WERKSMANS
ATTORNEYS



BANKING & FINANCE | REGULATORY

# Cryptocurrency fraud demands more than regulation

18 November 2026 *6 min read*

*by Natalie Scott, Director and Head of Sustainability, and Armand Swart, Director*

The promise of exceptional returns, sophisticated trading technology and an investment that seemingly cannot lose should invite scrutiny. In the crypto asset market, however, these claims have persuaded investors to part with their money before establishing who controls it, how it is being invested, and whether it can be recovered.

International Fraud Awareness Week provides an opportunity to revisit the lessons of crypto asset investment schemes and consider whether South Africa is sufficiently equipped to prevent, detect and prosecute the fraud that accompanies them. The regulatory framework has developed considerably. But regulating crypto assets requires mechanisms and strategies to detect deviations from what is legal, successfully prosecute those who break the law, and recover the proceeds of criminal activity.

On 19 October 2022, crypto assets were declared financial products under the Financial Advisory and Intermediary Services Act 37 of 2002. Providers of advice or intermediary services relating to crypto assets fall within the Financial Sector Conduct Authority's (FSCA) regulatory framework and must meet the applicable licensing, fit and proper, and other regulatory requirements.

Crypto asset service providers (CASPs) are also accountable institutions under the Financial Intelligence Centre Act No 38 of 2001 (FIC Act). Their obligations include registration, customer due diligence, record-keeping and the reporting of suspicious and unusual transactions. These requirements are necessary and important in identifying the people or entities behind crypto asset transactions and detecting the movement of funds, legitimate and otherwise.

The FIC's travel rule, effective from 30 April 2025, also requires relevant CASPs and financial services providers rendering financial services to crypto assets to obtain and transmit prescribed information to the receiving crypto asset services provider about the (sender) originator and

beneficiary (receiver) of crypto transfers. These requirements help investigators connect transactions to identifiable people.

Investors should verify a CASP's authorisation independently with the FSCA and ensure that it covers the services being offered. Authorisation does not guarantee returns or remove the need to scrutinise an investment proposal.

The earlier Mirror Trading International (MTI) scheme illustrates the risks. MTI encouraged investors to transfer Bitcoin into a pooled investment scheme, purportedly managed by an artificial intelligence trading bot and a trading team. It claimed average monthly returns of 10% and more than 200 consecutive days of positive gains. On 26 April 2023, the Western Cape High Court declared its business model unlawful, declared that the trading bot never existed or traded, and ruled all investor agreements void from the outset. MTI turned out to be no more than ponzi scheme and the case is a reminder that claims of sophisticated technology and exceptional returns cannot substitute for proper scrutiny. Crypto asset investors should be on the lookout for promises of unrealistic gains, complex jargon or technology claims (like AI bots), and unlicensed service providers.

Because crypto assets are digital in nature, they cannot be physically held. Transactions are typically recorded on a distributed ledger where the parties may or may not be identifiable. That notwithstanding, investigators can still follow the movement of crypto assets without knowing who in fact controls/ holds the keys to the wallets through which those crypto assets pass.

The ability to trace a transaction should not, however, be confused with the ability to reverse it or recover the crypto assets or cash equivalent. Further, direct crypto asset transfers do not carry the ordinary chargeback protections associated with card payments because they are direct "peer-to-peer" transactions between payers (the customers) and payees (the retailers') wallets, and do not include the usual protective layers or parties authorised/ licensed to accept, process, transfer, confirm and/ or settle payments within a regulated system (such as your card operator, bank and SAMOS operated by the South African Reserve Bank (SARB)). Recovery may require cooperation from service providers and legal action against the persons controlling the crypto assets.

Fraud and money laundering are distinct offences, but they may form part of the same sequence of events. Once investors transfer their crypto assets, unscrupulous sellers may seek to disguise the origin and ownership of the crypto assets. The steps for laundering funds using crypto assets are structurally similar to those for money laundering using FIAT currency.

This includes layering, which is where the source of illicit funds is further disguised by channelling those funds through multiple entities involving numerous transactions. The digital trail can assist an investigation. Its value, however, depends on the ability to connect transactions to individuals, obtain information from service providers and take appropriate steps to preserve the identified assets before they are liquidated or transferred to a jurisdiction with less stringent/identifiable anti-money laundering controls.

On 1 June 2026, the Gauteng High Court, Johannesburg, in *Mangundhla v South African Reserve Bank*, held that Bitcoin constituted both money and capital for exchange-control purposes. In so doing, it declined to follow the Gauteng High Court's earlier decision in *Standard Bank v South African Reserve Bank*, which held that cryptocurrency was neither money nor capital. The SARB and Ms Tshazibana were granted leave to appeal the *Standard Bank* judgment to the Supreme Court of Appeal (SCA) on 17 September 2025; whereas the applicants in *Mangundhla* were granted leave to appeal to the SCA on 20 July 2026. The conflicting Gauteng judgments illustrate the legal uncertainty (whether perceived or otherwise) surrounding cross-border crypto asset transactions. The SCA decisions in both appeals are awaited.

In August 2026, the SARB and National Treasury published the draft Crypto Asset Manual for Cross-Border Activities. Read with the draft Capital Flow Management Regulations, it proposes a framework for cross-border crypto asset activities, including authorisation, reporting and compliance requirements. In his Medium-Term Budget Policy Statement on 21 October 2026, Finance Minister Enoch Godongwana announced further consultation with a view to publishing revised draft regulations, and underscored that the proposed framework remains subject to change.

For investors, the practical implication is that the ease with which a crypto asset can be transferred should never be mistaken for an absence of legal obligations.

The battle against crypto asset crime cannot be addressed through policy alone: the response must also be innovative and practical. Law enforcement, regulators, and the private sector must collaborate on strategies to prevent, detect, combat, and prosecute crimes involving crypto assets. Such an approach, however, requires access to digital forensic tools, specialist investigative expertise and established channels for cooperation with service providers, crypto asset exchanges and foreign regulatory authorities.

The lack of resources available to law enforcement to engage in certain types of investigative work could, for a limited period of time, be mitigated by forming partnerships with the private sector. Training investigators in techniques of detection and investigation relevant to this area is crucial.

International Fraud Awareness Week should prompt authorities to strengthen their capacity to detect, investigate and prosecute crypto asset fraud, and investors to scrutinise crypto asset investments before parting with their money.




**Natalie Scott**

Head of Sustainability

View Profile



**Armand Swart**

Director

View Profile