Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering

Salman Ali Ibrahim[*]

Abstract

The emergence of cryptocurrencies has opened a new avenue for terrorist outfits and crime sydnicates to carry out their illegitimate monetary transactions. The ever-increasing use of cyrptocurrencies for terror financing, drug dealings, human trafficking and corruption has forced lawmakers around the world to undertake action to regulate the sale, purchase and exchange mechanisms of cryptocurrencies. While some countries like China have imposed an outright ban on cryptocurrencies, several other countries have embraced the potentials of cryptocurrency through mainstreaming and applying reasonable regulations. Amidst international efforts to regulate and harness the potential of cryptocurrency, Pakistan has imposed a ban on virtual assets and tokens. The rationale behind banning cryptocurrency is the number of challenges that the country will have to encounter in the form of tax evasion, transnational crimes, terrorism financing, cybercrimes, corruption, and kidnapping for ransom. While the current approach of Pakistan is very much in line with China, Pakistani policymakers need to take a hybrid approach of regulation for its economic and regulatory environment. Caution is necessary instead of taking a hasty decision and pursuance of long term planning for facilitating the introduction of cryptocurrencies in the country.

Keywords: Blockchain, Cryptocurrency, Terrorism, Money Laundering

[*] Salman Ali Ibrahim has done his MSc in Defence and Strategic Studies from Quaid-i-Azam University, Islamabad.

Introduction

The evolution and growing progression in technology have revolutionized methods, techniques, and tactics of warfare. This phenomenon also applies to strategies adopted by non-state entities and terror organisations for the advancement of their illicit operations. From the use of social media for recruitment to communication by means of encrypted web protocols, this is terrorism of the new age where technology forms an integral part of terror operations. Illegitimate monetary transactions and money laundering have always been a challenge for crime syndicates and terrorist organisations since the digitalisation of money and related controls made it relatively impossible to transact discreetly. However, the emergence of cryptocurrency has opened a new venture of Terrorism Financing (TF) and Money Laundering (ML) for the tech-savvy terrorist organisations such as ISIS, Al-Qaeda and other transnational criminal outfits.

Cryptocurrency is a form of virtual currency which has appeared as payment infrastructure built on software protocols.[1] This technology allows for anonymous transfer of funds globally as there is no centralised authority to monitor the transactions and distinguish the legitimate transfers from illicit dealings. While the initial acquisition of the currency may be traceable (e.g. through the banking system), all following transactions of the currency are difficult to detect for law enforcement agencies and regulatory authorities.

There was a time when paper currency was the only effective mode of payment for illicit purposes because of anonymity and discreetness of the nature of the transaction. However, physical currency does not provide real-time global transaction like virtual currencies. The digital mode of payment has not been effective for illicit actors in executing international transactions as it leaves a money trail to be traced subsequently. Cryptocurrency provides anonymity and swiftness, which may enable these elements to smooth their logistics and financial transactions. Furthermore, this new form of money can also be an easy way for terrorists to inconspicuously generate profits. Cryptocurrency does not have government backing, on the contrary to fiat currencies, which are currencies issued by a particular jurisdiction to be used as a legal tender.

Over the period of time, there has been continuous innovation in the field of cryptocurrency and new math-based currencies have emerged which are termed as alternative coins or Altcoins. These altcoins include Omni Layer (MasterCoin), BlackCoin, and Monero, which are considered as relatively

[1] *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (Paris: FATF, 2014).

more unobtrusive and protected than Bitcoin.[2] In addition, Zcash provides greater discreetness for example through services such as the ability to operate transactions while offline, which would make it highly challenging for state authorities to trace illegitimate transactions. There are more similar variants of cryptocurrency being proposed which would be inconspicuous and offer options of private contracts.[3]

This new wave of terror-financing through cryptocurrency is raising alarms worldwide. Recently, a US citizen of Pakistani-origin Zoobia Shahnaz, pleaded guilty in the US on the charges of financing and supporting ISIS by laundering over US Dollars 85,000 in Bitcoin.[4] Some militant outfits have even raised appeals for funding through cryptocurrency. Ibn Taymiyyah Media Centre, a Gaza based pro-ISIS propaganda arm of the terrorist group called their global supporters to use the medium to transfer their donations.[5] Similarly, the Palestinian militant group, Hamas has also resorted to cryptocurrency for collecting donations.[6]

In the presence of proliferation threat of chemical, biological, radiological, and nuclear (CBRN) materials, the use of cryptocurrency for a transaction of such components cannot be ignored. In contemporary times, most illicit transactions by global terrorists and criminals are being noticed on the dark web. Cryptocurrency is one mode of payment which eventually complements such businesses. Dark web or dark net is a network of encrypted websites and is accessible only by using a complex set of security tools. The threat becomes more severe due to implied complexity and impossibility to track transfers on the dark net.[7]

The transnational criminal syndicates previously relied on the *hawala* system as a method to carry out international financial transactions because of its suitability for illicit dealings. However, cryptocurrencies have provided them a more viable option as a replacement for *hawala* and *hundi* mechanisms. There have been reliable indications that cryptocurrencies are being used to execute dealings related to human trafficking, drug dealings, and corruption. According to the 2015 Europol

---

[2] Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, (Santa Monica: RAND Corporation, 2019)

[3] Ibid.

[4] Dan Mangan, "Woman pleads guilty to using bitcoin to launder money for terror group ISIS," *CNBC,* last modified November 26, 2018, https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html.

[5] David Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic", *Royal United Services Institute*, last modfied March 2, 2017, https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic.

[6] "Hamas calls for supporters to send bitcoins", *Al Jazeera*, last modfied January 30, 2019, https://www.aljazeera.com/news/2019/01/hamas-calls-supporters-send-bitcoins-190130065239528.html.

[7] Dan Patterson, "How the Dark Web works", *ZDNET,* last modified September 1, 2016, https://www.zdnet.com/article/how-the-dark-web-works/.

report, cryptocurrency has been used in more than 40 per cent of identified criminal transactions in Europe.[8]

On the basis of these risks, the world is taking initiatives to properly regulate the sale, purchase and exchange mechanisms of cryptocurrencies to curb the chances of its illegal use. Although, there has been a little empirical evidence of cryptocurrencies' application for money laundering or terror-financing in Pakistan, the associated risks are too immense to be ignored. Terrorism Financing and money laundering have already been matters of national security for Pakistan therefore, it is necessary to assess the emerging threats and challenges to Pakistan's Anti-Money Laundering/Combatting the Financing of Terrorism (AML/CFT) regime. This research explores the approaches being adopted globally to mitigate the risk of misuse of cryptocurrencies as well as the rationale behind Pakistan's outright ban on all kinds of virtual assets and currencies. The study also focuses on the challenges that have emerged in Pakistan's economic, social and security environment because of cryptocurrencies.

Regulating Cryptocurrencies to Prevent Money Laundering and Terrorism Financing

The regulators have been finding difficulty in embracing this unprecedented currency system with skepticism due to its distinct nature from the prevailing financial regime. The risks of money laundering and terrorism financing along with high possibility of tax evasion has created a dire need for legislation in this respect.

The most immediate protective measure at the governmental level in most of the countries was to notify the public regarding the risks associated with the investments in cryptocurrencies. Such cautions were mainly issued by the central banks to inform the public about the difference between currencies accepted as legal tenders and digital currencies.[9] The warnings also include cryptocurrencies' vulnerabilities toward facilitation of criminal activities.

Countries have responded differently to cryptocurrencies; some jurisdictions have adopted a stricter regulatory approach by imposing an outright ban on cryptocurrency and other virtual assets, while a few have decided to embrace the potentials of this form of currency through mainstreaming and applying reasonable regulations with regards to its trading.

Those jurisdictions which are regulating cryptocurrencies instead of an absolute ban have mostly focused on exchanges that deal in cryptocurrencies. These exchanges allow the customers to exchange

[8] *The Internet Organised Crime Threat Assessment* (Hague: Europol, 2015).
[9] *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, (UNODC, 2014), 55.

their fiat currency into cryptocurrency and vice versa. By adhering to Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols, these exchanges may mitigate the challenges posed by cryptocurrencies' anonymity. Recently, countries such as Australia, Canada and the Isle of Man have passed anti-money laundering and combating financing of terrorism legislations to facilitate legitimate cryptocurrency transactions through exchanges and financial institutions.[10] So far, Venezuela is the first and only country to launch a state-backed cryptocurrency named Petro.[11]

The growing trend in cryptocurrency has led the countries and international AML regimes, such as the Finanancial Action Task Force (FATF), to adopt regulations which can address the risks of money laundering and terrorism financing. FATF has been proactively working with regards to money laundering and terrorism financing risks connected to cryptocurrencies. In October 2018, the FATF amended its recommendations to incorporate financial activities related to virtual assets including cryptocurrencies. The FATF altered its Recommendation 15 to clarify the application of FATF standards to financial activities which involves virtual assets.[12] In addition, the international watchdogs also added the terms Virtual Assets (VA) and Virtual Asset Service Providers (VASP) into its glossary.

Recommendation 15 which is regarding New Technologies explicitly states that:

> '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.'[13]

The aforementioned updated FATF recommendation requires countries to ensure that all those VASPs that are operating within the county are duly regulated, licensed or registered, and are subjected to proper monitory and supervisory controls with regards to AML/CFT risks.

Among the major economies of the world, China has taken the strictest stance with regards to cryptocurrencies or virtual assets. In 2013, People's Bank of China (PBOC) issued a joint notice with other state authorities which defined the nature of Bitcoin and categorized it as a virtual currency which

---

[10] *Regulation of Cryptocurrency around the World* (The Law Library of Congress, 2018).
[11] "What is Venezuela's new petro cryptocurrency?", *Al Jazeera*, last modified Mar 23, 2018, https://www.aljazeera.com/news/2018/02/venezuela-petro-cryptocurrency-180219065112440.html.
[12] *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, (Paris: FATF, 2018).
[13] Ibid.

does not have legal status like a fiat currency. The notification explicitly restricted Bitcoin's circulation in the market as a fiat currency.[14]

The PBOC issued another joint statement in September 2017, with six other regulatory authorities, which reiterated the previous circular by mentioning that Bitcoin does not have a status of a fiat currency.[15] This circular further put a restriction on Initial Coin Offerings (ICO) in China and expressed that all financial activities related to virtual currencies would be deemed as illegitimate. The statement also advised the general public regarding the risks of investing and financing in cryptocurrencies.

However, China has not turned a blind eye toward this financial technology, in fact, it has been investing in research and development at the state level with respect to cryptocurrencies. The PBOC has been working on the feasibility of a state-sanctioned cryptocurrency named Digital Currency for Electronic Payment (DCEP), since March 2018.[16] The PBOC also established an Institute of Digital Money within its supervision in the year 2014 for the research and development of cryptocurrency.[17]

Contrary to the Chinese suppressive regulatory stance, the federal government officials and agencies in the United States have appreciated cryptocurrencies and resolved to continue a leading role in the advancement of this emerging financial technology.[18] Furthermore, the blockchain based cryptocurrencies are being considered as central to the United States' future of the financial technological framework.

The Financial Crimes Enforcement Network (FinCEN), which is a bureau of the US Department of Treasury, entrusted to combat money laundering and terrorism financing, issued guidance in March 2013, according to which all those exchanges and businesses which deal in convertible virtual currencies will be treated as Money Service Businesses (MSBs).[19] FinCEN regulations necessitate MSBs to conduct a risk assessment with regards to money laundering and formulate anti-money laundering frameworks which address the ML risks accordingly. In addition, MSBs are obliged by the law to develop and

---

[14] Lefan Gong and Luping Yu, "China" in *Global Legal Insights: Blockchain & Cryptocurrency Regulation: 2019*, ed. Josias Dewey (London: Global Legal Group, 2019), 262.
[15] "PBOC, CAC, MIIT, SAIC, CBRC, CSRC, and CIRC Announcement on Preventing Financial Risks from Initial Coin Offerings," last modfied September 4, 2017, http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html.
[16] Global Legal Insights, "China", 262-267.
[17] "Zhou Xiaochuan: Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now", last modfied March 10, 2018, http://www.xinhuanet.com/finance/2018-03/10/c_129826604.htm.
[18] Josias Dewey, "USA" in *Global Legal Insights: Blockchain & Cryptocurrency Regulation: 2019*, (London: Global Legal Group, 2019), 479-486.
[19] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," last modfied March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

implement controls and procedures to avoid MSBs from being exploited for the facilitation of money laundering and terrorist financing activities.

The US has provided sufficient opportunities for the cryptocurrency sector without any over restrictive regulations at the federal level. The cryptocurrency business has been experiencing and exploring ways to integrate cryptocurrency technology into the global financial system with the help of the US government.[20] Besides all this, the US government has presented only one requirement for the crypto-businesses: to comply with AML/CFT requirements.

Pakistan has so far adopted an approach which is relatively similar to what China has adopted with regards to cryptocurrencies and virtual assets. But China has also been investing in research and development, and capacity building in the areas of cryptocurrencies and virtual assets which Pakistan is not considering at present.

It is pertinent that somehow in the near future virtual assets or cryptocurrencies will be integrated into the global financial structure. Pakistan may learn from US' regulatory mechanism, which is well in alignment with the FATF's AML/CFT requirements with regards to VASPs. It is in Pakistan's interests to adopt a hybrid approach of regulation which is appropriate for its economic and regulatory environment.

Pakistan's Approach toward Regulating Cryptocurrencies

At the time when the world was seeing potential in cryptocurrency technology and trying to embrace the revolution in financial technology by giving space to cryptocurrencies and assets, the State Bank of Pakistan (SBP) enforced an absolute ban on all forms of virtual tokens and assets. This move was questioned by the Fintech enthusiasts and was even perceived as a prehistoric regulation.

The abrupt ban led to the closure of cryptocurrency exchanges, taking place in Pakistan. The regulation was disappointing for the CEO of Urdubit,[21] Danyal Manzar as he stated after the issuance of SBPs circular, 'It is a sad day indeed. A truly innovative system has been blocked.'[22]

Jaleel, who was the participant of the University of Oxford's Blockchain Strategy Programme, was relatively optimistic regarding cryptocurrencies being allowed as a legal tender in Pakistan.[23] She

[20] Yaya Fanusie, "Stronger AML Enforcement Might Actually Save Crypto", last modfied May 29, 2019, https://www.forbes.com/sites/yayafanusie/2019/05/29/stronger-aml-enforcement-might-actually-save-crypto/#536349857e78.
[21] Urdubit was the first and only bitcoin exchange in Pakistan.
[22] Danyal Manzar (CEO Urdubit), in discussion with Usman Hanif, May 13, 2018. https://tribune.com.pk/story/1708782/2-pakistan-bans-cryptocurrencies-people-may-find-alternative-means/.

inferred that the government will allow the use of cryptocurrencies once the opportunities become more feasible than the 'initial regulatory concerns'.

However, if observed rationally, the SBP's move of banning the virtual assets and cryptocurrencies was logical. Pakistan is currently striving to avoid the possibility of being blacklisted by FATF due to gaps in its AML/CTF regimes with regards to conventional banking and financial operations. The emergence of such virtual assets in the financial markets of Pakistan, which provide anonymity to the transacting parties, would have further complicated Pakistan's position in front of FATF.

Zeeshan Shahid, Partner at Deloitte Pakistan, backed the SBP's decision by maintaining that the size of the undocumented economy in Pakistan is still unknown to the authorities. In such a situation, allowing the exchanges to facilitate cryptocurrencies would provide ample opportunities for the money launderers to park and move their illicitly acquired proceeds.[24] According to him, by criminalizing the dealings of virtual assets and currencies, the SBP has secured itself and Pakistan to a considerable extent from money laundering and terrorism financing risks associated with crypto dealings. This action has also enabled law enforcement agencies to prosecute any dealings in cryptocurrencies under applicable laws, whenever they acquire any actionable intelligence in this regard.[25]

Pakistan's Rationale of Ban on Cryptocurrency

Before issuance of SBP's BPRD circular no. 3 in April 2018, there was a lack of clarity regarding the status of cryptocurrencies. Nonetheless, institutions such as the Federal Investigation Agency (FIA) and Financial Monitoring Unit (FMU) were diligently dealing with the cases related to cryptocurrencies. Even so, these institutions felt the necessity to have a legal clarity with respect to the digital currencies.

In early 2017, the SBP issued a warning related to Ponzi schemes associated with digital currencies.[26] The skepticism was proven real when Italy based cryptocurrency OneCoin was proven as a scam and the promoters were fined Euros 2.6 million by the Italian Competition Authority (IAA).[27] Resultantly, FIA launched a crackdown against OneCoin and Bitcoin in Pakistan.

---

[23] Nahas A Jaleel (Participant Oxford Blockchain Strategy Programme), in discussion with Usman Hanif, *The Express Tribune*, last modified May 13, 2018, https://tribune.com.pk/story/1708782/2-pakistan-bans-cryptocurrencies-people-may-find-alternative-means/.
[24] Zeeshan Shahid (Partner, Forensics, Financial Institutions Risk Advisory, Deloitte Pakistan) in discussion with the author, June 13, 2019.
[25] Ibid.
[26] Talha Hameed, "FIA takes action against OneCoin and Bitcoin", *TechJuice*, last mdofied August 15, 2017, https://www.techjuice.pk/fia-takes-action-against-onecoin-and-bitcoin/, Accessed June 25, 2019.
[27] "Italy: Regulator fines OneCoin promoters €2.6 million", *Competition Policy Institute*, last modified August 15, 2017, https://www.competitionpolicyinternational.com/italy-regulator-fines-onecoin-promoters-e2-6-million/.

The anti-money laundering cell of the Federal Board of Revenue (FBR) also initiated an investigation in mid-2017, on the suspicion of cryptocurrency being used for tax evasion and money laundering purposes.[28] The board had also issued summons to the major bitcoin traders to investigate the financial matters of the persons having huge investments in cryptocurrencies.

In a report submitted to the National Assembly of Pakistan on the implementation of Prevention of Electronic Crimes Act (PECA) 2016 by FIA in January 2018, the agency asked the legislators to illegalize the Bitcoin.[29] The report also requested for the punishments to be mentioned for those dealing in cryptocurrency. The argument which was presented by the FIA was that the digital currencies are not accepted as a legal tender by the SBP, hence, their trading is causing enormous financial losses to the national exchequer.

As the trading volume of cryptocurrency in Pakistan increased the FMU started receiving multiple Suspicious Transaction Reports (STR) [30] from different commercial banks. These reports were based on the suspicion that the account holders are involved with cryptocurrencies which are deemed as high risk by the regulating authorities due to the anonymity of the transacting parties.[31] The transactional patterns of these account holders suggested that the funds were credited to the accounts through the modes which were feasible for transactions related to virtual currency dealings. In addition, these account holders were mostly of young age, tech-savvy, and a few of them were even students. When the information was corroborated with their social accounts, it was revealed that they were actively involved in the propagation of virtual currencies.[32]

These STRs hinted towards vulnerabilities that cryptocurrencies can be converted into real money with ease and therefore be conveniently used for tax evasion, money laundering and terrorism financing. These strategic analyses of FMU were communicated to the SBP for enforcement of appropriate actions with regards to the use of bank accounts for the purposes of cryptocurrencies.

Based on these recommendations, the SBP issued a Banking Policy and Regulations Department (BPRD) circular no. 3 of 2018 to intimate banking and financial institutions regarding the prohibition of

---

[28] Mubarak Zeb Khan, "FBR goes after bitcoin traders", *Dawn*, last modified May 25, 2017, https://www.dawn.com/news/1335184.
[29] "FIA submits 'half-yearly' report on electronic crimes after a one year delay; asks for 7 offences to be declared 'non-bailable' and a ban on 'Bitcoin'", *Digital Rights Monitor*, last modified January 16, 2018, https://digitalrightsmonitor.pk/fia-submits-half-yearly-report-on-electronic-crimes-after-a-one-year-delay-asks-for-7-offences-to-be-declared-non-bailable-and-a-ban-on-bitcoin/.
[30] Suspicious Transaction Report (STR) is a report made by a financial institution about suspicious or potentially suspicious activity.
[31] "Strategic Analysis: Virtual Currency", *Financial Monitoring Unit*, accessed June 14, 2019, http://www.fmu.gov.pk/virtual-currency/.
[32] Ibid.

dealing in virtual currencies/tokens.[33] Similarly, the SBP issued FE circular no. 3 of 2018 for exchange companies and also issued a caution for the general public regarding the risks of virtual currencies.[34] [35]

The SBP advice to the public was based on the following risks associated with virtual currencies: (a) High degree of anonymity of the VCs facilitates potential criminal activities; (b) High volatility of exchange value makes the currencies unstable as these are merely based on speculations; (c) Because of a decentralized nature, there is no recourse available in case of loss or any fraudulent transaction; (d) Fake and phony schemes of virtual currencies are being offered in a country which promises high profits to the public. Such Ponzi schemes eventually result in losses to the public; and (e) High risk of hacking of cryptocurrency exchanges and wallet service providers as a number of hacking incidents have occurred worldwide where users have lost significant amounts.

Challenges for Pakistan

Cryptocurrency is not merely a threat to Pakistan's financial system rather it can have a larger impact on its economic as well as physical security. The challenges related to cryptocurrencies in Pakistan range from tax evasion, transnational crimes, terrorism financing, cybercrimes, corruption, and kidnapping for ransom. In summary, cryptocurrency can be considered as an innovation in financial crimes of every kind.

Pakistan's economic security can be jeopardized in case any illegal cryptocurrency exchange operates in its jurisdiction without any AML/CFT protocols in place. Such a scenario will raise many red flags for international regimes, working to curb money laundering and terrorism financing globally. Consequently, they pose a serious challenge to Pakistan CFT capabilities and intent.

Pakistan has been at war against terrorism and its facilitators, curbing every conventional aspect of terror financing. It is possible for terrorists to use cryptocurrencies as a means to finance their nefarious activities within Pakistan. Therefore, a well-executed financial transaction through cryptocurrency for terrorism in Pakistan can put hundreds of civilian lives at stake.

In addition, cryptocurrencies can facilitate the corrupt elements in Pakistani society by providing an opportunity to transfer their wealth abroad without being detected by the authorities. The risks and

---

[33], "BPRD Circular No. 03 of 2018: Prohibition of Dealing in Virtual Currencies/Tokens," *State Bank of Pakistan*, last modified April 06, 2018, http://www.sbp.org.pk/bprd/2018/C3.htm.

[34] "FE Circular No. 03 of 2018: Prohibition of Dealing in Virtual Currencies/Tokens," *State Bank of Pakistan*, last modified April 18, 2018, http://www.sbp.org.pk/epd/2018/FEC3.htm.

[35] "Caution Regarding Risks of Virtual Currencies", *State Bank of Pakistan*, last modified April 6, 2018, http://www.sbp.org.pk/press/2018/Pr-VC-06-Apr-18.pdf.

challenges in Pakistan are extended to the application of cryptocurrencies in crimes related to cyber domains as well as crimes committed on the streets.

i. Economic Security

Pakistan is among those countries which are currently facing a tough time with FATF with regards to its AML/CFT regimes. All institutions related to financial regulation or financial crimes are striving to comply with the FATF requirements in order to avoid placement among blacklisted countries. Pakistan is already categorized by the FATF as a high-risk jurisdiction which has strategic AML/CFT deficiencies. The efforts of state institutions are also directed toward removing its name from FATF's greylist.[36]

In June 2018, Pakistan was officially placed in the FATF's grey list, and as a result, it was also included in the European Union's (EU) list of high-risk countries which poses a threat to EU's financial structure.[37] [38] Such listing has serious repercussions on Pakistan's businesses within and exports to other countries, The impact is also on international banking transactions to or from Pakistan as such transactions will be highly scrutinized to prevent the risks of money laundering and terrorism financing.[39]

The advent of cryptocurrencies has added a complication in this respect. If Pakistan allows trading of cryptocurrencies in its jurisdiction then it would be difficult to implement AML/CFT requirements in line with international requirements. The reasons are mainly the absence of adequate laws and also that Pakistan's regulatory authorities would need to acquire knowledge and training with regards to cryptocurrencies.

On the other hand, it is also a challenge for the authorities to clamp down on any cryptocurrency exchange trading in Pakistan illegally. As SBP has put a ban on dealing of virtual assets, any business providing such services can be deemed as a potential money launderer or terrorist financier. Pakistan is not in a position to leave any law enforcement gaps with regards to cryptocurrencies.

ii. Corruption

---

[36] "FATF compliance will require all-out effort", *Dawn*, last modified June 23, 2019, https://www.dawn.com/news/1489898.
[37] "Improving Global AML/CFT Compliance: On-going Process", *Financial Action Task Force*, last modified June 29, 2018, http://www.fatf-gafi.org/countries/d-i/iraq/documents/fatf-compliance-june-2018.html.
[38] "European Commission adopts new list of third countries with weak anti-money laundering and terrorist financing regimes", *European Commission*, last mdofied February 13, 2019, http://europa.eu/rapid/press-release_IP-19-781_en.htm.
[39] Shahid Karim, and Usman Hayat, "Pakistan on FATF's grey list: what, why, and why now?", *Dawn*, last modified June 10, 2019, https://www.dawn.com/news/1418143/, Accessed June 24, 2019.

Corruption is amongst the greatest challenges faced by Pakistan. The current government of Pakistan has been displaying high resolve against corruption. The resolve must also incorporate the curbing of future prospects in corruption-related illegitimate outflows. SBP and other regulatory authorities are vigilantly acting against banking and non-banking financial institutions as well as the informal network of financial transactions: *hawala/hundi*.[40] However, the use of cryptocurrencies for laundering of corruption-related proceeds cannot be ignored. Due to the obvious advantages of cryptocurrencies over orthodox means of money laundering, the corrupt elements in Pakistan would probably adopt this innovative channel to transfer their illegitimate earnings abroad.

Cryptocurrency can also serve those corrupt elements who have been holding billions in cash and waiting for the right opportunity to clean their wealth.[41] As while explaining the risks of cryptocurrencies, Cybersecurity Expert and Former Regional Director FIA, Khawaja Mohammad Ali mentioned that the element of corruption will also surge in the society (with the rise in cryptocurrencies) because when it would become convenient to evade legal controls and to launder money then one can have more prospects of doing corruption without getting caught.[42]

iii. Transnational Crimes

Pakistan is geographically bordered with a neighbor which has been facing a situation of turmoil, chaos, and lawlessness for almost four decades. Afghanistan has been a hub of unlawful transnational crimes involving drug trade, human trafficking, arms smuggling as well as terrorism financing since the Soviet invasion in 1979. Due to the sharing of the lengthy and perilous border with Afghanistan, Pakistan has also been a transit or destination country for narcotics, weapons, proscribed chemical and trafficked persons.[43]

Pakistan is situated at the southern route of illicit trafficking for crime syndicates based in central Asian states to access middles eastern markets.[44] Such organized crimes require a discreet flow of financial transactions, which has always been a challenge as the financial trail can reveal and jeopardize the whole transnational criminal network.

---

[40] Tom Keatinge and Anton Moiseienko, *Security Through Financial Integrity: Mending Pakistan's Leaky Sieve* (London: Royal United Services Institute for Defence and Security Studies, 2019).
[41] "NAB recovers assets worth Rs1.3 billion from Mushtaq Raisani", *Geo News*, last modifed July 11, 2018, https://www.geo.tv/latest/202807-nab-recovers-assets-worth-rs13-billion-from-mushtaq-raisani, Accessed June 28, 2019.
[42] Khawaja Mohammad Ali CISA, CRISA (Cyber Security Expert & Former Regional Director FIA), in discussion with the author, May 29, 2019.
[43] "Illicit Trafficking and Border Management," *United Nations Office on Drugs and Crime*, accessed June 28, 2019, https://www.unodc.org/pakistan/en/illicit-trafficking-and-border-management.html.
[44] "West and Central Asia,"*United Nations Office on Drugs and Crime*, accessed June 28, 2019, https://www.unodc.org/unodc/en/drug-trafficking/central-asia.html.

Cryptocurrencies have the potential to serve the purposes of such transnational crime syndicates as it provides anonymity, swiftness, and less human involvement. Which was earlier executed through physical transportation of cash through air, sea or land route can easily be alternated to the digital world where the click of a button can accomplish an illegal deal.

It is a challenge for Pakistan's law enforcement agencies to follow and bust such a money trail which only exists in a virtual world. In order to cope up with this challenge, it is necessary to have an investment in capacity building of law enforcement personnel as well as equipping the forces with required technological tools.

iv. Terrorism Financing

Terrorism financing has a direct consequence on the physical security of Pakistan. Curbing terror-financing is one of the proactive approaches that have been adopted by security forces in Pakistan, to prevent terror operations in the country. The conventional methods of terrorism financing have been clamped down by law enforcement agencies in Pakistan and terrorists are finding it difficult to fund their operations. However, a surge in terror-incidents is possible if terrorists adopt sophisticated financing mechanism with the help of cryptocurrencies.

In Pakistan, the Financial Monitoring Unit (FMU) is designated for coordinating intelligence with other domestic law enforcement agencies with respect to money laundering and financing of terrorism. FMU has been instrumental in successfully foiling a number of potential terrorist operations with the help of FIA, and Counter Terrorism Department (CTD) of provincial polices.[45]

However, terrorists are getting acquainted with the technology and using it for unlawful purposes which is evident from the propaganda techniques used by sub-nationalist Baloch terrorist groups after each terrorist attack in the year 2019.[46] Similarly, a terrorist-group named Ansarul Sharia was using a customized mobile application for secure communications.[47]

Although there has been a little evidence whether Pakistan based terrorist groups have used cryptocurrencies or not, it is highly probable that terrorists may adopt a secure funding source, which is less regulated and offers all the features which are suitable for terrorists. As it is evident, the terrorists

---

[45] Asad Ullah Khan, *Deconstructing Terror Financing in Pakistan*, (Islamabad: Institute of Strategic Studies Islamabad, 2018).
[46] "India aided terrorist attack on Chinese Consulate in Karachi: police", *The News*, last modfied January 11, 2019, https://www.thenews.com.pk/latest/417530-indian-raw-helped-botched-terrorists-attack-on-chinese-consulate-in-karachi-police.
[47] "Tech-savvy Ansarul Sharia militants developed mobile phone apps for secure communication," *The News*, last modfied September 8, 2017, https://www.thenews.com.pk/latest/228607-Tech-savvy-Ansarul-Sharia-militants-developed-mobile-phone-apps-for-secure-communication.

are using innovative technology in other areas of terror operation such as propaganda and communications.

The risk of terrorism financing through cryptocurrency is also mentioned by FMU in its strategic analyses shared with SBP. FMU stated that cryptocurrency can be exchanged against fiat currency and has the potential for anonymous online transfers, therefore, it is possibly vulnerable to terror-financing.[48]

v. Cyber Crimes

Mainstreaming of cryptocurrencies has enabled cybercriminals to retain their anonymity while inflicting substantial damage on cybersecurity infrastructure as well as, in some instances, on the the social fabric of a society such as child pornography. There are cyber crimes which are simply of financial nature and do not involve physical harm on any person. These crimes include email scams, ransomware, data breaches, identity thefts, etc.

In the late 2010s, a new trend in ransomware emerged where the hacking system asks for ransom in cryptocurrencies.[49] Ransomware is a malware (virus) which denies access to the computers by locking the system until the ransom is paid.[50] Cryptowall, CryptoLocker, DMA Locker, and WannaCry are some of the ransomwares which have collected the highest amount of ransoms in Bitcoin.[51] Such ransomwares have been posing a serious challenge to law enforcement agencies around the globe.

Dark net or dark web would not have achieved popularity among criminals if cryptocurrency had not provided it with a financial solution. It has been estimated that Bitcoins worth US Dollars 872 billion were spent on illegal purchases in the year 2018.[52] Narcotics-related dealings are the most frequent trade on the dark net, but child pornography and stolen credit card data are also transacted regularly.

Pakistan witnessed its worst dark net scandal when it was revealed that hundreds of Pakistani children are being subjected to sexual and physical abuse and filmed to be sold online. In 2015, it was unearthed by a news report that nearly 280 children were physically violated only in Hussain Khanwala

---

[48] FMU, "Virtual Currency".
[49] Josh Fruhlinger, "The 6 biggest ransomware attacks of the last 5 years", *CSO*, last modfied April 5, 2019, https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html, Accessed June 27, 2019.
[50] "Ransomware," *US Department of Homeland Security*, accessed June 27, 2019, https://www.us-cert.gov/Ransomware.
[51] "True scale of Bitcoin ransomware extortion revealed", *Technology Review*, last modified April 19, 2018, https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/.
[52] Olga Kharif, "Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year", *Bloomberg*, July 1, 2019, https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year.

village in Kasur.[53] The perpetrators were involved in the filming of these heinous acts for monetary purposes.

The sudden rise of child abuse cases in Pakistan where children were raped, mutilated, and murdered in a similar fashion indicates that our children are suffering in the hands of international rackets of child pornography. Child's Play, Play Pen, and Red Room are some of the websites which were operating on the dark web with respect to child pornography. These websites and many other such websites require users to make payments in cryptocurrencies to access the content.[54] This is one aspect of cybercrimes which substantially inflicts damage on the social fabric of Pakistan.

While it is evident that Bitcoin and other cryptocurrencies are used for such dealings, it is also probable that facilitators of such international rackets in Pakistan may also be receiving payments in cryptocurrencies. This is one challenge with regards to cryptocurrencies which should be dealt with by the law enforcers of Pakistan on a priority basis as it threatens the social and physical security of citizens of Pakistan.

A number of Pakistan specific cases have emerged where personal and financial information of Pakistani citizens is being sold on the dark web against cryptocurrencies, specifically Bitcoin. In April 2019, it was reported that personal data of female students of University of the Punjab was hacked through spy apps and traded on the dark web against Bitcoins.[55]

Similarly, banking information of Pakistani nationals, which was acquired through hacking of banking systems on a large scale, was being sold on the dark web for cryptocurrencies. During October 2018, data of 19,864 debit/credits cards belonging to 22 Pakistani banks were available for sale online in auction style.[56]

In February 2019, Group-IB, an international cybersecurity company, discovered that database of 69,189 cards pertaining to Pakistani banks' customers was available for sale on the dark web. It was estimated that the database was worth nearly US Dollars 3.5 million.[57] These data breaches not only

---

[53] Alia Chugtai, "Hussain Khanwala: Village scarred by child abuse scandal," last modfied March 9, 2018, https://www.aljazeera.com/indepth/features/hussain-khanwala-village-scarred-child-abuse-scandal-180308110000963.html.
[54] Nayab Nasir, "Debunking dark web and child pornography in Pakistan", *The Nation*, last modified April 19, 2018, https://nation.com.pk/19-Apr-2018/debunking-dark-web-and-child-pornography-in-pakistan.
[55] Hassan Hafeez, "Hacking scandal unearthed: PU female students' data sold out on dark web," *Ary News*, last modified April 11, 2019, https://arynews.tv/en/punjab-university-hacking-scandal-dark-web/.
[56] "Card data of 20,000 Pakistani bank users sold on dark web: report," *Dunya News*, last modfied November 6, 2018, https://dunyanews.tv/en/Crime/465384-Card-data-Pakistani-bank-users-sold-dark-web-report.
[57] Pierluigi Paganini, "70000 Pakistani banks' cards with PINs go on sale on the dark web," *Security Affairs*, last modfied February 24, 2019, https://securityaffairs.co/wordpress/81579/cyber-crime/pakistani-banks-cards-darkweb.html.

raised alarms for enhanced information security in Pakistan, but also implied the possibility of use of cryptocurrencies in illegal sale and purchases of personal and financial records of Pakistani citizens.

Cryptocurrencies have also made their way to the crimes of conventional nature such as kidnapping for ransom. In March 2019, in Lahore a seven-member gang was arrested that demanded a ransom of Rupees 20 million in Bitcoin.[58] It was the first and only crime of its nature, however, it indicates that criminals in Pakistan have started experimenting with cryptocurrency by applying it in crimes of different nature.

Conclusion

The recent FATF's amendment to its recommendations to accept cryptocurrencies in the global financial system has hinted towards the inclination of the world. As different states have started regulating cryptocurrencies, it has become writing on the wall that the technology has a future in the global financial system. Pakistan needs to invest in research and development of cryptocurrencies from the perspective of Pakistans economy and security. Along with research and development, it is essential to have capacity building and training of regulators and law enforcement professional with regards to the investigation and prevention of cryptocurrency oriented financial crimes including ML and TF.

Generally, in Pakistan, the policymakers have deemed the technology of virtual assets as negative. This needs to change as the world has started investing and regulating cryptocurrencies at state-level. The positivities of cryptocurrencies, which include banking the unbanked or unregulated sections of the economy, instantaneous worldwide mobility of finances, and revenue opportunities for the public and private sectors, can prove advantageous for Pakistan's ever-struggling economy. In the meantime, the threats associated with cryptocurrencies which magnify especially in Pakistan's context cannot be neglected. Terrorism financing and money laundering are among the core challenges for the country's security apparatus.

It is also possible that giving space to cryptocurrencies in a prevailing political, economic and security environment will have more negative consequences than positive. However, Pakistan is moving in a direction to overcome these challenges in the years to come. Therefore, Pakistani policymakers must have an approach toward the acceptability of emerging financial technology by addressing structural issues in the current banking and financial system.

[58] Asif Chaudhry, "Gang demanding ransom in bitcoin busted," *Dawn*, last modified March 27, 2019, https://www.dawn.com/news/1472132.

The solution lies in learning the risks and threats associated with cryptocurrencies, developing expertise in blockchain and cryptocurrencies to incorporate virtual assets with the financial system in Pakistan and formulating a strategy to counter those threats through proper legislation and regulations in this regard. A proactive approach is essential for the effective incorporation of cryptocurrencies in Pakistan. Any decision in this regard, taken in hastiness, may have consequences on Pakistan's economic, physical or even national security. The government and state institutions can formulate a five-year-plan for the regulation of cryptocurrencies. In which the initial stage should be to have appropriate training and development, a well-planned study of feasibilities and applicable regulations in accordance with FATF recommendations.