



STRATEGIC ANALYSIS

Virtual Assets– Emerging risk of Money laundering and Terrorism financing

**Financial Monitoring Unit
Government of Pakistan**



Financial Monitoring Unit
Government 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 conduct two types of Analysis i.e. Tactical Analysis and strategic Analysis of STRs/CTRs. The purpose of strategic analysis is to identify potential ML/TF threats 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 year 2019. 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.

The ultimate purpose of the study is to assist the financial sector, regulators, law enforcement agencies and other stakeholders to develop legal/regulatory framework to govern the virtual assets.

021-99095034



info@fmu.gov.pk



<http://www.fmu.gov.pk>



2nd Floor, SBP Main Building, Karachi



Table of Contents

| | |
|--|----|
| 1. Understanding Virtual Assets..... | 1 |
| 1.1. Difference between Virtual Assets and E-money | 1 |
| 1.2. The system of Virtual Assets | 1 |
| 1.3. Taxonomy of Virtual Assets | 2 |
| 1.4. The Transaction Cycle of Virtual Assets | 3 |
| 2. Risks Associated with Virtual Assets | 4 |
| 3. FATF requirements on Virtual Assets..... | 5 |
| 4. Pakistan’s NRA and TFRA finding on Virtual Assets | 6 |
| 5. Controls in Pakistan to combat risk of Virtual Assets | 6 |
| 6. Scope of Strategic Analysis | 6 |
| 7. Objectives of the Strategic Analysis..... | 6 |
| 8. Methodology..... | 7 |
| 9. Data Limitation..... | 7 |
| 10. Analysis of suspicious transaction reports on Virtual assets | 8 |
| 10.1. Customers Analysis | 8 |
| 10.2. Geographic Analysis | 9 |
| 10.3. Demographic Analysis..... | 10 |
| 10.4. Product Analysis..... | 11 |
| 10.5. Delivery Channels..... | 11 |
| 10.6. Transactional Pattern..... | 11 |
| 10.7. Level of Transactional activity..... | 12 |
| 10.8. Status of accounts and transactions | 13 |
| 10.9. Investigation of Law enforcement agency..... | 13 |
| 11. Major Virtual Asset Service Providers (VASPs) and Merchants | 14 |
| 12. Predicate Offence linked with Virtual asset transactions | 15 |
| 12.1. Hawala/ Hundi | 15 |
| Case Study 1 (Hawala/ Hundi and Virtual Assets)..... | 16 |
| 12.2. Terrorism Financing | 16 |
| Case Study 2 (Terrorism Financing and Virtual Assets)..... | 17 |

- Case Study 3 (Terrorism Financing and Virtual Assets)..... 17
- 12.3. Fraud and Forgery 17
 - Case Study 4 (Fraud/Forgery and Virtual Assets) 18
- 12.4. Tax Evasion..... 18
 - Case Study 5 (Tax Evasion and Virtual Assets) 18
- 12.5. Other Offences..... 19
- 13. Red Flag indicators to identify transactions related to Virtual Assets..... 19
- 14. Challenges in dealing with Virtual assets..... 19
- 15. Regulatory Framework for Virtual Asset Service Providers 20
- 16. Suggestions for regulating Virtual asset Service Providers in Pakistan 23
- 17. Recommendations 24
- 18. Conclusion..... 25
- 19. Sources of external information 25

Virtual Assets

The emerging risk of Money Laundering & Terrorism Financing

1. 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 authority, and fulfils the above functions only by agreement within the community of users of the virtual assets.

1.1. 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.

1.2. 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 asset 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 asset exchange for real currency, funds, or other forms of virtual asset for a commission. The exchangers accept a wide range of payments, such as cash, wires transfers, credit cards, and other virtual

assets. Individuals typically use exchangers to deposit and withdraw money from virtual asset 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 asset and uses it to purchase real or virtual goods or services or send transfers in a personal use. Users can obtain virtual asset in several ways. For example, they can (1) purchase virtual asset, using real money from an exchanger or directly from the administrator/Miner (2) engage in specific activities that earn virtual asset 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 assets.
6. **Wallet provider** is an entity that provides a virtual asset wallet for holding, storing and transferring bitcoins or other virtual assets. A wallet provider facilitates participation in a virtual asset system by allowing users, exchangers, and merchants to more easily conduct the virtual asset transactions. The wallet provider maintains the customer's virtual asset 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.

1.3. 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 |

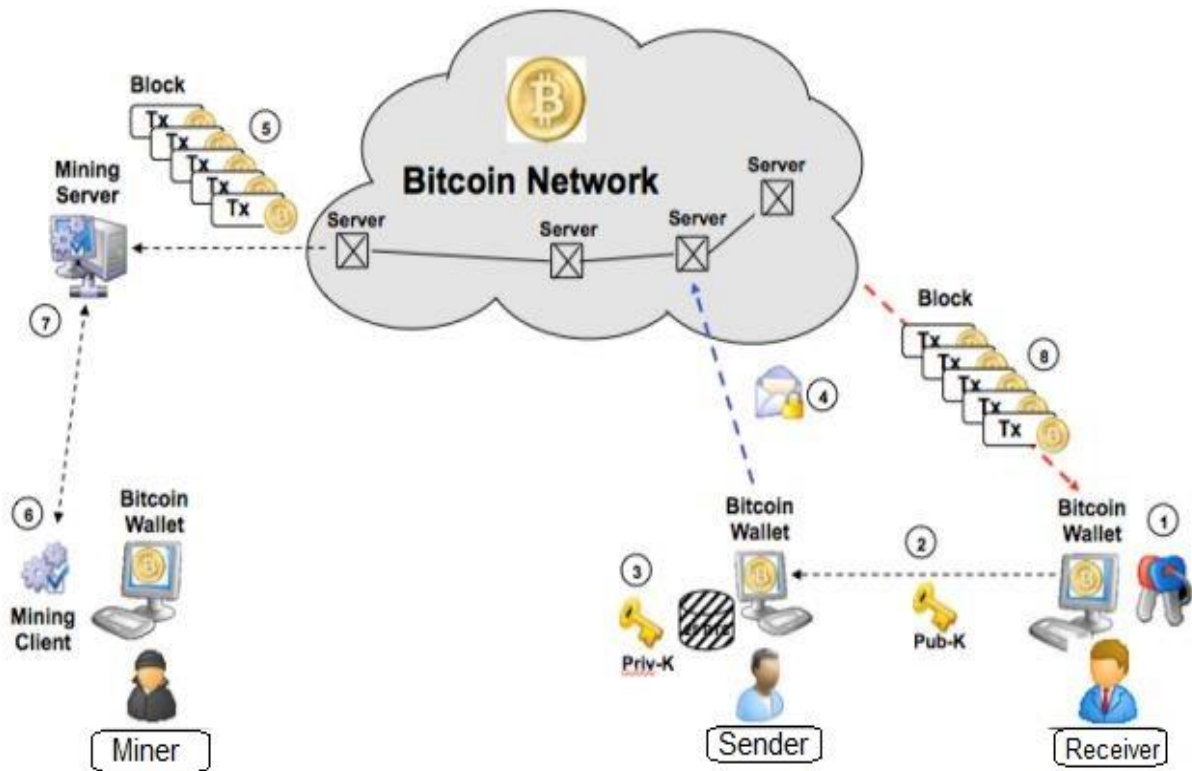
The decentralized virtual assets are particularly vulnerable to money laundering and terrorism financing abuse, due to easy convertibility and distributed architecture, which provides anonymous transfer of funds without passing through a central authority.

1.4. The Transaction Cycle of Virtual Assets

The transactions of virtual assets relies on public and private keys (provided through Virtual asset 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. Following is the transaction cycle to transfer virtual asset such as bitcoin from one person to another.

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 asset to be sent.
4. **Signature:** The sender will digitally sign the transaction with unique private key, 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.

2. Risks Associated with Virtual Assets

The potential AML/CFT risks 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.
- The transactions of virtual assets immediately executed and cannot be reversed.
- 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.
- It is difficult to make trail of transactions during investigation process.
- Virtual asset system 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 asset transactions may be conducted using dark net and commonly used in illegal trade commenced on dark web.
- There is risk of cheating and fraud in trading of virtual assets.

3. FATF requirements on Virtual Assets

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 measures for virtual assets.

4. 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 Assets' is considered to be “**High**” on overall basis. While no law currently governs the trade of virtual assets/ crypto currencies in Pakistan.

5. 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).

6. 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 assets and its abuse for money laundering and terrorism financing in December 2018.

7. Objectives of the Strategic Analysis

The purpose of Strategic Analysis is to understand the money laundering terrorism financing risk associated with the virtual assets and its transactions and define a way forward to mitigate these risk 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.

8. 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.

9. Data Limitation

The virtual assets are very complex in nature and there are variety of reports on the whole system of virtual assets and their transactions. The data obtained from some reports may vary from some other reports as there is lack of understanding as whole on virtual assets.

The analysis of data is based on suspicious transaction reports (STRs) filed to FMU during the year 2019, 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.

The study is based on financial sector of Pakistan, it might not be applied to the financial system of other countries which are different in nature.

10. 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. As per instructions of State Bank of Pakistan (SBP) the reporting entities are filling STRs on the transactions which involve the sale/purchase of virtual assets.

In this regard various STRs were reported by different banks on the basis of possible involvement of the individuals in trading of virtual assets through their bank accounts and other channels.

Below is the reporting entity wise breakdown of the STRs:

| Reporting Entity | No. of STRs |
|--|-------------|
| Askari Bank Limited | 33 |
| Habib Bank Limited | 26 |
| Standard Chartered Bank (Pakistan) Limited | 19 |
| Faysal Bank Limited | 8 |
| United Bank Limited | 8 |
| Allied Bank Limited | 7 |
| MCB Bank Ltd. | 6 |
| Bank Al Habib Limited | 4 |
| Bank Alfalah Limited | 4 |
| Meezan Bank Limited | 4 |
| Al Baraka Bank (Pakistan) Limited | 2 |
| Soneri Bank LIMITED | 2 |
| FINCA Microfinance Bank Limited | 1 |
| Government Agency | 1 |
| Total | 125 |

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

10.1. Customers Analysis

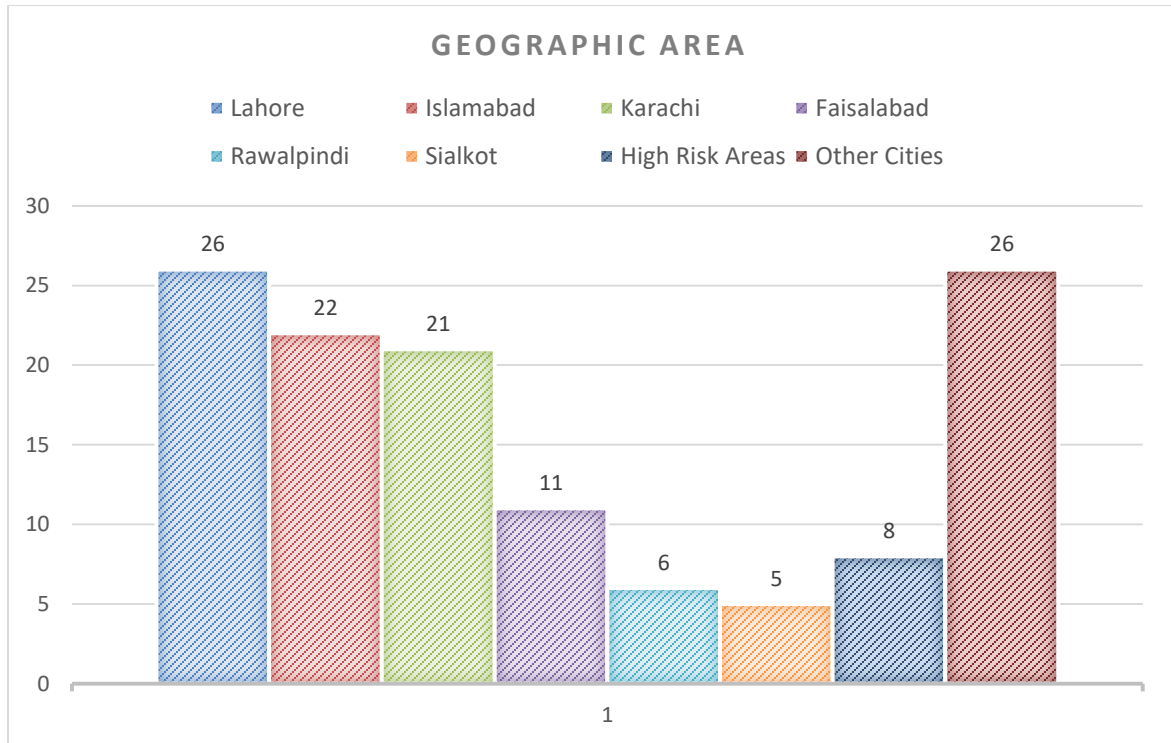
The type of customer involved in trading of virtual assets through banking channels are mostly salaried individuals, businessmen, Self-employed, students and service providers. Further, some other high risk customers such as housewives, unemployed individuals(source of income is Home remittances), real estate agents and travel agents were also found engaged in sale/purchase of virtual. The breakup of customer type is given below:



Further, most of the businessmen were the sole-proprietors engaged in business of trading, contracting, garments, mobiles and computers. While the Self-employed customers were identified as doctors, advocates, tailors, freelancer and online brokers. In addition, the service providers includes software developers, E-Commerce and communication service providers and services of Virtual asset trading.

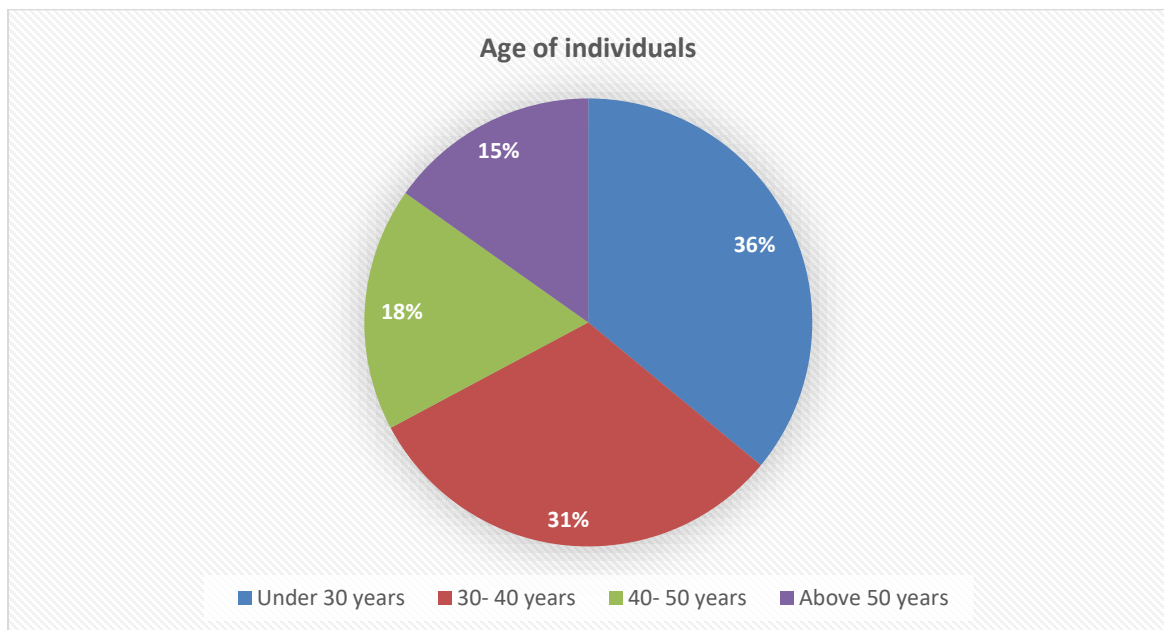
10.2. Geographic Analysis

The individuals are resident of different areas of Pakistan, however majority of them are from developed cities such as Lahore, Islamabad, Karachi, Faisalabad, Rawalpindi, Sialkot etc. Further, few instances were also reported from the domestic high risk geographies of Pakistan which includes Sargodha, Quetta, Peshawar, Jhang, Bhakkar, Attock and Bahawalpur. Below is the geographical segregation of individuals:



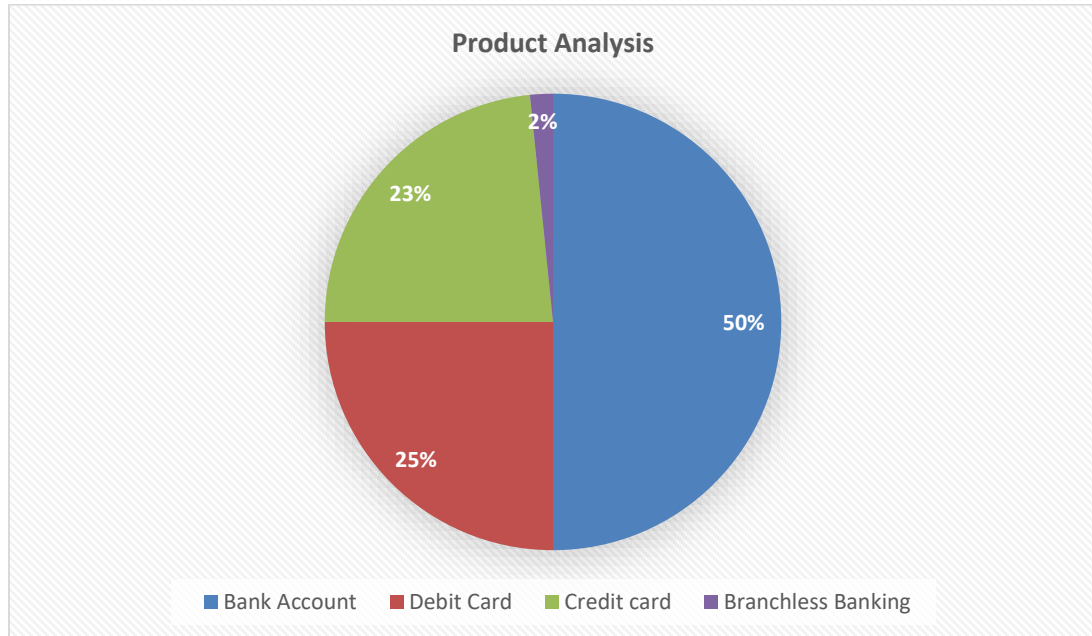
10.3. Demographic Analysis

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 (36 %) belong to young generation aging between 20 years to 30 years, 31 percent of individual fall in mid-age between ages 30 years to 40 years. The age brackets of individuals are given below:



10.4. Product Analysis

During the analysis of STRs it was found that the individuals were using their Bank Accounts, Debit Card, Credit Cards and Branchless Banking facility to sale/purchase virtual assets from online service providers. The tendency of product type use is appended below:



10.5. 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. It was noticed that they hardly use bank counters to perform their transactions.

10.6. 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

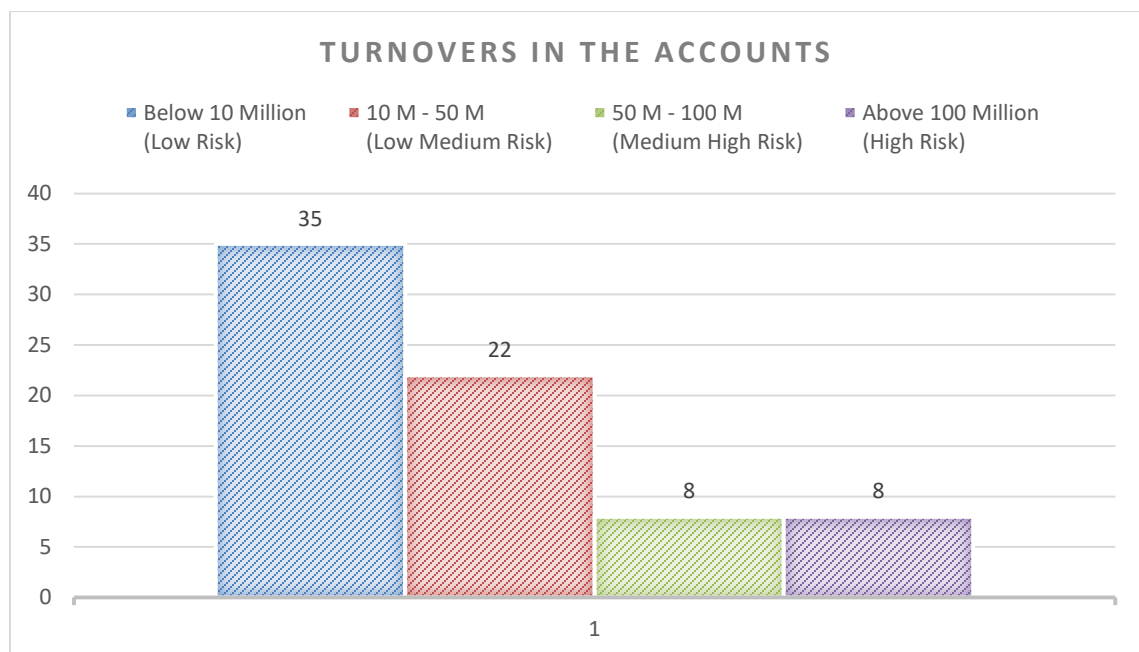
individuals have also conducted transactions with unrelated counterparties without any plausible purpose.

10.7. Level of Transactional activity

During the analysis of STRs, a significant level of transactional activity was observed in the bank accounts, branchless banking accounts, credit cards and debit cards. An overall suspicious activity of PKR 522.2 million was reported in suspicious transaction reports which were used to sale/purchase virtual assets during the year. The product wise breakdown of the funds involved in suspicious transactions is appended below:

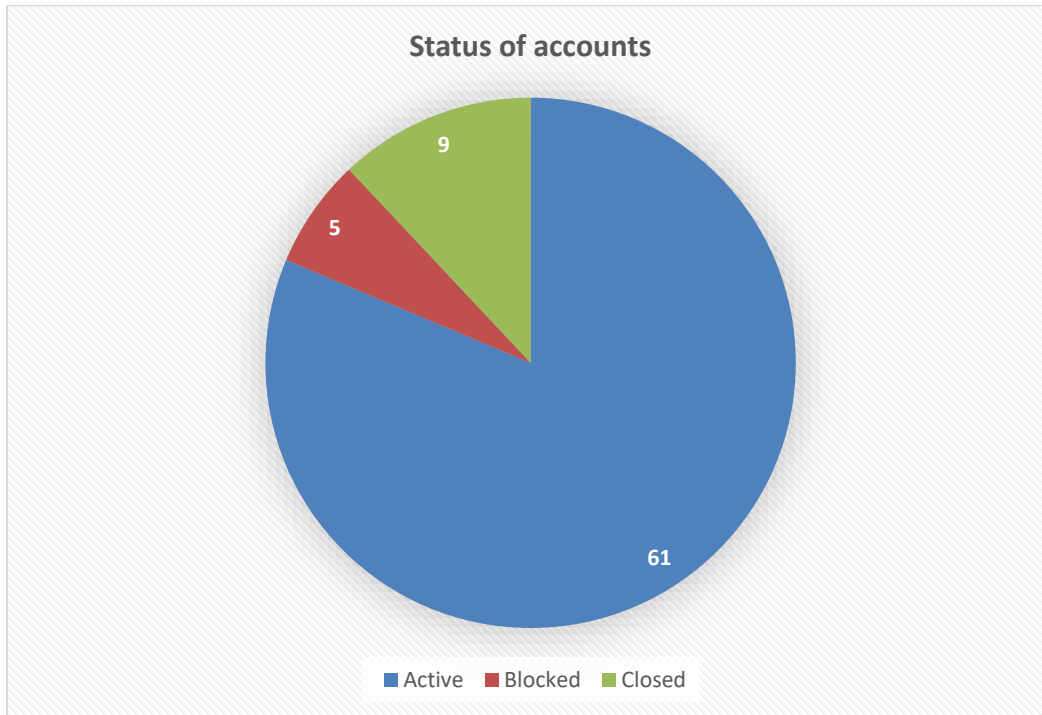
| Type of Product | Suspicious Amount |
|--------------------|--------------------|
| Bank Account | 489,884,188 |
| Credit card | 14,561,209 |
| Debit Card | 12,230,956 |
| Branchless Banking | 5,535,500 |
| Total | 522,211,853 |

The major transactional activity (PKR 489.88 million) has been observed in the 75 bank accounts, comprising of small but continuous transactions with high frequency. An aggregate turnover of PKR 2.8 billion was noticed in these account with an average turnover of PKR 37.3 million, which shows an increasing trend in sale/purchase of virtual assets as compared to previous year, whereby an average turnover of PKR 13 million was recorded in the accounts. Below is the segregation of accounts based on the aggregate turnovers;



10.8. Status of accounts and transactions

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



Further, some of the reporting entities have also successfully identified virtual assets related transactions and rejected them, as per instructions of SBP. In this regard, 37 virtual asset related transactions were declined. However, most of the time the transactions were executed.

10.9. Investigation of Law enforcement agency

During the analysis, it was found that some of the individuals are under investigation for trading in virtual assets. These individuals were identified in previous disseminations which were shared by FMU with the Federal investigation agency.

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

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

Domestic Platforms:

- www.Pay2Bey.com
- www.luckyorbit.com
- www.pakexchange.com
- www.easykamao.com
- www.e4earning.com
- www.a-cointechnologies.com/
- www.khalidxpert.alpcoin.com/
- www.paymentmedium.com/
- www.octafx.com/deposit/
- www.payexchanger.com
- www.pakearning.com
- www.pakexchange.pk
- www.bitcoindeals.info
- www.blockchaintech.com.pk
- www.blockchainsolutions1.com

International Platforms:

- www.localbitcoins.com
- www.iqoptions.com
- www.etoro.com
- www.coinmama.com
- www.instaforex.com
- www.cex.io
- www.mexbitcoin.com
- www.coinbase.com
- www.trade.com
- www.bitcoins.com
- www.fxpro.com
- www.plaster.co
- www.neteller.com
- www.axitrader.com
- www.fxpro.com
- www.cmcmarkets.com
- www.playtika.com
- www.mtlotcrypto.com
- www.eCollect.com.au
- www.coindirect.com
- www.bitsale.com
- www.bitlish.com
- www.24Option.com
- www.finq.com
- www.skrill.com
- www.moneypolo.com
- www.buysomebitcoins.com

- www.robokassa.ru
- www.donate24.io
- www.exness.com
- XmGlobal Nicosia
- N.exchange
- Hamilton Place London GBR
- Travelex UK Ltd Hounslow GBR
- International Capital Market PTY limited, Australia
- HF Markets SV LTD, Kingston
- Moneycorp CFX Ltd
- india@micous.com

12. Predicate Offence linked with Virtual asset transactions

During the analysis of STRs, some of the individuals were suspected to be involved in illegal activities such as Hawala/ Hundi, Fraud and Forgery, Smuggling and Illegal trade, Tax evasion through unauthorized capital flight or concealment of real beneficiaries. It has been learnt 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:

12.1. Hawala/ Hundi

The transactions of virtual asset trading have similarities with the transactional pattern of Hawala/ Hundi dealer. It might not be wrong if we say that virtual assets are the modern shape of Hawala, if it's not 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/ 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 is suspected that the individual is involved in Hawala and using the virtual assets for transacting the funds. Moreover, the risk of smuggling and/or terrorism cannot be discounted due to bordering area, which is known of 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.

12.2. Terrorism Financing

According to the National Terrorism Risk Assessment 2018 the TF risk associated with 'Virtual Assets' is considered to be **"High"**. 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.

While analyzing the STRs, it was found that few individuals (8 in numbers) who were dealing in virtual assets belonged to the high risk domestic geographies in terms of terrorism financing such as Quetta, Jhang, Sargodha, Peshawar, Attock, Bhakkar etc. Further, it was also observed that few of the individuals were transacting with individuals based in high risk geographic areas located either in western border of Pakistan or terrorism affected cities. It is difficult assess if any terrorism financing related funds were involved in the reported transactions at this stage, however the element of terrorism financing cannot be discounted, especially when there is an evident connection of virtual assets with the Hawala/ Hundi.

Moreover, appended are some case studies on virtual asset trading, which carry risk of terrorism financing:

Case Study 2 (Terrorism Financing and Virtual Assets)

STR was reported on Mr. MN, who was maintaining account at ABC Bank, Shadbagh Branch, Lahore. As per account opening form Mr. MN is the student, financial dependent on his father. He is quite young in age having DOB 1994, however the transactional activity did not commensurate with the stated profile. An overall activity of PKR 10 million (approx.) was noticed in his account. Upon inquiry by the Bank, Mr. MN declared that he has become an agent of MICO Coins and is receiving payments on sale/purchase of them. MICO Coins is an India based Virtual Asset Service Provider having email address (india@micous.com).

Keeping in view, the age factor and the linkage with India based VASP, the risk of terrorism financing cannot be ruled out.

Case Study 3 (Terrorism Financing and Virtual Assets)

STR was reported on Mr. JK, who is resident of Nowshera and maintaining account at ABC Bank, Risalpur Branch. As per account opening form Mr. JK declared his source of income as Home Remittance. However, the transactional activity revealed that he was receiving funds through branchless banking channel from several mobile numbers. The bank is of the suspicion that Mr. JK is engaged in Virtual Asset transactions. The modus operandi of the business is to seek crowd funding through internet based platform for onward investment in Cryptocurrency. During web searching by the Bank, a web page was found (<https://easykamao.com/?a=home>), whereby the address of Baluchistan was mentioned along with contact number and email address for making contacting with company.

Keeping in view the factor that an individual resident of Nowshera, maintaining account at Risalpur is engaged in virtual assets transactions, which has linkage with Baluchistan, the risk of terrorism financing cannot be ruled out.

12.3. Fraud and Forgery

The Financial Monitoring Unit (FMU) has received a number of STRs, whereby individuals received some funds (ranging from 50 K to 200K) in his account through IBFTs. But soon after the receiver's bank received complaint from the sender's bank that these funds were transferred through fraudulent activity. Upon inquiry by the receiver of funds, the individuals disclosed that they have received these funds against sale of Virtual assets.

Further, below case study is an example of fraud and forgery by the virtual asset trader:

Case Study 4 (Fraud/Forgery and Virtual Assets)

STR was reported on Mr. RU, who is sole proprietor of an e-commerce-web services Provider Company operated from his home. Mr. RU is resident of Lahore and maintaining multiple business and personal accounts at different Banks in Lahore. He has disclosed different profiles to the banks. The transactional activity in his accounts revealed that he was receiving funds through IBFTs and internet banking from several unrelated counterparties like salaried persons, housewives, travel agents, brokers etc. Further, he was engaged in suspicious trading in forex on platform of Octa Fx Company. Moreover, Mr. RU was using Bank's logo without authority for marketing purposes and inviting interested parties to deposit money into this account for trading purposes.

The Bank is of the suspicion that the individual is involved in trading of virtual assets and actively pursuing others to trade in virtual assets.

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.

12.4. 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. (Please refer Annexure C for accounts with high turnovers). Further, due to anonymity and free flow of funds without any check provide the opportunity to the individuals 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 5 (Tax Evasion and Virtual Assets)

STR was 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 15 accounts, whereby an aggregate activity of PKR 1.4 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 named as "B4U Trades" having registered office in Kuala Lumpur, Malaysia. 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 not paid any income taxes despite of high level of transactional activity. Hence, it's suspected that the individual is involved in tax evasion or facilitating other to conceal true beneficiaries for avoiding applicable taxes.

12.5. Other Offences

In addition to above, some instances were observed wherein it was suspected that the use of virtual assets may facilitate the settlement of smuggling and/or illegal trade related transactions. Purportedly, a virtual asset dealer was also found involved in Multilevel Marketing- Ponzi Schemes.

13. 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 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 belongs to IT profession/ salaried individuals are mostly involved in such type of activities.
- The trading of virtual assets is common in big/ developed cities of Pakistan, however the circle is expanding to other high risk 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 fund in the accounts is very less.

14. 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.

15. 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. Some of the countries who have setup the regulatory framework are given below:

Japan: Japan was first country to enacted law on virtual assets with purpose to protect customers of virtual asset exchangers and combating money laundering/ terrorism financing risk. The Virtual Asset Service Providers (VASPs) are required to be registered with the Japan Financial Services Agency as exchangers and comply with AML/CFT regulations.

- Virtual Assets: Legal, treated as property
- Virtual Asset Service Providers: Legal, must register with the Financial Services Agency

Further, the National Tax Agency of Japan ruled that gains on cryptocurrencies should be categorized as 'miscellaneous income' and investors taxed at rates of 15%-55%.

South Korea: South Korea categorizes cryptocurrencies as digital assets and recognizes crypto exchanges as regulated financial businesses. The regulatory framework require cryptocurrency exchanges to register with the Financial Services Commission (FSC) and comply with strict Know-Your-Customer (KYC) rules, Anti-Money Laundering (AML) regulations, as well as customer verification policies.

- Virtual Assets: Not legal tender
- Virtual Asset Service Providers: Legal, must register with FSC

Australia: The Virtual Asset Exchanger operating in Australia require mandatory registration, reporting and compliance obligations under the AML/CTF Act; and potential requirements to obtain and maintain a license to offer a financial service or financial market under the Corporations Act.

- Virtual Assets: Legal, treated as property
- Virtual Asset Service Providers: Legal, must register with AUSTRAC

Canada: Canada amended its AML/CFT legislation to treat persons and entities engaged in the business of dealing in Virtual Assets as money services businesses (MSBs) under the PCMLTFA and therefore subject to similar customer due diligence, recordkeeping, monitoring and reporting requirements as other reporting entities.

- Virtual Assets: Not legal tender
- Virtual Asset Service Providers: Legal, required to register with FinTRAC after June 1, 2020

China: The People's Bank of China, issued the Notice on Preventing Risks of Bitcoin, which required Virtual Asset Service providers including bitcoin registration, bitcoin wallet and bitcoin exchanging to fulfill AML/CFT obligations and take measures to identify its customers and record identification information.

United States: The USA regulates VASPs as money transmitters, subject to AML/CFT obligations, including registration, customer identification, record-keeping and reporting requirements.

- Virtual Assets: Not considered legal tender
- Virtual Asset Service Providers: Legal

United Kingdom: The UK allows some virtual assets to be traded based on the characteristics of virtual assets and has developed regulatory framework for them. However, it has banned some type of virtual assets, which are highly crypt in nature.

- Virtual Assets: Not legal tender but some of them may be traded online
- Virtual Asset Service Providers: Legal, registration requirements with FCA

France: The French Prudential Supervisory and Resolution Authority (ACPR) issued a position statement for regulating the Virtual asset exchanger as financial intermediary who receives funds on a third party's behalf and are therefore subject to AML/CFT requirements.

- Virtual Assets: Not legal tender
- Virtual Asset Service Providers: Legal, required to register

Germany: The German Federal Supervisory Authority (BaFin) qualifies Bitcoin with legally binding effect as financial instruments in the form of units of account in accordance with provisions of the German Banking Act (KWG).

- Virtual Assets: Not legal tender
- Virtual Asset Service Providers: Legal, required to register

Italy: Virtual Asset Service Provider in Italy are required to be listed in a special section of the register held by “Organismo degli Agenti e dei Mediatori” (OAM). VASPs are considered obliged entities and are subject to the full set of AML/CFT measures.

- Virtual Assets: Not legal tender
- Virtual Asset Service Providers: Legal, required to register

Switzerland: Entities engaged in Virtual Assets are required to get license from FINMA to operate as a directly supervised financial intermediary (DSFI) and comply with the obligation to verify the identity of the contracting party and establish the identity of the beneficial owner.

- Virtual Assets: Legal, accepted as payment in some contexts
- Virtual Asset Service Providers: Legal, regulated by SFTA

Sweden: The Financial Supervisory Authority of Sweden has considered virtual assets as means of payment, therefore VASPs are subject to a licensing regime and AML/CFT supervision.

Finland: VASPs are required to register (authorization) with the Finnish Financial Supervisory Authority (FINFSA) in Finland.

Hong Kong: The Hong Kong Securities and Futures Commission (SFC) has established regulatory framework for virtual asset trading platform operators. They have issued new licensing requirements for portfolio managers and imposed new requirements on fund distributors engaged in virtual asset activities.

Malaysia: The Securities Commission Malaysia has set out the regulatory framework for virtual assets. All token offerings in Malaysia are carried out only through platforms approved by the commission. The securities Commission Malaysia registers Initial Exchange Offerings (IEOs) and prohibited Initial Coin Offerings (ICOs) for conducting virtual assets sales.

Indonesia: Bank Indonesia states that bitcoin and other virtual assets are not currency or legal payment instrument in Indonesia. However, these type of assets may be traded as commodity.

Some of the countries like Argentina, India, Brazil, Bolivia, Colombia, Ecuador, Barbados, Jamaica, Austria, Belgium, Cyprus, Denmark, Finland, Poland, Romania, Georgia, Iceland, Kosovo, Macedonia, Moldova, Norway, Ukraine, Bahrain, Egypt, Iran, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, UAE, Kenya, Zimbabwe, Tajikistan, Bangladesh, Nepal etc. 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).

16. Suggestions for regulating Virtual asset Service Providers in Pakistan

A large number of exchanger 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, the have 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, a 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 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.

17. 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 virtual assets abuse.
- 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.
- Establishing best practices in implementation of preventive measures for 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.

18. Conclusion

Keeping in view the above analysis, it is evident that the Virtual Assets poses 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, the strategic Analysis is being shared with SBP 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, the red flag indicators/ information of the transactional activity conducted through the banking products is being shared with the banks in a sanitize manner, so that the banks be able to identify such instances and protect their institutions from risks posed by traders of virtual assets.

19. Sources 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>
- <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.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>
Overview and analysis of the concept and application of virtual currencies by Joint Research Centre, European Commission.
- <https://www.loc.gov/law/help/cryptocurrency/world-survey.php>