OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 17, Nº. 1
May 2026

JANUS.NET
e-journal of International Relations

CRYPTOCURRENCY TERRORISM FINANCING: A THREAT ASSESSMENT AND ANALYSIS OF GLOBAL RESPONSES

KANGDIM DINGJI MAZA
mdingji@gmai.com
teaches at the Department of Political Science, Karl Kümm University, Vom-Plateau State, (Nigeria). He earned his PhD from the Department of Political Science and International Relations, Near East University KKTC, Via Mersin 10, Turkey. Dr. Dingji's research focuses on issues around conflict, terrorism, insurgency, counterinsurgency, international security, and complex transnational threats in transitioned societies. He has published widely in these thematic areas in reputable local and international journals, policy briefs, and conferences. His research work can be found in academic journals such as: Religions, Sage Open, Journal of African Union Studies, Siyasal: Journal of Political Science. https://orcid.org/0000-0003-1059-8707

NANJWAN YALE DAMAP
nkydamap@gmail.com
Lawyer by training and currently a Doctoral Researcher at the Department of International Investment Law, University of Derby (United Kingdom). Damap's research interests revolve around issues regarding the regulation of cryptocurrency through the various legal instruments instituted by international actors. https://orcid.org/0009-0006-0481-3203

KWOPNAN IBRAHIM BULUS
kapal4uall@gmail.com
Docent at the Department of Political Science, University of Jos, Plateau State (Nigeria). He has a PhD from the Department of Politics and International Studies, Girne American University, Northern Cyprus, Via Mersin 10, Turkey. His research interests cover Gendered Narratives, on Peace, Conflict, and Security in post-conflict societies. He has several publications around these thematic areas and is consistently driven by the desire to teach, research, and provide community service. https://orcid.org/0000-0001-5579-8329

Abstract

The rise and popularity of cryptocurrency in the global financial system has presented opportunities and challenges in the fight against terrorism financing. This is because, the decentralized, pseudonymous, safety, privacy, and borderless nature of these digital currencies and assets has created the opportunity for terror groups to exploit. Terror groups take advantage of these opportunities to fund their operations, launder assets, organize, plan attacks, and consolidate their presence in the global financial system. Using the qualitative method of research, through the use of academic and non-academic documents, reports, and analysis from relevant institutions such as the Financial Action Taskforce (FATF), the United Nations (UN), The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), national governments and other relevant agencies, this article examines the global counter-measures taken by these actors in combating cryptocurrency terrorism financing. The article examine the prospects and challenges faced in combating the menace. The findings of the article show that in spite of the global efforts aimed at combating cryptocurrency terrorism financing the lack of global regulations and laws against money laundering, terrorism financing through the cryptocurrency ecosystem, lack of effective synergy and collaboration by relevant actors in the fight against cryptocurrency and terrorism financing and the evolving nature of the crypto and tactics of terror groups to evade surveillance continue to affect the counter-measures. To address these gaps, the article recommends the need for more collaboration

among actors in combating this threat, strengthening a stronger regulatory framework to protect and guarantee the safety of the cryptocurrency users from threats posed by terror groups and other transnational criminal networks operating in the crypto digital space..

Keywords

Cryptocurrency, Counterterrorism, Terrorism Financing, Financial Action Taskforce (FATF), The Inter-Governmental Action Group Against Money Laundering in West Africa (GIABA), & The United Nations (UN).

Resumo

A ascensão e a popularidade das criptomoedas no sistema financeiro global têm apresentado oportunidades e desafios na luta contra o financiamento do terrorismo. Isto deve-se ao facto de a natureza descentralizada, pseudónima, segura, privada e sem fronteiras destas moedas e ativos digitais ter criado oportunidades que os grupos terroristas podem explorar. Os grupos terroristas aproveitam-se destas oportunidades para financiar as suas operações, branquear ativos, organizar-se, planear ataques e consolidar a sua presença no sistema financeiro global. Utilizando o método de investigação qualitativa, através do recurso a documentos académicos e não académicos, relatórios e análises de instituições relevantes, tais como o Grupo de Ação Financeira Internacional (GAFI), as Nações Unidas (ONU), o Grupo de Ação Intergovernamental contra a Lavagem de Dinheiro na África Ocidental (GIABA), governos nacionais e outras agências relevantes, este artigo examina as contramedidas globais adotadas por estes atores no combate ao financiamento do terrorismo através de criptomoedas. O artigo examina as perspetivas e os desafios enfrentados no combate a esta ameaça. As conclusões do artigo mostram que, apesar dos esforços globais destinados a combater o financiamento do terrorismo através de criptomoedas, a falta de regulamentação e legislação globais contra a lavagem de dinheiro e o financiamento do terrorismo através do ecossistema das criptomoedas, a falta de sinergia e colaboração eficazes por parte dos atores relevantes na luta contra o financiamento do terrorismo através de criptomoedas, bem como a natureza em evolução das criptomoedas e as táticas dos grupos terroristas para escapar à vigilância, continuam a afetar as medidas de combate. Para colmatar estas lacunas, o artigo recomenda a necessidade de uma maior colaboração entre os intervenientes no combate a esta ameaça, reforçando um quadro regulamentar mais sólido para proteger e garantir a segurança dos utilizadores de criptomoedas contra as ameaças representadas por grupos terroristas e outras redes criminosas transnacionais que operam no espaço digital das criptomoedas.

Palavras-chave

Criptomoedas, Contraterrorismo, Financiamento do Terrorismo, Grupo de Ação Financeira Internacional (GAFI), Grupo Intergovernamental de Ação contra a Lavagem de Dinheiro na África Ocidental (GIABA) e Organização das Nações Unidas (ONU).

How to cite this article
Maza, Kangdim Dingji, Damap, Nanjwan Yale & Bulus, Kwopnan Ibrahim (2026). Cryptocurrency Terrorism Financing: A Threat Assessment and Analysis of Global Responses. *Janus.net, e-journal of international relations,* VOL. 17, Nº. 1, May 2026, pp. 285-303. https://doi.org/10.26619/1647-7251.17.1.15

Article submitted on 18 June 2025 and accepted on 16 January 2026.

CRYPTOCURRENCY TERRORISM FINANCING: A THREAT ASSESSMENT AND ANALYSIS OF GLOBAL RESPONSES

KANGDIM DINGJI MAZA

NANJWAN YALE DAMAP

KWOPNAN IBRAHIM BULUS

Introduction

The emergence of cryptocurrency has led to a paradigm shift throughout the international economic and financial system, necessitating a departure from the traditional financial system to a private and digitised system through blockchain technology (Zhuk, 2024). Cryptocurrency has been used as a means of exchange presupposing currency as well as a store of value (Mattke, Maier & Reis, 2020). There is no monolithic definition as to what cryptocurrency entails, as expressed in several studies. However, despite this non-monolithic stance, most of the studies regarding the subject matter have a consensus that the term could be operationalized as a digital currency typically lacking a centralized authority responsible for regulation and ensuring strict compliance. Rather, it utilises a decentralised system for transaction recording and issuance management. It relies on cryptography to prevent counterfeiting and fraud, thereby ensuring the security of transactions. The emphasis on security provides reassurance and instills confidence in the system (Zohuri, Nguyen & Moghaddam, 2022). Other studies similarly describe cryptocurrency as an electronic and virtual currency created to facilitate and buying, selling, and exchange of goods and services irrespective of physical borders, territories without any interference from a central authority (He, Li, Wang & Shah, 2024). It achieves this through encryption technology, which controls the creation of units and verifies transactions (Ibid).

The inherent characteristic of cryptocurrency resonates in its decentralisation and anonymity, and global accessibility devoid of the control of any centralized issuing authority, such as a Bank or a trusted party, has given rise to a myriad of challenges (Sharma, Pant, Sharma & Brahmachari, 2020). Proponents of the cryptocurrency school of thought, such as Changpeng Zhao (CZ) and Vitalik Buterin, believe that cryptocurrency emerged due to a lack of confidence in the extant international financial system (Doll-Steinberg & Leaf, 2023). Events of the 2008 economic recession alongside the COVID-

19 that followed, fuelled by the COVID Lock malware, became widespread due to the COVID and further propelled the use of cryptocurrency as a means of exchange, thus solidifying and entrenching the use of cryptocurrency in different jurisdictions (Dyntu & Dykyj, 2021).

The emergence of cryptocurrency has heralded an era where terrorist groups can take advantage of the anonymity of cryptocurrency, its decentralised and global accessibility to perpetrate transnational organised crimes in the form of Terrorism Financing (TF) (Majumder, Routh & Singha, 2019; Sestino, Tuček & Bresciani, 2024). Terrorist groups across the globe have used cryptocurrency as a conduit for the transfer of funds for terrorism in different parts of the world. Cryptocurrencies, owing to their anonymity, decentralized, and unregulated nature, have opened up vistas of opportunities and alternative channels for terrorist groups to fund, plan, and carry out attacks covertly without any scintilla of trace (Akcinaroglu & Shi, 2023). According to a US Department of Justice press release (15 December 2022), "defendants collected and transferred approximately USD 35,000 through cryptocurrency and other electronic means to Bitcoin wallets and accounts they believed to be funding ISIS" (See DOJ, 2022). The report also assert that Terrorist organisations are also using cryptocurrencies to raise funds. For example, Islamic State in Iraq and Syria (ISIS) called for cryptocurrency donations in this memorable poster (Ibid).

As put forward by the Anti-Money Laundering & Counter Financing of Terrorism AML/CFT, Terrorism financing is a course of action leading to the provision and facilitation of financial assistance to terror groups to enable them to carry out their violent act of terror on states and non-state actors in society (FATF Report 2015). This definition further supports the definition by Wang & Zhu (20221) that terrorist financing is the economic basis of terrorist activities and the lifeline of all terrorist organizations. Interestingly, since the emergence of cryptocurrency and its increasing usage, terrorist organizations have leveraged its non-regulatory and unrestricted access to plan and carry out attacks. Consequently, legislators around the world have called for global action to regulate the sale, purchase, and limit the exchange of cryptocurrencies (Ibrahim, 2019). According to the FATF 2023 Report, most time, terrorism financing takes the form of using digitally enabled technology for crowdfunding (see FATF Report, 2023). Research from notable institutions such as the FATF and subsequent assessments on emerging terrorist financing risks further revealed that terror groups and other violent non-state actors driven by ethnic and racial hate continue to rely on online crowdfunding as an avenue to fund their operations (FATF, 2015). This was evidenced in situations where violent extremist and terrorist groups often exploit and hijack the unregulated donation-based crowdfunding support to fund and sustain their operations (see FATF, 2023). The report gave examples with ISIS and other Salafist groups operating in Europe, particularly Germany, under the guise of charity organizations using crypto to plan, fund, and carry out acts of terror (Ibid).

The rise in using cryptocurrency systems to facilitate transnational organised crimes and support the activities of terrorist groups across the world is most alarming, hence the need to nip it in the bud to prevent it from resulting in increased global insecurity as currently being experienced (Carata, 2017). Studies by Amiram, Jørgensen, & Rabetti (2022) revealed that given the increase in terrorism financing, global peace has remained elusive, leaving many weaker states and developed states vulnerable to the activities

and threats of terror attacks. Although there have been responses by international organisations such as the Financial Action Task Force (FATF) in collaboration with Financial Intelligence Unit (FIU's), and International Police Organisation (Interpol) to address the menace of Terrorism financing, the phenomenon has continued due to the privacy-enhanced features of certain cryptocurrencies such as Monero and Zcash, used for crowdfunding for terrorism making them invisible for regulators(Gordon, 2011; Rébé, 2019; Wagman, 2022).

This article, therefore seeks to examine the strengths and weaknesses of the initiatives by international organisations such as the Financial Action Task Force (FATF) in curtailing terrorism financing and ensuring global peace. The challenges faced by these international organisations and lessons drawn from their regulatory challenges are used to inform the development of a suitable global regulatory framework to ensure global peace. To do this, the article uses the qualitative research approach by integrating academic and non-academic literature such as journal articles and reports from relevant regulatory agencies at the global, sub-regional, and national levels such as the Financial Action Task Force (FATF), United Nations Office on Drugs and Crime (UNODC), The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) and other relevant material relevant to analyzing the relationship between cryptocurrency, terrorism financing and its implication on various global countermeasures. This method relies on secondary data analysis, where the emphasis is carried out by reviewing and assessing extant policies, international laws, policies, and regulations from relevant institutions and actors in combating terrorism financing and other forms of transnational organized crimes. Needless to say, this method offers a comprehensive threat assessment of the various measures taken by relevant actors towards combating terrorism financing.

The research questions posed by this article are as follows: How is cryptocurrency used as a tool for financing terrorism? What are the regulatory and enforcement challenges in addressing terrorism financing? What measures have been implemented to stem the tide of terrorism financing globally, and how effective are these measures?

Following the introduction, the second section offers a theoretical discussion on the relationship between cryptocurrency and terrorism financing. The third section assesses how terror groups use various cryptocurrency methods to fund their operations and carry out their activities. The fourth section of the article responds to the global responses by relevant actors in the international arena to counter the threat of terrorism financing through cryptocurrency platforms. The fifth section addresses the challenges and threats faced by relevant actors in the global response to combating cryptocurrency terrorism financing. The sixth section concludes the article by providing a general overview and implications on how relevant actors involved in countering cryptocurrency terrorism financing can adequately achieve their objective in an evolving and challenging global financial and international system.

Cryptocurrency and Terrorism Financing: Theoretical Discussions

Research has shown that several theoretical paradigms from multiple academic disciplines, ranging from Criminology, Economics, Political Science, Psychology, and

International Relations, seek to assess and explain the relationship between cryptocurrency and terrorism financing (Hasan, 2023; Saha, Hasan, Mahmud, Ahmed, Parvin & Karmakar, 2024). These perspectives explain the link between cryptocurrency and terrorism financing.

As argued and put forward by the proponents of the Routine Activity Theory (RAT), try to link cryptocurrency financing because terror groups are often considered motivated offenders, exploit the vulnerability, lack of regulations, and censorship of the digital financial ecosystem to carry out their acts of terror and other forms of activities (Lee & Choi, 2022). Terrorist organizations believed that using this avenue would make it difficult for relevant regulatory agencies to detect, track, and counter their threats. Perspectives such as the Rational Choice Theory (RCT) and the Economic Theory of Crime see members of terrorist organizations are rational actors who always assess their economic benefits, opportunities, and risks before carrying out their attacks (Luong, 2024). Contextualizing this paradigm to cryptocurrency financing suggest the fact that the digital ecosystem operates within the prism of anonymity, borderless structure, decentralized financing, cost-effectiveness, and blockchain technology provides the platform for easy movement and laundering of assets and funds, does not only make it attractive for them, it also reduces the risk, scrutiny, and exposure from relevant regulatory agencies and traditional financial institutions (Klein, Assadi & Zwilling, 2024). The Network Theory (NT) situates its stance on the fact that the decentralized nature of digital funds and the crypto financial network presents the perfect opportunity for terror groups to fund their operations through crowdfunding, peer-to-peer transactions, and other digital marketplaces (Ferretti & D'Angelo, 2020). They easily launder and fund their operations without using the traditional banking system, which makes it difficult and cumbersome to fund their operations (Ekici & Tuzuner, 2024). Studies have also shown that global terrorist organizations such as the Islamic State in Iraq and Syria (ISIS), Al-Qaeda, and Hezbollah are leveraging on the advantage of these decentralized financial networks to not only fund their operations but also recruit and attract foreign fighters (Eaddy, 2019; Kushelevitch, 2025; Manning, Akartuna & Johnson, 2025).

In perspective, operationally, these theories offer a multipronged analysis and understanding of how terrorist organizations fund their operations through the digital ecosystem enabled by the growing global presence of cryptocurrency (Whyte 2023). This is because, within the theoretical lens of the routine activity approach, terrorist organizations exploit the opportunities offered by the decentralized nature of digital finance and the economic structure to effectively sustain and fund their operations (Movchan, Shliakhovskyi, Kozii & Fedchak, 2023). The Rational Choice stance seeks to point out the strategic resilience framework for these terror groups to adapt by thinking rationally and leveraging the opportunities offered by cryptocurrency to plan, fund, and carry out their attacks (Farber & Yehezkel, 2025). The theoretical integration of the economic theory of crime further justifies, measures, and points out the cost-benefit logic for terrorist groups and other violent non-state actors to make meaningful financial decisions that will not only sustain and consolidate the financial base of such groups, but the economic perspectives on crime will also determine the longevity of these groups (Whyte 2023; Bătușaru & Sbârcea, 2024; Akcinaroglu & Shi, 2025). The final theoretical intersection of the network theory further puts the crypto economy and ecosystem in

relation to decentralized and cell-like structures of modern terrorist organizations, which operate across different layers and network cells (Cascavilla, 2024).

Collectively, these theoretical positions further explain and reveal that financing terrorism today is an evolving process that requires technological, strategic thinking, economic incentives, and a decentralized network or layers, which tend to create the perfect opportunity for terrorist organizations to effectively fund their operations, carry out attacks, consolidate, and expand their frontiers without being hindered by territoriality and geography (Cascavilla, 2024; Akcinaroglu & Shi, 2025). It is also vital to state that the emergence of cryptocurrency does not create funding for acts of terror, but the innovation it brought to the digital financial ecosystem, directly or indirectly, created the platform for these violent non-state actors to fund and carry out their operations (Whyte, 2023). Therefore, understanding how terrorist organizations fund their operations and activities requires the integration and understanding of these integrated theoretical positions, given the fact that any counter terrorism measure must also address the structural deficits associated with the decentralized structure of cryptocurrency operations, altering the cost-benefit advantages by the economic opportunities associated with cries and disrupting the illicit networks that explain the operations of modern terrorist organizations.

How are Cryptocurrencies used to fund terror?

The decentralized, borderless, non-regulatory, cost-effective, and pseudonymous nature of cryptocurrency has increasingly become an avenue through which terror groups use to not only fund their operations, but also plan, recruit, and facilitate their attacks in the global system (Akcinaroglu & Shi, 2025). Research by experts reveals that due to the non-complexity and flexibility of the crypto ecosystem, it has become an easy avenue for terror organizations to continue perpetrating, sustaining, and consolidating themselves despite the various measures taken by states and non-state actors to combat their activities (Dyntu & Dykyj, 2021). Terror groups use several cryptocurrency avenues and methods to fund their operations around the world, as evidence from studies has shown there are several ways these organizations use to fund their operations (Akram, Nasar & Rehman, 2021). This argument is further supported by evidence suggesting that terror groups, including Al-Qaeda, ISIS, the Houthis in Yemen, and Hamas, have increasingly resorted to and turned to cryptocurrencies as a means to finance and sustain their operations and organizations (Krylova, 2023; Darwish, 2024). These groups are said to consistently use the cryptocurrency space to solicit funds through encrypted messaging platforms, social media, and darknet platforms (Bauer & Levitt, 2020). This fundraising process is usually carried out under the guise of false humanitarian support for charity organizations and crowdfunding activities (Vidino, Lewis, & Mines, 2020).

The fact that cryptocurrency presents an opportunity for Peer-to-Peer (P2P) transactions under its platform makes it easy for terror groups to use this method to fund its operations (Jovanovic, Kostić, Sebastian & Sedej, 2022). This is because P2P allows for direct transactions between persons irrespective of boundaries and the challenges associated with the traditional banking system, where it is easier to monitor, track, and regulate the movement of funds (Ibid). In addition, P2P transactions are not only anonymous, easier, faster, not regulated, and difficult to track, which makes terrorist

organizations leverage on these advantages to easily launder funds which making it difficult to trace (Teichmann, 2022).

Other studies revealed that terrorist organizations also take advantage of the fact that the use of mixers and tumblers for crypto transactions to fund their operations (Mehta & Chawla, 2024). This process involves the mixing of funds gotten through illicit means such as trafficking of drugs, persons, drug sales, kidnapping for ransom, etc., with clean funds by these transnational terror groups, thereby hindering the ability of law enforcement agencies to trace the origin of such funds and monitor such transactions (Burgess, Hamilton & Leuprecht, 2024; Navani & Cirella, 2024). This service has further enabled these groups to finance, consolidate, and sustain their activities, knowing it will be difficult to counter.

Research has also revealed that the use of privacy coins such as Monero and Zcash with enhanced security features, non-detectability, and traceability features has become an attractive digital coin used by terrorists to fund their operations (Silfversten, Favaro, Slapakova, Ishikawa, Liu, & Salas, 2020; Gross, Sedlmeir, Babel, Bechtel & Schellinger, 2021). This is because, unlike Bitcoin, whose transactions are sometimes traced, the introduction of these privacy coins into the crypto ecosystem has become a conduit used by terror groups and other transnational criminal organizations to fund their operations (Søgaard, 2024).

Furthermore, it has been revealed that the darknet marketplace has become an attractive and resource marketplace for these transnational terror organizations to purchase goods and services (Rawat, Mahor, Chouhan, Pachlasiya, Telang & Garg, 2022). Studies have shown that terrorist organizations like ISIS have used the dark web as a space for the procurement of weapons, recruiting fighters, planning, and executing attacks, and other resources needed for the expansion and sustainability of the organizations (Lakomy, 2024). The ongoing conflict in the Middle East between Israel and Hamas saw Hamas increasingly leverage cryptocurrency to plan and execute the October 7th, 2023, attacks (Darwish, 2024). The demand for ransom payment through cryptocurrency by terrorist organizations is also another method through which these organizations finance their operations. Studies have shown that terror groups like Al Qaeda, Boko Haram, Boko Haram, and ISIS are exploring the digital financial system to not only fund their operations but also demand ransom payments from their kidnapped victims (Gross, Sedlmeir, Babel, Bechtel & Schellinger, 2021; Ofusori & Hendradi, 2023; Goldbarsht, 2024).

It is on this note that, in today's international system, technological and innovative advancements meant for the development of societies have also become an alternative and high-resource avenue for terror groups to fund and sustain their operations.

What are the Global Responses Cryptocurrency Terrorism Financing?

It is trite that the emergence of cryptocurrency as a conduit pipe for terrorism financing has led to regulatory approaches around the world, particularly by states and international organisations, to curtail it (Majumder, Routh & Singha, 2019). Research had shown that finance serves as the lifeblood of terrorist groups, which not only guarantees the organization's operations, survival, and longevity; yet, paradoxically, it

also represents one of their most significant vulnerabilities, as these funds are constantly monitored, detected and disrupted by states and non-state actors in their counterterrorism engagements (Lormel, 2018). Therefore, disrupting the flow of funds is an antidote to preventing terrorism. One of the major international organisations providing a roadmap to mitigate terrorism financing using cryptocurrency is the Financial Action Task Force (Haider & Akhtar, 2024). The Financial Action Task Force (FATF) is a global organisation saddled with the responsibility of tackling money laundering, terrorism, and proliferation financing through research and monitoring how criminals raise, use, and move funds across the world. The role of the FATF is to set standards for compliance by states on how best to curtail terrorism financing (Bondaroff & Morrow, 2024).

The FATF has developed recommendations to be adhered to by states in the fight against terrorism financing, as well as funding for weapons of mass destruction. These recommendations are required to be implemented by member states of the FATF (Ibid). The FATF 40 recommendations are divided into seven distinct parts which include the following: AML/CFT Policies and coordination, Money laundering and confiscation, Terrorist financing and financing of proliferation, Preventive measures, Transparency and beneficial ownership of legal persons and arrangements, Powers and responsibilities of competent authorities and other institutional measures, international cooperation (see FATF Report 2015). Beyond these recommendations, the FATF has also developed recommendations regarding virtual currencies (Anggriawan & Susila, 2024). In this context, these virtual assets refer to any digital representation of value that can be electronically traded, transferred, used for payment, and exchanged for goods and services (Hrytsai, 2022). They have the potential of faster, cheaper, and easier payments without regard to the conventional payment system (Ibid). However, they are unregulated, thereby subjecting the process to enormous risk and becoming a haven for financial transactions of criminals and terrorists, making it easy for them to explore (Adaramola, 2025). Under the virtual currency standard, countries are expected to understand the money laundering and terrorist financing risks the sector faces, Licence or register virtual asset service providers, and supervise the sector in the same way it supervises other financial institutions (Ngo, Pham, Chung & Ryu, 2025). On the other hand, Virtual Assets service providers are expected to implement the same preventive measures as financial institutions, including customer due diligence, record keeping, and reporting of suspicious transactions, and obtain, hold, and securely transmit originator and beneficiary information when making transfers (see FATF Report, 2023).

Furthermore, research also revealed that national and regional governments have adopted diverse regulatory approaches to curtail terrorism financing within their jurisdictions (Giraldo & Trinkunas, 2007). As noted by Stigall, Miller & Donatucci, (2020), concerning National governments, the United States has played a vital role in stamping out terrorism financing. This is evidenced by the 2018 National Strategy for counterterrorism, which has an objective of examining:

> *"the capacity of terrorists to conduct attacks in the homeland and against vital United States interests overseas is sharply diminished; The sources of strength and support upon which terrorists rely are severed; Terrorists' ability to radicalize, recruit, and mobilize to violence in the homeland is diminished; Americans are prepared and protected from terrorist attacks in*

> *the homeland, including through more exacting border security and law enforcement actions; Terrorists are unable to acquire or use WMDs, including chemical, biological, radiological, and nuclear weapons, and other advanced weaponry; and public sector partners, private sector partners, and foreign partners to take a greater role in preventing and countering terrorism"* (see US Center for Counterterrorism, 2018).

Studies also revealed that in 2020, the US recorded the largest seizure of terrorist organizations' monetary funds in the form of cryptocurrency accounts of about 150 Bitcoin and 155 virtual currencies tied to Al-Qaeda (Mokhemar, 2022). The United States has also responded by identifying state sponsorship of terrorism financing and meting out necessary sanctions (Byman, 2020).

Other studies have also revealed that the European Union (EU) has responded to the emergence of cryptocurrency as a tool for terrorism financing through the process of issuing several directives and regulations to counter-terrorism financing, including Directive (EU) 2015/849 (Schindler, 2022). The fourth Anti-Money Laundering Directive (4AMLD) aims to prevent the financial system from being used for money laundering and terrorist financing. In the same vein, the New Anti-Money Laundering Directive (AMLD 6) and the Regulation of the European Parliament and the Council on the prevention of the use of the financial system for money laundering or terrorist financing present clearer rules for preventing money laundering and terrorist financing by the European Union (Premti, Jafarinejad & Balani, 2021).

In terms of law enforcement from the regional and international sphere in combating terrorism financing, Europol, Interpol, and the UNODC have played significant roles. In the case of Europol, several initiatives have been adopted to ensure enforcement and mitigate the risks of terrorism financing (D'Amato & Terlizzi, 2022). The Europol and Basel Institute consider investing in preventing and combating the misuse of the crypto ecosystem for financial crime as vital to safeguard both national and international security (Freudlsperger, Maricut-Akbik & Migliorati, 2022). They do that through investing in research and innovation, capacity building, and cross-border, multi-stakeholder collaborations are therefore pivotal in mitigating the menace of terrorism financing through cryptocurrency (Wahl, 2024). This position was also re-echoed by John Brandolino, UNODC Director, Division of Treaty Affairs during the 8th cryptocurrency conference in Vienna, 2024, stating that:

> *"Multilateral collaboration is essential to dismantling the finances of criminal organisations and terrorists. UNODC fully supports and promotes efforts to collectively strengthen our ability to prevent and counter the criminal misuse of crypto assets, which in turn contributes to overall global security"* (see UNODC, 2024).

This was also re-echoed by Iker Lekuona, Director of the Basel Institute's International Centre for Asset Recovery (ICAR), who said:

> *"In our work assisting with major transnational corruption and asset recovery cases, we see how money launderers and other criminals systematically*

> *target weak links in the chain. All institutions involved in detecting and investigating financial crimes and in recovering assets need to build their capacity to work on crypto-related cases"* (UNODC, 2024).

Law enforcement also involves the sharing of information between law enforcement agencies, financial institutions, financial intelligence unit (FIU) to track the movement of funds, ascertaining the source and purpose of usage of the funds (Wagman, 2022). This helps in determining the legality or otherwise of these funds for prosecution by law enforcement agencies, in collaboration with the FATF (Ibid).

Private sectors also have a role to play, particularly cryptocurrency exchanges and fintech companies, through compliance and monitoring (Alam & Zameni, 2019). This is because, cryptocurrency exchanges are required by law to provide know your customers KYC information for purposes of traceability for funds with the potential to be used for terrorism financing (Hasan, Talukder, Saju & Lysuzzaman, 2024). This involves the collection of identifying information from users for a range of reasons, such as confirming users are not subject to sanctions, blocking individuals residing in prohibited jurisdictions, and empowering proactive investigations in case of future suspicious activity (Ibid). They are also obliged to monitor transactions on an ongoing basis for suspicious activity that could reveal money laundering, terrorism financing, or other forms of financial crime. They are also required to monitor transactions effectively, as businesses will undoubtedly encounter some risky behaviour requiring direct outreach to customers, updating records, and reporting suspicious activity to relevant enforcement bodies (Takaragi, Kubota, Wohlgemuth, Umezawa & Koyanagi, 2023). Cryptocurrency service providers (VASPs) are also obliged to collect and disclose sender and beneficiary information for crypto asset transfers under FATF CTF standards (Kapsis, 2023). This is in conformity with the travel rule as developed by the Financial Action Task Force in their recommendations. This information helps regulators and law enforcement agencies to unravel the identity of criminals in various locations across the world. In the United Kingdom, for instance, crypto firms are required to register with the Financial Conduct Authority FCA and comply with the requirements of the regulations, if they intend to provide certain crypto asset services by way of business, and if this service will be during business carried on by them in the United Kingdom (see FCA 2019).

Studies by Uzougbo, Ikegwu & Adewusi (2024) also revealed a need for increased cooperation between the public and private sectors is essential for effective enforcement of cryptocurrency laws, given their important role in detecting and preventing illicit activities.

What are the Challenges and Gaps in addressing these threats?

The regulatory challenge in curtailing the use of cryptocurrencies as a channel for terrorism financing is embedded in the technology that governs cryptocurrency itself. Cryptocurrency exchanges like Coinbase often include user-centric information such as the "Know Your Customer" information needed for compliance with regulatory frameworks for transferring cryptocurrency and converting cryptocurrency to fiat (Kazerani, Rosati & Lesser, 2017). Consequently, due to its anonymity and decentralised

nature, cryptocurrency allows criminals to go undetected, particularly with cryptocurrencies with enhanced privacy features (Ibid). Research revealed that Cryptocurrencies with enhanced privacy features, such as Monero and Zcash, make identification of participants very challenging (Zhao & Zhang, 2021). In Monero, the privacy of the receiver identity is protected with a stealth address generated by the transaction sender, even the transaction receiver does not know the stealth address (Ibid). All Monero transactions are private by default, and the transaction amount is hidden with a cryptographic method (Thyagarajan, Malavolta, Schmidt & Schröder, 2020). In Monero, ring signatures and confidential transactions are combined to create Ring CT transactions, which can hide both the amount and origin of Monero transactions (Ibid). The implementation of robust security features, such as enhanced privacy features, makes it difficult for hackers to gain access, preventing unfortunate hacks such as the Mt. Gox exchange hack and the DAO attack on Ethereum (Arnone, 2024). In response to this concern, several privacy-enhanced cryptocurrencies have been developed that store the information "on-chain" (i.e., on the public blockchain) in a privacy-respecting manner that attempts to make the sender and receiver anonymous to third parties (Zheng, Xie, Dai, Chen & Wang, 2018).

Although these cryptocurrencies with enhanced privacy features provide security for the cryptocurrency against hacks, criminals explore these privatised features to avoid being detected as they engage in illicit activities using cryptocurrency (Maurushat & Halpin, 2022). However, for cryptocurrencies with decentralised and enhanced privacy features, such "Know Your Customer" information is non-existent, making it difficult for regulators to navigate and identify participants (Ibid).

Another challenge to cryptocurrency regulation lies on the fragmented regulatory approach across the world (Al-Tawil, 2023). Different international organisations and jurisdictions across the globe have developed approaches in diverse ways as to curtail transnational organised crimes like terrorism financing (Wronka, 2024). This multifaceted approach most often leads to regulatory arbitrage since there is no global consensus on a single window to curtail this transnational offence (Perdana & Jiow, 2024). This is because criminals are likely to explore less stringent jurisdictions to continue in their nefarious activities, thereby making regulatory approaches less effective. Therefore, developing standardised regulations across jurisdictions is necessary, considering the transnational nature of terrorist financing and money laundering (Al Naqbi, Nobanee & Ellili, 2025). This would greatly aid AML/CFT efforts in cases that span multiple international jurisdictions by fostering greater communication and the pooling of resources. Second, standardisation would mitigate the legal and jurisdictional mosaic of international perspectives on Bitcoin use and regulation (Fletcher, Larkin & Corbet, 2021).

In terms of enforcement gaps, the cryptocurrency regime is shrouded by inadequate enforcement in certain jurisdictions (Guseva, 2022). While there is effective enforcement in some jurisdictions, others are lagging, given room for arbitrage (Brummer, Yadav & Zaring, 2022). This creates a problem given the nature of cryptocurrency. Consequently, studies have also shown that law enforcement in certain jurisdictions does not have the requisite expertise to deal with complex issues relating to cryptocurrency (Uzougbo, Ikegwu & Adewusi, 2024). Cryptocurrency transaction involves parties in different countries, and they normally create ambiguity on which jurisdiction's laws apply. This

ambiguity can lead to regulatory gaps and enforcement challenges, which allow illicit activities such as money laundering and terrorism financing to flourish (Ibid).

Furthermore, another issue that poses a challenge to dealing with the issue of terrorism financing is inadequate international collaboration and information sharing by relevant stakeholders involved in tackling this challenge (Amiram, Jørgensen & Rabetti, 2022). Although certain international organisations have developed approaches fostering international cooperation by ensuring cross border cooperation in different jurisdictions, whether such initiatives have yielded positive result or is limited by sovereignty of states as this is a challenge to the effective regulation of cryptocurrency for counter terrorism financing since cross border information sharing need to be carried out with speed to prevent acts of terrorism happening.

Whilst regulatory approaches to curtailing cryptocurrency as a tool for terrorism financing is a step in the right direction, the major challenge is how this can be done without infringing on private rights of individuals. Hence the need to balance financial privacy with regulation becomes desirable (Li, Susilo, Yang, Yu, Du, Liu & Guizani, 2019). In addition, overregulation also whittles down the development of cryptocurrency as it stifles innovation and prevents it from growth (Džafić & Hečimović, 2023). Therefore, balancing regulation with innovation is necessary.

Conclusion

The emergence of cryptocurrency is a game-changer in today's global financial system given the immense opportunities and advantages it has in respecting individual and group privacy, ensuring financial decentralization, securing digital assets, dismantling some of the barriers associated with traditional banking, financial systems, and combating terrorism and other forms of complex global transnational crimes. Its efficiency in strengthening inclusion, non-regulatory, and non-interference nature from external sources makes it attractive to individuals and organizations who respect trade secrecy and financial anonymity. However, despite its attractive features, it has also presented an opportunity for terror groups and other criminal organizations to not only evade surveillance from relevant security agencies in countering the illicit movements and laundering of funds, but the platform is also an avenue for these groups to fund their operations but carry out other activities that threaten the peace and stability of the global financial and security system.

The findings of this study, suggest that these terrorist organizations have been leveraging on the fact that cryptocurrency transactions mostly involve P2P transactions, privacy coins, and dark web marketplaces to perpetuate their acts of terror and fund their operations despite the global efforts and responses from states and non-state actors in combating terrorism financing. Therefore, to combat these challenges, it is important for relevant actors such as states, global, regional, and sub-regional financial regulators, and other sectors utilizing the crypto digital space to strengthen and enhance their surveillance capabilities of tracking and stopping the various channels used by these groups to fund their operations. It is also important for these actors to initiate measures that further strengthen the safety and security of users in the crypto ecosystem and other Anti-Money Laundering Measures at the global, regional, sub-regional, national,

and individual levels. Furthermore, the need for increased stakeholder collaboration in the fight against terrorism financing is important, because counterterrorism involves the coalition of the willing for it to be more viable and effective.

References

Akcinaroglu, S., & Shi, M. (2025). Exploring the Impact of Cryptocurrency on Terrorism. *Terrorism and Political Violence*, *37*(1), 111-135. https://doi.org/10.1080/09546553.2023.2275057.

Akram, M., Nasar, A., & Rehman, A. (2021). Misuse of charitable giving to finance violent extremism; A futuristic actions study amidst COVID-19 pandemic. *Social Sciences & Humanities Open*, *4*(1), 100140.

Al-Tawil, T. N. E. (2023). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*, *26*(6), 1150-1164.

Arnone, G. (2024). Security and Privacy in the Digital Currency Space. In Navigating the World of Cryptocurrencies: Technology, Economics, Regulations, and Future Trends (pp. 63-77). Cham: Springer Nature Switzerland. Available at: https://baselgovernance.org/sites/default/files/2024-05/240506_Crypto-7th%20conference-recommendations.pdf

Bătușaru, C. M., & Sbârcea, I. R. (2024). Economic transformations and national security risks generated by cryptocurrencies. *Scientific Bulletin,"Nicolae Balcescu" Land Forces Academy, 29 (2)*, 202-213.

Bauer, K., & Levitt, M. (2020). *Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat*. International Centre for Counter-Terrorism (ICCT). Available at: Special-Edition-2-3.pdf accessed: 26th February 2025.

Black's Law Dictionary 11th Edition 2019

Bures, O. (2012). Private actors in the fight against terrorist financing: Efficiency versus effectiveness. Studies in Conflict & Terrorism, 35(10), 712-732.

Burgess, A., Hamilton, R., & Leuprecht, C. (2024). Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus. In *Financial Crime, Law and Governance: Navigating Challenges in Different Contexts* (pp. 203-227). Cham: Springer Nature Switzerland.

Byman, D. (2020). Understanding, and Misunderstanding, State Sponsorship of Terrorism. Studies in Conflict & Terrorism, 45(12), 1031–1049. https://doi.org/10.1080/1057610X.2020.1738682

Carata, C. (2017). Modern Methods of Financing Terrorism in a Global and Intercultural Society: Crypto-Currency. Redefining Community in Intercultural Context, 6(1), 192-198.

Cascavilla, G. (2024). The rise of cybercrime and cyber-threat intelligence: Perspectives and challenges from law enforcement. *IEEE Security & Privacy*, *23*(1), 17-26.

Darwish, A. (2024). "From Aid to Arms: The Duality of Cryptocurrencies in the Israel-Hamas Conflict". *Bloomsbury Intelligence & Security Institute.* 29th November. Available at: From Aid to Arms: The Duality of Cryptocurrencies in the Israel-Hamas Conflict — Bloomsbury Intelligence and Security Institute (BISI), accessed: 16th February 2025.

Dennis M. Lormel,(2019) "Terrorist Financing, Visualizing Funding Flows", Chartwell Compas, A PUBLICATION OF CHARTWELL COMPLIANCE, CHARTWELLCOMPLIANCE.COM, p6, Accessed at https://chartwellcompliance.com/wp-content/uploads/2021/04/2019-02.pdf

Doll-Steinberg, D., & Leaf, S. (2023). *Unsupervised: Navigating and Influencing a World Controlled by Powerful New Technologies*. John Wiley & Sons.

Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic journal of economic studies*, *7*(5), 67-72.

Džafić, J., & Hečimović, E. (2023). Striking The Balance: Cryptocurrencies At The Crossroads Of Regulation And Innovation. Zbornik Radova: Univerzitet'džemal Bijedić'u Mostaru, Ekonomski Fakultet, 21(33).

Eaddy, A. (2019). *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation).

Ejiofor, P. F. (2025). Accumulation by/for terrorism: the political economy of terrorism financing in Nigeria. *Small Wars & Insurgencies*, *36*(1), 120-159.

Ekici, B., & Tuzuner, M. (2024). Terrorism Financing Typologies: Comparison of the PKK and ISIL in Turkey. *Central European Journal of International and Security Studies*, *18*(1).

Farber, S., & Yehezkel, S. A. (2025). Financial Extremism: The Dark Side of Crowdfunding and Terrorism. *Terrorism and political violence*, *37*(5), 651-670.

FATF (2021) Ethnically or Racially motivated Terrorism financing - https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/ethnically-racially-motivated-terrorism-financing.html available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism Financing.pdf.coredownload.inline.pdf

FATF REPORT, Crowdfunding for Terrorism Financing, October 2023, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

Ferretti, S., & D'Angelo, G. (2020). On the ethereum blockchain structure: A complex networks theory perspective. *Concurrency and Computation: Practice and Experience*, *32*(12), e5493.

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. Research in International Business and Finance, 56, 101387.

Goldbarsht, D. (2024). Dancing in the dark: terrorist financing via the dark web. In *Financial crime and the law: identifying and mitigating risks* (pp. 167-190). Cham: Springer Nature Switzerland.

Gordon, R. (2011). Terrorism financing indicators for financial institutions in the United States. *Case W. Res. J. Int'l L.*, *44*, 765.

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a central bank digital currency with support for cash-like privacy. *Available at SSRN 3891121*.

Haider, K., & Akhtar, N. (2024). Money Laundering and Terrorism Financing through Virtual Currencies: Critical Analysis of International and Pakistan's Response. Pakistan Journal of Criminal Justice, 4(1), 195-210.

Hasan, M. F. (2023). Beyond Bitcoin: A review study on the diverse future of cryptocurrency. *IRE Journals,(7)*, *3*, 64-69.

He, C., Li, Y., Wang, T., & Shah, S. A. (2024). Is cryptocurrency a hedging tool during economic policy uncertainty? An empirical investigation. *Humanities and Social Sciences Communications*, *11*(1), 1-10.

Ibrahim, S. A. (2019). Regulating cryptocurrencies to combat terrorism-financing and money laundering. Stratagem, Journal of the Centre for Strategic and Contemporary Research (CSCR) 2(1). Available at https://journal.cscr.pk/stratagem/index.php/stratagem/article/view/38.

John B. (2016). "Why Criminals Can't Hide Behind Bitcoin". *Science*, 9th March. Available at: https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin accessed: 29th January, 2025.

Jovanovic, M., Kostić, N., Sebastian, I. M., & Sedej, T. (2022). Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens. *Technological Forecasting and Social Change*, *184*, 121981.

Kazerani, A., Rosati, D., & Lesser, B. (2017, August). Determining the usability of bitcoin for beginners using change tip and coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication* (pp. 1-5).

Klein, G., Assadi, D., & Zwilling, M. (2024). Fighting fire with fire: Combating criminal abuse of cryptocurrency with a p2p mindset. *Information Systems Frontiers*, 1-27.

Krylova, Y. (2023). Dubai: A Global Hub for Illicit Trade and Sanctions Evasion. In *Hubs of Illicit Trade in the Global Economy* (pp. 107-156). Routledge.

Kushelevitch, M. (2024). Unveiling the crypto-terror nexus: law enforcement intelligence challenges against terrorist financing. Journal of Financial Crime.

Lakomy, M. (2024). Dark web jihad: exploring the militant Islamist information ecosystem on The Onion Router. *Behavioral Sciences of Terrorism and Political Aggression*, *16*(4), 581-600.

Lee, H., & Choi, K. S. (2022). Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. In *The New Technology of Financial Crime* (pp. 82-103). Routledge; Nolasco Braaten, C., &

Li, Y., Susilo, W., Yang, G., Yu, Y., Du, X., Liu, D., & Guizani, N. (2019). Toward privacy and regulation in blockchain-based cryptocurrencies. IEEE Network, 33(5), 111-117.

Luong, H. T. (2024). Foundations and trends in the darknet-related criminals in the last 10 years: a systematic literature review and bibliometric analysis. *Security Journal*, *37*(3), 535-574.

Majumder, A., Routh, M., & Singha, D. (2019). A conceptual study on the emergence of cryptocurrency economy and its nexus with terrorism financing. In The Impact of Global Terrorism on Economic and Political Development (pp. 125-138). Emerald Publishing Limited.

Manning, M., Akartuna, E. A., & Johnson, S. (2025). Opportunities to future crime: Scoping the future of money laundering and terrorist financing through cryptoassets. *Technological Forecasting and Social Change*, *210*, 123894.

Mattke, J., Maier, C., & Reis, L. (2020, June). Is cryptocurrency money? Three empirical studies analyzing medium of exchange, store of value and unit of account. In Proceedings of the 2020 on Computers and People Research Conference (pp. 26-35).

Mehta, K., & Chawla, S. (2024). Illuminating the dark corners: a qualitative examination of cryptocurrency's risk. *Digital Policy, Regulation and Governance*, *26*(2), 188-208.

Mokhemar, M. E. (2022). Crypto-Terror on the Rise: Rethinking Regulation and Prosecution of Cryptocurrency Transactions. *Syracuse J. Sci. & Tech. L.*, *38*, 18.

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social and Legal Studios*, *4*(6), 123-131.

Navani, S., & Cirella, G. T. (2024). Cybercrimes in the cryptocurrency domain: identifying types, understanding motives and techniques, and exploring future directions for technology and regulation. *Journal of Geography, Politics, and Society*, *14*(2), 1-22.

Office of Public Affairs Four Defendants Charged with Conspiring to Provide Material Support to ISIS United States Department of Justice (accessed 29 January 2024- https://www.justice.gov/opa/pr/four-defendants-charged-conspiring-provide-material-support-isis

Ofusori, L., & Hendradi, R. (2023). Understanding the Impact of the Dark Web on Society: A Systematic Literature Review. *International Journal of Information Science and Management (IJISM)*, *21*(4), 1-21.

Press Release, Off. of Pub. Affs., Dep't of Just., Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020), https://www.justice.gov/opa/pr/globaldisruption-three-terror-finance-cyber-enabled-campaigns [https://perma.cc/579K-VD2F].

Rawat, R., Mahor, V., Chouhan, M., Pachlasiya, K., Telang, S., & Garg, B. (2022). Systematic literature review (SLR) on social media and the digital transformation of drug trafficking on the dark web. In *International Conference on Network Security and Blockchain Technology* (pp. 181-205). Springer, Singapore.

Rébé, N. (2019). Counter-Terrorism Financing: International Best Practices and the Law (Vol. 98). Brill.

Reyes, A., Silva, M., & Rodriguez, E. (2024). Unveiling the Subterranean Web using A Comprehensive Analysis of Digital Human Trafficking Networks and Covert Operations. *Journal of Judikaltura*, *2*(1), 19-35.

Saha, S., Hasan, A. R., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. *Multidisciplinary Reviews*, *7*(8), 2024168-2024168.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy* (pp. 459-474). IEEE.

Sharma, D. K., Pant, S., Sharma, M., & Brahmachari, S. (2020). Cryptocurrency mechanisms for blockchains: models, characteristics, challenges, and applications. Handbook of research on blockchain technology, 323-348.

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*. Santa Monica, CA, USA: RAND.

Søgaard Clausen, C. C. (2024). Crypto laundering on the dark web: Characteristics and Modus Operandi. Malmo University. Available at: Microsoft Word - SPECIALE-kopi.docx accessed: 2nd February 2025.

Stigall, D. E., Miller, C., & Donatucci, L. (2020). The 2018 US National Strategy for Counterterrorism: A Synoptic Overview. Nat'l Sec. L. Brief, 10, 1.

Teichmann, F. M. (2022). Current trends in terrorist financing. *Journal of Financial Regulation and Compliance*, *30*(1), 107-125.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: jurisdictional challenges and collaborative solutions. Magna Scientia Advanced Research and Reviews, 11(1), 068-083.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: jurisdictional challenges and collaborative solutions. Magna Scientia Advanced Research and Reviews, 11(1), 068-083.

Vaughn, M. S. (2021). Convenience theory of cryptocurrency crime: A content analysis of US federal court decisions. *Deviant Behavior*, *42*(8), 958-978.

Vidino, L., Lewis, J., & Mines, A. (2020). Dollars for Daesh: Analyzing the Finances of American ISIS Supporters. *NCITE Reports Research.* Vol. 16, available at: "Dollars for Daesh: Analyzing the Finances of American ISIS Supporters" by Lorenzo Vidino, Jon Lewis et al. accessed: 2nd February 2025.

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.

Whyte, C. (2023). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict & Terrorism*, *46*(7), 1126-1149.

Wronka, C. (2024). Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight. Journal of Banking Regulation, 25(1), 84-93.

Zhang, T. (2023). Privacy evaluation of blockchain based privacy cryptocurrencies: A comparative analysis of dash, monero, verge, zcash and grin. *IEEE Transactions on Sustainable Computing*. DOI: 10.1109/TSUSC.2023.3303180

Zhao, T., & Zhang, T. (2021, October). Revisiting anonymity and privacy of bitcoin. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1275-1280). IEEE.

Zhuk, A. (2024). Crypto-anarchy: a paradigm shift for society and the legal system. Journal of Computer Virology and Hacking Techniques, 1-27.

Zohuri, B., Nguyen, H. T., & Moghaddam, M. (2022). What is the Cryptocurrency? Is it a Threat to Our National Security, Domestically and Globally?. *I J T C Physcics,* 2022; 3(1): 1-14.