Shalva Bitsadze, Tinatin Karosanidze Free University of Tbilisi
sbits21@freeuni.edu.ge I t.karosanidze@freeuni.edu.ge

CRYPTOCURRENCY AS A NEW TOOL FOR TERRORIST FINANCING: THE CHALLENGES OF ANONYMITY AND LACK OF REGULATION FOR GLOBAL SECURITY

Abstract

The financing of terrorism is a serious global security challenge in the modern world. Against the background of technological development, new forms of financial transactions not only contribute to the development of the economy, but also provide new opportunities and other technological advantages to criminal or terrorist organizations. One such technological innovation is cryptocurrency: a decentralized and partially anonymous monetary system that works very differently from traditional financial channels. The sensitivity of the research topic makes it difficult to collect direct data, which implies studying the financing mechanisms of terrorist organizations through contact with a criminal entity, which is not only ethically but also legally unacceptable
.
Key words: cryptocurrency, terrorist financing, anonymity, global security.

Introduction

Terrorism is a constantly evolving phenomenon. When we talk about the terrorists, we should not only think about the cases of the last few years. Even in ancient times, there were groups that used violent actions for political or religious purposes, such as the Zealots or the Assassins of the Middle Ages. In the 19th century, anarchist terrorism actively spread in Europe and Russia, and in the 20th century, mass forms of terrorism took hold. Both in the past and today, terrorist acts are aimed at delivering a political or ideological message to society, although over time their scale, impact and technological means of implementation have changed significantly.

In recent years, terrorism has become a global problem that has been threatening international stability for many decades, and has become especially active in the 21st century. Terrorists pose such threat because their identification and appropriate response is a rather difficult and time-consuming process. The question arises as to why it is so difficult to identify a terrorist? It is very easy to make a distinction when you look at two radically different individuals, for example, a military man and an ordinary citizen, but in this case we are dealing with people who are almost impossible to distinguish from an ordinary citizen. Not only men, but also women and often children participate in organizations. In such cases, identification becomes difficult.

There are many terrorist organizations that differ from each other in size, structure, operational capabilities, main goal, recruitment methods and capabilities. Although their goals and methods may differ, they have one thing in common: the need for financial resources to translate their goals, ideas, and plans into actual terrorist acts. This is especially important for large-scale organizations that aim to control territories and expand

Shalva Bitsadze, Tinatin Karosanidze Free University of Tbilisi
sbits21@freeuni.edu.ge | t.karosanidze@freeuni.edu.ge

their influence. Their financial situation directly determines their operational capabilities. Accordingly, such organizations are constantly trying to ensure a stable flow of resources. The financial strategy of each group is different. However, the common goal is to develop infrastructure, expand the scope of operations, and have the appropriate weapons and military equipment. Terrorist organizations have several ways to ensure a constant flow of funds in order to carry out operations on time (FAFT 2015:9-10).

Terrorist organizations resort to traditional methods of transferring funds. They transfer quite large amounts of their money through banks. They specifically choose companies that are not officially registered and operate without the rules of the AML/CFT (Anti-Money Laundering and Counter-Terrorism Financing Act). Such unregistered companies are often chosen by Al-Qaeda, ISIS and similar groups, because any of their actions are under monitoring and with the help of these companies they can transfer safely. In addition, P2P (person-to-person) payment platforms such as Venmo, CashApp, Zelle are becoming increasingly active. Through these platforms, users no longer have to provide their bank details and send money only via a phone number or email address, which makes the trail of money circulation very vague and difficult to trace. Although registration is required on such platforms, their closed and easy-to-use structure makes them attractive to terrorists.

Money transfer companies (MSBs) play a major role in structured transactions. Despite regulations, some MSBs intentionally or unintentionally serve terrorist purposes. One example is the Lebanon-based company CTEX, which managed to transfer millions of dollars to Hezbollah. MSBs have a lower threshold for filing SARs ($2,000) than other regulated financial institutions ($5,000). MSBs are required to file suspicious activity reports (SARs). An analysis of SAR reporting shows that between 2020 and 2022, MSBs filed nearly 72% of all SARs related to TF (Terrorism Financing) (Treasury 2024).

However, traditional methods of financing terrorist organizations are becoming less and less effective, as sanctions have been imposed against them, which hinder this process. There have already been several cases where the money that was supposed to be used for terrorist purposes did not reach its destination due to the strong resistance of the state, ensuring that the organizations could not implement their plans. However, at this stage, states and those organizations that fight terrorism face a very big challenge. Despite sanctions, regulations and constant monitoring, in the modern world there is a method of transferring money through which it is almost impossible to leave a trace and find out, which is convenient for terrorists and their goals. This is cryptocurrency. Today, there are many electronic currencies, although initially the appearance of Bitcoin on the market caused confidence in crypto assets and blockchain as a whole. This technology first appeared in 2009, but at the initial stage it had little credibility. Bitcoin was very cheap and no one was putting their trust into it, but according to 2024, the total value of the Bitcoin market was $ 1.8 trillion, and at this stage it is already $ 2.1 trillion (Kerner 2024).

We are dealing with a huge industry. However, the question arises, why do millions of people use this system and why do they trust it? Blockchain has become one of the most important parts of modern technology. Nowadays, it is quite actively used by businesses, investors, governments and individuals. Blockchain is a special type of digital database that simultaneously stores information and is used by many computers that are connected to each other via a network. Blockchain is best known for Bitcoin, but its use is not limited to this. It can be used in almost all areas where we want information to be constantly protected and unchanged. The main strength of blockchain is that information once entered into it cannot be changed. Accordingly, there is no longer a need for mediators or third parties who have to periodically check the data and make corrections if necessary.

In blockchain, the system provides reliability. Transactions on blockchain are carried out according to a certain process, which may vary slightly in different systems. In the case of Bitcoin, the process is very long. Initially, the user‘s transaction is sent to a memory pool, where the information is temporarily stored until a special computer selects this information, a process known to us as „mining“. Each computer connected to the network works separately on its own block, as they select different transactions. Each one tries to solve

Shalva Bitsadze, Tinatin Karosanidze Free University of Tbilisi
sbits21@freeuni.edu.ge I t.karosanidze@freeuni.edu.ge

a difficult problem and uses a variable called a „nonce“ (Number used once). This is a number that increases each time it is used. The miner tests different values of the nonce and calculates the „hash“ of the block (when a block is filled, the program converts its contents into a unique code called „hash“. This hash is stored in the next block, and thus a chain of interconnected blocks is created, from which its name, the blockchain, comes from). If the result does not meet the desired conditions (the so-called target hash), one is added to the nonce and the attempt starts again. This cycle can be repeated several billion times per second. Ultimately, the miner who gets the „correct“ hash „wins“ and receives a reward. The block is then added to the blockchain and the transaction is considered complete. However, the transaction is only considered finally confirmed when five more blocks have been added since then. Since each block takes about 10 minutes to generate, the total confirmation time is on average 1 hour (ImmuneBytes 2023; Hayes 2024).

Crypto–activity of terrorist organizations

Despite this technological complexity, integrating crypto into any activity and fully utilizing it is available to everyone. For this very reason, terrorist organizations are already quite actively using crypto for their financing. Nowadays, it is very easy to obtain information about digital currency, as there are many articles, studies, and reports on it, and through it you will learn all the necessary information that will be needed to fully utilize crypto. Organizations such as ISIS, Al-Qaeda, the Houthis, and Hamas make hundreds of transfers every day. ISIS was the first group to integrate the use of cryptocurrency into their activities. They have been using electronic currencies since 2015. In 2019-2022 one person managed to collect and transfer more than $185,000 for the organization. In total, there were more than 300 cryptocurrency wallets, and everyone was actively using them. The case of Hamas is particularly interesting. ISIS was secretly trying to collect and send money, but in the case of Hamas, the Al-Qassam Brigades published the addresses of their Bitcoin wallets in 2019, where anyone could transfer money by going to a specific website. They had their own official website, a one-time Bitcoin address was posted, and below it was the inscription: „Donate to Jihad“ (TRM Blog 2024; TRM Blog 2025).

However, lone wolves are more dangerous than groups. They operate alone, leave almost no trace, and because their scale is much smaller, they are much more difficult to detect. They do not require large-scale logistics and large resources to achieve their goals. Lone wolves are not just „lone fighters, „ they actually occupy a very important place in the history of terrorism, where one person can influence society and the media with minimal cost (Hughes 2017; Goldbarsht 2024; Chainalysis 2020:73-77).

Global security challenges and regulatory responses, counter-terrorism measures and ways to stop the financing of terrorism. Terrorist organizations have largely mastered the use of crypto, which is why counterterrorism authorities have faced increasing challenges related to the creation and misuse of new and emerging financial technologies. Counterintelligence and counterterrorism authorities were initially unable to adapt to this sudden change and develop appropriate methods that would help them respond in a timely and appropriate manner. The UN Security Council's 2025 document on counterterrorism describes: These technologies, despite having a huge impact on society and a huge step forward in cyberspace, provide terrorists with good opportunities to finance their operations globally (Bendjama 2025:2-3).

To improve the response capacity of member states, the Algiers Guiding Principles set out four key non-binding regulatory points. The first is understanding the risks. States should study the risks of terrorist financing, especially when using new financial technologies. Having a map of potential risks allows them to identify suspicious channels in a timely manner. The second point concerns proportionate regulation. Innovation should not be stifled, but rather managed. It is important to create frameworks that identify unregistered entities without

Shalva Bitsadze, Tinatin Karosanidze Free University of Tbilisi
sbits21@freeuni.edu.ge I t.karosanidze@freeuni.edu.ge

excessive oversight. The third point involves proactively disrupting financial networks. States should improve their investigative capabilities, deploy blockchain analytics and participate in the global financial intelligence network. Mechanisms such as the use of Interpol databases, coordinated seizure of digital assets and simplified mutual legal assistance agreements are vital here. The fourth and final point concerns the measurement of the effectiveness and adverse effects of counter-financing measures. While strict enforcement is essential, these actions must comply with international law and must not disrupt legitimate financial activities. Excessive regulation can unintentionally stifle innovation in vulnerable populations and be much more damaging, as technological progress will be almost completely halted.

Consistent implementation of these basic guiding principles is very important and mechanisms such as artificial intelligence and machine learning should be implemented in financial monitoring. The creation of specialized virtual asset intelligence units and direct coordination with platforms and exchanges will be very effective in timely monitoring of transactions of any scale (Bendjama 2025:7-12).

In addition, the US has made significant strides in counterterrorism. All agencies were responsible for tracking any traces that terrorists might leave behind during their transactions. However, terrorists adapted these technologies so quickly that similar agencies could not develop the appropriate technology to neutralize the threat in time. Therefore, a new agency, the Virtual Assets Unit (VAU), was formed, as the FBI was almost inactive in this area. The VAU brought together experts in cybercrime, criminal and counterterrorism and formed a centralized, joint force that handles crypto-related cases in all sectors: from child exploitation and ransomware to terrorism and fraud. The VAU provides critical insights into how the Bureau has adapted its structure to address the emerging threat of terrorist financing in the cryptocurrency space. A key point is the VAU's fundamental integration with the FBI's Counterterrorism Division, Cyber, and Criminal Divisions (Wyman 2025).

Future prospects and risks

This issue is the most complex problem for state sectors, because when penetrating the virtual space, a specialist has almost unlimited possibilities, however, this possibility appears only if the penetration into the network was successful. And the problem lies precisely in this. Entering these networks is currently impossible, and that is why blockchain and Bitcoin are so reliable, so they are trying to improve it more and more, because transfers will be simplified and, at the end of the day, in terms of digitization of everything, people's daily purchases and activities will be relatively simplified. However, this increases new opportunities for terrorists. The future prospects of blockchain are so vast that we cannot give a specific direction for its development. In addition, a new initiative has emerged, at this stage work is already underway to integrate artificial intelligence into blockchain, as a result of which a „super-technology" will be created that will be able to do absolutely everything. Its potential goes beyond financial transactions. It includes data protection, smart contracts, global logistics, healthcare and, most importantly, the establishment of a new standard for security systems. However, this great power may turn out to be both a source of progress and a source of risk for humanity, especially when terrorist groups actively seek to exploit this technology to disperse financial flows, maintain anonymity and escape monitoring. The main motive of the state is always to develop appropriate means and implement them against terrorists, but they must approach this issue with great caution, because if it falls into the hands of a terrorist, it will have a counterproductive effect. States and international organizations will now have to not only review existing regulations, but also create completely new legal frameworks that can balance innovation and security. The opaque nature of blockchain means that no country can cope with this challenge individually. Collective, coordinated action is needed, both technologically, as well as in intelligence and diplomatic terms.

List of Literature

Bendjama, Amar. (20250. Letter dated 9 January 2025 from the President of the Security Council acting in the absence of a Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Securit. United Nations Security Council.

Chainalysis. (2020). THE 2020 STATE OF CRYPTO CRIME. Chainalysis. 2024. TRM Blog. Retrieved from https://www.trmlabs.com/resources/blog/virginia-man-convicted-for-crypto-financing-scheme-to-isis.

FAFT. (2015). „Emerging Terrorist Financing Risks.“ FATF REPORT. October. Retrieved from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf.

Goldbarsht, Doron. (2024). Sprink Nature Link. Retrieved from https://link.springer.com/chapter/10.1007/978-3-031-59547-9_9.

Hayes, Adam. (2024). Blockchain facts: what is it, how it works, and how it can be used. Retrieved from https://www.investopedia.com/terms/b/blockchain.asp.

Hughes, Seamus. (2017). Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks. The George Washington University. 2025. TRM Blog. Retrieved from https://www.trmlabs.com/resources/blog/from-uavs-to-sanctions-evasion-how-the-houthis-use-crypto.

ImmuneBytes. (2023). Pseudonymity and Anonymity: Be Untraceable in the Blockchain World. Retrieved from https://immunebytes.com/blog/pseudonymity-and-anonymity-be-untraceable-in-the-blockchain-world/#:~:text=In%20the%20context%20of%20blockchain,a%20person‘s%20real%2Dworld%20identity.

Kerner, Sean Michael. (2024). Why is cryptocurrency rising and bitcoin at an all-time high? Retrieved from https://www.techtarget.com/whatis/feature/Why-is-cryptocurrency-rising-and-bitcoin-at-an-all-time-high.

Treasury, Department of the. (2024). *2024 National Terrorist Financing Risk Assessment.* Retrieved from https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk Assessment.pdf#:~:text=While%20some%20of%20these%20groups%20relied%20on,charitable%20organizations%20or%20causes%20to%20raise%20funds.

TRM Blog.(2025). March 6. Retrieved from https://www.trmlabs.com/resources/blog/category-deep-dive-use-of-crypto-in-terrorist-financing-expanded-in-2024.

Wyman, Patrick. 2025. How the FBI Tracks and Seizes Illicit Crypto with the Virtual Assets Unit Chief Patrick Wyman. Retrieved from https://www.trmlabs.com/resources/trm-talks/trm-talks-how-the-fbi-tracks-and-seizes-illicit-crypto-with-the-virtual-assets-unit-chief-patrick-wyman.