Decrpyting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing

Salman Ali Ibrahim

Abstract

The emergence of an algorithm-based currency mechanism, known as cryptocurrencies, has raised alarms on account of the risks associated with money laundering and terrorism financing. Besides its merits, the decentralized nature of cryptocurrency provides ample opportunities for terror outfits and crime syndicates to park, move, or launder their illicit proceeds by keeping anonymity in transactions due to lack of administrating or central authority to supervise or authorize the legitimacy of transactions. Such issues compelled nation-states to strengthen their Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regimes to ensure their physical, economic, and national security, either through regulations or outright prohibition. Pakistan adopted the latter approach and criminalized any transaction in cryptocurrencies; however, in the absence of any specific legislation, authorities face difficulties in the prosecution of crypto-related offences. This study used a qualitative method of analysis to examine how cryptocurrencies functions, how they facilitate crime syndicates and terrorist financiers to launder their finances, and what measures are required to curb this aspect of illicit financing.

Keywords: Cryptocurrency, money laundering, terrorism financing, proliferation financing.

Introduction

A lot has been debated by academicians, economists, security analysts, government officials and computer scientists regarding the viability, possibilities, and threats associated with cryptocurrency. Some have advocated the use and mainstreaming of cryptocurrency by terming it as a revolution in the global financial system. While many have perceived cryptocurrency, and other related virtual currencies, as a significant threat to global AML and CFT regimes.

Salman Ali Ibrahim is Research Officer at The Pakistan Institute of International Affairs.
Cryptocurrencies and other virtual currencies are revolutionary and novel development in the global financial system. It is entrenched with sophisticated cryptographic functions, which makes it more technical than the prevailing financial technologies. This system has evaded the authority of the middleman by giving control in the hands of transacting parties. A new set of beneficiaries have also emerged who provide mining\(^1\) services and earn their revenues through the generation of cryptocurrency coins. With all these technicalities and advancement, cryptocurrencies are still being explored and financial wizards are looking for ways to develop synchronization between cryptocurrencies and conventional financial systems.

It is argued in favour of cryptocurrency that it promises to dismiss the huge costs associated with the bank-oriented mode of payments.\(^2\) The reason is that cryptocurrencies could help to include billions of unbanked people into the system of the global economy who would otherwise remain out of the economic cycle due to the intricacies associated with conventional financial systems. The blockchain-based currency arrangement has removed the presence of intermediaries or any other administering authority from the equation, which is a plus point for such currencies. A few global enterprises and market leaders in the retail business have started accepting cryptocurrencies as a value of the exchange.\(^3\) Microsoft, the US-based multinational tech giant, has been accepting Bitcoins\(^4\) since 2014 for the purchase of games, movies, and apps in Windows.\(^5\) The growth in acceptability and recognition by renowned business entities will eventually enhance the credibility of the relatively volatile form of currency.

---

\(^1\) Mining is a process to verify cryptocurrency transactions by using a designated set of tools (software and hardware). Miners solve cryptographic puzzles as a part of the proof of work system to add another block to the blockchain and in return, miners receive a number of the same crypto tokens or coin as a reward for their services.


\(^4\) Bitcoin is the first cryptocurrency mechanism which was invented by a software engineer under an alias Satoshi Nakamoto in 2009.

On the other hand, it is argued that the absence of regulatory transparency across jurisdictions has aggravated the vulnerabilities of the cryptocurrency mechanism. The linkage between anonymity and possible illicit use has led to the question that who is responsible for the identification of suspicious activity within the blockchain system. Furthermore, after the identification of a suspicious transaction, what required information can be retrieved and how? Law enforcement in this regard continues to be a challenge due to technical difficulties and lack of expertise and resources required for policing. Hence, the difficulties in the prevention, detection, and prosecution of money laundering and terrorism financing need to be addressed.

A wave of terror-financing through cryptocurrency has been raising alarms worldwide. In 2018, a US citizen of Pakistani-origin, Zoobia Shahnaz, pleaded guilty in the US on the charges of financing and supporting ISIS by laundering over $85,000 in Bitcoin. Some terror 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. Similarly, the Palestinian militant organization, Hamas, has also turned to cryptocurrency for receiving donations.

In the presence of the proliferation threat of chemical, biological, radiological, and nuclear (CBRN) materials, the use of cryptocurrency for a transaction of such components cannot be ignored. The transnational criminal syndicates who previously relied on the hawala are preferring cryptocurrency as a more viable and discreet option to execute

---

6 In cryptocurrency, the blockchain serves as a concept relatively similar to a bank ledger which is publicly available. The transactions of cryptocurrency are added in sequence to the ledger in blocks and thus formulate a chain of blocks of transaction.


international dealings. There has been evidence that cryptocurrencies are being used for human trafficking, drug trafficking, political crimes and corruption. According to the 2015 Europol report, Bitcoin has been used in more than 40 per cent of identified criminal to criminal transactions in Europe.\textsuperscript{11}

Based on these risks, the world is taking initiatives to regulate the sale, purchase and exchange mechanisms of cryptocurrencies to curb the chances of their illicit use. Although there has been little empirical evidence of cryptocurrencies application for money laundering or terror-financing in Pakistan, the associated risks are too serious to be ignored. Terrorism financing and money laundering have already been matters of national security for Pakistan, therefore, it is imperative to assess the emerging threats and challenges to Pakistan’s AML/CFT regime.

**What is cryptocurrency?**

The concept of cryptocurrency originated with the advent of algorithm-based currency – the Bitcoin. Bitcoin was the first of many other digital currencies which joined the bandwagon of the crypto world. All these currencies are dependent on the science of cryptography attached with a blockchain. Cryptocurrency can be best described as a digital value-exchange system, which runs through a peer-to-peer network without the presence of any third party assuming a supervisory or middleman role. The transactions or activities on cryptocurrency are duly recorded on a publicly accessible ledger called Blockchain.

Cryptocurrency is a kind of virtual currency which the Financial Action Task Force (FATF) has defined as ‘distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight.’\textsuperscript{12} The system is ‘decentralized’ as it is administered through algorithms and users, instead of any central body, and it is ‘distributed’ as the ledger is enforced by a distinct network of computers hosted at distant locations around the globe.\textsuperscript{13}

Cryptocurrency enables the users to possess, send or receive value electronically. The same purpose is also served through the banking


payment system of debit or credit cards; however, these processes are
governed through centralized authorities (banks or government
institutions) who keep oversight in authorizing the transactions and
maintain the records. In a cryptocurrency mechanism, there is no
centralized oversight to authorize or unauthorize any transaction.

The most acceptable and in-practice way of trading in cryptocurrency
is through designated exchanges and brokerage houses which are
authorized to deal in cryptocurrency. These exchanges provide services
such as the conversion of fiat currency\textsuperscript{14} to cryptocurrency, trading of
cryptocurrency against other cryptocurrencies and storing of
cryptocurrencies.\textsuperscript{15} However, there are countries where the authorities
have imposed an absolute ban on the trading of cryptocurrencies and
forbade any form of transactions in cryptocurrencies. In such cases,
people may resort to direct peer-to-peer platforms without any
interference of third-party exchanges.

**Cryptocurrency in Pakistan**

As Bitcoin and altcoins\textsuperscript{16} gained momentum and their conversion value
started increasing at an exponential pace, Pakistani investors also saw
this as a potential investment opportunity. Initially, due to the absence
of any proper regulation, there was a lot of uncertainty regarding the
legality of such investments. Although the volume of cryptocurrency
trading in Pakistan has been negligible as compared to other countries,
many Pakistanis were tempted to open accounts with various exchanges
and trading companies.\textsuperscript{17} Some Pakistan based altcoins were also offered
for the Pakistani audience, such as PakCoin.

Nonetheless, the State Bank of Pakistan (SBP’s) put an outright ban
on the use and offering of any virtual currency in Pakistan. SBP’s stated
in its circular issued on April 06, 2018, that the central bank has not

\textsuperscript{14} Fiat Currency is referred to as the actual coin or paper currency, of a given
jurisdiction or state, which is circulated and accepted as a legal medium of
exchange within the issuing country. The digital denomination of any fiat
currency is usually termed as e-money, which is used for electronic transfers or
transactions.

\textsuperscript{15} Rajarshi Mitra, ‘5 Simple Steps, Learn How to Trade Cryptocurrency –
Ultimate Guide,’ Blockgeeks, https://blockgeeks.com/guides/how-to-trade-

\textsuperscript{16} All cryptocurrencies other than Bitcoin are denoted as alternative coins or
Altoins.

\textsuperscript{17} ‘Pakistan Bans Cryptocurrencies,’ *The Express Tribune*, 6 April 2018,
authorized any individual or entity for transacting or facilitating any transaction in any form of virtual currency, coin, or token.\textsuperscript{18} It further states that all such transactions will be considered suspicious and shall be reported to the Financial Monitoring Unit (FMU). The primary concern of Pakistan’s regulating authorities, like many other jurisdictions, pertained to the potential risks of money laundering and terrorism-financing.

SBP’s circulars against cryptocurrencies were heavily criticized by financial technology enthusiasts and local cryptocurrency investors. However, the SBPs move of banning virtual assets and cryptocurrencies was logical. Pakistan is currently striving to avoid the possibility of blacklisting by FATF due to gaps in its AML/CTF regimes with regard to conventional banking and financial operations. The emergence of virtual assets, susceptible to illicit use, in the financial markets of Pakistan would have further challenged Pakistan’s compliance with FATF recommendations.

A major size of Pakistan’s economy is undocumented, and in such a situation, allowing the financial exchanges to deal in cryptocurrencies would facilitate black marketeers, tax evaders, and criminals to park and move their finances.\textsuperscript{19} By criminalizing the dealings in cryptocurrencies, the SBP has secured itself and Pakistan to a considerable extent from the 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.

**Risks of cryptocurrencies**

The decentralized nature of cryptocurrency has rendered opportunities for illicit actors to park and manoeuvre their illegally acquired finances and execute criminal dealings anonymously. The anonymity arises due to a lack of basic principles applicable in the conventional financial system such as Customer Due Diligence (CDD) / Know Your Customer (KYC).\textsuperscript{20} The absence of centralized or supervisory authority in the cryptocurrency

\textsuperscript{19} Zeeshan Shahid (Partner, Forensics, Financial Institutions Risk Advisory, Deloitte Pakistan) in discussion with the author, 13 June 2019.
\textsuperscript{20} Know Your Customer (KYC) and Customer Due Diligence (CDD) are background checks and compliance procedures of a general banking system which pertain to acquiring the customer’s information and its sources of income. These checks are performed to avoid money laundering and terror financing risks.
mechanism has left ample room for criminals, money launderers, and terrorist financiers to smartly evade the legal structure of any jurisdiction.

The threats pertaining to cryptocurrencies, such as terrorist financing or payment mechanism for criminal dealings or activities, need to be analyzed in connection with the Dark Web. There are hundreds of operational illicit marketplaces on Dark Web which deal in almost every prohibited and unlawful goods and services including drugs, weapons, child pornography, and the knowledge and components for the Weapons of Mass Destructions (WMDs). The usual mode of payment in these underground crime markets is cryptocurrencies.

From the perspective of frequency and possibility, it can be inferred that the prospects of money laundering through cryptocurrencies are more probable than terrorism-financing. The key reason is the vastness of the term _money laundering_ as it involves finances from every form of illicit activity and forms a parallel economy which is fuelled through the drug trade, arms smuggling, extortion, kidnapping for ransom, corruption and other means of crime.

On the contrary, terrorism financing is only focused on the organizations managing their funds to pursue violent means to achieve their political, religious, or social motives. Besides, terrorism has been considered as a matter of national security by almost every state in the world; hence, terrorism financing is given higher priority by law enforcement agencies than other crimes and subjected to more vigilance.

_Terrorism financing_

A terrorist organization can successfully execute its operations and strategies if it succeeds in building and maintaining an effective and discreet financial infrastructure. The most notable among terror outfits,

---

22 Dark Web, Deep Web, or Dark Net is a network of encrypted websites and accessible only by using a complex set of security tools.
which have remained active for years and left a transnational impact, are al-Qaeda (AQ) and the Islamic State of Iraq and Syria (ISIS). These organizations would not have been successful in establishing a functional decentralized terrorism network without the presence of their terror-financing network.

Both AQ and ISIS had footprints across continents; therefore, their financial systems actively involve the movement of funds across countries. The movement involves the generation of funds through illicit criminal enterprises in addition to crowdfunding from sympathizers and financiers. Nonetheless, proceeds from organized crimes such as arms, drugs and human trafficking; smuggling; kidnapping for ransom, and extortion, overshadow the funds generated through donations for terror operations.\textsuperscript{25}

Conventionally, terrorist organizations have mainly adopted two methods of financing and laundering of funds from one country to another: traditional hawala networks and conventional international banking.\textsuperscript{26} Hawala refers to an underground system of funds remittance on a trust basis without actual or physical movement of money.\textsuperscript{27} In 2015, it was estimated that the annual transaction volume of funds through the hawala network is around $400 billion which indicates the magnitude of use of the system.\textsuperscript{28}

Both these traditional terror-financing mechanisms have their risks and challenges for terrorist organizations. Even though hawala is a secure way of funds transfer for terrorists, it does not facilitate the simultaneous collection of finances from multiple geographical locations which is a key element in crowdfunding. Similarly, the hawala network is


\textsuperscript{26} Aaron Brantly, ‘Financing Terror Bit by Bit,’ \textit{CTC Sentinel}, Vol. 7, Issue 10, October 2014,p.2.


not as instantaneous as the emerging virtual currency options for terrorists.\textsuperscript{29}

In addition, the global financial bodies and AML/CFT enforcers, such as FATF, have keenly demanded from member countries to curb the operational hawala and \textit{hundi} networks within their jurisdictions.\textsuperscript{30} This has led to the busting of underground banking networks around the globe which has left limited avenues for terrorists to transfer their funds.

Conventional banking involves high scrutiny of international transactions for money laundering and terrorist financing, so it is a high-risk option for terrorists. The use of banking channels to move funds may bring the terrorists to the attention of intelligence officials and law enforcement agencies and consequently threaten the operational prospects of terrorist organizations.

According to a study conducted by the RAND Corporation, al-Qaeda, ISIS, Hezbollah, and other terrorist organizations invariably need an anonymous, safe and spontaneous finance mechanism, and cryptocurrency is a highly feasible option for them.\textsuperscript{31} The properties of cryptocurrencies, such as anonymity, usability, security, acceptance, reliability, and volume, makes it ideal for terror outfits for crowdfunding, illicit drugs and arms dealings, and movement of funds for operational needs.

Anonymity refers to the discreet movement of funds without revealing the identities of transmitting parties. Usability means the ability to conduct dealings in a particular currency with convenience. Security includes the cryptocurrency’s structure of maintaining confidentiality, integrity, and accuracy of transaction details and transacting parties. Reliability is the availability and speed of transactions for the users. Whereas, volume is the total amount of cryptocurrency transactions or trading executed in a given period over a particular exchange or within a jurisdiction.\textsuperscript{32}

\textsuperscript{29} Khawaja Mohammad Ali CISA, CRISA (Cyber Security Expert and former Regional Director FIA), in discussion with the author, 29 May 2019.
\textsuperscript{31} Cynthia Dion-Schwarz, David Manheim et al., \textit{Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats} (Santa Monica, CA: RAND Corporation, 2019), p.xii.
\textsuperscript{32} Ibid.
Currently, no single cryptocurrency offers a complete solution to terrorist groups for their financing needs. There is a range of cryptocurrency variants available for terrorists to adopt as per their needs. Where there is a high need for usability and reliability, Bitcoin can serve the purpose as it is widely recognized as compared to others; thus, it can be used for crowdfunding, fundraising, and attack funding. The anonymity aspect of Bitcoin has also improved over time, allowing more convenience to terrorists and other criminals to hide their identity, while executing financial transactions. Some companies provide dark-wallet services to illicit actors to completely anonymize the cryptocurrency transactions and leaving little to no trail for law enforcers. These anonymizing service providers may pose serious hindrances for the government striving to trace terrorist and illicit cash-flows.\(^{34}\)

The altcoins, such as Omni Layer (MasterCoin), BlackCoin, Monero, and Zcash, offer more privacy and secrecy for illicit transactions as compared to Bitcoin. Anonymity and security of transfer of funds hold critical significance for operational funding and illicit trafficking. Hence, terror outfits may opt for Monero or Zcash where there is a higher degree of privacy and which allow offline use and funds transfers. However, these options significantly lack usability, reliability and are not feasible for the transfer of large sums as is possible in the case of Bitcoin.

A significantly high exchange rate of Bitcoin in comparison to other cryptocurrencies can facilitate the terrorist financiers to transfer millions of dollars without adhering to KYC/CDD protocols and in return for nominal transfer cost. On 31 January 2021, the value of a single Bitcoin was US dollars 33,114.36, which indicates that around 30 coins are required to transfer a million US dollars via Bitcoin.\(^{35}\)

There have been instances where a user has either acquired or transferred Bitcoins worth more than 100 million US dollars and maintained anonymity in public.\(^{36}\) However, a transaction in hundreds of

---

33 Anonymizing is a process of removing traces from cryptocurrency transactions and making it virtually non-traceable to the actual beneficiaries of transactions by obscuring the source of the transaction. Dummy transactions and addresses are used to attain anonymity through such a process.


36 Nathan Reiff, ‘Anonymous Cryptocurrency Trader Buys $400 Million in Bitcoin,’ Investopedia, 25 June 2019,
millions of dollars may draw considerable attention in the Bitcoin market, as the ledger is publicly accessible and available to all the Bitcoin users, which is usually not desirable for terror enterprises.

It can be deduced that terrorists are moving towards Dark Web-oriented possibilities for fundraising, funds transfers, and procurement of weapons and explosives in exchange for cryptocurrencies. In 2010, it was estimated by a cybersecurity firm named, Procysive, that there are nearly 50,000 radical websites and above 300 terrorist forums operating on the Dark Web.37

There are pages on the Dark Web with names such as ‘Fund the Islamic Struggle without Leaving a Trace and Bitcoin and Charity for Jehad, calling for funds in cryptocurrencies to discreetly generate funds for terrorist operations’.38 During 2017-2018, an AQ linked Twitter account, al Sadaqah, called for donations in Bitcoin, Monero, Dash, and Verge to assist the terrorists fighting in Syria. The principal focus of the account was to ensure the potential financiers about the anonymity and non-traceability of the transactions.39

In 2015, it was reported that the al-Qaeda affiliated terrorists who attacked the Charlie Hebdo office in Paris acquired the funds for the attacks in Bitcoin.40 In November of the same year, Paris was struck by a series of deadly attacks by ISIS terrorists and it was reported later that four assault rifles used in the attacks were bought on Dark Web from a German vendor.41 Some even inferred that the payment of these weapons


40 Steven Stalinsky, ‘Terrorists have been using bitcoin for four years, so what’s the surprise?,’ The Hill, 8 March 2018, https://thehill.com/opinion/cybersecurity/377415-terrorists-have-been-using-bitcoin-for-four-years-so-whats-the-surge, accessed 17 July 2019.

was made from an ISIS-owned Bitcoin wallet possessing nearly 3 million US dollars.\textsuperscript{42}

Besides fundraising and transfer of funds for terror operations, the terrorist organization has used cryptocurrencies to generate funds through criminal dealings. Investigations have suggested that ISIS has been involved in the smuggling of antiques, robbed from ancient Syrian cities, to London, to sell them on the online black market against cryptocurrencies.\textsuperscript{43} Moreover, the terrorist organization has been engaged in various organized crimes including trafficking organs harvested from its captives and selling them on the Dark Web.

\textit{Proliferation financing}

The proliferation of weapons of mass destruction, components, and delivery systems is one of the highest risks to global security and stability. States, as well as non-state actors and terrorist organizations, are said to have tried in the past to acquire or build WMDs to pursue their interests.\textsuperscript{44} There is a persistent threat that terrorists or non-state actors may acquire CBRN capabilities for applying in terrorist activities.

Several international treaties and conventions in this regard have been formulated by the international community to maintain stability and order by preventing proliferation of WMDs.\textsuperscript{45} These preventive and detective mechanisms mainly include stringent export control regimes and curbing proliferation financing through the United Nations Security Council (UNSC) resolutions and FATF recommendations.

The International Convention on Terrorism Financing (1999) criminalizes all sort of funding and financial support to any outfit which is engaged in terror activities by stating that a person commits a criminal offence when he ‘by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be

used or in the knowledge that they are to be used, in full or in part, to carry out’ terrorist activities.\textsuperscript{46}

UNSC Resolution 1540 requires all the states to ‘establish, develop, review and maintain appropriate effective... controls on providing funds and services related to such export and trans-shipment such as financing, and transporting that would contribute to proliferation...’\textsuperscript{47}

Similarly, the International Convention for the Suppression of Acts of Nuclear Terrorism (2005) engages states to cooperate by taking practicable measures ‘to prohibit in their territories illegal activities of persons, groups and organizations that encourage, instigate, organize, knowingly finance or knowingly provide technical assistance or information or engage in the perpetration of’ offences, listed in the Article 2, which are related to radiological or nuclear terrorism.\textsuperscript{48}

Proliferation financing can be summarized in the words, as defined by the FATF, ‘providing financial services for the transfer and export of nuclear, chemical, or biological weapons; their means of delivery and related materials.’\textsuperscript{49}

All the aforementioned resolutions and conventions encourage states to actively pursue a course of actions to prevent the possibility of terrorists or non-state actors acquiring the finances, materials, knowledge or delivery means to develop or possess any weapon of mass destruction. It is the responsibility of states to enforce the required protocols and security measures within their jurisdiction to ensure collective security as the acquisition of WMDs by a non-state actor is a collective threat for the human race.

The global regimes on export controls and terror financing have impeded the possibilities of CBRN proliferation. However, the Dark Web has made it relatively convenient for terrorists to acquire the necessary material and technology along with the required knowledge to develop

devices comprising CBRN material.\textsuperscript{50} Even with the presence of suppliers on the Dark Web, one of the difficulties in acquisition was due to the intricacies of the financial trail. This problem has been potentially solved for the illicit actors by cryptocurrencies.

The synergy of anonymity offered by cryptocurrencies and the Dark Web has enabled the illicit actors to hide their identity and trade in the most lethal and destructive substances and materials without raising any alarms for the law enforcement agencies. Encrypted communications and virtually discreet payment methods can render an increase in the trade of CBRN substances.\textsuperscript{51}

The availability and successful acquisition of biological substances can be determined by the case where a graphic designer ordered a biological toxin (Abrin) from the Dark Web against Bitcoin worth £950.\textsuperscript{52} In 2016, the then US president Barack Obama described to fifty other heads of states how terrorists had acquired radioactive isotopes through the Dark Web.\textsuperscript{53}

In addition to non-state actors, experts believe that cryptocurrencies can offer a financial resort to rogue regimes facing sanctions due to proliferation activities. According to a study, North Korea is using cryptocurrency as an alternative financial recourse to evade sanctions and eventually fund its nuclear programme.\textsuperscript{54} It is perceived that North Korea, by using its cyber crime capabilities, may generate cryptocurrencies through exchange hacks and mining operations to finance its WMD programme.\textsuperscript{55}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{50} FBI, ‘A Primer on DarkNet’, op. cit.
\item \textsuperscript{51} Atlantic Treaty Association, ‘Final Report: Chemical, Biological, Radiological, and Nuclear Threats,’ (Brussels: 2017), p.5.
\item \textsuperscript{53} Gabrielle, ‘Terrorist migration to the Dark Web’, op. cit. p. 43.
\end{itemize}
\end{footnotesize}
Based on the sensitivity of the matter, the threat of proliferation financing with the help of cryptocurrencies shall be given primacy by the global agencies working for the non-proliferation of WMD technologies.

**Conclusion and recommendations**

Cryptocurrencies pose serious threats to prevailing AML/CFT regimes. The anonymity, either as a featured characteristic of a particular cryptocurrency or through anonymizing service providers, is a highly appealing element for terrorists and illicit actors. The challenges are diverse and range from threats to individuals to the states. These risks and challenges, which have amplified due to the rise of unregulated and decentralized cryptocurrencies, include cyber crimes, tax evasion, corruption, terrorist financing, proliferation financing, illicit arms and drug trafficking, organized crime and so on.

The aforementioned risks also extend to Pakistan: however, like many other jurisdictions, Pakistan has adopted an approach of criminalizing every form of dealing and exchange in cryptocurrencies. The decision was primarily based on the non-regulated, under-documented, and highly cash-based economy of Pakistan. Due to this very fact, the financial regulators and agencies responsible for combatting money laundering and terrorism financing are striving to comply with FATF recommendations to avoid Pakistan’s grey or blacklisting with the international money-laundering watchdog.

Pakistan’s response by banning cryptocurrencies has been deemed as a radical move. However, it has its logical reasoning. Any other option in the prevailing economic, social, and security environment would have created security complications for the country’s law enforcement institutions. Pakistan does not have a well-documented economy like those countries which have embraced this financial technology so far. To obtain the benefits of emerging financial technologies, Pakistan first needs to fill the vacuums in the prevailing AML/CFT regime.

Even though Pakistan has banned cryptocurrencies, the law enforcement agencies which deals in financial crimes, such as Federal Investigation Agency (FIA), are facing difficulties in prosecution of cryptocurrency-oriented crimes due to the lack of any specific regulations. Currently, such crimes are being charged under the Foreign Exchange Regulation Act, which does not provide the proportionate punishment for
such crimes.\textsuperscript{56} There is an imminent need for specific and relevant legislation with respect to cryptocurrencies well in accordance with the current approach of the authorities.

Cryptocurrency assets are here to stay and the technology cannot be resisted for long. The recent FATF’s amendment to its recommendations to accept cryptocurrencies in the global financial system has hinted towards the inclinations of the world.\textsuperscript{57} As different states have started regulating cryptocurrencies, it has become the writing on the wall that this technology has a future. Pakistan needs to invest in the research and development of cryptocurrencies from an economic and security context. Along with research and development, it is essential to have capacity building and training of regulators and law enforcement professionals with regard to the investigation and prevention of cryptocurrency-oriented financial crimes, including money laundering and terrorism financing.

Cryptocurrency involves the use of sophisticated technology and protocols, therefore, policing in this area demands the enrolment of technical professionals who can assist law enforcement officials in the investigation of crimes of such nature. Furthermore, these technical experts may also help in the training of detectives, intelligence officials, investigators, and prosecutors on technical grounds, which will eventually be beneficial in curbing illicit financing in cryptocurrencies.

Generally, in Pakistan, policymakers have deemed the technology of virtual assets and cryptocurrencies in negative terms. This needs to change as the world has started investing and regulating cryptocurrencies at the state level. In the meantime, the threats associated with cryptocurrencies that 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.

The solution lies in learning the risks and threats associated with cryptocurrencies, development of expertise in blockchain in Pakistan, and formulating a strategy to counter those threats through proper legislation and regulations.


A proactive approach is required for the effective incorporation of cryptocurrencies in Pakistan. Any decision in this regard taken in haste may have negative 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. The initial stage must involve appropriate training and development, a well-planned study of feasibilities, and applicable regulations under FATF recommendations.

It is also possible that giving space to cryptocurrencies in a prevailing political, economic, and security environment will have more negative consequences than positive ones. However, Pakistan is moving towards a direction to overcome these challenges in the years to come. Therefore, Pakistan’s policymakers must have a clear approach towards the acceptability of emerging financial technology by addressing the structural issues in the current banking and financial system. The emerging illicit financing tactics demand regional cooperation and coordination to cater to challenges by helping each other. Regional bodies can be established in which member states can assist their peers in the areas of drafting and implementation of regulations and training of law enforcement officials in the prevention and detection of potential money laundering and terrorism financing risks in a cryptocurrency system.

It is also pertinent that law enforcement agencies may not succeed in curbing money laundering and terrorism financing through cryptocurrencies due to the transnational aspect of the technology and the jurisdictional limitations of law enforcers. To counter this, an international mechanism of intelligence sharing, cooperation, and capacity building is essential.

Nonetheless, cryptocurrencies provide an opportunity for both, terrorists and criminals, to discreetly move their finances, therefore, this needs to be monitored at national and international levels. The risks, either arising from organized criminal enterprises, terrorist organizations or other illicit actors, may be mitigated by using technology-oriented tools and techniques to track down these elements. Secondly, strong and effective regulatory legislation for cryptocurrencies with regard to money laundering and terrorism financing can prove worthwhile in defeating criminals in this sphere of financial crimes.