INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 1

2020

Terrorism Financing Through Crypto-currencies

PRAPTI ALLAGH[1]

ABSTRACT

Terrorism financing is a global phenomenon that not only threatens the security of the states but also undermines the economic development and economic stability and therefore, it is the need of the hour to curb the funding of such organization. The terrorist organizations are directly or indirectly linked to organized criminal groups that engage in the funding of purchase of arms, bombs, narcotics etc. without which the terrorist groups possible cannot function. The track kept by the CTF(Counter Terrorism Finance) on the flow of money through bank accounts reduce the terrorist's access to fiat(the government issued) or the centralized flow of funds and this has raised serious concerns about the use of crypto-currencies such as bit coin to finance their activities. This report focuses on two main points-firstly, how the crypto-currencies are used to finance the terrorist organizations and the international laws which regulate such transactions and secondly, the requirement of criminalization of such activities in India. In this report, we will also analyze the new and future properties of crypto-currencies and what impact can it have on terrorist organizations in the future as it still a developing software. In order to answer these questions, extensive literature review shall be conducted along with scholarly activities and we aim to study the similarities and the differences among different terrorist groups with respect to their finance and if there is a potential for crypto-currencies to finance their operations whether the properties of such currency makes it more viable to be misused along with its legal implications in variety of jurisdictions.

Keywords- *Terrorism, Crypto-currencies, Finance, Organized Crime, Funding*

I. NEED FOR TERRORISM FINANCING

Terrorist organizations range from large state-like organizations like Hezbollah to comparatively small decentralized organizations and self-directed groups and all these organizations require funds to support their activities. From everyday living expenses such as food and shelter to training expenses and purchase of weapons, the funds are required. These

[1] Author is a student at UPES, Dehradun, India.

 [ISSN 2581-9453]

activities are either funded by a third party or by income generated either legally or by illegal proceeds.

The direct costs of mounting individual attacks have been low relative to the damage they may yield. However, maintaining a terrorist network or even a specific cell to provide for recruitment, planning, and procurement between attacks represents a significant drain on resources. Significant infrastructure is required to sustain international terrorist networks and promote their goals over time. Organizations require significant funds to create and maintain an infrastructure of organizational support, to sustain an ideology of terrorism through propaganda, and to finance the ostensibly legitimate activities needed to provide a veil of legitimacy for terrorist organizations.[2] This gives us a reason to believe that if the terrorist organizations were better funded, there might be more successful and larger attacks as that would lead to increased funding for better structures to enable these attacks including recruitment, training and inspiring lone wolves. They would also lead to less monetary pressure which would lead to larger and riskier attacks.

II. 9/11 & BEYOND

Before the crackdown of Al Qaeda after the 9/11 attack, the organization was heavily funded by donations and Islamic Charitable funds which were Zakat (an obligatory annual payment made under Islamic law for religious purposes) and Sadaqah (a voluntary contribution made under Islamic law used for religious purpose). Most of this funding was through a legal channel called the Hawala network and through informal but legal channel using traditional banks or through illegal but difficult to trace channels. The US government was mostly successful in tracing these funds and criminal charges were also bought against those who were involved in Terrorism Financing

The International Convention for the Suppression of the Financing of Terrorism (1999), Security Council resolution 1373 (2001), calls on States to prevent and suppress the financing of terrorism, inter alia, by criminalizing the collection and provision of funds for terrorist purposes, and urges them to set up effective mechanisms to freeze funds and other financial assets of persons involved in or associated with terrorism, as well as to prevent those funds from being made available to terrorists.[3]

The United Nations along with the intelligence and various counterterrorism agencies have

[2] OECD (2019), Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors, OECD, Paris

[3] Factsheet, United Nations Security Council Counter-Terrorism Committee Executive Directorate (Cted), https://www.un.org/sc/ctc/wp-content/uploads/2018/07/ctc_cted_fact_sheet_25_june_2018_designed.pdf

been able to identify the finance strategies used by various terrorist groups and have been effective in curtailing the financing activities.

III. TRADITIONAL METHODS OF TERRORIST FINANCING

An analysis of TF related law enforcement cases and prosecutions in the United States since 2001 found that approximately 33% of these cases involved direct financial support from individuals to terrorist networks.[4] Some of the wealthy private donors also play an important role for some terrorist groups. Secondly, the terrorist organizations target some nonprofit organizations (NPOs) in order to access materials and funds. The report found that traditional transnational terrorist organizations, which mainly attempt to exploit some legitimate NPOs or create 'sham' NPOs, comprise a large number of the cases demonstrating the threat to the NPO sector.[5] Thirdly, the terrorist organizations engage in illegal activities such as bank robberies, smuggling of goods, tax frauds etc. as a means to raise funds. Fourthly, the terrorist groups engage in extorting the local population as a way to sustain their activities.

The 2014 report on the Afghan opiates trade suggests that the Taliban uses funds collected from local populations to sustain local operations, whereas donations go to the Taliban Financial Commission that reports to the senior leadership of the Taliban.[6] Similarly, ISIL extorts the income of all inhabitants in areas where it operates. The 2014 FATF report noted that Iraqi government employees remaining in ISIL territory travel to Kirkuk and elsewhere to withdraw their salaries in cash, and return to ISIL-held territory where their salaries are then "taxed" by ISIL at rates of up to 50%[7] Kidnapping for ransom and self-funding for individual attacks is also a way of generating revenue by the terrorist groups Also several law enforcement investigation have found that some of the legitimate commercial enterprises such as used car dealerships, restaurant franchise where the revue from a terrorist enterprise is routed for supporting the terrorist organizations. A variety of publicly-available sources and national governments have claimed that certain terrorist groups have been, and continue to be, financially supported by a number of national governments.[8] The mere possibility of

[4] US Department of Treasury (2015), p. 44, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[5] FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris,http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

[6] FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, FATF, Paris, http://www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

[7] FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

[8] FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

states funding the terrorist activities is a threat to world peace and security and it also undermines the effectiveness of FATF activities which are conducted to disrupt terrorist financing. For example, the 2014 Afghan drugs trafficking report noted that the Taliban are believed to have used the regulated banking system (as well as money service businesses) to move the proceeds from drug trafficking[9]. Several FATF reports have referred specially to the use of the bank accounts of NPOs to move funds to terrorist organizations.[10] One of the methods used are cash couriers but they are also but the increase of bulk cash smuggling across borders pose a great threat as it seems too risky.

The above traditional methods are still very much prevalent in terrorism financing. Although the Anti-Money Laundering (AML) and Combating the financing of terrorism (CTF) regulations are imposed by the International Monitory Fund in compliance with FATF 40+9 recommendations, the terrorist financing techniques are constantly evolving and a strategic analysis of the evolving risks can help the policy makers in formulating and implementing the necessary legal actions that are required to be taken in order to combat the financing of terrorism which will ultimately lead to reduction of the terrorist activities.

However, this success of CTF in reducing the terrorist activities has resulted in rising of concerns regarding the use of digital currencies by the terrorist organizations to fund their activities.

IV. UNDERSTANDING CRYPTOCURRENCY

The technology of crypto currency is based on cryptography, from where it derives its name as well. Cryptography helps exchanging financial transactions digitally, verify the transfers and secures the creation of every new unit of currency created. Unlike digital currency, which is paperless money, is different from real money since it is operated in decentralized form.

A cryptographic attack allows an attacker to significantly reduce or eliminate the security provided by encryption. This approach is especially powerful in the case of crypto currency and could allow theft, counterfeiting, or almost any other type of attack against the system.[11]

[9] FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, FATF, Paris, p 43, http://www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

[10] FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, FATF, Paris , p 33, http://www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

[11] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorist use of Crypto currencies, Technical and organizational barriers, 2019, 978-1-9774-0234-9, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

It means the transfer taking place between users is in peer-to-peer network of computers. There is no authority to regulate and control over this form of money. While transacting crypto currency, one does not need to take approval from any authority, like in case of banks. Value of units of crypto currency is decided by the market participants without the help of banking institutions, or any transactional guidelines that are adhered by real currencies. Crypto currencies also takes care of its user's privacy by hiding the identity of the individuals dealing in this technology, meaning everyone's privacy remains intact. Basically anyone in the world can create a Bit coin address and start dealing in the exchange of digital currencies without even giving a name or an address.

Cryptocurrencies work with the help of **block chain technology**, which is a complex system that ensures its properly functioning. Cryptocurrencies usually represents itself in form of units which are lodged into a database to determine how much currency is held against each individual name or address. The working is similar to that of banking. Each transaction is recorded in the database and there is no actual physical exchange taking place. The movement of cryptocurrency that is recorded on a platform of 'blockchain' is a peer-to-peer, global distributed ledger that records transactions between members on the blockchain platform without the interference of any third party. The next step is encryption of transactional data which then is distributed across the network. Data has to go through "mining" process which confirms that a transaction is valid and only then is that data recorded permanently. Specialists who do mining are called "miners" who get incentives in a form of block reward, through which new coins are generated.[12] This process is repeated continuously, which provides for a robust and incentivized monetary system called cryptocurrency.

Holders of cryptocurrency with the help of a private key authenticate their identity because of which they exchange and trade units.[13] Such private key, which is formatted as whole numbers between 1 to 78 digits, make them have access to currency. In the absence of any key, the holder cannot spend their cryptocurrency. Losing a private key is like throwing away a wad of cash into a trash. A new key represents a new set of units. However, one main advantage of having a private key is to keep cryptocurrency safe and private.

Therefore, there is an urgent need to understand the potential of technological advancements and sophistication of the terrorist groups.

[12] crypto currency technical explanation, " the ultimate guide to understanding crypto currency", (September 02, 2019, 19:00) https://www.blockchaintechnologies.com/cryptocurrency/

[13] Brian Mariucci, "what is crypto currency- how it works, history, Bit coins alternatives", (September 02, 13:40) , https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

V. INSTANCES WHERE BITCOINS HAVE BEEN USED BY TERRORIST GROUPS:

1. The International Institute of Counter-Terrorism (ICT) in its report titled Identifying Money Transfers and Terror Finance Infrastructure on Monday, January 20, 2020.went in depth to link a Bitcoin address to a high volume transaction which included a webmaster tied to Hamas having used it as a currency to source of funding terrorism in the West Bank. [14] Hamas which controls the Palastinian territory of Gaza originally received its donations from the foreign governments like Qatar. Then the Islamic State of Syria subsisted taxes on the region it controlled. Thus, the organization had its financing curtailed and they reacted to these economic sanctions by saying that they are going to use Bitcoin. [15]

2. A leading sheikh with one of the biggest terrorist groups in Syria, Hayat Tahrir al-Sham, posted a long video to his online followers in July, explaining the origins of Bitcoin and declaring that it is permissible to use for charitable donations, according to a translation of the video by Memri.[16]

3. Due to security protocols by the government and companies like Pay Pal, Moneygram, Western Union and at the same time when major offences against ISIS were well underway which shrinked its territory and removed ISIS from many of its oil fields thus cutting on the financial resources in 2016. These were the perfect circumstances which let to the embracing of crypto by the Jihadists. As the situation worsened as Syria was a virtual dead zone for money transfers and the only real way to get money from the families, friends and supporters was through hawala system which was also a risky process and even less reliable because of heavy monitoring by the Government agencies. Therefore, by 2016, Al Qaeda and ISIS fighters were already calling for donations through cryptocurrencies on social media. [17] By 2017, ISIS had long been receiving Bitcoin donations from all over the world, with numerous cases coming out of the US in places like New York and Virginia.[18] An Israeli blockchain forensic firm has claimed the suicide bombers involved in Sri Lanka during Easter were funded by cryptocurrency.[19]

[14] Dr. Eitan Azani, Dr. Michael Barak, Edan Landau, Nadine Liv, Identifying Money Transfers and Terror Finance Infrastructure, International Institute of Counter Terrorism, 20.01.2020
[15] Nathaniel Popper, Terrorists Turn to Bit coin for Funding, and They're Learning Fast, NY Times, Aug. 18, 2019
[16] Nathaniel Popper, Terrorists Turn to Bit coin for Funding, and They're Learning Fast, NY Times, Aug. 18, 2019
[17] rita-katz, Tales of Crypto-Currency: Bit coin Jihad in Syria and Beyond, thedailybeast.com, Oct. 13, 2019
[18] rita-katz, Tales of Crypto-Currency: Bit coin Jihad in Syria and Beyond, thedailybeast.com, Oct. 13, 2019
[19] yashu-gola, Breaking: ISIS Used Bit coin to Fund Horrific Sri Lanka Easter Bombings, Research Claims, May 2, 2019, https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/

From the above instances, it can be clearly observed that cryptocurrencies are the biggest potential for the terrorists to facilitate their finance operations

A study was conducted by RAND.ORG where organizations like ISIS, Al Qaeda, Hazbollah and lone wolf attackers were the groups studied and five activities were taken into account being fundraising, illegal drug and arms trafficking, remittance and transfer of funds, attack funding, and operational funding.. The properties of cryptocurrency in importance of facilitating these activities were evaluated. Features such as anonymity, usability, acceptance and reliability were studied on the above activities and it was found that cryptocurrencies would make a much more viable meathod of financing the terrorist activities. [20]

VI. HOW IS THE CRYPTOCURRENCY USED TO FUND TERRORISM?

In order to understand the potential use of cryptocurrencies by the terrorists, we need to look back and analyze how had it been used earlier so that the future use can be prevented and regulations could be made accordingly. Actual use of cryptocurrency started back in 2016 when ITMC (Ibn Taymiyyah Media Center), a jihadist group based in Gaza launched a public crowdfunding donation campaign using cryptocurrency. It named its campaign Jahezona[21]. ITMC promoted it on platforms like Twitter, YouTube, and Telegram, posting a Bitcoin address to which donors could send funds.[22] Over the two years the fundraising campaign ran, ITMC received tens of thousands' worth of cryptocurrency across more than 50 individual donations, with a notable spike in June 2017.[23] This may seem an insignificant amount of donation but this was just the beginning of the modern way of financing of terrorism and in 2019 one of the biggest terrorism financing campaign through cryptocurreny was discovered. Izz ad-Din al-Qassam Brigades (AQB) solicited donations in Bitcoin using a very sophisticated way of receiving donations by generating a new address for every donor and generated tens of thousands of dollars of bitcoins which makes it difficult to identify addresses and transactions associated with these addresses. Therefore, because of increased banking regulations and FATF requirements after the 9/11 attack, the donors refrain from donating because of the legal and financial risks involved. This is why these groups are rely on the receipt of crypto donations.

[20] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorist Use of CryptocurrenciesTechnical and Organizational Barriers and Future Threats, 2019,
[21] ariel-ben-solomon, Gaza-based pro-ISIS group urges Muslims on social media to donate for weapons, The Jerusalem Post, June 25 2016,
[22] Chainalysis, 2020 Crypto Crime Report
[23] Chainalysis Team, Terrorism Financing in Early Stages with Crypto currency But Advancing Quickly, January 17, 2020, https://blog.chainalysis.com/

Once these funds are generated, the terrorist organizations need to manage the funding and this is a fairly challenging task as one needs technical expertise to manage crypto funds effectively. As noted by the Financial Action Task Force (FATF), large organizations rely on relatively sophisticated financial infrastructure with multiple levels of management, reporting and accounting, and financial planning.[24] The third and the most critical challenge is the way the virtual currency is spent as the topmost priority is to maintain anonymity and to avoid large transactions as they seem suspicious. Also it is difficult to separate licit operations and expenses, such as salaries and social services, from clearly illicit spending, such as terrorism recruitment and training, because of the lack of information about and the close relationship between these activities, and especially because the legitimate activities create incentives and inducements to illegal actions.[25]

However, even though there are "still only a small number of publicly-documented and confirmed cases of TF [terrorist finance] involving VCs [virtual currencies],"[26] it can be seen that the major terrorist organizations such as ISIS, Al Qaeda and Hamas fall under the confirmed cases. It can be conferred that these organizations are extremely dynamic and are getting more sophisticated and technologically advanced in their methods. This indicates a potential and a challenging threat of the use of virtual currency in the near future and thus the cryptocurrency must be regulated. We will further discuss the regulatory frameworks, both internationally as well as within India with regard to the dealings in crypto crime in relation with financing of terrorism.

VII. REGULATION OF CRYPTO CURRENCY IN DIFFERENT JURISDICTIONS

A report provided by the United States Government in June 2018 on the Regulation of Crptocurrencies by various jurisdictions said that one of the most common actions identified across the surveyed jurisdictions is government-issued notices about the pitfalls of investing in the cryptocurrency markets. [27] These warnings are given to the citizens of the countries around the world to educate them on the fact that the cryptocurrency is not centralized and is not guaranteed by the state and thus the citizens investing in this currency are doing so on their own risk which means that there is no legal recourse available to them when they are at

[24] FATF, Emerging Terrorist Financing Risks, Paris: Financial Action Task Force and the Organization for Economic Co-operation and Development, October 2015.
[25] Eli Berman, Radical, Religious, and Violent: The New Economics of Terrorism, Cambridge, Mass.: MIT Press, 2009
[26] 5 Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses, Brussels: European Parliament, 2018, p. 9.
[27] Staff of Global Legal Research Directorate, Regulation of Crypto currency Around the World, June 2018, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

a loss. Some of the countries surveyed go beyond simply warning the public and have expanded their laws on money laundering, counterterrorism, and organized crimes to include cryptocurrency markets, and require banks and other financial institutions that facilitate such markets to conduct all the due diligence requirements imposed under such laws.[28] For instance, Australia, Canada, and the Isle of Man recently enacted laws to bring cryptocurrency transactions and institutions that facilitate them under the ambit of money laundering and counter-terrorist financing laws.[29] Some of the jurisdictions such as Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam have banned any activities involving cryptocurrency. On the other hand there are countries like Spain, Belarus, the Cayman Islands, and Luxemburg which have not recognized cryptocurrency as a legal tender but see a potential in the technology behind it and are developing a cryptocurrency-friendly regulatory regime as a means to attract investment in technology companies that excel in this sector[30]. There are countries like Marshall Islands, Venezuela, the Eastern Caribbean Central Bank (ECCB) member states, and Lithuania who seek to develop their own system of cryptocurrency.

VIII. REGULATORY FRAMEWORK REGARDING CRYPTOCURRENCY IN INDIA

The government of India stated in early 2018 that cryptocurrencies such as bitcoin are not legal tender in India[31] thus banning the fianancial firms and induviduals from trading in crytocurrency. While the government has not yet enacted a regulatory framework for cryptocurrencies,[32] the Reserve Bank of India (RBI) has advised caution on their use and has issued three notifications596 that "cautioned users, holders and traders on the risk of these currencies and clarified that it has not given any licence or authorisation to any entity or company to operate such schemes or deals.[33]

The decision of RBI to ban the virtual currencies in India was challenged by various petitions and thus even though a draft bill was pending to be passed in both the houses under which all the activities relating to crytocurrencies were punishable with a fine or imprisonment of upto

[28] Staff of Global Legal Research Directorate, Regulation of Crypto currency Around the World, June 2018, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
[29] Staff of Global Legal Research Directorate, Regulation of Crypto currency Around the World, June 2018, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
[30] Staff of Global Legal Research Directorate, Regulation of Crypto currency Around the World, June 2018,https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
[31] P. Suchetana Ray, Gov. Plans to Bring in Law to Regulate Crypto currency Trade, Forms Panel, HINDUSTAN TIMES (Jan. 14, 2018), https://www.hindustantimes.com/india-news/government-plans-to-bring-in-law-to-regulatecryptocurrency-trade/story-SpAO63DDfk6Gg7lo5yNKCJ.html, archived at https://perma.cc/6HLK-G9LD.
[32] Seema Jhingan et al., LexCounsel Law Offices, India: Legal Status of Virtual Currencies/Crypto currencies in India, MONDAQ (Apr. 6, 2017), http://www.mondaq.com/india/x/583670/fin+tech/Legal+Status+Of+Virtual+
[33] Vivina Vishwanathan, Bit coin Regulations in India, LIVEMINT (Dec. 21 2017), http://www.livemint.com/

5 years. The Supreme Court in *Internet and Mobile Association of India*[34] found that while RBI has the power to regulate the virtual currencies but the Circular of April 2018 was disproportionate and thus it was ultra vires the Constitution and therefore, it uplifted the ban imposed by RBI on the trading through cryptocurreny. According to Supreme Court, since there was absence of any legislative provision, the ban on the use of crytocurrency violated Article 19(1)(g) of the Constitution. But the RBI is planning to file a Review petition on this Judgment. Some major concerns arise regarding the financing of terrorism in India along with this Judgment uplifting the ban on the use of crytocurrency impsed by the RBI.

As compared to Middle East where the internet infrastructure is poor which discourages the terrorist from using Bitcoins, India has a much better and advanced internet infrastructure along with better IT skills and the use of currencies like Zebpay are on a rise. It is a bitcoin exchange reported that in the last months of 2017, they were adding 300,000 to 400,000 users on its exchange every month as compared to 150,000 in June and July. Also, a vast flourishing network of grey-market and the underground economy already exists. A few years back, radioactive mineral cobalt-60 ended up in Delhi's scrap market, from Delhi University and was being sold in Delhi's greymarket[35]. India is in a unique position in that it provides a fertile ground for all kinds of illicit activities on the 'darkweb', including money laundering and terror financing through virtual currencies [36]. If this is the scenario of organized crime on the dark web, it would be a cake walk for the terrorist to make India the hub for the use of crytocurrency to finance terrorism. India could also be a hub for cryptocurrency because of it being legal due to the 2020 Judgment as the grey market and underground economy of India already flourishes in terms of trade of illicit material including Bombs, weapons and drugs. Moreover India's financial regulatory structures, and AMP/CTF monitoring and surveillance capabilities are not sufficiently developed.[37] The law-enforcement agencies and intelligence agencies are understaffed, poorly equipped and insufficiently skilled to tackle such high-tech cases of cyber fraud and disruption[38]

[34] Writ Petition (Civil) No.528 of 2018

[35] Abhinav Pandya, India needs to check the use of crypto currencies in terror funding, Economic Times, Aug 06, 2018, https://economictimes.indiatimes.com/news/defence/india-needs-to-check-the-use-of-cryptocurrencies-in-terror-funding/articleshow/65290424.cms?from=mdr

[36] Abhinav Pandya, Crypto currency- A new Scourge of terror Financing, August 2018, https://www.vifindia.org/sites/default/files/Cryptocurrencies-A-New-Scourge-of-Terror-Financing.pdf

[37] Abhinav Pandya, Crypto currency- A new Scourge of terror Financing, August 2018, https://www.vifindia.org/sites/default/files/Cryptocurrencies-A-New-Scourge-of-Terror-Financing.pdf

[38] Nupur Anand, "The Ongoing Bit coin Boom is Drawing Indian Investors like Never Before," Quartz.November,2017. https://qz.com/india/1141021/the-bitcoin-boom-is-drawing-indian-investors-like-never-before/

IX. INTER-MINISTERIAL COMMITTEE ON CRYPTOCURRENCY

In November 2017, high level ministerial committee was constituted to look upon the issues associated with digital currencies. Committee submitted its report in February 2019 and the same was realised in July 2019. Few Key recommendations are as below[39]:

- Since no other country accept virtual currency as a legal tender, in India cryptocurrencies, other than government-backed currency, should be banned and trading in cryptocurrency should be criminalised.
- Keeping in mind the positive aspect of digital market and its need, a lot of infrastructural investment would be required such as a high computation power and high electrical requirements. A committee should be set up to look after an appropriate model for cryptocurrencies and its working.
- There are certain issues with this technology that does not make it replace traditional currency. Issues include (i) there decentralised nature which makes them difficult to regulate; (ii) these transactions cannot be reversed i.e. there is no redress to wrong transactions; (iv) cryptocurrencies are more vulnerable to money laundering and terrorist funding activities; (v) crypto currencies have market fluctuations in their value.
- Technology used in cryptocurrency has several plus points as well. It includes detection of dual transactions which would help in keeping a check on fraud. According to the committee, the Department of Economic Affairs should understand the underlying technology to exploit its uses at the most.

X. DRAFT OF CRYPTOCURRENCY REGULATIONS BILL, 2019

The draft bill was proposed by the Inter-Ministerial committee suggesting criminalizing the activities and the key features of the bill include:

- **Definition of cryptocurrencies and mining:** Cryptocurrency is any information, number, token or code that represents a value digitally which is exchanged with or without any consideration on a promise that it will have a utility value in business activities whereas "mining" is defined as a process that validates cryptocurrency transactions and further creates new crypto currencies.[40]

39"Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019"; "Bills and acts"; "PRS Legislative Research"; (September 22, 2019, 20.38), https://www.prsindia.org/billtrack/draft-banning-cryptocurrency-regulation-official-digital-currency-bill-2019

40 "Gov. committee recommends ban on crypto currency in India Gov. committee recommends ban on crypto currency in India"; "India Today"; (September 22, 2019, 21:04); **https://www.indiatoday.in/technology/news/story/govt-committee-recommends-ban-on-**

- **Prohibition of the activities:** The bill suggests the non-use of cryptocurrencies and a legal tender in India i.e. prohibition buying selling trading holding mining issuance and disposal of cryptocurrencies. The bill prohibits use of cryptocurrencies as (i) a medium of exchange (ii) for paying bills (iii) for providing registrations, selling, clearing or trading of cryptocurrencies to individuals (iv) a basis of credit (v) trading it with another currencies (vi) a means of raising funds and investments.

  However the bill allowed use of cryptocurrency for the purpose of experiment or research or teaching.

- **Penalties:** The following table shows the suggested penalties to related offences:

Punishment of fine and imprisonment for up to 10 years or both for: offense of using cryptocurrency for trading, issuing, holding or mining purposes.

Punishment of fine and imprisonment for up to 7 years or both for: offense of advertising, soliciting or assisting participation in cryptocurrency.

Fine incase of acquiring or storing cryptocurrency

For any subsequent commitment of any offense, there shall be imprisonment of 5-10 years plus fine. And any further attempts to commit offences would be punished with 50% of the maximum punishment assigned to such offense. All fine bound offenses should be compoundable and offences related to issuing financial products and use of cryptocurrency to raise funds and investment shall be cognizable and non-bailable. All other offences should be non-congnisable and bailable.

Maximum fine that could be levied will be higher of either the three times the loss caused or three times the gain made by the person. If these two cannot be determined then in such cases, the fine shall be upto one lakh rupees for offenses related to storing disposing acquiring of cryptocurrencies and for all other offenses, fine upto 25 lacs. To bring affect to such offenses, an amendment to prevention of money laundering act, 2002 should be made.

- ***Investigation process:*** Deputy Superintendent of police or higher rank officer may have investigation powers under the bill.
- ***Regulation of digital rupee:*** Under the bill, CG., in consultation with RBI, approve virtual digital currency as a legal tender and foreign digital currency as foreign currency in India which would in that case be governed by Foreign Exchange Management act, 1999.

 [ISSN 2581-9453]

- ***Exemptions and Immunity:*** CG. will have powers to grant immunity to any person from prosecution under the Act if such person discloses about the violation similarly, any activity can also be exempted from purview of the Act. However, the same shall be in public interest.
- ***Transitional Period****:* the bill provides a transition period of 90 days from the date of commencement of the act, which would allow any person to dispose of any cryptocurrency in their possession.

Since the Supreme Court of India upheld the plea by *Internet and Mobile association of India*[41], it lifted the ban on virtual currencies which was imposed by RBI in Paragraph 13 of the circular asked entities governed by RBI not to deal with – or give services to – any person or business organizations dealing with or transacting in virtual currencies.[42] The popular interpretation of this judgment would be the legitimization of the virtual currency which means that the trading in cryptocurrency would now be legal but n its judgement, the court observed, "It is no doubt true that the Reserve Bank Of India has pervasive powers not only in view of the statutory design but also in view of the special status and role that it possesses in the economy of India. These powers can be applied both in the form of preventive as well as curative measures."[43]

The "Banning of Crypto currency and Regulation of Official Digital Currency Act", the draft bill is yet to be presented in front of the legislature. If passed, it could make buying, selling, mining, and even holding of cryptocurrency a punishable offence. [44] And therefore, the interpretation of the judgment legitimizing the use of cryptocurrency in India could be changed as Court stated that RBI did not give any imperical data of the damage caused by the use of Cryptocurrency exchanges. The above report on how the India can become the potential hub for the terrorist to use cryptocurrency in financing the terrorist activities indicates that there is infact sufficient damage that can be caused by cryptocurrency if it is legitimized in India.

[41] Writ Petition (Civil) No.528 of 2018

[42] Vishal Chawla, SC VERDICT ON LIFTING CRYPTOCURRENCY BAN IN INDIA MAY BE MISINTERPRETED, AND WE MAY SEE THE BAN REINSTATED, 8th July 2020, https://analyticsindiamag.com/cryptocurrency-ban-india-verdict/

[43] Vishal Chawla, SC VERDICT ON LIFTING CRYPTOCURRENCY BAN IN INDIA MAY BE MISINTERPRETED, AND WE MAY SEE THE BAN REINSTATED, 8th July 2020, https://analyticsindiamag.com/cryptocurrency-ban-india-verdict/

[44] Vishal Chawla, SC VERDICT ON LIFTING CRYPTOCURRENCY BAN IN INDIA MAY BE MISINTERPRETED, AND WE MAY SEE THE BAN REINSTATED, 8th July 2020, https://analyticsindiamag.com/cryptocurrency-ban-india-verdict/

XI. Conclusion – The present and the uncertain future of cryptocurrency in India:

Despite of mixed reactions coming along, there are already instances which show how bleak and dark future cryptocurrency holds in India. Koinex, a leading cryptocurrency exchange in India has already been shut down in June 2019 reasoning the disruptions and uncertainty of cryptocurrency in India. Similarly, Zebpay, another India's largest exchange which is responsible for starting cryptocurrency, shut down in September, 2018. In 2018, RBI banned banks and e-wallets from providing any services to the businesses or individuals who trade in virtual currencies. At the other parts of the world, in U.S, in February 2018, JP Morgan is the first bank that tested a digital coin that is pegged to the U.S Dollar representing the amount held in the accounts. Singapore too is testing the ways to use digital currency across blockchain platforms. Denmark recently had internal elections to remove rigging and bring transparency using the blockchain platform.

There is still no clarity on the part of the government as of now. Every technology has its own pros and cons and a wise act is to consider both of them than to just be bias against banning it. India's technology is still evolving and until there is a way to track or prevent the crypted transactions by the terrorist organizations, there should be a blanket ban on the cryptocurrency. For example, the U.S. Treasury "has access to unique financial data about flows of funds within the international financial and commercial system," which is invaluable for tracking illicit flows of money.[45] And even though deanonymization is always plausible because of the advancement in technology, until it is achieved we cannot underestimate the sophistication and brilliance of the terrorist minds and till then the plausibility of the use of cryptocurrency in financing terrorism should be continuously monitored. The dynamic and uncertain natute of cryptocurrency creates more challenges as it allows the terrorist groups to circumvent monitoring and on the other hand in money laundering where sophistication matters , use of cryptocurrency makes it harder to detect. As it indicates, the terrorist groups are evolving both in creative methods and technicality, the CTF needs to evolve accordingly and the countries need to regulate the policy changes accordingly.

XII. Suggestive Analysis

1. Complete ban: A complete ban on cryptocurrency is not the only solution to resolve the problem of terrorism financing as it will create a great concern for those who see this as a way to evade the shortcomings of traditional financial institutions and those of state control.

[45] Zarate, 2013, p. 137

It will also make it impossible to track any suspicious transactions as the users will become more discreet and untraceable due to the ban. there are already 50 lakh traders involved and implementing the bill brings out a great challenge before the government. If the bill gets passed, over 5 million Indians will have to dispose their holdings and lose years of wealth time and energy invested into it. It is a major reason to consider the bill for any modification and settle at a midway against completely banning it.

2. Central Bank Digital Currency (CBDC): In India, the draft bill proposes to introduce only government backed cryptocurrency. The same solution has been adopted or considered by many other countries. Recently, Venezuela has launched its own currency, Petrodollar. CBDCs are digital currencies which are regulated by a central government. By this the cryptocurrency loses its property of being a decentralized currency. They don't aim to become decentralized like most cryptocurrencies — instead, they simply represent fiat money, only in a digital form. Each CBDC unit acts as a secure digital equivalent of a paper bill and is normally powered by blockchain or some other form of distributed ledger technology (DLT).[46] However CBDCs have certain advantages and will lead to reduction in terrorism finance because of the regulatory framework that will establish the rules of trading. But on the other hand, the privacy and anonymity will be lost and the authorities will have complete control over the data of transactions and the cryptocurrency will just become a modern way of digital banking. So this solution is also not completely viable one.

3. De anonymization: There is another possibility of tracking suspicious transactions done by cryptocurrency for terrorism financing. De anonymization is a data mining strategy where the anonymous data is cross referenced with another data to re-identify the anonymous data source. For example In Zcash there is a record of logs of transactions where the IP address, time and place of transaction are recorded. This is called an audit trail and the transactions will not be regulated by a central authority but will be recorded and thus this will prevent any illegal transactions as there will be a certain level of accountability. If the cryptocurrency regulatory bill makes this feature a compliance to in all the cryptocurrencies, the suspicious transactions can be tracked. This might make cryptocurrencies much less hospitable for the terrorist organizations to finance their activities.

If the law enforcement agencies like the CBI and CTF coordinate with the cyber security domains, de-anonymization is possible and the cryptic transactions can be tracked without

[46] stephen-oneal, CBDCs of the World: The Benefits and Drawbacks of National Cryptos, According to Different Jurisdictions, June 19 2019, https://cointelegraph.com/news/cbdcs-of-the-world-the-benefits-and-drawbacks-of-national-cryptos-according-to-different-jurisdictions

any government backed currency and without imposing a complete ban on cryptocurrencies. The two domains have earlier coordinated to track child pornography, drug smuggling and money laundering. Its high time the concerns of financing of terrorism through crypto currencies be taken seriously as along with the evolution of technology, the terrorist organizations are also advancing technically and so should our law enforcement agencies and regulations.

*****

 [ISSN 2581-9453]