Bulletin of Business and Economics, 13(1), 177-181
https://bbejournal.com
https://doi.org/10.61506/01.00176

Digital Currency Financing Terrorists in Pakistan. The Way Forward

Dr. Munir Ahmad[1], Muhammad Idrees[2], Muhammad Saleem Qazi[3]

Abstract
Cryptocurrencies have become a preferred mode of terror financing. it is imperative to analyze the role of cryptocurrencies in empowering terrorist organizations especially in developing states. It takes on a more serious form in developing countries like Pakistan, which is fighting a battle against terrorism for the last few decades. Now digital financing has become an undeniable reality of the modern world, it is essential to devise a comprehensive strategy for breaking the nexus between terrorism and cryptocurrencies. This article intends to explore the answers to the questions that why cryptocurrencies are becoming a preferred mode for terror financing. It argues that the anonymity, decentralization and operational ease of cryptocurrencies make them a preferred medium for terrorist organizations. Therefore, enhancing institutional capacity by training human resources and making dedicated efforts at the national level will prove to be instrumental in delinking terrorism and cryptocurrencies. Moreover, close collaboration between international watchdogs and national institutions is essential in mitigating the threat of the use of cryptocurrencies for terrorism.
Key Words: Cryptocurrencies, Terror financing

1. Introduction

Cryptocurrencies have become a preferred mode of terror financing as it has the potential to unleash new opportunities for terrorist groups who aim to circumvent surveillance system enacted nationally and internationally (Marshall, 2017). In such conditions, it is imperative to analyze the role of cryptocurrencies in empowering terrorist organizations especially in developing states. Pakistan remained confronted with the challenges of terrorism and militancy since the post-Afghan war era. Reportedly 80,000 Pakistanis have lost their lives because of the menace of extremism. The country also suffered economic losses worth billions of dollars in the fight against terrorism. Pakistan has launched several military operations to root out terrorism. Zarb E Azb was followed by a series of operations, resultantly Pakistan emerged as one of the few countries which countered terrorism successfully.

However, the presence of the Islamic State of Khorasan (IS-K), Tehreek Taliban Pakistan (TTP) and militant groups in Afghanistan continued to pose a serious threat to Pakistan. Coupled with this, the use of digital economy for terror financing has emerged as an existential threat to the country. It is thus imperative to wipe out all sources of terror financing due to precarious geostrategic threats existing already. Pakistan has successfully closed major avenues of terror financing which is also lauded by the Financial Action Task Force (FATF), a specialized agency committed to ending money laundering and terror financing. Despite significantly improving the formal channels used for circulation and flow of cash, terrorists may transfer money to any part of the world through cryptocurrencies.

Therefore, significant strategies are needed to act swiftly and decisively. A smooth flow of money and aid is a lifeline for terrorist outfits. They chalk out different strategies for diversifying their sources of funding. People from different walks of life participate in funding terrorist organizations (Hileman & Rauchs, 2017). The nature and source of funding vary according to organizational structures and objectives of the terrorist groups. The organizations use available means to grasp maximum resources for the attainment of their malicious objectives (Torpey, 2016; Ali et al., 2023).

Terrorist organizations need finances for two purposes primarily. Firstly, to carry out the acts of violence and terrorist operations. Secondly, it is needed for technical necessities and organizational sustainability. Terrorism is a source of living for terrorists.10 Therefore, money is inevitable for any terrorist organization (Dion-Schwarz et al., 2019). The sources of terrorist financing are wide-ranging. Criminal activities like theft, robberies, extortion, ransom human trafficking and drug trade are the preferred choices of terrorist organizations. With the above-mentioned sources of funding, organizations have to deposit their illegal money to legitimate bodies. Therefore, cryptocurrencies due to their nature provide relative ease to a terrorist organization for terror financing. The current modus operandi of the cryptocurrency dealers, traders and financer are through large-scale companies. For instance, Binance Holding Inc is an international company worth $100bn.

Money can be transferred, like that of other digital exchanges, to any part of the world from this platform. It remains legit and there are no legal ramifications to assess the underlying regularities. The companies working through appear legitimate in the exchange of money. Another major source is getting money from legal sources such as fundraising campaigns. Terrorist organizations have sympathizers who provide them with money. Moreover, arms trade and money laundering are also a source of funding for terrorist organizations. The most glaring example in this regard is ‘Fund the Islamic Struggle without leaving a trace (Weimann, 2018). It is a notorious dark web page that campaigns for funds to sponsor terrorist causes in different parts of the world. It has been allegedly operated by ISIS. According to Weimann et al, this website has been actively employing cryptocurrency for its operation. In a similar context, the FBI traced and closed a mammoth network named, ‘The Silk Road’ which was involved in such activities. It was operating through the Dark web and received funds from Bitcoin. Similarly, Barhun Naim, who sponsored and conducted the 2016 Jakarta attacks, used Bitcoins and other cryptocurrency sources. Moreover, a group was apprehended in America which used to facilitate ISIS in collecting Bitcoins. The examples simply show that there has been an incessant rise in the utilization of all possible means by terrorists to use cryptocurrencies for illicit purposes.

[1] Corresponding Author, Department of Pakistan Studies Bahauddin Zakariya University, Multan, Pakistan, munirsandhu79@gmail.com
[2] Department of Pakistan Studies Bahauddin Zakariya University, Multan, Pakistan, khanidrees385@gmail.com
[3] Department of Pakistan Studies Bahauddin Zakariya University, Multan, Pakistan, saleem82.taunsvi@gmail.com

A cryptocurrency is a unit of measure, medium of exchange and store of value. Cryptocurrencies do not have any inherent value. Their value depends on the value of other currencies and assets. Forbes defines cryptocurrency as a medium of exchange that is digital, encrypted and decentralized. Unlike the U.S. Dollar or the Euro, there is no central authority that manages and maintains the value of a cryptocurrency (Perkins, 2020). Instead, these tasks are broadly distributed among a cryptocurrency's users via the internet whereas cryptocurrencies use blockchain technology for implementing their transactions. The parties involved in the transaction validate and authenticate the entire ledger and transaction. Alistair Milne defines cryptocurrencies as an asset on a blockchain that can be exchanged or transferred between network participants and hence used as a means of payment—but offers no other benefits. Cryptocurrency works through peer-to-peer transactions (Perkins, 2020). There is no involvement of any banking channel. Payment can be sent and received from any part of the world without involving in any legal and financial formalities. Advance coding techniques are used to verify and authenticate transactions. Encryption is provided to currency and public ledgers. Complex mathematical problems are solved during the mining of cryptocurrency (Gowda & Chakravorty, 2021).

2. Literature Review

Dion-Schwarz et al (2019) have discussed the use of cryptocurrencies for terror financing. They argue that terror financing has been shifting in size and scope. Modern and more volatile sources have entered the domain. The most threatening among them is cryptocurrency. Their research has focused on two basic questions. The first one is the tendency of terrorist organizations to use cryptocurrency. The second question is how the organizations will use money in the future. They will be using future technologies to expand their sources of information and money (Teichmann, 2018).

It has furthered the unanimity and the level of high-volume transactions. They believe that the future endeavours of terrorist organizations will flow from cryptocurrencies. Several features have been identified which make the digital currency a vigorous source of money laundering and then terror financing and five basic characteristics of cryptocurrencies have been highlighted (Dion-Schwarz et al., 2019). The first among them is anonymity. One cannot know who is sending and receiving the money. It protects the parties at both ends. It makes the whole process cumbersome for law enforcement agencies to detect. The second pivotal aspect is the usability of cryptocurrencies. They are more prone to be used in any type of circumstances. The third important aspect is the acceptance of cryptocurrencies. They are widely accepted by the people and organizations as no authentication mechanism exists to recognize if the currency is earned through illicit and illegal means. The fourth important characteristic of cryptocurrencies is their reliability. They are simply efficient for the end-users. The last characteristic which makes it more effective is the volume of transactions. People can use these transactions for a high volume. Furthermore, scholars believe that currently, the use of cryptocurrencies is relatively low. People are not properly aware of the severity. In the years to come, the use of cryptocurrencies by terrorist organizations will be the prime source of funding. They will be using it without any fear of the law. The researchers recommend that the government and law enforcement agencies must take proper measures to counter and curtail proliferation of terror financing sources (Dion-Schwarz et al., 2019).

The use of cryptocurrencies has been increasing. It will rise at an incessant pace in the future. Cryptocurrencies were developed to safeguard the economy against shocks and recessions (Dion-Schwarz et al., 2019). Yet, the hostile actors have infused it for their vicious purposes. It is because of the inherent and inalienable characteristics of cryptocurrencies. The key is the hidden identity of its users. Terrorist groups like ISIS and Al Qaeda have also already used these means to attain their terrorist and violent ends (Dion-Schwarz et al., 2019). Government agencies from different parts of the world need to collaborate and take multilateral initiatives in this regard. It would ensure that companies, organizations and people comply with the rules and regulations, otherwise, implications of cryptocurrencies for global peace and harmony are detrimental.

Cryptocurrency will become a prime source of terror financing in the future. The developing countries would be at a higher risk. They further argued that there is a need to strengthen supervision of national and international institutions. Their research concluded that it would only be possible by making a consensus-based international system. The governments around the world must develop their national-level plans of action as well. Financial technologies and digital payment methods have ushered in a new era for terrorists. They are more motivated and equipped to exploit vulnerabilities of the international system. Terrorist organizations will use cryptocurrencies for terrorism purpose. Globally, the state agencies may not be able to decipher the sources. It would have become a distant choice for the end-users.

Cryptocurrencies are illicit and illegal means of transfer of money. The Federal Board of Revenue and Federal Investigation Agency do not allow trade and transactions through cryptocurrencies. These institutions have recognized the negative aspects of trading via cryptocurrencies and are focusing on taking appropriate measures for regulation of digital financing as a key priority. This research explains the threats that cryptocurrency and online financing have posed to developing states. It also suggests viable solutions and policy recommendations to counter the threats and challenges in the context of Pakistan. This research highlights that the present pitfalls in the legal structures regarding cryptocurrencies need to be reformed.

The existing literature does not explain and elucidate the use of cryptocurrencies for terrorist activities in the case of Pakistan. There is a dearth of proper empirical research which can provide an effective analysis of the cryptocurrencies in the context of Pakistan. The existing literature either focuses on terror financing issues or the prospects of the cryptocurrency. In addition, the government has banned cryptocurrencies. It will not work in the future, because the technology cannot be stopped from making its inroads. Thus, the inflow of cryptocurrency needs efficient preventive and pre-emptive measures. Otherwise, it will be difficult in the years to come to stop terrorists from employing these digital means. So, there must a comprehensive strategy to curtail the use of cryptocurrencies in terror financing.

3. Methodology

The following study is qualitative, exploratory and descriptive. Data is collected from secondary sources. For the secondary data, journals, research articles, newspapers, reports, laws, cases and internet sources have been consulted. An analytical approach is adopted to identify and comprehend the multifarious aspects of the subject under consideration. The components of cryptocurrency and terror financing are discussed thoroughly for better and deeper introspection. The analysis provided is opinion-based, however, it is firmly rooted in evidence. The study is an effort to cover and thoroughly analyze the prospects of mitigating the security threat of cryptocurrency for Pakistan. The implications of the cryptocurrency have been discussed by observing different cases in various countries and inference has been made in the context of Pakistan.

3.1. Threats and Challenges of Online Financing for Pakistan

The existing literature shows that developing countries lack laws and regulations to govern the issues of terror financing through cryptocurrency. In this regard countries need to implement policies to counter threats of terror financing.

3.2. The Need for Consolidated Formal Mechanism

A formal mechanism is needed to eliminate the terrorist financing sources. The FATF tried to convince the states to manage conventional sources of terror financing. The government has implemented different policies to end terror financing through banking channels. It has control over digital mechanisms of payment. Now, there is a need to build policies to tackle the emerging threat of cryptocurrencies too (Aliens, 2016).

3.3. Money Laundering for Terror Financing

Organizations like ISIS can get money from cryptocurrency. As cryptocurrency is decentralized and the state usually does not have access to the transactions, it can be used to conduct trans-national terrorist operations and to finance acts of terrorism globally. This has the potential to strengthen various militant groups in different parts of the world (Andreessen, 2014).

3.4. Anonymous Nature of Finance

The picture below shows how cryptocurrency works. It explains the overall covert mechanism of its operation. In the long term, it would empower the enemies of the state. It must be dealt with by the government with severe action.

3.5. Coordination between the Institutions and Allocation of Funds

The concerned institutions need to enhance their capacity and capability to handle this emerging threat. They must develop an efficient governmental policy and institutional framework to cooperate with other states and engage international institutions. It would lead to significant reforms in the long term. Moreover, dedicated funds for curbing cryptocurrencies in terror financing are required. The threats are real and the activities of the terrorist organizations are increasing hence, appropriate response is inevitable (Baron et al., 2015).

3.6. Crypto Scams and Terror Financing

Similarly, Crypto scams and frauds are on the rise. According to CNBC, an American TV channel, the scammers plundered more than $7.8bn from crypto investors in 2021 alone. It was done by getting access to their accounts. The most notorious example of a crypto scam in 2021 was related to Save the Kids. It was celebrity sponsored and lauded the initiative. The people behind it had good intentions but the cryptocurrency dealing in it was fraudulent. It was run through FaZe but the people investing in it sold their coins. It led to a disastrous end for the investors. On the other hand, the Squid Coin was also a malicious scheme. It was promoted and sponsored by the creators of the Squid Game. It was amply planned as the creators fled with millions of dollars. In addition, the Poly Network hack led to the loss of $600mn. In a similar domain, the maintainers and developers of the Afriscyrpt fled with billions of dollars. The developers were running a currency exchange. Yet once they developed to a certain extent they fled with the money. Lastly, Bored Club Non-Fungible Token faced incessant fraud, too. Contrary to it, the situation in Pakistan has not been different. Federal Investigation Agency has filed a case against Binance, the largest crypto exchange. The agency has alleged that more than 100,000 people have been looted through fake transactions (Saeed & Sial, 2023).

According to FIA, the majority of people have complained that they are unable to access their apps. The money involved in this scam is more than $100 million. Now it is imperative to analyze what it holds for militant organizations. The incidents of crypto frauds indicate that cryptocurrency carries attraction for militant organizations. Terrorist groups can gather funds from different parts of the world. It would give them shear cover. For instance, ISIS and other terrorist organizations can collect money from external sources (Saeed & Sial, 2023). Similarly, the terrorist groups working under the banner of other larger outfits can also benefit from it. The two major financial regulators of Pakistan, the Securities and Exchange Commission of Pakistan and the State Bank of Pakistan require to develop a policy framework to monitor cryptocurrencies. Yet, the data shows that people are interested to invest in it. However, in the absence of any legal and regulatory framework in place, the whole business has been declared illicit. It is pertinent to mention that effective laws to regulate the transfer, exchange and trade of cryptocurrencies should be developed. In the absence of laws, the anti-state elements may exploit the vulnerabilities and compromise peace and stability (Saeed & Sial, 2023).

4. Policy Recommendations

Virtual currencies are emerging at an incessant rate. There is a need to have effective strategies. In this regard, the government must take the following policy actions. These actions are vital to eliminating the threat of terrorism through cryptocurrencies. In this regard, the partnership between private entities and organizations is inevitable. That requires dynamic national cooperation based on coherent and pragmatic actions.

4.1. Robust, Effective, Efficient, Comprehensive Rules & Regulations

Governments must develop rules and regulations to keep a check on the flow of cryptocurrencies. Banning cryptocurrencies is merely a cosmetic action.35 For instance, YouTube, PUBG and other social media and internet platforms were previously banned by the Pakistan Telecommunication Authority. Yet, the people managed to find ways of accessing and using these platforms even during the ban. Any similar approach for cryptocurrency would be insufficient. So, the total expulsion of cryptocurrencies is part of

the problem. Hence there is a dire need for reforms in the legal and regulatory mechanisms. It should be done through the national and provincial consensus. The regulators must devise frameworks that can curb the malicious use of cryptocurrency and educate the youth about its consequences. The most effective way will be to develop a framework to regulate and monitor the use of virtual currency. It would be possible by getting help from international institutions. It can be attained through the advancement in technology and investing in research and development spheres (Biryukov & Pustogarov, 2015).

Similarly, there is a need to have expert working groups at different policy levels of the government. In this regard, cooperation between the Securities and Exchange Commission of Pakistan, Federal Investigation Agency, and Federal Board of Revenue, national intelligence agencies and provincial revenue and police authorities is required. They should collaborate to comprehend the depth of the problem. For instance, European Union, through European Commission has been working to make rules of crypto transfer public. European Banking Authority regulates the affairs related to cryptocurrency. It has been working to intercept and have a check over the transfer of cryptocurrencies under the guidelines of FATF. Pakistan must also work to develop and become part of such a system.

4.2. Capacity Building of Law Enforcement Agencies

There must be proper training sessions and agency-level frameworks. The government agencies must allocate substantial resources to handle the proliferation of cryptocurrencies. The capacity of law enforcement agencies to investigate cases related to cryptocurrencies needs to be enhanced. It will help the government to find out the culprits. But without prior training, it is not possible. Agencies, like FIA, which deal with cybercrime and cryptocurrency need to develop skills and expertise. They need to augment their capabilities through training.

4.3. Cooperation with Foreign Governments and International Agencies

The government of Pakistan must engage and collaborate with international institutions. In this regard, technical and technological cooperation from United Nations, European Union, ASEAN, SAARC and World Economic Forum must be sought. Similarly, engagement with International Monetary Fund, World Bank Group and Financial Action Task Force should be accelerated. It would help to trespass the route of counter-terrorism with relative ease. These international organizations must also ensure to provide suitable assistance to underdeveloped countries. Otherwise, developing countries have insufficient financial and economic resources to combat terror financing.

4.4. Enhanced Intelligence Sharing

There should be internal and external intelligence sharing. The government agencies must enhance institutional cooperation. Interdepartmental and inter-governmental intelligence should be strengthened. It would empower institutions to properly check activities of agents and entities working against the interests of the state. It would develop a salubrious mechanism to comprehensively eliminate terror organizations in the long run. Terrorist organizations are not oblivious of modern trends. They use money at the ground level. So proper check and balance over suspicious organizations will help to eliminate chances of proliferation of ill-gotten money. It is beneficial to mention that through effective coordination of SECP, FIA and State Bank of Pakistan, the targets of the FATF 2018 agenda have been achieved. Pakistan achieved 26 out of 27 points, including terror financing in the 27 Point Action Plan of 2018. With the effort of different agencies, 4 out of 7 points have been achieved in the 2021 Action Plan. Overall, it indicates that inter-agency coordination and cooperation is a remedy against terror financing (Callimachi, 2017).

4.5. Registration

As per the Financial Action Task Force Guidelines, the government must register the entities trading in virtual currencies. It should be done at the federal level. The trading companies must be held legally bound to the laws and rules of Pakistan. It is imperative to have a ruled-based system for dealing with cryptocurrencies. In his regard, international cooperation is also essential (Blowers, 2015). It is pertinent to mention that international organizations related to cryptocurrency have shown empathy toward the stance of Pakistan. FIA has consulted with Binance to unearth the crypto scam in December 2021 and to explain the company's association with fake ‘online investment mobile applications. These applications were identified as OKIMINI, BB001, HTFOX, MCX, HFC and FXCOPY, to name a few, that were using Binance blockchain addresses for transactions. Binance assured the FIA’s Cyber Crime Wing of its support regarding the matter. The company appointed two of its officials to analyze the matters and to cooperate in the process of investigation. Such steps would be effective in curbing the misuse of cryptocurrency.

4.6. Supervision of the Financial Sector

Government must work to supervise the digital platforms giving access to cryptocurrencies. It is necessary to have a comprehensive market. It would curb the malicious intentions of the terrorist organizations. In this regard, there is a need to have a comprehensive national plan of action. So the role of the State Bank of Pakistan is crucial. For instance, the Reserve Bank of India has been working to devise rules for managing crypto training. Similarly, the US Federal Reserve, Federal Deposit Insurance Corporation and OCC have been working to frame rules.

4.7. Compelling Crypto Currency Providers

The government must build structures to validate transactions through online service providers. Companies should be guided in implementing rule based systems. For instance after 9/11, the US intelligence agencies got access to bank accounts of thousands of people, according to The New York Times. The program was defended on the pretext of public welfare. The situation is quite similar. Companies and organizations can be forced to comply with the government request related to access to the data of the suspects (Lichtblau & Risen, 2006).

5. Conclusion

Terror financing in the digital age has become a grave challenge. Countries should build suitable conditions in which the use of cryptocurrencies can be regulated and there should be proper checks on terror financing. The assistance of the government institutions and private sector, as well as the international organizations, is equally important. The present rules and regulations do

not have the capacity to handle the menace of digital terror financing. It can only be handled through coordinated efforts at all policy levels. This study examines the growing problem of cryptocurrencies being used for terror financing as well as the threats it poses to the financial and economic stability of developing countries like Pakistan. It also highlights the national and international structures and institutions needed to address the danger and to alleviate the problem. It is critical to recognize that, as technology advances, hostile actors will have more access to the digital finance world. This study offered a thorough analysis of the issue to help scholars, decision makers and researchers with better comprehending the situation.

References

Aliens, C. (2016). Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization. *Deep. Dot. Web*.

Ali, A., Hasan, Z. U., Abbasi, Q., & Sulehri, F. A. (2023). Business or Politics: Exploring the Determinants of Policy Mix in South Asia. *Bulletin of Business and Economics (BBE)*, *12*(3), 114-123.

Andreessen, M. (2014). Why bitcoin matters. *New York Times*, *21*.

Baron, J., O'Mahony, A., Manheim, D., & Dion-Schwarz, C. (2015). National Security Implications of Virtual Currency. *Rand Corporation*.

Biryukov, A., & Pustogarov, I. (2015, May). Bitcoin over Tor isn't a good idea. In *2015 IEEE Symposium on Security and Privacy* (pp. 122-134). IEEE

Blowers, M. (Ed.). (2015). *Evolution of cyber technologies and operations to 2035*. Springer International Publishing.

Callimachi, R. (2017). Not'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar. *International New York Times*, NA-NA.

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist use of cryptocurrencies. *Technical and Organizational Barriers and Future Threats, Santa Monica*.

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*. Rand Corporation.

Gowda, N., & Chakravorty, C. (2021). Comparative study on cryptocurrency transaction and banking transaction. *Global Transitions Proceedings*, *2*(2), 530-534.

Hileman, G., & Rauchs, M. (2017). 2017 global cryptocurrency benchmarking study. *Available at SSRN 2965436*.

Lichtblau, E., & Risen, J. (2006). Bank data is sifted by US in secret to block terror. *New York Times*, *23*, 66-205

Marshall, A. (2017). P2P Cryptocurrency Exchanges, Explained. *Cointelegraph. Retrieved March*, *3*, 2023.

Perkins, D. W. (2020). Cryptocurrency: The economics of money and selected policy issues. *Congressional Research Service*, 1-27.

Saeed, M. A., & Sial, M. H. (2023). Issues of Legislation of Cryptocurrency in Pakistan: An Analysis. *Annals of Social Sciences and Perspective*, *4*(2), 429-443.

Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies–a danger for Europe?. *Journal of Money Laundering Control*, *21*(4), 513-519.Torpey, K. (2016). Darknet Customers Are Demanding Bitcoin Alternative Monero. *Bitcoin Magazine*.

Weimann, G. (2018). Terrorism as theater: Mass media and redefinition of image. In *Language and communication in Israel* (pp. 497-518). Routledge.