STRATEGIC ANALYSIS REPORT
(2021-22)

Virtual Assets- The emerging risk of Money Laundering and Terrorism Financing

FINANCIAL MONITORUNG UNIT
Govt. of Pakistan

Preface:

The Financial Monitoring Unit (FMU) is the central authority in Pakistan to receive, analyze and disseminate suspicious transaction reports (STRs) and Currency Transaction Reports (CTRs). The FMU conducts two types of Analysis i.e. Operational Analysis and Strategic Analysis of STRs/CTRs. The purpose of strategic analysis is to identify potential ML/TF threads and vulnerabilities of products, customers, geographies and delivery channels for the stakeholders to proactively deter the emerging risks.

The objective of this strategic analysis is to understand the virtual assets, underlying mechanism for transferring value and risks/vulnerabilities associated with such assets. The strategic analysis is based on different domestic and international reports on virtual assets and the suspicious transactions reports received to FMU during the period of July 2021 to June 2022. The report covers the demographics and geographic analysis of individuals involved in virtual assets and products/ delivery channels used by them to perform transactions of virtual assets. Further, the report also tends to identify possible predicate offences linked with virtual assets with help of case studies.

Previously, FMU carried out similar nature of strategic analysis of STRs reported on transactions of virtual assets in December 2018, March 2020 and August 2021 which were shared with relevant stakeholders.

The purpose of this strategic analysis is to assist the financial sector, regulators, law enforcement agencies and other stakeholders to develop legal/regulatory framework to govern the virtual assets as currently there are no regulations placed in Pakistan to tackle the risk of virtual assets.

021-99095034
info@fmu.gov.pk
http://www.fmu.gov.pk
SBP Main Building, I.I.C Road, Karachi

Table of Contents

Virtual Assets

The emerging risk of Money Laundering & Terrorism Financing (2021-22)

1. Executive Summary

Virtual Asset refers to any digital representation of value that can be digitally traded, transferred, and can be used for payment or investment purposes. Virtual Assets are considered high risk in terms of money laundering and terrorism financing due to anonymous and decentralized of peer-to-peer online transactions. FMU has conducted the strategic analysis on Virtual assets related transactions to identify and assess the risk/ vulnerabilities associated with them. The strategic analysis is based on different domestic and international reports on virtual assets and the suspicious transactions reports received to FMU during the period of July 2021 to June 2022. Below are the highlights of the strategic analysis:

- FMU received 1841 Suspicious Transaction reports related to virtual Assets during the period of July 2021 to June 2022.
- The students, youngsters belong to IT profession and salaried individuals are mostly involved in sale/ purchase of virtual assets.
- The individuals are using different channels for sale/purchase of virtual assets such as bank accounts, debit cards, credit cards, mobile wallets and Western Union.
- An overall suspicious activity of PKR 930.7 million was reported in attempted or conducted suspicious transactions which involve purchase of virtual assets, sale of virtual assets and P2P transactions related to virtual assets.
- The analysis also identifies the major Virtual Asset Services Providers (VASPs) and merchants facilitating the trade of Virtual assets.
- The strategic analysis also highlights the criminal offences such as Terrorism Financing, Hawala/ Hundi, Ponzi Schemes, Drug Trafficking, Sexual Exploitation, Fraud and Forgery, Smuggling and Illegal trade, Tax evasion suspected to be linked with virtual asset related transactions with help of case studies and media reports. It has been assessed through the analysis that the Virtual assets may fuel the criminal activities with free flow of funds and may attract the criminals and terrorists to evade concerned authorities.

The strategic analysis transpires that Virtual Assets pose significant money laundering and terrorism financing risk, which requires collaborative efforts among the stakeholders to develop a regulatory framework. The virtual assets are penetrating to the society at a rapid pace, despite of warnings to the general public and stance of declaring virtual assets “not a legal tender” by the State Bank of Pakistan.

2. Understanding Virtual Assets

According to the Financial Action Task Force (FATF), the term '**virtual asset**' refers to any digital representation of value that can be digitally traded, transferred, and can be used for payment or investment purposes. It can perform following functions:

- Medium of exchange
- Unit of account
- Store of value, but does not have legal tender status in any jurisdiction

Virtual Assets are not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual assets.

2.1. Difference between Virtual Assets and E-money

Virtual Assets and E-money both are digital currencies. The difference between them is that E-money is backed by the fiat currency (currency that has legal tender status), used as transfer mechanism for fiat currency. However, the Virtual assets are not backed by the fiat money, created and held electronically, and can be traded digitally to transfer value.

2.2. The system of Virtual Assets

As per FATF Report, following are the major participants of Virtual Asset's system:

1. **Administrator** is the person or entity, which issue centralized virtual asset, establish the rules for its use; maintain a payment ledger; and has the authority to redeem the virtual asset.
2. **Miner** is the person or entity that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a distributed proof system used to validate transactions in the virtual asset system.
3. **Exchanger** is the person or entity engaged in business of virtual currency exchange for real currency, funds, or other forms of virtual currency for a commission. The Exchangers accept a wide range of payments, such as cash, wires transfers, credit cards, and other virtual currencies. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts. Some of the well-known exchangers are Binance, Skrill, Bitfinex, Coinbase, Bitstamp, Coinmama, CEX.IO etc.
4. **User** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal use. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money from an exchanger or directly from the administrator/Miner (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide

a real or virtual good or service); (3) self-generate units of the virtual assets currency by "mining"

5. **Virtual Asset wallet** is the software application for holding, storing and transferring bitcoins or other virtual currency.
6. **Wallet provider** is an entity that provides a virtual currency wallet for holding, storing and transferring bitcoins or other virtual currency. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. Some of well-known Wallet providers are Bitcoin Core protocol, Electrum, Exodus, Jaxx, Copay, Coinbase, Blockchain etc.

2.3. Taxonomy of Virtual Assets

Based on the involvement of different participants from virtual asset system, virtual assets can be distinguished into centralized and decentralized Virtual assets:

Criterion	Centralized	Decentralized
Software Architecture	Centralized	Distributed (Blockchain)
Issuer	Administrator	Miner
Exchange Rate	Pegged	Floating
Convertibility	Exchanged for fiat currency	Exchanged for fiat currency
Participants	Administrator, Exchanger, User	Miner, Exchanger, User
Examples	E-gold, WebMoney, Linden Dollars	Bitcoin, Onecoin, Litecoin, Ripple

The decentralized virtual assets are particularly vulnerable to money laundering and terrorist financing abuse, due to easy convertibility and distributed architecture, which provides anonymous transfer of funds without passing through a central authority.

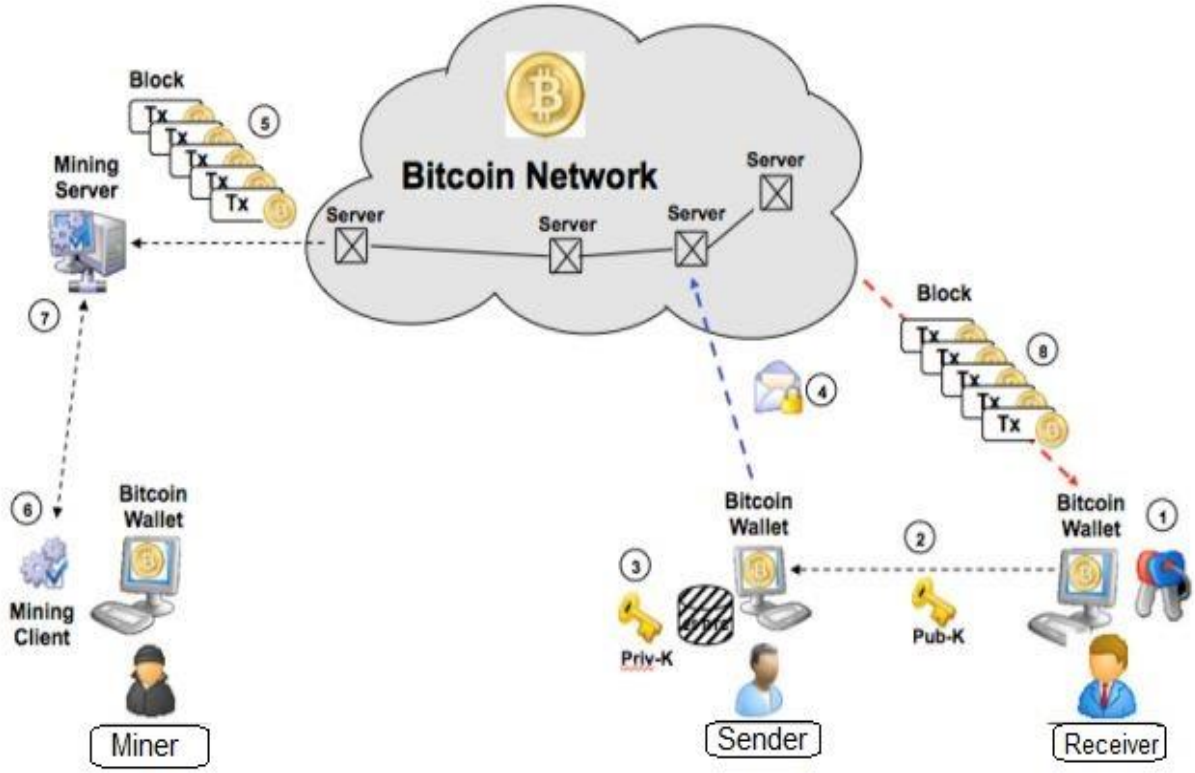
2.4. The Transaction Cycle of Virtual Assets

The transactions of Virtual Assets relies on public and private keys (provided through Virtual Currency Wallet) to transfer value from one person to another. The safety, integrity and balance of virtual asset ledgers is ensured by a network of mutually distrustful parties (miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee.

1. **Virtual Asset Wallets:** The individuals (sender and receiver) require Virtual Asset Wallets for performing a transaction in virtual assets. A Virtual Asset Wallet contains a public key and a private key.

2. **Address Creation:** The receiver randomly generates a new address (public key) for the sender using the Wallet.
3. **Payment Submission:** The sender will enter the unique address (public key) shared by the receiver in the wallet along with amount of virtual currency to be sent.
4. **Signature:** The sender will digitally sign the transaction with unique private kay, which will prove the integrity of transaction.
5. **Propagation and validation:** The transaction will flood through the distributed network to nodes who perform verification checks and re-propagate the verified transaction to other peers in the network.
6. **Creation of Block:** After validation, the miners will include the transaction in the next block to be mined.
7. **Proof-of-Work:** The miners will compete each other to calculate a hash that will solve the Proof-of-Work. This process takes 10 minutes on average.
8. **Confirmation of transaction:** Once the transaction is included in a block, the sender and receiver will receive a confirmation in their Wallets that the transaction has been completed.

Below is the graphical transaction cycle of virtual asset, in which a Bitcoin transfer transaction is performed.



Picture Credit: Joint Research Centre, European Commission

Once the transaction gets included in a block, it cannot be reversed or tempered. A set of virtual asset's transactions creates a block and these blocks kept on creating with the transactions, hence this process is termed as Blockchain.

3. Virtual Assets Service Provider (VASP)

As per FATF, VASP means any natural or legal person who as a business conduct one or more of the following operations on behalf of its clients:

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

This definition encompasses a range of crypto businesses, including exchanges, ATM operators, wallet custodians, and hedge funds.

4. Risk Associated with Virtual Assets and VASP

The potential AML/CFT risk associated with virtual assets are as following:

- Virtual Assets are considered high risk due to decentralization of peer-to-peer online transactions, which also enable criminals to use VPNs to obfuscate location and the origin/destination of transactions.
- There is high level of anonymity in transactions of virtual assets on the internet, which makes it difficult to identify individuals and source of funds involved in transactions. Further, there are various privacy or anonymity enhancing coins, which are even harder to trace.
- Virtual Assets are easily convertible to/from fiat money and potentially not subject to AML/CFT requirements.
- VASPs located in one jurisdiction may offer their products and services to customers located in another jurisdiction where they may be subject to different AML/CFT obligations and oversight. The criminals can exploit countries with weak, or absent, national measures for VAs.
- Risk of VASPs to operate without a license and/or registration, which require range of tools and resources for investigating the presence of an unlicensed or unregistered VASP.

- Law enforcement cannot target one central location or entity (administrator) for investigation or virtual asset seizure purposes.
- VAs can be used to quickly move funds globally, nearly instantaneously and largely irreversibly, and to facilitate a range of financial activities—from money or value transfer services to securities, commodities or derivatives-related activity, among others.
- Lack of screening and required information relating to VA transfers in order to comply with the targeted financial sanctions obligations (UNSCR-1267 & UNSCR-1373), and subsequent freezing of assets. No clear mechanism for real time blocking of transactions.
- May fuel the criminal activities in any region by concealing and disguising the proceeds of crimes.
- Virtual assets and its transactions are potentially vulnerable to raise funds for terrorism.
- Virtual Assets transactions may be conducted using dark net and commonly used in illegal trade commenced on dark web.

5. FATF Recommendation on Virtual Assets and VASPs

Financial Action Task Force (FATF) issued following guidance on virtual assets on time to time basis.

- "Virtual currencies: Key Definitions and Potential AML/CFT Risks" were issued in June 2014.
- "Guidance for a Risk-Based Approach to Virtual Currencies" was issued in June 2015.
- The FATF adopted two new Glossary definitions, "virtual asset" (VA) and "virtual asset service provider" (VASP) and updated Recommendation 15 in October 2018.
- FATF added an interpretive Note to Recommendation 15 to further clarify the FATF requirements in wake of ML/TF Risk associated with Virtual Assets in June 2019.
- In September 2020, the FATF released a report on Virtual Asset Red Flag Indicators of ML/TF.
- Update guidance for a risk-based approach- Virtual Assets and virtual asset service providers in October 2021.
- Targeted Update on Implementation of FATF's Standards on VAs and VASPs in June 2022.

The FATF requires its member countries "To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations." FATF requires jurisdictions to conduct customer due diligence, ongoing monitoring, suspicious transaction reporting, record keeping and other AML/CFT preventive measure.

6. Pakistan's NRA and TFRA finding on Virtual Assets

Virtual Assets have been identified as potential threat for ML/TF in updated National Risk Assessment of Pakistan (NRA), 2019. Further, as per National Terrorism Risk Assessment (TFRA) 2018 the TF risk associated with 'Virtual Currencies' is considered to be **"High"** on overall basis. While no law currently governs the trade of virtual assets/ crypto currencies in Pakistan.

7. Controls in Pakistan to combat risk of Virtual Assets

The State Bank of Pakistan (SBP) does not recognize Virtual Assets as legal tender to store and transfer value. SBP has issued caution regarding risks of virtual currencies and prohibited general public from trading in any type of virtual asset through its circular vide letter # ERD/M&PRD/PR/01/2018-31 dated April 6, 2018. Further, SBP has also refrained all banks, exchange companies and other financial service providers through its Circular # 03 of 2018 of BPRD dated April 6, 2018 (http://www.sbp.org.pk/bprd/2018/C3.htm) from facilitation of transactions related to virtual currencies and directed them to immediately report such type of transactions if found in any account to Financial Monitoring Unit (FMU) as an Suspicious Transaction Report (STR). However, there is a need for placing a regulatory framework in Pakistan to mitigate the ML/TF risk posed by virtual assets.

8. Scope of Strategic Analysis

This strategic analysis assesses and evaluates the money laundering and terrorism financing risks associated with emergent use of virtual assets. The analysis is based on domestic and international reports on virtual assets and the STRs reported to Financial Monitoring Unit (FMU) during the year 2021-22. Previously, FMU carried out similar nature of strategic analysis of STRs reported on transactions of virtual assets in December 2018, March 2020 and August 2021 which were shared with relevant stakeholders.

9. Objectives of the Strategic Analysis

The purpose of Strategic Analysis is to understand the money laundering and terrorism financing risk associated with the virtual assets and its transactions and define a way forward to mitigate these risks in Pakistan by focusing on best international practices. More specifically following are the major objective of the analysis:

- Understanding of virtual assets, underlying mechanism for transferring value and risk/vulnerabilities associated with such assets.

- To identify the customer type, who are involved in trading of virtual assets as users or exchangers.
- To identify the financial sectors, products, delivery channels and transactional pattern adopted by the virtual assets dealers for sale/purchase virtual assets.
- To assist the regulators, law enforcement agencies and other stakeholders to develop legal/regulatory framework to govern the virtual assets.
- To develop the red flag indicators which will assist the reporting entities to identify the customer, products, delivery channels and geographies involved in virtual asset trading, to safeguard the financial sector from the risk posed by virtual assets.
- To explore challenges in AML/CFT framework Pakistan while dealing with virtual assets.
- To suggest some recommendations in developing regulatory framework of virtual assets and virtual assets services providers in Pakistan.

10. Methodology

The report is based on primary data of Suspicious Transaction Reports (STRs) from the reporting entities, domestic and international cooperation requests from authorities, and secondary data obtained from different open-source reports such as FATF recommendations and reports on Virtual Assets, AML/CFT regulations of different countries, Pakistan's National Risk Assessment and Terrorism Risk assessment reports etc. The Data was analyzed using different analytical tools available with Financial Monitoring Unit of Pakistan such as goAML, internal and external databases and case typologies.

11. Data Limitation

The analysis is largely based on suspicious transaction reports (STRs) filed to FMU during the period of July 2021 to June 2022, the results may vary from the previous reports based on reporting quality and trends opted by the virtual assets dealer in recent past. Further, the quality of reported STRs may have impact on the overall strategic analysis. Further, the information received through domestic and international cooperation requests were utilized for analysis in sanitized manner.

12. Analysis of suspicious transaction reports on Virtual assets

As per State Bank of Pakistan (SBP) Circular No. 03 of 2018 dated April 06, 2018, the financial institutions are required to file STRs on the transactions which involve the sale/purchase of virtual assets. In this regard a number of STRs were reported to FMU by different financial institutions on the basis of possible involvement of the individuals in trading of virtual assets through their bank accounts and other channels during the period of July 2021 to June 2022. The reporting entities found the involvement of the individuals on the basis of following parameters:

- Transactions (attempted or conducted) with online exchanges providing cryptocurrency of virtual assets related services
- Individuals conducted transactions with other individuals, who were involved in virtual asset trading (P2P transactions)
- On the basis of market information and public information found on social/electronic media
- Upon declaration of individuals regarding their involvement in virtual assets
- Individuals are already under inquiry by any law enforcement agency for alleged involvement in virtual asset trading
- The reporting entity identified in involvement in virtual assets based on transactional pattern
- The reporting entity received fraud complaints from customers, whereby they were cheating for making payment for virtual assets

Below is the sector wise summary of the STRs reported on the basis of possible involvement of the individuals in trading of virtual assets:

Reporting Sector	Total No. of Reports
Islamic Banks	1007
Private Banks	740
Public Banks	34
Microfinance Banks	5
Electronic Money Institution (EMI)	44
Exchange Companies	11
TOTAL	1841

FMU received high number of STRs (1841) during the period of July 2021 to June 2022, as compared to 374 STRs reported during July 2020 to June 2021.

12.1. Customers Analysis

The individuals involved in sale/purchase of virtual assets through banking and other financial channels can be categorized into following:

a. **Business individuals/ Sole proprietors:** This includes individuals involved in different businesses such as forex trading, software houses, computer shops, mobile shops, general trading, import export, furniture, fruits and vegetables, Online shopping businesses, pharmacy, commission agents and others.

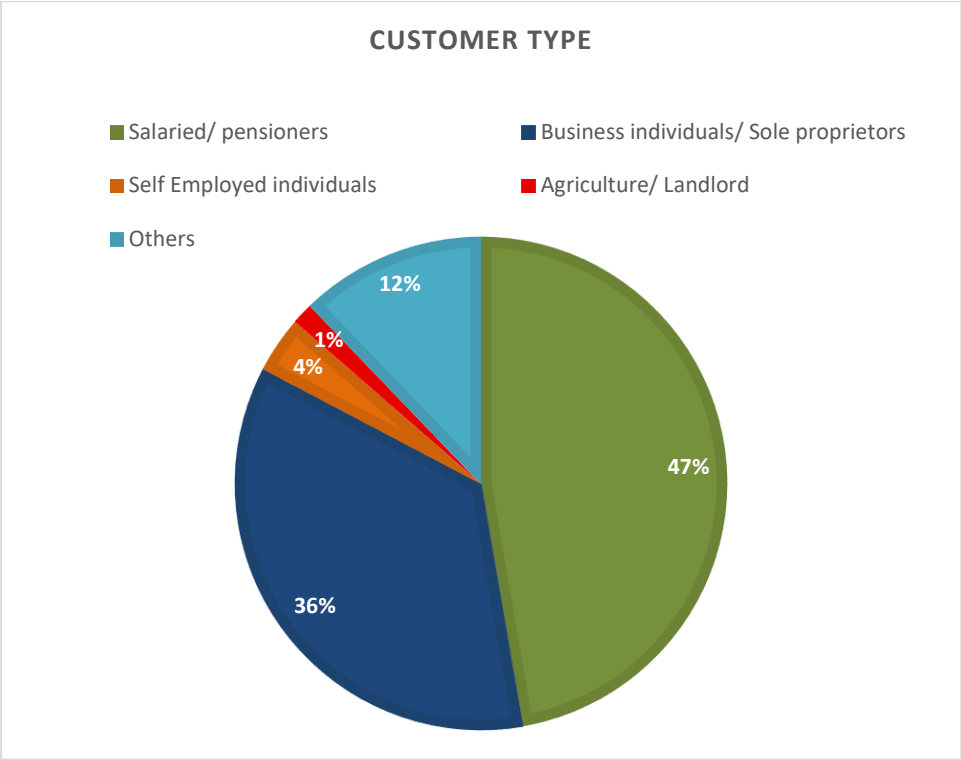
b. **Self Employed individuals:** Under this category freelancers, real estate agents, jewelers, Lawyers, carpenters, consultants, anchors, doctors, handicrafts, boutique and parlors, electricians, movie makers and labors are included.

c. **Salaried/ pensioners:** This includes persons associated with different organizations and their source of income is salary or pension. This category contains private employees, government officials, armed personals, bankers, teachers and professor, online service providers, IT employees etc.

d. **Agriculture/ Landlord:** The individuals associated with agriculture or owners of agricultural, residential and commercial properties.

e. **Others:** Other's category includes some high-risk customers such as housewives, students and unemployed individuals (source of income is home remittances).

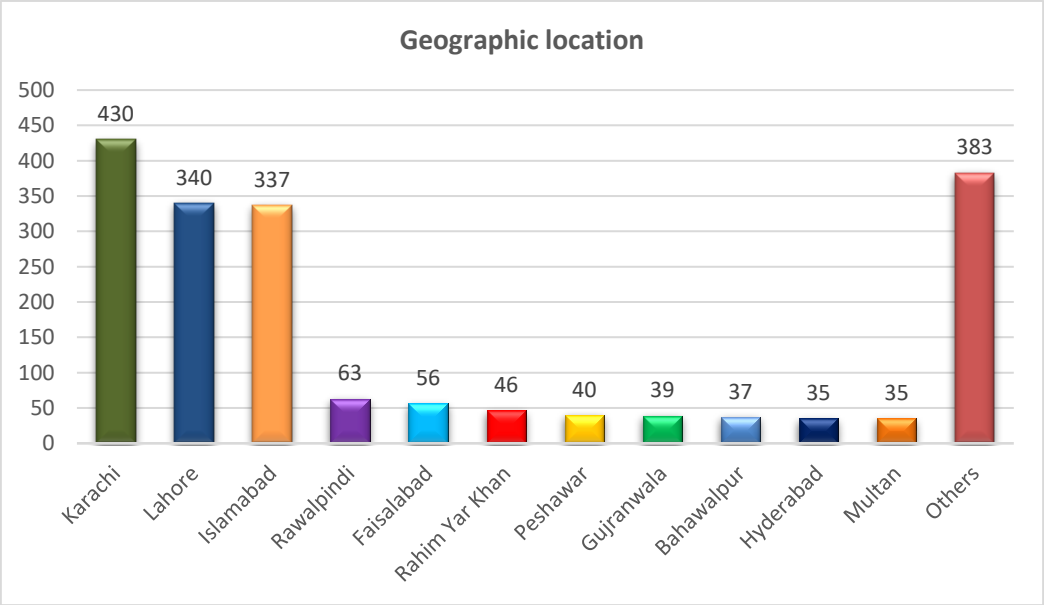
The breakup of customer type is given below:



Almost 47 % individuals involved in sale/purchase of virtual assets are salaried or pensioners, followed by businessmen (36 %) and 12 % individual belong to others category, which includes students, housewives and unemployed persons.

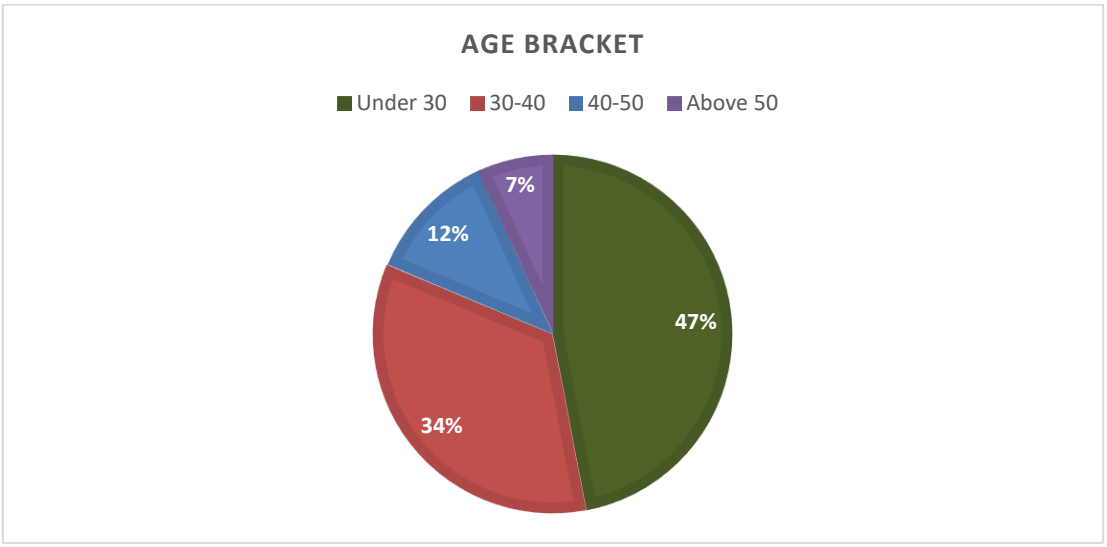
12.2. Geographic Analysis

The individuals are resident of different areas of Pakistan, however majority of them (almost 60 %) are from developed cities such as Karachi, Lahore and Islamabad. Below is the geographical segregation of individuals:



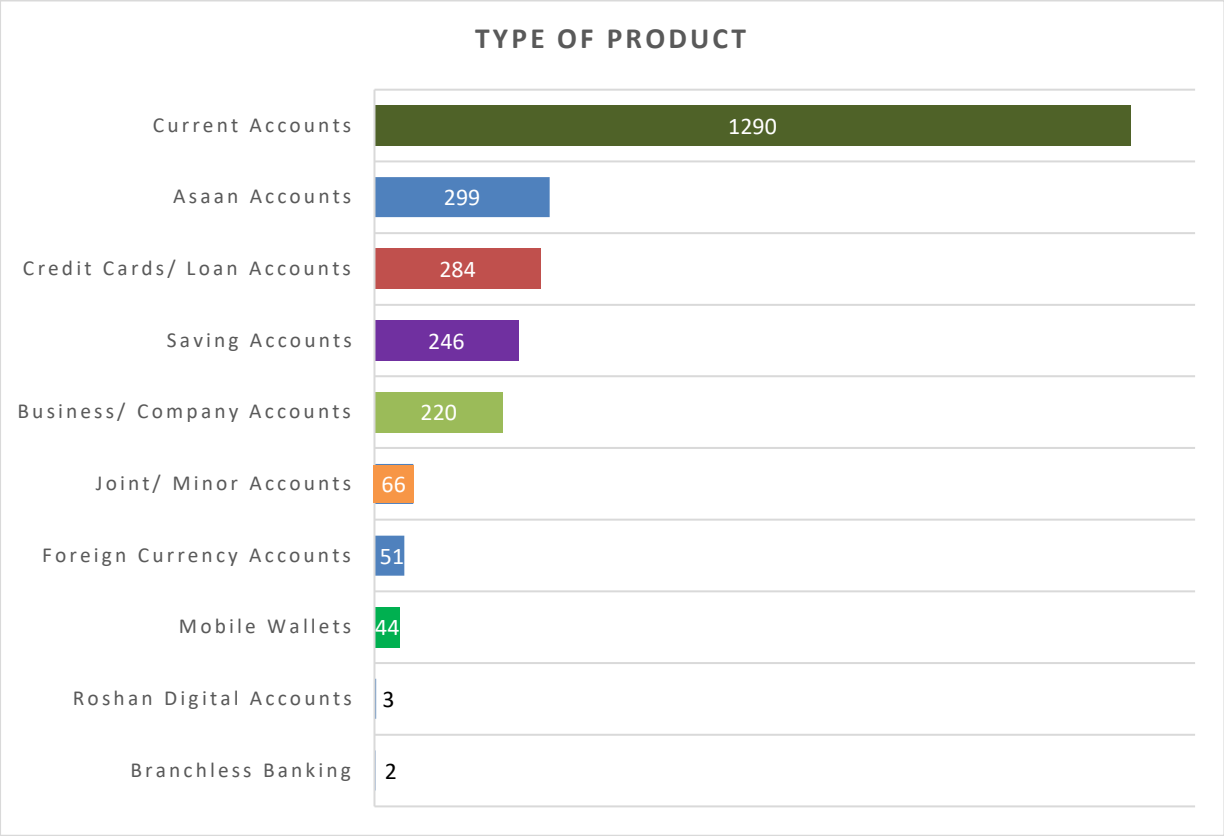
12.3. Demographic Analysis

Most of the individuals had declared their source of income as salaried persons, IT businesses and students, which shows that mostly educated persons are engaged in virtual assets business. Further, 47 % of individuals are underage of 30 years. The age brackets of individuals are given below:



12.4. Product Analysis

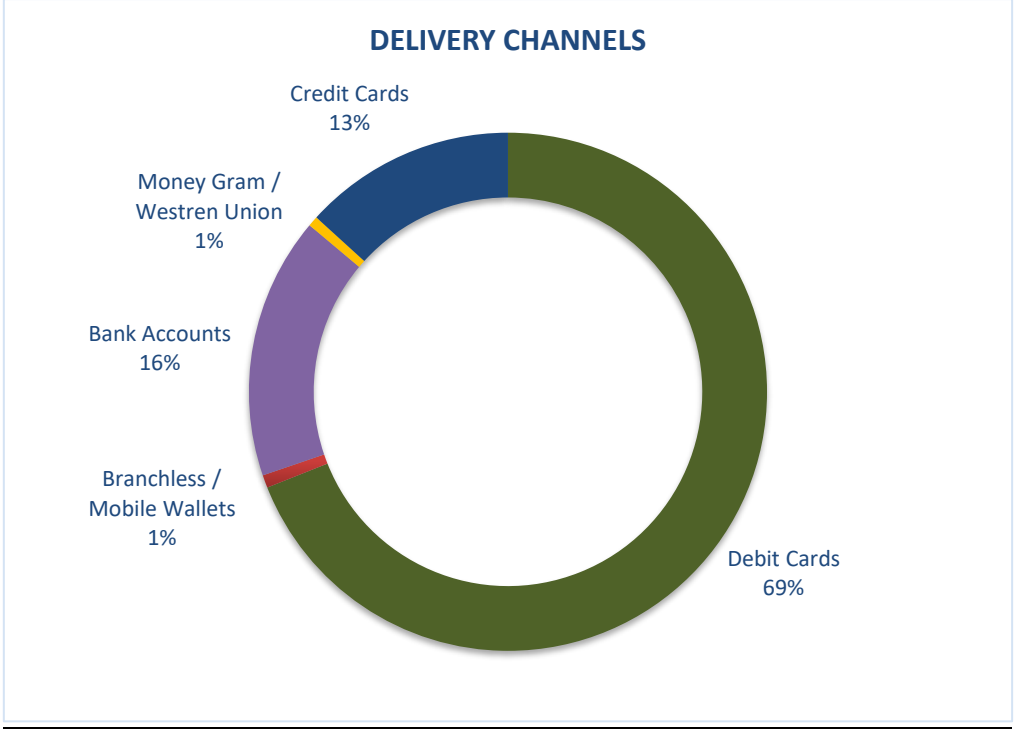
As most of the STRs were reported from banking sector, therefore it has been transpired that the individuals are mostly using their bank accounts of different nature for sale/purchase of virtual assets from online Virtual Asset Service Providers (VASPs). Below is the analysis of different account types used for virtual assets related transactions:



Further, some individuals conducted transactions through Western Union and Money Gram facilities as walk in customers to receive funds related to trading of virtual assets.

12.5. Delivery Channels

The individuals have used different delivery channels to purchase virtual assets from the virtual asset service providers (VASPs) and merchants such as Point of Sale (POS) using the credit cards and debit cards, Inter Bank Fund Transfers (IBFTs) and Internet transfers (INET) through bank accounts. Further, the individuals mostly use ATMs, CDMs for cash deposit and withdrawals, Mobile Banking and Mobile Wallets, Western Union and Money Gram etc. for virtual asset transactions. Some of the individuals have also received funds through wire transfers and electronic fund transfers to receive money in their bank account from the Virtual Asset Exchangers and merchants. The analysis of different delivery channels used for virtual asset related transactions is illustrated below:



12.6. Transactional Pattern

It has been found that these individuals are mostly maintaining accounts in local currency (PKR) with the purpose of savings, receipt of salaries, remittances and business revenues. The transactional pattern in their accounts reveals that they received funds through IBFT (Inter Bank Fund Transfers), INET (Internet transfers), Mobile Banking, transfers through ATM and online cash deposits, cash deposits through CDM, followed by POS transactions through their debit and credit cards, IBFTs, IBanking, and cash withdrawals via ATM. Moreover, the individuals have also conducted transactions with unrelated counterparties without any plausible purpose.

12.7. Transactional activity

During the analysis of STRs, a significant level of transactional activity was observed in sale/purchase of virtual assets through bank accounts, credit cards, debit cards and other channels. During the analysis of STRs reported in year 2021-22, it was noticed that activity involving a total amount of **PKR 930.7 million** was reported in attempted or conducted suspicious transactions which involve sale/purchase of virtual assets during the period of January 2020 to June 2021. In previous year (July 2020 to June 2021), a sum of PKR 583.4 million was reported as suspicious transactions, which involved sale/purchase of virtual assets. The product wise breakdown of the funds involved in suspicious transactions is appended below:

Type of Product	Suspicious Amount	
	No. of transactions	Amount Transacted
Bank Account	2957	489,756,711
Debit Card	13163	337,838,212
Credit card	4494	93,434,756
Branchless/ Mobile Wallets	71	574,196
Western Union	13	3,722,202
Total	**20885**	**930,757,659**

11.7.1. Nature of transactions

The transactional activity explained above involved three types of transactions i.e. purchase of virtual assets, sale of virtual assets and Person-to-Person (P2P) transactions for indirect sale/ purchase of virtual assets or settlements. Transaction nature wise summary of amounts is following:

Type of Product	Suspicious Amount	
	No. of transactions	Amount Transacted
Purchase of Virtual Assets	18787	512,605,323
Sale of Virtual Assets	740	89,402,889
P2P transactions	1203	328,749,447
Total	**20885**	**930,757,659**

11.7.2. Rejected Financial services

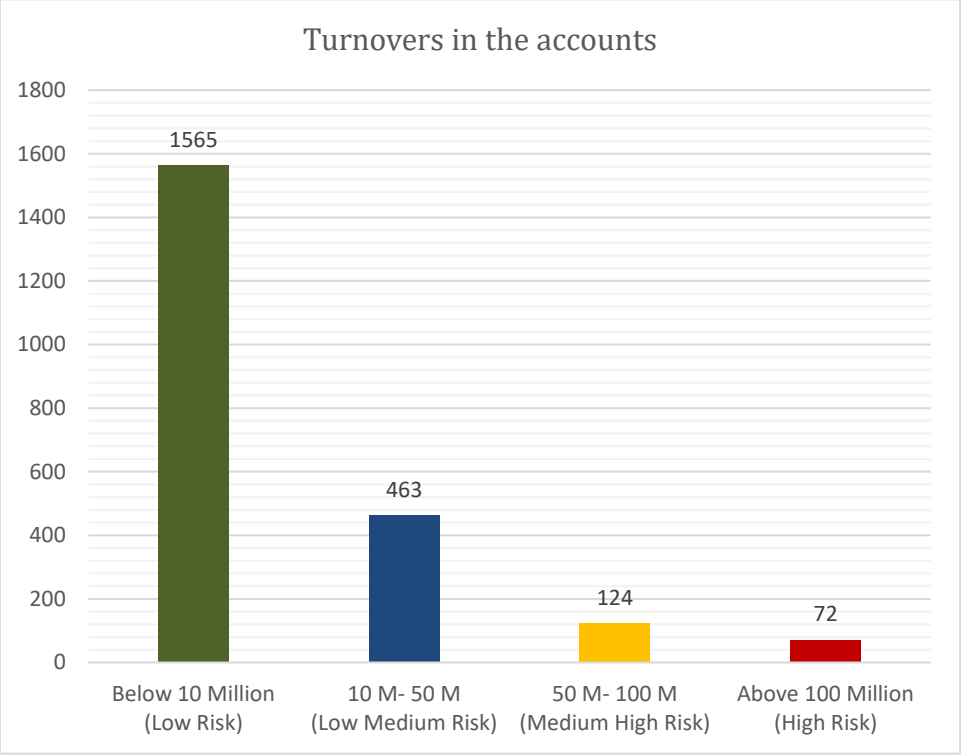
It is pertinent to mention here that several transactions of sale/purchase of virtual assets were also blocked by the financial institutions. The summary of blocked transactions is appended below:

Period	No. of transactions blocked	Involved amount
Total	**293**	**14,864,273**

Out of 20885 transactions reported for sale/purchase of virtual assets or P2P transactions involving trade of virtual assets, only 293 transactions were declined by the financial institution. Hence, there is possibility that the financial institutions are not being able to detect transactions of virtual assets on real time basis, as required by the regulator. Further, four instances were reported whereby the bank declined to open the account of individuals on suspicion of their unclear source of income and banks suspected that the individuals are engaged in virtual assets trading.

11.7.3. Level of transactional activity in the accounts

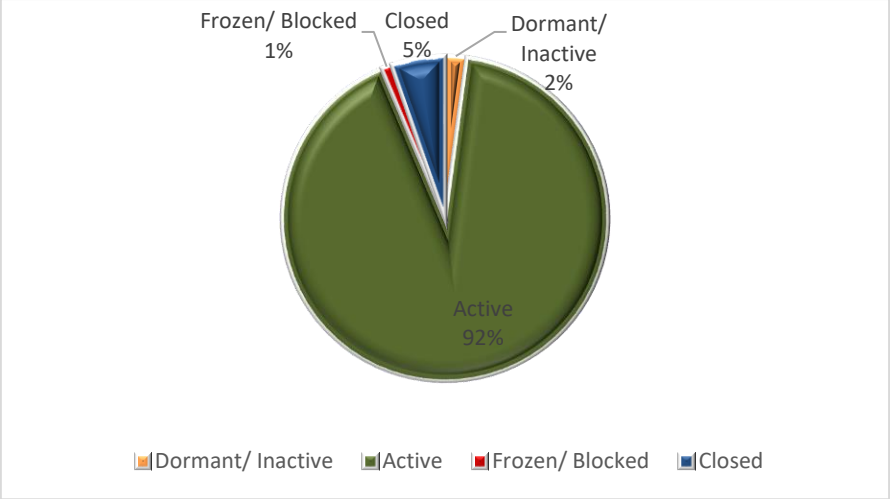
The individuals involved in virtual assets transactions were maintaining individual/Business accounts, Credit Cards, Branchless Banking Accounts and Mobile Wallets. The major transactional activity for sale/purchase/P2P transactions of virtual assets was carried through their bank accounts. In this regard, 2504 bank accounts were identified, wherein it was observed that transactions in small amounts were continuously conducted with high frequency. An aggregate turnover of PKR 45.0 billion was noticed in these accounts with an average turnover of PKR 20.0 million. Below is the segregation of accounts based on the aggregate turnovers;



It is pertinent to mention here that almost 70% of accounts fall under low risk category i.e, having turnover below PKR 10 million.

11.7.4. Status of accounts

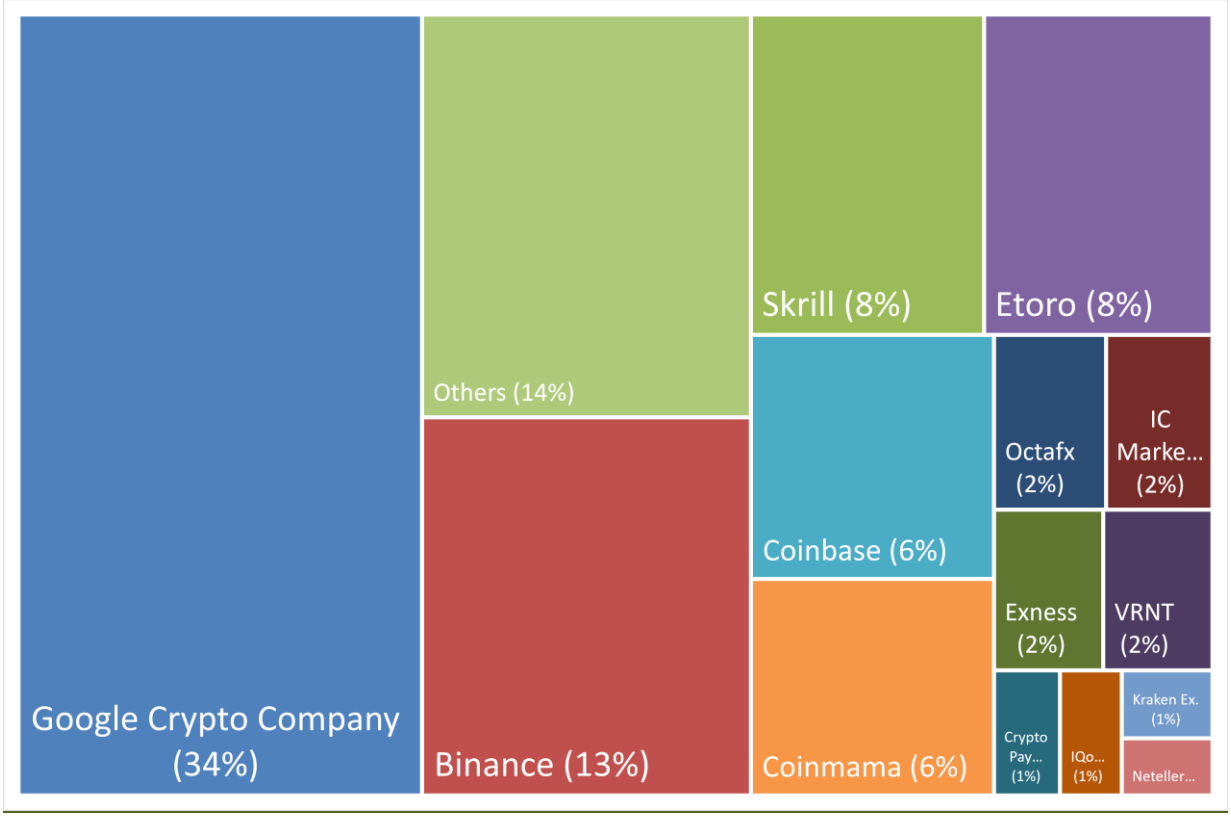
While analyzing the suspicious transaction reports it was noticed that some individuals were maintaining multiple account, with significant transactional activity. Below is the status of bank accounts:



It is worth mentioning here that almost 92% of accounts are active, while others are either closed, inoperative or frozen by the banks.

13. Major Virtual Asset Service Providers (VASPs) and Merchants

As per FATF updated guidance for a risk-based approach on Virtual Assets and Virtual Assets Service Providers (October 2021), the degree to which ML/TF risks materialize depends on the extent mass-adoption of a particular virtual currency, criminals tend to make use of the more widely adopted or popular virtual assets in their illicit activities. The individuals are using multiple online channels for trading of virtual currencies. Below are some major channels identified through STRs:



In addition to above, following platforms were identified from the reporting of STRs, which are apparently engaged in providing services of virtual assets trading/investment locally.

- **MCM** application for crowd funding, which provides reward on inviting other individuals, investment in cryptocurrency and cloud mining.
- **Fiberpay.pk** is a payment processor for digital currencies, similar to the payment processors, gateways, and acquiring bank credit cards use.
- **Profit4x.com** provide services of trade in forex, commodities, spot metals, indices and crypto currencies from a single account.
- **B4U Global** is a cryptocurrency trading company, its infrastructure facilitates investment in the cryptocurrencies industry with daily profit growth on investment.
- **Walton Traders** has been identified/suspected to be acting as an agent for OctaFx (foreign forex broker) and facilitating forex trading by accepting deposits/ withdrawals from general public in its accounts tagged with the application of OctaFX.

14. Criminal Offence linked with Virtual asset transactions

Virtual assets can be used for illicit activity, like for traditional means of payment. The difference lies in the underlying technology i.e. Blockchain, which allows two persons to exchange value directly with one another without a trusted intermediary. According to Chainalysis Crypto Crime Report (2022), the value of transactions associated with illicit activities was USD 14 billion in the year 2021, as compared to USD 7.8 billion in year 2020. These illicit activities involved scams, frauds, cybercrimes, darknet market, terrorism financing, child abuse etc.

During our analysis, it was noticed that most of the individuals are engaged in sale/purchase of virtual assets for investment/ profit purpose. However, the analysis set out vulnerabilities/ risks that the virtual assets are suspected to be used in criminal activities such as Terrorism Financing, Hawala/ Hundi, Ponzi Schemes, Drug Trafficking, Sexual Exploitation, Gambling, Fraud and Forgery, Smuggling and Illegal trade, Tax evasion through unauthorized capital flight or concealment of real beneficiaries. Virtual assets may fuel the criminal activities with free flow of funds and may attract the criminals and terrorists to evade concerned authorities. It is worth mentioning here that various individuals involved in virtual assets related transactions were found under inquiry by the law enforcement agencies. In this regard, following predicate offences are suspected to be linked with the Virtual Assets:

14.1. Hawala/ Hundi

The transactions of virtual asset trading have similarities with the transactional pattern of Hawala/ Hundi dealer. It might not be wrong to say that virtual assets are the modern shape of Hawala, in the scenarios where it is not being regulated. Below is the comparison of modus operandi of Hawala and virtual asset transactions:

Characteristics	Hawala/ Hundi	Virtual Assets
Counterparties	Unrelated	Unrelated
Geographies	Far flung Areas	Far flung Areas
Transactional Activity	Deviate the declared profile	Deviate the declared profile
Tax History	No or minimum tax filed	No or minimum tax filed
Transactional Pattern	Inter-account transfers, Online Cash deposit and withdrawals	IBFTs, INET, Online/ CDM Cash deposit, withdrawals through ATMs
Retention of funds	No retention	No retention
Use of Bank Counter	Avoid	Avoid

Further, appended is the case study which illustrates the link of Virtual assets with the Hawala/ Hundi Operators:

Case Study 1 (Hawala and Virtual Assets)	
BACKGROUND	STR was reported on Mr. HA, who was maintaining account at ABC Bank, Jinnah road Branch, Quetta. He is resident of Qila Abdullah and engaged in the business of trading in the name of HA & Company based in Quetta (High risk domestic geography). The suspicion was raised that the transactional activity of Mr. HA does not commensurate with the stated profile and he is transacting with unrelated counterparties.
MODUS OPERANDI	The transactional activity in his accounts revealed that he was receiving fund through ATM transfers, CDM deposits and internal transfer from various cities such as Peshawar, Multan, Lahore, Karachi, Rawalpindi etc., followed by withdrawals via IBanking and ATM. During the analysis of STR, it was found that he had conducted heavy transactions with the virtual asset service providers (VASPs). Further, it was found that the individual is under the inquiry of Federal Investigation Agency due to involvement in Hawala/ Hundi related activities. Moreover, he was maintaining various sole proprietorship accounts at different banks, whereby high level of turnovers were observed.
OUTCOME	Based on the available information, it was suspected that the individual was involved in Hawala and using the virtual assets for transacting the funds. Moreover, there was risk of involvement in smuggling and/or terrorism due to high risk bordering area, which is known for such activities.

Case Study 2 (Hawala and Virtual Assets)	
BACKGROUND	STR was reported on Mr. AH, who was maintaining account at ABC Bank, Chiniot. As per STR, he was engaged in business of Real Estate and Developers. The suspicion was raised that the transactional activity of Mr. HA does not commensurate with the stated profile and he is transacting with unrelated counterparties. Upon inquiry by the bank, the individual informed that he was involved in trading (sale/purchase) of virtual assets/ crypto currency.
MODUS OPERANDI	During analysis, an aggregate activity of more than PKR 100 million was noticed in the account. The transactional activity in his accounts revealed that he was receiving fund through internet fund transfers, followed by immediate withdrawals in cash. The individual received funds from unrelated

	counterparties such as kiryana merchant, mobile & computer business, commission agent, poultry & dairy farm business, travel & tours etc. Upon inquiry by the bank, the individual informed that he was involved in trading (sale/purchase) of virtual assets/ crypto currency. The individual was also maintaining account in other banks, and it was found that he declared different businesses i.e. real estate and garment to different banks for opening of accounts, while none of these businesses have been declared on NTN. The individual also exchanged multiple foreign currencies like AED, AUD, GBP, USD, SAR, Euro etc. from open market equals to PKR 20 million. It was also found that the individual frequently travelled to neighboring countries through land route.
OUTCOME	Based on the analysis, it was suspected that the individual was probably involved in Hawala and using the virtual assets for transacting the funds. Moreover, there was risk of cash smuggling and/or terrorism due to bordering area, which is known for such kind of activities.

Keeping in view, the Modus Operandi and case typology the connection between the Hawala and virtual assets cannot be ruled out.

14.2. Ponzi Schemes and frauds

Ponzi schemes are investment frauds that pay existing investors with funds collected from new investors. During the analysis few companies and individuals were found, who were offering unauthorized investment schemes with high rate of return to general public. Few case studies are provided below of Ponzi schemes, whereby virtual assets were used for fraud and cheating public at large. It has been noticed that the virtual assets has opened a window for fraud/ Ponzi schemes in Pakistan, wherein a group of individuals are raising funds from general public as virtual assets investments by offering lucrative returns and defrauding the public by engaging in unauthorized activity. Following are few cash studies of Ponzi schemes, using virtual assets as tool:

Case Study 1: (Ponzi Schemes and Virtual Assets)	
BACKGROUND	Mr. GM declared himself as proprietor of M/s WAL Traders, engaged in business of IT services, E-commerce and online advertisement services. The individual opened five accounts in the name of M/s WAL Traders at different banks in the year 2019. The transactional activity in the accounts was comprised of online transfers (IBFTs, Internet Banking, Mobile applications) and cash deposits from a large pool of individuals all over Pakistan. The credit transactions were of small amounts but frequency of credit transactions was very high, while debits were less in numbers but high in values. An aggregate activity of PKR 1.5 billion was noticed in the account and all the accounts were closed at the end of year 2020. Simultaneously, the individual registered a private limited company with SECP in the name of M/s WAL Trader (Pvt) Ltd. which was involved in business of online shopping and E-Commerce. As per company registration form, it had three directors namely Mr. GM (51% shareholder), Mr. SH (25% shareholding) and Mr. AA (24% shareholding). The individuals opened 7 company accounts in name of M/s WAL Trader (Pvt) Ltd. with different banks in Pakistan at start of year 2021. However, Mr. GM was the only authorized signatory in all the company accounts opened in different banks. An aggregate activity of PKR 2.50 billion was noticed in the company accounts, mostly comprised of online transfers (IBFTs, Internet Banking, Mobile applications) and cash deposits from different individuals as investment. The analysis transpired that the accounts were used to raise fund from general public from all over Pakistan as investments by offering lucrative profits, which against the mandate of the company. The financial institutions, regulatory bodies and law enforcement agencies started to get complaints against the entity from general public regarding frauds and cheating public at large. Upon inquiries by the banks,

	the individuals withdrew all funds from the accounts. Later, all the accounts were either closed or blocked by the banks, upon instruction of LEA.
MODUS OPERANDI	Mr. GM opened accounts in name of M/s WAL Traders and M/s WAL Traders (Pvt) Ltd. During the analysis, it was identified that various accounts were used for crowd funding, which were opened in the name M/s WAL Traders and M/s WAL Traders (Pvt) Ltd. and operated by only Mr. GM. An aggregate activity of PKR 4.0 billion was noticed in the accounts, which appears to be raised from general public using Ponzi Scheme. Further, FMU also identified personal account of director of M/s WAL Traders (Pvt) Ltd. at different banks. Moreover, the major counterparties of M/s WAL Traders (Pvt) Ltd. were also analyzed, which transpired that most of the counterparties were middle- and low-income individuals doing small businesses or employed in public or private sectors, who transferred funds to M/s WAL Traders (Pvt) Ltd. as investment. While few counterparties appeared to be agents of Walton Traders (Pvt) Limited, who were mobilizing the public for investment in M/s WAL Traders (Pvt) Ltd. using social media and YouTube. Based on the analysis of transactional activity and information from different sources, it was suspected that M/s WAL Traders (Pvt) Ltd. was involved in unauthorized activities such as Multi-Level Marketing and Ponzi Schemes, and collecting deposits from the public by offering lucrative investment packages. It was learnt from the reports that M/s Walton Traders (Pvt) Limited was working as agent of OctaFX in Pakistan and various social media accounts/ YouTube videos showed the walk-through process to make payment to the foreign forex trading app (OctaFx) through accounts of Walton Traders (Pvt) Ltd. Further, the State Bank of Pakistan (SBP) has declared online forex trading platforms such as OctaFX, Easy Forex etc. illegal and has barred Authorized Dealers from facilitating forex trading activity on these platforms.
OUTCOME	The financial intelligence was shared with relevant law enforcement agency i.e. FIA, who already has started inquiry against the M/s WAL Traders (Pvt) Ltd and its directors. The intelligence was also shared with the regulators for sensitizing the financial institution and appropriate regulator action. The SECP has included M/s WAL Traders (Pvt) Ltd. in the list of companies indulged in unauthorized activities of leasing/financing facility, MLM, pyramid/Ponzi schemes, seeking deposits from the general public in the name of jobs, investment and trading etc. Further, the FIA has registered a case against M/s WAL Traders (Pvt) Ltd. and its directors.
Case Study 2: (Ponzi Schemes and Virtual Assets)	
BACKGROUND	Multiple STRs were reported to FMU on M/s ABC Trading from different banks. ABC Trading was raising unauthorized deposits from the general public in the name of different investment plans. The company declared that it invests 60 % of its deposits to virtual assets and 40% to other business areas such as transport, technology, real estate etc. M/s ABC Trading is not registered with the SECP and lured people by offering high rates of return and marketed its schemes through local newspapers, social media, websites, and pamphlets, etc. Moreover, the SECP has also received several complaints and queries regarding ABC Trading.
MODUS OPERANDI	During analysis, Mr. SR was identified as CEO of M/s ABC trading and multiple business and personal accounts of Mr. SR and his family members were identified, wherein an overall transactional activity of more than PKR 10 billion was noticed, which appears to be raised from general public using Ponzi Scheme. Most of the funds were credited through online cash and debited through inward clearing, pay orders and cash. The credit transactions were of small amounts, but frequency of credit transactions was very high, while debits were less in numbers but high in values. Further, multiple companies were found to be registered on NTN of Mr. SR and he was maintaining various accounts on companies name under sole-proprietorship category. However, nominal or no income taxes were filed by the individual or its companies. The individual also registered a company in foreign jurisdiction, which was engaged in virtual assets trading. They marketed virtual assets as source of hefty returns and collected funds from general public in Pakistan as investment.
OUTCOME	The financial intelligence was shared with the relevant Law Enforcement Agencies and regulators for appropriate action. A regulator has imposed penalty of PKR 4 billion on M/s ABC Trading and an LEA issued arrest warrant for owner.

FMU received several suspicious transactions of IBFTs and Internet Banking, wherein the beneficiary bank received complaint from the sender's bank that the funds involved in the transactions were transferred fraudulently. Upon inquiry, the beneficiaries of funds disclosed that the funds were received against sale of Virtual assets.

14.3. Terrorism Financing

According to the National Terrorism Risk Assessment 2018 the TF risk associated with 'Virtual Currencies' is considered to be **"High"**. It was further stated in the NRA that FIA has registered 17 cases so far against individuals dealing in Virtual assets as it is legally not allowed in Pakistan. The global reports suggest that terrorist organizations primarily utilize virtual assets as part of their fundraising campaigns due to the anonymizing features and the lack of legal or regulatory framework. As per public sources, Ibn Taymiyyah Media Centre, a media wing of jihadist group based in Gaza, lunched a public crowdfunding donation campaign using virtual assets/cryptocurrency in 2016. Further, a case has been reported in United States where Daesh associates used virtual assets for terrorism financing. Moreover, the anonymity, convertibility, rapidity and global reach of virtual assets poses high risk to be used for transnational movement of terrorism financing.

Following is the case study on terrorism financing, wherein the use of virtual asset can be transpired:

Case Study (Terrorism Financing and Virtual Assets)	
BACKGROUND	STRs were reported on Mr. UK, who was maintaining accounts at different banks, in Karachi. The STRs were reported based on adverse media news, wherein Mr. UK was arrested by the Counter Terrorism Department (CTD) on 13-Jan-2021 in connections with funding for banned/proscribed entities. Reportedly, the suspect was student at an Engineering University of Karachi.
MODUS OPERANDI	During the analysis of STR, it was revealed that Mr. UK was using multiple channels in context of terror financing. He was also found in multiple WhatsApp groups of crypto currencies/ virtual assets, where he was purchasing crypto currencies/ virtual assets. Further, Mr. UK sent money through Electronic Fund Transfers (EFTs), to three (03) different individuals (a shop keeper, a policeman and a pharmaceutical sales manager), identified as major counterparties. During the investigations, all 3 recipients of funds revealed they sold cryptocurrency in a WhatsApp group to the accused Mr. UK. Overall activity of account turnover was reported Rs. 2.7 million approx. wherein the accused received funds from various housewives and self-employed individuals.
OUTCOME	Upon suspicion of terrorism financing, the financial intelligence was shared with CTD for probing the matter as deemed appropriate under the provisions of AML Act, 2010.

14.4. Corruption

Corruption is one of the high-risk predicate offences for money laundering in NRA-2019. As per NRA-2019, corruption is usually transnational in nature which means that although the offence may have been committed within the country, the proceeds are typically laundered in foreign jurisdictions such

as USA, UK and UAE (proceeds of corruption in other countries are rarely laundered through Pakistan, although there may be round-tripping and final integration of such proceeds in Pakistan). Virtual assets being a swift channel for transmitting funds across the border is vulnerable medium for corruption. Below case studies explain risk of virtual assets to be used for corruption:

Case Study 1 (Corruption and Virtual Assets)	
BACKGROUND	Mr. AM was a high-level retired Govt. officer (BPS-20) and maintaining an account at ABC Bank, Peshawar Cantt. Reportedly, the individual was involved in trading of virtual assets.
MODUS OPERANDI	The analysis of transactional activity transpired that the individual received high value of funds through Interbank Fund Transfers (IBFTs) and ATM transfers, and spent high volume of funds PKR 1.0 million on some online exchanges i.e. forextime.com, Skrill.com and OctaFX.com through multiple debit card transactions. As per FMU's database, it was found that the individual was under inquiry by NAB, regarding accumulation of Assets beyond know source of income.
OUTCOME	The financial Intelligence was shared with relevant Law enforcement agency as it was suspected that Mr. AM might route the proceeds of crimes using virtual assets.

Case Study 2 (Corruption and Virtual Assets)	
BACKGROUND	Mr. AM was a involved in real estate business and owner of a housing society in Pakistan. The individual was maintaining a large number of personal and business accounts is different currencies and various banks.
MODUS OPERANDI	The analysis of transactional activity transpired a high level of turnovers in the personal accounts of individuals (Approx. PKR 4.5 billion). The individual was also involved in purchase of foreign currency from the open market. Reportedly, he purchased a sum of USD 10 million in period of few months during the year 2021. During analysis, high volume of foreign remittances were also noticed in his accounts. It was also noticed that the individual spent high volume of funds on online exchanges using his credit card for purchase of virtual assets. Further, it was found that the individual was nominated in a case FIR registered with Police by Land Development Authority for cheating public at large and issuing fake or forged property documents to number of individuals related to his housing society.
OUTCOME	The financial Intelligence was shared with relevant Law enforcement agency as it was suspected that Mr. AM might route the proceeds of crimes using virtual assets. Further, the level of transactional activity in the account did not commensurate with the declared income and tax filed by the individual over the year. Therefore, the information was also shared with tax authorities. The relevant law enforcement agency has authorized the inquiry against the individual.

It is worth mentioning here that a number of Government officials/employees were also found in trading of virtual assets.

14.5. Drug Trafficking

Drug Trafficking has been identified as one of the high-risk predicate offences for money laundering in NRA-2019. Pakistan is considered as the transit country for opium and its derivatives produced in neighboring Afghanistan and destined for other countries. However, the bulk of proceeds realized outside of Pakistan and Pakistani-based organized groups only receive a small share for facilitating the transit of the drugs in the country. The virtual assets provide high level of anonymity due to decentralization of peer-to-peer online transactions.

Case Study 1 (Drug Trafficking and Virtual Assets)	
BACKGROUND	STR was reported on Mr. AM, who was maintaining account at ABC Bank, Taunsa Branch, DG Khan. The transactional activity in the account of Mr. AM was reportedly unusual due to high turnovers in the account and transactions with unrelated counterparties.
MODUS OPERANDI	The analysis of transactional activity transpired that the individual was involved in trading of virtual assets. The individual was also found on a Virtual Asset trading platform. Mr. AM was conducting high value transactions with various unrelated counterparties, mostly were suspectedly involved in Hawala and other crimes, as per FMU's database. One of his counterparties, Mr. BA proprietor of M/s AA was found under investigation by ANF for acquiring proceeds of drugs. The account of Mr. BA was credited with PKR 2.7 million from the account of Mr. AM with unclear purpose.
OUTCOME	The financial Intelligence was shared with relevant Law enforcement agencies as it was suspected that Mr. AM is involved in virtual asset transactions and possibly facilitating others to route the proceeds of crimes using virtual assets.

Case Study 2 (Drug Trafficking and Virtual Assets)	
BACKGROUND	STR was reported on Mr. NAS who was a salaried person, working in a private firm. He was maintaining account in ABC Bank for salary purpose. His account was blocked by the bank upon request of a law enforcement agency, for his alleged involvement in Drug Trafficking. Further, international cooperation request was also received on the individual for using Bitcoins for payment of drugs.
MODUS OPERANDI	As reported, Mr. NAS indulged in online purchase/sale of controlled drugs in USA and UK. He used to purchase controlled drugs online through websites at Dark Web and made the payments thereof through crypto currency (Bitcoin). The sale of controlled drugs was made through websites with IP jumpers (to hide the real identity), designed and operated by Mr. NAS and his associates in Karachi for international customers. He had contacts in UK for arrangement and subsequent transportation of controlled drugs in UK. Funds were generated through these sales and payments thereof were received in multiple accounts in UK. After deduction of commission, freight charges, expenses, remaining amounts are transferred to Mr. NAS in Pakistan. For this purpose, he had multiple Crypto Currency accounts outside Pakistan and received payments via Bitcoin (crypto currency), Western Union, Money Gram, Ria Money Transfer in Pakistan by using names/CNICs of different persons (his employees).
OUTCOME	The financial intelligence was shared with Anti-Narcotics Force (ANF), which is under investigation by the competent authority.

14.6. Sexual Exploitation

Sexual exploitation is rated as medium risk in NRA-2019. Although, prostitution in Pakistan is illegal but there are many brothel houses, that are working under the garb of some other professions. Further, online applications and social media is being exploited for the sexual crimes and most of such applications use digital currencies (diamond coins) as source of income or payment.

Further, multiple STRs were reported on the individuals involved in sale/purchase of virtual diamonds used in various applications like BIGO LIVE, which was banned by PTA in July 2020 due to immoral contents.

Case Study (Sexual Exploitation and Virtual Assets)	
BACKGROUND	An STR was filed on the accounts of M/s LT (Pvt) Ltd. on the basis of unusual transactional activity and inquiries by a law enforcement agency. Reportedly, the company had two directors Mr. JW (foreign national) and Mr. FN (Pakistani national) and it was involved in business of IT/Software programming. As per public domain information, M/s LT (Pvt) Ltd. was also involved in live interactive video streaming and developed a mobile application "StreamKar", for this purpose. The company hired women for part time online marketing jobs. However, multiple complaints were lodged at FIA from female workers hired by M/s LT (Pvt) Ltd. that they were forced to do online sexual activities.
MODUS OPERANDI	As per media News, FIA has discovered an international network running 'porn app' from Karachi. FIA arrested the group who was working for a mobile application "Streamkar". FIA revealed that the App was owned by a female Ms. RM and Mr. FN was her partner who published job advertisements in different newspapers to hire female workers. The individuals were managing a team comprising 35 employees across Pakistan. According to the FIA Cyber Crime Wing, the group used the mobile app to connect their female workers with international clients. These women were then paid in 'diamond' (a form of virtual asset) for sexually explicit video calls with their clients. As per STRs, the accounts of M/s LT (Pvt) Ltd. and its director were blocked upon request of FIA. The transactional activity in the accounts was apparently unusual, as transaction amounts swing from small tickets to very large amounts through online/Funds transfer/ATM transfer. The banks were informed that the company is dealing with local as well as global clients for web designing in three strategically located countries across globe with a team of numerous professionals. While the funds were locally deposit/withdraw to/from different accounts within the country. Further, the directors and employees of M/s LT (Pvt) Ltd. and Stramkar received some foreign remittances through Western Union and Money Gram. Such as, Mr. MK, one of the members of group arrested by FIA visited Chishtian branch of ABC Bank in October 2020 to receive funds amounting to PKR 12,000 sent from Saudi Arabia through Western Union. Upon inquiry by the bank, Mr. MK stated that this money was received against the sale of coins for a mobile application "Streamkar". However, the transaction was rejected by the bank based on unclear purpose. It was suspected that Mr. MAK might be working as employee/agent of the group and was collecting remittance against sale of coins (virtual currency) for "Streamkar" mobile application. It is also pertinent to mention that Mr. MK has collected Rs.20,790 earlier on August 7, 2020 sent by the same remitter from Saudi Arabia through Western Union.
OUTCOME	Keeping in view, the involvement of diamond coins for above mention illegal activity, the risk of virtual assets to be used for sexual exploitation cannot be discounted. The financial intelligence was shared with FIA.

In addition, FMU received international cooperation requests from a foreign FIU on the individuals suspectedly involved in child pornography and online grooming of underage children. The individuals made online payments for purchase of child pornography using bitcoins.

14.7. Tax Evasion

During the analysis of STRs, it was found that some individuals have very high turnovers in their accounts but they have not filed income taxes or have filed minimum taxes which are not aligned with their transactional activity. Further, due to anonymity and free flow of funds without any check provide opportunity to evade taxes through unauthorized capital flight and hide the beneficial owners of funds. Below is case study that explains the use of virtual assets for tax evasion purpose.

Case Study (Tax Evasion and Virtual Assets)	
BACKGROUND	STRs were reported on Mr. SRK, who was running multiple private limited/ sole proprietorship concerns engaged in businesses of import/export, general order supplier and commodity trading. Mr. SRK is resident of Karachi and was maintaining various business accounts in the name of those companies at different banks. He has disclosed different profiles to the banks. The transactional activity in his accounts revealed that he was receiving high value funds through IBFTs, internet banking, internal transfers and cash deposits from several unrelated counterparties based in far flung areas.
MODUS OPERANDI	During the analysis, it was found that he was maintaining almost 70 accounts, whereby an aggregate activity of more than PKR 10 billion (approx.) was noticed during the last 3 years. Further, it was found that Mr. SRK is the owner of a renowned company operating in the business of Crypto currency, registered in foreign jurisdiction. Therefore it was suspected that the funds routed from his account might be linked to the virtual assets trading. It was further observed that Mr. SRK is registered for tax in Pakistan, but he had paid no/nominal income taxes despite of high level of transactional activity. Hence, it was suspected that the individual is involved in tax evasion or facilitating other to conceal true beneficiaries for avoiding applicable taxes.
OUTCOME	The financial intelligence was shared with the relevant authority to probe the matters related to taxes.

Case Study (Tax Evasion and Virtual Assets)	
BACKGROUND	Mr. SS was involved in business of Mobile Phone Accessories and was maintaining multiple business accounts at different banks. His business accounts were opened in different names like P4X, SS Mobile Centre, CC Consultancy etc.
MODUS OPERANDI	During the analysis, a high level of transactional activity PKR 500 million was noticed in the accounts of individual opened in the name of different business. The individual received funds in small chunks from a large number of individuals belongs to wide range of professions. As per public information, a website on the name of P4X was found, which was providing forex and cryptocurrency trading services. However, that company was incorporated in offshore territory. Further, a number of counterparties depositing funds in accounts of P4X, were reportedly involved in virtual assets. It was suspected that the funds routed from his accounts might be linked to the virtual assets trading. It was further observed that Mr. SS was registered for tax in Pakistan, but he had paid no/nominal income taxes despite of high level of transactional activity in the accounts. Hence, it was suspected that the individual is involved in tax evasion or facilitating other to conceal true beneficiaries for avoiding applicable taxes.
OUTCOME	The financial intelligence was shared with the relevant authority to probe the matters related to taxes.

During the analysis, some accounts were found with high turnover (as categorize as high-risk accounts). These accounts may be evaluated for tax matters.

15. Red Flag indicators to identify transactions related to Virtual Assets

Virtual Assets are not a legal tender in Pakistan and Virtual Assets Service Providers are prohibited in Pakistan. However, the individuals are using number of online exchanges or platforms for sale and purchase of Virtual Assets. Based on analysis, following are some red flag indicators to identify transactions related to Virtual Assets:

- The Virtual asset dealers mostly utilize their bank accounts, debit cards and credit cards for sale/purchase of virtual assets.

- Bank accounts and credit/ debit cards with high IBFT limits are attractive to the virtual asset traders.
- The individuals involved in Virtual Assets, mostly utilize IBFTs, mobile banking and ATMs for transacting funds and tends to avoid on-counter transactions.
- The students, youngsters, IT profession and salaried individuals are mostly involved in such type of activities.
- The trading of virtual currencies is common in big/ developed cities of Pakistan; however, the circle is expanding to other high risk domestic jurisdictions.
- The individuals also transact with unrelated counterparties in different locations.
- They conduct low/average size transactions in accounts with high frequency.
- The retention of funds in the accounts is very less.

16. Challenges in dealing with Virtual assets

The virtual assets carry significant money laundering and terrorism financing risk due to its nature of anonymous peer to peer transactions. It is crucial to bring them under the ambit of Anti-Money laundering and Combating the Financing of Terrorism. Following are the major challenges to deal with the Virtual assets:

- Virtual Assets are very complex in nature, it is difficult to understand the mechanism behind the creation and transactions of virtual assets.
- VASPs are prohibited in Pakistan, however many online VASPs are offering services for sale/purchase and transfer of virtual assets. The unregulated VASPs do not collect data on their customers or transactions, so no information is available to analyze and investigate the transactions.
- There is lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for transactions related to virtual assets.
- The virtual assets are globally traded and do not have boundaries for swift supervisor.
- It is difficult for the financial institutions to identify the transactions related to the virtual asset on real time basis.
- It is challenging to identify and verify the source of funding in virtual asset transactions.
- Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes.
- The authorities and financial institutions do not have access to any blockchain analytical tool, so it is almost impossible to make trail of transactions during investigation process.

17. Regulatory Framework for Virtual Asset Service Providers

The anonymity, convertibility, speed and global reach of virtual assets have made them attractive for the criminals and terrorists. It may warrant a substantial risk to societies, financial system and countries, if virtual assets will be left unregulated. In response to emergent use of virtual assets, its price speculation and introduction of new token, the regulators and governing bodies around the world have stepped into governing the use and trade of such digital assets. According to FATF updated guidance for a risk-based approach on Virtual Assets and Virtual Assets Service Providers (October 2021), anonymity is a major potential ML/TF risk posed by virtual assets, which can be addressed by placing AML/CFT obligations on VASPs. Some countries are regulating the virtual assets as commodity, however, most of them have accepted virtual asset service providers (VASPs) as money service providers. However, some of the countries including Pakistan have issued warning in trading of virtual assets and did not accept virtual assets as legal tender yet. However, a number of countries around the globe are in process of developing regulatory framework for the virtual assets after the recommendation of FATA (Rec. 15).

18. Suggestions for Financial Institutions:

As per SBP requirements, the financial institutions have developed good systems for identifications of transactions related to virtual assets and actively reporting STRs on such type of transactions, which is appreciated. However, following suggestions should also be taken into consideration to further enhance the quality of STRs being reported relating to virtual Assets.

- Properly explain in reason for reporting that how the reporting entity identified the transactions which are related to virtual assets.
- Reporting entities should explain any possible criminal activity or predicate offence (if any), found during analysis of transactions related to virtual assets.
- Reporting entities should identify and provide the detail of online exchange/ virtual asset service provider/ merchant on which the transactions were conducted for sale/purchase of virtual assets.
- Reporting entities are required to provide detail of all transactions conducted by the individual for sale/purchase of transactions over a period of time, as per goAML format.
- Provide nature of product and deliver channels used for purchase of virtual asset
- Explain type of customers and their geographic location
- Share purpose of purchasing virtual assets
- Highlight any transnational elements/ international linkages, while reporting of STRs
- If possible, try to capture wallet addresses and IP addresses

It is suggested that the financial institutions should carry periodic risk assessment of their products and services to curtail the inherent risk posed by the virtual assets. They should enrich their systems for proper screening of virtual asset transactions, such type of transactions may potentially be used for transmitting proceeds of crimes or for financing of terrorism. There are variety of blockchain analytical tools and compliance software for analysis of cryptocurrency transactions and monitoring on the blockchain, for risk management of virtual assets. The reporting entities may consider using such technologies for analysis of cryptocurrency transactions and to identify the parties in transactions involving virtual assets.

19. Conclusion

Keeping in view the above analysis, it is evident that the Virtual Assets pose significant money laundering and terrorism financing risk, which requires collaborative efforts of the stakeholders to develop a regulatory framework. The virtual assets are penetrating to the society at a rapid pace, despite of warnings to the general public and stance of declaring virtual assets as "not a legal tender" by the State Bank of Pakistan. Further, as per FATF updated recommendations, the member countries are required to set up a regulatory framework for the Virtual Asset Services Providers (VASPs). Therefore, the Strategic Analysis Report has been shared with relevant stakeholders under AMLA-2010 for appropriate measures/ controls on emergent use of bank accounts/ products/ services for trading of virtual assets such as Bitcoins.

20. Source of external information

- *Pakistan National Risk Assessment on Money Laundering and terrorism financing updated 2019*
- *Pakistan National Terrorist Financing Risk Assessment, 2018*
- *https://go.chainalysis.com/2022-Crypto-Crime-Report.html*
- *http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf*
- *http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf*
- *https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105207/lbna28386enn.pdf*
- *https://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf*
- *https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html*
- *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html*
- *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html*