Virtual Assets

The emerging risk of Money Laundering and Terrorism Financing

2021

FINANCIAL MONITORUNG UNIT
Govt. of Pakistan

2nd Floor SBP Main Building
I.I. Chundrigar Road, Karachi

Table of Contents

1. Executive Summary 1
2. Understanding Virtual Assets 2
2.1. Difference between Virtual Assets and E-money 2
2.2. The system of Virtual Assets 2
2.3. Taxonomy of Virtual Assets 3
2.4. The Transaction Cycle of Virtual Assets 3
3. Risk Associated with Virtual Assets 5
4. FATF Recommendation on Virtual Assets 6
5. Pakistan's NRA and TFRA finding on Virtual Assets 6
6. Controls in Pakistan to combat risk of Virtual Assets 6
7. Scope of Strategic Analysis 7
8. Objectives of the Strategic Analysis 7
9. Methodology 7
10. Data Limitation 8
11. Analysis of suspicious transaction reports on Virtual assets 8
11.1. Customers Analysis 9
11.2. Geographic Analysis 10
11.3. Demographic Analysis 10
11.4. Product Analysis 11
11.5. Delivery Channels 11
11.6. Transactional Pattern 11
11.7. Transactional activity 12
11.7.1. Nature of transactions 12
11.7.2. Rejected Financial services 12
11.7.3. Level of transactional activity in the accounts 13
11.7.4. Status of accounts 13
12. Major Virtual Asset Service Providers (VASPs) and Merchants 14
13. Criminal Offence linked with Virtual asset transactions 14
13.1. Hawala/ Hundi 14
13.2. Terrorism Financing 15

13.3. Drug Trafficking 16
13.4. Ponzi Schemes 16
13.5. Sexual Exploitation 17
13.6. Fraud and Forgery 17
13.7. Tax Evasion 18
14. Red Flag indicators to identify transactions related to Virtual Assets 18
15. Challenges in dealing with Virtual assets 19
16. Regulatory Framework for Virtual Asset Service Providers 19
17. Suggestions for regulating Virtual asset Service Providers in Pakistan 20
18. Recommendations 21
19. Conclusion 21
20. Source of external information 22

Virtual Assets
The emerging risk of Money Laundering & Terrorism Financing (2020-21)

1. Executive Summary

Virtual Asset refers to any digital representation of value that can be digitally traded, transferred, or used for payment. 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 January 2020 to June 2021. Below are the highlights of the strategic analysis:

- FMU received 447 Suspicious Transaction reports related to virtual Assets during the period of January 2020 to June 2021.
- The students and youngsters belong to IT profession/ salaried individuals are mostly involved in such type of activities.
- The individuals are using different channels for sale/purchase virtual assets such as bank accounts, debit cards, credit cards and Western Union.
- An overall suspicious activity of PKR 701.9 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 or used for payment. 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 decentralised 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 Bitfinex, Coinbase, Bitstamp, Poloniex, 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.

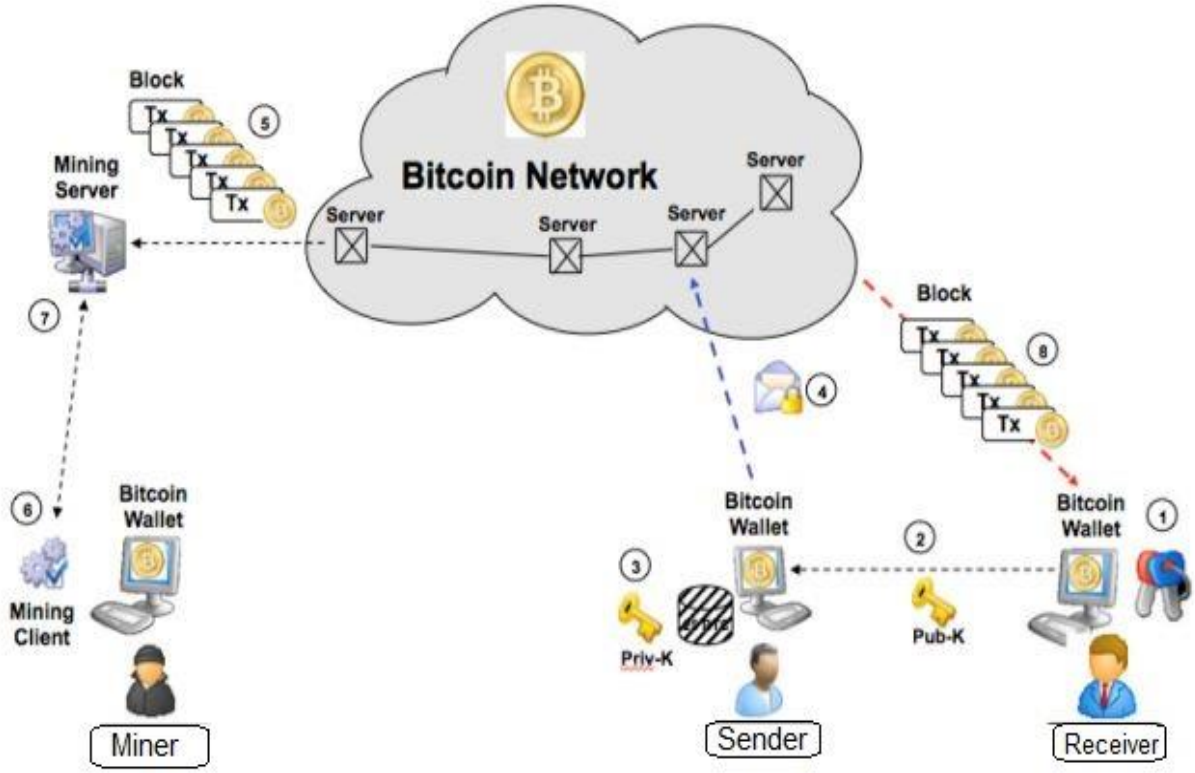
2.4. The Transaction Cycle of Virtual Assets

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. Risk Associated with Virtual Assets

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

- Virtual Assets are considered high risk due to decentralization of peer-to-peer online 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.
- Price Volatility and speculative nature of virtual assets make them risky.
- Virtual Assets are easily convertible to/from fiat money and potentially not subject to AML/CFT requirements.
- Lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries.
- There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns with regards to Virtual Assets.
- Law enforcement cannot target one central location or entity (administrator) for investigation or virtual asset seizure purposes.
- Difficult to make trail of transactions during investigation process
- Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers.
- May fuel the criminal activities in any region by concealing and disguising the proceeds of crimes.
- May hurt the countries' economies by unauthorized capital flight.
- Virtual assets and its transactions are potentially vulnerable to terrorism financing.
- Virtual Assets transactions may be conducted using dark net and commonly used in illegal trade commenced on dark web.

4. FATF Recommendation on Virtual Assets

Financial Action Task Force (FATF) has 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.

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.

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

Virtual Assets have been identified as potential thread 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.

6. Controls in Pakistan to combat risk of Virtual Assets

Currently, there is no law or regulations placed in Pakistan to mitigate the ML/TF risk posed by virtual assets. However, 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).

7. 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 2019. Previously, FMU had already conducted a strategic analysis on virtual currencies and its abuse for money laundering and terrorism financing in December 2018.

8. 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.

9. Methodology

The report is based on primary data received from the reporting entities as Suspicious Transaction Reports (STRs) and secondary data obtained from different domestic and international reports such as FATF recommendations and reports on Virtual Assets/ currencies, 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.

10. Data Limitation

The analysis is based on suspicious transaction reports (STRs) filed to FMU during the period of January 2020 to June 2021, 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.

11. Analysis of suspicious transaction reports on Virtual assets

Under the provisions of AML Act, 2010 a Suspicious Transaction Report (STR) is filed with FMU for a suspicious transaction conducted or attempted through a financial institution. The transaction is considered suspicious, inter alia, if there are reasons to suspect, after having examined the available facts including the background and possible purpose of the transaction, that the transaction involves funds derived from illegal activities or has no apparent lawful purpose or conducted in order to hide or disguise the funds involved. As per instructions of State Bank of Pakistan (SBP) 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 January 2020 to June 2021.

Below is the sector wise summary of the STRs:

Reporting Sector	2020 (Jan-Dec)	2021 (Jan-Jun)	Total No. of Reports
Private Banks	262	158	**420**
Islamic Banks	14	5	**19**
Public Banks	1	0	**1**
Microfinance Banks	3	1	**4**
Exchange Companies	0	2	**2**
Law Enforcement Agency	1	0	**1**
TOTAL	**281**	**166**	**447**

During the analysis of these STRs, following observations were noticed:

11.1. 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. Mostly the individual are associated with IT businesses.

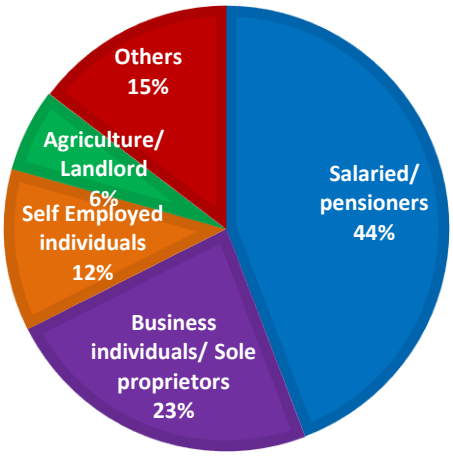
b. **Self Employed individuals:** Under this category freelancers, real estate agents, jewelers, Lawyers, carpenters, consultants, anchors, doctors, handicrafts, boutique and parlors, electricians, movie makers and labors are included.

c. **Salaried/ pensioners:** This includes persons associated with different organization 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).

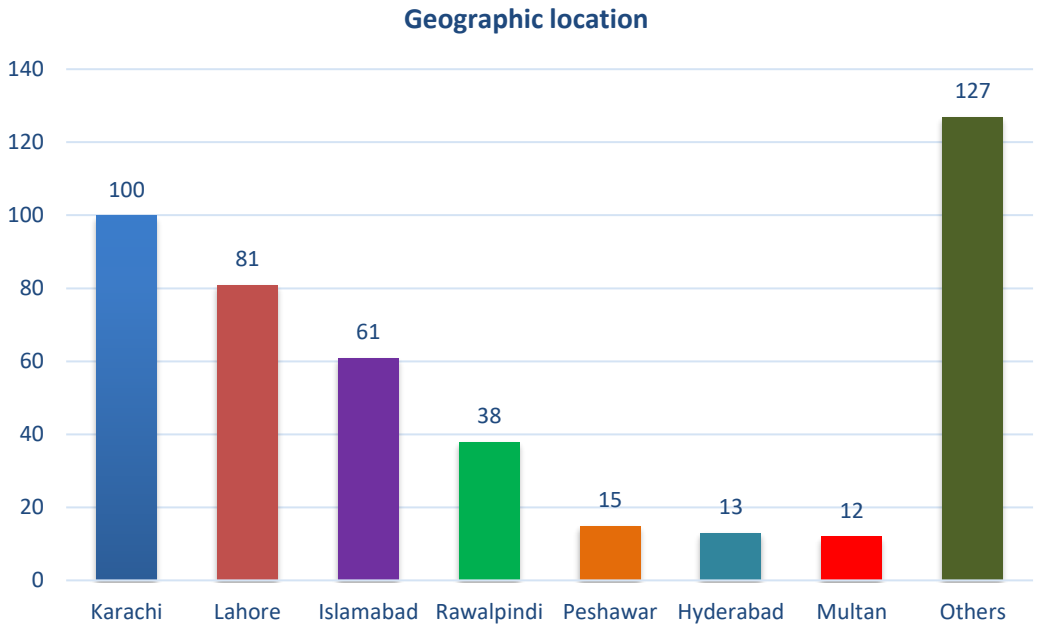
The breakup of customer type is given below:



More than 44 % individuals involved in sale/purchase of virtual assets are salaried or pensioners, followed by businessmen (23%) and 15 % individual belong to others category, which includes students, housewives and unemployed persons.

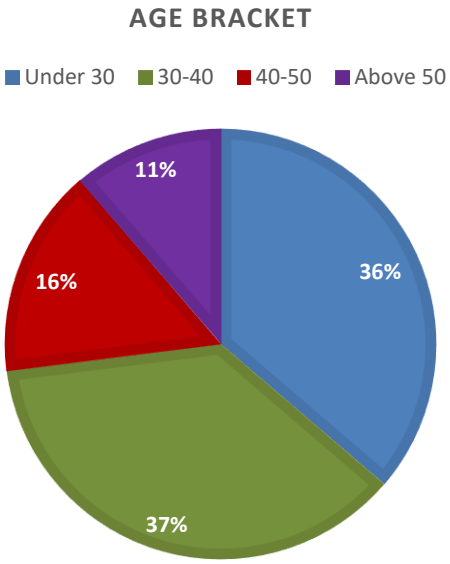
11.2. Geographic Analysis

The individuals are resident of different areas of Pakistan, however majority of them are from developed cities such as Karachi, Lahore, Islamabad, Rawalpindi, Peshawar etc. Below is the geographical segregation of individuals:



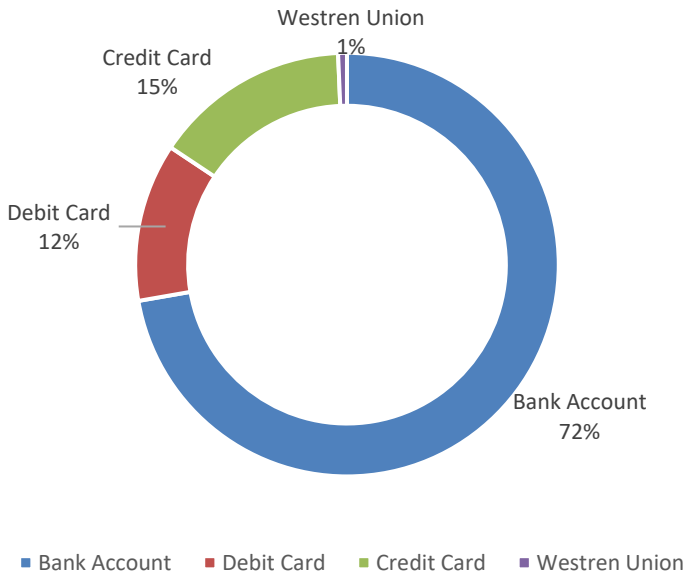
11.3. Demographic Analysis

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. Moreover, most of the individuals (73 %) belong to young or mid-age generation. The age brackets of individuals are given below:



11.4. Product Analysis

During the analysis of STRs it was found that the individuals were using their Bank Accounts, Debit Card, Credit Cards and Western Union facility to sale/purchase virtual assets from online Virtual Asset Service Providers (VASPs). The tendency of product type used is appended below:



11.5. 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 Branchless Banking such as Easypaisa, Omni accounts, western union 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.

11.6. Transactional Pattern

It has been found that these individuals are 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.

11.7. 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 Western Union. An overall suspicious activity of **PKR 701.9 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. The product wise breakdown of the funds involved in suspicious transactions is appended below:

Type of Product	Suspicious Amount	
	2020 (Jan-Dec)	2021 (Jan-June)
Bank Account	283,298,343	267,480,757
Credit card	67,310,016	27,698,303
Debit Card	24,198,644	31,522,061
Western Union	20,790	387,688
Total	**374,827,792**	**327,088,809**

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 sale/ purchase of virtual assets or settlements. Transaction nature wise summary of amounts is following:

Type of Product	Suspicious Amount	
	2020 (Jan-Dec)	2021 (Jan-June)
Purchase of Virtual Assets	120,618,453	105,295,982
Sale of Virtual Assets	27,725,622	74,240,369
P2P transactions	226,483,716	147,552,458
Total	**374,827,792**	**327,088,809**

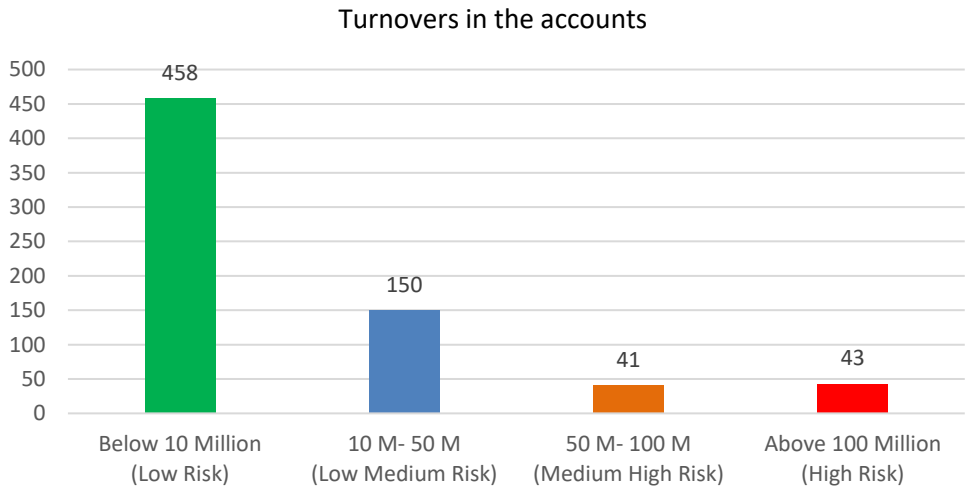
11.7.2. Rejected Financial services

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
2020 (Jan-Dec)	86	8,412,957
2021 (Jan-June)	78	7,688,398
Total	**164**	**16,101,355**

11.7.3. Level of transactional activity in the accounts

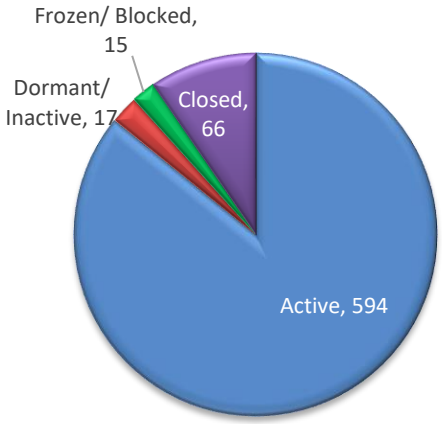
The individuals involved in virtual assets transactions were maintaining individual accounts or business accounts. The major transactional activity for sale/purchase/P2P transactions of virtual assets was carried through their bank accounts. In this regard, 692 bank accounts were identified, wherein it was observed that transactions in small amounts were continuously conducted with high frequency. An aggregate turnover of PKR 25.0 billion was noticed in these accounts with an average turnover of PKR 38.6 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 85% of accounts are active, while others are either closed, inoperative or frozen by the banks.

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

The individuals are using multiple online channels for trading of virtual currencies. Below are some major channels identified through STRs:

www.skrill.com	www.etoro.com	www.binance.com
www.icmarkets.com	www.b4uglobal.com	www.octafx.com
www.localbitcoins.com	www.iqoptions.com	www.coinmama.com
www.neteller.com	www.finq.com	www.axi.com

13. Criminal Offence linked with Virtual asset transactions

During the analysis of STRs, some of the individuals were suspected to be involved 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. 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. In this regard, following predicate offences are suspected to be linked with the Virtual Assets:

13.1. Hawala/ Hundi

The transactions of virtual asset trading have similarities with the transactional pattern of Hawala/ Hundi dealer. It might not be wrong if it is said 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 (Hawala/ Hundi and Virtual Assets)

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 do not commensurate with the stated profile and he is transacting with unrelated counterparties. 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 noticed. Based on the available information, it was suspected that the individual is 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 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.

13.2. 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. Further, a case has been reported in United States where Daesh associates used virtual assets for terrorism financing in relation to Pakistan. 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)

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. 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. 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.

13.3. 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 (Drug Trafficking and Virtual Assets)

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. 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. 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.

13.4. Ponzi Schemes

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. However, the funds were actually being used to purchase virtual assets.

Case Study (Ponzi Schemes and Virtual Assets)

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. 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. Most of the funds were credited through online cash and debited through inward clearing, pay orders and cash. 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 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.

13.5. 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)

An STR was filed on Mr. MAK on the basis of adverse media news. 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" and was involved in hiring of women for part time online marketing jobs. After hiring, one of the female workers was forced to do illegal activities who lodged the complaint in FIA. Reportedly, FIA revealed that the App was owned by a female Ms. RAM and Mr. FAQ 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.

Mr. MAK was one of the members of group arrested by FIA. Reportedly, Mr. MAK visited Chishtian branch of ABC Bank in October 2020 to receive funds amounting to Rs.11,929 sent to him from Saudi Arabia through Western Union. Upon inquiry by the bank, Mr. MAK 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. MAK has collected Rs.20,790 earlier on August 7, 2020 sent by the same remitter from Saudi Arabia through Western Union. 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.

13.6. Fraud and Forgery

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.

Case Study (Fraud/Forgery and Virtual Assets)

STR was reported on Mr. AA, who was owner of a computer shop and was maintaining personal account at ABC Bank, Mardan Branch. The ABC Bank received a complaint from XYZ Bank against Mr. AA. According to the complainant's account was hacked and funds amounting to PKR 120,000/- were debited from the account through internet banking. These funds were credited to the account of Mr. AA. Upon inquiry, the individual stated that these funds were the sale proceeds of Bitcoins (Virtual Assets). The bank officials visited the business place of individual, but he has windup the business and not in contact with the bank. The account of individual has been blocked by the bank due to involvement in fraudulent activity.

Based on the analysis of STRs reported to FMU and the above typology, there is sufficient ground to suspect that virtual assets are being used to fraud and cheat general public.

13.7. 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 explains the use of virtual assets for tax evasion purpose.

Case Study (Tax Evasion and Virtual Assets)

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.

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. The financial intelligence was shared with the relevant authority to probe the matters related to taxes.

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

- The Virtual asset dealers utilize their bank accounts, credit cards, debit cards, Branchless banking facilities and western union/ money gram services 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 and youngsters belong to IT profession/ 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.

15. 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.
- 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.
- There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns.
- It is difficult for the financial institutions to identify the transactions related to the virtual asset on real time basis.
- The identification and verification of participants involved in virtual asset related transaction is limited.
- It 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
- Almost impossible to make trail of transactions during investigation process.
- The record of virtual asset related transactions is kept in distributed network, not easy to access for investigation purpose.

16. 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. 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).

17. Suggestions for regulating Virtual asset Service Providers in Pakistan

Many exchange platforms available online who provide the services of buying and selling virtual assets. These exchanges accept payment via bank transfer, credit card/ debit card, mobile banking, internet banking etc. Moreover, as learnt from the above analysis that many Pakistan nationals are engaged in virtual assets as service provider or user. The scope and use of virtual assets is increasing in Pakistan. Therefore, there is need for regulatory framework for virtual asset service providers (VASPs) in order to comply the FATF requirements and matching the international standards.

As evident from the above that many developed countries have setup laws and regulations for governing the Virtual Asset Service Providers as exchanger/ payment system or commodity/ security. In light of above, following are some suggestions for developing a regulatory framework for the virtual asset dealers:

- The Virtual Assets are not considered as legal tender in Pakistan, as per SBP circular. Most of the countries are also following the same stance in regard. However, these countries have issued regulations for the Virtual asset Service Provider (VASPs) as exchanger, payment system or commodity traders. Therefore, the distinction needs to be made on virtual assets in Pakistan, whether to treat them as payment system, exchangers or brokers.
- Based on the above distinction, the role of the regulator for Virtual Asset Service provider may be assigned to State Bank of Pakistan (SBP) or Securities Exchange Commission of Pakistan (SECP).
- As per FATF, countries should designate one or more authorities that have responsibility for licensing and/or registering VASPs. In this regard, SBP or SECP may license the Virtual assets service providers.
- AML/CFT requirement should be applied on the Virtual Asset Service Providers (VASPs), in which the exchanger must be required to obtain verified identification for opening a Wallet or account. Further, the VASPs should perform other KYC/CDD requirements, Record preservation and provision of record requirements.
- The anonymous virtual asset exchanger and wallets should be banned and virtual asset transactions should be made taxable depending on the type of activity.

18. Recommendations

- A committee should be formed at national level to develop legal/regulatory framework to govern the virtual assets.
- A regulatory body for virtual assets must be established for implementation of AML/CFT regulations and risk assessment.
- The financial institutions must carry out risk assessment of virtual assets to curtail the inherent risk posed by the virtual assets.
- The regulators should increase awareness and provide guidance on common deficiencies across the financial sector.
- There is need of capacity building initiatives on abuse of virtual assets.
- The stakeholders are required to apply international best practices to mitigate the risks associated with the virtual assets.
- Need to develop a flexible regulatory framework in response to FATF requirements and emerging risk of money laundering and terrorism financing associated with virtual assets.
- There is need for optimizing the sharing of information and coordination between domestic and international stakeholders.
- There is need 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.
- Virtual Asset transactions should be made taxable depending on the type of activity.

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 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. 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, it is suggested that strategic Analysis may be shared with SBP, SECP and FIA under AMLA-2010 for appropriate measures/ controls on emergent use of bank accounts/ products/ services for trading of virtual assets such as Bitcoins. Further, it is suggested that the red flag indicators/ information of the transactional activity conducted through the banking products should be shared

with the banks in a sanitize manner, so that the banks be able to identify such instances and protect their banks from risks posed by trader of virtual assets.

20. Source of external information

- *Pakistan National Risk Assessment on Money Laundering and terrorism financing updated 2019*
- *Pakistan National Terrorist Financing Risk Assessment, 2018*
- *http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf*
- www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html
- *http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf*
- *https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105207/lbna28386enn.pdf* *Overview and analysis of the concept and application of virtual currencies by Joint Research Centre, European Commission.*
- *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*