed by the FATF.

The articles in this June edition of *FIH Insights* feature contributions from leading global experts exploring the ongoing reform of virtual asset and VASP regulation. Together, they examine the opportunities and challenges posed by the expanding role of virtual assets in financial systems and offer valuable comparative perspectives from multiple jurisdictions. From legal reform and regulatory design to enforcement and supervision, this edition provides timely insights and practical lessons for policymakers, regulators, and industry stakeholders committed to strengthening financial integrity in the digital age.

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS: GAPS CONTINUE TO ENABLE CRIMINAL ABUSE

Louis de Koker

Globally, countries are making slow progress in implementing the Financial Action Task Force's (FATF) standards for Virtual Asset Service Providers (VASPs). Yet even full implementation would be insufficient to address the illicit use of virtual assets.

In 2018, FATF adopted new standards requiring jurisdictions to ensure that VASPs - businesses that administer or assist in the exchange or transfer of virtual assets and fiat currencies, or between different forms of virtual assets- are licensed or registered and are subject to AML/CTF supervision. Where this is not feasible, jurisdictions are expected to prohibit their operation.

In June 2024, FATF reported that while some jurisdictions had made progress in introducing AML/CTF regulations, global implementation remained patchy. Of the 147 jurisdictions that responded to an FATF survey in April 2024, 42 had not yet conducted a virtual asset risk assessment. Furthermore, more than a quarter of respondents (27%, or 39 out of 147) had not yet determined whether or how they would regulate the VASP sector. This picture had not changed significantly by 2025.

Where VASP measures have been implemented, their scope remains limited. The FATF's regulatory approach is based on a nation-state model that worked well in the 20th century, when bricks-and-mortar financial institutions had a clear geographic presence. Jurisdictional and enforcement questions rarely arose. By contrast, VASPs operate in the digital space and are often decentralised. Identifying a single jurisdiction for the regulation and enforcement of a VASP is not always straightforward. For years, for example, it was unclear where Binance, the world's largest cryptocurrency exchange, was headquartered.

FATF uses long-standing, practical tests to determine whether a business operates in a specific jurisdiction. The so-called "mind and management" tests focus on where the board meetings take place and the corporate records as held. Those tests are not particularly helpful in relation to VASPs that operate in cyberspace. While countries can extend their laws to cover foreign VASPs, enforcing compliance becomes difficult, especially for jurisdictions without the extraterritorial enforcement traditions and powers of the United States. The challenge is even greater when the VASP is not a legal entity in the traditional sense, but a decentralised autonomous organisation (DAO), an arrangement governed partially or wholly by code, with governance and financial transactions managed through decentralised ledgers such as blockchains.

The most significant regulatory gaps, however, relate to unhosted wallets and person-to-person (P2P) transactions.

Financial regulation typically focuses on service providers, not users. Yet virtual assets were designed to be exchanged directly between users, without the need for service providers as intermediaries. This means P2P trading falls outside the scope of traditional financial regulation, including FATF VASP standards. While VASP services are popular for reasons such as convenience, many users continue to rely on unhosted wallets. Some may only use a VASP to convert virtual assets to fiat currency.

In 2021, FATF engaged seven blockchain analytics companies to estimate the prevalence of P2P transactions. Using their own methodologies, three of these firms concluded that approximately 60% of all transactions between 2016 and 2020 - representing more than 50% of total traded value - were P2P. Crucially, they also found that most identified illicit transactions, particularly those of higher value, occurred outside the VASP framework.

In many cases, efforts to combat financial crime do not eliminate it but instead displace it. AML/CTF measures targeting traditional financial systems, for instance, have driven criminal proceeds into virtual asset markets, thereby prompting the need for virtual asset regulation. Similarly, regulation of VASPs risks pushing illicit activity into the unregulated P2P space, beyond the reach of existing compliance frameworks. It would be reasonable to expect urgent action to mitigate this risk.

Yet, despite the scale and risks of P2P activity, FATF noted in 2024 that:

"[E]ven amongst jurisdictions with more advanced VASP regulations (i.e., those that have passed legislation implementing the Travel Rule for VASPs or are in the process), the majority of respondents (64%; 51 of 80) have not yet evaluated or started evaluating the specific risks related to self-hosted wallets or P2P transactions. Data gaps remain as a main challenge, as noted by many jurisdictions." (Paragraph 61)

The lack of action to assess and address the criminal misuse of unhosted wallets and P2P transactions is concerning, particularly in light of 2021 research highlighting their significant role in illicit activity. Strengthening the walls of the fortress is essential, but doing so while leaving the main gate wide open and the portcullis raised makes little sense.

Professor Louis de Koker, Professor at La Trobe Law School and Advisory Board Member of the Financial Integrity Hub.

VIRTUAL ASSETS AND FINANCIAL CRIME: A CALL FOR AGILE AND SMARTER GLOBAL REGULATION

Katherine Shamai

Introduction

Throughout history, societies have assigned value to various materials for trade; from bartering grains and livestock to using precious metals, paper currency, and credit systems. Although cryptocurrency has existed for nearly two decades, it continues to present regulatory challenges. Given the rapidly evolving nature of virtual assets (VAs) and the pace of technological advancement, can regulatory frameworks keep pace with the associated risks of money laundering, terrorism financing, and proliferation financing?

Origins of Virtual Assets

Bitcoin, introduced by Satoshi Nakamoto in 2008, leveraged blockchain technology to enable peer-to-peer transactions secured through cryptographic consensus. This innovation marked a significant milestone in digital value exchange by establishing trust without intermediaries.

Subsequent innovations expanded on this concept, such as:

- Ethereum introduced programmable smart contracts.
- Privacy-focused coins like Monero, ZCash, and Dash offered built-in anonymity.
- Non-fungible tokens (NFTs) which enabled unique digital ownership of assets like art, music, and virtual real estate
- Decentralized finance (DeFi) introduced new mechanisms for virtual value transfer without intermediaries.

These innovations, while transformative, also introduced new financial crime risks due to their decentralised and pseudonymous nature.

As new VA types emerged, so did virtual asset service providers (VASPs), offering platforms for cryptocurrency exchange, trading, transfers, and digital wallets. VASPs are typically regulated based on their jurisdiction, and due to inconsistent global standards and varied implementation of FATF guidance, regulatory scrutiny and transparency differ significantly across regions.

Emerging Trends in the Virtual Asset Ecosystem

Decentralised Finance (DeFi) and Decentralised Exchanges (DEXs)

DeFi and DEX platforms enable users to trade, lend, and hold VAs without centralised oversight. While efficient, their permissionless and pseudonymous nature facilitates regulatory evasion and misuse for illicit purposes. Regulatory influence is most feasible at the entry and exit points of DeFi ecosystems. As these platforms attract more mainstream investors, the influx of legitimate funds complicates the identification of illicit activity and regulatory enforcement.

Tokenisation of Real-World Assets
Tokenizing traditional assets, such as real estate and government bonds, enhances liquidity and transparency but introduces regulatory ambiguity. Hybrid models combining VAs with conventional custodianship challenge traditional financial frameworks, especially when assets are not backed by central banks or fiat currencies. For instance, in Australia, some real estate transactions now accept cryptocurrency, increasing placement and layering risks from a financial crime perspective.

Privacy-Enhancing Technologies (PETs)
Technologies like blockchain mixers (e.g., Tornado Cash) and zero-knowledge proofs obscure transaction trails. While these tools support privacy rights, they are increasingly exploited by malicious actors. Such technologies conflict with AML/CTF objectives and can significantly hinder regulatory oversight and detection efforts.

Stablecoins and Central Bank Digital Currencies (CBDCs)
Stablecoins offer price stability for transactions and remittances but often lack clear regulatory oversight. In contrast, CBDCs provide state-controlled alternatives with embedded compliance mechanisms. Both forms of VAs are gaining traction as perceived safer alternatives to more volatile cryptocurrencies.

Proliferation Financing Risks
Reports from RUSI (2021) and FATF (2024) highlight North Korea's use of VAs to circumvent sanctions and acquire dual-use goods. Exploiting weak enforcement, state-affiliated actors launder stolen crypto through DeFi platforms and peer-to-peer networks.

Regulatory Challenges

FATF Framework and the Travel Rule
In 2019, FATF extended its Recommendations to include VASPs, mandating customer due diligence (CDD), suspicious transaction reporting, and compliance with the Travel Rule (Recommendation 16), which requires VASPs to share identifying information for transactions exceeding a specified threshold. In Australia, the AML/CTF regime has been extended to services provided by VASPs, including the travel rule obligations, as part of upcoming reforms set to commence on 31 March 2026. The effectiveness of these measures will depend on how reporting entities adapt, implement the obligations, and the quality of data collection and reporting.

Fragmented Global Implementation
While countries like Japan and Singapore have adopted stringent licensing regimes, many others lag behind. This regulatory disparity enables "jurisdictional arbitrage," where illicit actors relocate operations to less-regulated regions. Startups often engage in "jurisdiction shopping" to find favorable regulatory environments with minimal oversight or inactive regulators.

Supervision and Enforcement Gaps
VASPs, often operating virtually and across borders, challenge traditional supervisory models. Few financial intelligence units (FIUs) and law enforcement agencies possess the blockchain analytics capabilities needed to trace transactions and assess risk networks at scale. These gaps are exacerbated by limited regulatory authority and enforcement capacity, as well as constraints regarding international police cooperation and cross-border information exchange.

Beyond AML: Cyber and Proliferation Risks
Financial crime tools and typologies often overlap. The misuse of VAs intersects with ransomware, fraud, and state-sponsored cyberattacks. These typologies span multiple blockchains, asset classes, and jurisdictions, complicating investigations and necessitating cross-border collaboration.

insufficient Investment in ML/TF Controls by VASPs
Many VASPs, particularly startups, lack robust AML/CTF expertise. This results in poorly designed controls and unmitigated ML/TF risks. There is often little incentive to invest in compliance, as it may conflict with customer expectations. For example, in a past engagement with a now-insolvent crypto exchange, analysis revealed that customer due diligence was not prioritised, complicating efforts to repatriate wallets without breaching AML/CTF obligations or inadvertently facilitating money laundering.

Call to Action: The Case for Smarter Regulation

Global Harmonisation of Standards
Consistent implementation of FATF's VA standards is essential. Regional bodies like the EU and Asia-Pacific Group (APG) should emphasize Travel Rule enforcement and mutual evaluation preparedness to close regulatory gaps. In Australia, the effectiveness of Travel Rule implementation and AUSTRAC's enforcement will be critical, and poses a challenge for reporting entities to implement.

Enhancing Supervisory Tools and Capabilities
Regulators must invest in blockchain forensics and transaction monitoring technologies. Given the scarcity of domain expertise, partnerships with RegTech firms may enhance oversight efficiency. The inclusion of VASPs in Australia's AML/CTF regime will require new supervisory competencies to assess VASP operations and associated ML/TF risks.

Strengthening Public–Private Collaboration
Initiatives such as the Joint Chiefs of Global Tax Enforcement (J5) and AUSTRAC's Fintel Alliance illustrate the value of cross-sector and cross-border intelligence sharing in identifying typologies and disrupting illicit networks.

Integrating Proliferation Financing Indicators
VASPs should expand their risk frameworks to include proliferation financing red flags, such as high-risk jurisdictions, NFT or metaverse-based layering, and open-source procurement networks. While proliferation financing will be incorporated into ML/TF risk assessments once the AML/CTF reforms is enacted, how reporting entities integrate these into their ML/TF/PF risk assessment remains to be realised. Historically, the level of proliferation financing awareness within reporting entities has been immature.

Conclusion
Virtual assets are reshaping the financial landscape. Without robust and harmonised global regulation, they risk undermining financial system integrity. The tools for misuse are sophisticated, rapidly evolving, and increasingly state-enabled. Regulatory responses must be equally advanced, collaborative, and global.

Regulators, VASPs, and technologists must work collaboratively to stay at the edge of technological developments and emerging VA products. Relying solely on existing standards will rapidly leave regulatory frameworks outdated. There is a pressing need for smarter and more agile regulation. The question is no longer whether virtual assets can be regulated. The question now is how regulators can do so intelligently, swiftly, and globally.

Katherine Shamai, Partner, Risk Consulting at Grant Thorton

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS: NAVIGATING CHALLENGES IN GLOBAL AML/CTF FRAMEWORKS

Janya Eighani

In recent years, the rapid evolution of digital technology has revolutionised the financial landscape, giving rise to a new class of assets known as virtual assets. These digital representations of value, which include cryptocurrencies (like Bitcoin and Ethereum) and other forms of tokens, issued on various blockchain platforms, have and continue to transform how individuals and entities conduct transactions worldwide. While virtual assets offer numerous benefits such as increased efficiency in time and costs, accessibility, and innovative financial products, they also pose significant regulatory challenges, especially in the realms of Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance.

This article attempts to examine, broadly, the nature of virtual assets and Virtual Asset Service Providers (VASPs), examines the regulatory gaps they expose, and discusses the pressing need for a cohesive international framework to address these challenges.

Understanding Virtual Assets and VASPs
Virtual Assets (VAs):
Virtual assets broadly refer to any digital representation of value that can be transferred, stored, or exchanged electronically. Unlike traditional currencies issued and regulated by Central Banks, virtual assets are often decentralised, operating on blockchain or distributed ledger technology (DLT). They enable peer-to-peer transactions without the need for intermediaries, offering new opportunities for financial inclusion and innovation and facilitate fast, low-cost cross-border payments and other financial transactions.

Types of virtual assets include:
- Cryptocurrencies
- Utility tokens
- Security tokens
- Stablecoins (digital tokens backed by fiat currency or assets)

lIt's important to note here that the simple description of the assets as one of the ones listed above, doesn't make it so in the eyes of the law. The structure, form and substance of the blockchain and the asset, as well as real-life use case, will determine how the asset is viewed in the eyes of the law and the regulators.

VASPs:
VASPs are entities that facilitate the exchange, transfer, or management of virtual assets. They encompass a broad spectrum of businesses, including:
- Cryptocurrency exchanges (decentralised or traditional)
- Wallet providers
- Custodians
- Initial Coin Offering (ICO) platforms
- Crypto ATMs

- Cryptocurrency brokers and OTC desks
- DeFi (Decentralised Finance) platforms

VASPs play a critical role in the virtual asset ecosystem, acting as intermediaries that connect the traditional financial world with the digital asset space and thus carry both the responsibility and liability of compliance

Challenges Posed by Virtual Assets to AML/CTF Frameworks

While virtual assets have revolutionised finance, they also introduced unique challenges for AML and CTF efforts:

1. A**nonymity and Pseudonymity:**

Many virtual assets can be transacted pseudonymously, masking the identities of the parties involved. Although blockchain transactions are transparent, linking these transactions to real-world identities remains complex, hindering enforcement efforts.

2. **Cross-Border Nature:**

Virtual assets operate seamlessly across borders, complicating jurisdictional authority and enforcement. This transnational feature often results in regulatory arbitrage, where illicit actors exploit lax regulations in certain jurisdictions.

3. **Rapid Innovation and Its Regulation:**

The fast-paced evolution of blockchain technology and financial products has outpaced regulatory responses. This creates gaps where VASPs often operate with minimal oversight.

4. **Difficulty in Tracking and Monitoring:**

The pseudonymity and technological complexity hinder the ability of authorities to track suspicious activities effectively, making virtual assets attractive for money laundering and terrorist financing as well as general tax avoidance.

I**nconsistent and Fragmented Global Regulations**

The diverse regulatory landscape around virtual assets exacerbates existing AML/CTF challenges, with different countries adopting varied approaches, resulting in significant compliance gaps, such as:

- Regulatory Clarity: Some jurisdictions, like Japan and the European Union, have established comprehensive regulations requiring VASPs to conduct customer due diligence (CDD) and report suspicious transactions, whilst more developing countries, lack specific regulations, creating safe havens for illicit activities.
- Licensing and Registration: VASPs in different regions face disparate licensing requirements. Inconsistent enforcement often leads to unlicensed operators that evade oversight.
- Compliance Responsibilities: VASPs are subject to varying obligations, including KYC and AML procedures, as well as data reporting standards, depending on jurisdictional mandates.

This fragmentation enables criminal entities to exploit regulatory disparities and loopholes, which undermines global AML/CTF efforts.

The Need for a Cohesive International Framework

Addressing the AML/CTF challenges posed by virtual assets requires international cooperation and harmonised standards. Several initiatives underscore this necessity:

- **Financial Action Task Force (FATF):**

FATF, the leading global AML/CTF standard-setting body, has issued guidance emphasising that VASPs should be subject to similar AML obligations as traditional financial institutions, including KYC procedures and transaction monitoring. The FATF's "Travel Rule" mandates VASPs to share information about the sender and recipient of virtual asset transfers to prevent illicit use.

- **International Cooperation:**

Coordination among regulatory authorities, law enforcement, and financial institutions is vital. Sharing intelligence, best practices, and technical capabilities enhances the capacity to identify and prosecute illegal activities involving virtual assets.

- **Developing Universal Standards:**

Establishing international minimum standards for VASP licensing, AML compliance, consumer protection, and cybersecurity is crucial, as such standards reduce regulatory arbitrage and create a level playing field.

- **Encouraging Blockchain Transparency and Innovation:**

Promoting transparency features within blockchain platforms, such as enhanced transaction traceability, can aid compliance efforts. Simultaneously, fostering responsible innovation, including privacy-enhancing technologies, ensures user protection without enabling illicit activities.

Future Outlook and Recommendations

The growing adoption of virtual assets makes it imperative for regulators and industry stakeholders to collaborate actively in closing the existing compliance gaps. Key recommendations include:

- Harmonise Global Regulations: International organisations like FATF should continue to refine and promote uniform standards for VASPs, ensuring consistent enforcement across jurisdictions.
- Strengthen VASP Licensing and Supervision: Countries should establish clear licensing regimes and robust supervisory frameworks to hold VASPs accountable and promote responsible operations
- Implement Robust Customer Due Diligence: VASPs must adopt comprehensive KYC/AML procedures, including verifying customer identities and monitoring transactions for suspicious activity.
- Enhance Cross-Border Cooperation: Law enforcement agencies and regulators should develop bilateral and multilateral cooperation mechanisms to track and combat illicit use of virtual assets effectively.
- Leverage Technology for Compliance: Employ advanced analytics, artificial intelligence, and blockchain analytics tools to improve monitoring, detection, and investigation of suspicious activities.
- Promote Transparency and Education: Providing education for users about virtual asset risks and promoting transparency within the ecosystem can help deter misuse.

Conclusion: Securing the Future of Finance

Virtual assets have transformed the financial ecosystem with their innovative promise of decentralised, efficient, and inclusive financial services, representing a paradigm shift in the financial ecosystem. However, their intrinsic features, namely pseudonymity, cross-border operation, and technological complexity, pose significant challenges to existing AML and CTF frameworks, much of which is playing catch-up and not fit-for-purpose, when it comes to tackling the innovative features of the digital assets ecosystem.

The current regulatory landscape, characterised by fragmentation and inconsistency, creates not only compliance gaps but is an invitation to criminal actors, including certain State actors, to exploit and undermine global security and financial stability.

To tackle these risks, international cooperation and harmonised standards are essential. Regulatory bodies, industry participants, and law enforcement must work together to develop adaptive and forward-looking frameworks that foster innovation whilst safeguarding the financial system against illicit use.

By advancing cohesive policies, leveraging technological advancements, and fostering international collaboration, the global community can harness the benefits of virtual assets while effectively combating their misuse. Addressing these challenges not only enhances the integrity of the virtual asset sector but also promotes a safer and more secure global financial environment for all participants, which combats not only criminal misuse of the system, but also plays an enormous role in protecting and safeguarding national security interests of nations as well as the stability of the international financial and security apparatus.

Janya Eighani, Managing Partner at Lehman Walsh Lawyers, Compliance and Financial Law

THE LEGAL COMPLEXITY OF SEIZING VIRTUAL CURRENCIES FOR FORFEITURE PURPOSES

Amit Levin

In recent years, virtual currencies have become a powerful tool used both in legitimate financial activity and by criminal actors. As assets such as Bitcoin and Ethereum gain widespread use, law enforcement agencies around the world face a fundamental challenge in the digital age: how can virtual assets, which by their nature are intangible, decentralised, and difficult to locate, be effectively seized and preserved?

The Challenge of Seizure in a Decentralised Era
Unlike traditional assets (bank accounts, vehicles, or real estate), virtual currencies are not managed by a central registry or controlling authority. In the classical financial world, courts can issue an order to a bank or a land registry to freeze or forfeit an asset. In decentralized blockchain networks, there is no intermediary. This absence of a "gatekeeper" necessitates new enforcement strategies that combine legal expertise with advanced technological tools. Seizing cryptocurrencies often requires sophisticated digital investigations, access to private keys, and international cooperation. Even so, law enforcement must act swiftly, as suspects can transfer funds in seconds, sometimes through mixers or privacy coins designed to obscure the transaction trail.

Volatility and Legal Risk: A Double-Edged Sword
Seizing digital assets is only the first step. Holding them exposes the state to additional legal risks. Virtual currencies are notoriously volatile. Their value can drop by 30% in a week or double within days. If a suspect is ultimately acquitted and their assets have depreciated while held by the state, a civil lawsuit may follow. On the other hand, if the state converts the assets into fiat and their value later rises, the suspect may claim financial damage that could have been avoided. This situation places prosecutors in a difficult position: should they preserve the asset in its original form and risk a claim for depreciation, or convert it to fiat and risk a claim for lost profits?

A Structured Response: The Protocol of the Israeli Cyber Unit

During my tenure as a senior prosecutor in the Cyber Unit of the Israeli Ministry of Justice, we encountered these dilemmas in practice. As the use of virtual currencies in criminal proceedings increased, we developed a standardized protocol to mitigate the legal exposure of the state. Based on rulings of the Israeli Supreme Court and the *Criminal Procedure Ordinance*, the protocol requires that within 24 hours of seizing virtual currencies, the prosecutor must contact the suspect's attorney and present two options:

1. Preservation: The assets may be held in their original digital form, provided the suspect signs a waiver of any future claims against the state for depreciation.
2. Conversion: The assets may be converted into fiat currency, provided the suspect signs a waiver of any claims should the value of the virtual currency increase later.

If the parties cannot reach an agreement, the matter must be brought before a court for judicial determination. The decision should balance the suspect's rights with the public interest. This approach promotes transparency and fairness, limits the state's exposure to civil liability, and ensures judicial oversight over the management of seized assets.

International Approaches: The U.S., Germany, and Beyond

Different countries have adopted varying strategies regarding the management of seized digital assets. In the U.S., for example, it is common for authorities to retain the assets in their original form. This avoids premature liquidation that could draw criticism if the value increases—but exposes the state if the value drops during the course of the proceedings.

In Germany, authorities have sometimes chosen to hold the assets for extended periods, in some cases profiting from their appreciation. However, this approach raises ethical and legal questions about state enrichment and opens the door to potential claims from suspects.

In the absence of unified standards, each jurisdiction must handle the issue independently. The Israeli model, based on either mutual consent or judicial determination, may offer a useful framework for balance.

Legal Asymmetry: The State vs. the Courts

A critical point to consider is that while the state can be sued for damages resulting from decisions regarding seized property, the courts in Israel cannot be held liable for judicial decisions.

This means that transferring the decision to a judge is not only a matter of transparency but also a way of appropriately allocating legal responsibility within the system.

Toward an International Standard: A Policy Proposal

The disparities between jurisdictions highlight the urgent need to establish international norms for managing seized virtual assets. Organisations such as the Financial Action Task Force (FATF) and the Egmont Group could help formulate recommended protocols, which might include:

- Clear timelines for decision-making regarding conversion of assets
- Mandatory waivers or consent forms from suspects
- Judicial oversight requirements
- Guidelines for valuation and proper documentation

Such standards would enhance legal certainty, ensure fairness to suspects, and facilitate international cooperation in cross-border cases involving virtual assets.

Conclusion: A Delicate Balance in a New World

Digital currencies have created a parallel financial system, one that does not align easily with traditional legal mechanisms. Seizing, holding, and forfeiting these assets requires a careful balance between efficiency, fairness, and technological sophistication.

The framework developed in Israel offers a practical response to these challenges, grounded in legal precedent and structured procedures. As more countries face similar issues, the next challenge may be to develop unified international policies that protect public interests while safeguarding individual rights in the evolving world of finance. This is not merely a matter of policy. It is a test of the legal system's ability to uphold justice in an age where value moves freely, but accountability must remain rooted in the law.

Amit Levin, Legal & Tech Advisor, Blockchain Investigator and Former Cybercrime Prosecutor

NFTS: ART, ASSET, OR MONEY LAUNDERING INSTRUMENT?

Mikayla Ozga and Christian Leuprecht

The digital art boom

The rise of non-fungible tokens (NFTs) has upended the art market and sparked a debate: are digital artworks simply collectible pieces, or do they function akin to stocks and investments? Since the mid-2010s, artists and collectors have embraced NFTs, unique digital tokens on blockchains that certify ownership of a piece of art, music, or other creative work. Growth in sales since 2021 has been exponential, with total NFT transactions reaching tens of billions of dollars. Major auction houses such as Christie's and Sotheby's got in on the frenzy, selling digital artworks for millions. One famous example: Christie's sold a Beeple NFT for $69 million. That same year Sotheby's and Christie's handled tens of millions in NFT sales. NFT auctions tend to attract younger buyers who see digital art as both an investment and a new form of cultural participation.

NFTs are democratizing the art market -- in some ways. Anyone can browse online NFT marketplaces, invest relatively small amounts, and own a digital asset linked to an artist. There are even tokens tied to real-world collectibles (sports memorabilia, vintage music recordings, virtual real estate) and fractional ownership schemes where expensive art or NFTs are divvied up into many smaller pieces. Yet, rapid growth in NFTs comes with risks. As art moves onto the blockchain, criminals have seized opportunities for fraud and money laundering. The traditional art market has long wrestled with opaque pricing and shady transactions; add the anonymity and borderless nature of crypto, and new loopholes emerge.

NFTs and the law: security or art?

Under current rules, whether an NFT is treated like a security (e.g. a stock or bond) or a collectible (e.g. a painting) depends on context. In general, auction houses and regulators have treated NFTs sold as one-off artworks as collectible assets. The U.S. Securities and Exchange Commission (SEC) has said that a finished art piece – digital or physical – is not automatically a security just because its price may appreciate. However, there are strong arguments for classifying many NFTs as securities, especially when they're sold with the expectation of profit. The key tool here is the Howey Test, a four-part legal checklist from U.S. law:

Investment of money: Did the buyer put money into the project?
Common enterprise: Are the fortunes of all investors tied together? (For instance, if you buy a fraction of an NFT, its value rises or falls for everyone who owns a share.)
Expectation of profit: Was the buyer hoping to make money from the purchase?
Efforts of others: Does profit depend largely on the efforts of the creators or promoters?
If all four conditions are met, a transaction can be deemed an investment contract.

Who's regulating what?

The regulatory picture is fragmented worldwide. In the United States, securities rules apply case by case: a one-off art sale is treated as art, but a collectible series sold with hype and profit-sharing could trigger SEC scrutiny. Most individual states and the U.S. Treasury have flagged NFTs as money-laundering risks, but no bright-line law dictates their status. In the European Union, new crypto laws (MiCA) explicitly exclude "unique assets" such as art NFTs from certain protections, treating them more like collectibles than currencies. Canada, likewise, is still defining NFTs through existing investment-tests, but so far most digital art is not (yet) treated as a security.

Even global watchdogs diverge. The Financial Action Task Force (FATF) says that pure art or collectible NFTs aren't automatically virtual assets unless they're used as payment or become fungible. But if NFTs are actively traded and marketed as investments, they qualify as a virtual asset. That requires exchanges and sellers to do anti-money-laundering (AML) checks. In practice, jurisdictions vary widely.

Auction houses under the microscope

High-end auction houses such as Christie's and Sotheby's have enthusiastically entered the NFT market, intent on evolving their market reach in the digital age. Traditionally, auction houses have known their clientèle. Big bidders usually go through background checks or maintain a trusted relationship with the auction house. They are not formal financial institutions. In the U.S., auctioneers are not automatically subject to the strict anti-money laundering laws that banks or brokerage firms face – at most they must report any cash transaction over $10,000 (similar to jewelers or luxury car dealers). Cryptocurrencies are not a neat fit for those rules.

This discrepancy raises red flags. Auction houses often process millions of dollars in crypto payments, yet they are not classified as Virtual Asset Service Providers (VASPs). Crypto exchanges are VASPs, which means they must verify customer identities, monitor transactions, and report suspicious activity. Auction houses that sell NFTs, however, have largely avoided that framework. In effect, a high-value NFT sale at Sotheby's could be less vetted than a sale on an online exchange, even though amounts might be comparable.

Experts argue that this gap could turn auction houses into inadvertent enablers of financial crime. Without mandatory Know-Your-Customer (KYC) checks on crypto buyers, stolen or illicit funds could flow through an NFT sale. Likewise, the auction houses' own due diligence on NFT issuers may be superficial: one recent lawsuit alleges a prestigious auction house failed to spot red flags about an NFT seller and ended up auctioning a collection that quickly collapsed in value. Unlike banks or stock exchanges, traditional auction houses lack internal compliance departments focused on AML, and many staff may not fully understand blockchain technology. This makes it difficult for them to spot money laundering schemes camouflaged as digital art purchases.

A high-profile NFT lawsuit

In 2023 buyers of a famous NFT collection sued an auction house for allegedly misrepresenting the sale. In late 2021, Bored Ape Yacht Club NFTs, cartoon ape images from a startup called Yuga Labs, were auctioned. One buyer paid over $24 million for a bundle of NFTs, encouraged by celebrity endorsements and online hype. Within months, the market had tanked, and the NFTs were worth only a fraction of that price. Plaintiffs claim the auction house gave the collection a "stamp of approval" without warning of risks, and that well-connected insiders had artificially inflated the price. Notably, Yuga Labs and its partners were already under federal scrutiny: whether their sales amounted to unregistered securities offerings. This lawsuit highlights the gray zone: if those NFTs were securities, the auction house was acting akin to a VASP without proper registration. Regardless of the legal outcome, the case has shaken confidence. It illustrates how an auction house's brand can attract ordinary collectors into highly speculative markets.

Mikayla Ozga is a researcher at the Institute of Intergovernmental Relations at Queen's University

Christian Leuprecht is professor at the Royal Military College of Canada and Queen's University

WALKING THE TIGHTROPE: UPHOLDING PRIVACY WHILE REGULATING VIRTUAL ASSETS TO FIGHT FINCRIME

Suman Podder

"Virtual assets" is the new buzzword in the world of investment. The distinguishing feature of virtual assets is that they allow for certain degree of anonymity in financial transactions. As virtual assets are byproducts of technological advancement, the constant evolution of virtual assets poses a challenge not only to the boundaries of traditional financial instruments but also to the notions of established governance frameworks and the effectiveness of existing regulatory tools. This has generated heightened attention from not only investors but also regulators and scholars. As virtual assets are here to stay and evolve in the wake of technological progress, the regulators are burdened with the unenviable task of walking a tightrope, ensuring responsible oversight without undermining the need of investors to enjoy privacy in their financial transactions.

The Benefits and Risks of Virtual Assets

Virtual assets have garnered significant attention from investors as an alternative investment avenue due to their lower transaction costs, borderless nature, and higher financial inclusivity when compared to traditional financial instruments. In addition, these virtual assets offer a higher degree of anonymity to investors, providing privacy-enhanced nontraditional investment instruments. For the majority of people without access to traditional financial systems or those in countries with volatile currencies, these virtual assets offer an alternative means of financial inclusion. However, the very nature of these benefits brings with it a plethora of risks, which, if not addressed effectively, will undermine the benefits of virtual assets. While the borderless and decentralised nature of virtual assets challenges regulatory boundaries and jurisdictions, their anonymity and existence outside the traditional financial system make them lucrative for money laundering and the funding of other criminal activities, including terrorism.

As a result, the regulation of virtual assets is heavily centred around the enforcement of anti-money laundering (AML) and Counter-terrorism financing (CTF). Virtual assets are created and transacted, bypassing the traditional financial intermediaries, making it difficult to track the transactions. Admittedly, operating within a regulatory blind spot is the biggest drawback of virtual assets. However, with the right regulatory framework, it will be possible to enjoy the benefits of virtual assets without exacerbating the risks damaging to investors and society at large. As a result, the FinCrime regulators such as the Financial Action Task Force (FATF), Australian Transaction Reports and Analysis Centre (AUSTRAC) and more recently Markets in Crypto-Assets Regulation (MiCA) are engaged in regulating the financial system and especially the virtual assets in such a manner that it becomes more transparent and thereby renders it unattractive for financing criminal activities.

Balancing Transparency with the Individual's Right to Privacy

While transparent financial transactions are the bedrock of any strong FinCrime regulation, the urge to monitor and trace every transaction of the virtual asset can easily encroach upon the digital privacy of the innocent investors. While the right to privacy has been recognised as a human right, it often takes a secondary position when considered in relation to other legislation. The right to conduct their financial transactions outside the traditional financial ecosystem with the instrument of their choice and in any jurisdiction is a justified demand of the global citizen.

This does not mean that virtual assets provide complete anonymity. Since virtual assets are generally linked to real-world assets, bought and sold using cryptocurrencies, and conducted on a digital platform, all transactions are recorded on a blockchain, which is not only unalterable but also highly traceable if needed. However, blanket surveillance of virtual assets at the cost of the privacy of innocent investors will only lead to the creation of additional avenues of financial transactions and the abandonment of traditional ones. Therefore, the question regulators need to ask is what drives the need of these investors to invest in virtual assets? What is the underlying motivation of these investors to be attracted to the notion of anonymity offered by the virtual assets?

It would be beneficial for the regulators to understand that the notion of digital privacy is not to restrict the sharing of personal information, but to provide adequate guardrails so that information is collected or processed by authorised entities in a lawful and transparent manner. In the same vein, transactions involving virtual assets should only be monitored and disclosed if there is overwhelming evidence of wrongdoing. While there are privacy-enhancing technologies in virtual asset transactions that have the potential to enable regulatory compliance while preserving user privacy, these technological tools will not receive due consideration until the right to privacy is acknowledged on equal footing, if not superior to other legislations.

The other important challenge to overcome is that regulators, whether financial or FinCrime, are traditionally focused and often lack the technical knowledge and understanding necessary to evaluate risks and recommend new technological controls for regulating emerging areas, such as virtual assets. The regulators will need to work with the platforms on which the virtual assets are created and traded. These platforms can undergo some form of accreditation, which will not only allow them to act as gatekeepers for nefarious actors, they will attract innocent investors by upholding some form of regulatory endorsement. In such a manner, they will be responsible for upholding the privacy of investors unless there is a reason for disclosing the identity or transaction to the regulator.

While the various Central Bank Digital Currencies (CBDCs) are being created to increase financial inclusion and offer investors an alternative means of investment, it is still in the early stages of rollout. It will be interesting to see whether investors view CBDCs as a genuine alternative for investment or if they will ultimately be used as a replacement for traditional currency only. The success of such digital currencies will depend on the Government and the country of their origin. Countries with strong privacy legislations, therefore, stronger awareness of digital privacy, will come out on top by recognising that privacy-enhanced digital currency will garner more trust and traction among investors.

To enable the general public to enjoy the benefits of virtual assets without exacerbating the risks of becoming a hub for criminal transactions, regulators must create a regulatory framework that prioritises consumer protection, financial stability, and a balanced consideration of both privacy and anti-crime measures. The government should recognise that in the modern era, upholding privacy does not mean the absence of accountability, and providing anonymity does not equate with the absence of oversight. The role of privacy in the world of virtual assets is to highlight the need for fair and proportionate disclosure in a world that is rapidly moving towards universal surveillance.

Dr Suman Podder, Data and Privacy Officer at Cubic Transportation Systems

SMOOTH SEAS, NEVER MADE FOR A GOOD SAILOR: THE DIGITAL ASSETS REFORMS AHEAD

Liam Hennesy

Open Seas

Digital assets, including cryptocurrencies, stablecoins, and tokenised real-world assets, offer transformative benefits across financial markets based on the underlying technology. By enabling faster, borderless transactions, programmable compliance, and real-time settlement, they reduce friction and increase transparency. Tokenisation, in particular, allows fractional ownership of traditionally illiquid assets like property, infrastructure, or private equity, unlocking new capital flows and democratising access to investment opportunities. These innovations promise efficiency, liquidity, and resilience, but also demand a modern regulatory response. Australia – and indeed the broader world – is grappling with how to best regulate digital assets now to support businesses, promote innovation and protect consumers.

ASIC's own research from years ago indicated that digital assets are held second to only shares by Australians; the market has turned into a trillion-dollar industry; nations are competing to offering nuanced regulation and support for the sector (most evident in the US, within the Trump Administration); and specialist law firms are leveraging the technology to make traditional financial products e.g. funds more flexible, efficient and commercially attractive.

As these digital instruments proliferate, so too do the challenges they pose for regulatory regimes, particularly in the areas of effective consumer disclosure, anti-money laundering (AML), and financial services licensing. In Australia, Digital Currency Exchanges (DCEs), entities exchanging fiat currency for various digital assets, sit at the frontline of these reforms. While previously largely subject only to AUSTRAC registration and AML/CTF compliance, DCEs are now facing increasing scrutiny from ASIC and Treasury as financial product definitions, enforcement actions, and token assessments converge.

Scylla: ASIC's CP 381 and Expanding INFO 225:

In December 2024, ASIC released Consultation Paper 381 (CP 381), proposing significant amendments to INFO 225, its digital asset guidance document. CP 381 aims to provide clearer boundaries around when a digital asset is a "financial product" under the Corporations Act 2001 (Cth), thereby triggering the need for an Australian Financial Services Licence (AFSL). An assessment of the current law as it applies to digital assets, the practical effect of these reforms is that many tokens previously issued outside the AFSL regulatory perimeter now need to be examined within that context. Examples include currency (see [21] of ASIC CP 381) and yield-bearing stable coins – tokens connected with a traditional fiat currency, and increasing in popularity.

The revised INFO 225—also supplemented by ASIC MIU 167 emphasises the importance of "token assessments". These assessments require DCEs and token issuers to evaluate whether a token:

- Confers rights or interests in a financial product (e.g. a managed investment scheme or security);

Facilitates non-cash payment functionality akin to a stored value facility;

- Is embedded within a broader financial service (e.g. custody, margin lending, or portfolio management).

ASIC expects DCEs and related platforms to undertake a legal characterisation of tokens and to maintain defensible, documented rationales for their conclusions. This is especially critical for platforms offering access to yield products, stablecoins, synthetic assets, or tokenised real-world assets.

Charybdis: Qoin and Block Earner - Regulatory Divergence in Action

Two pivotal cases illustrate how ASIC's evolving stance is being tested in the courts:

- Qoin (BPS Financial Pty Ltd): In a significant 2024 decision, the Federal Court held that Qoin's digital wallet offering constituted a non-cash payment (NCP) facility, a type of financial product. BPS was found to have operated without an AFSL and made misleading representations about Qoin's usability. The case confirmed that "closed-loop" or utility tokens may still constitute regulated products if broadly marketed or exchangeable. The subsequent appeal is also of huge market importance in terms of the bounds of what AFSL "Authorised Representatives" can do with respect to "issuing" of financial products under their borrowed licence;
- Block Earner (Web3 Ventures Pty Ltd): By contrast, the Full Federal Court overturned penalties against Block Earner in early 2025, finding that its "Earner" yield product did not constitute a managed investment scheme (reliant as it was on fixed interest debt obligations). While Block Earner had initially been found liable for unlicensed conduct, the Full Court accepted that it had acted honestly and reasonably, and that ASIC's guidance lacked sufficient clarity at the time of offering. The case is potentially going to the High Court, and the outcome is far from certain.

These cases highlight the importance for DCEs of undertaking token-specific legal analysis and maintaining up-to-date assessments, and ASIC's willingness to regulate through guidance (see above) and also enforcement to define the regulatory perimeter. Braithwaites' Pyramid is alive and well!

Cyclops: AUSTRAC Enforcement Trends

While ASIC focuses on financial product definitions, AUSTRAC is ramping up enforcement in the AML/CTF domain. Since 2023, AUSTRAC has moved from education and guidance to active supervision and legal action. Notably:

- In March 2025, AUSTRAC issued an infringement notice to Cointree Pty Ltd, a registered DCE, for failing to comply with obligations under the AML/CTF Act. The penalty related to deficiencies in its AML/CTF Program, including inadequate (delayed) reporting of Suspicious Matter Reports. More enforcement actions are expected.
- AUSTRAC has also released targeted guidance on crypto asset teller machines (CATMs), clarifying that operators must be registered DCEs and must implement full AML/CTF programs, including customer verification, transaction monitoring, and suspicious matter reporting. AUSTRAC considers CATMs to carry heightened ML/TF risks due to their potential for anonymous cash transactions, and has imposed a number of more stringent conditions on their operations e.g. tightened transaction limits, and specific scam warnings.
- More broadly, AUSTRAC has signalled an increased willingness to refer non-compliant DCEs to law enforcement, particularly where there are failures to report suspicious matters or where the business poses a high residual risk. Non-compliance with Part A and Part B obligations of AML/CTF Programs now carries both regulatory and reputational consequences.

This shift underscores that registration as a DCE alone is no longer a shield against liability. DCEs must invest in robust and dynamic AML/CTF frameworks, and consider whether they are offering products which may be financial products e.g. stablecoins, capable of adapting to evolving regulatory expectations and technology-driven risks.

Circe: Treasury's 2025 Digital Asset Reform Agenda

In March 2025, just before the election, the Australian Treasury released a digital assets roadmap, reaffirming the government's intention to regulate digital asset platforms more comprehensively. Central to this roadmap are:

- A proposed custody and licensing regime, i.e., modified AFSL authorisations for crypto asset platforms, is expected to apply to DCEs that hold client assets.
- Continued work with ASIC and APRA to explore regulatory frameworks for stablecoins, tokenised deposits, and Central Bank Digital Currencies (CBDCs);
- Recognition that regulatory gaps in both financial services and AML law must be addressed for Australia to remain competitive while protecting retail and institutional investors.
- Treasury's language indicates a move toward functional regulation, "same risk, same rules", which would close many of the arguable grey areas DCEs currently operate within. The Albanese Government's move to legislate the regulation of digital assets follows similar legislation in advanced financial services jurisdictions, e.g., the US with the 'GENIUS Act' (which is designed to regulate the stablecoin market, minimise risk, and protect consumers and the broader financial system).

Practical Steps to Ithaca: Implications for DCEs

DCEs now face multi-dimensional regulatory obligations:

Area of Law	Practical Advice
AML/CTF (AUSTRAC)	Maintain nuanced and operationally effective compliant Part A & Part B AML/CTF Programs; monitor, report suspicious matters; conduct KYC and ECDD.
Financial Services (ASIC)	Undertake token assessments; determine whether services (e.g. wallets, yield, stablecoin facilities) are financial products requiring an AFSL. Obtain AFSL if so.
Disclosure	Avoid misleading claims around token liquidity, functionality, and platform features.
Treasury Reform Readiness	Plan for a future licensing regime around client asset custody, market conduct, and platform licensing.

Many DCEs will need to undertake a wholesale compliance uplift (possibly remediation), not only to survive increased regulatory scrutiny but also to ensure future scalability in a tightening legal environment. There are currently circa. 440 DCEs in the Australian market, comprising large exchanges, funds, crypto ATMs, and other digital asset businesses. Without effectively responding to the changed regulatory environment, this market is likely to condense appreciably.

Penelope's test: the challenge ahead

DCEs are now operating in an increasingly sophisticated and scrutinised legal environment. Australia's challenges exist in a microcosm of the broader global regulatory reform push, and the crypto market is defined by its globalism. ASIC's expanded token assessment obligations, AUSTRAC's active enforcement stance, and Treasury's reform roadmap all point toward a future where DCEs will be subject to full-spectrum regulation.

For the DCE sector to thrive, it must invest in legal structuring, compliance talent, and dynamic risk assessments. The days of regulatory arbitrage are fading, and a new era of accountable innovation is emerging. Australia's approach, measured, collaborative, and principles-based, offers a promising template for global jurisdictions wrestling with the digital asset frontier

Liam Hennessy, Partner Thomson Geer, Adjunct Professor of Law at Griffith University

CRYPTO FORENSICS AS AN ADAPTIVE AML/CFT COMPLIANCE TOOL FOR VIRTUAL ASSET SERVICE PROVIDERS IN DEVELOPING COUNTRIES

Oluwabunmi Adaramola

In 2024, Sub-Saharan Africa received an estimated $125 billion in on-chain value, a $7.5 billion increase from the previous year. This surge underscores the region's growing stake in the digital asset economy. Yet, with the rapid expansion of FinTech and Virtual Asset Service Providers (VASPs), developing countries are confronting a critical gap, where traditional AML/CFT frameworks are proving ill-equipped to manage the complexities of virtual (or crypto) assets. This article thus explores how integrating crypto forensics and RegTech solutions can address compliance gaps in VASP regulation across developing economies, particularly where regulatory capacity is weak or under-resourced.

An Overview of Crypto Laundering

Virtual (or crypto) Asset Service Providers (VASPs) act as gatekeepers of the growth of crypto assets in relevant regions, since they are primarily tasked with facilitating exchange, trading, and storage of digital assets such as cryptocurrencies, tokenized securities, and NFTs. However, inconsistent regulations, limited oversight and weak enforcement have rendered these intermediaries vulnerable to criminal misuse such as crypto laundering, crypto fraud and other related criminal activities. Crypto laundering thus occurs where digital assets are used as vehicles to commit traditional money laundering activities, through hiding the sources of illicit flows and funds through cryptocurrencies such as Bitcoin, Ethereum or more complex privacy coins like ZCash and Monero, either during the layering or integration stages of the traditional money laundering process. This is particularly due to their decentralised and pseudonymous nature, which make them particularly attractive for criminals seeking to obfuscate existing financial and AML frameworks. This is particularly harmful to the financial systems and economic structures in developing countries and emerging markets with weak regulatory systems and even weaker enforcement measures.

Why Traditional AML/CFT Regimes for VASPs are Inadequate

Due to the growing and consistent complexities that exist with cryptocurrencies, with increased advancement in mixing technologies and the advent of privacy coins, it is an undeniable fact that traditional rule-based compliance frameworks are proving insufficient. This is evident where amidst the existence of traditional AML requirements and processes, there have been high record losses due to crypto fraud and scams across jurisdictions, with Rustamaji and Faisal citing the losses as $6 billion from security breaches, almost $5 billion from decentralised financial hacking and almost $8 billion from cross-border fraud schemes. As such, current AML regulatory frameworks integrated into VASP regulations if they exist, can be concluded to be underdeveloped and running in parallel with the fast paced development of technology within this area, prompting a need for the exploration of newer strategies such as AI tools and predictive technologies within crypto forensics, for a more effective compliance strategy.

On this point, it is thus evident that AI plays a pivotal role in fraud detection and anti-money laundering efforts, employing advanced algorithms to analyze transaction patterns and identify potential irregularities, thereby fortifying the security of financial systems to combat the illicit activities associated with the use of cryptocurrencies.

For VASPs and similar financial intermediaries to successfully develop a deep understanding of their client's wealth generation and other activities, financial institutions traditionally implement Know Your Customer (KYC) techniques, which typically revolve around risk reporting based on customers profiles as well as customer due diligence methods (CDD), which focuses on customer information and relationships, requirements for reporting suspicious activities (SAR) to the relevant authorities for investigation and enforcement all as a means to preserve the integrity of financial markets and enhance consumer trust in the system.

Given how integral AML compliance is to the overall integrity and stability of the entire financial market, institutions and other financial intermediaries [which is now inclusive of VASPs and related entities] must adopt more intelligent, scalable and adaptable solutions to identify suspicious transactions, track and trace illicit activities and prevent any criminal obfuscation, abuse and misuse of digital channels. This is where blockchain or crypto forensics comes into play within VASPs, as they offer newer and sophisticated methods and techniques for VASPs to curb the activities of fraudsters and criminals using cryptocurrency as fraudulent vehicles.

Crypto Forensics and Reg Tech as Enabling Technologies for AML Compliance.
Blockchain or cryptocurrency forensics, as a starting point on investigative technologies, has been described as immutable, providing a rich source of evidence that, when properly analysed, can reveal intricate patterns of activity and link digital identities to real-world entities. As such, given that many cryptocurrencies first exist on the blockchain technology, it only seems appropriate to use blockchain forensics as an adequate tool to sift through and analyse blockchain transactions for an efficient enforcement strategy. As such, the main aim of this forensic tool really is to excavate and evaluate as much evidence as can be obtained from the blockchain digital ledger, with some of the key techniques involved ranging from transaction tracing, address clustering, which makes use of various clustering heuristics, entity identification, and attribution tags.

Due to constant activity within the tech space, private owners of RegTech solutions have begun exploring techniques to 'follow the money' to aid investigation and customer due diligence as part of AML techniques. This is an important point to note within the development of blockchain analysis, as RegTech (short for regulatory technology) is a subset of FinTech and LegalTech solutions and AI-powered tools with the overarching aim of using new technologies and such AI tools to aid regulatory compliance and processes, mainly through FinTech software applications. These RegTech solutions are thus integral to the idea of crypto forensics as a tool for VASPs, given that many AML/CTF regulated entities use these RegTech solutions to screen their operations and detect anomalous activities in an automated way. RegTech, therefore, can automate workloads as well as provide real-time tracking and monitoring and other analytics, all of which are beneficial to aiding KYC and other due diligence methods undertaken by VASPs to meet AML requirements. For Instance, Natural Language Processing (NLP) and Risk scoring models powered by AI can process and analyse unstructured text data from a variety of sources including KYC documents and assess the likelihood of illicit activity based on behavioural patterns and transaction history, which ultimately serve to create more effective customer due diligence, while navigating these complex crypto ecosystems.

Researchers further suggest a range of other technologies around predictive AML compliance that VASPs may adopt such as adaptive learning systems, given the constantly and rapidly evolving nature of cryptocurrencies, with criminals constantly testing the limits of new platforms and services as well as Machine Learning (ML) and behavioural analytic tools, all aiming at successfully identifying suspicious activities and transactions as effectively and as quickly as possible, to maintain the integrity of the exchange and/or trading platform. Johnson further explores the idea of smart contracts as compliance tools, using them in a way that codifies AML rules into self-executing protocols that trigger alerts or restrict suspicious activities in real time. As such, this reduces the risks of human error, making AML compliance processes integrated in VASPs' regulations more precise, efficient, and reliable.

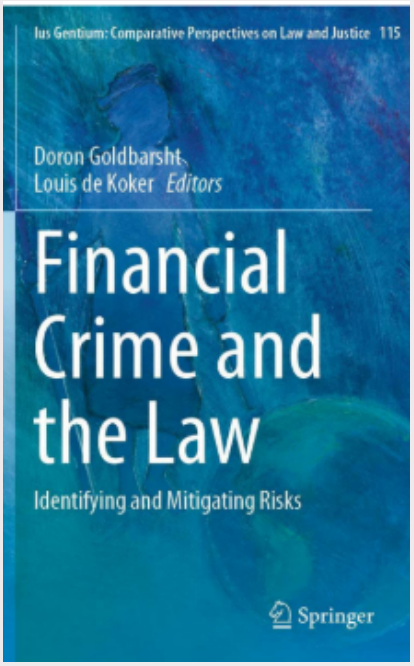
It must be noted that these new adaptive technologies are not without their risks; one of the major concerns is issues around privacy and integrity of personal information. On the overall complexity of cryptocurrency forensics, investigative errors may occur, which may potentially lead to false suspicion or conviction in extreme cases, where, in the deployment of blockchain analysis, for instance, certain transactions may distort clustering results, unifying entities that are not related…and false and unrelated actors. Challenges become further complicated with the advent of privacy coins, which employ even more advanced techniques to mask and complicate user and transaction identity. Other challenges with regard to enforcement and using digital forensic tools as compliance tools in developing countries like Nigeria revolve around the general deficits in Nigeria's technological infrastructure, to the extent that such tools may not be sustainable in the long run. Due to digital and electronic constraints prevalent in Nigeria and challenges with a consistent infrastructure to uphold newer technological advancements, the advancement of such crypto forensics and RegTech solutions may prove challenging and costly. As such, to harness the potential of crypto forensics and RegTech, developing countries may consider a layered compliance strategy that requires VASPs to integrate basic blockchain monitoring tools as part of licensing conditions. Furthermore, solutions such as collective resource and information sharing among various regional and international blocs, as well as partnerships with think tanks and global blockchain analytics firms, may serve to address complex cases that span multiple jurisdictions.

As cryptocurrencies continue to reshape the financial landscape, developing countries cannot afford to rely on outdated compliance frameworks. Crypto forensics, supported by RegTech tools, offers a viable, adaptive pathway to bridge regulatory gaps in VASP oversight. However, these technologies must be embedded within broader structural reforms, including legal updates, skills development, and regional cooperation. To maintain the integrity of global financial systems, stakeholders in the Global South must move from being passive recipients of imported compliance models to active co-creators of context-specific, tech-enabled AML solutions. The future of financial integrity will depend not only on new technologies but on how equitably and intelligently they are deployed.

Oluwabunmi Adaramola, PHD Law Student at the University of Leeds

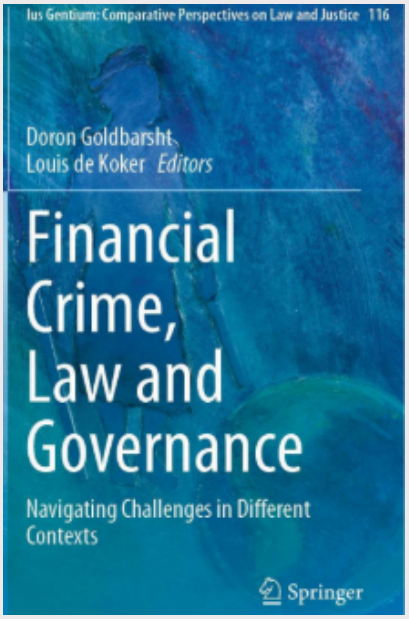
RESEARCH AT FIH

Financial Crime and the Law: Identifying and Mitigating Risks



Edited by Doron Goldbarsht and Louis De Koker, this collection explores financial crimes like crypto crime, terrorist financing, and money laundering. It offers insights into risk-based compliance, challenges in regulating weapons of mass destruction financing, and the connection between cannabis regulation and money laundering. The book also critiques the effectiveness of the risk-based approach, highlighting concerns about bias and the role of Financial Action Task Force (FATF). Essential for professionals and scholars, it deepens understanding of the complexities in financial crime risk management.

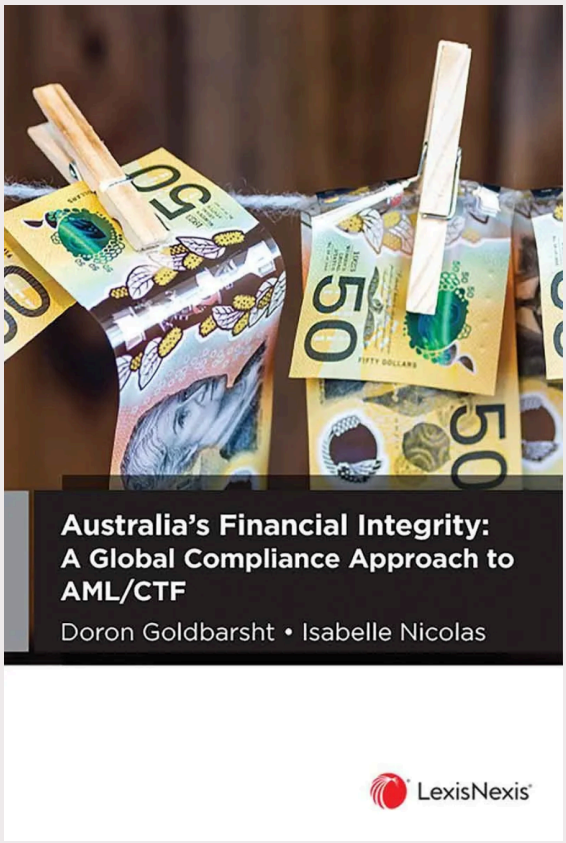
Financial Crime, Law and Governance: Navigating Challenges in Different Contexts



Edited by Doron Goldbarsht and Louis De Koker, this collection was curated by leading researchers to explore the dynamic landscape of global financial crime. It offers profound insights into the nuanced world of financial crime across diverse jurisdictions including Australia, Germany, New Zealand, Nigeria and the United Kingdom. While global standards on financial crime have solidified over the past three decades, the future direction of standard-setting and compliance enforcement remains uncertain in the complex global political landscape.

RESEARCH AT FIH

Australia's Financial Integrity: A Global Compliance Approach to AML/CTF



Co-authored by Doron Goldbarsht and Isabelle Nicolas, this book provides readers with a comprehensive understanding of the measures adopted by Australia to address global anti-money laundering and counter-terrorism financing standards set by the Financial Action Task Force (FATF). The book is structured in a way that reflects and aligns with the global standards set out by the Financial Action Task Force (FATF). Each chapter helpfully adopts the title of one of the FATF's 40 recommendations, including those recommendations and their interpretive notes, followed by questions and answers. This book's unique structure breaks down complex research findings into simple, digestible insights for practitioners and students.

FIH PODCAST

Listen to us on Spotify!

Season 2 of the *Financial Integrity Hub Podcast*

The Financial Integrity Hub hosts regular podcasts, featuring speakers with financial crime and compliance expertise. Each podcast involves an interview with a global or local expert, allowing the Financial Integrity Hub to harness critical voices and ensure the Financial Crime community can stay up-to-date on the latest AML/CTF challenges and trends.

Episode 1 - Perspectives on AML/CTF and Risks with global experts with Dr Rachel Southworth, Prof Michael Levi, Prof Louis De Koker, and Charles Littrell.

Episode 2 - Risk Management in Casinos with Armina Antoniou

Episode 3 - Financial & Environmental Crime with Davyth Stewart

Episode 4 - The AML/CTF Act and the Reform with Jeremy Moller

NEW! Episode 5 - Meet the CEO: In Conversation with Brendan Thomas
In this episode, Dr Hannah Harris speaks with AUSTRAC CEO Brendan Thomas about his professional journey, AUSTRAC's evolving strategic priorities, and the agency's innovative use of data and technology in financial intelligence. The conversation offers valuable insights on leadership, career development in the financial crime space, and the role of academic research centres like the Financial Integrity Hub in

Thank you to our podcast partner - CFCE!

CFCE sets itself apart as an exceptional AML/CTF course provider with a unique focus on the Australian industry. What makes CFCE even more appealing is that these valuable educational opportunities are not only highly informative but also cost-effective.

CFCE
CERTIFIED FINANCIAL CRIME EXPERTS

CFCE offers 50% discounts to FIH readers: Fundamentals in AML, Fundamentals in CTF, AML/CTF for Clubs and Pubs, KYC, CDD, and others. Just use the code "CFCE-FIH". Contact: office@cfce.com.au

END OF YEAR EVENT

End-of-year event: AML/CTF regulation and the growing war on talent

This event explores the intersection of AML/CTF compliance and the growing war on talent in the financial crime sector. As regulatory expectations increase, so does the demand for skilled professionals, creating challenges in recruitment, retention, and capability-building.

Bringing together experts from industry, government, and academia, the event will examine workforce gaps, emerging skills, and innovative solutions to strengthen the pipeline of talent critical to combating financial crime.

For tickets, please visit the FIH Website.

WORK WITH US

The Financial Integrity Hub (FIH) relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of financial crime by bringing together perspectives from the fields of law, policy, security, intelligence, business, technology and psychology.

The FIH offers a range of services and collaborative opportunities. These include professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being part of a cross-sector network and having a greater understanding of the complex issues surrounding financial crime, please contact us to discuss opportunities for collaboration: fih@mq.edu.au.

If you would like to contribute your op-ed for our future FIH Insights, please contact us.

FINANCIAL INTEGRITY HUB

MACQUARIE University
SYDNEY·AUSTRALIA