International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 8 Issue 5 May - 2024, Pages: 123-128

Cryptocurrencies and Jihadi Terrorist Financing: Potentials and Challenges.

Princewilliams Odera Oguejiofor

Department of Political Science,Nnamdi Azikiwe University Awka,
Anambra State, Nigeria.
po.oguejiofor@unizik.edu.ng
ORCID: https://orcid.org/0000-0001-8008-4467

Abstract: *This conceptual study examines the potential and challenges of using cryptocurrencies for terrorist financing by jihadi groups through the lens of network theory. By conducting a literature review, content analysis, and scoping review, the research synthesises data from academic sources, reports, and online repositories. The study finds that while anonymity and decentralisation of cryptocurrencies raise concerns about terrorist exploitation, several technological, regulatory, and ideological barriers have limited their widespread adoption for illicit financing so far. Key impediments include technological complexities, a lack of true anonymity, difficulties in converting cryptocurrencies, extreme volatility, and cultural factors favouring traditional financing methods. The analysis concludes that, over the near-term, cryptocurrency use by jihadists will likely remain confined to technologically sophisticated plotters. However, counterterrorism efforts must maintain vigilance as cryptocurrency adoption grows globally. Implementing robust monitoring mechanisms and regulations is recommended to mitigate emerging threats.*

Keywords: Cryptocurrencies, Jihadi Terrorists, Terror financing, Network theory.

Introduction

In the shadowy digital underworld where numbers dance in cryptic cyphers, a digital frontier rife with intrigue and speculation. The anonymous whispers of encrypted transactions echo through the ether, fuelling both hopes of financial liberation and fears of nefarious exploitation. In this labyrinth of decentralized ledgers, some envision a path for the clandestine flow of funds, evading the watchful eyes of authority. Yet, beneath the veil of anonymity, a complex tapestry of technological hurdles, ideological divides, and regulatory scrutiny weaves a narrative that challenges such notions. The volatility of these digital assets, akin to a mercurial tempest, further casts doubt upon their viability for illicit purposes. Thus, the stage is set for a captivating discourse, where the realms of finance, technology, and security collide, leaving us to ponder the enigmatic potential and perils of this enigmatic digital frontier.

The rapid growth and proliferation of cryptocurrencies over the past decade have indeed led to significant changes in the global financial landscape. It is projected that the worldwide cryptocurrency market will experience a compound annual growth rate (CAGR) of 12.5% between the years 2023 and 2030 (Grand View Research, 2024). The global cryptocurrency market cap currently stands at $2.49 Trillion (CoinGecko, 2024). The expanding adoption of distributed ledger technology and the increasing prominence of AI-based cryptocurrency platforms are anticipated to propel the cryptocurrency market's growth during the forecast period (Grand View Research, 2024).

The decentralised, anonymous, and transnational characteristics of cryptocurrencies have presented novel security challenges and concerns on a global scale. The dearth of regulation surrounding cryptocurrencies gives rise to apprehensions regarding their security. Crypto exchanges are susceptible to a multitude of malicious and illicit activities, including cyber-attacks, system malfunctions, data leaks, financial breaches, hacks, and malware, due to their digital nature (Collier, 2021). The volatile nature of these digital assets remains a considerable risk, frequently exceeding that of traditional investment options. The quick rise of crypto exchanges and organisations that did not practise proof of reserves, a lack of self-custody, and the significant volatility of crypto assets have all contributed to the industry's insolvency risk (Natarajan, Martínez, & Iavorskyi, 2023). Additionally, the legal classification of a cryptocurrency asset may be intricate. Since cryptocurrency is composed primarily of cryptographic code, the legal classification of these assets becomes a concern. Is it currency, property, security, or something else? The matter at hand lacks universal agreement, and the ability to obtain a restraining injunction against an insolvent company may be impacted by the classification of this asset, contingent upon the applicable jurisdiction and the agreement reached by the involved parties (Natarajan, Martínez, & Iavorskyi, 2023).

Furthermore, the (supposed) anonymity of crypto assets leaves regulators with data voids, which may be manipulated for illicit purposes. While it may be possible for authorities to trace illicit transactions, it may be more challenging to ascertain the identities of the involved parties. Complicating matters further is the fact that the cryptocurrency ecosystem is governed by diverse regulatory frameworks in various nations. For instance, the majority of transactions on cryptocurrency exchanges are conducted by entities based predominantly in offshore financial centres. This renders oversight and compliance not only arduous but practically unattainable, in the absence of global cooperation trillion (Drakopoulos, Natalucci, & Papageorgiou, 2021).

The arguments adduced above have led a good number of scholars to predict and speculate that cryptocurrencies will be increasingly be adopted by terrorists especially Islamic jihadi terrorists for terrorist financing in order to avoid the hassles attached to doing so through the traditional regulated financial institutions. The operational foundation for terrorist groups is fundamentally rooted in terrorist financing, which dictates their ability to execute terrorist acts (Wang & Zhu, 2021). International bodies such as the Financial Action Task Force (FATF), the International Monetary Fund (IMF), the United Nations, the World Bank, among others, have been instrumental in the rigorous suppression of terrorist financing (Wang & Zhu, 2021). Concurrently, these organisations have been proactive in aiding less developed regions to bolster their financial infrastructure and undertake counter-terrorism measures. This study thus investigates whether cryptocurrencies are intrinsically and extrinsically viable options for jihadi terrorist financing.

Theoretical Framework: Network Theory

This article employs the network theory as the guiding theoretical framework. Network theory, popularized by Robert Metcalfe, highlights how the value of a network increases as more users join (Emerging Technology from the arXivarchive, 2018). For cryptocurrencies, gaining popularity and establishing themselves as viable alternatives to established financial systems is dependent on network effects (DEFIX SOLUTIONS, 2023). Cryptocurrencies, by their very design, create a global network of transactions that transcend traditional financial and geographical boundaries. This network-based structure enables the rapid movement of funds and the potential for the exploitation of vulnerabilities in the system (Serena, Ferretti, & D'Angelo, 2021).

In contrast to traditional banking systems, cryptocurrencies make use of distributed ledgers to store their data. This allows the information to be decentralised and eliminates the risk of having a single point of failure. Blockchain technology, also known as distributed ledger technology (DLT), is a database that is both immutable and decentralised. It is the responsibility of the nodes that are engaged in DLT administration and update activities to verify the consistency and integrity of the data, which in turn ensures that the system is accurate. Because distributed ledger technologies (DLTs) are permissionless networks, active involvement in the vast majority of DLTs does not require prior authorization (Serena, Ferretti, & D'Angelo, 2021).

Diverse implementations of a distributed ledger are possible, but the majority of cryptocurrencies utilise the blockchain, a data structure that records transactions in blocks, which are logically interconnected via cryptographic methods. A consensus strategy is an essential component of every cryptocurrency, facilitating agreement among all system nodes regarding the current state of the distributed ledger. In this regard as well, various schemes are feasible; however, the prevailing implementations employ the so-called Proof of Work (PoW), which necessitates the resolution of computationally demanding crypto puzzles to authenticate the blocks and transactions they comprise. "Mining" is the process by which cryptographic puzzles are solved. Bitcoin, which was introduced to the market first, continues to be the most well-known and widely utilised cryptocurrency. Recently, Ethereum has also acquired popularity because it enables the execution of "smart contracts," which are actual contracts written in code, in addition to simple transactions (Serena, Ferretti, & D'Angelo, 2021).

Users are typically identified with addresses that are generated using their public cryptographic key in the majority of systems. Correlating these addresses with the true identities of the users is not a straightforward task. Thus, it is possible (and frequently occurs) for a single account to be associated with multiple addresses and for certain users to have control over multiple accounts (Serena, Ferretti, & D'Angelo, 2021). This network-based structure and the (supposed) anonymity of crypto assets enable the rapid movement of funds and the potential for the exploitation of vulnerabilities in the system. The salient question becomes, are these perceived vulnerabilities good enough reasons to believe that crypto terror financing is possible?

Cryptocurrency and Terrorist Financing

Cryptocurrency has been utilised by terrorist organisations for illicit trading of substances such as drugs and weapons on the black market. An instance of this is the dark web platform 'Fund the Islamic Struggle without Leaving a Trace', which facilitates the transfer of bitcoins to jihadists. Extremists have even authored a book, Bitcoin wa Sadaqat al Jihad, that provides explicit instructions on how to send bitcoins from North America and Western Europe to jihadists (Weimann, 2016). Bahrun Naim, who orchestrated the 2016 terrorist attacks in Jakarta, reportedly used Bitcoin to transfer funds to militants and finance terrorist activities (Hasbi & Mahzam, 2018).

Furthermore, Islamic law is yet to have a definite stand on the use of Bitcoin and other cryptocurrencies.

> "National "sharia authorities" have not ruled on whether cryptocurrencies are permissible, and while several global bodies recommend standards for Islamic finance, none has the authority to impose them. Many governments seem ambivalent, worried about the potential for instability, but unwilling to lose the chance of benefiting from new technology." (AlJazeera, 2018).

This ambiguity has led to some acceptance of cryptocurrency as an alternative to conventional financial systems and legal tender among a section of the global Muslim population. In 2015, an American teenager confessed to instructing members of the Islamic

State on Bitcoin usage. He offered advice on creating bitcoin wallets for potential donors and using the 'dark wallet' service (Irwin & Milad, 2016).

The Islamic State has been known to kidnap and extort Europeans in Syria, using Bitcoin as a tool for ransom payments. This method allows terrorists to raise and transfer funds, which are subsequently used to finance terrorist attacks in Europe (Teichmann, 2018). There are also numerous accounts of terrorists exploiting cryptocurrency in online blackmail schemes. For instance, a company was threatened with the disclosure of its data unless a ransom of 1,000 BTC was paid (Hampton & Baig, 2015).

In 2016, the Lincoln Group's computers were compromised by ransomware, with the criminals demanding a Bitcoin ransom equivalent to 500 USD, although this attempt was unsuccessful. In 2015, three Greek banks were threatened with blackmail, with the culprits demanding Bitcoin payments amounting to hundreds of thousands of euros (Brown, 2016).

The Weaknesses of Cryptocurrency Terror Financing

Despite the widespread apprehension that digital currencies could become a primary conduit for terrorist funding and potentially facilitate actual terrorist attacks, the evidence supporting this notion is limited. Following the November 2015 Paris attacks orchestrated by the Islamic State, there were unconfirmed speculations that bitcoin partially financed the assault. Similar unverified reports emerged in the wake of the Easter 2019 terrorist attacks in Sri Lanka, but these were later deemed baseless (Davis, 2019). One of the few documented instances of a terrorist attack funded through cryptocurrency was the July 2016 assault on the Solo Police Headquarters in Indonesia. Reports suggest that the attack's orchestrator, a deceased militant based in Syria named Bahrun Naim, utilised PayPal and bitcoin to transfer funds for the attack. Even though the total amount Naim transferred for the attack was relatively modest – under $1,000 – it signified a novel approach in jihadist operational financing (Arianti & Yaoren, 2022). In more recent racially or ethnically motivated violent extremism (REMVE) and anti-government, anti-authority violent extremism (AGAAVE) attacks, the assailants have opted not to use cryptocurrencies, instead leveraging other fintech platforms, such as PayPal, to fund their attacks. For example, the Buffalo shooter used funds from his bank account and his PayPal account to finance some of his weapons and equipment purchases. He also sold some of his personal items at flea markets to raise additional funds for further purchases, deliberately avoiding the use of cryptocurrency for any aspect of his attack's financing (Davis, 2022).

Cryptocurrency and other disruptive financial technologies have not been extensively utilised to fund jihadist attacks for a variety of reasons that span the political and ideological spectrum and apply to all group types. Initially, there are still technological hurdles to overcome in using cryptocurrency. Despite the fact that cryptocurrency has been around for more than ten years, acquiring it in certain jurisdictions can be difficult. Numerous banks forbid the transfer of funds to exchanges, and some nations have begun to outlaw cryptocurrency ATMs (Argentino, Davis, & Hamming, 2023). To begin the use of cryptocurrencies, there are technical jargons that must be understood in order to make utility seamless, and there are even greater obstacles to truly anonymous usage. Also, The U.S. Department of Justice has successfully dismantled several sophisticated online fundraising campaigns run by U.S.-designated terrorist organizations that were using cryptocurrencies. This underscores the vulnerabilities of these networks and provides valuable lessons for future attempts at terrorist financing (Mines & Margolin, 2020).

Secondly, cryptocurrency transactions are not as anonymous as advertised. A study by Buczak (2024), posits that the anonymity of users is potentially compromised due to the fact that each user possesses a public address that could, in theory, be traced back to an exchange account or IP address through network analysis, thereby unmasking the user's actual identity. For example, if a bitcoin address is associated with an individual's identity, bitcoin offers no privacy since the ledger is public and easily accessible. The study exposes further that there exist several methods to associate digital wallet addresses with individuals' identities. One such method is through the enforcement of Know Your Customer/Anti-Money Laundering policies by major cryptocurrency exchanges. Another method, as previously mentioned, involves blockchain analysis, which includes address clustering as a viable technique. The bitcoin ledger contains data on the balance of each account. Therefore, if an individual's identity is linked to their digital wallet, their bitcoin balance becomes publicly known. "It is a myth that bitcoin and other public ledger-based cryptocurrencies are anonymous" (Buczak, 2024).

Thirdly, converting cryptocurrency into state-backed currency or using it to buy weapons or components for attacks can be technologically challenging and time-consuming, and it can expose a user to potential theft. Although "informal" exchanges are beginning to incorporate cryptocurrencies in places like Syria and Afghanistan, this is still a limited phenomenon (Argentino, Davis, & Hamming, 2023).

Furthermore, one of the key reasons jihadist groups may be less likely to adopt crypto terrorist finance is the cultural and ideological factors that shape their approach to finance and fundraising. Many jihadist groups, such as the Islamic State (IS), have historically relied on more traditional methods of fundraising, such as extortion, kidnapping, and the exploitation of natural resources (Europol, 2021). These groups may be less likely to adopt new and unfamiliar financial technologies, such as cryptocurrencies, that are perceived as being at odds with their cultural and religious beliefs (Fisher, Prucha, & Winterbotham, 2019).

It is also noteworthy that cryptocurrency has been beset by a succession of fraudulent transactions, theft of inadequately protected funds, and comparable incidents since it acquired value. A portion of these security infringements can arguably be attributed to user mistakes and misplaced confidence, yet they continue to provide evidence to many observers that cryptocurrency is insecure (Dion-Schwarz, Manheim, & Johnston, 2019). Additional issues reveal inherent weaknesses in the standard use of the system: The use of unencrypted wallets on machines connected to the internet and the reuse of addresses are now recognised as regrettable errors. If similar problems persist in being identified and exploited, confidence in cryptocurrency systems will likely remain diminished, which will make it very unattractive for terror financing (Dion-Schwarz, Manheim, & Johnston, 2019).

Lastly, the extreme volatility of many cryptocurrencies renders them impractical as a means of transferring funds. This volatility is primarily due to the speculative nature of cryptocurrencies and the lack of a central authority to regulate their value. For instance, Bitcoin, the largest cryptocurrency, had an annualized volatility rate of 81% in 2021, with investors experiencing an average daily price change of 4% (Armstrong, 2022). Ethereum, another major cryptocurrency, had an even higher annualized volatility rate of 107% and a 6% average daily volatility rate (Armstrong, 2022). Moreover, other cryptocurrencies exhibit even greater volatility. For example, Solana was found to be the most volatile cryptocurrency in 2021, with its volatility rates being twice those of Bitcoin (Armstrong, 2022). Such high levels of volatility can lead to significant financial losses for users, particularly those who are not well-versed in the dynamics of the cryptocurrency market. Thus, it is possible that one may send out a certain amount of money in cryptocurrency and the receiver will receive an amount far less than what the sender sent originally. This in itself renders cryptocurrency unattractive for both legitimate and illegitimate business transactions.

Over the next few years, the use of cryptocurrencies by jihadi terrorists to fund attacks is likely to remain limited and largely within the purview of more technologically sophisticated plotters. Some extremists might seek to purchase cryptocurrencies as a form of investment, the proceeds of which could be used to fund attacks or a terrorist organisation. However, given the current volatility of these speculative assets, this is unlikely to materialise in the near term and would likely be a longer-term financing strategy. Despite these limitations, counterterrorism professionals will need to maintain situational awareness of cryptocurrencies and fintech, as their adoption is likely to grow over time in line with increased societal adoption.

Research Methodology

Research Design:

This is a theoretical or conceptual study that employs a literature review and analysis approach to examine the intersection of cryptocurrencies and terrorist financing from a network theory perspective.

Method of Data Collection:

1. Literature Review: The researchers consulted various scholarly sources, including books, journal articles, and reports from reputable organizations such as the Europol. This literature review helped in understanding the theoretical framework, and previous research related to the use of cryptocurrencies by jihadi terrorists.

2. Content Analysis: The researchers conducted content analysis of reports, news articles, and other publications from reputable sources like Al Jazeera, and NBC News. This content analysis helped in understanding the ambiguities in the position of sharia law on cryptocurrency as well as the vulnerabilities inherent in cryptocurrencies.

3. Internet-based Repositories: The researchers consulted online repositories and databases, such as ProQuest Central (PQC), to access relevant scholarly sources and reports.

4. Scoping Review: The researchers conducted a scoping review to map the existing literature and identify relevant studies and reports related to the research topic.

Summarily, data for this research were gathered and synthesized from various secondary sources, including academic journals, reports from think tanks and research institutions, news articles, and online resources. The study drew upon a wide range of materials to examine the theoretical underpinnings, potential vulnerabilities, and documented instances of cryptocurrency use for terrorist financing.

Method of Data Analysis:

The study employed a narrative review approach to analyse the collected data. The data from various sources were evaluated and synthesized to identify key themes, patterns, and arguments related to the research problem. The analysis involved the following steps:

Literature review: An extensive review of relevant literature, including academic publications, reports, and online resources, was conducted to gather information on the topic.

Thematic analysis: The collected data were analysed using a thematic approach, where recurring themes, concepts, and perspectives related to cryptocurrency and terrorist financing were identified and organised.

Critical evaluation: The gathered data were critically evaluated, assessing the strengths, limitations, and contradictions within the existing literature and evidence.

Synthesis and interpretation: The gathered data were synthesized the analysed to develop a comprehensive understanding of the potential and challenges of using cryptocurrencies for jihadi terrorist financing. The findings were interpreted in the context of relevant theoretical frameworks, such as network theory, thereafter, conclusions were drawn based on the analysis.

Conclusion

This study has examined the viability of cryptocurrencies as a means of financing for jihadi terrorist groups. While there are concerns that the decentralized, anonymous, and transnational nature of cryptocurrencies could enable terrorist financing, the evidence supporting this notion remains limited. The study outlined several key reasons why cryptocurrencies have not been extensively utilized by terrorist groups thus far. These include technological barriers to acquiring and using cryptocurrencies, the lack of true anonymity on public blockchains, the challenges of converting cryptocurrency into usable funds, and the extreme volatility of many digital assets. Additionally, cultural and ideological factors appear to make traditional financing methods more appealing to many jihadi organizations.

While the threat of cryptocurrency-enabled terrorist financing cannot be discounted entirely, the perceived vulnerabilities of cryptocurrencies have not yet translated into widespread adoption by terrorist groups. Counterterrorism efforts aimed at monitoring and disrupting illicit financing activities, including through blockchain analysis and enforcement of regulations, have also helped curb the exploitation of these novel financial technologies.

Overall, over the near-term, the use of cryptocurrencies by jihadi terrorists to fund attacks is likely to remain limited, confined primarily to more technologically sophisticated plotters. However, as cryptocurrency adoption continues to grow globally, counterterrorism professionals will need to maintain vigilance and adapt their practices to address any evolving threats in this domain.

References

Aljazeera. (2018). Islam and cryptocurrency, halal or not halal? Retrieved April 10, 2024, from https://www.aljazeera.com/economy/2018/4/8/islam-and-cryptocurrency-halal-or-not-halal

Argentino, M., Davis, J., & Hamming, T. R. (2023). Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies. National Counterterrorism Innovation, Technology, and Education Center; International Centre for the Study of Radicalisation.

Arianti, V., & Yao Yaoren, K. (2020). How Terrorists Use Cryptocurrency in Southeast Asia. The Diplomat. Retrieved April 12, 2024, from https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/

Armstrong, M. (2022). The Varying Volatility of Cryptocurrencies. Statista. Retrieved April 10, 2024, from https://www.statista.com/chart/27577/cryptocurrency-volatility-dmo/

Brown, S. D. (2016). Cryptocurrency and Criminality. The Bitcoin Opportunity. The Police Journal, 89(4), 327–339.

Buczak, A. (2024). Is Cryptocurrency Anonymous? The Myth of Anonymity Debunked. Ulam Labs Blog. Retrieved April 10, 2024, from https://www.ulam.io/blog/is-cryptocurrency-anonymous

CoinGecko. (2024). 2024 Q1 Crypto Industry Report. Retrieved May 5, 2024, from https://www.coingecko.com/en/global-charts

Collier, K. (2021). Crypto exchanges keep getting hacked, and there's little anyone can do. NBC News. Retrieved April 14, 2024, from https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870

Davis, J. (2019). A Canadian Cryptocurrency Caper in the Sri Lanka Attack? Unlikely. INTREPID. Retrieved April 14, 2024, from https://www.intrepidpodcast.com/blog/2019/5/6/a-canadian-cryptocurrency-caper-in-the-sri-lanka-attack-unlikely

Davis, J. (2022). Buffalo Shooting: Financing Terrorism. Insight Intelligence. Retrieved April 14, 2024, from https://insightintel.substack.com/p/buffalo-shooting-financing-terrorism

DEFIX SOLUTIONS. (2023). Cryptocurrency Technologies: Communicating through Theories. The Dark Side. Retrieved April 10, 2024, from https://medium.com/thedarkside/cryptocurrency-technologies-communicating-through-theories-19431d660ea5

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. RAND Corporation. Retrieved April 2, 2024, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

Emerging Technology from the arXivarchive. (2018). How network theory predicts the value of Bitcoin. MIT Technology Review. Retrieved April 13, 2024, from https://www.technologyreview.com/2018/03/29/67091/how-network-theory-predicts-the-value-of-bitcoin/

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. Retrieved April 13, 2024, from https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Fisher, A., Prucha, N., & Winterbotham, E. (2019). Global Research Network on Terrorism and Technology: Paper No. 6 Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability. Royal United Services Institute for Defence and Security Studies. Retrieved April 10, 2024, from https://static.rusi.org/20190716_grntt_paper_06.pdf

Grand View Research. (2024). Cryptocurrency Market Size, Share & Growth Report, 2030. Retrieved April 10, 2024, from https://www.grandviewresearch.com/industry-analysis/cryptocurrency-market-report

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the Cyber-Extortion Menace. In Proceedings of the 13th Australian Information Security Management Conference (pp. 47-56). Perth, Australia: Edith Cowan University. Retrieved from https://ro.ecu.edu.au/ism/180

Hasbi, A. H., & Mahzam, R. (2018). Cryptocurrencies: Potential for terror financing? RSIS Commentary, (075). Retrieved April 12, 2024, from https://www.rsis.edu.sg/wp-content/uploads/2018/04/CO18075.pdf

Irwin, A. S. M., & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control, 19(4), 407-425.

Mines, A., & Margolin, D. (2020). Cryptocurrency and the Dismantling of Terrorism Financing Campaigns. Lawfare. Retrieved April 17, 2024, from https://www.lawfaremedia.org/article/cryptocurrency-and-dismantling-terrorism-financing-campaigns

Natarajan, H., Martínez, A. F., & Iavorskyi, M. (2023). Fear, uncertainty and doubt: Global regulatory challenges of crypto insolvencies. World Bank Blogs. Retrieved February 23, 2023, from https://blogs.worldbank.org/en/psd/fear-uncertainty-and-doubt-global-regulatory-challenges-crypto-insolvencies

Serena, L., Ferretti, S., & D'Angelo, G. (2021). Cryptocurrencies activity as a complex network: Analysis of transactions graphs. Peer-to-Peer Networking and Applications. Retrieved April 11, 2024, from https://arxiv.org/abs/2110.14765

Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies – a danger for Europe? Journal of Money Laundering Control, 21(4), 513-519.

Wang, S., & Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. Policing: A Journal of Policy and Practice, 15(4), 2329–2340. Retrieved April 10, 2024.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. Studies in Conflict & Terrorism, 39(3), 195–206.