Research report

Forum: United Nations Office on Drugs and Crime

Issue: Addressing the role of cryptocurrency in facilitating money laundering and organised crime networks

Student Officer: Anna Glienke & Jasper Visser

Position: Head Chair & Deputy Chair

LMUNA
Lorentz Lyceum
Model United Nations
Arnhem

Introduction

The banking industry has been transformed by cryptocurrencies due to their anonymity, decentralisation, and transactional convenience. Nonetheless, there are disadvantages that accompany these benefits. One of the most severe challenges is that cryptocurrencies have become a popular means to finance illicit activities such as drug trafficking and other illegal operations. Because of the structure of cryptocurrencies, they do not rely on banks, enabling individuals to send, purchase, and exchange money and assets through cryptocurrencies. The lack of a centralised authority is a double edged sword. While it is a benefit for users, the same aspect makes it impossible to enforce compliance with regulatory bodies, thus exercising law enforcement control becomes extremely difficult.

The use of digital currencies to finance terrorist groups and activities has been a major growing concern for governments and international organisations around the world. So far, countries and regulatory groups such as the Financial Action Task Force (FATF) and the United Nations (UN) have actively worked on new frameworks and policies such as Resolution 2462 stating that “all States shall prevent and suppress the financing of terrorist acts and to refrain from providing support to those involved in them.”(Security Council”) to increase responsibility and security among cryptocurrency exchanges to mitigate the risks involved in transactions.

Definitions of key terms

Cryptocurrency

A digital or virtual form of currency that operates independently of a central bank. However, some currencies known as stable coins may rely on governments or banks to maintain a fixed rate.

FATF (Financial Action Task Force)

A multi-governmental body that is responsible for setting policies to prevent money laundering as well as the funding of terrorism. The FATF was established in 1987 and has a public blacklist. If a country ends up on this blacklist, FATF member states will impose economic penalties or restrictive measures. Countries on the blacklist include the DPRK, Iran, and Myanmar. To add further precision to this process, they additionally have a grey list which includes the countries under increased monitoring.

Blockchain

A system in which a record of transactions, especially those made in a cryptocurrency, is maintained across computers linked in a peer-to-peer network. (Ark21 shares)

Dark Web

Websites that require specific software configuration or authorisation to access, allowing users and website operators to remain anonymous or untraceable. It is a hidden, unindexed section of the internet which requires additional anonymising software such as Tor. Most times illicit activities take place, which include the trade of stolen data and illegal goods.

Terrorist Financing

The use of either legal (regulated) or illegal means to provide finances to terrorist organisations frequently with the purpose to fund actions supporting and/or promoting one's political and cultural beliefs.

KYC (Know Your Customer)

A mandatory process in which financially focused businesses verify the identity of their customers. This is extremely vital for the prevention of illegal activities such as money laundering, fraud, and terrorist financing. It is a general regulatory measure which has steadily been increasing in popularity over the last few years.

Money Laundering

Money laundering is a process in which illegal money is made to look legitimate. This illegal money usually originates from drug trafficking, fraud, tax evasion or corruption. Oftentimes this money is also linked to other crimes such as kidnapping, blackmailing, or large-scale robberies.

Mixers

Crypto mixers are used to hide the origin and destination of cryptocurrency coins. They do this by blending the funds of a multitude of users and concealing the origin and future destination of the digital currencies. This makes crypto mixers efficient tools in covering the traces of cryptocurrency transferrals and makes them a popular tool for money laundering.

AML/CTF

AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) refers to a set of laws, regulations, and procedures designed to prevent and detect the illegal movement of funds through the financial system.

General overview

The implications of financing crime through the use of cryptocurrencies pose a major threat to international security and the global economy as a whole.

Due to the anonymity of transactions and the absence of a centralised body regulating such transfers, traces are left covered, resulting in highly attractive transfer environments for illicit groups. These illicit groups are primarily responsible for facilitating money laundering, organised crime networks, and even funding terrorist organisations such as Hamas, al-Qaeda, and ISIS. The use of digital currencies to finance terrorist groups has been a rising concern for governments and international organisations around the world due to previous examples of terrorist attacks such as 9/11, the Munich Massacre, or the Oklahoma City Bombing.

When looking at the structure of cryptocurrencies, they are not reliant on banks, which enables individuals to send and purchase without being registered to a specific government-registered economic forum. This is very impractical for being able to trace back illicit activities, since this gives criminal users the perfect framework for hiding their identities when making transactions. This transactional convenience is primarily caused by a lack of regulations due to no real centralised authority being put in place to control and implement, supervise and adjust accordingly.

A major aspect in combating this issue is the challenge in prosecution. Due to the central lack of authority, it becomes increasingly difficult to hold criminals accountable for their actions and prosecute them. So far, countries and regulatory groups such as the FATF and the UN have actively worked on new frameworks and policies such as Resolution 2462, stating that “all States shall prevent and suppress the financing of terrorist acts and refrain from providing support to those involved in them.” (Security Council) to increase responsibility and security among cryptocurrency exchanges to mitigate the risks involved in transactions.

Cryptocurrencies allow transnational terrorist groups to self-operate without funding from banks and avoid detection by financial intelligence due to their decentralised nature and the ability to obscure identities behind wallet addresses. This poses a great threat to the international market since the use of cryptocurrencies for financing crimes undermines international security and destabilises the economy.

While blockchain transactions are public, the anonymity of wallet addresses makes it challenging to identify individuals involved in transactions. Also, holding criminals who shift funds through the use of cryptocurrency accountable is extremely difficult, as there is no governing body to take action on those who aid terrorists and convict them for their crimes. Due to this lack of a governing body being in place, terrorist organisations can send and receive funds worldwide without regulatory restrictions, complicating enforcement.

Major parties involved

United States

The United States advocates regulating the use of digital currencies and has also attempted to confiscate digital assets associated with terrorist groups. They actively seize cryptocurrency wallets which are tied to terrorist groups such as Hamas, al-Qaeda, and ISIS. Their Department of Justice (DOJ) and Treasury's OFAC get actively used to investigate and sanction illicit crypto activity. By balancing innovation with concern over terrorist financing, money laundering, and fraud, they have been one of the main parties actively taking part in combating this issue. Their main goal is to implement a strong regulation for digital assets to prevent misuse.

European Union

The European Union backs markets in Crypto-Assets Regulations (MiCA) for a single EU-wide framework. Their main goal is to increase transparency to protect consumers from crypto-related risks. A big requirement the EU has established is that they require crypto-asset service providers (CASPs) to register and comply with AML/CTF standards. They seek to close the gap that could allow terrorist groups to exploit loopholes and further improve safety standards, eliminating potential risks entirely. Their main goal is to impose a singular framework for cryptocurrency, which everybody complies with.

China

Through the implementation of bans on crypto mining and trading in 2021, they have been promoting their own "central bank digital currency" (CBDC/the digital yuan) and offering their state-controlled alternative. Their reasoning behind this is that "cryptocurrency transactions are a threat to financial security and illegal financial activities." According to China, crypto poses high risks in crime prevention,

and they have therefore strongly cracked down on the use of cryptocurrencies, making them part of the 42 other countries that have implicitly banned digital currencies through restrictions or direct prohibition.

Financial Action Task Force (FATF)

To combat the financing of terrorism and money laundering, the FATF highly suggests regulatory measures and frameworks which member states can implement. By setting international standards, they additionally take an active role in combating this issue and have been quite successful in the process of doing so. A recommendation for member states to regulate Virtual Asset Service Providers (VASPs) was also something they have been adamant about. They push for a "Travel Rule" for crypto transactions which would require the exchange of the sender and receiver's information. Additionally, they monitor different countries' compliance with these suggested regulatory measures and mark states that are non-compliant on the "grey" or "black list", which results in FATF member states imposing economic penalties or restrictive measures.

United Nations

The United Nations take on an active role within this issue, as they call for global collaboration to deal with the usage of new tools like cryptos by terrorists. In 2019 the United Nations passed resolution 2462, which says that "all States shall prevent and suppress the financing of terrorist acts and refrain from providing support to those involved in them." ("S/RES/2462(2019) | Security Council") This resolution reaffirmed the close collaboration of the UN and the FATF when creating and implementing global standards which can effectively combat the ongoing issue of money laundering and terrorist financing.

Non-profit organizations

Many organisations, like Chainalysis and Elliptic, have been concentrating on tracing and monitoring illegal cryptocurrency transactions and working closely with law enforcement agencies. Their special focus is on blockchain analytics to track illicit crypto flows. They provide many tools and data to law enforcement, regulators, and governments, which is very practical for logistical planning and analysing the success or failure of newly implemented laws. Huge support in the seizure of assets by mapping wallet networks linked to criminal and extremist groups has also been something NGOs have proven to be vital to. Additionally, their help in uncovering terrorist fundraising campaigns using Bitcoin, Ethereum, and privacy coins has been very successful and quite helpful.

Timeline of Key Events

Year	Event
2009	Bitcoin becomes the first decentralized cryptocurrency being created by an unknown person or group using the alias Satoshi Nakamoto.
2013-2014	Law enforcement and regulatory agencies express their concerns about the potential funding of terrorism through the usage of various cryptocurrencies.
2015	The Financial Action Task Force (FATF) presents its first report that defined virtual currencies, identified potential AML/CFT risks, and proposed a risk matrix. This effort laid the groundwork for subsequent guidance on regulating cryptocurrencies to combat illicit activities.
2019	FATF extends anti-money laundering (AML) and counter-terrorist financing (CFT) standards to virtual assets and virtual asset service providers.
2019	Hamas initiates its first large scale cryptocurrency collection campaign. The US goes on to freeze several cryptocurrency accounts and websites associated with the Hamas militarized faction, the Izz al Din al Qassam Brigade.
2020	The Office of the Comptroller of Currency in USA places a sanction on Safra Bank of New York citing noncompliance to counter of money laundering and financing terrorism in relation to cryptocurrencies.
2021	Coinbase noted that Hamas was involved in raising funds through cryptocurrencies.
2021	Israeli authorities started the confiscation of dozens of cryptocurrency addresses related to Hamas, PIJ, and other terrorist groups.
2022	The Basel Committee on Banking Supervision (BCBS) releases a proposed set of global power-based regulations for banks participating in crypto markets.

April 2023	The U.S. Treasury puts out a notice regarding financing of terrorism connected with Hamas, alerting the public to the phenomenon of fundraising with virtual currency.
June 2023	The European Union brings into effect the Market in Crypto Assets regulation (MiCA), which sets out a detailed policy to regulate the crypto-asset market.
October 2023	Attacks on Israel by Hamas brought renewed attention to how cryptocurrencies are used to fund terrorism.
November 2023	The Treasury Department draft legislation to mitigate the cryptocurrency-based AML challenge.

Previous attempts to solve the issue

Money laundering and crypto-crime groups remain substantial and unresolved global issues, however, there have been attempts made to address it, attempts that pave the way whereupon frameworks can be constructed.

The United States drafted amendments to existing Anti Money Laundering & Counting Funding of Terrorism legislature, adding increased focus on risks posed by cryptocurrency. These laws cover wide ranges of asset actors including wallet providers and intermediaries. Stricter obligations on reporting suspicious crypto transactions and greater emphasis on penalties for non-compliance greatly improved the safety within trading communities.

Additionally, the European Union implemented regulations aimed to increase the traceability of crypto transactions by obliging providers of such services to collect and share sender and recipient data. The EU also tackled jurisdictional loopholes by strengthening cooperation across borders and targeted money laundering and terrorist financing within the ever-growing digital asset space.

To ease the process of tackling and convicting such illegal activities and criminals, The United Kingdom passed laws granting authorities the power of seizing crime/terrorist linked crypto-assets swiftly and efficiently.

While these legislatures and regulations are effective, they are not complete. These attempts should be seen as inspiration, forming foundations for UN resolutions to address these issues on a global scale, unifying nations with the same clearer and more effective ways to tackle the fraudulent use of cryptocurrencies.

Possible solutions

To combat money laundering and crypto-crime in the global atmosphere, we must act now or suffer the consequences. It is imperative that this council construct a resolution, recognising, addressing and combating the issue. Some member states have adopted legislature, but some have not, and in a global age of polarity it is crucial that nations stand together and maintain the same effective preventative and responsive measures.

International cooperation can only exist with functioning national cooperation.By stimulating Public-Private partnerships, agencies collaborate with cryptocurrency exchanges, thus combating illegal activities more effectively. Government agencies and the private sector both lack what the other has, with cooperation standing strong as centre of operations.

By implementing targeted financial sanctions, similar to those used to combat the financing of weapons, involving the freezing of assets and prohibition of providing funds to individuals and/or entities. These measures could be taken to combat (extreme) terrorist funding through cryptocurrency programs, bearing in mind the possible necessity of UN Security Council authority.

Only by focusing on these above-named points together, cooperating through and within borders, can this committee produce a clear and effective resolution for all.

Further reading

www.imf.org/en/Topics/Financial-Integrity/amlcft

www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/

www.jonesday.com/en/insights/2023/06/cryptocurrencies-and-risk-under-the-antiterrorism-act

www.weforum.org/stories/2022/07/cryptocurrency-regulation-global-standard/

https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.htm

https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Bibliography

"Anti-Money Laundering and Combating the Financing of Terrorism." IMF, 22 Mar. 2023, www.imf.org/en/Topics/Financial-Integrity/amlcft. Accessed 20 Feb. 2025.

"Anti-Money Laundering and Countering the Financing of Terrorism at EU Level." Finance, 2023, finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en. Accessed 20 Feb. 2025.

Cottreau, Steven T, et al. "Cryptocurrencies and Risk under the Antiterrorism Act." Jonesday.com, Jones Day, 13 June 2023, www.jonesday.com/en/insights/2023/06/cryptocurrencies-and-risk-under-the-antiterrorism-act. Accessed 20 Feb. 2025.

"Fight against Money Laundering and Terrorist Financing." Consilium, 2024, www.consilium.europa.eu/en/policies/fight-against-terrorist-financing/. Accessed 20 Feb. 2025.

"Here's What You Need to Know about Cryptocurrency Regulation." World Economic Forum, 20 July 2022, www.weforum.org/stories/2022/07/cryptocurrency-regulation-global-standard/. Accessed 20 Feb. 2025.

Hummel, Kristina. "The Digital Terror Financing of Central Asian Jihadis." Combating Terrorism Center at West Point, 28 Apr. 2023, ctc.westpoint.edu/the-digital-terror-financing-of-central-asian-jihadis/. Accessed 20 Feb. 2025.

International Regulation of Crypto-Asset Activities a Proposed Framework -Questions for Consultation. 2022.

"Legal and Regulatory Framework for Blockchain." Shaping Europe's Digital Future, 27 Sept. 2023, digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain. Accessed 20 Feb. 2025.

REPORT on ABUSE of VIRTUAL ASSETS for TERRORIST FINANCING PURPOSES.

Team, Chainalysis. "Cryptocurrency and Terrorism Financing: Correcting the Record." Chainalysis, 18 Oct. 2023, www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/. Accessed 20 Feb. 2025.

Terrorist Financing: Hamas and Cryptocurrency Fundraising.

The Regulatory Review, and Tyler Hoguet. "Preventing Terrorist Financing through Regulation | the Regulatory Review." The Regulatory Review, 20 June 2024, www.theregreview.org/2024/06/20/hoguet-preventing-terrorist-financing-through-regulation/. Accessed 20 Feb. 2025.

“What Is Counter-Terrorism Financing (CTF), and How Does It Apply to Crypto?” Notabene.id, 2024, notabene.id/crypto-travel-rule-101/counter-terrorism-financing-crypto. Accessed 20 Feb. 2025.