

ECONOMIC TRANSFORMATIONS AND NATIONAL SECURITY RISKS GENERATED BY CRYPTOCURRENCIES

Cristina Maria BĂTUȘARU

batusaru.cristina@armyacademy.ro

“NICOLAE BĂLCESCU” LAND FORCES ACADEMY, SIBIU, ROMANIA

Ioana Raluca SBÂRCEA

ioana.sbarcea@ulbsibiu.ro

“LUCIAN BLAGA” UNIVERSITY OF SIBIU, ROMANIA

ABSTRACT

The proliferation of cryptocurrencies has brought significant changes in the global economic market while introducing new risks to national security. This paper explores the economic transformations driven by the rise of digital currencies, analyzing their impact on traditional financial systems, monetary policy, and international trade. While cryptocurrencies offer opportunities for innovation and economic growth, they also pose substantial challenges for regulators, particularly in addressing illicit activities such as money laundering, terrorism financing, and tax evasion. Furthermore, the decentralized nature of these digital assets presents unique vulnerabilities for national security, as they can be used to avoid financial controls and sanctions. This paper aims to provide a comprehensive analysis of the economic benefits and security risks associated with cryptocurrencies, emphasizing the need for coordinated regulatory frameworks. By examining the intersection of technological innovation, economic impact, and security concerns, this research contributes to the ongoing debate on how to handle the main challenges brought by the growth of cryptocurrencies in a globalized, digital economy.

KEYWORDS:

Blockchain, cryptocurrencies, economic transformations, national security

1. Introduction

The rise of cryptocurrencies has stimulated significant interest across multiple sectors, driven by their decentralized nature, the technological innovation behind blockchain, and the potential for reshaping traditional financial systems. However, alongside these advancements come critical challenges, especially concerning economic stability and national security. Governments and regulatory groups are trying to figure out how to handle the economic integration of cryptocurrencies while safeguarding against threats such as cybercrime, money laundering, and economic destabilization. The objective of this paper is to examine

the technological, economic, and security implications of cryptocurrency adoption, with a particular focus on how these digital currencies intersect with national security (Stankevicius & Andrulevicius, 2020) concerns by highlighting the need for comprehensive policy frameworks that balance economic benefits with the protection of national interests.

The paper approaches the subject by analyzing cryptocurrencies from a multidisciplinary perspective, exploring both the opportunities they present for economic innovation and the potential vulnerabilities they introduce into the financial and national security infrastructure,

and how the economic transformations driven by cryptocurrencies are associated with risks to national security. It seeks to provide an in-depth analysis of how the adoption and proliferation of cryptocurrencies impact the financial market and present security challenges that require urgent attention.

The importance of this topic is represented by the evolving nature of cryptocurrencies and their far-reaching implications. As governments struggle to keep pace with these developments, understanding the economic and security dimensions of cryptocurrency use becomes critical. The originality of this paper stems from its integrative approach, combining economic analysis with security concerns, offering a new perspective on a subject that demands multidisciplinary attention.

2. Literature review

The growth of cryptocurrencies has led to major changes in the global economy and introduced complex challenges for national security frameworks (Saleh et al., 2020; Limba et al., 2019). These digital assets, underpinned by blockchain technology, promise decentralized financial systems, cross-border transactions, and innovative ways to store and transfer value (Arnone, 2022). While these developments offer economic opportunities and drive technological advancement, they also bring new risks that national governments and security institutions must address. The lack of regulation (Schaupp et al., 2018), the potential for illicit activities, and the anonymity provided by certain cryptocurrencies create vulnerabilities that may be exploited for criminal purposes (Reddy & Minnaar, 2018), including money laundering (Oosthoek & Doerr, 2020), financing terrorism (Dyntu & Dykyj, 2021), and evading sanctions.

Cryptocurrencies have emerged as revolutionary financial technology, reshaping the concept of global finance and commerce. Defined as digital or virtual currencies that use cryptography for security, cryptocurrencies operate on decentralized networks based on blockchain technology.

Economically, cryptocurrencies challenge traditional financial systems by enabling decentralized, peer-to-peer transactions that bypass central banks and government oversight. This decentralization reduces transaction costs and increases financial inclusion, especially in regions with limited access to banking services (Scott, 2016). However, it also disrupts traditional economic controls, such as monetary policy, posing challenges for national economies (Georgiou, 2020) in managing inflation and currency stability. Additionally, the speculative nature of cryptocurrency markets creates volatility, raising concerns about potential economic instability (Alzahrani & Daim, 2019) if mass adoption occurs.

One of the most significant economic impacts of cryptocurrencies is their potential to disrupt traditional financial systems (Titov et al., 2021). By providing a decentralized means of transaction, cryptocurrencies allow individuals to transfer value without the need for intermediaries such as banks or payment processors. This can lead to reduced transaction costs and increased financial inclusion, particularly for those who are unbanked or underbanked. For example, cryptocurrencies enable people in developing countries (El Hajj & Farran, 2024; Button, 2018) to access financial services without relying on traditional banking infrastructure.

Cryptocurrencies have also created new investment opportunities (Lee et al., 2018), attracting millions of investors seeking to capitalize on their price volatility. Bitcoin, the first and most well-known cryptocurrency, has seen dramatic price fluctuations, creating both opportunities for profit and significant risks for investors. The cryptocurrency market is characterized by its speculative nature (Giudici et al., 2020), with prices influenced by market sentiment, regulatory news, and technological advancements. This volatility poses challenges for investors and raises questions about the stability of cryptocurrencies as a reliable store of value.

The rise of cryptocurrencies poses challenges for traditional monetary policy (Claeys et al., 2018; Elsayed & Sousa 2022). Central banks have long used monetary policy tools to influence inflation, interest rates, and economic growth. However, the increasing adoption of cryptocurrencies may limit the effectiveness of these tools. As more individuals and businesses transact in cryptocurrencies, central banks may find it more difficult to control the money supply and manage economic conditions. This could lead to significant changes in how monetary policy is implemented and the overall effectiveness of central banking.

From the technological point of view, cryptocurrencies are built on blockchain technology, which ensures transparency and security through a distributed ledger system. This structure is resilient to tampering, making it attractive for secure transactions but also for illicit activities. The anonymity and cross-border nature of cryptocurrencies have been exploited for illegal purposes, including money laundering (Dupuis & Gleason, 2020), drug trafficking (Bertola, 2020), and cybercrime (Nadareishvili & Kakulia, 2022). This presents a significant security challenge, as tracking and regulating these transactions can be difficult for law enforcement agencies (Sathilkumar & Graham, 2018).

The blockchain technology is a decentralized and distributed ledger that records all transactions across a network of computers. Blockchain technology ensures transparency and security, as transactions are immutable and can be verified by anyone in the network. This technological foundation allows cryptocurrencies to operate without a central authority, making them resistant to censorship and fraud.

While blockchain technology offers enhanced security features, it is not immune to risks. Cybersecurity threats, such as

hacking and phishing attacks (Tsochev et al., 2020), pose significant challenges for cryptocurrency users and exchanges. High-profile hacks have resulted in the loss of millions of dollars in digital assets, raising concerns about the security of cryptocurrency holdings. Additionally, the decentralized nature of cryptocurrencies makes them attractive to malicious actors who may use them for illegal activities, such as money laundering and financing terrorism (Movchan et al., 2023).

Beyond basic transactions, blockchain technology enables the development of smart contracts (Wang et al., 2019; Hamilton, 2020) and decentralized applications (Raval, 2016). Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automate processes and reduce the need for intermediaries, further enhancing efficiency in various sectors, including finance, real estate, and supply chain management. Decentralized applications, on the other hand, leverage blockchain technology to provide services without a central governing body, fostering innovation and new business models (Kazan, et al., 2015; Aini et al., 2023).

These economic and technological aspects intersect with national security, as cryptocurrencies could potentially undermine a nation's regulatory frameworks (Silva et al., 2022) and financial sovereignty. Cybersecurity threats associated with digital wallets and exchanges further exacerbate risks (Houy et al., 2023), requiring robust defense mechanisms to protect national interests.

The main ideas derived from an extensive literature review have been synthesized in Figure no. 1, which presents the economic and technological implications of cryptocurrency use and their implications on national security.

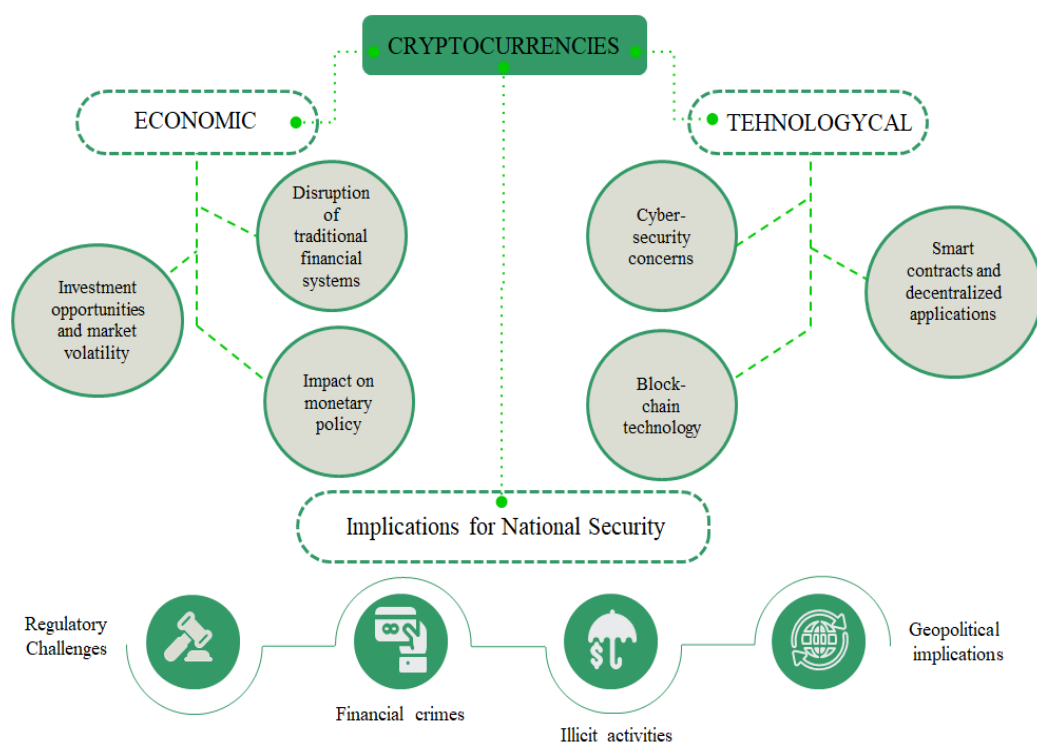


Figure no. 1: *Economic and technological aspects of cryptocurrency use and their implications on national security*
(Source: Author's conceptualization)

The cryptocurrencies use as payment system presents regulatory challenges (Irina, 2018; Chenguel, 2021; Singh & Chawla, 2019) for governments worldwide. Traditional regulatory frameworks often struggle to keep pace with the rapid evolution of cryptocurrency technologies and markets. The lack of regulatory clarity (Corbet, 2020) can create an environment conducive to illicit activities, as people might take advantage of gaps in the system to avoid oversight. Considering these references, it can be stated that empirical research has consistently shown that the lack of clear and consistent regulation has been a significant barrier to the acceptance of cryptocurrencies as legitimate payment systems. This regulatory gap created obstacles to trust and adoption, as the risks associated with fraud, volatility, and money laundering concerns deterred potential users. Recognizing these issues, governments and regulatory bodies worldwide have moved to

introduce comprehensive frameworks that address these concerns, aiming to create a stable and predictable environment for cryptocurrency transactions. In recent years, the adoption of structured regulations like the Markets in Crypto-Assets (MiCA) rules in the EU and similar initiatives elsewhere reflect an acknowledgment of this challenge.

The regulatory framework for cryptocurrency and blockchain is rapidly evolving, with several major legislative frameworks emerging to establish clear guidelines and protections. In the European Union, the Markets in Crypto-Assets (MiCA) regulation, adopted in 2023, aims to create a unified legal framework for digital assets across the EU. MiCA's primary goals are to protect consumers, mitigate market abuse, and establish transparency by requiring licensing for crypto-asset service providers. These measures are widely seen as a way to legitimize and stabilize the crypto industry

in Europe. However, some critics (Zetzsche et al., 2021; Van der Linden & Shirazi, 2023) argue that the compliance costs associated with MiCA may hinder smaller startups, favoring larger players who can more easily absorb regulatory expenses.

In the United States, recent legislative efforts include the Financial Innovation and Technology (FIT) for the 21st Century Act and the Blockchain Regulatory Certainty Act. The FIT Act aims to provide regulatory clarity by distinguishing between digital assets that are considered commodities and those that are deemed securities, assigning regulatory oversight to either the Commodity Futures Trading Commission (CFTC) or the Securities and Exchange Commission (SEC). Some proponents (Karisma & Tehrani, 2022) argue that this could resolve long-standing ambiguity in U.S. crypto regulation and attract innovation by creating a more predictable regulatory environment. However, concerns persist (Ramos, Melon & Ellul, 2022) that this dual framework could lead to inconsistent enforcement and oversight gaps.

Another recent regulation, the Blockchain Regulatory Certainty Act focuses on clarifying tax and regulatory requirements for non-custodial blockchain services, such as miners, validators, and software developers, asserting that they should not be classified as money transmitters. This legislation is intended to protect individuals and entities who facilitate blockchain transactions without handling customers' funds, thus promoting innovation while reducing legal uncertainties.

These frameworks aim to establish a foundation that promotes security and transparency but the challenge remains in balancing innovation with adequate protections for consumers and markets.

Cryptocurrencies are often associated with illicit activities (Panda & Jani, 2019; Leuprecht et al., 2023) due to their pseudonymous nature, which can make it difficult to trace transactions. Criminal organizations have utilized cryptocurrencies

for money laundering, drug trafficking, and financing terrorism (Kapsis, 2023; Teichmann, 2022). This creates major challenges for law enforcement agencies, as traditional methods of tracking financial transactions may not be effective in the context of cryptocurrencies. The rise of decentralized finance platforms (Chen & Bellavitis, 2020; Cumming et al., 2025) further complicates this issue, as they provide services without central oversight, making it harder for regulators to monitor activities.

Cryptocurrencies can also have geopolitical implications (Neașu et al., 2022; Su et al., 2020; Fang, 2024), as they offer countries the ability to bypass traditional financial systems and sanctions. Nations facing economic sanctions may turn to cryptocurrencies as a means of conducting trade and preserving their financial autonomy. This can undermine the effectiveness of international sanctions and create new avenues for illicit financing (Morell et al., 2021). Additionally, state-sponsored actors may leverage cryptocurrencies to fund operations without detection, raising concerns about national security (Bobric, 2021).

The main findings resulted from the literature review underscore the importance of a balanced regulatory approach that mitigates the potential economic disruptions and security threats posed by cryptocurrencies while fostering their positive contributions to financial innovation (Mikhaylov, 2020; Shetty, 2022). Such an approach is essential for nations seeking to leverage the benefits of cryptocurrency technology without compromising their economic stability or national security.

3. Cryptocurrencies in organized crime and illegal activities affecting national security

Corruption using cryptocurrency is a significant issue in the modern economic and administrative context (Choo, 2015), manifesting in various illicit forms. A central

aspect is money laundering, where proceeds from illegal activities are converted into cryptocurrencies, transferred, and then reconverted, making it difficult to trace the original source of the funds. Tax evasion represents another key dimension, with individuals or companies using cryptocurrencies to hide income and evade tax obligations. Additionally, cryptocurrencies can serve as a means of bribery, where public officials accept these digital assets in exchange for favorable decisions, such as granting public contracts or permits. The illegal financing of political campaigns is also facilitated through anonymous cryptocurrency contributions, allowing circumvention of legal limits and regulations (Yadav, 2022; Solowey et al., 2022). Market manipulation is another major concern, as influential individuals use cryptocurrencies to sway financial asset prices to their advantage. These practices undermine trust in public institutions and legitimate economic processes. Two telling examples come from the United States in 2022 and Russia in 2019 (<https://www.trmlabs.com/report#Bribery-and-Corruption>). According to this publication, in 2022, the U.S. Department of Justice accused two Chinese intelligence officers of attempting to bribe a U.S. government employee with 61,000 \$ in bitcoin in order to steal documents related to an investigation into the Chinese tech giant Huawei. In the case of Russia, according to the same source, cryptocurrencies were used to influence voters during election campaigns. In 2019, a candidate for the governor's office in St. Petersburg, Russia, distributed crypto tokens to voters during his campaign.

Cryptocurrencies used in espionage are a major threat to national and international security due to the high level of anonymity and security they offer. These digital assets make it easier to fund secret operations without leaving clear traces, allowing agents to be paid, equipment to be purchased, and other espionage activities to be supported. They are also used to pay informants within targeted organizations or

governments, keeping both parties' identities protected. Using cryptocurrency also makes it easier to obtain sensitive information without raising suspicion through traditional banking systems. Additionally, cryptocurrencies are important for securing communication in espionage operations, as they help keep information private and anonymous. There have been many examples, but three relatively recent cases drew international attention (<https://www.trmlabs.com/report#Espionage>): In November 2022, American nuclear engineer Jonathan Toebbe and his wife Diana were sentenced to 18 and 21 years in prison for trying to pass on secret nuclear propulsion technology to another country. In their exchanges with FBI agents pretending to be foreign officials, the couple asked for payment in the privacy-focused cryptocurrency Monero. Later that year, in December, Iran executed four suspected Israeli spies accused of receiving payments in cryptocurrency. Meanwhile, in South Korea, two citizens were arrested for allegedly accepting cryptocurrency to spy for North Korea.

Cryptocurrencies are also used in ransomware attacks, where attackers encrypt victims' data and demand ransoms paid in cryptocurrency, ensuring difficult-to-trace transactions. They are also used to pay hackers for various illegal services, including unauthorized access to computer systems, data theft, and cyberattacks, protecting the identity of those involved.

One of the most recent reports on crypto crime released in 2024, presents the evolving nature of these activities, examining the interplay between various crime categories and the preferred asset types employed by cybercriminals. By analyzing a comprehensive dataset of illicit transactions it can be seen the trends, patterns, and emerging threats within the cryptocurrency ecosystem. The analysis, according to the report, show the extent to which different cryptocurrencies are utilized for illicit purposes and the preferred methods of laundering proceeds, data being presented in Figure no. 3.

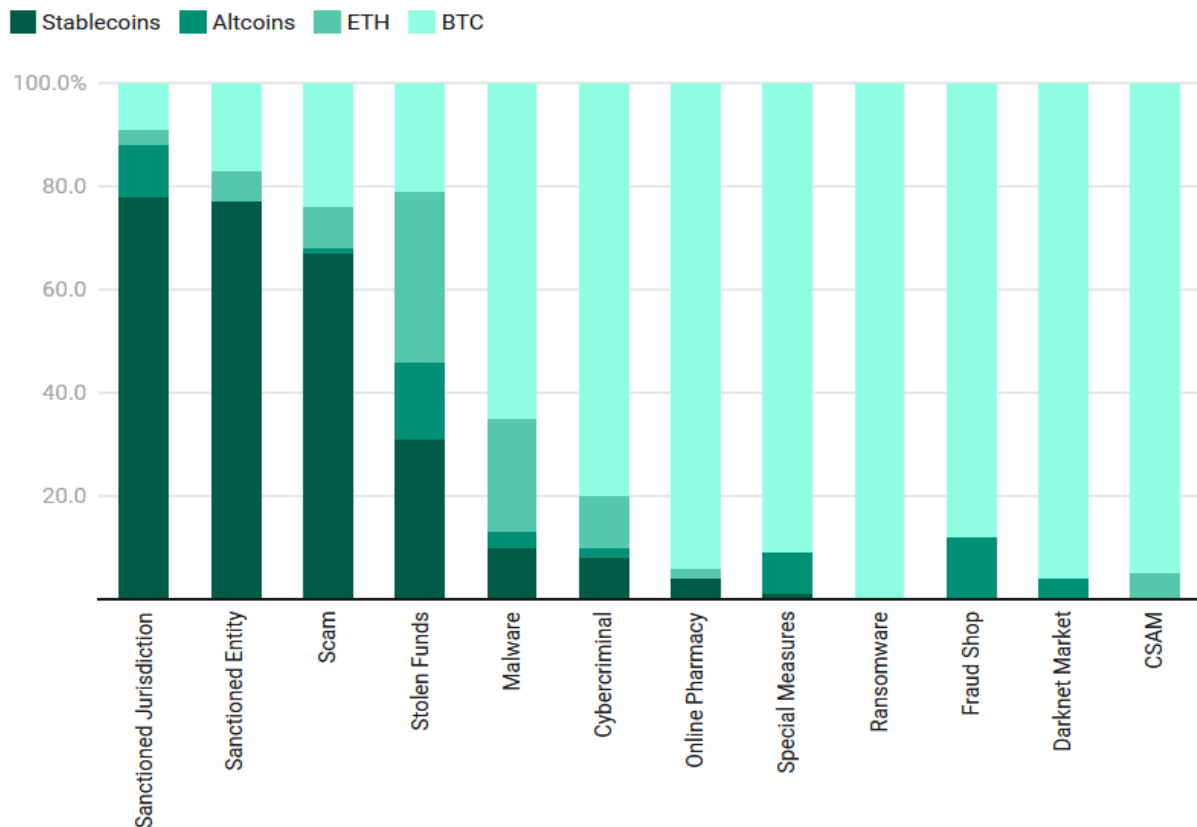


Figure no. 2: *Illicit transaction volume by crime category and asset type 2023*
 (Source: Author's creation in Datawrapper App, based on The 2024 Crypto Crime Report)

The dominance of Bitcoin (BTC) in illicit transactions highlights their appeal for criminals due to their decentralized nature and pseudonymous transactions that offer a degree of anonymity, making it difficult to trace the origin and destination of funds. While Altcoins (any cryptocurrency other than Bitcoin) and ETH (Electronic Funds Transfer) have limited involvement, their presence in certain categories suggests a preference for diversification or potential anonymity benefits. However, it's important to note that the cryptocurrency landscape is dynamic, and these trends may evolve over time.

As presented in the chart, Stablecoins

are also widely used in illicit transactions due to their stability and ease of use. They offer a bridge between traditional finance and the volatile cryptocurrency market, allowing criminals to launder money, evade sanctions, and conduct darknet market activities.

On online black markets, cryptocurrencies facilitate the trade of illicit goods and services such as drugs, weapons, CSAM (child sexual abuse material) and hacking services, due to their anonymous nature. Additionally, online scams, including Ponzi schemes and investment fraud, often rely on cryptocurrencies to attract and deceive victims.

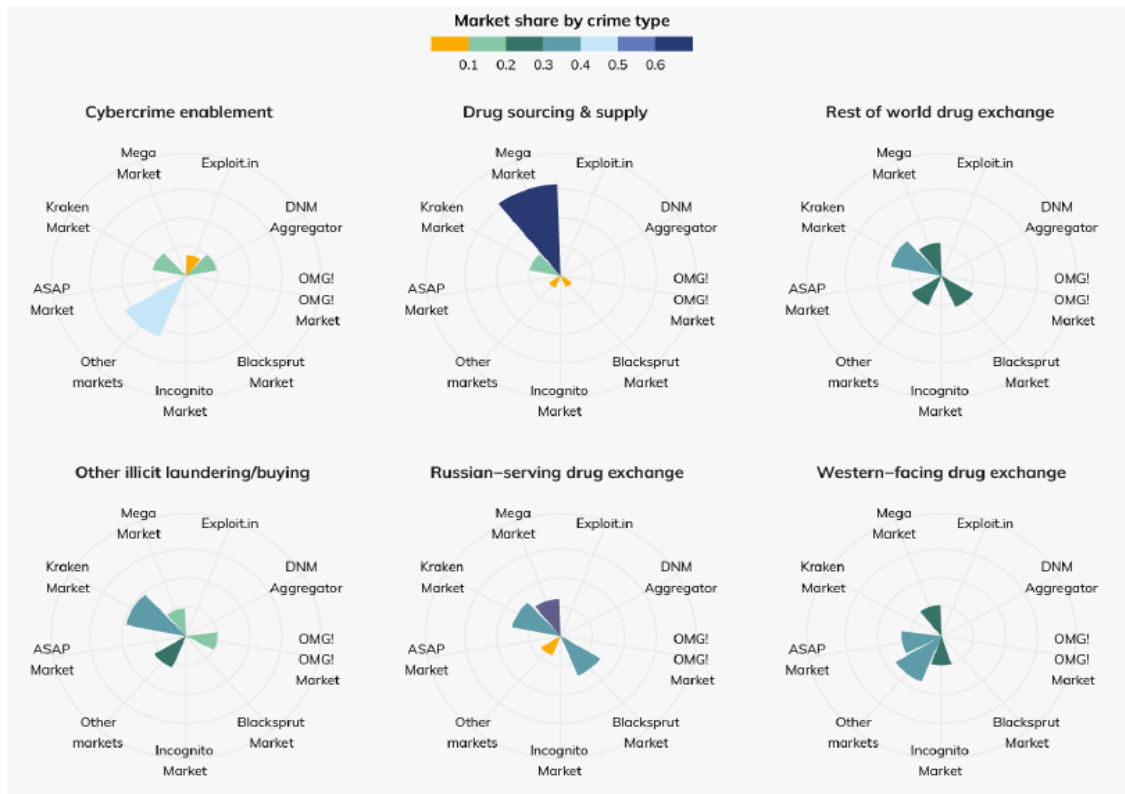


Figure no. 3: *Dominant darknet markets by criminal function in 2023*
(Source: The 2024 Crypto Crime Report, p. 95)

Unlike traditional cryptocurrencies, stablecoins maintain a relatively stable value, making them less risky for illicit purposes. Additionally, their integration with various payment systems and exchanges facilitates seamless transactions, further contributing to their popularity among criminals.

Some types of illegal cryptocurrency activities, like selling things on the darknet or demanding ransom payments, still mostly use Bitcoin. But other types, like scams and transactions linked to countries under sanctions, have switched to stablecoins. These are also the biggest types of crypto crime, which makes them the main driver of this trend.

Groups and individuals from countries under sanctions or involved in terrorism financing are more likely to use stablecoins. This is because they might have trouble getting U.S. dollars the normal way, but they still want the stability that the dollar offers.

These criminal activities are often interconnected and rely on each other to operate effectively within the global underground economy. The use of cryptocurrencies in this context provides a digital and global solution for illegal money transfers, taking advantage of their decentralized, fast, and anonymous nature. Cryptocurrencies have created an ideal infrastructure for conducting and interconnecting these illegal activities. Drug trafficking and contraband generate illicit funds that are then laundered through cryptocurrencies to be used legally or to finance other illegal activities, including terrorism. The anonymity and security offered by blockchain technology complicate the efforts of authorities to detect and prevent these activities. This interconnectedness underscores the need for strict regulations and efficient monitoring mechanisms to combat the use of cryptocurrencies for illegal purposes.

A significant threat for national security is represented by terrorist organizations that have increasingly leveraged cryptocurrencies to finance their activities. The anonymity and ease of cross-border transfers offered by cryptocurrencies make them attractive for raising funds and evading financial regulations. According to the The 2024 Crypto Crime Report (2024), fundraising campaigns for terrorist groups, such as those associated with ISIS, often rely on cryptocurrencies to solicit donations from supporters worldwide. Additionally, these funds can be used to purchase weapons, explosives, and other materials needed for terrorist operations. The decentralized nature of cryptocurrencies and the difficulty in tracking transactions pose significant challenges to law enforcement agencies in combating terrorist financing. Terrorist organizations and their supporters have increasingly turned to cryptocurrencies for financing their activities. The perceived anonymity and ease of cross-border transfers offered by cryptocurrencies have made them an attractive option for raising funds and evading financial regulations. For instance, according to FATF Report (2023) fundraising campaigns for ISIS families in internment camps have relied heavily on cryptocurrency donations. Additionally, pro-ISIS groups in various countries have utilized cryptocurrencies to finance propaganda, recruitment, and other operational expenses. The increasing preference for stablecoins like Tether (USDT) over Bitcoin for terrorist financing highlights the evolving landscape of crypto-based illicit activities.

4. Conclusions

The economic and technological aspects of cryptocurrencies present both opportunities and challenges for individuals, businesses, and governments. As cryptocurrencies disrupt traditional financial systems, they offer new avenues for financial inclusion and innovation. However, their volatility, potential impact on monetary policy, and association with illicit activities raise significant concerns. The underlying blockchain technology provides a secure and transparent foundation, but it also poses cybersecurity risks and regulatory challenges.

The implications of cryptocurrencies on national security are profound, requiring policymakers to develop comprehensive regulatory frameworks that address the dual challenges of fostering innovation while ensuring security and compliance. Without proper oversight, cryptocurrencies can be exploited by malicious actors to destabilize financial systems, undermine national security, and evade sanctions. Therefore, implementing robust regulations to monitor and control cryptocurrency transactions is essential to safeguard national security interests and maintain financial stability. As the cryptocurrency use continues to evolve, ongoing dialogue and collaboration among stakeholders will be essential to navigate the complexities of this new financial frontier. Understanding the economic and technological dimensions of cryptocurrencies is crucial for effectively addressing their implications on national security in an increasingly digital world.

REFERENCES

- Aini, Q., Manongga, D., Rahardja, U., Sembiring, I., & Efendy, R. (2023). Innovation and key benefits of business models in blockchain companies. *Blockchain Frontier Technology, Vol. 2, Issue 2*, 24-35.
- Alzahrani, S., & Daim, T.U. (2019, August). Analysis of the cryptocurrency adoption decision: Literature review. *In 2019 Portland International Conference on Management of Engineering and Technology (PICMET)* (1-11). IEEE.

- Arnone, G. (2022). Blockchain and cryptocurrency innovation for a sustainable financial system. *International Journal of Industrial Management*, Vol. 15, 1-16.
- Bertola, F. (2020). Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime. *American Journal of Qualitative Research*, Vol. 4, Special Issue 2, 27-34.
- Bobric, G.D. (2021). Risks to the National Security Generated by the Widespread Use of Cryptocurrency. *Scientific Bulletin*, Vol. 26, Issue 2, 87-97.
- Button, S. (2018). Cryptocurrency and Blockchains in Emerging Economies. *Software Quality Professional*, Vol. 20, Issue 3.
- Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: market analysis and perspectives. *Journal of Industrial and Business Economics*, Vol. 47, 1-18.
- Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, Vol. 13, e00151.
- Chenguel, M.B. (2021, November). Blockchain and Cryptocurrency: Development Without Regulation? In *International Conference on Business and Technology* (663-679). Cham: Springer International Publishing.
- Choo, K.K.R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In *Handbook of digital currency* (283-307). Academic Press.
- Corbet, S. (2020). Evaluating a decade of cryptocurrency development: navigating financial progress through technological and regulatory ambiguity. *Cryptocurrency and Blockchain Technology*, 185.
- Claeys, G., Demertzis, M., & Efstathiou, K. (2018). *Cryptocurrencies and monetary policy* (No. 2018/10). Bruegel Policy Contribution.
- Cumming, D., Drobetz, W., Momtaz, P.P., & Schermann, N. (2025). Financing decentralized digital platform growth: The role of crypto funds in blockchain-based startups. *Journal of Business Venturing*, Vol. 40, Issue 1, 106450.
- Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, Vol. 28, Issue 1, 60-74.
- Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic journal of economic studies*, Vol. 7, Issue 5, 67-72.
- El Hajj, M., & Farran, I. (2024). The Role of Cryptocurrencies in Emerging Markets: Investigating the Growing Adoption of Cryptocurrencies in Developing Countries, Their Potential to Improve Financial Inclusion and Economic Empowerment. *Business, Economics and Management*. DOI:10.20944/preprints202407.0114.v1 .
- Elsayed, A.H., & Sousa, R.M. (2022). International monetary policy and cryptocurrency markets: dynamic and spillover effects. *The European Journal of Finance*, 1-21.
- Fang, Y., Tang, Q., & Wang, Y. (2024). Geopolitical Risk and Cryptocurrency Market Volatility. *Emerging Markets Finance and Trade*, 1-17.
- FATF Report. (October 2023). Available at <https://www.fatf-gafi.org/en/topics/Terrorist-Financing.html>.
- Georgiou, G.C. (2020). Cryptocurrency challenges sovereign currency. *World Economics*, Vol. 21, Issue 1, 117-141.
- Hamilton, M. (2020). Blockchain distributed ledger technology: An introduction and focus on smart contracts. *Journal of Corporate Accounting & Finance*, Vol. 31, Issue 2, 7-12.
- Houy, S., Schmid, P., & Bartel, A. (2023). Security aspects of cryptocurrency wallets – systematic literature review. *ACM Computing Surveys*, Vol. 56, Issue 1, 1-31.

Irina, C. (2018). Cryptocurrencies legal regulation. *BRICS law journal*, Vol. 5, Issue 2, 128-153.

Karisma, K., & Tehrani, P.M. (2022). Legal and Regulatory Landscape of Blockchain Technology in Various Countries. In *Regulatory Aspects of Artificial Intelligence on Blockchain* (52-81). IGI Global.

Kapsis, I. (2023). Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing. *Organised Crime, Financial Crime, and Criminal Justice*, 122-141.

Kazan, E., Tan, C.W., & Lim, E.T. (2015). Value creation in cryptocurrency networks: Towards a taxonomy of digital business models for bitcoin companies. *PACIS 2015 Conference Proceedings*.

Lee, D.K.C., Guo, L., & Wang, Y. (2018). Cryptocurrency: A new investment opportunity? *Journal of Alternative Investments*, Vol. 20, Issue 3, 16.

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, Vol. 30, Issue 4, 1036-1054.

Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Towards sustainable cryptocurrency: Risk mitigations from a perspective of national security. *Journal of security and sustainability issues*. Vilnius: Generolo Jono Žemaičio Lietuvos Karo akademija, 2019, Vol. 9, No. 2.

Mikhaylov, A. (2020). Cryptocurrency market analysis from the open innovation perspective. *Journal of Open Innovation: Technology, Market, and Complexity*, Vol. 6, Issue 4, 197.

Morell, M., Kirshner, J., & Schoenberger, T. (2021). *An Analysis of Bitcoin's Use in Illicit Finance*. Crypto Council for Innovation.

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social & Legal Studios*, 122.

Nadareishvili, I., & Kakulia, S. (2022). Cryptocurrency-Related Cybercrime Types and Threats. *Law & World*, Vol. 22, 116.

Neacșu, M.C., Andrei, M.I., Zgură, D., & Țăranu, D. (2022). "Cryptocurrencies" Phenomenon and Geopolitical Risks. In *8th BASIQ International Conference on New Trends in Sustainable Business and Consumption* (757-764).

Oosthoek, K., & Doerr, C. (2020). Cyber security threats to Bitcoin exchanges: Adversary exploitation and laundering techniques. *IEEE Transactions on Network and Service Management*, Vol. 18, Issue 2, 1616-1628.

Panda, P.C., & Jani, N. (2019, November). Growth of cryptocurrency and illegal activities. In *5th International Conference on Economic Growth and Sustainable Development: Emerging Trends* (15-16).

Ramos, S., Melon, L., & Ellul, J. (2022, June). Exploring blockchains cyber security techno-regulatory gap. An application to crypto-asset regulation in the EU. In *10th Graduate Conference in Law and Technology, Sciences Po* (2022).

Raval, S. (2016). *Decentralized applications: harnessing Bitcoin's blockchain technology*. "O'Reilly Media, Inc."

Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology*, Vol. 31, Issue 3, 71-92.

Saleh, A.J., Alazzam, F.A.F., Rabbo Aldrou, K.K.A., & Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. *Journal of Security & Sustainability Issues*, Vol. 10, Issue 1.

Sathilkumar, A., & Graham, N. (2018). Cryptocurrency: Law Enforcement Challenges and Opportunities. A Risk Perspective. *Society of Evidence Based Policing, Vol. 3, Issue 1*, 11-13.

Schaupp, L.C., & Festa, M. (2018, May). Cryptocurrency adoption and the road to regulation. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (1-9).

Scott, B. (2016). *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?* (No. 2016-1). UNRISD Working Paper.

Shetty, A. (2022). Regulating Cryptocurrencies: Balancing Innovation and Financial Security. *Jus Corpus LJ, Vol. 3*, 197.

Singh, A., & Chawla, S. (2019). Cryptocurrency regulation: Legal issues and challenges. *International Journal of Reviews and Research in Social Sciences, Vol. 7, Issue 2*, 365-375.

Silva, E.C., & Mira da Silva, M. (2022). Research contributions and challenges in DLT-based cryptocurrency regulation: a systematic mapping study. *Journal of Banking and Financial Technology, Vol. 6, Issue 1*, 63-82.

Solowey, J., & Schulp, J.J. (2022). Practical Legislation to Support Cryptocurrency Innovation. *Cato Briefing Paper*, 140, 2022.

Stankevicius, A., & Andrulevicius, A. (2020). Cryptocurrency and national security: peculiarities of interaction. *Transformations in Business & Economics, Vol. 19, Issue 2*, 50.

Su, C.W., Qin, M., Tao, R., Shao, X.F., Albu, L.L., & Umar, M. (2020). Can Bitcoin hedge the risks of geopolitical events? *Technological Forecasting and Social Change*, 159, 120182.

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

The 2024 Crypto Crime Report, 2025, available at <https://www.chainalysis.com/>.

Titov, V., Uandykova, M., Litvishko, O., Kalmykova, T., Prosekov, S., & Senjyu, T. (2021). Cryptocurrency open innovation payment system: Comparative analysis of existing cryptocurrencies. *Journal of Open Innovation: Technology, Market, and Complexity, Vol. 7, Issue 1*, 102.

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020, October). Cyber security: Threats and challenges. In *2020 International Conference Automatics and Informatics (ICAI)* (1-6). IEEE.

van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial innovation, Vol. 9, Issue 1*, 22.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol. 49, Issue 11*, 2266-2277.

Yadav, S.P., Agrawal, K.K., Bhati, B.S., Al-Turjman, F., & Mostarda, L. (2022). Blockchain-based cryptocurrency regulation: An overview. *Computational Economics, Vol. 59, Issue 4*, 1659-1675.

Zetzsche, D.A., Annunziata, F., Arner, D.W., & Buckley, R.P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal, Vol. 16, Issue 2*, 203-225.