



CCPCJ Chair Report

Topic 1: Regulating and Preventing the Use of
Cryptocurrencies and Digital Capital to
Finance Terrorist Organizations



Table of Contents

Personal Statements	3
Chair – Julia Oraa	3
Deputy Chair – Sunny Naha	3
Introduction	4
Glossary	5
Issue Explanation	6
Perspectives of Parties Involved	7
History of the Topic	8
Early Developments (2009–2018)	8
Increased Terrorist Involvement & Regulatory Response (2019–2024)	8
Potential Solutions for the issue:	10
Bibliography	12



Personal Statements

Chair – Julia Oraa

Distinguished guests, fellow chairs, and honorable delegates,

I am Julia Oraa, a 10th-grade student from the American School of Bilbao, and I am very excited to be your chair of the Commission of Crime Prevention and Criminal Justice this April 2025. I am from Spain and it is my first time attending MUNISS. Although I don't have previous chairing experience, I have gone to a total of 7 conferences, including those both in and out of Spain, and have experience in a variety of committees, such as Human Rights, Security Council, the International Court of Justice, etc. I am sure we will have a very fruitful and enjoyable debate and am looking forward to seeing all of you in April!

Kind regards,

Julia Oraa.

Deputy Chair – Sunny Naha

Dear Delegates,

My name is Sunny Naha, and I am a 15-year-old student at the International School of Stuttgart. I am very excited to serve as your deputy chair for MUNISS 2025. In the past, I have participated in five MUN conferences including three at MUNISS and conferences in the Netherlands and Morocco. In these conferences, I have served twice as an admin and three times as a delegate in committees such as GA4, UNODC, and the Historic Security Council.

Although this will be my first time chairing, I look forward to bringing my experience and passion for Mun to the CCPCJ committee.

I look forward to a fun and engaging conference with all of you, See you all in April!

Best

Sunny Naha

regards,



Introduction

Cryptocurrencies have reshaped the banking industry by providing anonymity, decentralization, and transaction efficiency. However, these advantages lead to several difficulties, as notably since the rise of cryptocurrencies they have become a popular tool for the funding of illegal operations such as terrorist financing. Cryptocurrencies use a decentralization system that allows people to send, purchase, and exchange financial assets without relying on banks. This causes them to operate outside financial regulators' direct jurisdiction, making detecting and preventing criminal transactions very difficult.

The use of digital currencies to finance terrorist groups and activities has been a major growing concern for governments and international organizations 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 which says that "all States shall prevent and suppress the financing of terrorist acts and to refrain from providing support to those involved in them." ("S/RES/2462(2019) | Security Council") to increase responsibility and security among cryptocurrency exchanges to mitigate the risks involved in transactions.

One example of successful combating of the misuse of cryptocurrencies is from 2021, when the U.S. Department of Justice was able to successfully seize millions of dollars worth of cryptocurrency which were traced to terrorist organizations such as Al-Qaeda and ISIS. Along with many blockchain analytics firms like Chainalysis have begun to assist law enforcement agencies when identifying and disrupting illicit crypto transactions. However, this has been quite the challenge due to the decentralized platforms, along with the anonymity of users, and lack of universal regulations as they have made enforcing laws and convicting people for disobeying them very difficult.



Glossary

Cryptocurrency: A digital or virtual form of currency that operates independently of a central bank.

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.

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

Dark Web: websites that require specific software configuration or authorization to access, allowing users and website operators to remain anonymous or untraceable (Oxford Languages)

Terrorist Financing: The use of either legal (regulated) or illegal means to provide finances to terrorist organizations as well as fund their criminal activities.

UNODC (United Nations Office on Drugs and Crime): An organization of the UN responsible for the global monitoring of money laundering and financing terrorism.

KYC (Know Your Customer): A regulation method used by financial institutions to verify customer identities and prevent illegal activity.

Money Laundering: The disguising of financial assets so they can be used without detection of the illegal activity that produced them

Mixers: crypto mixers are used to hide the origin and destination of cryptocurrency coins.

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



Issue Explanation

The implications of terrorist financing through cryptocurrencies: Can become a major threat to international security and the global economy as a whole. Due to the anonymity of transactions and the absence of a centralized body regulating the transfers, terrorist groups have increasingly started to adopt cryptocurrencies. Leading to the following issues.

Allowing the unregulated movement of money: With the use of cryptocurrencies, terrorist organizations can receive and send funds to anyone globally without regulatory limitations, which makes it difficult for officials to seize and freeze the funds. (*Terrorist Financing: Hamas and Cryptocurrency Fundraising*, n.d.)

Evading financial investigation: Cryptocurrencies allow transnational terrorist groups to self-operate without funding from banks and avoid detection by financial intelligence due to their decentralized nature and the ability to obscure identities behind wallet addresses. ("Anti-Money Laundering and Countering the Financing of Terrorism at EU Level," 2023)

The issue of convicting criminals: 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. (*Terrorist Financing: Hamas and Cryptocurrency Fundraising*, n.d.)

Fostering terrorism: Prior to cryptocurrency, terrorist organizations used more traceable and tightly regulated tactics like state sponsorship, cash smuggling, and charity exploitation. However, the growing usage of cryptocurrency allows a lot of terrorist groups to overcome restrictions put in place by financing authorities, greatly endangering the efforts towards



restricting the financing of terrorists. (“Anti-Money Laundering and Countering the Financing of Terrorism at EU Level,” 2023)

Perspectives of Parties Involved

United States: The United States advocates of regulating the use of digital currencies, they have also attempted to confiscate digital assets associated with terrorist groups. (*Terrorist Financing: Hamas and Cryptocurrency Fundraising*, n.d.)

European Union: Backs Markets in Crypto-Assets Regulation (MiCA) regulations, which seek to impose a single regulatory framework for cryptocurrency to mitigate potential risks. (“Anti-Money Laundering and Countering the Financing of Terrorism at EU Level,” 2023)

China: Bans all forms of cryptocurrency transactions and mining, claiming threats to financial security and illegal financial activities. (“What Is Counter-Terrorism Financing (CTF)” 2024)

Japan: Uses a form of registering exchange services as a legal business, with accompanying obligations for the operators to implement anti-money laundering programs. (“What Is Counter-Terrorism Financing (CTF), and How Does It Apply to Crypto?,” 2024)

Financial Action Task Force (FATF): Suggests regulatory frameworks for member states to fight money laundering and the financing of terrorism about virtual asset service providers. (“Anti-Money Laundering and Countering the Financing of Terrorism at EU Level,” 2023)

United Nations: Calls 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 to refrain from providing support to those involved in them.” (“S/RES/2462(2019) | Security Council”)

Developing nations: Many developing countries lack the technical infrastructure and expertise to effectively monitor and challenge terrorist use of cryptocurrencies, creating potential safe havens for illicit transactions

Non-profit organizations: Many organizations, like Chainalysis and Elliptic, have been concentrating on tracing and monitoring illegal cryptocurrency transactions and working closely with law enforcement agencies. (*Terrorist Financing: Hamas and Cryptocurrency Fundraising*, n.d.)



History of the Topic

Early Developments (2009–2018)

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.

Increased Terrorist Involvement & Regulatory Response (2019–2024)

2019:

FATF extends anti-money laundering (AML) and counter-terrorist financing (CFT) standards to virtual assets and virtual asset service providers. (“Here’s What You Need to Know about Cryptocurrency Regulation”)

Hamas initiates its first large scale crypto currency 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.

Israeli authorities started the confiscation of dozens of cryptocurrency addresses related to Hamas, PIJ, and other terrorist groups.

OCC grants conditional national trust charter to Anchorage Digital Bank, a crypto custodian.

2022:

The Basel Committee on Banking Supervision (BCBS) releases a proposed set of global power-based regulations for banks participating in crypto markets.

2023:

April: 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: 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: Attacks on Israel by Hamas brought renewed attention to how cryptocurrencies are used to fund terrorism.

November: The Treasury Department draft legislation to mitigate the cryptocurrency-based AML challenge.

The U.S. settles with Binance on anti money laundering and sanctions



breaches including terrorist group-linked payments.

2024:

June 19: The EU publishes an anti-money laundering and countering the financing of terrorism (AML/CFT) rules package in the Official Journal.

September 12: The 8th Global Conference on Criminal Finances and Cryptocurrencies was held in Vienna and attended by experts who discussed the new methods of abuse associated with crypto assets for organized crimes like money laundering, evasion of sanctions, and terrorism financing.²

November 6: The Council of Europe organized a seminar on "Crypto-assets and investigations" to analyze the novel approaches being used to investigate crypto-assets for laundering or terrorism financing.

Potential Solutions for the issue:

Enhanced Blockchain Analysis: Law enforcement and intelligence through blockchain innovations are actively investigating donations, facilitators, and cash links. This effort has produced successful seizures of the funds associated with Hamas and Hezbollah. (Team)

Improved Policies: New policies were drafted in November 2023 by the U.S. Department of the Treasury amending certain policies regarding anti-money laundering (AML) and counter-terrorist financing (CFT) laws with a focus towards cryptocurrency circumvention risks. They aimed to expand AML/CFT requirements across the digital world and strengthen enforcement. (*Terrorist Financing: Hamas and Cryptocurrency Fundraising*)

Global Collaboration: The EU has adopted new regulations to trace the movement of cryptocurrencies to curb money laundering and terrorist financing. Additionally, the UK has passed new laws, permitting prompt



seizure of cryptocurrencies associated with terrorist activities.(Cottreau et al.)

Public-Private Partnerships: strengthening the collaboration between government agencies and private companies. Has allowed agencies to team up with cryptocurrency exchanges and blockchain analysis firms to combat illegal activities more effectively. (“Anti-Money Laundering and Combating the Financing of Terrorism”)

Targeted Financial Sanctions: The implementation of targeted financial sanctions, similar to those used in combating the financing of weapons of mass destruction proliferation, which involve freezing assets and prohibiting the provision of funds to designated individuals or entities, typically under UN Security Council authority. Are being considered for terrorist financing through cryptocurrencies. (Team)



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 Hogue. "Preventing Terrorist Financing through Regulation | the Regulatory Review." *The Regulatory Review*, 20 June 2024, www.theregreview.org/2024/06/20/hogue-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.

