



Strategic Analysis Report, 2025

Virtual Assets

Financial Intelligence Unit
Nepal Rastra Bank
Baluwatar, Kathmandu

Foreword

The Financial Intelligence Unit, Nepal (FIU-Nepal) serves as the national agency responsible for receiving and analyzing Suspicious Transaction Reports (STRs) and other information relevant to money laundering, terrorist financing, and proliferation financing. It develops intelligence from the collected information and disseminates intelligence reports to the law enforcement agencies. The FIU analysis—a core FIU function—mainly involves tactical, operational, and strategic analysis. Unlike tactical and operational analyses, a strategic analysis is not concerned with a particular STR or case, but rather involves the analysis of broader trends and patterns.

In recent years, the rapid emergence of Virtual Assets and Virtual Asset Service Providers has fundamentally transformed the global financial landscape. While these innovations present opportunities for efficiency and financial inclusion, they also introduce complex risks, particularly related to anonymity, cross-border movement of funds, and regulatory arbitrage that challenge traditional mechanisms of financial system, supervision and law enforcement.

Recognizing these evolving threats, FIU-Nepal has prepared this Strategic Analysis Report on Virtual Assets to assess the domestic and international dimensions of VA-related risks and their implications for Nepal's financial integrity. The report examines patterns and typologies observed in STRs and SARs received by FIU-Nepal, highlights emerging trends, and reviews the legal and institutional responses within Nepal's AML/CFT framework. Case examples from the domestic as well as foreign jurisdictions have also been incorporated to shed light on the trends and modus operandi regarding VA-related financial crimes.

This report underscores the need for continued vigilance, enhanced regulatory coordination, and capacity building among reporting entities, supervisory agencies, and law enforcement bodies. As Nepal moves forward in its digital transformation journey, FIU-Nepal remains committed to strengthening its analytical capability, adopting technology-driven tools and contributing to the collective effort to prevent the misuse of innovative financial products for illicit purposes.

I extend my appreciation to Deputy Director Mr. Sachin Raj Piya and Assistant Director Mr. Kamal Paudel of the Policy Desk, as well as all FIU-Nepal colleagues. Likewise, I would like to acknowledge Assistant Director Ms. Sharada Gurung for her diligent effort in drafting the report. Further, I am grateful to our domestic and international partners for their continued cooperation and support.

Bashu Dev Bhattarai

Director/Head of FIU-Nepal

Table of Contents

1. Introduction	1
1.1 Overview of VAs and VASPs	1
1.1.1 Virtual Assets	1
1.1.2 Ecosystem of Virtual Assets	2
1.1.3 Classification of Virtual Assets	2
1.1.4 Operational Modality of VAs	3
1.1.5 Virtual Assets Service Providers (VASPs)	6
1.2 Scope, Objectives and Limitations of the Report	6
1.2.1 Scope of the Report	6
1.2.2 Objectives of the Report	6
1.2.3 Data Collection for the Report	7
1.2.4 Limitations of the Report	7
2. ML/TF/PF Risks associated with VAs and VASPs	9
2.1 Risks Associated with Virtual Assets (VAs)	10
2.2 Risks Associated with Virtual Asset Service Providers (VASPs)	12
2.3 Threat Landscape	13
2.4 Regulatory Regime around the World	14
3. VA Landscape in Nepal: Emerging trends and typologies	17
3.1 Legal Provision on VAs in Nepal	17
3.2 Emerging Trends and Typologies observed in VAs with Examples/Cases	17
3.3 Virtual Assets Awareness, Investigation and confiscation- challenges	22
4. Review and Analysis of VA-related STRs	25
4.1 Virtual Assets related STRs/SARs and FIU-Nepal	25
4.1.1 RE-wise Virtual Assets related STR/SARs	26
4.1.2 Dissemination of SAR/STRs related with Virtual Assets	26
4.1.3 Dissemination of SAR/STRs related with VAs to Competent Authorities	27
4.2 Analysis of VA related STRs	27
4.2.1 Age group of the individuals reported in VA related STR/SARs	27
5. Findings and Recommendation	31
5.1 Key Findings	31
5.2 Recommendations	32
5.2.1 Recommendations to Reporting Entities	32
5.2.2 Recommendation to LEAs and investigative agencies	33
5.3 Recommendations to regulators/supervisors	34
Annex I : Red flags	35
Annex II : International efforts/practices to prevent VAs and VASPs from misuse by illicit actors	37
Annex III : Public awareness notices	41
Annex IV : Related legal Provisions	44

List of Figures

Figure 3.1	Google Trends: Crypto	22
Figure 3.2	Google Trends: Binance	22
Figure 4.1	VA related STR/SARs received at FIU-Nepal	25
Figure 4.2	RE-wise VA related STR/SARs received at FIU-Nepal	26
Figure 4.3	VA related STR/SARs Disseminated by FIU-Nepal	26
Figure 4.4	VA related STR/SARs Disseminated by FIU-Nepal to Competent Authorities	27
Figure 4.5	Age group of individuals suspected in VAs	28
Figure 4.6	Occupation of individuals suspected in VAs	28
Figure 4.7	Various triggering points for generation of STR/SARs by REs	29
Figure 4.8	Reasons for suspicion of individuals in VAs	29

List of Abbreviations

Abbreviation	Definition
ALPA	Asset (Money) Laundering Prevention Act
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CEF	Cyber Enabled Fraud
CFT	Combating Financing of Terrorism
CIB	Central Investigation Bureau
DLT	Distributed Ledger Technology
DEXs	Decentralized Exchanges
DMLI	Department of Money Laundering Investigation
DPT	Digital Payment Token
DRI	Department of Revenue Investigation
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IMF	International Monetary Fund
LEA	Law Enforcement Agency
ML	Money Laundering
NRB	Nepal Rastra Bank
NFTs	Non-Fungible Tokens
PF	Proliferation Financing
PSD	Payment Systems Department
REs	Reporting Entities
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
VA	Virtual Asset
VASP	Virtual Assets Service Provider

1. Introduction

1.1 Overview of VAs and VASPs

1.1.1 Virtual Assets

Virtual assets (VAs) have emerged as one of the most transformative innovations in the global financial landscape. They can function as a medium of exchange, a store of economic value, a unit of account, or an investment; although their effectiveness in these roles can vary and is still evolving. Cryptocurrencies, non-fungible tokens (NFTs), security tokens, and stablecoins are the major types of VAs. Unlike traditional assets, they are not issued or backed by any central authority but instead maintained on decentralized, blockchain-based networks. Hence, they do not include digital representations of fiat currencies. The [Financial Action Task Force \(FATF\)](#) has defined virtual assets as *a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*¹.

The publication of the Bitcoin white paper by [Satoshi Nakamoto in 2008](#), followed by the launch of the [Bitcoin network in 2009](#), is widely regarded as the starting point of the modern VA ecosystem and the first practical implementation of the blockchain technology. Bitcoin is a decentralized peer-to-peer electronic cash system that enables online payment directly among the parties without relying on financial institutions or trusted third parties. Traditional electronic payments require intermediaries, leading to higher costs, fraud risks, and limits on small transactions. Bitcoin addresses these issues by introducing a peer-to-peer network that timestamps transactions using proof-of-work (PoW) which records the transactions immutably on a distributed ledger known as the block-chain². Currently, VAs are broadening the boundaries of existing financial and regulatory paradigms due to its innovation at the nexus of finance, technology, law, and economics. It challenges traditional banking and finance by offering faster transactions, increased efficiency, broader access to financial services and new investment opportunities. However, the significant challenges that it has brought in terms of regulatory uncertainty, cyber security threats, high volatility, consumer protection, and technological complexity might prevent its wider acceptance and long-term incorporation into the global financial system. Many countries like Nepal have restrictive approach on the use of VAs. The users engaging in VAs could face legal repercussions including fines, penalties and imprisonment in Nepal.

In October 2018, the FATF expanded its standards to address the growing use of VAs and new types of service providers. It adopted new glossary definitions for VA and VASP, and updated Recommendation 15 to ensure consistent global regulation and mitigate ML/TF risks associated with VA activities clarifying that standards apply to both virtual-to-virtual and virtual-to-fiat transactions as well as interactions involving VAs. In June 2019, the FATF further issued an Interpretive Note to Recommendation 15 to provide guidance on applying a risk-based approach, supervising and licensing VASPs, implementing customer due diligence and record-keeping requirements, reporting suspicious activities, enforcing sanctions, and enhancing international cooperation in relation to VA activities³.

1 See more at <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

2 See more at <https://bitcoin.org/bitcoin.pdf>

3 See more at <https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

1.1.2 Ecosystem of Virtual Assets

The ecosystem of VAs is a dynamic and rapidly evolving digital landscape that encompasses all entities, technologies, platforms, services and regulatory frameworks involved in the creation, transfer, storage, management and exchange of virtual assets. It is powered by blockchain and distributed ledger technology (DLT), which provides the foundational infrastructure for secure and transparent transactions.

The key components of virtual asset ecosystem include:

- **Virtual assets:** These are digital forms of value such as cryptocurrencies (e.g., Bitcoin, Ethereum), stablecoins, utility tokens, and other tokenized assets that can be traded, transferred, or used for payments and investments.
- **Participants:** This includes users who hold and transact virtual assets via digital wallets, miners or validators who maintain the blockchain network's integrity, VASPs such as crypto exchanges, brokers, wallet providers, and custodians who facilitate access and services around VAs.
- **Products and Services:** The ecosystem offers direct access to VAs through crypto firms, as well as indirect access via cryptocurrency derivatives, exchange-traded funds, investment funds, and shares in blockchain companies. Innovations also include decentralized finance (DeFi), non-fungible tokens (NFTs), metaverse-related assets, and asset tokenization.
- **Technology:** Blockchain and DLT underpin the ecosystem, enabling secure, transparent, and decentralized record-keeping and transactions. This technology supports the issuance, trading, and governance of VAs without centralized intermediaries.
- **Regulatory frameworks:** Given the risks associated with VAs including financial stability, money laundering/terrorist financing (ML/TF), and consumer protection concerns, various jurisdictions have developed or are developing regulatory frameworks to oversee VASPs and virtual asset activities. These frameworks aim to balance innovation with risk mitigation. The FATF recognized its potential misuse and has provided guidelines urging member countries to regulate and supervise VASPs, ensuring compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) and reporting of suspicious transactions/activities to Financial Intelligence Unit (FIU).

1.1.3 Classification of Virtual Assets

The FATF, as the global standard-setter for AML/CFT, has been instrumental in providing guidance on how its recommendations apply to VAs and VASPs. The IMF largely aligns with these definitions in its policy advice and technical assistance to member countries. The classification of VAs is primarily driven by the need for regulatory clarity and to address risks such as ML/TF. It is based on several key factors, depending on its characteristics, functions, and usage.

Initially viewed primarily as speculative investments or digital collectibles, VAs now also feature in payments, remittances, and value storage necessitating a more organized and comprehensive approach for classification.

Category	Description	Examples	Key Features
Cryptocurrencies	Decentralized digital currencies primarily used as a medium of exchange or store of value	Bitcoin, Ethereum	Operate on blockchain/DLT; peer-to-peer transfer; volatile

Category	Description	Examples	Key Features
Utility Tokens	Tokens granting access to a product or service within a blockchain ecosystem	Filecoin, Golem	Do not confer ownership or investment rights; Provide access to services
Security Tokens	Digital tokens representing ownership or investment rights in assets	Tokenized stocks and bonds	Subject to securities laws; confer ownership or dividends
Stablecoins	Tokens pegged to fiat currencies or assets to reduce price volatility	Tether (USDT), USD Coin (USDC)	Designed for price stability; used for payments and transfers
Tokenized Assets	Digital representations of real-world assets enabling fractional ownership	Tokenized real estate, art	Represent physical assets; enable liquidity and trading
Non-Fungible Tokens (NFTs)	Unique digital assets representing ownership of specific items or rights	Digital art, collectibles	Unique, indivisible tokens; represent distinct ownership

1.1.4 Operational Modality of VAs

Virtual assets operate through decentralized networks that record and verify transactions using distributed ledger technology (DLT). Each transaction is stored in a digital ledger that is shared among network participants, ensuring transparency and immutability without the need for a central authority. VAs operate through cryptographic and blockchain technologies. Blockchain is decentralized, distributed and public immutable digital ledger that records transactions across multiple computers. It uses a decentralized peer-to-peer network in which every participant (or node) keeps a copy of the ledger eliminating the need for a central authority. Transactions are clustered into blocks and each block is connected to the previous one via cryptography which ultimately forms a chronological chain of blocks. The network independently verifies each transaction, adds it to the ledger and timestamps it. It is impossible to alter/manipulate the records of transactions once it is entered into the block and added to blockchain which ensures immutability and security of the data.

1) Creation/Acquisition:

Blockchain networks are the foundation for the VAs. VAs are created through;

- Mining (Proof of Work): Like Bitcoin where users validate the transactions by solving complex mathematical problems or cryptographic puzzles and produce new coins.
- Minting (Proof of Stake): Consensus mechanism where owners stake their cryptocurrency to earn the opportunity to validate transactions and create new blocks.

2) Storage:

VAs are stored in digital wallets which consist of:

- a) **Public Key:** It serves as account number of the user and used to receive the assets.
- b) **Private Key:** It acts as password which is used to authorize the transactions.

Wallets can be custodial and non-custodial which are explained as follows: ;

- **Custodial:** Custodial wallets are managed by third-party entities, such as centralized exchanges like Binance or financial service providers. These entities hold and manage private keys on behalf of users/customers. The custodian has control over private keys, meaning they manage the security and access to funds of users. Generally, it is more user-friendly, offering password recovery options and customer support. Even though custodians implement security measures, sometimes, they can be targets for hacks. Custodial services may be subject to regulatory oversight, and users should be aware of the terms and conditions governing their assets.
- **Non-custodial:** They are controlled by users. Non-custodial wallets give users full control over their private keys and, consequently, their assets like MetaMask. Users are solely responsible for managing their private keys, providing complete control over their assets. It may have a steeper learning curve and lack features like password recovery, placing the onus of security entirely on the user. While it is less susceptible to centralized hacks, the loss of private keys or seed phrases can result in irreversible loss of assets. Non-custodial wallets typically offer greater privacy and may not be subject to the same regulatory scrutiny as custodial services.

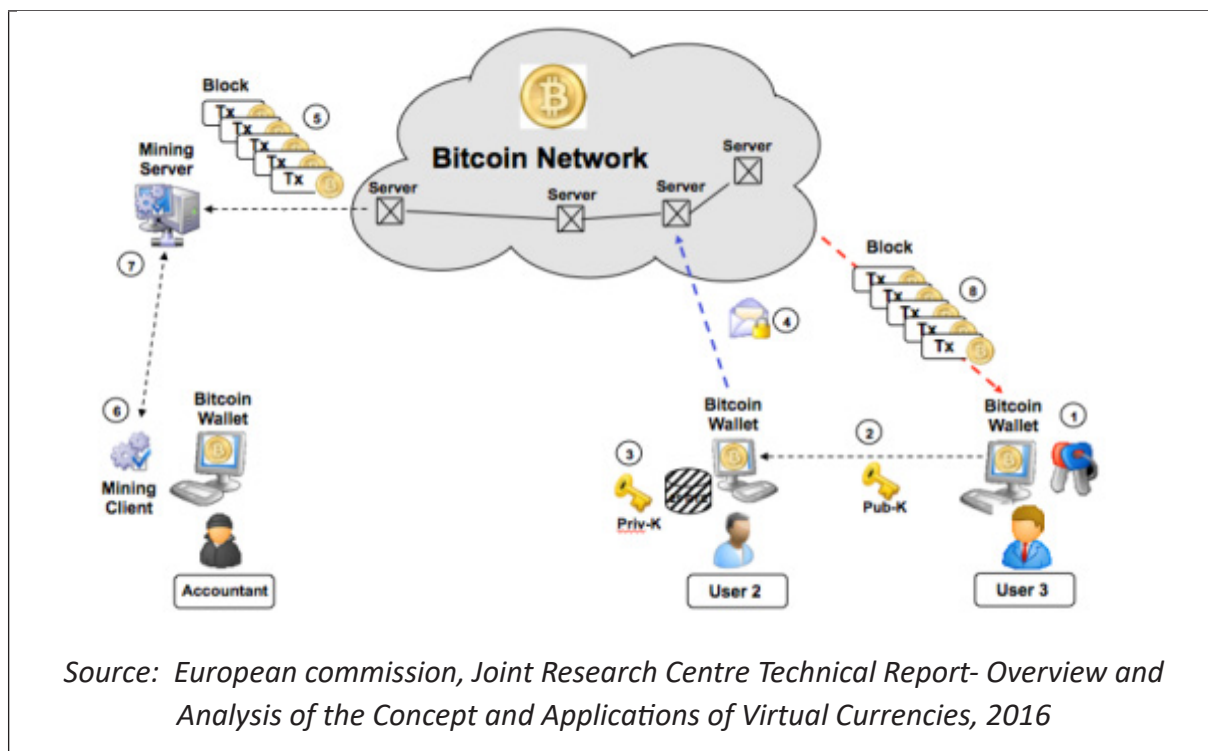
Hence, custodial wallets are ideal for users who prioritize convenience and are comfortable entrusting their assets to third-party providers whereas non-custodial wallets are suitable for users who value complete control over their assets and are prepared to manage their own security measures. Understanding these differences is essential for making suitable decisions about how to store and manage virtual assets securely.

3) Transactions

When a VA is transferred from one user to another, that transaction is signed by private key of the particular user. Then, it is shared to the blockchain network. Miners confirm it based on the network's consensus mechanism; the transaction is added to a block and becomes permanent.

4) Verification and Security

Each blockchain has protocols that ensure only valid transactions are added. Once added, data is immutable and publicly available to the block explorer.



The diagram above represents the transaction cycle of VAs, using a Bitcoin transfer as an example. After a transaction is recorded in a block, it becomes permanent and cannot be altered or undone. Multiple transactions are grouped together to form a block, and as more transactions take place, new blocks are added. This ongoing sequence of blocks is referred as the Blockchain.

Joint Research Centre Technical Report- Overview and Analysis of the Concept and Applications of Virtual Currencies published by European commission (2016) explained that every Bitcoin user must generate a Bitcoin address to send and receive payments. A user's public key is used to derive their Bitcoin address, which acts as their account address. The private key is the most crucial element for securing bitcoins, accessing the wallet, and making payments. Its possession signifies ownership of the bitcoins in the wallet, making private keys a prime target for illegal attacks. The recipient shares their Bitcoin address with the sender where accuracy of the Bitcoin address is paramount. Once the sender has the correct Bitcoin address, they use their private key to open their local wallet. This decrypts all stored transactions, making the amounts and total balance accessible. If the wallet balance is sufficient, an outgoing transaction is created and then encrypted using the recipient's public key. Encrypted transactions are sent to the Bitcoin network. These nodes broadcast the received transaction to all other servers in the network. Bitcoin network nodes collect individual transactions and package these transactions into a specially structured block and send it to mining servers. Mining servers distribute these blocks to their clients, called miners. Miners perform an iterative cryptographic procedure. When a miner successfully creates a correct hash for a block, they return it to their mining server, which then sends it to the Bitcoin network. Each Bitcoin network node distributes the newly validated block to all linked Bitcoin wallets. Then, the transaction is validated⁴.

4 European commission (2016), JRC Technical Report- Overview and Analysis of the Concept and Applications of Virtual Currencies, see more at <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105207/lbna28386enn.pdf>

1.1.5 Virtual Assets Service Providers (VASPs)

VASPs are entities or businesses that facilitate activities involving VAs and play a central role in the virtual asset ecosystem by enabling users to access, exchange, transfer, and safeguard these assets. The FATF defines VASPs as any natural or legal person who conducts as a business one or more of the following activities for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies
- exchange between one or more forms of virtual assets
- transfer of virtual assets
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

VASPs are the backbone of the VA ecosystem, providing essential services that range from basic exchange and storage to complex financial offerings and, most importantly, acting as the primary agents for regulatory compliance. They enable individuals and businesses to interact with virtual assets in a more accessible and user-friendly way.

1.2 Scope, Objectives and Limitations of the Report

1.2.1 Scope of the Report

This report is mainly focused on the ML/TF/PF risks associated with the use of VAs and VASPs, the emerging trends and typologies observed in Nepal related to the use of VA, the review and analysis of the nature of STRs received and analyzed by FIU-Nepal, and the key findings and recommendations regarding the strategic analysis of VA-related activities in Nepal.

The report also covers other risks related to the use of VAs, the benefits VAs could provide in cross border transactions and financial inclusion, legal provisions on VAs and VASPs in Nepal, and case examples of VA related activities that have been linked to other financial crimes and ML/TF activities.

The analysis of the nature of STRs is based on the STRs submitted to FIU Nepal by different REs, mainly commercial banks, in the last five years. The case examples have been mainly retrieved from the news published on the website.

1.2.2 Objectives of the Report

The main objective of this study is to analyze emerging trends and typologies pertinent to VAs and provide recommendations to the concerned stakeholders based on the key findings. The related objectives include:

- To enhance understanding of VAs and VASPs and risks, especially ML/TF related risks associated with them.
- To assess the emerging trends and typologies related to VAs based on the nature of STRs/SARs submitted to FIU-Nepal and data available on external sources.

- To provide further guidance on red flag indicators that can help REs detect VA-related transactions and its potential misuse.
- To offer policy recommendations to REs, regulators/ supervisors, and LEAs regarding the use of VAs.

1.2.3 Data Collection for the Report

Both primary and secondary sources of data have been used.

- Primary sources encompass data from internal source i.e, goAML system. Required data on STR/SARs received, analyzed and disseminated, retrieved from goAML database for the period of January 1, 2021, to July 16, 2025. In addition, REs report the STR/SARs related with VAs and VASPs under “Money, Banking, Finance, Foreign Exchange” category of predicate offences prior January 02, 2025 as use of virtual currency had not yet been classified as a separate offence. Following its incorporation as separate predicate offence dated January 02, 2025, relevant STRs/ SARs have since been reported under “virtual currency” category. Therefore, data is retrieved using the keywords such as Cryptocurrency, Crypto, Bitcoin, Ethereum, Binance, MetaMask etc.
- Secondary sources of data include the publications by FATF, IMF, European Commission, reports published by other jurisdictions and different external sources including notices of key national agencies (Nepal Police, Department of Revenue Investigation), media reports, blogs etc.

1.2.4 Limitations of the Report

Limitations of this report include:

- Although goAML offers important primary data on STRs/SARs linked to virtual assets, it reflects only the suspicious activities/transactions that have been reported. It does not account for the broader range of illicit or unregulated virtual asset activities taking place outside the formal financial system or those that remain undetected. Additionally, the ability and reach of reporting entities—particularly Designated Non-Financial Businesses and Professions (DNFBPs)—in Nepal to identify and report virtual asset-related STRs are still evolving which could have resulted in underreporting.
- Data from internal sources was extracted using keywords like Cryptocurrency, Crypto, Bitcoin, Ethereum, Binance, MetaMask, etc., and STR/SARs related to virtual assets and VASPs reported under the “ Money, Banking, Finance, Foreign Exchange” category prior January 02, 2025 as it was not incorporated as distinct predicate offence previously. Therefore, the dataset is entirely based on the information provided by REs in STR/SARs and their individual assessments or judgments.
- Published data related to VAs is limited within LEAs, and information on prosecutions or court judgments is also limited.

2. ML/TF/PF Risks associated with VAs and VASPs

Virtual assets (VAs) and Virtual Asset Service Providers (VASPs) present significant risks related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF) due to their unique characteristics and operational environments. While virtual assets themselves possess characteristics that can be exploited for illicit finance, it is often through the entry and exit points facilitated by VASPs that these risks materialize into actual illicit financial flows.

According to Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2025)⁵, there has been a continued rise in the use of stablecoins by illicit actors, terrorist financiers, and drug traffickers since the 2024 Targeted Update. Currently, stablecoins are involved in the majority of illicit activities. The widespread adoption of stablecoins or virtual assets (VAs) could further escalate the risks of illicit financial activities, particularly with uneven implementation of FATF Standards for VAs and VASPs across jurisdictions.

Virtual Assets Risk Assessment Report Singapore (2024) suggested that the virtual asset-related cases observed in Singapore involve Digital Payment Tokens (DPTs)/ cryptocurrencies. These DPTs pose higher inherent ML/TF/PF risks due to their pseudonymous nature and the ability to transfer value across borders almost instantly. Although transactions using virtual assets are generally recorded on publicly accessible blockchains, criminals can exploit tools and techniques like mixers²³ and chain-hopping to obscure transaction trails. Furthermore, there are privacy/anonymity-enhanced coins that conceal transaction details and ownership information to evade tracing efforts by law enforcement agencies⁶.

Strategic Analysis Report (2021-22) of Financial Monitoring Unit of Pakistan concluded that Virtual assets have been identified as posing considerable risks related to ML and TF highlighting the need for a coordinated response from all relevant stakeholders to develop an effective regulatory framework. Despite repeated public advisories and the State Bank of Pakistan's declaration that virtual assets are not considered legal tender, their use continues to grow rapidly within society⁷. Considering its growing use, The gazette of Pakistan published an ordinance on 8th July, 2025 to establish a regulatory authority (Pakistan Virtual Assets Regulation Authority) for the licensing, regulation and supervision of virtual assets and virtual assets service providers with objectives of protecting the customers and investors by enforcing appropriate safeguards, and promote innovation and financial inclusion within in framework that manages risks and maintains market integrity⁸.

5 See Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2025), <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>

6 See Virtual Assets Risk Assessment Report Singapore (2024), Page 12, <https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/virtual-assets-risk-assessment.pdf>

7 See Strategic Analysis Report (2021-22), Virtual Assets- The emerging risk of Money Laundering and Terrorism Financing, <https://www.fmu.gov.pk/docs/2022/Strategic-Analysis-Report-Virtual-Assets-2022.pdf>

8 See <https://www.scribd.com/document/909568407/Virtual-Assets-Ordinance-2025>

According to Virtual Asset Risk Assessment (VARA) 2024, Malaysia⁹, VA is not recognized as legal tender and is not accepted as a mode of payment for purchase of goods and services. The materiality of VA illicit activities in Malaysia is negligible but observed a notable upward trend due to its increasing association with high-risk ML crimes. More than 90% of VA cases in Malaysia involves Fraud activities and common modus operandi includes investment scams/ darknet activities, use of cross-border virtual asset platforms to carry out layering and abuse of commonly used virtual assets like Bitcoin, Ethereum, and Tether.

Fintech note published by IMF (2021) suggested that though VAs are commonly used for legitimate purposes, they have also been exploited for unlawful activities. Numerous cases involving large-scale fraud, theft, money laundering, and other crimes have seen the movement of millions of U.S. dollars through virtual assets. While transactions, such as those involving Bitcoin, are often recorded on public blockchains and can be tracked from one wallet to another, identifying the individuals behind these wallets is difficult. This difficulty is heightened by the use of technologies specifically intended to obscure transaction trails. These include privacy-enhancing tools like mixers, layered encryption, stealth addresses, and ring signatures, which limit the visibility of transaction details, including the amount and parties involved. Additionally, some techniques obscure identities by hiding associated secondary information. Hence, countries must enhance their understanding of virtual asset technologies, strengthen the skills of policymakers, supervisors, FIUs, law enforcement, and the judiciary and engage closely with VASPs. Strong international cooperation is vital due to the cross-border nature of VAs. The broader AML/CFT community including the FATF and IMF should continue offering guidance, monitoring developments, and supporting capacity building to ensure effective implementation of global standard¹⁰.

2.1 Risks Associated with Virtual Assets (VAs)

VAs present a wide range of risks that stem from their decentralized, borderless, and largely pseudonymous nature. They pose significant money laundering and terrorist financing concerns, as users can rapidly transfer value across jurisdictions without intermediaries, often using privacy tools that obscure identities and transaction trails. Weak traceability also increases the risk of their misuse for tax evasion, capital flight, online gambling, hundi operations, and other illicit activities.

- **Anonymity and Decentralization:** VAs enable peer-to-peer transactions that are often anonymous or pseudonymous, making it difficult to identify parties and trace illicit funds.
- **Rapid Cross-Border Transfers and Scams:** VAs allow instant, global transfers without intermediaries, facilitating the quick movement of illicit proceeds across jurisdictions and provides the space for frauds and investment scams as well.

9 See <https://www.sc.com.my/api/documentms/download.ashx?id=13d1e6d6-3148-4a85-8559-8db4a0049b8c>

10 See Fintech Notes, IMF, 2021-Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1) Some Legal and Practical Considerations, <https://www.imf.org/en/publications/fintech-notes/issues/2021/10/14/virtual-assets-and-anti-money-laundering-and-combating-the-financing-of-terrorism-1-463654>

Box 1. South Africa's Mirror Trading International (MTI) – Crypto Investment Scam

In February 2021, a media report revealed that MTI is being investigated after it was provisionally liquidated in December 2020, with regulators now calling for more power to prosecute perpetrators of fraud and oversee dealing in cryptocurrencies. The scheme presented itself as a passive income source. According to its website, users simply deposit a minimum of \$100 worth of Bitcoin, and MTI promised to grow it using an AI-powered foreign exchange trading software. The group said that customers can achieve consistent daily returns of 0.5%, which would translate to yearly gains of 500%. Algorithmic trading is a common premise for many cryptocurrency investment scams.

In August 2020, cryptocurrency website CoinDesk encouraged all MTI users to withdraw their funds as soon as possible, citing the decision of Texas state regulators to formally label the company a scam, as well as a pending investigation by South Africa's Financial Services Conduct Authority (FSCA). On December 18, 2020, the FSCA acted against MTI after its investigation found that the company falsified trade statements, didn't declare losses, and committed other acts of fraud to deceive the market.

The investigation also found that MTI had over 16,000 Bitcoin of claimed customer investment funds unaccounted for. MTI claimed to have transferred those funds to a new FX trading platform after its old platform banned MTI due to its scamming reputation, but the new platform says these funds were never deposited. Since those charges were filed, MTI customers have complained that they can no longer access or withdraw funds they've deposited to the platform, and MTI chief executive Johan Steynberg has disappeared.

Source: Businesstech, <https://businesstech.co.za/news/finance/468162/south-africas-mti-named-as-the-biggest-crypto-investment-scam-in-the-world/>

- **Use of Privacy Coins and Mixing Services:** Criminals exploit privacy-enhancing technologies and tumblers to obscure transaction trails and launder money.
- **Darknet Marketplaces and Illicit Trade:** VAs are widely used to purchase illegal goods and services, including drugs and weapons, on darknet platforms.

Box 2. Mexican Sinaloa Cartel-Use of Cryptocurrency in Drug Trafficking

According to media report, U.S. drug enforcement agents seized more than \$10 million in cryptocurrency linked to Mexico's Sinaloa cartel during raids that also netted massive quantities of fentanyl and other drugs. The Sinaloa cartel is one of six Mexican drug trafficking groups that President Trump has designated as global "terrorist" organizations. The cryptocurrency seizure in Miami was part of nationwide operations that netted 44 million fentanyl pills, 4,500 pounds of fentanyl powder and nearly 65,000 pounds of methamphetamine since January, 2025.

The Drug Enforcement Administration (DEA), in coordination with its FBI partners seized over \$10 million dollars in cryptocurrency, directly linked to the Sinaloa cartel.

Source: CBS NEWS, <https://www.cbsnews.com/news/u-s-drug-raids-net-10-million-in-crypto-linked-to-notorious-mexican-sinaloa-cartel-officials-say/>

- **Terrorist Financing:** Terrorist groups and extremist organizations use VAs to receive and transfer funds anonymously, including donations to conflict zones.
- **Sanctions Evasion:** VAs can be used to circumvent international sanctions, enabling proliferation financing and illegal trade.
- **Limited Regulatory Oversight:** Many countries lack comprehensive regulations, creating loopholes exploited by criminals.

Box 3. Abuse of virtual assets by Terrorist Groups

Jihadi terrorist groups are increasingly exploiting virtual assets to finance their operations, using the anonymity and decentralized nature of cryptocurrencies to evade counter-terrorist financing (CFT) controls. Groups such as Hamas, Hezbollah, Palestinian Islamic Jihad (PIJ), and Islamic State Khorasan (ISK) have intensified the use of social media to solicit crypto donations, capitalizing on encrypted transactions and blockchain technologies that complicate detection and enforcement. Despite efforts by global authorities—including the U.S. Treasury, Israel’s National Bureau for Counter Terror Financing, and FATF—to seize wallets and disrupt illicit crypto flows, blocking these transactions remains challenging. Recent cases highlight the severity of the threat: ISK attackers involved in the 2024 Crocus City Hall massacre received crypto funds shortly before the attack, and the U.S. Treasury sanctioned Gaza-based exchange Buy Cash for supporting Hamas’ military wing. The arrest of Tornado Cash developer Alexey Pertsev further underscores the role of crypto-mixing tools in laundering terrorist funds. Although groups like Hamas once claimed to move away from Bitcoin, they continue to receive significant cryptocurrency donations across various blockchain networks, with many organizations shifting from Bitcoin to TRON for enhanced privacy. Seizures by Israeli authorities—\$41 million from Hamas and \$94 million from PIJ—demonstrate the scale of terrorist financing through virtual assets, reaffirming the growing challenge for global CFT efforts.

Source: The Soufan Center, <https://thesoufancenter.org/intelbrief-2024-october-16/>

2.2 Risks Associated with Virtual Asset Service Providers (VASPs)

VASPs facilitate the exchange, transfer, and custody of virtual assets, but their operations also pose specific ML/TF/PF risks:

- **Unlicensed or Unregulated VASPs:** Many VASPs operate without licenses or in jurisdictions with weak AML/CFT controls, increasing vulnerability to misuse.

Box 4. Phishing Scam in Binance

In January 2025, National Cyber Security Centre NCSC, Switzerland revealed that they have seen an increase in calls from purported banks about alleged security problems or fake invoices from various service providers. What is special about these cases is that the victims are not tricked into clicking on a link, but into calling a number. Phone calls allow scammers to better engage with victims and keep them on the line – this extra effort is likely to be worthwhile as it increases the scammers’ chances of success. Last week, the crypto trading platform Binance was the focus of scam attempts. Scammers now use all channels available to them for phishing scams. In particular, phishing by telephone has recently become more common. A phishing attempt in the name of the cryptocurrency exchange Binance attracted particular attention. The attackers used various stories to try and get the victim to call them.

In one case, the victim received an SMS claiming that their passkey had been reset and that if it wasn’t them, they should call Binance. A Swiss phone number was provided. In another version of the scam, victims receive an SMS claiming that a new smart contract or device has been added to their account. Again, they are asked to call the number provided if this was not them. Scammers make it look like their text messages are coming from the real Binance phone number. Because the messages appear in the same SMS folder on your phone as legitimate Binance messages, it is very difficult to tell that they are fraudulent. Interestingly, most of the messages are addressed to people who actually have an account with Binance: in virtually all cases reported to us, the victims had also received legitimate SMS messages from Binance before they were scammed.

Source: National Cyber Security Centre (NCSC), Switzerland https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/wochenrueckblick_3.html

- **Inadequate Customer Due Diligence:** Weak or absent KYC processes allow criminals to use VASPs to convert illicit funds into virtual assets or vice versa without detection.
- **Complex Transaction Chains:** VASPs may process layered or complex transactions that obscure the origin and destination of funds, complicating investigations.
- **Cross-Border Regulatory Arbitrage:** Criminals exploit differences in regulatory regimes by using VASPs in low-compliance jurisdictions to launder money or finance terrorism.
- **Use in Terrorist Financing:** VASPs have been linked to cases where terrorist organizations receive or move funds, sometimes via exchanges in regions with insufficient controls.
- **Challenges in Law Enforcement:** Authorities often face difficulties in tracing virtual assets held or moved through VASPs due to limited access to information and technical complexities.

Box 5. Bybit Cyber Attack

On February 21, 2025, a group of hackers from North Korea pulled off the largest cryptocurrency heist in history after stealing \$1.5 billion in Ethereum tokens from the Dubai-based cryptocurrency exchange ByBit. The hackers exploited a free storage software product that ByBit used to move Ethereum to another location, most likely coupled with phishing attacks to access control and download malware. It is estimated that at least \$160 million of the funds stolen from ByBit were laundered within the first 48 hours of the attack. Although ByBit does not offer services or products in the United States, the hack's ripple effects hurt the global crypto market. The price of Bitcoin experienced a 20 percent drop from its all-time high in January and renewed concerns about the security of these decentralized transactions.

Source: Center for Strategic & International Studies,

<https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation#:~:text=On%20February%2021%2C%202025%2C%20a,Dubai%2Dbased%20cryptocurrency%20exchange%20ByBit>.

2.3 Threat Landscape

The case examples in the boxes show the risks associated with the use of VAs and VASPs. These cases represent such uses around the world. The threat landscape with major actors, motivations, and enablers are as follows:

Actors	Motivations	Enablers
• Scammer companies/ Fraudsters • Illegal traders, • Drug cartels, • Terrorist groups • Cybercriminal groups	• Financial gain by scamming unsuspecting general public, • Profit generation through illegal trade and transfer, • Circumvent traditional financial system, • Maintain secrecy through encrypted, decentralized system • Strategic Disruption	• Cryptocurrency technology and infrastructure, • Misleading promises, • Regulatory gaps, • Social media platforms, • Digital infrastructure vulnerabilities • Phishing techniques • Vulnerable free storage software

Considering threats that involve various actors, motivations, and enablers, as well as, vulnerabilities in VA and VASP sectors, international organizations such as the FATF, the IMF are continually working to develop and implement standards that require VASPs to act as responsible gatekeepers to prevent the abuse of these innovative technologies for illicit purposes. The FATF also adopted an Interpretive Note to Recommendation 15 that sets out the application of the FATF Standards to virtual asset activities and service providers. From an AML/CFT perspective, the key concern lies in the pseudonymous and borderless nature of VAs transactions. These features make it difficult to identify beneficial owners, trace cross-border transfers, and enforce reporting or sanctions obligations. Moreover, the use of mixers (Online services or software that blend multiple users' cryptocurrency transactions together to obscure the origin and destination of funds), privacy coins (Cryptocurrencies designed with built-in anonymity features (e.g., Monero, Zcash, Dash), and decentralized exchanges (DEXs) -platforms that allow users to trade crypto directly with each other (peer-to-peer) without intermediaries or central custody can further obscure transaction trails, challenging both FIUs and law enforcement agencies.

2.4 Regulatory Regime around the World

Despite ML/TF risks linked with the use of virtual currency, many jurisdictions around the world have refrained from the outright ban. In fact, some jurisdictions have shifted from prohibiting VAs to regulating them. Countries around the world see VAs as a part of the fourth industrial revolution and banning them would risk missing out on long-term economic benefits.

VAs have driven financial innovation, enabling new business models such as tokenization, programmable money, and smart contracts. This has led to increased efficiency and better interoperability. A regulated ecosystem could attract fintech startups, investments, and high-skilled jobs contributing to the national competitiveness.

VAs also potentially enhance financial inclusion lower cost and improved outreach. VAs enable low-cost, cross border transfers, especially for migrant workers, small entrepreneurs and people without access to traditional banking. The decentralized platforms also offer faster, cheaper payment solutions, supporting digital financial inclusion goals.

The transactions through VAs are also more transparent and traceable than cash. Blockchain systems offer auditable transaction trails. LEAs can track suspicious activities using blockchain analytics, sometimes more efficiently than cash. Regulated models allow supervisory authorities to monitor VA wallets and VASPs.

A recent study¹¹ on the role of cryptocurrency in cross-border transactions shows significant faster settlement and reduced transaction costs making cryptocurrency a highly efficient alternative to traditional banking systems.

The FATF endorses regulation, albeit under risk-based approach, not prohibition of VAs and VASPs. Many jurisdictions such as EU, UK, Singapore now operate under a "same risk, same regulation" principle. The outright ban may push activities underground, reducing visibility for regulators and increasing ML/TF risk. A regulated environment may actually keep VA activities within the formal financial system, enabling KYC/AML obligations, record keeping, as well as, licensing and supervision. This may reduce criminal abuse compared to an unregulated or banned jurisdiction.

11 https://www.researchgate.net/publication/388931317_The_Role_of_Cryptocurrency_in_Cross-Border_Transactions_Opportunities_and_Risks_for_Banks

According to the Atlantic Council¹², among the 75 countries in the study, cryptocurrency (a form of VA) is legal in 45 countries, partially banned in 20, and generally banned in 10. In twelve G20 countries, representing over 57% of the world's GDP, cryptocurrencies are fully legal. Regulation is under consideration in all G20 countries. However, both emerging-market and advanced economies still lag on comprehensive regulation and oversight. Only 28 of the 75 countries studied have regulations for taxation, AML/CFT, consumer protection, and licensing. As per the study, cryptocurrency adoption rates are weakly correlated with regulatory restrictiveness. Even for countries with partial or general bans in place, adoption rates remain high, suggesting that bans are generally ineffective.

12 <https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker/>

3. VA Landscape in Nepal: Emerging trends and typologies

3.1 Legal Provision on VAs in Nepal

Nepal's legal framework prohibits all virtual asset activities, maintaining a hardline approach that prioritizes financial stability, AML/CFT compliance, and consumer protection. Nepal Rastra Bank Act, 2002 (2058 BS) empowers the Nepal Rastra Bank (NRB) to regulate monetary and foreign exchange policies, issue currency, and manage the country's foreign exchange reserves. The Foreign Exchange (Regulation) Act 2019 establishes the legal framework for regulating foreign currency, foreign exchange transactions and cross-border movement of monetary instruments in Nepal. The Act requires individuals, firms and institutions to obtain a license from NRB to buy, sell, borrow, lend or transfer foreign exchange, and mandates that such transactions follow the procedures and exchange rates determined by the Bank. NRB has issued the public notice stating that the use of virtual currency is illegal and could result in legal punishment as virtual currencies are not legal tender and have not obtained legal recognition as currency or foreign exchange and such transactions could lead to outward foreign investment.

National Criminal Code Section 262(A) (amended on 2024/04/12 AD) specifically defines virtual assets (including information, code, token, cryptocurrency, or similar virtual assets) and prohibits their production, sale, trade, storage, or transfer for payments or business transactions in Nepal, unless issued or recognized by the Nepal Rastra Bank. This amendment explicitly criminalizes virtual asset-related activities, making them not just regulatory breaches but criminal offenses with penalties including imprisonment and confiscation of properties.

Regulatory frameworks of Nepal maintain a strong stance against virtual assets, primarily due to concerns about capital flight, financial stability, consumer protection, and the potential for illicit activities like ML/TF. While the global landscape of VA regulation is evolving, Nepal has consistently opted for a prohibitive approach, making any involvement in virtual assets highly risky and illegal within the country.

3.2 Emerging Trends and Typologies observed in VAs with Examples/Cases

Although Nepal has outlawed all VA-related activities, several underground and cross-border schemes involving VAs have emerged. Its informal and often illicit use persists. Modus operandi associated with VAs often intertwine with existing financial crimes due to the inherent features of VAs (cross-border, pseudo-anonymous) and the lack of a regulated framework.

(i) Illegal Foreign Exchange and Remittance (Hundi Operations)

Individuals use virtual assets, particularly crypto or Bitcoin, to bypass formal banking channels for cross-border money transfers. Funds are converted into crypto in one country, sent to Nepal, and then converted back into NPR (or vice-versa) through informal networks of "exchangers" who operate illicitly. This evades foreign exchange regulations, taxes, and AML/CFT checks.

Box 6. Hundi Operations and Crypto Settlement

Mr. RS and his spouse Ms. RA are suspected to be involved in hundi and crypto-currency. Mr. RS is associated with XYZ Company and maintained account at bank X. While reviewing his account, volume of transactions is significantly increasing and deposits are made by multiple unrelated third parties where most of the credit transactions are cash deposit and purpose of transaction is mentioned as borrowing return. Then, funds are transferred to accounts of different parties on same day or next day through clearing by segregating the transactions into smaller amounts. The repeated use of “borrowing return” as the transaction purpose raises concerns regarding the legitimacy and actual source of these funds. Furthermore, his spouse and mother’s account also found at bank X and he is likely to be the ultimate beneficial owner of those accounts as well.

Ms. RA is employed as a counselor at an educational consultancy as per the KYC maintained at Bank Y. Transaction volume of Ms. RA in bank X and Bank Y is significantly higher. Nature and purpose of transaction observed in the accounts of Ms. RA is similar to her spouse Mr. RS’s account where most of the credit transactions are cash deposits mentioning “borrowing, borrowing return” as transaction purpose. Furthermore, Ms. RA has received NPR 20 million from ABC Company and NPR 1.9 million from the individual Mr. AG who is reportedly involved in crypto-currency as per adverse media report.

Considering the transaction patterns and the financial linkages observed in the accounts of both Mr. RS and Ms. RA, they are suspected of involvement in money laundering associated with hundi operations and crypto-currency transactions, where cryptocurrency has been used for hundi settlement.

Source: FIU Case Analysis

Details of the Case

- **Modus Operandi:**
Cash deposits by unrelated individuals into accounts held by Mr. RS and his family members. Use of misleading transaction purposes “borrowing return” to disguise illegitimate funds. Immediate or next-day outward transfers to multiple parties, suggesting layering of funds. Structuring transactions into smaller amounts to avoid detection. Receiving large sums (e.g., NPR 20 million from ABC Company and NPR 1.9 million from AG), with Mr. AG reportedly involved in cryptocurrency, indicating possible crypto-based hundi settlement. Transactional behavior of both spouses mirrors each other indicating to coordinated illicit financial activity.
- **Impact/ Victims:**
Formal financial system-misuse of regulated institutions for illegal value transfer.
General public and the national economy-capital leakage, foreign exchange risks, and distortion of legitimate financial flows.
- **Operational Base:**
Bank X and Bank Y of Nepal where Mr. RS and his family members maintained accounts.
- **Arrests and charges:**
Possible charges against money laundering and hundi operations.

(ii) Online Frauds

In Nepal, cryptocurrency trading through use of money acquired from online fraud has become a major criminal concern despite the government’s outright ban on virtual assets. Coordinated law enforcement action and heightened public awareness is essential to prevent victimization of online crypto frauds.

Box 7. Online Financial Scam and Cryptocurrencies Fraud

The Central Investigation Bureau (CIB) of Nepal Police uncovered an international network involved in large-scale online financial scams and cryptocurrency fraud worth over Rs. 3 billion. The group operated across Nepal and India, targeting bank and digital wallet users through phishing, social engineering, and fraudulent digital advertisements. CIB arrested multiple individuals and seized high-tech equipment, cash, mobile devices, cheques, and evidence of crypto-based laundering activities.

Source: republica, <https://myrepublica.nagariknetwork.com/news/cib-busts-international-online-scamming-racket-15-80.html>

Details of the case:

- **Modus operandi:**

The scammers posed as bank and digital wallet officials to obtain users' otp/pin credentials, then, illegally accessed the accounts and transferred victims' funds. They also used whatsapp, telegram, facebook, and similar platforms to spread fake job ads, work-from-home offers, gambling links, and high-income schemes to trick users into sharing their account details and access the users' banks and wallets using cyber phishing. Additionally, they paid individuals to open bank and wallet accounts using their personal documents, later using these "mule accounts" to receive, layer, and move illicit money. The group further laundered stolen funds by converting them into cryptocurrency.

- **Impact/ victims:**

Banks and digital wallets who were deceived into sharing their otp/pin and had their account balances drained. Banks and digital wallets also affected by fraud, reputation damage, and increased financial risk. Individuals who provided accounts for the use by fraudsters may face legal risks or financial consequence

- **Operational base:**

Primary base in nepal and cross-border links with india. Involvement of suspects from bihar indicates integration with international scam and crypto networks. Operations heavily relied on social media, messaging apps, and online financial networks.

- **Arrests and charges:**

Arrested suspects, seized computers, mobile phones, cheques and cash.

(iii) Concealment of Nature Of Business and Cryptocurrency Trading Under Its Cover

The use of legitimate-seeming businesses as a cover for illicit cryptocurrency trading and related financial crimes is a notable and growing trend in fraudulent activities worldwide including Nepal. This method leverages the complexities of modern business operations and the pseudonymous nature of cryptocurrencies to evade detection by authorities and financial institutions.

Box 8. Trading of Cryptocurrencies under the cover of Registered Business Entities

In July 2025, the Central Investigation Bureau (CIB) of Nepal Police arrested 52 individuals, including six Chinese nationals, for their involvement in an illegal call center operation that used the “Metoo” dating app and other platforms to conduct a cryptocurrency and dating scam.

Source: The Kathmandu Post, <https://kathmandupost.com/national/2025/07/02/52-people-including-six-chinese-nationals-arrested-for-online-dating-scam-and-illegal-crypto-trade>

Details of the Case:

- **Modus Operandi:**
Scammers created fake profiles on the “Metoo” dating app to lure victims, promising high returns on investments in unregulated cryptocurrency schemes.
- **Impact/ Victims:**
The operation targeted individuals for financial exploitation through social manipulation.
- **Operational Base:**
The group operated under the guise of a legally registered company called “Social Software Development Company Pvt Ltd” with a call center in Lalitpur and a branch in Kathmandu.
- **Arrests and Charges:**
The suspects were charged with offenses related to digital currency under Nepali law. Police confiscated a significant amount of cash, mobile phones, and laptops.

(iv) Use of Money Mules

The use of money mules in virtual assets is a significant concern in Nepal. This method is frequently employed by criminals to bypass the formal financial system and launder illicit funds. Money mules act as an intermediary, adding layers of distance between the initial illicit activity and the final beneficiaries of the funds, making it harder for law enforcement to trace the money trail. In some cases, whole family members account have used as facilitators or money mules.

Box 9. Family Involvement in Cryptocurrency Trading

On January 25, 2022, the Department of Revenue Investigation (DRI) filed a case at the Kathmandu District Court against four individuals from a family in Lamkichhuha Municipality, Kailali, for alleged involvement in large-scale cryptocurrency trading. The DRI has demanded **Rs. 370 million** in fines, citing significant unaccounted transactions carried out through the family members’ bank accounts.

Source: Nepal Press, <https://english.nepalpress.com/2022/01/25/dri-files-complant-against-4-members-of-a-family-for-involvement-in-crypto-currency-trading/>

Details of the Case:

- **Modus Operandi:**
The key suspect, Mr. DK, allegedly conducted extensive cryptocurrency trading by using not only his own bank account but also those of his sister, father, and a friend. By dispersing transactions across several accounts, he attempted to obscure the volume and origin of funds, indicating an effort to avoid regulatory detection. Significant sums were moved through those accounts.

- **Impact/ Victims:**

Misuse of bank accounts and unregulated crypto trading undermined the transparency and stability of Nepal's financial monitoring framework and challenged regulatory integrity.

- **Operational Base:**

Banking channels within Nepal were used for crypto-related financial movements.

- **Arrests and charges:**

Suspects were charged with unauthorized cryptocurrency trading and misuse of banking system with Rs. 370 million in fines.

(v) Online Gambling and Cryptocurrencies

The intertwining of online gambling and cryptocurrencies is another challenge for Nepal. Despite clear legal prohibitions and ongoing enforcement efforts, the borderless nature of both activities, combined with the anonymity offered by crypto, allows these illicit operations to persist in informal sectors. Cryptocurrencies are used in online gambling in many cases.

Box 10. Online Gambling and Cryptocurrencies.

Five youths were arrested for their involvement in illegal cryptocurrency trading and online gambling, conducted from the residence of RG in Anupam Tol, Pokhara-14. The group ran large-scale financial transactions using multiple person and relatives' bank accounts.

Source: Himal Press, <https://en.himalpress.com/five-arrested-in-pokhara-for-illegal-cryptocurrency-trading-online-gambling/>

- **Modus Operandi:**

The group organized gambling activities in three daily shifts, each handling up to USD 3,000 in transactions, managed from Rupendra's home. They opened bank accounts in their own names and in the names of relatives to conduct and conceal illegal transactions. They relied on WhatsApp, Telegram, Cash App, and Crime App to conduct gambling operations, communicate, and move the funds. Most suspects were relatives, enabling trust-based coordination for high-volume gambling and crypto transactions.

- **Operational Base:**

The operations were conducted from the residence of Rupendra GC in Pokhara-14, Kaski. Rupendra, an IT engineer working in the USA for the past 10 years and currently pursuing a PhD, coordinated operations while on leave in Nepal. Some suspects used their businesses (a fancy store and a consultancy) to support or mask financial activities.

- **Victims:**

Nepal's financial system and regulatory framework have incurred losses due to illegal gambling activities, unauthorized cryptocurrency trading, and the misuse of bank accounts. Online gambling schemes pose significant financial risks to individuals, who are often targeted through digital platforms.

- **Arrests and Charges:**

The suspects have been charged with the illegal use of cryptocurrency and involvement in online gambling activities. Mobile phones, laptops, and cash were seized during the operation.

3.3 Virtual Assets Awareness, Investigation and confiscation- challenges

Nepal has not formally recognized or regulated VAs and VASPs. However, law enforcement agencies have increasingly encountered VA-related activities during investigations into financial crimes. Most cases identified so far involve the use of cryptocurrencies such as Bitcoin and USDT to facilitate cross-border payments, online gambling, hundi operations, and other unauthorized financial transactions. In several investigations, authorities have observed that individuals used unlicensed digital wallets and peer-to-peer platforms to conduct virtual currency transactions outside the formal financial system. These activities often bypass existing regulatory controls, creating challenges for monitoring, tracing, and enforcing compliance.

Law enforcement agencies including the Nepal Police, Central Investigation Bureau (CIB), and Department of Revenue Investigation (DRI) along with FIU-Nepal have reported instances where virtual assets were used to obfuscate fund flows, remit money unlawfully from abroad, or settle transactions related to illegal online gambling and hundi operations. Due to the absence of licensed VASPs, there is a big challenge in confiscation of virtual assets. However, several cases have involved the seizure of electronic devices, cash, and transaction records linked to VA-related offenses.

Figure 3.1 Google Trends: Crypto

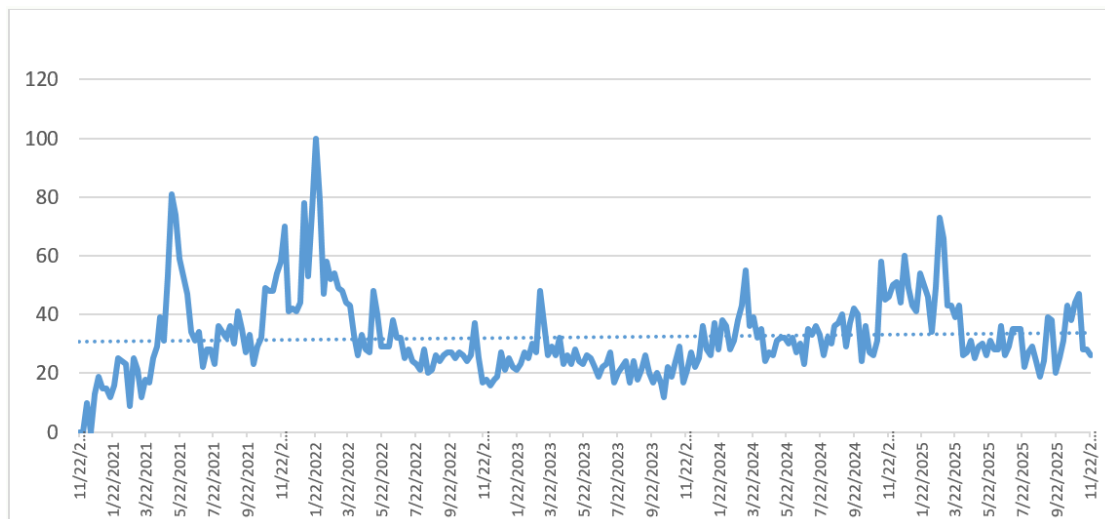
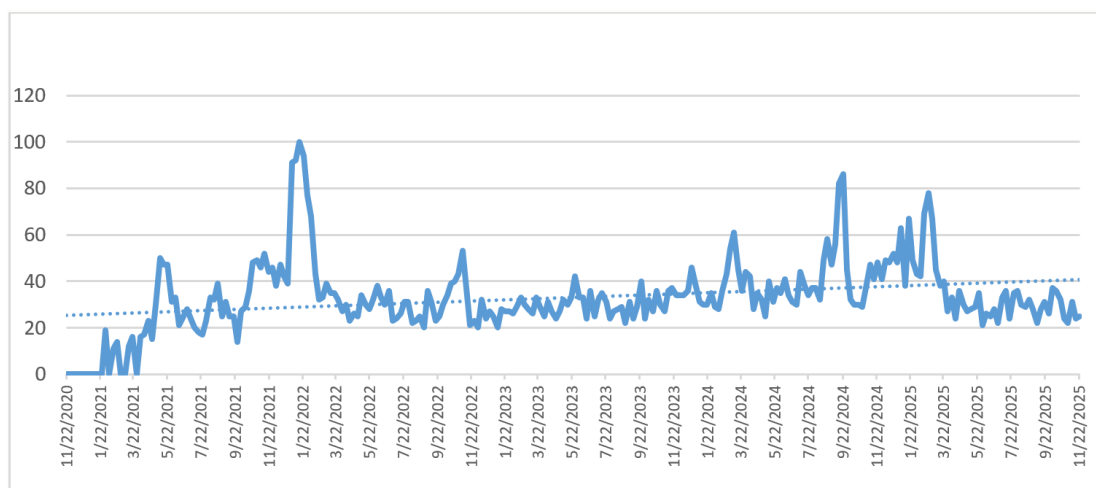


Figure 3.2 Google Trends: Binance



The figures above provide quick snapshots of rising public interest/ awareness pertinent to VAs and VASPs in the context of Nepal. The data is extracted through Google Trends using keywords “Crypto” and “Binance”. The google trends show that there was a peak interest (as shown by Score 100) just after the Covid-19 pandemic. The interest waned afterwards but rose in late 2024 and early 2025.

Despite the legal prohibition, investigating and confiscating VA present unique and significant challenges for Nepalese authorities, as evidenced by the cases reviewed in this report.

The challenges include:

Technical and Expertise Hurdle : Law enforcement agencies are undertaking initiatives to acquire specialized blockchain forensic tools and build the capacity of trained personnel to analyze complex cross-border transactions—particularly those involving mixers, privacy coins, and decentralized exchanges (DEXs) which require extended time for full implementation.

Jurisdictional and Cross-Border Hurdles: The borderless nature of VAs means illicit funds are often moved through VASPs in other jurisdictions, complicating evidence gathering and asset recovery. Effective international cooperation, as facilitated by FIU-Nepal’s Egmont Group membership, is critical but often slow.

Legal and Procedural Ambiguity: The current legal framework lacks clear procedures for the seizure, secure custody, and management of private keys as well as the eventual disposal of confiscated virtual assets. The example from China and Hong Kong (Annex II), where a formal mechanism was created to liquidate seized crypto via licensed exchanges, highlights a potential model, but one that requires a legal foundation Nepal currently lacks.

Asset Volatility and Preservation: The high volatility of virtual assets poses a practical challenge, as the value of confiscated assets can diminish significantly during lengthy investigation and judicial processes.”

4. Review and Analysis of VA-related STRs

4.1 Virtual Assets related STRs/SARs and FIU-Nepal

FIU-Nepal plays a crucial role in the country's AML/CFT, serving as the central agency for receiving, analyzing, and disseminating financial intelligence as mandated by Asset (Money) Laundering Prevention Act (ALPA), 2008. While Nepal has a blanket ban on VAs, FIU-Nepal is keenly aware of their misuse for illicit activities and is actively working to enhance its capacity for improved analysis of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) related to them.

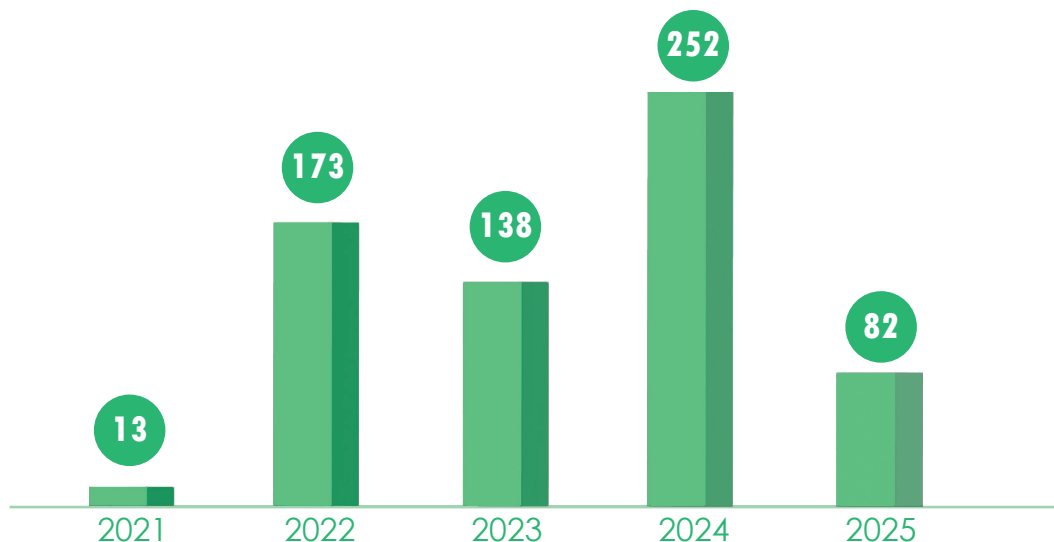
While the use of mixers, privacy coins, and decentralized exchanges is not legally permitted in Nepal, instances of indirect exposure through cross-border online platforms have been observed in STR/SAR analysis. These typologies represent emerging global risks that FIU-Nepal must continue to monitor for potential domestic implications.

Consequently, FIU-Nepal's focus in this context is not on the underlying technological design but on the analytical implications for financial intelligence gathering, STR/SAR analysis, and inter-agency coordination. Understanding of VAs and VASPs helps FIU-Nepal anticipate typologies, recognize emerging ML/TF risks, and recommend proportionate regulatory or supervisory measures consistent with FATF Recommendations 15 and 16.

The use of virtual currency was not previously designated as a distinct predicate offense; therefore, VA-related STRs/SARs were earlier reported under the "Money, Banking, Finance, Foreign Exchange" category. With its formal inclusion as predicate offence dated January 02, 2025 through Nepal Gazette, REs are now obliged to report STR/SARs under this new offense category.

The chart below depicts total SARs/STRs related with virtual assets based on data retrieved from goAML database using the keywords such as Cryptocurrency, Crypto, Bitcoin, Ethereum, Binance, MetaMask etc.

Figure 4.1 VA related STR/SARs received at FIU-Nepal

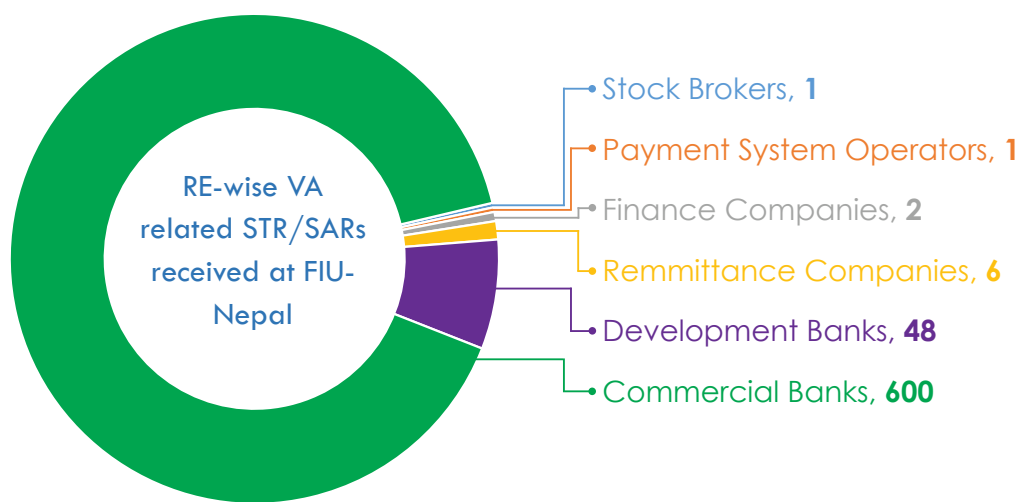


The total number of STR/SARs from the REs related with virtual assets exhibited a fluctuating pattern from 2021 to July 16, 2025. In 2021, 13 STR/SARs were reported, which increased to 173 in 2022. The number reached to 138 in 2023 and increased to 252 in 2024. As of July 16, 2025, 82 STR/SARs have been reported.

4.1.1 RE-wise Virtual Assets related STR/SARs

Total number of virtual assets related STR/SARs received at FIU-Nepal during the period of January 1, 2021 to July 16, 2025 via goAML web reporting was 658. Figure below presents RE- wise reporting of VA related STR/SARs.

Figure 4.2 RE-wise VA related STR/SARs received at FIU-Nepal

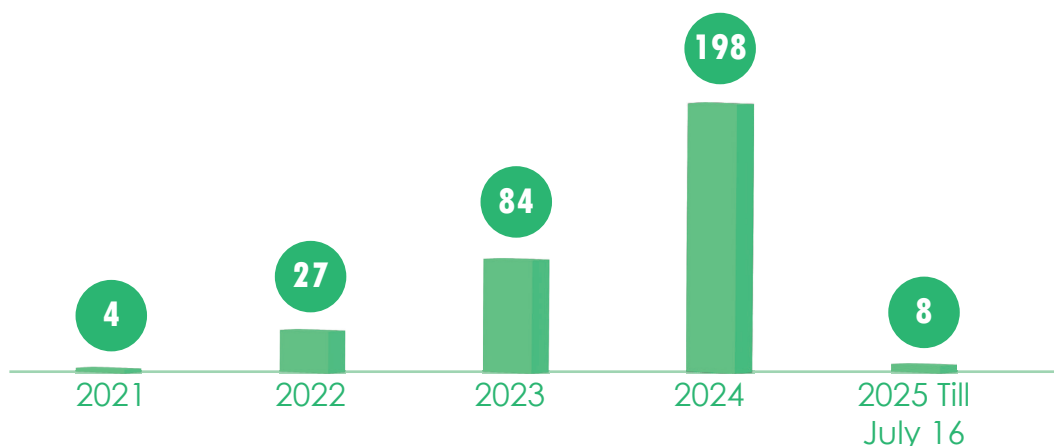


Commercial banks were the source for the highest number of STRs/SARs related with virtual assets, submitting a total of **600** reports. Development banks submitted **48**, followed by remittance companies with **6** and finance companies with **2**. Only a single STR/SAR was reported by a payment system operators and stock brokers as illustrated in the above figure.

4.1.2 Dissemination of SAR/STRs related with Virtual Assets

The total of number of SAR/STRs disseminated for the period of January 1, 2021 to July 16, 2025 is presented in the below figure.

Figure 4.3 VA related STR/SARs Disseminated by FIU-Nepal



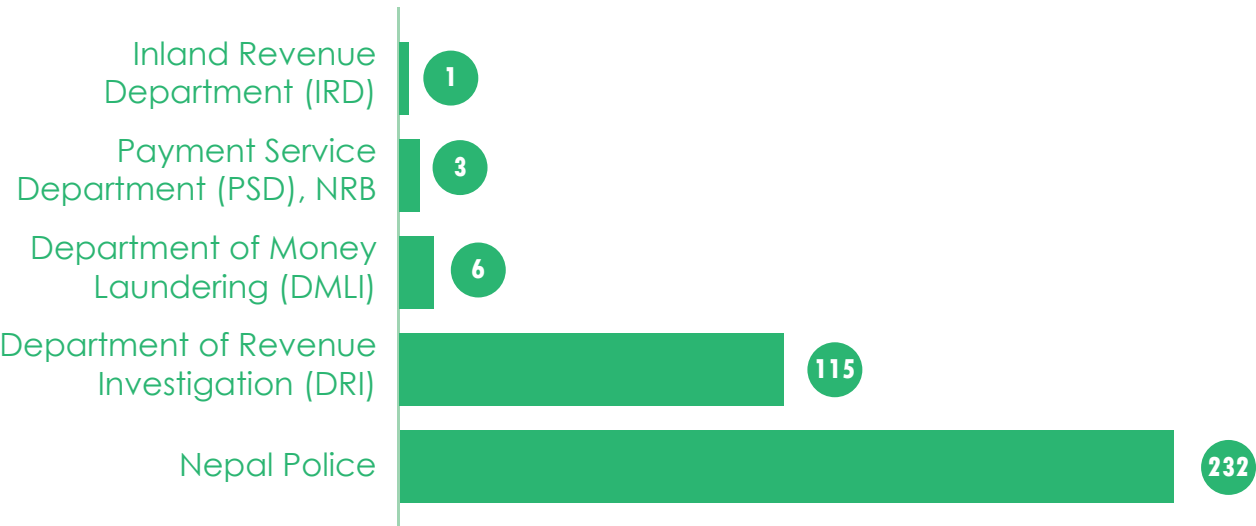
*The STR/SARs disseminated in a year includes those received by FIU-Nepal in the previous year as well.

A total of 321 STR/SARs related with virtual assets were disseminated by FIU-Nepal to LEAs and investigative agencies for further investigation. The number of dissemination continuously increased from 2021 to 2024.

4.1.3 Dissemination of SAR/STRs related with VAs to Competent Authorities

Financial intelligence produced from analysis of SAR/STRs related with Virtual Assets were disseminated to different LEAs, investigative agencies and other competent authorities.

Figure 4.4 VA related STR/SARs Disseminated by FIU-Nepal to Competent Authorities



The figure above illustrates that the Nepal Police is the primary recipient of financial intelligence related to VAs, with a total of 232 STR/SARs disseminated to them for further investigation. Among 232 disseminations to Nepal Police, 195 STR/SARs were disseminated to Nepal Police only and remaining 37 were disseminated to other agencies as well along with Nepal Police based on the intertwining of other predicate offences.

Similarly, 115 STR/SARs were disseminated to Department of Revenue Investigation, six to Department of Money Laundering, and one to Inland Revenue Department for investigation. Three STR/SARs were disseminated to Payment Service Department, NRB for supervisory review.

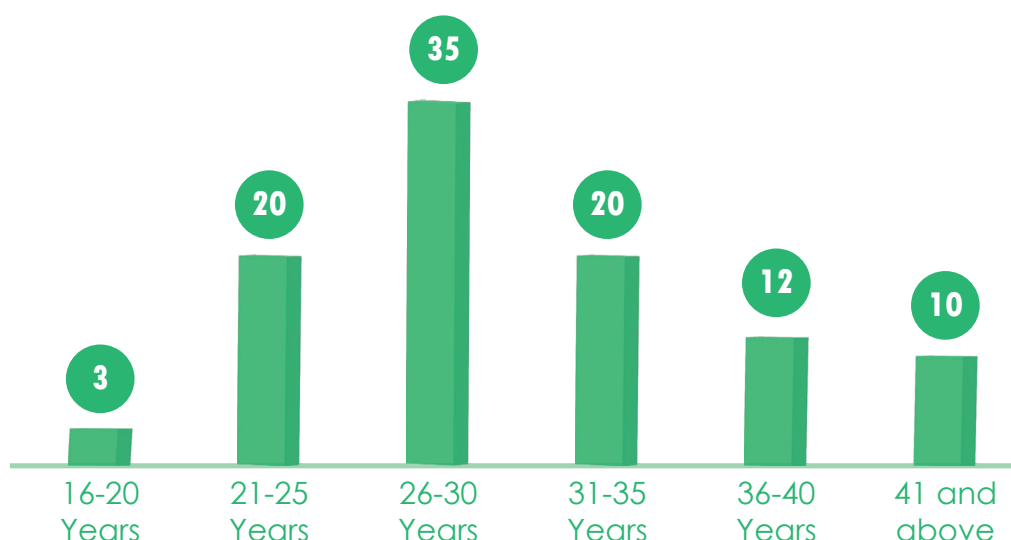
4.2 Analysis of VA related STRs

To get the clear understanding of VAs, STR/SARs reported to FIU Nepal from 2022 to July 16, 2025 were analyzed where 25 STR/SARs from each year have been incorporated in this report based on simple random sampling.

4.2.1 Age group of the individuals reported in VA related STR/SARs

Among the 100 STR/SARs, the individuals under different age group is presented in the below figure.

Figure 4.5 Age group of individuals suspected in VAs

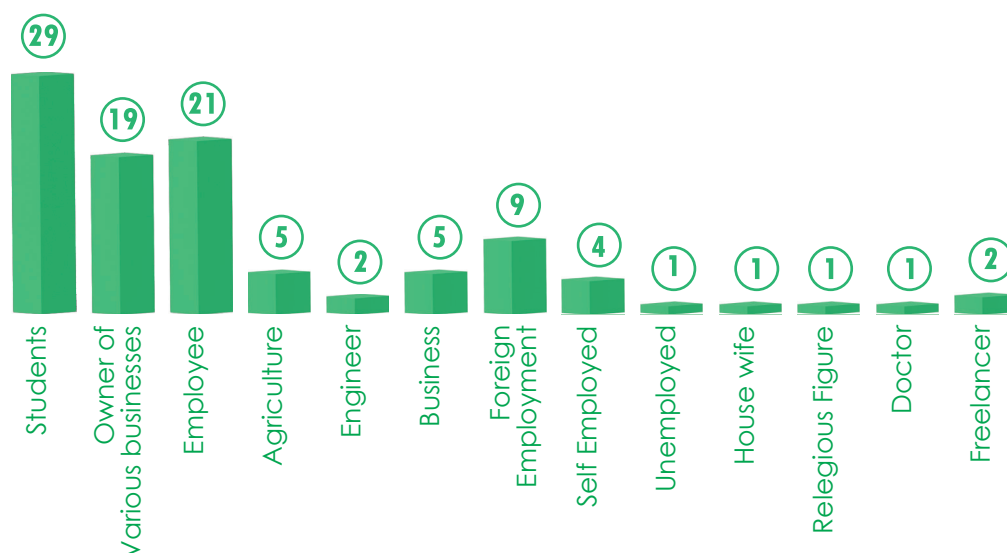


Of the individuals reported for suspicion of VAs, 35 % were in age group 26-30 years, 20% in age group of 21-25 years and 20% in the age group 31-35 years. Likewise, 12 % belonged to age group of 36-40 years and 10% in 41 years and above. Only 3% found to be in age group of 16-20 years. Overall, 75% of suspected individuals were aged 21-35, indicating concentration among young adults.

4.2.2 Occupation of the individuals reported in VAs related STR/SARs

Occupation was mentioned in the Know Your Customer (KYC)/Account opening form of individuals. Among 100 individuals, the largest group were students (29). Employees (21) and owners of small business like grocery shop, jewelry shop (19) followed. Others included individuals involved in foreign employment (9), agriculture (5) and smaller counts across doctors, engineers and housewife.

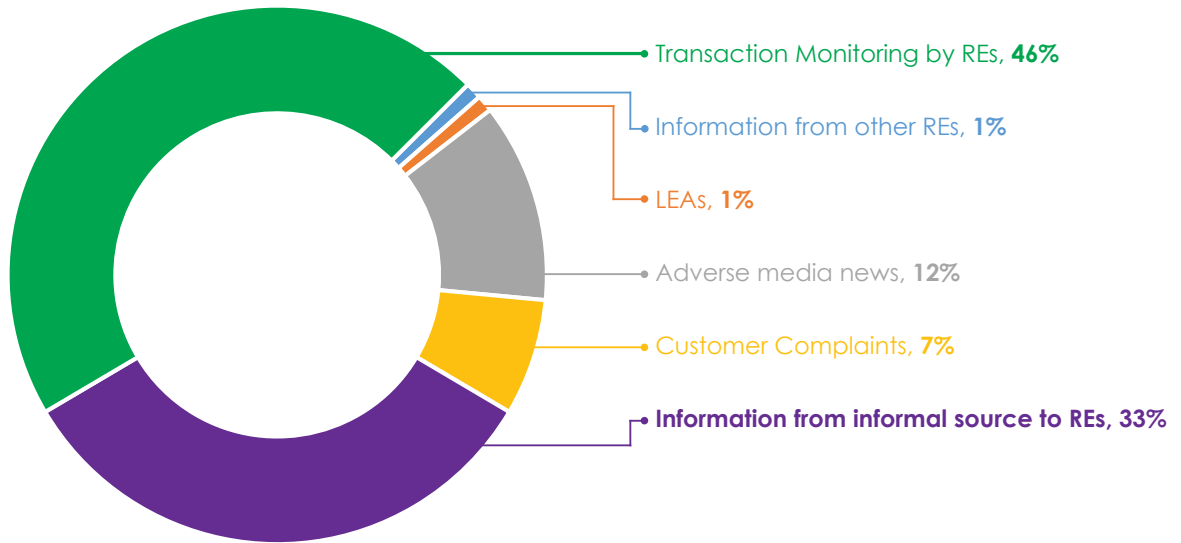
Figure 4.6: Occupation of individuals suspected in VAs



4.2.3 Triggering points for generation of STR/SARs by REs

VA related STR/SARs are primarily initiated by REs themselves through transactions monitoring of their customers. STR/SARs reported by REs are also initiated based on information provided to them from informal source as well. Various triggering points for generation of STR/SARs by REs is given in the figure below.

Figure 4.7 Various triggering points for generation of STR/SARs by REs

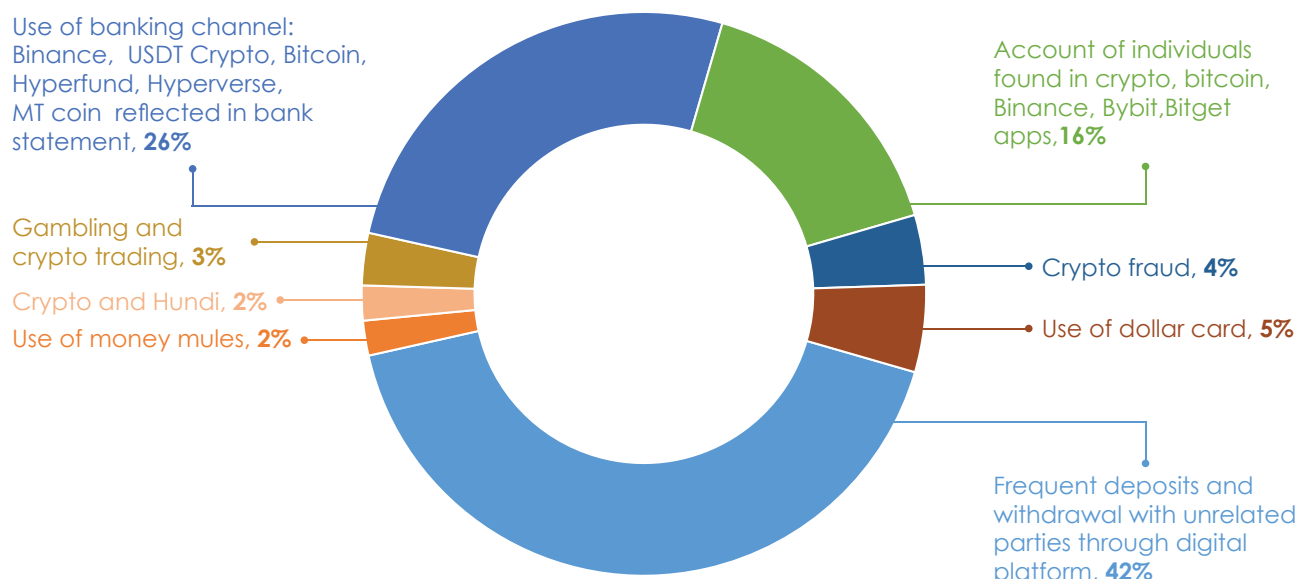


The figure 4.7 depicts that among 100 STR/SARS reported at FIU-Nepal, 46% of STR/SARs were reported by REs proactively through transactions monitoring. Sometimes, the REs may initiate the reporting when they receive the information from informal source (emails or screenshots that were received at REs where user's account is found in VAs related app like Binance; in some instances, only emails were provided, while others included both emails and screenshots) about the involvement of individuals in VAs and it constitutes 33% in this study. Similarly, 7 % and 12% STR/SARs were reported based on customer complaints and adverse media news of individuals in different crimes and offences.

4.2.4 Reasons for suspicion of individuals in VAs

The content in reason field of STR/SARs, keyword used by REs as well as attachments provided were studied to identify reasons for suspicion of individuals in VAs. Identifying involvement of individuals in VAs was easier in STR/SARs where reporting entities discovered that individuals used banking channel to buy/sell virtual assets as Binance, USDT, Crypto, Bitcoin, Hyperfund, Hyperverse, MT coin reflected in their bank statement which is 26 % presented in figure below.

Figure 4.8 Reasons for suspicion of individuals in VAs



Similarly, 16 % of the individuals were suspected in VAs as their accounts were found in crypto, bitcoin, Binance, Bybit, and Bitget apps as per provided screenshots and emails from the informal source; 2 % of them were suspected on using money mules (using other person's bank account) for crypto trading. Likewise, 5 % of them were suspected for using dollar card for crypto/bitcoin payment and purchase of skale tokens, 2% of them were suspected for gambling and crypto, and 2 % of them were suspected in crypto and hundi. 4% of the individuals were suspected in crypto fraud as they persuaded the victims to transfer the funds for bitcoin/crypto investment to realize higher returns. Majority of the individuals (42%) were suspected in VAs based on transactions patterns ie; frequent deposits and withdrawals with unrelated parties through digital platforms.

5. Findings and Recommendation

5.1 Key Findings

- VA-related STR/SARs reported by REs exhibited a fluctuating pattern in the last five years. Thirteen STR/SARs reported in 2021, which jumped to 173 in 2022. The figure decreased to 138 in 2023 and again increased to 252 in 2024. As of July 16, the STR/SARs reported in 2025 was 82.
- A significant portion (91.19%) of VA-related STR/SARs has been reported by commercial banks. This could be due to the use of bank accounts for VA-related activities, including receiving return on investment in VAs. The integration of all commercial banks into goAML system and stronger suspicious transaction reporting mechanism put in place by them also may have led to higher reporting.
- Majority of VA-related STR/SARs are disseminated to the Nepal Police, followed by the Department of Revenue Investigation. Most dissemination was made to the Nepal Police as they are responsible for investigating predicated offenses such as the use of VA and Hundi related. Only six cases have been disseminated to Department of Money Laundering Investigation. Most analyses resulted in the suspicion of the use of VAs, but only few cases could be directly linked with the money laundering through VAs.
- Key typologies observed in VA-related activities include illegal foreign exchange, hundi, online frauds, disguising the true nature of business and engaging in cryptocurrency trading under its cover, and the use of money mules involving the bank accounts of family and relatives.
- FIU-Nepal analysis reveals that 75% of individuals suspected in VA-related activities are between 21 and 35 years old, with students (29%) and salaried employees (21%) constituting the largest occupational groups. This is a critical vulnerability indicator. This digitally adept demographic is disproportionately targeted by and susceptible to online investment scams and get-rich-quick schemes, as seen in the South African Mirror Trading International case (Box 1). This finding underscores a significant financial literacy and consumer protection gap, highlighting an urgent need for targeted public awareness campaigns aimed specifically at young adults and student populations.
- VA-related STR/SARs are primarily triggered by the ongoing transaction monitoring conducted by BFIs and information received from informal sources (emails or screenshot where user's account is found in VAs related app like Binance). Other key drivers for these reports include direct inquiries from law enforcement and investigative bodies, as well as intelligence obtained from walk-in customers.
- In few instances, money mules are observed to be unaware of involvement of their accounts in VAs and legal prohibitions on it. Some individuals found to be misusing their dollar card to buy crypto and some scammed the victims persuading them to transfer the funds for attractive returns through crypto/bitcoin investment.

- Despite prohibitions, STR/SAR reporting and case filings continue, suggesting control measures face evasion.
- Since, Nepal is in the early phase of digitization and technological adoption, other predicate offences and illegal activities such as digital frauds, investment scams, online gambling, hundi are intertwined with the use of VAs, which make VAs more prone to ML/TF/PF risks.
- The persistent rise in VA-related STRs, despite the legal prohibition on the use of VAs, indicates that restrictive measures alone are insufficient to eliminate the risks. This suggests a strategic shift may be required from total ban to one of enhanced detection, investigation, and public awareness to manage the evolving threat, which is now operating in the informal and illicit economy.

5.2 Recommendations

5.2.1 Recommendations to Reporting Entities

Although VAs and VASPs are prohibited in Nepal, they are being used for investment and even in connection with financial crimes like hundi and online frauds. All reporting entities (REs) should ensure robust compliance frameworks, diligent reporting, and proactive customer awareness regarding associated risks. The key recommendations for REs in Nepal regarding VAs are as follows:

- **Strict adherence to existing prohibition of VAs and VASPs:** This entails refraining from facilitating any transactions involving virtual assets, opening accounts intended for VA trading, or participating in any related activities.
- **Implementation of Enhanced Customer Due Diligence (ECDD):** REs to thoroughly verify identification and address of customers, identify the source of funds and the ultimate beneficial owners of funds possibly linked with VAs.
- **Ongoing Monitoring:** REs to continually monitor transactions and behavior of customers for any deviations from their normal activity or expected patterns, especially if VA involvement is suspected. Timely KYC update is essential.
- **Implementation of Risk-Based Approach and adherence to Travel Rule (FATF Recommendation 16):** REs need to develop and implement a robust risk-based approach for identifying customers, products, services, and geographic areas that may be susceptible to VA-related illicit activities and applying proportionate risk mitigation measures. Adherence to Travel Rule that requires the financial institutions to collect and transmit originator and beneficiary information (names, account numbers, and identifying details of each transfer) during transfers to combat ML and TF.
- **Timely Reporting of STR/SARs:** VA-related STR/SARs must be reported immediately to FIU-Nepal through the goAML system after RE's assessment leading to suspicion. Any delay or tipping-off should to be avoided. REs to ensure STR/SARs include comprehensive details including nature of the suspicious activity/transaction and how it relates to VAs, identities of all involved parties (individuals and entities), connected transactions, transaction details (amounts, dates, methods, originator and beneficiary information) and any known virtual asset addresses or platforms along with narrative linking observed red flags to suspected VA activity.
- **Regular training and public awareness:** REs to ensure that all relevant staff, especially front-line employees, compliance officers, and management, receive regular training on emerging VA-

related typologies, identification of red flags and proper procedures for filing STRs/SARs related to VAs. Educating the general public through notices, circulars, advertisement and campaigns is essential for awareness to reduce illicit activities related with VAs.

- **Updated internal control:** REs to review and update internal policies and guidelines to explicitly prohibit dealing with virtual assets.

5.2.2 Recommendation to LEAs and investigative agencies

Coordination among LEAs and investigative agencies like Nepal Police, Department of Revenue Investigation, Department of Money Laundering Investigation, and the Office of the Attorney General is critical for an effective fight against financial crimes. The key recommendations for LEAs and investigative agencies in Nepal regarding VAs are as follows:

- **Capacity Building and Specialization:** LEAs should enhance investigators' skills through foundational and advanced training in blockchain technology and forensics, including tracing complex transaction flows, identifying common obfuscation techniques (e.g., mixers/tumblers), and linking on-chain activity to real-world identities. Regular training on extracting and analyzing digital evidence from devices (computers, mobile phones) that may contain cryptocurrency wallets, exchange login details, or communication related to VA-related crimes also plays crucial role to strengthen investigation effectiveness.
- **Cross-Agency Knowledge Sharing and interaction:** Regular workshops, interaction programs and information exchange among LEAs and investigative agencies are essential to share expertise, emerging trends, and successful investigative strategies. All LEAs and investigative agencies should institutionalize and regularly facilitate such collaborative programs.
- **Enhancement of Investigative Tools and Techniques:** LEAs and investigative agencies should adopt advanced blockchain analysis platforms (e.g., Chainalysis, TRM Labs, CipherTrace) for visualizing transaction flows, identifying clusters of addresses linked to specific entities such as exchanges or illicit actors, tracing funds across multiple blockchains and generating court-admissible analytical reports.
- **Leverage financial intelligence:** LEAs and investigative agencies should actively utilize financial intelligence disseminated by FIU-Nepal on VA-related activities and maintain close coordination with FIU-Nepal for ongoing intelligence sharing, analysis and exchanging feedback.
- **Focus on international cooperation:** Effective exchange of financial intelligence and other relevant information with foreign counterparts is vital for supporting investigations and evidence development. FIU-Nepal serves as the focal point for obtaining such information through the secured network of Egmont Group of FIUs.
- **Forge Partnership with foreign Jurisdictions:** LEAs should proactively establish formal partnerships with jurisdictions (e.g. member jurisdictions of APG) that have advanced virtual asset regulatory and asset recovery frameworks. A concrete example to emulate is the mechanism between the Beijing PSB and Hong Kong's licensed exchanges (Annex II), which allows for the compliant liquidation of seized crypto. LEAs, in coordination with FIU-Nepal and the Office of the Attorney General, should initiate dialogue with counterparts in such jurisdictions to develop a formal process for the identification, freezing, and lawful liquidation of illicit virtual assets held abroad, ensuring proceeds are repatriated to Nepal.

5.3 Recommendations to regulators/supervisors

The key recommendations for regulators /supervisors in Nepal regarding virtual assets include:

- **Ensuring enforcement of the current prohibition on VAs and VASPs:** Regulators/supervisors should ensure consistent and stringent application of existing laws (e.g., Foreign Exchange (Regulation) Act 2019, National Criminal Code 2017) that restrict or prohibit VA activities.
- **Public awareness campaigns on risks and legality:** Regulators and supervisors should conduct nationwide awareness campaigns to inform the public about the legal prohibition of VA activities and transactions in Nepal and the associated risks such as fraud, money laundering, and capital flight.
- **Guidance and supervision:** Regulators and supervisors should issue clear guidance to financial institutions and other REs on monitoring of transactions related to VA. These institutions should have mechanisms that raise alerts or red flags related to VA activities in line with FIU-Nepal's STR guidelines and other internally developed criteria.
- **Cross-Border Collaboration:** Regulators and supervisors should collaborate with foreign counterparts, build and maintain formal channels for international cooperation and information exchange on illicit virtual asset flows. This should help to track new risks and regulatory responses related with virtual assets.
- **Sectoral risk assessment:** A blanket ban on VA-related activities and VASPs are in place in Nepal. While VAs and VASPs pose ML/TF/PF risks owing to their possible use in disguising illicit origin of funds obtained through financial crimes such as online fraud, hundi or drug trafficking, they have shown some benefits regarding lower cross border transaction cost, faster processing time, and enhancing financial inclusion. Besides, the ban has not stopped the use of VAs either as investment or as vehicle for concealing the illicit origin. In fact, the outright ban may push activities underground, reducing visibility for regulators and increasing ML/TF risk. Hence, as a foundational step, a sectoral risk assessment focused on virtual assets should be conducted immediately. This assessment is needed to systematically evaluate the ML/TF/PF threats, vulnerabilities, and consequences posed by VA activities in Nepal. This would align with the FATF's guidance and follow the example of Malaysia's Virtual Asset Risk Assessment (VARA) 2024 and Singapore's VA Risk Assessment Report (2024), which provide structured methodologies for understanding the domestic risk landscape. The findings will inform whether the current prohibitive approach is effective or if a shift towards a regulated model is necessary to manage risks effectively. NRB, as a regulator of Nepal's payment system and foreign exchange regime, could lead the assessment in coordination with SEBON, the securities sector regulator, and Nepal Telecommunications Authority (NTA), the telecommunication sector regulator of Nepal. If Nepal decides on lifting the complete ban and adopt a regulated model, it should be effectively regulated, which could be carried out through an existing regulator, by a second tier institution within an existing regulatory body, or by establishing a new regulator.

Annex I: Red flags

Reporting Entities should consider the following transactional and behavioral indicators as potential red flags for suspicious virtual asset activities. In addition to red flag indicators included in the STR Guidelines, following red flags derived from the STR/SAR analysis and case studies within this report could be adopted. Further, REs can add additional red flags as per nature of business, APG typology reports and similar studies.

Category	Red Flag Indicator	Reference in Report
Transaction Patterns	Frequent, round-figure deposits from multiple unrelated parties, followed by rapid consolidation and withdrawal to a new, unrelated account.	Section 4.2.4: 42% of suspicions were based on “frequent deposits and withdrawals with unrelated parties.”
Transaction Descriptions	Payment descriptions, notes, or beneficiary names containing keywords such as “Binance,” “USDT,” “Crypto,” “Bitcoin,” “Bybit,” “MetaMask,” “HyperFund,” or “P2P.”	Section 4.2.4: 26% of STRs were triggered by terms like “Binance, USDT, Crypto, Bitcoin” in bank statements.
Customer Behavior	A customer’s account is used to receive funds from individuals who then complain of being defrauded in online investment schemes.	Section 4.2.4 & Box 7: 4% of individuals were suspected of “crypto fraud” by persuading victims to transfer funds.
Use of Intermediaries	Use of accounts belonging to homemakers, or low-income individuals (potential money mules) to conduct high-value, rapid transactions inconsistent with the account holder’s profile.	Section 4.2.4 & Box 9: 2% of cases involved the use of money mules, including family members’ accounts.
Instrument Usage	Use of international debit/credit cards (dollar cards) for repeated payments to merchants identified as cryptocurrency exchanges or platforms.	Section 4.2.4: 5% of individuals were suspected for “using dollar card for crypto/bitcoin payment.”
Information from Sources	Receipt of information from informal sources or adverse media reports providing screenshots, emails, or other evidence linking a customer to crypto wallets or trading apps.	Section 4.2.4: 33% of STRs were initiated based on “information from informal source.”

Category	Red Flag Indicator	Reference in Report
Link to Other Crimes	Transactions that are simultaneously indicative of other predicate offenses, such as online gambling (rapid, small-stake transactions) or Hundi (cross-border transfers with no legitimate trade purpose).	Box 10 (Online Gambling) & Box 6 (Hundi Operations)

Annex II: International efforts/practices to prevent VAs and VASPs from misuse by illicit actors

(A) FATF:

- | | |
|------|---|
| 2018 | Recommendation 15 amended |
| 2019 | Adoption of Interpretive Note to R.15
Creation of the FATF Virtual Assets Contact Group (VACG)
Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021) |
| 2020 | 12 month review of the new FATF Standards: 1st12-month review
Report to the G20: FATF Report to the G20 on So-called Stablecoins
Risk indicators: List of Red Flag Indicators of ML/TF through VAs |
| 2021 | Updated guidance for regulators ³ : Updated Guidance for a Risk-Based Approach to VA and VASPs
24 month review of the FATF Standards: 2nd12-month review |
| 2022 | Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs |
| 2023 | Report on ransomware, with a focus on VA risks and trends: Countering Ransomware Financing
Report on implementation of R.15: VAs: Targeted Update on Implementation of the FATF Standards |
| 2024 | Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity |
| 2025 | Targeted Update on Implementation of the FATF Standards on VAs and VASPs |

See more at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>

(B) Singapore:

Building a stronger understanding of the Travel Rule landscape (Singapore)

Singapore's Monetary Authority of Singapore (MAS) introduced the Payment Services Act in January 2020 to license and regulate VASPs in Singapore. All licensed VASPs are subjected to AML/CFT requirements, including the Travel Rule. In order to facilitate implementation of the Travel Rule domestically, MAS:

- a) engaged with available Travel Rule Compliance tool providers in order to gain a better understanding of the different tools available;
- b) took steps to raise industry's awareness of the Travel Rule via industry engagement sessions. The objective was to explain the requirements and MAS' supervisory expectations, as well as to gather feedback on the possible challenges faced by VASPs;
- c) issued additional guidance to the sector in March 2021, which included further clarity on supervisory expectations on the Travel Rule and the enhanced risk mitigating measures that should be considered. The guidance took into consideration the feedback received during the industry engagement sessions; and
- d) supported the industry's initiative to help its members comply with AML/CFT requirements. Specifically, in 2020, a crypto-currency industry association conducted an independent evaluation on the available Travel Rule compliance tool providers. The objective of the industry initiative was to encourage its members to duly assess which provider would be most suitable for them.

As part of MAS' ongoing monitoring of the sector, all licensed VASPs are required to submit regular data on the number and value of transactions that are facilitated between obliged entities as well as to un-hosted wallets. This information allows the supervisor to maintain an understanding of the implementation of the Travel Rule and monitor the risk of the sector on an ongoing basis.

Thematic Inspections of VASPs

To raise the awareness of this newly regulated sector towards ML/TF risk and AML/CFT obligations, MAS conducted thematic inspections of selected entities of higher risk in 2022-2023. The thematic inspections focused on assessing the key AML/CFT controls of VASPs, including the measures VASPs had taken to comply with the Travel Rule. Specifically, MAS reviewed the VASPs' AML/CFT policies and procedures and sought to understand the VASPs' considerations behind their selection of Travel Rule technological solutions. MAS found that while the entities had AML/CFT controls in place, the controls could be further strengthened in some areas, such as enhanced CDD measures for higher risk customers and the assessment of ML/TF risks arising from new products. To further embed the sector's risk awareness, MAS regularly engages the entities through industry townhalls, outreach sessions and webinars since 2019, and issued a guidance paper in March 2021 to provide additional information to facilitate their implementation of AML/CFT controls. MAS will also be issuing additional guidance detailing key observations from the thematic inspections, including VASPs' Travel Rule controls and implementation of risk mitigation measures, so that the industry can conduct a self-assessment of their controls and strengthen them where relevant.

See more at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf>

(C) Hongkong:

Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022

The Hong Kong Government has set out a clear policy direction to develop a vibrant but well-regulated virtual asset (VA) ecosystem. In October 2022, it issued a Policy Statement emphasizing the principle of “same activity, same risks, same regulation,” seeking to strike a balance between promoting innovation and ensuring safeguards against risks such as money laundering, terrorist financing, financial instability, and inadequate investor protection. A key development was the introduction of the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022, which came into effect on 1 June 2023. This established a licensing regime under which all virtual asset trading platforms (VATPs) operating in Hong Kong, or actively marketing to local investors, must obtain a licence from the Securities and Futures Commission (SFC). Pre-existing platforms were given transitional arrangements, while licensed VATPs are required to meet strict standards in areas such as asset custody, auditing, cybersecurity, and investor suitability.

See more at: https://www.legco.gov.hk/yr2023/english/hc/sub_com/hs01/papers/hs0120240719cb1-1070-2-e.pdf

Regulatory Regime for Stablecoin Issuers

Following the implementation of the regulatory regime for stablecoin issuers under the [Stablecoins Ordinance](#) on 1 August 2025, the business of issuance of fiat-referenced stablecoins is a regulated activity in Hong Kong and a license is required. This page sets out the details in relation to the regulatory regime.

- **Licensing for stablecoin issuers:** The [Explanatory Note on Licensing for Stablecoin Issuers](#) sets out guidance on the licensing regime as well as licensing procedures. Entities interested in applying for a license should familiarize themselves with the relevant guidance, and are encouraged to reach out to the HKMA for early discussion. Interested parties may reach out to the HKMA via stablecoin_licensing@hkma.gov.hk. The [Explanatory Note on Transitional Provisions for Pre-existing Issuers](#) outlines the guidance for stablecoin issuers that have been operating in Hong Kong prior to the effective date of the regulatory regime (i.e. 1 August 2025)
- **Supervision of licensed stablecoin issuers:** The HKMA has published [Guideline on Supervision of Stablecoin Issuers](#) and [Guideline on Anti-Money Laundering and Counter-Financing of Terrorism \(AML/CFT Guideline\)](#) to set out regulatory expectations for licensed stablecoin issuers.
- **Register of licensed stablecoin issuers.** The [Register of Licensed Stablecoin Issuers](#) contains the name and basic information of licensed stablecoin issuers in Hong Kong. The public may refer to the Register for the updated list of entities that have been granted a license. Currently, there is no licensed stablecoin issuer. The list will be updated in a timely manner as appropriate.

Source: <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/>

(D) China:

China has developed a strict legal and regulatory framework for crypto currencies, starting with the 2013 Circular on Preventing Bitcoin Risks, expanding to all token-related activities in 2017, and declaring crypto trading and related services as illegal financial activities in 2021. Despite these prohibitions, courts and enforcement agencies face growing challenges in seizing, storing, valuing, and disposing of crypto assets in criminal and civil cases, particularly due to anonymity, volatility, and technical barriers.

See more at: <https://hankunlaw.com/upload/portal/20241126/a99a3ef1e2db7a3210c9d5bb4e595767.pdf>

The Beijing Municipal Public Security Bureau has teamed up with a state-owned exchange in Hong Kong to establish a mechanism to dispose of virtual currencies that doesn't run afoul of the Chinese mainland's ban on trading digital assets. The Chinese mainland is taking a new approach to disposing of cryptocurrency seized in law enforcement cases, allowing the authorities to convert illicit digital assets into real money through licensed exchanges in Hong Kong in a way that complies with the mainland's stringent regulations on virtual currencies. The Beijing Municipal Public Security Bureau (PSB) announced that it has teamed up with the China Beijing Equity Exchange (CBEX), a state-owned platform for trading equities and other assets and established a mechanism to dispose of virtual currencies in a compliant way. Under the mechanism, the Beijing PSB and its sub-bureaus can entrust the disposal of virtual currencies to the CBEX, which will select professional service institutions to verify, accept and transfer the assets, the bureau's legal affairs department said in a statement. As direct conversion of digital assets like cryptocurrencies into real money is banned on the mainland, the assets will be publicly converted through one of the 10 licensed crypto exchanges in Hong Kong. After the sale, the proceeds will go through the approval process of the State Administration of Foreign Exchange and then be repatriated to a special account for that particular case before being deposited into the state treasury.

Source: <https://www.globalneighbours.org/hong-kong-offers-beijing-legal-route-to-sell-seized-crypto/#:~:text=Under%20the%20mechanism%2C%20the%20Beijing%20PSB%20and,legal%20affairs%20department%20said%20in%20a%20statement.>

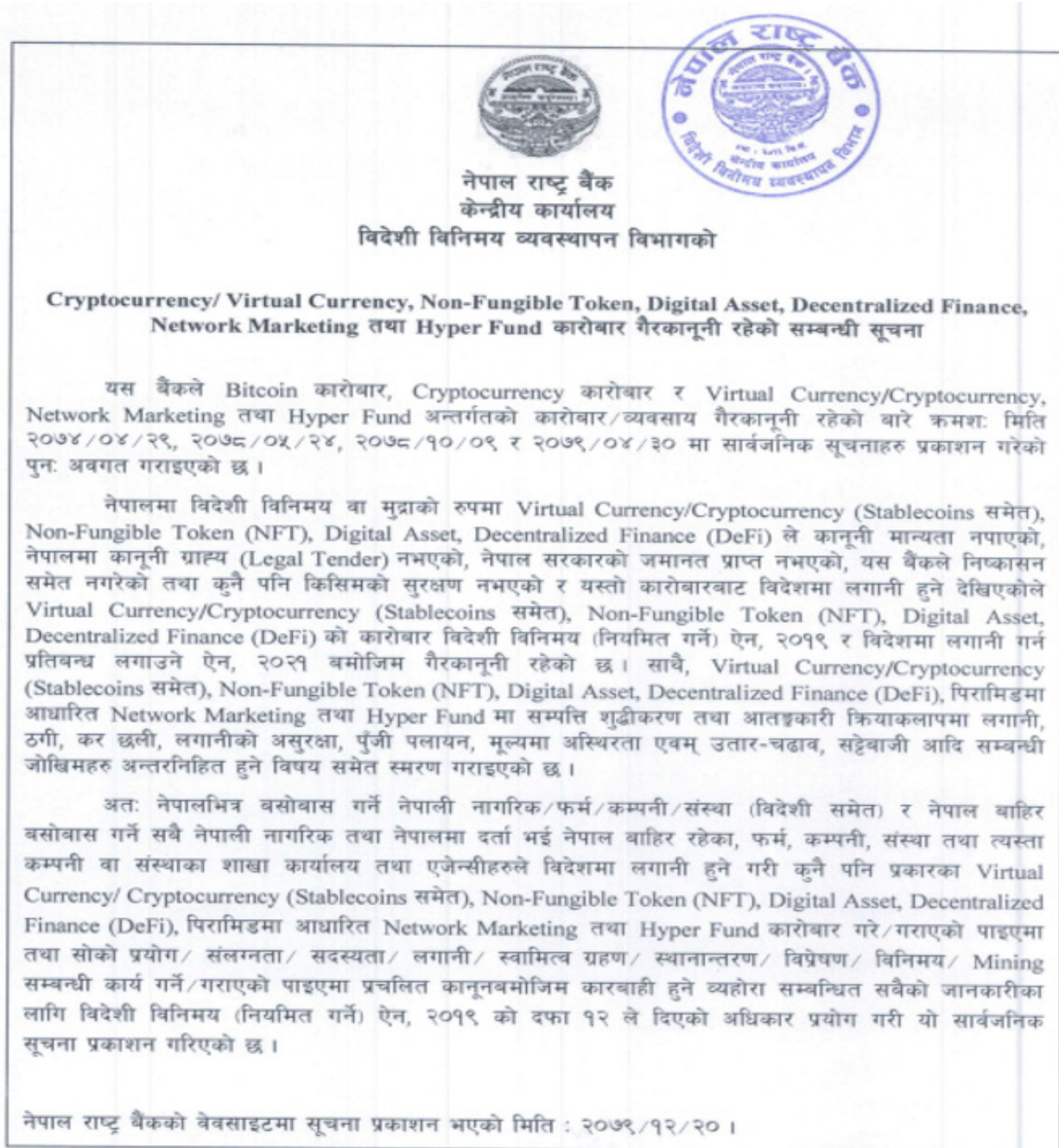
(E) India:

Virtual Digital Assets (VDAs) including cryptocurrencies and other digital assets, are recognized as a separate category of assets under the Income-tax Act, 1961. Pursuant to 115BBH of Income-tax Act, 1961, gains from transfer of VDAs are taxed at a flat rate of 30%, regardless of whether held short-term or long-term. Losses from VDA transfers cannot be offset against other income. In addition, Section 194S mandates a 1% TDS on payments made for transfer of VDAs, applicable if the transaction exceeds a specified threshold to ensure compliance, transparency, and monitoring. These amendments reinforce the government's policy of "tax but do not ban" crypto assets.

Source: <https://incometaxindia.gov.in/Documents/income-tax-act-1961-as-amended-by-finance-act-2025.pdf>

Annex III: Public awareness notices

(A) Public notices issued by Foreign Exchange Management Department of Nepal Rastra Bank:



Available at: https://www.nrb.org.np/contents/uploads/2023/04/FXMD-Notice-Cryptocurrency_2079.12.20.pdf



नेपाल राष्ट्र बैंक
विदेशी विनिमय व्यवस्थापन विभागको
Virtual Currency/Cryptocurrency तथा Network Marketing अन्तर्गतको
कारोबार/व्यवसाय गैरकानूनी रहेको सम्बन्धी सूचना

हालका दिनहरूमा छोटो अवधिमा उच्च प्रतिफल दिने प्रलोभन देखाई Virtual Currency/Cryptocurrency हरूको कारोबार/प्रयोग गर्न तथा त्यस्ता Virtual Currency/Cryptocurrency हरूसँग सम्बन्धित Hyper Fund जस्ता कोषमा लगानी गर्न र Jocial, Crowd 1, Solemax Global जस्ता पिरामिडमा आधारित Network Marketing मा आवद्ध हुन प्रोत्साहन गर्ने/गराउने गरेको जानकारी प्राप्त हुन आएकोले सो सम्बन्धमा यस बैंकको गम्भीर ध्यानाकर्षण भएको छ । नेपालमा विदेशी विनिमय वा मुद्राको रूपमा Virtual Currency/Cryptocurrency ले कानूनी मान्यता नपाएको सन्दर्भमा उपर्युक्त बमोजिमका गैरकानूनी वित्तीय औजारमा आवद्ध भई कारोबार गर्दा सर्वसाधारण ठगिने, अवैधानिक तरिकाले रकम बाहिरिई स्वदेशी पूँजी पलायन हुने भएकाले त्यस्ता कारोबार तथा व्यवसायमा संलग्न भई नेपालभित्र बसोबास गर्ने नेपाली तथा विदेशी नागरिक र विदेशमा बस्ने नेपाली नागरिकहरू समेतले त्यस्तो कार्य गरे/गराएको पाइएमा प्रचलित कानूनबमोजिम कारवाही हुने व्यहोरा सर्वसाधारण सबैको जानकारीका लागि यो सूचना प्रकाशन गरिएको छ ।

नेपाल राष्ट्र बैंकको वेबसाइट www.nrb.org.np मा प्रकाशन भएको मिति: २०७८/१०/०९



Available at : https://www.nrb.org.np/contents/uploads/2023/01/Notice_FXMD_2079.09.29.pdf



नेपाल राष्ट्र बैंक
केन्द्रीय कार्यालय
विदेशी विनिमय व्यवस्थापन विभागको
Cryptocurrency कारोबार गैरकानूनी रहेको सम्बन्धी सूचना

नेपालमा कुनै पनि प्रकारका Cryptocurrency हरूको कारोबार/प्रयोग/Mining गैरकानूनी रहेकोले यस्ता प्रकारका Cryptocurrency हरूको कारोबार/प्रयोग/Mining सम्बन्धी कार्य नगर्नु/नगराउनु हुन विदेशी विनिमय (नियमित गर्ने) ऐन, २०१९ ले दिएको अधिकार प्रयोग गरी यो सूचना जारी गरिएको छ ।

हालका दिनहरूमा Cryptocurrency हरूको कारोबार/प्रयोग/Mining जस्ता कार्यमा संलग्न हुन प्रोत्साहन गर्ने/गराउने समेत गरेको पाइएको र त्यस्तो कार्यबाट सर्वसाधारणहरू ठगिएको/ठगिन सक्ने देखिएको हुँदा कसैले त्यस्तो कार्य गरे/गराएको पाइएमा प्रचलित कानूनबमोजिम सजाय हुने व्यहोरा समेत जानकारी गराइन्छ ।

भवदीय,

रामु पौडेल

(कार्यकारी निर्देशक)

नेपाल राष्ट्र बैंकको वेबसाइट www.nrb.org.np मा सूचना प्रकाशन भएको मिति : २०७८/०५/२४ ।

Available at : <https://www.nrb.org.np/contents/uploads/2021/09/FXMD-Notice-03-207879-Cryptocurrency.pdf>



नेपाल राष्ट्र बैंक, केन्द्रीय कार्यालय
विदेशी विनिमय व्यवस्थापन विभागको
Bitcoin कारोबार गैरकानुनी रहेको बारेको सूचना

नेपाल राष्ट्र बैंक ऐन, २०५८ र विदेशी विनिमय (नियमित गर्ने) ऐन, २०१९ बमोजिम यस बैंकबाट इजाजतपत्र लिएर मात्र विदेशी विनिमयको कारोबार गर्न सक्ने स्पष्ट कानुनी व्यवस्था रहेको र हालसम्म नेपालमा Bitcoin लाई मुद्राको रूपमा कानुनी मान्यता प्राप्त नभएको अवस्थामा यदाकदा केही व्यक्तिहरूले इन्टरनेटको माध्यमबाट Bitcoin सम्बन्धी कारोबार गरिरहेको भन्ने बुझिन आएकोले Bitcoin सम्बन्धी कारोबार नेपालमा पूर्णरूपमा गैरकानुनी रहेको व्यहोरा जानकारी गराउँदै कसैले पनि सो सम्बन्धी कारोबार नगर्न नगराउनुहुन सर्वसाधारणको जानकारीको लागि यो सूचना प्रकाशन गरिएको छ ।

कार्यकारी निर्देशक
विदेशी विनिमय व्यवस्थापन विभाग

मिति : २०७४।४।२९

Available at : <https://www.nrb.org.np/contents/uploads/2019/12/BitcoinNotice.pdf>

Annex IV: Related legal Provisions

(A) Nepal Rastra Bank, 2002:

५२. बैङ्क नोट र सिक्का निष्कासन गर्ने अधिकार : (१) बैङ्कलाई नेपाल [■] भित्र बैङ्क नोट तथा सिक्का निष्कासन गर्ने एकाधिकार हुनेछ । यस्तो नोट तथा सिक्का नेपाल [■] मा कानूनी ग्राह्य हुनेछ ।

(२) उपदफा (१) बमोजिम बैङ्कले नोट निष्कासन गर्दा सुरक्षण राखेर मात्र निष्कासन गर्नेछ र यस्तो निष्कासित नोटको दायित्व सुरक्षण बापत राखिएको सम्पत्तिको मूल्य बराबर हुनेछ । सुरक्षण बापत राखिने सम्पत्तिको कमसेकम पचास प्रतिशत सुन, चाँदी, विदेशी मुद्रा, विदेशी धितोपत्र र विदेशी विनिमय अधिकारपत्रमध्ये एक वा एक भन्दा बढीमा र अरु बाँकी प्रतिशत सिक्का (मोहर, डबल र सो भन्दा बढी दरको), नेपाल सरकारले निष्कासन गरेको ऋणपत्र र बैङ्कबाट पुनः भुक्तानी दिएको बढीमा अठार महिनाभित्र नेपालमा नै भुक्तानी हुने प्रतिज्ञापत्र वा विनिमयपत्रमध्ये एक वा एक भन्दा बढीमा राखिनेछ ।

Available at : <https://www.nrb.org.np/contents/uploads/2021/03/%E0%A5%A7.%E0%A4%A8%E0%A5%87%E0%A4%AA%E0%A4%BE%E0%A4%B2-%E0%A4%B0%E0%A4%BE%E0%A4%B7%E0%A5%8D%E0%A4%9F%E0%A5%8D%E0%A4%B0-%E0%A4%AC%E0%A5%88%E0%A4%99%E0%A5%8D%E0%A4%95-%E0%A4%90%E0%A4%A8-%E0%A5%A8%E0%A5%A6%E0%A5%AB%E0%A5%AE.pdf>

(B) Foreign Exchange (Regulation) Act 2019:

५. केही मुद्रा र बुलियन निकासी वा पैठारी गर्नमा प्रतिबन्ध : (१) कुनै व्यक्ति, फर्म, कम्पनी वा संस्थाले बैङ्कबाट इजाजतपत्र नलिई कुनै खास किसिमको नेपाली मुद्रा वा विदेशी मुद्रा नेपाल [■] को सबै वा कुनै खास इलाकाभित्र ल्याउन वा पठाउन नपाउने गरी नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी आदेश जारी गर्न सक्नेछ । त्यस्तो आदेश जारी गर्दा नेपाल सरकारले कुनै व्यक्ति, फर्म, कम्पनी वा संस्थाका सम्बन्धमा वा कुनै खास किसिमको नेपाली मुद्रा वा विदेशी मुद्राको सम्बन्धमा त्यस्तो प्रतिबन्ध नलान्ने गरी त्यस्तो आदेशमा तोकिदिन सक्नेछ ।

Available at : <https://www.nrb.org.np/contents/uploads/2021/03/%E0%A5%A7.%E0%A4%A8%E0%A5%87%E0%A4%AA%E0%A4%BE%E0%A4%B2-%E0%A4%B0%E0%A4%BE%E0%A4%B7%E0%A5%8D%E0%A4%9F%E0%A5%8D%E0%A4%B0-%E0%A4%AC%E0%A5%88%E0%A4%99%E0%A5%8D%E0%A4%95-%E0%A4%90%E0%A4%A8-%E0%A5%A8%E0%A5%A6%E0%A5%AB%E0%A5%AE.pdf>

(C) National Criminal Code Section 262(A):

२६२क. अभौतिक मुद्राको प्रयोग गर्न नहुने : १ (नेपाल राष्ट्र बैङ्कले जारी गर्ने मुद्रा बाहेक कसैले पनि नेपालमा प्रयोग गर्ने, गराउने वा नेपालभित्र वा बाहिरको व्यावसायिक कारोबारको भुक्तानी लिने, दिने वा हिसाब मिलान गर्ने वा अन्य कुनै प्रयोजनको लागि मुद्राको नाम लिई वा नलिई अभौतिक भर्चुअल (मुद्राको उत्पादन, बिक्री, कारोबार, सटही वा स्थानान्तरण गर्न, राख्न) होल्ड गर्न (वा त्यस्तो मुद्रा जारी वा हस्तान्तरण गर्न वा गराउन हुँदैन।

स्पष्टीकरण: यस दफाको प्रयोजनको लागि "अभौतिक (भर्चुअल) मुद्रा" भन्नाले क्रिप्टोग्राफी वा अन्य कुनै तरिकाले सिर्जना वा उत्पादन गरिएको विद्युतीय माध्यमबाट मूल्य दर्शाउने वा मूल्यको प्रतिनिधित्व गर्ने व्यापारिक क्रियाकलापमा महत्व वा उपादेयता रहेको वा मूल्य वा खाताको एकाइमा सञ्चित वा भण्डारण गर्न सकिने सूचना, कोड वा सङ्केत नम्बर, टोकन, क्रिप्टो करेन्सी वा यस्तै किसिमको भर्चुअल सम्पत्ति सम्झनु पर्छ।



**Financial Intelligence Unit
(FIU-Nepal)**

Nepal Rastra Bank

Baluwatar, Kathmandu

Tel: 01-5719653 (Ext. 2841/2842)

Email: fiupolicy@nrb.org.np

Website: www.nrb.org.np/departments/fiu