Forum:	Disarmament & International Security Committee (GA1)
Issue:	Addressing the Implications of the Use of Cryptocurrencies in Financing Terrorism and other Illicit Activities
Student Officer:	Maritella Petsa
Position:	Co-Chair

PERSONAL INTRODUCTION

Dear Delegates,

My name is Maritella Petsa and I am an 11th grade student in Athens College. I am beyond grateful and excited to welcome you to the thirteenth PSMUN conference. PSMUN was the first conference I ever attended, so I am beyond excited to be able to chair in the same conference two years later!

Being comparatively new to chairing it is important for me to conduct a not only correct and helpful, but an also inclusive and creative study guide. So, feel free to use this guide to navigate through the topic and acquire any information you may possibly need prior to conducting your research and writing your resolutions!

Personally, this will be my 10th overall conference but my 4th time chairing and thus I am really excited to be part of this conference and to be able to collaborate with every and each one of you.

The only thing I would like for you to remember is to always be yourselves and never be afraid to speak up. We would love to hear your voice! For anything you might need you can contact me at maritella.petsa9@icloud.com.

Best wishes,

Maritella Petsa

INTRODUCTION

Cryptocurrencies, a type of encrypted data strings denoting a unit of currency, have become a means of progress and an opportunity for financial advances from the moment of their initial development[1]. Cryptocurrencies are considered to be one of the first steps to remodelling the entirety of society's economic system and structure. This symbol of development, though, may present an embellished image. In the absence of physical currency, a technicality that allows individuals and groups to escape violating the law via the protection pseudonymity and anonymity offer, was created. The use of cryptocurrencies to fund terrorism has emerged as one of the drawbacks of this technological milestone, demonstrating that cryptocurrencies are, in fact, a two-sided coin.

Terrorist organisations require substantial funding in order to carry out their objectives. Criminal resources, as well as purchases of weapons, bomb-making equipment, and numerous kinds of illicit goods are high-cost, making simple transactions almost impossible. Traditionally, terrorist funding tends to come from drug trafficking, weapon smuggling, kidnapping, exortion, and other such illegal activities. Fraud is also a very common way of majorly profiting. There are also some more "legitimate" ways for groups to acquire funding. New members may potentially make donations, while non-profit organizations, in an attempt to help, may be abused or mis-used. Finally, illicit trade in commodities such as oil may provide financial gain. When using funds that come from such illicit sources, criminals run a significant risk of bringing the underlying illegal activity to the attention of authorities. This means that criminals have to conceal any illicit gains through money laundering and other complex mechanisms.

Cryptocurrencies have provided terrorist groups with a favorable economic environment that facilitates such illicit transactions and economic activities. In order to enable attempts to minimise financing illicit activities in general, it is necessary to comprehend the reasons why cryptocurrencies appeal to terrorist groups. Cryptocurrencies' decentralized nature and the anonymity they offer to users while being able to execute private transactions without engaging with banks are attractive to such groups. The ability to send and receive money from and to anyone, anywhere, even across borders, allows for all types of financing without requiring justification. The identities of individuals remain private, and all types of illicit activities occur with no one in particular being held accountable. In addition, the use of cryptocurrencies is low cost and fast, with no extra fees, making them accessible to almost anyone and financially more responsible, so as to increase the profit of terrorist groups.

[1]" Cryptocurrency." *Definition*, www.trendmicro.com/vinfo/us/security/definition/cryptocurrency. Accessed 7 Nov. 2023.

Cryptocurrencies have exceeded their original supplementary nature, being deemed one of the main funding types for illicit activities. Their primary use is in the form of donations. The most common type of financial contribution to such teams is provided via Bitcoin. Moreover, groups choose to utilise cryptocurrencies to not only raise but also to move and use funds so as to facilitate connections with the Black Market and regulate illegal transactions due to the decentralisation in the blockchain.

Despite being an imperative need of society, progress is also a part of human nature and evolution. In today's society, which is full of innovation, changes, modifications, and corrections, the idea of progress still remains a paradox. The way humanity has been formulated is of great complexity. The difficulty of distinguishing "good" from "bad" is such that the aforementioned distinction is rather utopic. Cryptocurrencies are a major component of today's financial system, offering numerous advantages and contributing to the evolvement of society as a whole. Nonetheless, they have been proven lethal when used by certain individuals and groups with malicious intent. As presented in the specific topic, groups including terrorists are making profits from the exploit of a beneficial economic factor. Consequently, ensuring the lawful, ethical, acceptable utilisation of various means is of major significance due to humankind and international integrity being imperilled.

DEFINITION OF KEY TERMS

Bitcoin

"Bitcoin is the first, most-traded, and best-known cryptocurrency. The digital currency was created by an anonymous computer programmer or group of programmers known as Satoshi Nakamoto in 2009. Owners of Bitcoins can use various websites to trade them for other cryptocurrencies or even physical currencies, such as U.S. dollars or euros, or can exchange them for goods and services from a number of vendors."[2]

Blockchain

"A blockchain is a distributed database that maintains a continuously growing list of ordered records, called blocks." These blocks "are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network."[3]

[2] Gregersen, Erik. "Bitcoin." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 30 Aug. 2023, www.britannica.com/money/topic/Bitcoin.
[3] "What Is Blockchain and How Does It Work?" *Synopsys*, www.synopsys.com/glossary/what-is-blockchain.html.

Counterterrorism Financing (CTF)

"Counter-terrorist financing (CTF), or combating the financing of terrorism (CFT), seeks to stop the flow of illegal cash to terrorist organizations. It is closely tied to anti-money laundering (AML)."[4] Due to the increased use of cryptocurrencies, CTF policies are currently attempting to combat the specific type of illicit activity funding.

Cryptocurrencies

"Cryptocurrencies are an alternative form of payment. Transactions are done digitally through encrypted technology known as blockchain."[5] Due to the anonymity and pseudonymity they offer to users, they have become one of the major components of funding terrorism and other illicit activities. The most commonly used cryptocurrencies are Bitcoin and Ethereum.

Decentralisation

"In the blockchain, decentralization alludes to the transfer of supervision and decision-making from a centralized association such as an individual, corporation, or group of people to a dispersed network. Decentralized networks endeavor to undermine the members' capacity to exercise authority and to decrease the inter-member trust necessary for any and all transactions."[6] In terms of cryptocurrencies, none of the transactions need to be approved nor assessed by any third-member parties. This in addition to the anonymity that arises from the pseudonymity of users is utilised by certain groups so as to facilitate processes such as Money Laundering and other illicit activities.

Money Laundering

"Money laundering is the processing of criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source."[7] The specific process is greatly facilitated via the use of cryptocurrencies.

Quick-Response Codes (QRCs)

"A QR code is a pattern of black and white squares that can be read by a smart phone, allowing the phone user to get more information about something. QR code is an abbreviation for ' Quick Response code'."[8]

---

[4] "What Is Counter-Terrorist Financing (CTF)?" *Dow Jones Professional*, 30 Mar. 2023, www.dowjones.com/professional/risk/glossary/financial-crime/counter-terrorist-financing/.

[5] "UN Trade Body Calls for Halting Cryptocurrency Rise in Developing Countries | UN News." *United Nations*, news.un.org/en/story/2022/08/1124362.

[6] Bhalla, Anshika. "What Is Decentralization in Blockchain?" *Blockchain, AI & Web3 Certifications*, 13 Dec. 2022, www.blockchain-council.org/blockchain/what-is-decentralization-in-blockchain/.

[7] "Money Laundering." *United Nations : UNODC ROMENA*, www.unodc.org/romena/en/money-laundering.html.

[8] QR Code Definition and Meaning | Collins English Dictionary, www.collinsdictionary.com/dictionary/english/qr-code.

Silk Road

"The Silk Road was an ancient trade route that linked the Western world with the Middle East and Asia. It was a major conduit for trade between the Roman Empire and China and later between medieval European kingdoms and China."[9]

Terrorism

"The term "terrorism" lacks a standardised, internationally accepted definition, and thus the High Commissioner for Human Rights, in accordance with the Security Council Resolution 1566, acknowledges the following: as a minimum, terrorism involves the intimidation or coercion of populations or governments through the threat or perpetration of violence, causing death, serious injury or the taking of hostages."[10] Recently, due to the increasing needs of such attempts, their financial support or funding is being provided through cryptocurrencies.

Terrorist Cell

"A terrorist cell is a group of terrorists consisting usually of 3 to 5 members."[11]

BACKGROUND INFORMATION

Brief Historical Background of Cryptocurrencies

Cryptocurrencies were first introduced in 2009, when the first decentralised currency, Bitcoin, was originally created. Its creator was a software developer known only by his pseudonym Satoshi Nakamoto. Cryptocurrencies were established as a secure and anonymous means of transferring funds without being able to track each party's activity. Nowadays, virtual assets are of great value that they, amongst NFTs are considered "digital gold". Bitcoin, and cryptocurrencies in general, gained popularity due to their ability to execute immediate and direct transactions, without mediators, bank controls, fees or border restrictions. Shortly after the creation of Bitcoin, Blockchain and Ripple emerged.

Cryptocurrencies and their Mechanisms

Cryptocurrencies were originally created so as to offer users the anonymity, security and individuality physical banks were not providing costumers. Nevertheless, in order for them to ensure their functionality, certain new mechanisms needed to be developed including Blockchain technology, decentralised networks and encryption techniques. Blockchain Technology refers to "an advanced database mechanism that allows transparent information sharing within a business network. A blockchain

[9] Britannica, The Editors of Encyclopaedia. "Silk Road." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 17 Aug. 2023, www.britannica.com/money/topic/Silk-Road-trade-route.

[10] "Ohchr and Terrorism and Violent Extremism." *OHCHR*, 10 Feb. 2023, www.ohchr.org/en/terrorism. Accessed 31 Aug. 2023.

[11] "Terrorist Cell - Definition, Meaning & Synonyms." *Vocabulary.Com*, www.vocabulary.com/dictionary/terrorist%20cell.

database stores data in blocks that are linked together in a chain".[12] A decentralised network is "a network configuration where there are multiple authorities that serve as a centralized hub for a subsection of participants. Since some participants are behind a centralized hub, the loss of that hub will prevent those participants from communicating". [13] Finally, encryption techniques are "method[s] by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*. In computing, unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms, or ciphers".[14]

Examples of cryptocurrencies

Bitcoin(BTC)

Bitcoin, being one of the oldest and most well-known cryptocurrencies, has been previously utilised in terms of financing a variety of illicit activities. Its impact on terrorist attacks has been deemed negligible but it shall not be ignored due to its terrorist financing capabilities and the interaction between attacks and its price. Bitcoin is often correlated to illicit activities, mostly money laundering and terrorism. Bitcoin has been preferred amongst other virtual currencies for its anonymity and the ability of users to raise and transfer funds worldwide. Moreover, with current anti-terrorism projects, terrorist groups have realised the potential tracing risks of depositing funds in physical bands, and have, thus, resulted in the search for a means to deposit and withdraw funds from oil trafficking and smuggling without their physical presence. Finally, Bitcoin prices are highly affected by terrorist attacks, with the value of the specific currency increasing. The Bitcoins in possession of terrorist organisations will increase in value and, thus, facilitate illicit acts, but they will also encourage individuals and groups to seek for another means of transferring funds, potentially the traditional banking system, due to the need of a surveillance mechanism. TF-related organisations known to have acquired profit through BTC are al Qaeda, ISIS and Hamas.

Ethereum(ETH)

ETH was first received by specific terrorist organisations in August 2020 through August 2021, amongst other donations and tokens. This type of financing almost similar to a fundraiser was encouraged by a Saudi-led jihadi activist movement which began requesting donations in such form. The

[12]" What Is ..." *Amazon*, The University, 1978, aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc.
[13] Editor, CSRC Content. "Decentralized Network - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/decentralized_network. Accessed 17 Nov. 2023.
[14] Loshin, Peter, and Michael Cobb. "What Is Encryption and How Does It Work? - Techtarget." *Security*, TechTarget, 28 June 2022, www.techtarget.com/searchsecurity/definition/encryption.

movement and its leader have advocated for the Taliban uprising in Afghanistan and have taken advantage of multiple cryptocurrencies so as to incite violence. Apart from ETH, BTC, XRP and ERC20 were used. 18.6% of the movements' income was through ETH according to coinbase. Terror financing in ETH has been alternating since.

Non-fungible tokens (NFT)

NFTs are very commonly used in terms of laundering the profits of TF-related activities. NFTs are very similar to cryptocurrencies, but private cryptographic keys are needed for them to be transferred or raised. NFTs have been used due to several of their traits. The private cryptographic keys are not necessarily connected to an identity, meaning users are allowed to connect their keys to a pseudonymous without stating their true identity. Furthermore, when the keys are known to both ends of a transaction, it can be carried out on a public blockchain without verification, by anyone towards anywhere in the world with no inspection or custom check. At last, the pricing is subjecting. The value and price of an NFT is constructed based on demand and buyers' offers.

Use of Cryptocurrencies in Terrorism Financing

Cryptocurrencies in terms of financing terrorism are not typically used via legitimate means. Groups take advantage of cryptocurrencies and their characteristics so as to manipulate an audience and make profit from certain situations. The specific case could be characterised as an abuse of cryptocurrencies and their traits. Terrorist organisation prefer cryptocurrencies over physical currencies due to the high levels of discretion, anonymity and potential pseudonymity. More specifically, their use is a rather effect means of conceal sources, location, funds and personal data that could be disclosed via a banking system. With the true identities of individuals being hidden, it is very difficult for illicit activities to be tracked but mostly apportioned for.

Due to certain beliefs popular amongst terrorist groups, communication or collaboration with third parties, organisations or government is of great difficulty. Thus, groups are looking for ways to transfer and raise funds without requiring a mediator or the involvement of anyone not deemed trusted. Cryptocurrencies allow for transactions without third parties or banks. Crypto-funds are not backed by governments or nations and, thus, make exchanges easier and safer for illicit activities to be funded. Finally, due to this "liberty" in transactions, funds can be moved without restrains, even across borders to anyone, at any time without being taxed extra. This allows for terrorist organisations to participate in money laundering and receive funds from worldwide sources without those being tracked.

Nowadays, the needs of terrorism have exceeded the funding of specific illicit activities. Groups have been organising attacks and violent outbursts with donations from civilians or other groups. Nonetheless, significant financing is also required for other procedures. Groups act similarly to organisations with some type of structure, function and goal. In order to provide for the members, the technical necessities and the maintenance of stability, funding is vital. Finally, terrorists base their goals and aspirations to their beliefs and ideologies which they attempt to spread and fully support. This type of promotion is of high cost considering the risk, the necessary anonymity and the illicit activities involved.

Case studies

ISIS and crypto funding

With jihadi families trapped in Syrian refugee camps, women, mostly Europeans, in an attempt to acquire their freedom have commenced to engage in fundraising drives. Such fundraisers utilise social media platforms and numerous transfer apps, including cryptocurrencies. Multiple of these attempts are ISIS-affiliated, exactly like the individuals engaging in such. The "Independent" has conducted a research showing women all over Syria promoting fundraising drives via the use of cryptocurrencies and other virtual funds so as to send laundered money to smugglers, with the ultimate goal of bribing security officials and allowing the escape of such camps. Moreover, when the aforementioned is not possible women desperate to facilitate their stay or to accelerate their escape, send messages on Facebook pages and online Telegrams to individuals requesting funds. A great example would be Sara[15]. She is a European woman deemed to be affiliated with ISIS. She is one of the Manu women directing messages to the wider community begging for cash or money transfers. Her request is specific. She needs 15.000$ so as to flee to Turkey, Idlib or anywhere else. She states to have already acquired 2.000$, with that sum not being sufficient as a counterweight for her freedom. Sara, in order to execute her plan towards freedom, utilises an encrypted application while being in al-Hol, a desert camp with 65.000 residents from the caliphate.

[15]" Cryptocurrency and the Crumbling Caliphate." *The Independent*, Independent Digital News and Media, 26 Oct. 2021, www.independent.co.uk/news/world/islamic-state-women-syria-money-b1763450.html?src=rss.

Al-Qaeda and Bitcoin

Amongst a great number of groups and organisations in Syria utilising cryptocurrencies, Al-Qaeda is definitely a prominent one, with the exploitation of Bitcoin. Such schemes included Jaish al-Ummah, an Al-Qaeda affiliated organisation based in Gaza engaging in a fundraising drive in May of 2019, with the aim of supplying fighters with weapons and ammunition. In general, Al-Qaeda established a bitcoin money-laundering network utilising social media platforms and other digital applications via which they were able to request funds. Such funds, necessary for the execution of violent acts of terrorism were presented as donations to charity. The aforementioned scheme gained attention when undercover Homeland Security Investigations (HSI) officers communicated with the administrator of Reminder for Syria, a charity requesting bitcoin donations to fund illicit activities, who stated the destruction of the United States of America as the primary goal of the fundraiser and discussed the price of surface to air missiles (SAMs) while warning the officers about potential criminal consequences of carrying out a jihad in the US.[16]

Use of Cryptocurrencies in financing illegal activities

Due to the constantly increasing use of virtual funds, cryptocurrencies have also been utilised as a means to finance further illicit activities. Besides terrorism and such organisations there have been numerous cases during which cyber-criminals utilised cryptocurrencies to execute multiple illegal activities. Payments demanded in cryptocurrencies, Dark Net market demands, money laundering and scams have now adapted to the developing digital economy. Some great examples of the aforementioned circumstances include Silk Road, the Mt. Gox Hack and Ransomware attacks such as WannaCry and NotPetya.

[16]“ Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.” Office of Public Affairs | Global Disruption of Three Terror Finance Cyber-Enabled Campaigns | United States Department of Justice, 13 Aug. 2020, www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Moreover, Silk Road is the name given to an anonymous narcotics illegal market. The whole exchange process of narcotic and cryptocurrencies took place in an anonymous, encrypted network. According to Forbes[17], Silk Road as a whole was estimated to be making about 30 to 45 million $ in annual revenue. It was fully functioning as the main network for the digital purchase of drugs via the use of cryptocurrencies for 2 and a half years when the main administrator's identity was discovered by FBI agents. The Dread Pirate Roberts was unmasked. The specific pseudonym, at that time was referring to Ross William Ulbricht, but it is not certain whether or not he had acquired from the creator of the aforementioned network. Ulbricht was arrested in San Francisco after a series of mistakes and miscalculations. The FBI chose not to disclose a variety of information but after certain of their statements, it is believed that his interview with Forbes, and a package addressed to the place he was found in containing multiple counterfeit documents with his picture but different names, were the main components that cost him his freedom. Despite the careful use of pseudonyms and encryption techniques it has been suggested that he has also made quite a few mistakes in IP dresses for a VPN server, leading to a handle connected to his personal Gmail address. Briefly, Ulbricht was able to establish an online environment functioning as a "narcotics bazaar" as it has been characterised, via the exploitation virtual funds. Cryptocurrencies provided both the administrator of the network and the users with the appropriate anonymity and pseudonymity so as for them to fully partake in the already described type of exchanges. Regardless of Silk Road's activity being ceased, cryptocurrencies were prominently used to fund a type of illicit activity and even today there still are different similar network taking advantage of virtual currencies, which do not allow for the criminals behind these attempts to be identified.

Mt. Gox[18] was one of the largest Bitcoin exchange companies. It was based in Japan and was established by US programmer Jed McCaleb in 2010. Almost a year later, in 2011, it was sold to French developer Mark Karpelés. 2013 was the year during which Mt. Gox handled 70% of the total worldwide transactions of Bitcoin. By the end of February 2014, though, everything had changed. Mt. Gox was hacked and it was, thus, never able to return to its previous standards. It is believed that the hacking activity can be traced all the way to 2011. In June of the same year, the company suffered from an early act of hacking, including the change in Bitcoin price to 1 cent. Cyber-criminals purchased Bitcoin at the specific price via the use of the private hot wallet keys of users, meaning they acquired access to personal digital wallets of Mt. Gox customers. Through the described process, they obtained 2.000 bitcoin. In the specific timeframe, customers purchased an estimate of 650 bitcoin with 0 of that amount

[17] Greenberg, Andy. "End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market." *Forbes*, Forbes Magazine, 29 Jan. 2014, www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/.

[18] Jordan, Tuwiner. "Mt Gox Hack Explained." *Date, History & More (2014)*, buybitcoinworldwide.com/mt-gox-hack/#what-was-mt-gox. Accessed 23 Nov. 2023.

ever being returned to them. In an attempt to prevent what was proven to be inevitable, the administrators of Mt. Gox increased security measures. Nevertheless, the company failed to preserve the transactions and finally, in February 2014, hackers accessed and stole 740.000 bitcoin from Mt. Gox users and a further amount of 100.000 directly from the company. After certain investigations, it was proven that the necessary private keys to access the company was unencrypted and stolen already in 2011. It still remains unknown whether this decryption is connected with the past hacking attempts or if it is a case of an individual from within the company aiding the execution of the specific activity. Even today, numerous details and pieces of information have not been disclosed. Former employees state to have been aware of mismanagement or organisation issues within the company, but nothing was ever officially confirmed. It has even been alleged that 80.000 bitcoin was already missing when the company was bought by Karpelés. Thus, the aforementioned is another one of the numerous schemes devised so as for cryptocurrencies to be used in a manner opposite to their reason of creation.

Challenges and Issues

Due to the way society has been formulated, cryptocurrencies even though developed to aid an international economy in need are currently being used in a way which is harmful not only for financial systems but for nations as a whole. The use of cryptocurrencies today has produced a great number of issues and obstacles that need to be faced. The majority of such challenges refer to the regulation of financing terrorism and further illicit activities. More specifically, cryptocurrencies are characterised by a set of traits which were actually fundamental for their creation. These include the anonymity and pseudomyity they provide to users and the ability to execute cross-border transactions while utilising decentralised technologies and not allowing the interference of third parties.

Such issues can be divided to both physical challenges and ethical considerations or dilemmas. In terms of the first subdivision, the anonymity of users which occurs as a result of the pseudonymity provided to them by the virtual currency platforms is a major problem. Individuals and groups are able to transfer, exchange and purchase funds without disclosing any type of personal information. Thus, it is of utmost difficulty for regulations to be set. By depriving users of their anonymity, the concept of cryptocurrencies ceases being in order and virtual funds will be of no use to the wider public. For the exact same reason, it is not feasible to impose third parties into the transaction process making monitoring the situation almost impossible. In addition, the execution of cross-border transactions with no taxation is being allowed. As beneficial as it could be proven in numerous occasions, the origins of virtual funds shall still be examined. The absence of taxes does not allow for the free transportation of all funds, since it is of major significance for their sources to be scrutinised and their documentation available.

Concerning ethical dilemmas, it is of great difficult to showcase one as the prominent one, but the following are the two most common ones. The subject at hand is balance. It is rather concerning that nations might not be able to balance regulations while

allowing innovation. Furthermore, it is difficult to find a balance between privacy rights of individuals and security concerns. The concept of anonymity functions like a safety net for users not wishing to disclose personal data. In certain cases, this ability to hide someone's identity could be hazardous. Thus, it is impossible for nations to make any amendments. Which should be prioritised, the well-being and facilitated transactions for users or prevention of risks? It is not easy for a nation to decide upon a matter that decreases the benefits of either its citizens or its financial system. Cryptocurrencies finally offer the advantage of censorship-resistant transactions, which means that they allow individuals to conduct financial activities without a centralised agency interfering. This feature raises ethical questions when cryptocurrencies are used for illegal purposes, such as funding terrorism or facilitating the sale of illicit goods.

Regulatory Efforts and International Response

The majority of nations have established certain regulations towards the hazardous use of cryptocurrencies. The aforementioned have occurred either as national means of protection or as a result of international collaboration so as to tackle the issue of the extensive utilisation of virtual funds to fund terrorism and other illicit activities. These include case/nation-specific attempts with the ultimate goal of minimising the exploitation of virtual funds for the execution of illegal actions.

A great example showcasing an international response action plan is the following of the International Monetary Fund (IMF). On the 24th of February 2023[19], the IMF constructed a 9-point plan about nations' necessary response to virtual assets. In addition to the above, the importance of not allowing cryptocurrencies to gain legal tender status was stressed, while a paper was discussed: "Elements of Effective Policies for Crypto Assets". Some of the solutions nations were provided with were to strengthen their frameworks and policies and to increase requirements for all virtual funding networks. The status of a cryptocurrency shall be monitored and in accordance with future international arrangements that are to be established, supervision should be enforced. Thus, it is imperative for nations to comply to such attempts while developing, adapting and enhancing their own. The aforementioned is only an example with a more thorough review of specific nations' existing response plans and legislations being given in the major countries and organisations involved section of this guide.

Implications on international peace and security

Concerns and threats to international peace and security have arisen from the rapidly growing use of cryptocurrencies in financing terrorism. Due to the anonymity and pseudonymity, terrorist organisations take advantage of situations which has resulted in an increase of cyber-attacks, strengthening digital terrorism initiatives.

Moreover, certain cryptocurrencies such as Bitcoin, when used as a form of TF, have the power to undermine government authority by circumventing capital controls

[19] Jones, Marc. "IMF Lays out Crypto Action Plan, Recommends against Legal Tender Status." *Reuters*, Thomson Reuters, 24 Feb. 2023, www.reuters.com/technology/imf-lays-out-crypto-action-plan-recommends-against-legal-tender-status-2023-02-24/.

imposed by it. Numerous cryptocurrencies allow users to avoid taxes and control even when transferring funds worldwide. The specific transaction system which does not include a third party, in contrast to traditional banking, may destabilise a nation's financial system by enfeebling the existing infrastructure and decreasing a government's role in it.

At last, criminal activity and illicit acts are being funded by cryptocurrencies and, thus, terrorists have discovered a more advanced means of executing unlawful projects. Terrorist activity is becoming very difficult to track, creating various safety issues. The behaviour and decision-making of such organisations which is based on their funds cannot be predicted due to lack of surveillance in terms of their transactions and "easily-laundered" money. Cryptocurrencies have increased the financing opportunities for terrorism and, thus, constitute a major component in the attacks, violence and illicit activities taking place.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Syrian Arab Republic

Numerous terrorist groups in Syria have received or requested financing through cryptocurrencies to benefit from their traits and take advantage of people's donations. From Bitcoin to even Google Play gift cards, civilians and supporters of illicit activities have been attending to fund them throughout the whole world. Multiple terrorist organisations in Syria have now created Bitcoin wallets requesting funds from worldwide sources.

On February 2023[20], a woman in New York City known as Bakhrom Talipov or Victoria Jacobs, was charged for financing acts of terrorism in Syria using cryptocurrencies. She provided the funds necessary for multiple illicit activities including money laundering and other crimes. Malhama Tactical received more than 5.000 dollars from Victoria Jacobs. In addition to the above, in an attempt to aid the same organisation, she laundered 10.661 dollars on their behalf, via the use of cryptocurrency amongst others. She was even encouraging other civilians to join her contributions, as proven from her cell phone notes.

Similarly, in December 2022, four defendants [21] were charged with utilising cryptocurrency, Bitcoin wallets, and GoFundMe to support the Islamic State of Iraq and the Levant (ISIS). According to them, they were collecting "blood money". In

[20] *ABC News*, ABC News Network, abcnews.go.com/US/new-york-city-woman-charged-financing-terrorist-groups/story?id=96818461. Accessed 16 Nov. 2023.
[21]" Four Defendants Charged with Conspiring to Provide Cryptocurrency to Isis." Eastern District of New York | Four Defendants Charged with Conspiring to Provide Cryptocurrency to ISIS | United States Department of Justice, 15 Dec. 2022, www.justice.gov/usao-edny/pr/four-defendants-charged-conspiring-provide-cryptocurrency-isis.

general, apart from the specific case, there have been quite a few cases of cyber-enabled campaigns financing Syrian terrorist groups. Those participating, engaging, and helping were not always directly connected to Syria.

Nevertheless, there are various factors limiting the utilisation of virtual funds when funding terrorism and other illicit activities in Syria. The most prominent include the lack of internet access of certain groups and individuals, the absence of technological education of the general population in the Syrian Arab Republic and finally, the difficulty in accessing vendors converting digital currencies to other financial assets. Still, numerous private ledgers and cryptocurrencies are being used to enhance the anonymity of fund-transfers in Syria. [22]

United Nations Office of Counter-Terrorism (UNOCT)[23]

The United Nations Office of Counter-Terrorism provides UN Member States with the necessary policy support, spreads in-depth knowledge of the United Nations Global Counter-Terrorism Strategy, and, wherever necessary, expedites the delivery of technical assistance across four pillars. Those include: measures to address the conditions conducive to the spread of terrorism, measures to prevent and combat terrorism, measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard, and measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism[24]. It was established on June 5, 2017 through the UN General Assembly Resolution 71/291. The specific office works closely with the Security Council and its bodies to prevent and respond to terrorist attacks. The Counter Terrorism Committee (CTC) of the Security Council (SC) collaborates greatly with the UNOCT while conducting informative and research-related seminars and missions to numerous nations dealing with hazards caused by increased illicit activities. The CTC prioritises cases of recorded crypto-funds being donated to such causes.

Among its functions and responsibilities, the UNOCT has previously attempted to deal with the financing of terrorism via cryptocurrencies. On September 23, 2021, the UNOCT, in collaboration with other programs, conducted a workshop in Cairo on "The risks of financing terrorism through digital payment methods (digital currencies)". Sixty participants, representing several countries, gathered to receive information and come to a decision on an action plan. Among the topics discussed were risk assessment, prevention of digital financing, crypto-related crimes, security, and

[22] Hummel, Kristina. "Examining Digital Currency Usage by Terrorists in Syria." *Combating Terrorism Center at West Point*, 14 Apr. 2022, ctc.westpoint.edu/examining-digital-currency-usage-by-terrorists-in-syria/.

[23] "What We Do | Office of Counter-Terrorism." *United Nations*, www.un.org/counterterrorism/what-we-do .

[24]" United Nations Global Counter-Terrorism Strategy | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/counterterrorism/un-global-counter-terrorism-strategy. Accessed 8 Nov. 2023.

justice agencies. Finally, they emphasised the need for multilateral cooperation so as for cryptocurrencies to not be used as a means of funding terrorism. The participants exchanged experiences, strengthened control mechanisms, and became familiarised with several frameworks. Not only were representatives from different nations able to interact and familiarise with regulations and effective means of decreasing crypto-funding of illicit activities, but they acquired information and feedback on how to ameliorate their own nations' situation. This was only the beginning, with more workshops expected to take place.

International Monetary Fund (IMF)

The IMF is a financial institution of the United Nations that sets standards for the global economy with the ultimate aim of bolstering the international economy. The specific body was funded in July 1944. It currently consists of 190 members, for whom they work to achieve sustainable growth and prosperity. One of the three main missions of this organisation is to expand trade and economic growth through collaboration. A major obstacle the IMF is facing is terrorism and its funds. The IMF has been involved in both Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). They aim to minimise and gradually terminate the access terrorist organizations have acquired to funds and cryptocurrencies through means such as but not limited to researching and establishing effective policies to protect national economies from the excessive use of virtual funds. In terms of Less Economically Developed Countries (LEDCs), the IMF, understanding the significance of a comprehensive and consistent approach to cryptocurrencies, is attempting to ensure international financial integrity, via the establishment of the aforementioned policies.

United States of America (USA)

The USA, among other nations, has faced issues with terrorism. However, there have been quite a few cases of funding terrorist organisations sourced from the US. Numerous cases of individuals utilising cryptocurrencies to fund illicit activities have been documented. Nevertheless, the increasing number of whole, individual, online campaigns bolstering virtual funds, being organised so as to support and finance terrorism of illicit activities is concerning. The specific schemes could and are taking place in the worldwide sphere, while simple citizens, within the US, reinforce their activity.

Such campaigns were operating with the aim of aiding the al-Qassam Brigades, Hama's military wing, al-Qaeda and ISIS. All the above cases have been dismantled by the US Justice Department. The common element was the use of cyber-tools and cryptocurrency donations. This type of cyber-terrorism has been detected on over four websites and Facebook pages, while criminal enterprises have also been affiliated with over 300 cryptocurrency accounts.

US Senators, nevertheless, have attempted to minimise terrorism financing. Elizabeth Warren and Roger Marshall introduced the "Digital Asset Anti-Money Laundering Act

of 2022"[25]. The aforementioned legislation would minimise the risks of money laundering and decrease the use of cryptocurrencies to finance illicit activities. Moreover, it would be capable of fully prohibiting financial institutions from using or transacting with cryptocurrencies and other virtual assets exploiting anonymity and pseudonymity based technologies. The above was designed to ameliorate and complete prior AML and CFT frameworks. Their basic intention was for cryptocurrencies to be set up based on certain ground rules, exactly like physical banks. The goal was for all financial transactions to have similar standards. The Senate prioritised validating, securing and facilitating virtual transactions via requesting that banks verify customer identities, keep records and reports of all virtual transactions under their jurisdiction and record digital wallet activities.

Afghanistan

After the takeover by the Taliban, the potential use of cryptocurrencies by terrorists quickly became a concern. Since then, their use has greatly increased. In the face of sanctions, civilians and families used such funds to cover their basic needs and for their relatives to reliably transfer them money. Non-Governmental Organisation also use cryptocurrencies as a means of aid provision due to the sanctioned state of Afghan banks. The emerging crypto-economy has been noticed by the Taliban and other affiliated terrorist organisations. The funding of Taliban in cryptocurrencies has not yet been executed. Considering the situation, though, there is a high risk of Afghanistan becoming a safe harbour for the development of illicit activities funded by digital currencies accompanied by online radicalisation campaigns. Finally, the triangular cooperation between Taliban, Beijing, and Pakistan has increased the risk of technology and cryptocurrency transfers from China to Afghanistan. China and Pakistan have affirmed their willingness to aid the Afghan population and their reconstruction commitments. Nonetheless, during their trilateral meeting with the Afghan representatives, they noted the need for the Taliban to address the security concerns with Afghanistan's neighbours. Both of the aforementioned nations are willing to collaborate so as to tackle terrorism and bolster security cooperation, and, thus, their increased cooperation has raised concerns of potential hazardous bonds being formed, including the illicit transfer of funds.

[25] *The Digital Asset Anti-Money Laundering Act of 2022 - Elizabeth Warren*, www.warren.senate.gov/imo/media/doc/Crypto%20National%20Security%20One-Pager%20draft_12.13.22.pdf. Accessed 16 Nov. 2023.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
July 1944	The IMF was funded.
26 October 1970	The BSA was signed by President Richard Nixon.
1999	The FSAP was established.
January 2009	Bitcoin was first launched by Satoshi Nakamoto.
18 July 2010	Mt. Gox was founded.
6 March 2011	Mt. Gox was sold to Mark Karpelés.
2013	Mt. Gox was handling 70% of the total worldwide Bitcoin transactions.
October 2013	The Federal Bureau of Investigation (FBI) shut down Silk Road.
24 February 2013	Mt. Gox was hacked and the website went offline.
5 June 2017	The UN General Assembly established the UNOCT via Resolution 71/291.
28 March 2019	Adoption of Resolution 2462 by the SC
August 2020-August 2021	ETH was first received by specific terrorist organisations.
23 September 2021	The UNOCT conducted the workshop on “The risks of financing terrorism through digital payment methods (digital currencies)”.
December 2022	Four defendants were charged for utilising cryptocurrency, Bitcoin wallets and GoFundMe to support ISIS.
15 December 2022	Elizabeth Warren and Roger Marshall introduced the “Digital Asset Anti-Money Laundering Act of 2022”.
February 2023	Bakhrom Talipov was charged for financing acts of terrorism in Syria.
24 February 2023	The IMF constructed a 9-point plan in terms of the international response to virtual assets.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Financial Sector Assessment Program (FSAP)

The Financial Sector Assessment Program[26] was established in 1999, and it includes an assessment of a nation's financial sector. The IMF is the organisation conducting such assessments in MEDCs, while it collaborates with the World Bank in cases of LEDCs or crises. The findings of the assessments are used to create country-specific recommendations for a state's financial system and advances. The final step is a Financial System Stability Assessment (FSSA). The FSAP provides surveillance on the economic sector and protection for its structure. The FSAP also assesses countries' anti-money laundering mechanisms (AML) as well as safeguards against terrorist funding (CTF), assuring adherence to global norms in this domain.

During the inspection, the IMF is able to identify the major components of financial systems, which, nowadays, could potentially be cryptocurrencies. FSAP does not, however, provide any particular regulations pertaining to cryptocurrencies, which compromises its effectiveness in addressing the issue of terrorism funding and financing other illicit activities through cryptocurrencies. Even though the FSAP does not have specific regulations for cryptocurrencies, since the evaluation of AML/CFT measures works within the FSAP framework, it indirectly addresses the regulation of cryptocurrencies as it encourages countries to align their regulatory frameworks with international standards, including those related to virtual assets. The aforementioned assessments and tests have not been able to prove with concrete facts the crypto-funding of terrorism. Due to anonymity, it is almost impossible for the IMF to identify certain transactions and activities, and, thus, even the FSAP, which has been very beneficial in other sectors, has not been able to aid in the situation at hand.

In order for a more successful implementation of the FSAP, a certain type of enhancement is necessary. Matters of anonymity and pseudonymity need to be considered prior to future actions. When identifying major financial components of a national economy, virtual currencies shall be inspected. It is necessary for the appropriate regulations to be established and when deemed necessary for case-specific plans or policies to be implemented, by the IMF in accordance with said nations as a whole.

[26]" Financial Sector Assessment Program (FSAP)." *IMF*, 13 Jan. 2023, www.imf.org/en/About/Factsheets/Sheets/2023/financial-sector-assessment-program-FSAP.

Bank Secrecy Act/ Anti-Money Laundering (BSA/AML) [27]

The Bank Secrecy Act[28] refers to a series of laws and regulations passed within the USA Congress in 1970 and signed by President Richard Nixon on the 26th of October 1970, which function as an attempt to tackle money laundering and terrorism financing. The BSA applies to national banks, federal savings associations, federal branches and agencies of foreign banks. It aims to achieve financial transparency and not allow anyone to abuse the existing financial system so as to engage in illicit activities. All banks and financial institutions are required to establish a BSA/AML-related program.

Among numerous laws and regulations including the establishment of BSA compliance programs, customer due diligence systems and the development of anti-money laundering programs, suspicious activity reports are of major significance. More specifically, institutions are asked to address any suspicious activities at any time and complete reports in cases of potential criminal violations of federal law or the BSA.

As beneficial as BSA has been proven, it does not at all consider the case of financing terrorism via cryptocurrencies. The emphasis is being given to physical banks and the traditional banking system, disregarding the anonymity and pseudonymity of other funding opportunities. Although banking systems should be secure and reliable, additional steps should be taken to combat illegal activity. The BSA is not the only attempt to minimise terrorism financing that does not mention cryptocurrencies, which underscores a shortfall and emphasizes the necessity of taking appropriate action in that direction.

Financial Action Task Force (FATF)

A similar set of regulations concerning the whole international community is the Financial Action Task Force Travel Rule (FATF). The above recognises the significance of cryptocurrencies in today's financial world and aims to combat money laundering as well as terrorism financing. The FATF is an inter-governmental organisation established in 1989 with the above aims. It bolsters certain policies while protecting states globally. It has 39 members and it collaborates with numerous other organisations, in an attempt to impose stricter requirements and standards on virtual asset service providers (VASPs).

---

[27]" Financial Action Task Force (FATF) Travel Rule." *Sanction Scanner*, sanctionscanner.com/blog/financial-action-task-force-fatf-travel-rule-140. Accessed 16 Nov. 2023.

[28]" Bank Secrecy Act (BSA)." *OCC.Gov*, 25 Mar. 2019, www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.

Combating the Financing of Terrorism (CFT)[29]

CFT is an attempt to deal with the financing of terrorism in general. It had been adopted by different nations and organisations and utilised as part of their legislation and strategies. After the tragic events of September 11, 2001 the IMF intensified their efforts to combat terrorism and included CFT in their AML policies and legislations. Within the first year of the CFT policy implementation, the IMF was working to assess nations' compliance to its standards and improve technical assistance on such approaches to AML. The European Union considers it the cornerstone of combating terrorism. The IMF has also engaged in CFT actions along with AML attempts. The UNODC is focusing on combating funding first and then terrorism as a whole. One of the major issues concerning CFT attempts is their insufficiency towards cryptocurrencies. The hazards evoked by the evolving virtual economy are not combated via the CFT nor are they even recognised. Thus, despite acknowledging the importance of such policies and their significant implementation into AML policies, their failure to safeguard the rights of online currency users and to ensure the appropriate documentation of transferred funds is still prominent.

Resolution 2462 (2019) [30]

On the 28th of March 2019, the Security Council (SC) adopted Resolution 2462. Through the specific resolution, the SC recognised the financial innovations and the development of new technologies. Not only was this financial progress noted, but the potential hazards of the usage of such technologies, products and services including virtual funds was also presented. The SC was deeply concerned about the potential threat to international peace and security due to the possibility of such cryptocurrencies being utilised for the funding of illicit activities and terrorism and, thus, they called upon member states to address the risks associated with digital funds. In the resolution they promoted AML policies and validates CFT standards. Financial inclusion was also bolstered while finally suggesting the use of new emerging regulatory technologies.

[29] Vbrazhko. "United Nations Office on Drugs and Crime." *Countering Terrorism Financing Is in Focus of the UNODC Training-Course for Tajik Authorities*, www.unodc.org/centralasia/en/news/countering-terrorism-financing-is-in-focus-of-the-unodc-training-course-for-tajik-authorities.html. Accessed 7 Nov. 2023.

[30] *ODS - Sédoc - United Nations*, documents-dds-ny.un.org/doc/UNDOC/GEN/N19/090/16/PDF/N1909016.pdf?OpenElement. Accessed 16 Nov. 2023.

POSSIBLE SOLUTIONS

Promotion and Modification of AML Policies

Strict Anti-Money laundering policies could be very beneficial for nations dealing with numerous cases of illicit activities and terrorism, but when terrorist organisations don't have the above options, they seek new procedures. Terrorists in need of a means to make their funds less discoverable turn to cryptocurrencies, which cannot be sourced and do not require users to disclose a real identity. Thus, AML policies in their current form could actually encourage the use of cryptocurrencies in financing terrorism. Nations should acknowledge all the above and attempt to modify existing policies and frameworks via means such as Virtual Asset Service Providers (VASPs) needing to comply with such regulations, so as to take into account all TF possibilities. Nevertheless, it is of major importance for nations' integrity to establish clear and comprehensive frameworks for virtual assets including AML and CFT regulations.

International Cooperation and Increased Transparency

Terrorism is a worldwide phenomenon that cannot be tackled within each nation separately. It is necessary for all nations to cooperate in order to combat illicit activities as a whole. It is very important that states collaborate on a financial level as well. Common policies, border taxes, worldwide transactions, and banking systems are all connected and affiliated with one another. Cryptocurrencies are the only type of financial enterprise that does not allow government or nation cooperation. Nations should increase transparency and attempt to minimise the secrecy of cryptocurrencies. International cooperation among countries and regulatory bodies to share information, best practices, and intelligence regarding illicit cryptocurrency activities is a vital aspect especially in the case of cryptocurrencies, due to their borderless, decentralised nature. The international community must also collaborate to promote the adoption of international standards, such as those set by the Financial Action Task Force (FATF), to create a consistent regulatory environment globally. In addition, international cooperation could include enhancing law enforcement capabilities. The use of cryptocurrencies to fund illicit activities has become a worldwide phenomenon, disregarding all types of borders. Thus, nations need to provide resources internationally as well as to promote responsible innovation via establishing regulatory sandboxes that allow cryptocurrency companies to innovate within a controlled environment, encouraging responsible experimentation and development.

Implementation of BSA in terms of cryptocurrencies

The BSA, in its current form, does not recognise the hazards of cryptocurrencies. The BSA shall concern cryptocurrencies and be implemented in that sector as well. In order for nations to achieve transparency and structure, it is necessary for digital funds to

be transferred in accordance with established protocols, frameworks, and pre-existing banking systems. Banks and governments are not required to be the mediators, but a potential third party could benefit the states in question due to safer transactions and better suspicious activity detention. Moreover, assessments including the FSAP could benefit numerous nations if conducted properly and in accordance to regulations about virtual currencies. The FSAP could potential require virtual wallets and funds to share certain documentation on all executed transactions so as for a means of identification of users to be available at all times. The BSA should, then, recognise the virtual funding and require banks, organisations or specific bodies to intermediate in the aforementioned processes to ensure the implementation of all standards and the transparency and safety during all types of transactions.

Increasing Public Awareness via the recognition of addresses and Quick response Codes (QRCs)

Multiple digital currencies require "keys", addresses or QRCs for a transaction to be completed. It is imperative for both nations and civilians to be aware of these addresses. QRCs and link requesting donations should be not opened nor tolerated by states. Educating the general population on whether or not to trust such campaigns is really important as well as hiring professionals able to "crack" such digital pages. Generally, though, raising awareness is always of great significance when dealing with a matter similar to combating illicit activities.

BIBLIOGRAPHY

ABC News, ABC News Network, abcnews.go.com/US/new-york-city-woman-charged-financing-terrorist-groups/story?id=96818461. We

"About Us | Office of Counter-Terrorism." *United Nations*, www.un.org/counterterrorism/about.

Abuse of Cryptocurrency to Funding International Terrorism Activities ..., prosiding.umy.ac.id/grace/index.php/pgrace/article/view/190.

Aceves, Paula. "Afghanistan's Crypto Lifeline." *Intelligencer*, 14 Sept. 2022, nymag.com/intelligencer/2022/09/afghanistans-crypto-lifeline.html.

Ali, Ikram. "D.A. Bragg, NYPD Commissioner Sewell Announce Indictment of Upper East Side Woman for Using Cryptocurrency to Fund Syrian-Based Terrorist Groups; Launder Supporters' Contributions." *Manhattan District Attorney's Office*, 31 Jan. 2023, manhattanda.org/d-a-bragg-nypd-commissioner-sewell-announce-indictment-of-upper-east-side-woman-for-using-cryptocurrency-to-fund-syrian-based-terrorist-groups-launder-supporters-contributions/.

An Overview of the Use of Cryptocurrencies in Terrorist Financing, www.coinbase.com/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing.

Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) - Topics, www.imf.org/external/np/leg/amlcft/eng/aml1.htm.

"Are Terrorist Groups Using Cryptocurrency in Afghanistan?" *Center for a New American Security (En-US)*, www.cnas.org/publications/video/are-terrorist-groups-using-cryptocurrency-in-afghanistan.

"Banker Resource Center: Bank Secrecy Act / Anti-Money Laundering (BSA/AML)." *FDIC*, www.fdic.gov/resources/bankers/bank-secrecy-act/.

cavendish_cms. The Evolution of Cryptocurrency." *Cavendish Professionals*, 15 Sept. 2021, www.cavendishprofessionals.com/the-evolution-of-cryptocurrency/.

Comment 217 - Terrorism Financing: Crypto-Taliban?, fid4sa-repository.ub.uni-heidelberg.de/4553/1/217_COMMENT-217.pdf.

"Countering the Use of Cryptocurrencies to Finance Terrorism in the Middle East | Office of Counter-Terrorism." *United Nations*, www.un.org/counterterrorism/events/coutering-use-of-cryptocurrencies-to-finance-terrorism-in-Middle%20East.

DAngelo, Christian. "Everything You Need to Know about NFT Money Laundering." *Alessa*, 14 Feb. 2023, alessa.com/blog/nft-money-laundering/.

"Financial Sector Assessment Program (FSAP)." *IMF*, 19 Mar. 2020, www.imf.org/en/Publications/fssa.

"Financing of Terrorism - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - Www.Coe.Int." *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*, www.coe.int/en/web/moneyval/implementation/financing-terrorism.

"Global Disruption of Three Terror Finance Cyber-Enabled Campaigns." *Office of Public Affairs | Global Disruption of Three Terror Finance Cyber-Enabled Campaigns | United States Department of Justice*, 13 Aug. 2020, www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Greenberg, Andy. "End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market." *Forbes*, Forbes Magazine, 29 Jan. 2014, www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/.

Hummel, Kristina. "Examining Digital Currency Usage by Terrorists in Syria." *Combating Terrorism Center at West Point*, 14 Apr. 2022, ctc.westpoint.edu/examining-digital-currency-usage-by-terrorists-in-syria/.

Identifying and Preventing Terrorist and Other Illicit Financing - DNI, www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/135s_-_First_Responders_Toolbox_-_Identifying_and_Preventing_Terrorist_and_Other_Illicit_Financing.pdf.

International Convention for the Suppression of the Financing of Terrorism, treaties.un.org/doc/db/Terrorism/english-18-11.pdf.

McWhinney, James. "Why Governments Are Wary of Bitcoin." *Investopedia*, www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp.

"Money Laundering." *United Nations : UNODC ROMENA*, www.unodc.org/romena/en/money-laundering.html.

Song, Yu, et al. "Cryptocurrency Technology Revolution: Are Bitcoin Prices and Terrorist Attacks Related?" *Financial Innovation*, U.S. National Library of Medicine, 2023, www.ncbi.nlm.nih.gov/pmc/articles/PMC9860235/.

"Warren, Marshall Introduce Bipartisan Legislation to Crack down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations: U.S. Senator Elizabeth Warren of Massachusetts." *Warren, Marshall Introduce Bipartisan Legislation to Crack Down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations | U.S. Senator Elizabeth Warren of Massachusetts*, 14 Dec. 2022, www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations.

"What Is the IMF?" *IMF*, 11 Apr. 2022, www.imf.org/en/About/Factsheets/IMF-at-a-Glance.

"What We Do | Office of Counter-Terrorism." *United Nations*, www.un.org/counterterrorism/what-we-do.

MULTIMEDIA RESOURCES

Clark, Adam. "Bitcoin Falls below $26,000. Here Are the next Price Levels to Watch." | *Barron's*, Barrons, 28 Aug. 2023, www.barrons.com/articles/bitcoin-ethereum-prices-crypto-markets-today-bfc4cd69.