Page 1234 - 1256

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Assets Recovery Challenges in Investigation, Prosecution and Adjudication of Money Laundering Crimes Involving Virtual Assets in Rwanda: A Comparative Study with the USA and Singapore

JONAS NIYITEGEKA*

ABSTRACT

The rapid proliferation of virtual assets has fundamentally transformed the landscape of financial crime, presenting unprecedented challenges to law enforcement agencies, prosecutors and adjudicating courts worldwide. This article examines the multifaceted challenges confronting Rwanda in recovering assets derived from money laundering offences involving virtual assets, with particular emphasis on the investigative, prosecutorial and adjudicative dimensions of this complex problem. Drawing on Rwanda's evolving legal framework, including Law No. 001/2025 on the prevention and punishment of money laundering and Law No. 023/2026 regulating virtual asset business, the article undertakes a comparative analysis with the United States of America and Singapore, two jurisdictions that have developed relatively mature frameworks for virtual asset regulation and proceeds-of-crime recovery. The comparative methodology reveals significant structural, institutional and technical gaps in Rwanda's current approach, while also identifying opportunities for capacity-building and legal reform. The article argues that effective asset recovery in the virtual asset context requires not merely legislative intervention but a comprehensive ecosystem encompassing technological infrastructure, skilled human capital, robust international cooperation mechanisms, and an independent, well-resourced judiciary. The article contributes to the growing body of scholarship on virtual asset governance and offers concrete recommendations for Rwanda's ongoing reform trajectory.

Keywords: *asset recovery, virtual assets, cryptocurrency, money laundering, Rwanda, financial crime, blockchain, AML/CFT*

Declaration of preprint availability: this manuscript is available as a preprint on SSRN at https://doi.org/10.2139/ssrn.6950318.

* Author is a PhD Research Candidate at Chhatrapati Shahu Ji Maharaj University, Kanpur, Uttar Pradesh, India.

I. Introduction

The intersection of financial crime and digital technology represents one of the most formidable challenges confronting contemporary criminal justice systems. The emergence and proliferation of virtual assets, encompassing cryptocurrencies, non-fungible tokens (NFTs), decentralised finance (DeFi) instruments, and other blockchain-based assets, have created new avenues for the concealment, layering and integration of illicit proceeds, thereby complicating the already arduous task of asset recovery. For jurisdictions such as Rwanda, which are simultaneously navigating economic development imperatives and financial integrity obligations, the challenge is particularly acute.

Asset recovery constitutes the cornerstone of any meaningful anti-money laundering (AML) regime. The fundamental rationale is straightforward: crime should not pay. Where the proceeds of criminal conduct are not effectively recovered, criminals retain the incentive to persist in their activities, and the social harm of financial crime is compounded by the enrichment of wrongdoers at the expense of victims and the broader public. As Brun and his co-authors observe in the *Asset Recovery Handbook*, the identification, tracing, freezing and confiscation of proceeds of crime serve both punitive and preventive functions, disrupting criminal enterprises and deterring future offending.[1]

The virtual asset environment, however, has dramatically altered the calculus of asset recovery. Traditional asset recovery frameworks were designed for a world of tangible property and conventional financial instruments: bank accounts, real estate, motor vehicles, and similar assets susceptible to physical seizure and straightforward legal process. Virtual assets, by contrast, are characterised by decentralisation, pseudonymity, cross-border fungibility, and a technical complexity that renders conventional recovery mechanisms inadequate.[2] The pseudonymous nature of blockchain transactions, the absence of intermediaries in many decentralised protocols, and the use of privacy-enhancing technologies such as mixers and zero-knowledge proofs create formidable obstacles for investigators, prosecutors and courts.

Rwanda occupies an interesting position in this landscape. As a small, landlocked East African nation with an impressive track record of post-conflict reconstruction and economic transformation, Rwanda has demonstrated remarkable institutional capacity and regulatory ambition. The country has adopted a progressive stance toward digital financial services,

---

[1] Jean-Pierre Brun et al., Asset Recovery Handbook: A Guide for Practitioners (Stolen Asset Recovery Initiative, World Bank & UNODC, 2d ed. 2020).

[2] S. Sittlington & J. Harvey, *Prevention of Money Laundering and the Role of Asset Recovery*, 70 Crime, Law & Social Change 421 (2018).

positioning itself as a regional fintech hub while simultaneously grappling with the money laundering and terrorist financing risks that attend such ambitions. The enactment of Law No. 001/2025 on the Prevention and Punishment of Money Laundering, Terrorist Financing and the Financing of Proliferation of Weapons of Mass Destruction,[3] and the landmark Law No. 023/2026 Regulating Virtual Asset Business,[4] signal Rwanda's commitment to establishing a comprehensive regulatory architecture for the digital asset space.

Yet legislative frameworks alone do not guarantee effective outcomes. The translation of legal provisions into operational realities requires institutional capacity, technical expertise, inter-agency coordination and robust international cooperation, dimensions in which Rwanda continues to face significant challenges. A comparative lens, examining how the United States and Singapore have approached analogous challenges, offers valuable insights for Rwanda's ongoing reform process.

This article proceeds in eight substantive sections. Following this introduction, Section II provides a conceptual and definitional framework, situating virtual assets within the broader context of money laundering and asset recovery. Section III analyses Rwanda's legal and institutional framework for asset recovery in the virtual asset context. Section IV examines the specific challenges confronting investigators in Rwanda. Section V addresses prosecutorial challenges. Section VI considers the difficulties faced by adjudicating courts. Sections VII and VIII present comparative analyses of the United States and Singapore frameworks respectively. Section IX synthesises the comparative insights and offers recommendations for Rwanda. A conclusion follows.

II. Conceptual Framework: Virtual Assets, Money Laundering and Asset Recovery

A. Defining Virtual Assets

The definitional landscape of virtual assets is contested and rapidly evolving. The Financial Action Task Force (FATF), the international standard-setting body for AML/CFT, defines a virtual asset as 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.[5] This definition deliberately excludes digital

[3] Law No. 001/2025 of 22/01/2025 on the Prevention and Punishment of Money Laundering, Terrorist Financing and the Financing of Proliferation of Weapons of Mass Destruction (Rwanda). The Law replaces Law No. 75/2019 of 29/01/2020 on the same subject, as amended by Law No. 038/2021 of 28/07/2021.

[4] Law No. 023/2026 of 25/05/2026 Regulating Virtual Asset Business (Rwanda), gazetted on 28 May 2026. It is Rwanda's first dedicated statute on virtual asset business.

[5] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 2019).

representations of fiat currencies (central bank digital currencies) and securities already covered by other FATF Recommendations.

Rwanda's Law No. 023/2026 Regulating Virtual Asset Business adopts a similarly broad approach, defining virtual assets to encompass cryptocurrencies, utility tokens, security tokens, and other digital representations of value transacted on distributed ledger technology platforms.[6] This legislative definition is significant because it determines the scope of regulatory obligations applicable to virtual asset service providers (VASPs) and, by extension, the asset recovery mechanisms available in cases involving such instruments.

For the purposes of this article, the term 'virtual assets' is used broadly to encompass cryptocurrencies (such as Bitcoin and Ethereum), stablecoins, NFTs and DeFi instruments, acknowledging that their distinct technical and legal characteristics may give rise to different investigative and recovery challenges.

B. Money Laundering and the Asset Recovery Imperative

Money laundering is conventionally understood as the process by which the proceeds of criminal activity are transformed into ostensibly legitimate wealth. The classic three-stage model of placement, layering and integration describes the sequential steps through which illicit funds are introduced into the financial system, obscured through complex transactions, and ultimately reintegrated into the legitimate economy.[7] Virtual assets have proven particularly amenable to the layering stage, where their pseudonymity, speed and global reach facilitate the rapid and complex movement of funds across multiple wallets and jurisdictions.

Rwanda's Law No. 001/2025 defines money laundering comprehensively to include the conversion, transfer, concealment, disguise, acquisition, possession and use of property known to be proceeds of crime, as well as participation in, association to commit, attempts to commit, and aiding, abetting, facilitating and counselling the commission of such acts.[8] This definition aligns with the standard articulated in the United Nations Convention against Transnational

[6] Law No. 023/2026, *supra* note 4. Note that the Law adopts the FATF formulation of 'virtual asset' but expressly excludes digital representations of fiat currency, regulated payment instruments, securities, central bank digital currencies, non-fungible tokens and stablecoins from its statutory definition.
[7] R. Sheshi & K. Treska, *The Judiciary's Confrontation with Complex Financial Crimes: Challenges in Detecting, Investigating, and Adjudicating Sophisticated Money Laundering Schemes*, in PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE 'JUSTICE, SECURITY AND HUMAN RIGHTS' (ICJSHR-LFUL 2025) (2025).
[8] Law No. 001/2025, *supra* note 3.

 [ISSN 2581-5369]

Organized Crime (the Palermo Convention) and the United Nations Convention against Corruption (UNCAC), to which Rwanda is a party.[9,10]

Asset recovery refers to the suite of mechanisms by which the state identifies, traces, freezes, seizes and ultimately confiscates or repatriates proceeds of crime and instrumentalities of offending. Brun and his co-authors identify four principal modalities of asset recovery: criminal confiscation (attached to a criminal conviction), non-conviction-based (NCB) forfeiture (a civil forfeiture proceeding independent of criminal conviction), administrative forfeiture, and international asset recovery.[11] Each modality presents distinct procedural and evidentiary requirements, and the virtual asset context creates specific challenges in each.

The imperative of effective asset recovery is underscored by international legal obligations. Both UNCAC (Article 54) and the Palermo Convention (Article 12) require States Parties to adopt legislative and other measures to enable confiscation of proceeds and instrumentalities of crime.[12] These instruments further require States to give effect to orders for confiscation issued by other States, establishing the framework for international asset recovery cooperation that is indispensable in the cross-border virtual asset environment.

C. The Virtual Asset Money Laundering Threat Landscape

The use of virtual assets in money laundering has grown substantially over the past decade. While it is important to avoid overstating the magnitude of this threat relative to conventional financial channels, since cash remains the predominant medium for money laundering by volume, the distinctive characteristics of virtual assets create qualitatively distinct challenges for asset recovery systems.

The pseudonymity of blockchain transactions means that wallet addresses, rather than identifiable natural persons, are the visible participants in on-chain transactions. While blockchain forensics tools such as Chainalysis, Elliptic and CipherTrace have made significant advances in linking wallet addresses to real-world identities through cluster analysis and exchange data, these tools remain expensive, technically demanding, and dependent on data that may not be available in jurisdictions with nascent VASP regulatory regimes. In Rwanda's context, where the formal VASP sector is at an early stage of development and regulatory infrastructure is still being built, these limitations are particularly salient.

---

[9] United Nations Convention against Transnational Organized Crime art. 6, adopted 15 Nov. 2000, G.A. Res. 55/25, 2225 U.N.T.S. 209 (entered into force 29 Sept. 2003) [hereinafter Palermo Convention].

[10] United Nations Convention against Corruption art. 23, adopted 31 Oct. 2003, G.A. Res. 58/4, 2349 U.N.T.S. 41 (entered into force 14 Dec. 2005) [hereinafter UNCAC].

[11] BRUN ET AL., *supra* note 1.

[12] UNCAC, *supra* note 10, art. 54; Palermo Convention, *supra* note 9, art. 12.

The use of privacy-enhancing technologies, including mixing services, CoinJoin protocols, privacy coins such as Monero and Zcash, and zero-knowledge proof systems, presents an additional layer of obfuscation that can defeat even sophisticated blockchain analysis.[13] Cross-chain bridges, which allow assets to be moved between different blockchain networks, further complicate the tracing exercise. These technical realities demand that investigators, prosecutors and courts develop not merely familiarity with general concepts but genuine operational expertise in digital forensics and blockchain analysis.

III. Rwanda's Legal and Institutional Framework for Virtual Asset Recovery

A. The Asset Recovery Legal Framework

Rwanda's primary legislation governing asset recovery is Law No. 42/2014 of 27/01/2015 Governing Recovery of Offence-Related Assets, as amended by Law No. 037/2021 of 28/07/2021.[14] This framework establishes the legal basis for the identification, tracing, freezing and confiscation of assets derived from criminal activity, and creates the institutional architecture through which these functions are exercised.

Law No. 42/2014, as amended, provides for both conviction-based confiscation and, importantly, non-conviction-based asset recovery, the latter representing a significant departure from the traditional common law approach that required a criminal conviction as a prerequisite for confiscation.[15] The non-conviction-based modality is particularly significant in the virtual asset context, where the technical complexity of proving individual criminal conduct beyond reasonable doubt may render conviction-based approaches insufficient to capture the full range of illicit proceeds.

The predicate offence framework of Law No. 001/2025 extends money laundering liability to a broad range of serious crimes, including corruption, drug trafficking, terrorism, cybercrime and human trafficking.[16] The virtual asset dimension is explicitly addressed through the law's provisions on proceeds of crime derived from or facilitated by virtual asset transactions, reflecting Rwanda's recognition that the money laundering threat landscape has evolved to encompass digital instruments.

---

[13] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021).

[14] Law No. 42/2014 of 27/01/2015 Governing Recovery of Offence-Related Assets, Official Gazette No. 07 of 16/02/2015 (Rwanda), as amended by Law No. 037/2021 of 28/07/2021 Amending Law No. 42/2014 of 27/01/2015 Governing Recovery of Offence-Related Assets, Official Gazette No. Special of 30/07/2021 (Rwanda).

[15] Law No. 42/2014, *supra* note 14.

[16] Law No. 001/2025, *supra* note 3.

B. The Virtual Asset Regulatory Framework

Law No. 023/2026 Regulating Virtual Asset Business represents the culmination of Rwanda's deliberate effort to establish a comprehensive legal framework for the virtual asset sector. The law establishes a licensing regime for VASPs, including exchanges, wallet providers, custodians and issuers of virtual assets, and imposes AML/CFT obligations on licensed entities commensurate with those applicable to conventional financial institutions.[17]

Critically for asset recovery purposes, Law No. 023/2026 requires licensed VASPs to implement robust customer identification and verification (KYC) procedures, transaction monitoring systems, and suspicious transaction reporting (STR) obligations.[18] These requirements are foundational to the asset recovery ecosystem: without reliable customer identification data held by VASPs, the pseudonymity of blockchain transactions cannot effectively be pierced to identify the natural persons controlling virtual asset wallets associated with criminal activity.

The law also designates the Capital Market Authority of Rwanda as the principal regulatory authority for the virtual asset sector, with oversight responsibilities encompassing licensing, supervision and enforcement, while the National Bank of Rwanda (NBR) retains oversight wherever virtual assets intersect with payment systems, monetary policy and financial stability.[19] The Financial Intelligence Centre (FIC) of Rwanda, which receives and analyses STRs from VASPs and other reporting entities, and may disseminate financial intelligence to law enforcement agencies for investigative purposes, supplements the regulators' role in the AML/CFT framework.[20]

C. International Legal Framework

Rwanda's domestic framework is embedded within a broader international legal architecture. As a party to the Palermo Convention and UNCAC, Rwanda has assumed binding obligations to criminalise money laundering, to establish confiscation mechanisms and to cooperate internationally in asset recovery proceedings. The mutual legal assistance (MLA) framework established under these conventions provides the principal vehicle for Rwanda to seek and

---

[17] Law No. 023/2026, *supra* note 4.

[18] Law No. 023/2026, *supra* note 4. Licensed providers are required, among other obligations, to report all suspicious transactions without any threshold, to file periodic returns on accounts and transactions, and to comply with originator and beneficiary information requirements for virtual asset transfers.

[19] Law No. 023/2026, *supra* note 4. The Law designates the Capital Market Authority of Rwanda as the 'Regulatory Authority' for virtual asset business, with power to issue, suspend, revoke or alter licences, to issue regulations, directives and guidelines, and to suspend or ban specific types of virtual assets. The National Bank of Rwanda retains oversight where virtual assets intersect with payment systems, monetary policy and financial stability, and its authorisation is required before virtual assets may be used as a means of payment.

[20] Law No. 001/2025, *supra* note 3 (providing for the reporting, receipt and analysis functions discharged by Rwanda's Financial Intelligence Centre).

 [ISSN 2581-5369]

provide international assistance in virtual asset recovery cases involving cross-border elements.[21]

Rwanda is also a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body whose mutual evaluation process provides an external assessment of the effectiveness of member states' AML/CFT frameworks. The most recent ESAAMLG mutual evaluation of Rwanda identified significant gaps in technical compliance and effectiveness, with particular emphasis on the limited capacity for financial investigation and asset recovery, findings that have provided additional impetus for the legislative reforms noted above.[22]

D. Institutional Architecture

The institutional landscape for asset recovery in Rwanda encompasses multiple agencies whose mandates and activities must be effectively coordinated. The Rwanda Investigation Bureau (RIB) bears primary responsibility for criminal investigation, including financial crime and money laundering investigations. The National Public Prosecution Authority (NPPA) exercises prosecutorial authority in money laundering and related offences.

The Financial Intelligence Centre plays a critical intelligence function, receiving and analysing financial information from reporting entities, including, increasingly, VASPs, and disseminating actionable intelligence to the RIB and the NPPA. The National Cyber Security Authority (NCSA) provides technical support in cases involving digital evidence, including blockchain transactions. The Rwandan courts have the authority to decide cases involving asset recovery in criminal proceedings.

This multi-agency architecture, while comprehensive on paper, presents coordination challenges in practice. The virtual asset context demands seamless information-sharing, technical expertise and operational collaboration among agencies with distinct mandates, cultures and resource constraints. The following sections examine in detail the specific challenges encountered at each stage of the asset recovery process.

[21] Palermo Convention, *supra* note 9, arts. 13, 18; UNCAC, *supra* note 10, arts. 46, 55.

[22] Eastern and Southern Africa Anti-Money Laundering Group, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Rwanda, Follow-Up Report* (Aug. 2025). The underlying Mutual Evaluation Report of Rwanda was approved by the ESAAMLG Council of Ministers in July 2024.

IV. Investigative Challenges in Virtual Asset Recovery

A. Technical and Forensic Capacity Gaps

The most fundamental challenge confronting investigators in Rwanda's virtual asset context is the gap between the technical sophistication of virtual asset money laundering schemes and the forensic and analytical capacity of investigative authorities. Effective virtual asset investigation requires proficiency in blockchain analysis, digital forensics, open-source intelligence (OSINT), and an understanding of the technical architecture of distributed ledger systems, competencies that are not yet systematically embedded within the Rwanda Investigation Bureau or other relevant agencies.

Blockchain analysis involves the identification and clustering of wallet addresses associated with specific actors, the tracing of fund flows across multiple transactions and wallets, and the identification of exchange or VASP accounts through which pseudonymous addresses can be linked to real-world identities. Commercial blockchain analytics platforms such as Chainalysis Reactor, Elliptic Investigator and TRM Labs provide powerful tools for this purpose, but their acquisition and operation require significant financial investment and sustained technical training. Rwanda's current investigative infrastructure does not yet reflect the depth of capability required to deploy these tools effectively at scale.

Digital forensic challenges extend beyond blockchain analysis to the seizure and preservation of digital evidence relevant to virtual asset investigations. Private keys, the cryptographic credentials that control access to virtual asset wallets, must be identified and secured through forensically sound procedures to avoid the risk of triggering wallet security mechanisms (such as multi-signature requirements or time-locks) that could render assets inaccessible. The volatile nature of cryptocurrency markets means that delays in securing evidence can result in significant value loss even where assets are identified and their location known.

B. Pseudonymity and Tracing Difficulties

As noted above, the pseudonymous character of blockchain transactions presents a systemic challenge for investigators. While blockchain transactions are, in principle, publicly visible on distributed ledgers, the association of wallet addresses with identifiable natural persons requires either disclosure by a VASP holding KYC data or sophisticated on-chain analytical techniques. In Rwanda's context, where the regulatory framework for VASPs is nascent and the domestic VASP sector is not yet well developed, investigators may face difficulty obtaining reliable customer identification data even where domestic VASPs are involved in a transaction chain.

The challenge is compounded where virtual assets pass through foreign VASPs not subject to Rwanda's regulatory jurisdiction. In such cases, investigators must rely on mutual legal assistance procedures to obtain customer data from foreign authorities, a process that, even in the most efficient bilateral relationships, involves significant time delays that may allow offenders to move assets beyond the reach of recovery mechanisms. The use of decentralised exchanges (DEXs), which operate without a central operator and do not collect customer data, presents an even more intractable problem: there is, in many cases, simply no custodian from whom identification data can be sought.

The adoption of privacy-enhancing technologies creates further difficulties. Bitcoin mixing services (tumblers) break the transactional link between sending and receiving addresses by pooling funds from multiple users. Monero and similar privacy coins use cryptographic techniques (ring signatures, stealth addresses and confidential transactions) that render transaction tracing effectively impossible using current blockchain analytics methods. Investigators confronted with assets that have passed through such technologies face a fundamental evidential problem: they may be unable to establish the requisite nexus between a specific criminal predicate and the assets sought to be recovered.

C. Cross-Border Jurisdictional Complexity

Virtual assets are inherently borderless: a transaction between a Rwandan wallet and a foreign wallet is technically identical to a domestic transaction, occurring in milliseconds and without the geographic constraints that characterise conventional asset movements. This borderlessness creates acute jurisdictional challenges for investigators, who must determine which law applies, which authority has jurisdiction, and through what mechanism they can access evidence and assets located in foreign jurisdictions.

Rwanda's MLA framework, while aligned with international standards through its treaty obligations under the Palermo Convention and UNCAC, is in practice constrained by limited bilateral treaty relationships, resource constraints within the agencies responsible for processing MLA requests, and the varying levels of responsiveness of foreign jurisdictions. The speed at which virtual assets can be moved and converted into other assets or cash means that the time required to process formal MLA requests often exceeds the window within which protective measures (freezing orders) remain practically effective.

The cross-border dimension also raises difficult questions of proof in Rwandan courts. Where the predicate offence was committed or the proceeds derived in a foreign jurisdiction, investigators must obtain and authenticate sufficient evidence of foreign criminal conduct to satisfy the evidentiary standards applicable in Rwanda's domestic proceedings. This 'predicate proof' requirement is particularly demanding where foreign criminal justice systems operate under different legal frameworks and standards of proof.

D. Resource Constraints and Capacity

Effective virtual asset investigation is resource-intensive, requiring sustained financial investment in training, technology and institutional development. Rwanda's investigative authorities operate under significant resource constraints that limit their capacity to maintain pace with the evolving tactics of virtual asset launderers. The acquisition and maintenance of commercial blockchain analytics subscriptions, the training of sufficient numbers of investigators to apply these tools effectively, and the establishment of dedicated financial crime investigation units with specialised virtual asset expertise all require financial commitments that must compete with other institutional priorities.

Human capital constraints are particularly pressing. Blockchain forensics is a highly specialised field in which global demand for skilled practitioners far outstrips supply. Rwanda's relatively small investigative workforce and compensation structures that may not be competitive with private sector alternatives create recruitment and retention challenges that are difficult to address through conventional human resource strategies. Partnerships with international organisations, including INTERPOL's financial crime and anti-corruption capability,[23] the United Nations Office on Drugs and Crime (UNODC) and bilateral technical assistance programmes, offer partial mitigation, but cannot substitute for the development of sustainable domestic capacity.

V. Prosecutorial Challenges in Virtual Asset Money Laundering Cases

A. Proving the Predicate Offence and Criminal Nexus

The prosecutorial challenge in virtual asset money laundering cases begins with the need to establish, beyond a reasonable doubt, that the assets sought to be recovered represent the proceeds of a predicate criminal offence. In conventional money laundering prosecutions, this requirement is typically met through evidence of specific criminal conduct, such as drug trafficking, corruption or fraud, from which identifiable proceeds flowed into the financial system. In virtual asset cases, establishing this nexus is significantly more complex.

[23] INTERPOL, *INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC)* (Jan. 2022). IFCACC leads INTERPOL's operational support against money laundering associated with virtual assets and against the identification and forfeiture of criminal assets.

The tracing of funds from a predicate offence through multiple blockchain transactions, across different cryptocurrencies and protocols, and through possible privacy-enhancing technologies, generates a complex technical narrative that must be reduced to a form comprehensible to a court. Prosecutors must work closely with expert witnesses, in particular blockchain forensic analysts, to present this evidence in a manner that satisfies the applicable standard of proof while remaining accessible to judges who may lack a technical background in distributed ledger technology. As Sheshi and Treska observe, the complexity of financial crime evidence is itself a systemic challenge that courts and prosecutors must confront, demanding investment in both technical expertise and evidentiary presentation skills.[24]

Rwanda's Law No. 001/2025 provides for a 'proceeds of crime' presumption in certain circumstances, which can assist prosecutors in meeting the evidential burden. However, this presumption must be properly invoked and applied within the constitutional framework protecting individual rights, including the right against self-incrimination and the presumption of innocence. The interface between prosecutorial burden-shifting provisions and constitutional protections has not yet been fully elaborated in Rwanda's jurisprudence, creating uncertainty for prosecutors.

B. Evidentiary Standards and Digital Evidence

The admissibility and weight of digital evidence in Rwandan courts presents a distinct set of prosecutorial challenges. Digital evidence, including blockchain transaction records, exchange account data, digital communications and forensic device extractions, must be obtained, preserved and presented in accordance with applicable rules of evidence to be admitted and relied upon. Rwanda's evidentiary framework, while increasingly attentive to digital evidence, does not yet reflect the comprehensive treatment of electronic evidence contemplated by international best practice standards.

Authentication of digital evidence is a particular concern. Prosecutors must be able to demonstrate that blockchain data presented to a court has not been tampered with and accurately represents the transactions recorded on a public ledger. While the immutability of blockchain records is generally well established in technical terms, translating this technical property into a legally sufficient foundation for the admission of blockchain evidence requires careful evidentiary procedure and, in contested cases, expert testimony. The chain of custody requirements applicable to digital evidence are equally demanding, particularly where evidence has been obtained through international channels.

[24] Sheshi & Treska, *supra* note 7.

Expert witnesses play a critical role in virtual asset prosecution, although their use can present some challenges. The scarcity of individuals qualified to testify as blockchain forensics experts, particularly in Rwanda, means that prosecutors may face difficulty identifying and securing appropriately qualified witnesses. Where foreign expert witnesses are required, issues of admissibility, cost and the availability of such witnesses for cross-examination add further complexity. The development of a cadre of locally qualified expert witnesses is a priority that requires investment in legal and technical education.

C. Identification and Valuation of Virtual Assets

The valuation of virtual assets for the purposes of confiscation proceedings presents challenges that do not arise in the same form in conventional asset recovery cases. The extreme volatility of cryptocurrency markets means that the value of virtual assets at the time of seizure may differ substantially from their value at the time of the predicate offence, the time of the freezing order, or the time of the final confiscation order. This temporal valuation problem has significant practical implications for the quantum of confiscation orders.

Rwanda's law, consistent with international practice, generally provides for confiscation of the value of proceeds of crime rather than in-kind confiscation of specific assets where the original assets are no longer available or identifiable. This 'value confiscation' approach requires prosecutors to establish the value of assets at the relevant time, which in the virtual asset context may involve complex technical and financial analysis. Where assets have been converted or dissipated, prosecutors must also consider whether substitute assets held by the defendant can be confiscated to the equivalent value.

D. Coordination and Institutional Challenges

Effective prosecution of virtual asset money laundering cases requires seamless coordination between multiple agencies: the Rwanda Investigation Bureau (which conducts the investigation and gathers evidence), the Financial Intelligence Centre (which may hold relevant financial intelligence) and the NPPA (which conducts the criminal prosecution). In practice, inter-agency coordination presents challenges related to information-sharing protocols, differing institutional priorities and resource constraints.

The prosecution of complex financial crime cases is also extremely time-consuming and resource-intensive, requiring prosecutors with specialised skills to manage multi-layered evidentiary records over extended periods. Rwanda's current prosecutorial capacity does not yet reflect the depth of specialisation required for the systematic and effective prosecution of sophisticated virtual asset money laundering schemes. Investment in specialised financial crime prosecution units, modelled on the practices of more advanced jurisdictions, is a structural reform that merits serious consideration.

VI. Adjudicative Challenges in Virtual Asset Recovery

A. Judicial Capacity and Technical Understanding

The adjudicative stage of virtual asset recovery presents its own distinctive challenges, centred primarily on the capacity of the judiciary to understand and evaluate complex technical evidence within an appropriate legal framework. Judges in Rwanda, like their counterparts in many jurisdictions, are trained primarily in legal analysis rather than the technical sciences underpinning virtual asset technology. The assessment of blockchain forensics evidence, the evaluation of expert witness testimony on distributed ledger systems, and the application of legal standards to novel technical facts demand a level of judicial technical literacy that must be actively cultivated.

The complexity of virtual asset cases also raises systemic concerns about court efficiency and the appropriate allocation of judicial resources. Complex financial crime trials involving substantial volumes of digital evidence, multiple expert witnesses and intricate transactional narratives can extend over months or years, placing significant demands on judicial time and infrastructure. Rwanda's court system, while notably efficient by regional standards, faces capacity constraints that are likely to intensify as the volume of virtual asset-related litigation increases.

B. Legal Framework Gaps and Novel Legal Questions

Adjudicating courts in Rwanda will inevitably confront novel legal questions for which existing jurisprudence provides limited guidance. The application of established legal principles, such as ownership, possession, constructive trust and proceeds of crime, to virtual assets raises conceptual questions that domestic courts must resolve without the benefit of a developed body of precedent. Is a cryptocurrency 'property' capable of being 'possessed' in the legal sense? Can a non-conviction-based forfeiture order be made in respect of assets held in a cold storage wallet? How should courts treat assets that have been staked in a DeFi protocol or locked in a smart contract?

These are not merely academic questions: their resolution has direct consequences for the effectiveness of asset recovery in practice. A court that declines to treat cryptocurrency as 'property' capable of confiscation under Rwanda's asset recovery statutes, for example, could create a significant loophole in the framework that perpetrators would be quick to exploit.

Rwanda's judiciary must therefore be positioned to engage with these novel questions with both legal rigour and policy awareness, guided by the progressive interpretation principles applicable to remedial legislation.

C. Enforcement of Confiscation Orders

Even where a court issues a confiscation or forfeiture order in respect of virtual assets, the practical enforcement of that order presents challenges that have no close parallel in conventional asset recovery. Unlike a bank account or real property, which can be frozen or transferred by administrative direction to a financial institution or registry, virtual assets are controlled by private cryptographic keys. If a defendant refuses to disclose the private key to a wallet containing assets subject to a confiscation order, the court and enforcement authorities may face an effective impasse.

Rwanda's asset recovery legislation does not yet fully address the mechanisms for compelling disclosure of private keys or for technically accessing wallets where keys are not voluntarily surrendered. The contempt of court framework and compulsion provisions of Law No. 42/2014 offer some basis for coercive measures, but their application to the private key problem requires careful legal analysis and may face constitutional challenges on grounds of self-incrimination. Legislative clarification and, potentially, the development of state-level technical capabilities for hardware wallet forensics would assist in addressing this gap.

D. International Enforcement Challenges

Where confiscation orders relate to assets held in foreign jurisdictions, whether in foreign VASP accounts or in wallets accessible only through foreign intermediaries, enforcement requires international cooperation that may not always be forthcoming. The international asset recovery framework under UNCAC and the Palermo Convention obliges States Parties to give effect to each other's confiscation orders, but in practice this obligation is subject to numerous conditions and limitations, and the practical effectiveness of international enforcement varies enormously between jurisdictions.

Rwanda's bilateral relationships for enforcement of foreign confiscation orders are still developing, and the absence of dedicated bilateral agreements with key virtual asset jurisdictions (including certain offshore financial centres and emerging crypto hubs) creates gaps in the international enforcement architecture. Strengthening these relationships, including through membership of asset recovery inter-agency networks and bilateral mutual legal assistance treaties with key partners, should be a priority for Rwanda's international legal cooperation programme.

VII. Comparative Analysis: The United States Framework

A. Legislative Architecture

The United States possesses one of the most developed and comprehensive legal frameworks for anti-money laundering and asset recovery, reflecting decades of legislative and institutional development. The cornerstone of this framework in the money laundering context is the Money Laundering Control Act of 1986, which first established money laundering as a federal criminal offence,[25] and the Bank Secrecy Act (BSA), which imposes extensive financial institution reporting and record-keeping obligations that serve as the intelligence substrate for money laundering investigations.[26]

The USA PATRIOT Act of 2001 significantly expanded the AML framework, extending BSA obligations to a broader range of financial institutions and strengthening the government's ability to seek information and assets through subpoenas and court orders.[27] In the virtual asset context, the BSA's definition of 'money services business' has been applied to encompass cryptocurrency exchangers and administrators, and the Financial Crimes Enforcement Network (FinCEN) has issued guidance making clear that virtual currency exchangers must comply with BSA registration, recordkeeping and reporting requirements.[28]

Asset forfeiture in the United States operates through two parallel channels: civil forfeiture under 18 U.S.C. § 981, and criminal forfeiture under 18 U.S.C. § 982 (and various other provisions specific to particular offences).[29] Criminal forfeiture, like Rwanda's conviction-based confiscation, requires a criminal conviction and attaches to the defendant's interest in the specific property. Civil forfeiture, by contrast, is a proceeding *in rem* against the property itself, without the requirement of a criminal conviction or even the identification of a specific defendant, a feature that can significantly facilitate asset recovery in complex virtual asset cases where individual culpability may be difficult to establish.

The Civil Asset Forfeiture Reform Act (CAFRA) of 2000 introduced significant procedural safeguards into the civil forfeiture process, including an innocent owner defence and enhanced due process protections, reflecting concerns about the potential for overreach in the exercise of

---

[25] Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207 (codified as amended at 18 U.S.C. §§ 1956, 1957).

[26] Bank Secrecy Act, 31 U.S.C. §§ 5311-5336.

[27] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272.

[28] Financial Crimes Enforcement Network, U.S. Dep't of the Treasury, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (9 May 2019).

[29] 18 U.S.C. § 981 (civil forfeiture); 18 U.S.C. § 982 (criminal forfeiture).

civil forfeiture powers.[30] These safeguards represent an important lesson for jurisdictions considering the expansion of non-conviction-based forfeiture: the power must be exercised within a framework that adequately protects the rights of innocent parties.

B. Virtual Asset Specific Developments

The United States Department of Justice (DOJ) and Internal Revenue Service Criminal Investigation (IRS-CI) have been among the most active global authorities in pursuing virtual asset money laundering cases. High-profile actions, including the seizure of approximately 69,370 Bitcoin traced to the Silk Road dark web marketplace in 2020, then the largest cryptocurrency seizure in United States history,[31] and the 2022 seizure of approximately 94,000 Bitcoin linked to the 2016 Bitfinex hack,[32] have demonstrated both the operational capability and the legal framework supporting large-scale virtual asset recovery in the United States.

The DOJ's National Cryptocurrency Enforcement Team (NCET), established in 2021, represented an institutionalised commitment to virtual asset enforcement, providing a dedicated locus of expertise, coordination and prosecutorial capacity within the federal enforcement architecture.[33] The team worked closely with the FBI's Virtual Asset Exploitation Unit,[34] IRS-CI's cybercrimes function and Homeland Security Investigations, reflecting an integrated, multi-agency approach to virtual asset investigation and prosecution.

The United States has also invested significantly in technical capability, including through inter-agency digital asset working arrangements, partnerships with commercial blockchain analytics firms, and the maintenance of cryptocurrency wallets by federal agencies to manage seized virtual assets pending forfeiture proceedings. The development of secure custody protocols for seized virtual assets, including hardware security modules and multi-signature wallet arrangements, addresses the practical enforcement challenges discussed above in the Rwanda context.

---

[30] Civil Asset Forfeiture Reform Act of 2000, Pub. L. No. 106-185, 114 Stat. 202.

[31] The seizure of 69,370.22491543 Bitcoin traced to the Silk Road marketplace was effected in November 2020 from an individual identified in the forfeiture complaint only as 'Individual X', and was then the largest cryptocurrency seizure in the history of the U.S. Department of Justice. It should be distinguished from the separate seizure of approximately 50,676 Bitcoin, valued at about USD 3.36 billion, taken from James Zhong in November 2021: see Press Release, U.S. Attorney's Office, S.D.N.Y., *U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud* (Nov. 2022).

[32] Press Release, U.S. Dep't of Justice, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* (8 Feb. 2022). Law enforcement seized over USD 3.6 billion in cryptocurrency, comprising approximately 94,000 Bitcoin traced to the 2016 Bitfinex hack.

[33] The National Cryptocurrency Enforcement Team was announced by the Deputy Attorney General in October 2021. It was disbanded on 7 April 2025 by a memorandum of the Deputy Attorney General realigning the Department of Justice's digital asset enforcement priorities; the account in the text therefore describes the position as it stood before that date.

[34] The Federal Bureau of Investigation's Virtual Asset Exploitation Unit was announced in February 2022 and combines cryptocurrency expertise, blockchain analysis and virtual asset seizure capability in a single unit.

C. Lessons for Rwanda

Several features of the United States framework offer valuable lessons for Rwanda. The institutionalisation of virtual asset enforcement expertise through dedicated units such as the NCET provides a model for concentrating scarce specialist capacity where it can be most effectively deployed. The integration of civil and criminal forfeiture pathways, with appropriate procedural safeguards, offers a more flexible and resilient framework than a purely conviction-dependent approach. The investment in inter-agency coordination mechanisms, formalised through memoranda of understanding and joint task forces, addresses the coordination challenges that characterise multi-agency financial crime enforcement. Finally, the extensive United States network of bilateral MLA treaties and its active participation in multilateral asset recovery cooperation forums provide a template for the international cooperation infrastructure that Rwanda should seek to develop.

VIII. Comparative Analysis: The Singapore Framework

A. Legislative Architecture

Singapore has established itself as a global financial hub with a reputation for rigorous regulatory standards and effective enforcement of financial crime laws. Its approach to AML and asset recovery is embodied principally in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA), which provides the legislative basis for the confiscation of proceeds of crime across a broad range of predicate offences.[35] The CDSA establishes conviction-based confiscation and, through its civil recovery provisions, a non-conviction-based pathway for the recovery of assets where criminal proceedings are not feasible or appropriate.

Singapore's approach to virtual asset regulation has evolved through the Payment Services Act (PSA) 2019, as amended by the Payment Services (Amendment) Act 2021, which brought digital payment token (DPT) service providers, including cryptocurrency exchanges, custodians and wallet service providers, within the licensing and AML/CFT regulatory framework of the Monetary Authority of Singapore (MAS).[36] The MAS's AML/CFT requirements for DPT service providers are comprehensive and substantially aligned with FATF standards,[37] including

[35] Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (2020 Rev. Ed.) (Sing.).
[36] Payment Services Act 2019 (Act 2 of 2019) (Sing.), as amended by the Payment Services (Amendment) Act 2021 (Sing.).
[37] Monetary Authority of Singapore, Notice PSN02, *Prevention of Money Laundering and Countering the Financing of Terrorism: Digital Payment Token Service* (issued 5 Dec. 2019, effective 28 Jan. 2020).

the implementation of the FATF travel rule (requiring VASPs to transmit originator and beneficiary information along with virtual asset transfers).[38]

B. Enforcement Approach and Institutional Capacity

Singapore's enforcement approach to virtual asset money laundering reflects the city-state's characteristic emphasis on rule-based regulatory compliance and strong deterrence. The Singapore Police Force's Commercial Affairs Department (CAD) functions as the principal investigative authority for financial crime, supported by a dedicated anti-money laundering team and close working relationships with the MAS, the Attorney-General's Chambers and international counterparts.

In August 2023, Singapore uncovered what became known as the 'S$3 billion money laundering case', one of the largest money laundering operations detected in Asia. The case involved 10 foreign nationals who had used shell companies, real estate, luxury goods and cryptocurrency to launder proceeds of overseas criminal syndicates. The Singapore authorities seized, froze or obtained the surrender of assets ultimately valued at more than S$3 billion, including significant amounts of cryptocurrency, demonstrating the capacity of Singapore's investigative and prosecutorial machinery to handle large-scale virtual asset recovery operations.[39]

Singapore's financial intelligence infrastructure, centred on the Suspicious Transaction Reporting Office (STRO), which functions as the country's financial intelligence unit, provides a high-quality analytical function that processes STRs from a well-developed reporting entity base, including a mature and well-regulated DPT service provider sector, and disseminates timely and actionable intelligence to law enforcement. This financial intelligence ecosystem is a critical enabler of effective virtual asset investigation and represents an aspect of Singapore's institutional architecture that Rwanda is in the earlier stages of developing.

C. International Cooperation and Mutual Legal Assistance

Singapore's position as a major international financial centre and its reputation for regulatory integrity have enabled it to develop an extensive network of bilateral and multilateral cooperation relationships. Singapore is a member of the FATF and of the Asia/Pacific Group on Money Laundering (APG, a FATF-style regional body), its financial intelligence unit is a

---

[38] FINANCIAL ACTION TASK FORCE, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*, Recommendation 15 (as amended Oct. 2018) and Recommendation 16 (the travel rule).

[39] The investigation became public on 15 August 2023, when island-wide raids led to the arrest of 10 foreign nationals and the seizure of assets then valued at about S$1 billion. The value of assets seized, frozen or surrendered subsequently rose to more than S$3 billion, making it the largest money laundering case in Singapore's history.

member of the Egmont Group of Financial Intelligence Units,[40] and it participates in the regional asset recovery inter-agency network for Asia and the Pacific. It has also concluded comprehensive MLA arrangements with numerous jurisdictions. These relationships provide Singapore's law enforcement authorities with effective channels for securing assistance in cross-border virtual asset recovery cases.

Singapore's MLA framework under the Mutual Assistance in Criminal Matters Act (MACMA) is highly regarded for its operational effectiveness, reflecting both the quality of the legal instruments and the institutional capacity and will to deploy them in complex financial crime cases.[41] Rwanda's more limited treaty network and institutional capacity in this area represents one of the most significant gaps relative to the Singapore model, a gap that will require sustained diplomatic and institutional investment to address.

D. Lessons for Rwanda

Singapore's experience offers several lessons particularly relevant to Rwanda's situation. The integration of a mature VASP regulatory framework, including comprehensive KYC requirements, the travel rule and robust STR obligations, has created a data infrastructure that supports effective virtual asset investigation. This underscores the importance of Rwanda's Law No. 023/2026 as a foundational element of an effective asset recovery ecosystem: regulation is not merely a compliance exercise but an intelligence-generating function. The institutional specialisation of Singapore's CAD, with its dedicated financial crime investigation capacity and close relationship with the financial regulator and prosecutorial authority, also offers a model for Rwanda to consider in designing its institutional architecture for virtual asset enforcement. Finally, Singapore's investment in international cooperation, both bilateral and multilateral, demonstrates that for a jurisdiction with limited size and resources, external relationships are a force multiplier that can substantially enhance domestic enforcement capacity.

IX. Synthesis and Recommendations

A. Key Gaps in Rwanda's Framework

The foregoing analysis reveals a constellation of gaps in Rwanda's framework for virtual asset recovery that span the legislative, institutional, technical and international cooperation dimensions. While Rwanda has made significant progress, notably through Law No. 001/2025 and Law No. 023/2026, the distance between a legislative framework and an operationally

[40] Singapore has been a member of the Financial Action Task Force since 1991 and is a founding member of the Asia/Pacific Group on Money Laundering; the Suspicious Transaction Reporting Office joined the Egmont Group of Financial Intelligence Units on 30 June 2002.
[41] Mutual Assistance in Criminal Matters Act 2000 (2020 Rev. Ed.) (Sing.).

effective asset recovery system is substantial, and the specific demands of the virtual asset environment make this translation particularly challenging.

In summary, the principal gaps identified include: (i) insufficient technical capacity in investigative and prosecutorial agencies for blockchain forensics and digital evidence management; (ii) an underdeveloped VASP sector that limits the availability of KYC data to investigators; (iii) limited inter-agency coordination mechanisms for virtual asset cases; (iv) gaps in the legal framework for compelling disclosure of private keys and enforcing confiscation orders against virtual asset wallets; (v) a limited international cooperation network relative to the scale of cross-border virtual asset activity; and (vi) insufficient judicial capacity and technical literacy for complex virtual asset cases.

B. Recommendations

i. Institutional Capacity Building

Rwanda should establish a dedicated Virtual Asset Financial Crime Unit within the Rwanda Investigation Bureau, modelled on the NCET in the United States. This unit should be staffed by investigators with specialised training in blockchain forensics, digital evidence and virtual asset regulation, and should be resourced with access to commercial blockchain analytics platforms. The unit should operate in close coordination with the FIC and the NPPA, with formalised information-sharing protocols and joint operational planning mechanisms.

ii. Legal Framework Enhancement

Rwanda's asset recovery legislation should be amended to address expressly the following: the treatment of virtual assets as property capable of confiscation under Law No. 42/2014; mechanisms for compelling the disclosure of private keys, including coercive contempt provisions with appropriate constitutional safeguards; technical procedures for the seizure, custody and disposal of virtual assets by state authorities; and provisions for value confiscation where virtual assets have been dissipated, converted or concealed.

iii. VASP Sector Development

The effective implementation of Law No. 023/2026 is essential to building the KYC data infrastructure that underpins virtual asset investigation. The Capital Market Authority, working with the National Bank of Rwanda, should prioritise the licensing and supervision of VASPs, with particular emphasis on the implementation of AML/CFT obligations including the FATF travel rule.[42] Public-private engagement with the emerging VASP sector, through industry

[42] FINANCIAL ACTION TASK FORCE, *supra* note 38, Recommendation 16.

consultations, regulatory guidance and the development of compliance standards, will be important in ensuring that regulatory requirements translate into the data quality needed for investigation.

iv. Judicial Capacity Development

The Rwanda Judiciary and the Rwanda Law Reform Commission should collaborate to develop specialist training programmes for judges and court staff on financial crime, digital evidence and virtual asset concepts. Consideration should be given to the designation of specialist financial crime courts or specialist panels within existing courts, providing a concentrated locus of expertise for complex virtual asset cases. Judicial exposure to comparative jurisprudence from the United States, Singapore and other advanced jurisdictions will assist in navigating the novel legal questions that virtual asset cases will present.

v. International Cooperation

Rwanda should prioritise the expansion of its bilateral MLA treaty network to include key virtual asset jurisdictions, and should actively pursue membership or observer status in the relevant multilateral forums for asset recovery cooperation and for virtual asset standard-setting. Bilateral technical assistance programmes with the United States, Singapore and other advanced jurisdictions, leveraging existing diplomatic relationships, offer an efficient pathway to capacity building that complements domestic investment.

vi. Regional Leadership

Within the East African Community and ESAAMLG frameworks, Rwanda has an opportunity to exercise regional leadership on virtual asset governance and asset recovery. The development of model legislative provisions, shared investigative databases and regional training programmes, building on Rwanda's relatively advanced regulatory framework, would not only enhance Rwanda's own capacity but contribute to the broader financial integrity of the region.

X. Conclusion

The challenge of recovering assets derived from virtual asset money laundering is one of the defining financial crime issues of the contemporary era. For Rwanda, a country simultaneously pursuing economic digitalisation and financial integrity, addressing this challenge effectively is a matter of both regulatory credibility and national interest. The analysis presented in this article demonstrates that while Rwanda has taken important legislative steps, particularly through Law No. 001/2025 and Law No. 023/2026, the full realisation of an effective virtual asset recovery regime requires sustained investment across the investigative, prosecutorial, adjudicative and international cooperation dimensions.

The comparative analysis with the United States and Singapore reveals that effective virtual asset enforcement is not primarily a matter of legal architecture, though robust laws are necessary, but of institutional capacity, technical expertise, inter-agency coordination and international integration. Both comparator jurisdictions have invested heavily in these enabling conditions over many years, and their relative effectiveness in virtual asset enforcement reflects these investments. Rwanda's reform trajectory must be calibrated to these lessons, adapting best practices to the country's specific context, resources and developmental stage.

The virtual asset environment will continue to evolve, driven by technological innovation, market dynamics and the adaptive strategies of criminal actors. Rwanda's regulatory and enforcement framework must therefore be designed not merely for the present landscape but for a future characterised by continued technical complexity and cross-border integration. This requires not just specific legal reforms but a sustained commitment to institutional learning, international engagement and the cultivation of technical excellence within Rwanda's financial crime enforcement community.

The asset recovery imperative, that crime must not pay, is no less urgent in the virtual asset context than in any other dimension of financial crime. Indeed, the potential scale of proceeds flowing through virtual asset channels, and the reputational and developmental consequences of Rwanda becoming a conduit or destination for laundered virtual assets, make it more urgent still. The road ahead is long and demanding, but the direction, toward a comprehensive, capacity-rich, internationally integrated virtual asset enforcement framework, is clear.

*****