KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 13, No. 2 (2023), p. 50 – 63

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Influence of the Cryptocurrency on the Economic Component of National Security

Vplyv kryptomeny na ekonomickú zložku národnej bezpečnosti

Vitalli HAVVA[1]

[1] *Postgraduate at the Department of Finance named after Victor Fedosov, Kyiv National Economic University named after Vadym Hetman, Ukraine*

The manuscript was received on 25. 09. 2023 and was accepted after revision for publication on 23. 11. 2023

Abstract:

This study is dedicated to researching the impact of cryptocurrency markets on national security, specifically analysing how cryptocurrency's ability to function as conventional money can distort the supply and demand of money, accelerate inflationary processes, and facilitate an increase in illicit transactions (such as drug and weapon trade, and terrorism financing). It is evident that inadequate regulation of professional participants within the cryptocurrency market can result in substantial losses for both the public and businesses, leading to adverse macroeconomic effects. Using the FTX crypto exchange bankruptcy as a case study, this research illustrates the potential for a cryptocurrency-induced crisis to spill over into stock and currency markets. The study relies on statistical data to demonstrate that the national security risks associated with cryptocurrencies are closely linked to the size of the local economy. In response to these findings, this article provides recommendations for national regulators to mitigate the risks posed by cryptocurrencies to national security. Furthermore, it underscores the importance of global regulation of the cryptocurrency market and the revitalization of central bank digital currency (CBDC) issuance. These measures are proposed as effective ways to reduce cryptocurrency risks, particularly for smaller economies.

Keywords: c*ryptocurrency, national security, risks, function of money, fiat money.*

Abstrakt:
Táto štúdia je venovaná výskumu vplyvu trhov s kryptomenami na národnú bezpečnosť, konkrétne analyzuje, ako schopnosť kryptomeny fungovať ako konvenčné peniaze môže narušiť ponuku a dopyt po peniazoch, urýchliť inflačné procesy a uľahčiť nárast nezákonných transakcií (ako sú drogy a obchod so zbraňami a financovanie terorizmu). Je zrejmé, že nedostatočná regulácia profesionálnych účastníkov na trhu s kryptomenami môže viesť k značným stratám pre verejnosť aj podniky, čo vedie k nepriaznivým makroekonomickým účinkom. Tento výskum, ktorý ako prípadovú štúdiu používa bankrot kryptoburzy FTX, ilustruje potenciál krízy vyvolanej kryptomenami preliať sa na akciové a menové trhy. Štúdia sa opiera o štatistické údaje, aby preukázala, že národné bezpečnostné riziká spojené s kryptomenami sú úzko spojené s veľkosťou miestnej ekonomiky. V reakcii na tieto zistenia tento článok poskytuje odporúčania pre národné regulačné orgány na zmiernenie rizík, ktoré predstavujú kryptomeny pre národnú bezpečnosť. Ďalej podčiarkuje dôležitosť globálnej regulácie trhu s kryptomenami a revitalizácie vydávania digitálnych mien centrálnou bankou (CBDC). Tieto opatrenia sú navrhnuté ako účinné spôsoby na zníženie rizík kryptomien, najmä pre menšie ekonomiky.

Kľúčové slová: *kryptomena, národná bezpečnosť, riziká, funkcia peňazí, fiat peniaze.*

Introduction

In January 2009, the genesis block of 50 bitcoins was mined, ushering in a new digital era in the realm of money circulation. Cryptocurrencies possess the inherent potential to substitute traditional currencies issued by central banks. While they offer numerous advantages in terms of transaction speed and convenience, cryptocurrencies also introduce a range of significant risks to national security, particularly on the economic front. Despite the burgeoning popularity of cryptocurrencies relative to fiat currencies, especially in emerging markets, there remains a dearth of research that delves into the threats that fiat currencies can pose to the national security of individual nations. These threats encompass disruptions in the money circulation, facilitation of tax evasion and money laundering, and exposure to substantial operational risks. This list of potential threats, especially for countries with smaller economies, is far from exhaustive.

Methods and material

The study employs various research methodologies, including analysis and synthesis, historical comparisons, and historical analogies. To gather data, the research relies on official statistics sourced from central banks, international organizations, research centres, and academic institutions. Given the novelty of the issues investigated, the lack of prior research on cryptocurrency's impact on national security, and the impossibility of conducting experiments in this domain, additional research methods such as observation, abstraction, and the axiomatic approach are also integrated into the research framework.

Result and Discussion

In December 2022, Rostin Behnam, the chairman of the US Commodity Futures Trading Commission (CFTC), expressed concerns about the potential threat posed by cryptocurrencies to US national security [1]. His remarks came in response to the bankruptcy of the prominent crypto-exchange FTX. Additionally, Mr. Behnam highlighted the recurring issue of cryptocurrencies being utilized in criminal activities. In the same month, two US senators (Sherrod Brown and Jon Tester) advocated for the

necessity of banning cryptocurrencies, with Sherrod Brown emphasizing their perilous nature and the threat they could pose to US national security [2]. Earlier in September 2022, the US Department of Justice established a task force dedicated to combatting criminal activities within the cryptocurrency industry, encompassing not only cryptocurrencies but also various other crypto assets [3]. The pronounced response in the United States to the cryptocurrency issue stemmed largely from the FTX bankruptcy and the revelation of fraudulent activities by market operators who duped unsuspecting individuals into purchasing cryptocurrencies and other digital assets.

Notably, in September 2021, China took the unprecedented step of banning cryptocurrencies altogether. The authorities of the People's Republic of China officially justified their actions by citing concerns about the potential threats posed by cryptocurrencies to national security and the security of citizens' assets. Presently, within the PRC, the exchange, acquisition, and issuance of virtual currencies, as well as activities involving related derivatives and futures, are strictly prohibited. Additionally, foreign companies are barred from offering these services to Chinese citizens [4]. Starting in June 2014, the Financial Action Task Force on Money Laundering (FATF) has been issuing recommendations aimed at regulating the virtual assets market to mitigate the potential risks of money laundering. As per FATF requirements, all jurisdictions were mandated to regulate crypto-asset transactions starting in 2019 [5].

In May 2023, the European Union introduced the Markets in Crypto-Assets Regulation (MiCA), encompassing various provisions, one of which pertains to the tracking of cryptocurrency movements. Starting in 2024, all cryptocurrency transfers within the EU, irrespective of the transaction amount, will be subject to the 'travel rule'. This rule mandates that information concerning the origin of the asset and its recipient be transmitted alongside the transaction and retained by both parties involved [6]. An analysis of this issue yields the following conclusions:

Firstly, although the FATF had urged the resolution of crypto-asset-related issues as early as 2014, substantial regulatory measures concerning national security threats were only effectively implemented in the USA, the EU, and the PRC between 2020 and 2023. In the European Union, such regulatory norms are set to become effective in 2024 and will apply across all 27 EU member states.

Secondly, the discourse surrounding the regulation of crypto-assets impact on national security has transpired over just a few years. Consequently, there is a scarcity of sufficient scientific research and statistical data on this matter. This scarcity necessitates the application of abstraction methods and the axiomatic approach in research efforts.

In the academic literature, there is no broad discussion about the essence of cryptocurrencies' impact on national security. However, there are several studies that can serve as foundational references when delving into this area of scientific debate. For example, Mrs. Shlomit Wagman, Research Fellow at the Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School notes:

'*Cryptocurrencies can be a haven for criminals, terrorists, and sanction evaders. The early, romantic ideology underlying blockchain technology envisioned a decentralized currency without geographical boundaries, governmental supervision, central bank control, or any identification required. Cryptocurrency was meant to be a fast, cheap, and reliable way of transferring value among strangers*' [7]

In 2022, the Pentagon, represented by The Defense Advanced Research Projects Agency (commonly known as DARPA), collaborated with the crypto intelligence firm Inca Digital to initiate the development of tools aimed at providing the Pentagon with a detailed understanding of the inner workings of crypto markets. This initiative, in part, aims to assist authorities in addressing illicit activities involving digital assets [8]. This official engagement in studying the algorithms related to cryptocurrency threats underscores that, even within the US, specialized agencies continue to explore the complexities of this issue, despite having already acknowledged the threat posed to their nation's security.

One particularly noteworthy and comprehensive study exploring the impact of cryptocurrencies on national security, titled 'Cryptocurrency and National Security: Peculiarities of Interaction', was conducted by a team of researchers from Mykolas Romeris University. According to their findings, these scholars identified several national security risks associated with cryptocurrencies, including the potential for fund theft, arbitrage losses, money laundering, tax evasion, and the financing of terrorist activities [9]. A similar list of risks is often identified by researchers studying this issue in the US, EU, and other major markets. However, it's important to note that this classification may not encompass the full spectrum of risks that cryptocurrencies present, particularly in developing markets. Furthermore, the situation is further complicated by the fact that many of these studies are authored by scientists working in the security and defence sectors. They tend to focus on specific concerns such as terrorist financing, money laundering, and arms trade while often overlooking monetary risks such as inflation and issues related to money supply and demand. A comprehensive summary of the outcomes from the ongoing scientific debate on the risks posed by cryptocurrencies to national security can be found in the 'Research and results' section below.

Research results

It is imperative to acknowledge that cryptocurrencies, to varying degrees, currently fulfil the roles of traditional money. The extent to which individual cryptocurrencies can fully carry out these functions is contingent upon the regulatory framework governing them. However, it is worth highlighting that even in countries where cryptocurrencies are prohibited, they may still perform some money-related functions, albeit with limitations. Figure 1 illustrates the interplay between the functions of money and the associated national security risks posed by cryptocurrencies. These risks are examined in greater detail below (Figure 1).

1. The displacement of fiat money by cryptocurrencies in contemporary contexts is a distinct possibility. This risk, unfortunately, remains underexplored within the economic literature, particularly as it pertains to smaller economies. When a seller or producer sets prices for their products or services in cryptocurrency, they effectively operate outside the official circulation of goods.

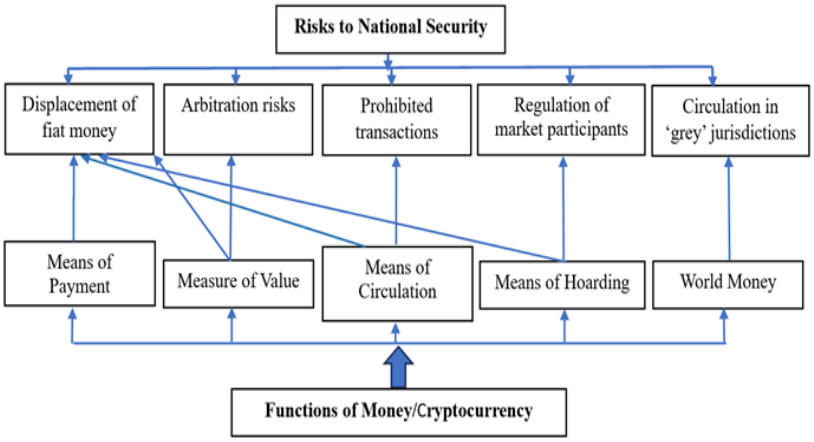

Figure 1: The national security risks of using cryptocurrencies in light of their functions of money
Source: Autor

The primary concern here is that as cryptocurrency payments gain popularity, it can distort the demand for the national currency, effectively placing domestically produced goods and services beyond the scope of monetary aggregates like M0 (physical currency in circulation) and M1 (physical and non-cash national currency in circulation). The displacement of traditional currencies by cryptocurrencies has the potential to trigger inflation and unwarranted interest rate increases by central banks. The impact of cryptocurrency on the demand for a country's central bank-issued national currency can be likened to the introduction of counterfeit money into the national economy. When individuals sell goods or services for cryptocurrency, it implies that the buyer no longer requires conventional currency. Consequently, the quantity of goods and services transacted with traditional currencies decreases, while the overall volume of currency in circulation remains unchanged. Therefore, when conventional money is substituted by cryptocurrencies, inflationary pressures are likely to accelerate automatically. This occurs because fewer goods and services are available in circulation for the same amount of traditional currency.

In practice, the process of transitioning from traditional fiat currencies to cryptocurrencies within money circulation can prove quite intricate. For instance, cryptocurrencies may gradually supplant conventional foreign currencies on a nation's unofficial exchange market, or they may only partially integrate into the broader spectrum of goods circulation, with a neutral impact on GDP money coverage metrics. The impact of cryptocurrency on supply and demand dynamics within commodity markets and the service sector necessitates individualized assessments for each jurisdiction. The development of regulatory algorithms for managing the transition from fiat to cryptocurrency is an ongoing area of study. This challenge is relatively new, spanning only the last 3-5 years, and empirical data specific to local markets is still lacking, making it difficult to establish and validate a standardized regulatory framework. Consequently, regulators find themselves compelled to respond in a somewhat ad-hoc manner, manually implementing restrictions in accordance with the traditions and regulatory practices of each unique local market.

To underscore the magnitude of the challenge posed by cryptocurrencies potentially supplanting traditional fiat currencies, a comparative analysis of the global

cryptocurrency market capitalization in relation to World GDP, EU GDP, and Thailand's GDP was conducted. The aim of this comparison is to provide insight into how extensively the cryptocurrency market could potentially encompass the entirety of the World GDP, the GDP of a major jurisdiction such as the EU, and the average GDP of nations worldwide. In 2022, Thailand's GDP stood as an average representation among the 210 countries across the globe. Intriguingly, in the same year, Thailand also ranked within the Top 20 economies based on the 'Digital currency ownership as a share of the population' indicator, securing the 11th position [10].

In 2021, we witnessed the highest recorded peak in the ratio of cryptocurrency capitalization to global GDP. During that year, the ratio between the total capitalization of cryptocurrencies and world GDP reached 2.43%. Furthermore, this ratio was even more substantial when compared to the GDP of the EU, standing at 10.70%. Most notably, the GDP of Thailand in 2021 was dwarfed by the total capitalization of cryptocurrencies, surpassing it by a significant margin of 4.64 times (Figure 2).

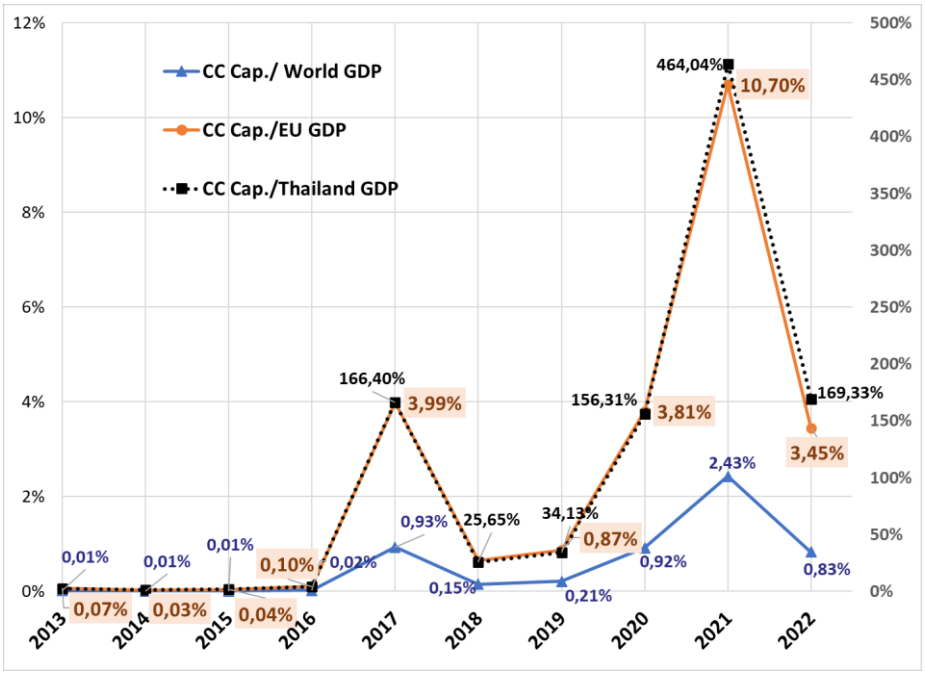

Figure 2: The dynamics of the ratio of the Global Cryptocurrency Market Capitalization to the World GDP, EU GDP, and Thailand GDP, %
Source: Own Processing from [11, 12]

When interpreting Figure 2, it is essential to consider that the crypto-asset market operates on a global scale. Consequently, the extent to which national currencies are displaced by cryptocurrencies hinges on various factors, including local currency market regulations, the level of taxation, capital flow controls, and more. Nevertheless, an analysis of empirical data spanning the years 2013 to 2022 reveals a noteworthy trend: the smaller the scale of the economy, the more vulnerable it is to the

risk of fiat currency displacement. In particular, countries with economies roughly comparable in size to that of Thailand (approximately $500 billion) face heightened vulnerability, stemming from the immediate concentration of the cryptocurrencies' use within the domestic economy's real sector. Such concentration can potentially lead to a cascade of challenges, including uncontrolled inflation, loss of control over exchange rates, and the proliferation of shadow economies or money laundering activities. The displacement of fiat currencies occurs when cryptocurrency implements such functions of conventional money as:

- A means of payment (paying for goods and services);
- A measure of value (establishing the prices in cryptocurrencies);
- A means of circulation (conducting the cryptocurrency transactions);
- A means of hoarding (placing cryptocurrencies in a bank, or buying assets, the price of which is set in cryptocurrencies).

2. Risks associated with the arbitration of the cryptocurrencies that occur when conducting transactions in cryptocurrencies for goods and services, the prices of which are denominated in fiat currencies, or conversely, purchasing goods and services in fiat currencies at prices set in cryptocurrencies. These risks are adaptive and well-known to all market participants who engage in transactions involving foreign currencies. The exchange rates of cryptocurrencies against major reserve currencies like the US dollar, euro, and yuan are subject to rapid fluctuations. It becomes evident when examining the price dynamics of the most popular cryptocurrencies, such as Bitcoin and Ethereum, during the period from 21/09/2022 to 22/09/2023 (Figure 3).

Figure 3. The price dynamics of Bitcoin and Ethereum from 21/09/2022 to 22/09/2023 [13]

An examination of the price dynamics of the world's two most popular cryptocurrencies reveals a notable instability in their exchange rates in relation to the US dollar. The pronounced fluctuations in cryptocurrency exchange rates lead to

challenges in conducting transactions when prices are established in one currency, but transactions occur in another. Additionally, scenarios where buyers need to convert fiat currency into cryptocurrency just before a transaction can be particularly problematic, given the changes in exchange rates within short timeframes. To mitigate these risks in the traditional foreign exchange market for fiat currencies, market participants often turn to various financial instruments such as forwards, futures, options, and other derivatives. As crypto-currency derivative instruments develop, the risks associated with arbitration may decrease. It's important to note that risks associated with arbitration lack a prominent macroeconomic character and may not appear in the national security segment, provided that exchange operations between fiat currencies and cryptocurrencies are effectively regulated. Analysing the practices of cryptocurrency exchanges reveals that risks associated with arbitration can exert a considerable impact on a country in the absence of well-defined regulations for currency exchange. In such circumstances, where operations are artificially impeded, market dealers facilitating exchanges can manipulate rates and profit at the expense of their clients. If such manipulations become widespread, they can trigger a surge in public dissatisfaction and undermine confidence in the nation's financial system and its overall financial stability.

3. Prohibited transactions are among the most significant national security concerns when dealing with cryptocurrencies. Cryptocurrency circulation transcends national boundaries, operating on a global scale. Cryptocurrency owners can acquire it through provided services or purchase it in countries with lax currency regulations, enabling them to engage in transactions that are deemed illegal in the majority of jurisdictions. Such illicit activities include:

- Money laundering of unlawfully acquired funds;
- Trafficking in humans, organs, narcotics, firearms, and other prohibited goods;
- Financing of terrorist activities;
- Sanctions circumvention and evasion;
- Facilitating corruption.

The mentioned risks are undeniably real and substantiated by numerous instances. For instance, in January 2023, Spanish authorities apprehended multiple employees of the russian cryptocurrency service Bitzlato on suspicion of money laundering [14]. In May 2023, the FBI and US police dismantled a cryptocurrency exchange network involved in transactions executed by hackers and individuals who had obtained assets through fraudulent means [15]. Numerous analogous cases exist in various countries, all underscoring the fact that criminals frequently employ cryptocurrencies for illicit activities. Notably, there have been documented instances of russian intelligence services using cryptocurrencies to finance terrorism, including within the territory of Ukraine [16].

Additionally, it's important to emphasize that tax evasion warrants special attention within the category of prohibited transactions. Accepting payments in cryptocurrency, unless it's a Central Bank Digital Currency (CBDC), essentially represents an effort to operate outside the official financial sector. In cases where national cryptocurrency regulations do not mandate taxation upon cryptocurrency sales, it often results in a reduction of taxes, given that tax authorities have no access to cryptocurrency transactions. The risks associated with tax evasion can only be

mitigated if market participants utilize CBDCs, as all other forms of crypto assets provide varying degrees of opportunity to evade taxes.

Statistically interpreting the risks linked to prohibited transactions proves challenging since these risks cannot be easily quantified. Nevertheless, there is a burgeoning body of research dedicated to examining how these risks manifest within the realm of national security (Tab. 1).

Tab. 1. Risks of cryptocurrency to national security [9]

Priorities of National Security	Risks that are brought by cryptocurrencies				
	Money theft	Lack of arbitrage	Money laundering	Tax avoidance	Financing terrorism
Instruments of masked military intelligence		+	+		
Instability in the region	+	+	+	+	+
Terrorism, extremism, radicalism	+	+	+		+
Informational threats		+	+		+
Cybernetic threats	+	+	+	+	+
Economic, energetic dependency	+		+	+	+
Corruption		+	+	+	
Organized crime	+	+	+	+	+

4. Regulating the activities of professional participants in the cryptocurrency market stands as a cornerstone of financial stability, thereby holding direct implications for national security. The challenge arises from the fact that financial institutions are not merely engaged in cryptocurrency exchanges; they also accept cryptocurrencies as deposits and extend loans in cryptocurrencies, treating them on par with conventional currencies. The unique nature of operations of the professional cryptocurrency market's participants gives rise to distinct vulnerabilities concerning national security, specifically:

- Fraud incidents related to cryptocurrency exchange or storage;
- Regulation of cryptocurrency exchanges and crypto asset issuers;
- Regulation of financial intermediaries, such as banks, that both accept cryptocurrency deposits and provide cryptocurrency loans;

The magnitude of cryptocurrency-related fraud on a global scale is so substantial that it can potentially jeopardize the financial stability of entire nations. In 2022, the crypto market lost $1.46 trillion in value [2]. For instance, as of the end of 2022, the collective losses stemming from only the top 10 cryptocurrency fraud cases exceeded a staggering $4.3 billion (Tab. 2).

The most prevalent form of fraud involves hacker attacks targeting professional market participants, including exchanges, banks, and cryptocurrency exchange offices. The lack of technical requirements, compounded by the global distribution of cryptocurrency market infrastructure, makes it exceedingly challenging to establish uniform security measures. It is essential to note that hacker attacks often carry political motives and are exploited by intelligence agencies from rogue states. For instance, a notable hacking incident in March 2022, which resulted in the theft of Ethereum assets worth $625 million, was traced back to North Korea.

Tab. 2. TOP-10 cryptocurrency fraud cases

Platform	Losses, $ million	Cryptocurrency
Ronin Network	625 (March 2022)	Ethereum, USDC (stablecoin)
Poly Network	611 (August 2021)	Tether (stablecoin)
FTX	600 (November 2022)	FTT
Binance	570 (October 2022)	BNB
Coincheck	534 (January 2018)	NEM
Mt. Gox	473 (2011-2014)	BTC
Wormhole	325 (February 2022)	Ethereum
Bitmart	196 (December 2021)	Ethereum
Nomad Bridge	190 (August 2022)	USDC (stablecoin)
Beanstalk	182 (September 2022)	BEAN (stablecoin)

Source: Own Processing from [17]

The challenge of overseeing the security of cryptocurrency exchange offices represents just one facet of the broader issues regulators must address on a global scale. Regulating cryptocurrency exchanges presents a far more substantial concern for national security. The motivations behind the founders of these exchanges may not diverge from those of common fraudsters, and their client (depositor) engagement models may mirror classic financial pyramid schemes (Ponzi scheme). Significant insights can be gleaned from an examination of cases like the FTX exchange's bankruptcy. When FTX faced insolvency, it had $900 million in liquid assets but was burdened with staggering liabilities amounting to $9 billion. Shockingly, it was discovered that the exchange lacked an in-house accounting department, with reports being outsourced to a third-party entity. Moreover, tracing the allocation of the exchange operator's (Alameda Research) funds turned out impossible [18]. FTX had established its official incorporation in the offshore jurisdiction of Antigua and Barbuda, with its headquarters situated in the Bahamas. In a further revelation in March 2023, it was unveiled that the management of FTX had funnelled $3.2 billion into their own accounts through Alameda Research [19].

The case of FTX underscores that the company wasn't just situated in a jurisdiction with favourable tax conditions but also in one with lax reporting regulations. FTX's bankruptcy localisation was possible mainly due to the actions of US authorities, which prevented the crisis from spreading to the traditional stock market, as a significant portion of deposits on FTX belonged to investment funds, notably SoftBank Vision Fund. However, the crisis could not be entirely contained, as the scandal involving FTX resulted in a rapid decline in cryptocurrency values. In just a few days in November 2022, Bitcoin dropped by 25%, Ethereum by 19% (see Figure 3), and Binance Coin by 9%. The case of FTX underscores that private trade organisers and cryptocurrency issuers are ill-prepared for the issuance activities that central banks facilitate in today's world. They often seek jurisdictions with high levels of transactional anonymity and lack transparent record-keeping. Only through the regulation of these pressing issues can the risks associated with the activities of professional market participants be mitigated, ultimately reducing the market's impact on national security. Consequently, without strengthening market circulation regulation, scenarios in which a crisis transitions from the cryptocurrency market to traditional currency and stock markets remain possible.

5. The circulation of cryptocurrencies in 'grey' jurisdictions poses significant risks to national security. Cryptocurrencies, particularly the most popular ones like Bitcoin, Ethereum, and Binance Coin, inherently serve as global forms of currency. Bypassing the traditional banking system, cryptocurrency owners can send them as payment for goods or services to another country. Similarly, sellers can transfer cryptocurrencies to offshore bank accounts and receive fiat currency in return. It is precisely the embedded function of cryptocurrencies as a global currency that makes them a tool for evading currency market restrictions and effectively removes them from the oversight of anti-money laundering authorities. The significant advancements in cryptocurrency regulation achieved in the US and the EU in 2023 do not diminish the heightened risks to national security. Instead, these developments lead to a migration of cryptocurrency operations to jurisdictions with favourable tax climates and formal financial reporting requirements. It is precisely the operations in 'grey' jurisdictions and the parallel use of cryptocurrencies in countries where they are officially prohibited that render the cryptocurrency industry hazardous, especially for smaller economies, including EU countries that do not fall under the purview of the European Central Bank (ECB) and are not part of the Eurozone.

Conclusions and recommendations

1. The displacement of fiat currencies by cryptocurrencies represents a tangible national security risk, with the potential to drive inflation, exacerbate fiscal deficits, and jeopardize financial stability, particularly in economies with a GDP below $500 billion. National regulations pertaining to cryptocurrency circulation and the oversight of professional participants in the cryptocurrency market can only partially mitigate these security risks. To prevent a substantial impact of the cryptocurrency market on the national monetary system, it is imperative that national governments and central banks avoid imposing overly stringent restrictions on foreign exchange markets and refrain from exerting excessive fiscal pressure on the population and businesses. Enforcing an outright ban on cryptocurrency circulation will not curtail transactions in cryptocurrencies among individuals and businesses, as these transactions operate autonomously outside the purview of national banking systems and are not confined to specific jurisdictions.

2. The risks associated with the arbitration of cryptocurrency share inherent similarities with those found in the traditional currency market. However, owing to the unique characteristics of cryptocurrencies, the widespread manifestation of arbitrage risks can transcend the boundaries of a single nation and have adverse consequences on the financial stability of an entire region. To mitigate risks associated with arbitration within local markets, it is advisable to strengthen the regulation of professional participants in the cryptocurrency market, including exchange offices and exchanges. The substantial advancements in cryptocurrency market regulation achieved within the EU should serve as a valuable model for examination and potential expansion beyond the Eurozone. Such regulatory measures should be viewed as a means to safeguard the national economy and the system of money circulation against risks and fraudulent activities associated with arbitration.

3. Efforts to combat prohibited transactions and mitigate their consequences hinge on proactive measures. Activities such as money laundering, human trafficking, drug and weapons trade, terrorism financing, corruption, and other illicit transactions must be subject to thorough criminal investigations, with resulting data compiled into

databases for periodic analysis. Subsequently, this information should be shared with national cryptocurrency market regulators to facilitate appropriate actions against professional participants in the cryptocurrency market who are consistently involved in facilitating prohibited transactions. In addressing tax evasion through cryptocurrency, it is crucial to consider the motivations of market participants. In particular, excessive tax burdens have the potential to significantly diminish the incentives for both citizens and businesses to utilize traditional forms of currency.

4. The circulation of cryptocurrencies in 'grey' jurisdictions significantly undermines the efficacy of regulating transactions within national financial markets. Even commendable regulatory initiatives by the USA, the EU, and Japan are undermined by the fact that a substantial portion of the cryptocurrency market operates within classic offshore zones. Presently, there is no effective system for monitoring cryptocurrency transactions by market participants who combine these transactions with activities through non-public offshore entities with anonymous owners. To address this risk, two approaches can be taken. First, central banks should expedite the development of their own Central Bank Digital Currencies (CBDCs). Currently, progress in this regard is slow, with only a few jurisdictions, such as The Bahamas, Jamaica, and Nigeria, having introduced CBDCs. As the implementation of CBDC gains momentum, loosely regulated cryptocurrencies may gradually be supplanted by central bank currencies, which hold official status. Secondly, on a global level, there is a need for the FATF to establish a universal framework for regulating cryptocurrency circulation, accompanied by the creation of standardized rules applicable to all countries. While this may be a time-consuming endeavour, concurrently pursuing both these approaches can enhance the security of the cryptocurrency market and substantially reduce national security risks.

References

[1] LANG, H., PRENTICE, C. (2022, December 1). U.S. CFTC head urges Congress to act fast on crypto regulation. Reuters. https://www.reuters.com/technology/us-cftc-chair-be-questioned-over-ftx-collapse-by-lawmakers-2022-12-01/

[2] SHILLSALOT, S. (2022, December 19). A ban on cryptocurrencies in the near future? This US Senate Banking Chair thinks. AMBCrypto. https://ambcrypto.com/a-ban-on-cryptocurrencies-in-the-near-future-this-us-senate-banking-chair-thinks/

[3] U.S. Department of Justice. (2022, September 6). The Role of Law Enforcement in Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets. The Report of the Attorney General. Washington. https://www.justice.gov/ag/page/file/1535236/download

[4] HANG, L. (2021, October 13). China: Central Bank Issues New Regulatory Document on Cryptocurrency Trading. Library of Congress. https://www.loc.gov/item/global-legal-monitor/2021-10-13/china-central-bank-issues-new-regulatory-document-on-cryptocurrency-trading/

[5] FATF (2023), Targeted Upate on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, https://www.fatf-gafi.org/content/fatf-

gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html

[6]Regulation of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations. (EU) 2023/1114. (2023). http://data.europa.eu/eli/reg/2023/1114/oj

[7]WAGMAN, S. (2022) Cryptocurrencies and national security: the case of money laundering and terrorism financing. Harvard National Security Journal. Vol. 14:87. https://harvardnsj.org/wp-content/uploads/2022/12/Wagman_14-Harv.-Natl-Sec.-J.-87-2022.pdf

[8] NEWMYER, T. (2022, September 23). Pentagon launches effort to assess crypto's threat to national security. The Washington Post. https://www.washingtonpost.com/business/2022/09/23/darpa-crypto-national-security/

[9] LIMBA, T., DRIAUNYS, K., STANKEVICIUS, A., ANDRULEVICIUS, A. (2020). Cryptocurrency and National Security: Peculiarities of Interaction. Transformations in Business & Economics, Vol. 19, No 2 (50), pp.138-158. https://etalpykla.lituanistika.lt/object/LT-LDB-[10]

[10] J.04~2020~1618838699464/J.04~2020~1618838699464.pdf10. Triple-A (n.d.). Cryptocurrency Ownership Data. Retrieved September 1, 2023 from https://triple-a.io/crypto-ownership-data/#

[11] CoinGecko (n.d.). Global Cryptocurrency Market Cap. Retrieved September 20, 2023 from https://www.coingecko.com/en/global-charts

[12] The World Bank (n.d.). GDP (current US$). Retrieved September 20, 2023 from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=chart

[13] CoinMarketCap (n.d.). Bitcoin Markets. Retrieved September 22, 2023 from https://coinmarketcap.com/currencies/bitcoin/

[14] CAREY, J. S., CARLIN, J. P., GONZALEZ, R. J., KESSLER, D. (2023, September 2). DOJ and FinCEN Take Coordinated Action Against Bitzlato Cryptocurrency Exchange and Its Owner. Compliance & Enforcement. https://wp.nyu.edu/compliance_enforcement/2023/02/09/doj-and-fincen-take-coordinated-action-against-bitzlato-cryptocurrency-exchange-and-its-owner/

[15] PAGANINI, P. (2023, May 2). FBI and Ukrainian police seized 9 crypto exchanges used by cybercriminal. SecurityAffairs. https://securityaffairs.com/145668/cyber-crime/crypto-exchanges-seizure.html

[16] PALYVODA, N. (2023, May 1). An unknown hacker stole $300,000 worth of bitcoin from the Russian FSB and transferred it to Ukraine. MIND. https://mind.ua/en/news/20256773-an-unknown-hacker-stole-300000-worth-of-bitcoin-from-the-russian-fsb-and-transferred-it-to-ukraine

[17] GEORGE, K. (2022, November 17). The Largest Cryptocurrency Hacks So Far. Investopedia. https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/

[18] YELTEKIN, D.S. (2023, March 29). 5 lessons to learn from the collapse of FTX. Simon Business School University of Rochester. https://simon.rochester.edu/blog/5-lessons-learn-collapse-ftx

[19] DAMBEL, E. (2023, March). Alameda Research Funneled $3.2 Billion To Former FTX CEO's Personal Circle. Bitcoinist. https://bitcoinist.com/alameda-research-funneled-3-2-billion-to-ftx/

Autors:

[1]**Vitalii Havva** - Kyiv National Economic University named after Vadym Hetman, Department of Finance named after Victor Fedosov, 54/1 Beresteysky prospect(ProspectPeremogy),03057,Kyiv,Ukraine,email:vitaliihavva2022@gmail.com