

Bitcoin financial crimes and its economic impacts Authors



Kalkil Nouredine

University of Batna 1, Algeria, nouredine.kalkil@univ-batna.dz

Received date: 03/05/2024

Accepted date: 02/06/2024

Publication date: 01/07/2024

Abstract:

Bitcoin (as a cryptocurrency) has numerous advantages that it offers to users, such as low cost, the speed of completing transactions, in addition to enjoying privacy and further characteristics that differentiate this cryptocurrency from further payment ways, whether e-payments or paper money in its conventional forms. However, it has specific issues in dealing with it. This required an economic assessment of these threats, employing the approach of applied analysis. The research concluded that the risks arising from Bitcoin were multifaceted and diverse; affecting both nations and individuals, and their influence could extend to the whole world. Hence, Bitcoin could be a risky cryptocurrency when matched to further conventional currencies. The first of these risks come in exposure to virtual fraud, and the second is that its transactions are irreversible, while the third and fourth are the risks of use in further illegal activities such as money laundering, and the regulatory risks involved in dealing with it, and the last challenge is the great fluctuation in its price. Notwithstanding the posed risks by this cryptocurrency, it caused a major breakthrough in the digital payment technology field, which reinforces the digital transformation trend and boosts e-commerce, along with making further competition between varied payment means. This research dealt with an objective discussion about Bitcoin, its nature and characteristics, and represented the risks and financial crimes related to it, as well as the economic impacts resulting from it.

Keywords: *cryptocurrencies; financial crimes; fraud; money laundering; cybercrime.*

* Corresponding author: Nouredine, nouredine.kalkil@univ-batna.dz

Introduction:

Technological progress and the resulting innovations have led to a radical change in the way organizations manage their business and provide their services, not to mention the consumer behavior towards various services and products, besides the rapid development by these technologies that reflect numerous changes and developments in the information and communication technology sector. The types and size of these technologies and their significant impact on the financial and banking industry, specifically the payment and money transfer sector through advanced payment and settlement systems, and cryptocurrencies were revealed. The global monetary system has witnessed radical developments as well in the former decade. The most obvious of which is related to the emergence of cryptocurrencies, where "Bitcoin" is the most famous and widespread one, despite the global concerns raised by this currency owing to the severe fluctuations in its value, along with the presence of numerous associated risks with it (Kayal & Rohilla, 2021). Nonetheless, it gradually began to gain the confidence of numerous online dealers due to its decentralization and smoothness in its trading, and issuance, in addition to the possibility of benefiting from the financial services associated with it easily and conveniently through the trading platforms spread over the Internet. This prompted specific institutions around the world to accept it as a method of payment. From this standpoint, this research presented an objective and analytical discussion about Bitcoin (as a cryptocurrency), its nature and characteristics, and demonstrated the risks and financial crimes related to it (Holtmeier & Sandner, 2019). In addition to describing the economic impacts resulting from these crimes, which harm the country's economy, and finally, represents necessary recommendations to reduce and control these crimes.

1. Cryptocurrencies:

Since 2008, numerous virtual currencies that are traded electronically through the Internet have appeared as a means of eliminating the role of regulators in terms of issuing, monitoring, and controlling cash, and eliminating the role of financial institutions in financial intermediation to transfer funds. The term cryptocurrency is defined as units or digital values that rely on distributed database technologies for trading and issuance, such as blockchain technology with the help of algorithms and cryptography, which enables them to be traded securely between varied parties deprived of the need for former knowledge between them or an intermediary to accomplish the clearing process. It is traded among individuals quickly, at low costs, and without the need for banks. Cryptocurrencies are one of the aspects of digital currencies that appeared in the financial markets more than a decade ago and have emerged strongly in recent years, and one of the most prominent of these cryptocurrencies is Bitcoin (Kethineni & Cao, 2019). Several articles indicated that cryptocurrencies have acted a remarkable role in the rise of financial crime, resulting in losses of billions of dollars (Faridi, 2019).

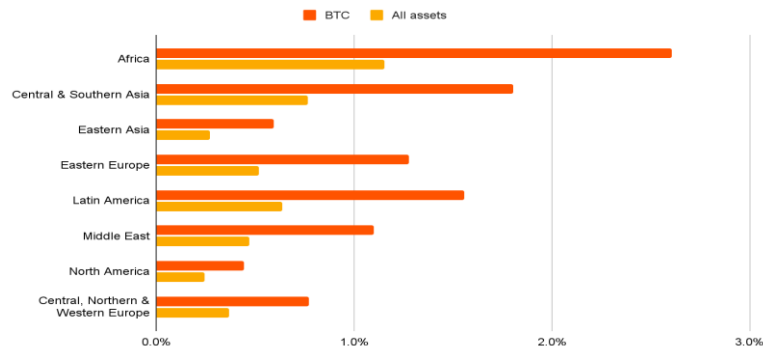


Figure 1 : Peer-to-peer (P2P)share of the whole transaction volume by region from July 2020 to June 2021 (Fries, 2021)

The cryptocurrencies' pseudo-anonymity makes transactions public and relatively anonymous. This technique guarantees anonymity, comprising non-repudiation and integrity of transactions (Litchfield & Herbert, 2018). Their real identities are not easily recognizable by compliant users, nonetheless; as account numbers, they enable only limited identification, either voluntarily or when required. Specific cryptocurrencies strive for complete anonymity, for example, Bitcoin and Monero use protocols so that the user's identity is visible only to the receiver and sender, and Dash attempts to match cryptocurrency units to diverse owners to achieve complete anonymity (Lansky, 2018).

The emergence of digital currencies dated back to published articles in 1982 by David Schum in which, he introduced the idea of completing transactions digitally instead of regular physical payment systems. This eventually led to the establishment of the Pay Pal E-Bank in 1998, where clients' accounts in traditional banks are linked to their electronic accounts to settle their numerous transactions, especially those related to e-commerce. Accordingly, numerous similar institutions and companies were established that sought to complete client transactions using digital currencies until Bitcoin appeared in 2008, which is the first virtual digital currency.

2. BITCOIN:

The "Bitcoin" currency is the first class of the emergence of cryptocurrencies, which appeared as a result of the white paper published by an anonymous programmer named Satoshi Nakamoto in 2008 under the title "A Peer-to-Peer Electronic Cash System". The paper comprised a clarification of the "Bitcoin" currency system as an open source program in which, its presentation and trading are based on "distributed ledger technology" that relies on a network of members to exchange transactions from P2P (peer-to-peer) deprived of the existence of an intermediary for exchange such as banks. The encryption

techniques are used in its trading and issuance (for the safety of transactions conducted through the network). The currency is decentralized, not backed by the government or any further legal entity, and cannot be exchanged for gold or any further commodity (Nakamoto, 2008).

In 2010, the first "Bitcoin" transactions began through users of the (Bitcointalk) forum buying pizza for ten thousand units of this currency at a value of (\$ 0.003) per unit, after which the prices of this currency continued to gradually rise. By January 2011, the value of one "Bitcoin" unit amounted to \$0.30, and the total market capitalization ceiling was guaranteed to exceed one million US dollars. In 2012, the beginning to accept bitcoin as a form of payment at official merchants on websites in which, WordPress was the first website to accept payment in this currency, and other retail companies soon followed, including Microsoft. This is the first step towards widely and internationally accepting "bitcoin" and cryptocurrency as legitimate payment methods (Böhme, et al., 2015). In 2015, the American Coinbase platform (based in the USA) became the first regulated Bitcoin exchange. By October 2017, there were nearly 1,500 ATMs for currency around the world, and the value of Bitcoin rose to (\$ 20,000) in December of the same year.



Figure2: Significant decrease in market capitalization of crypto-assets from a peak in Jan 2018 (ECB, 2019)

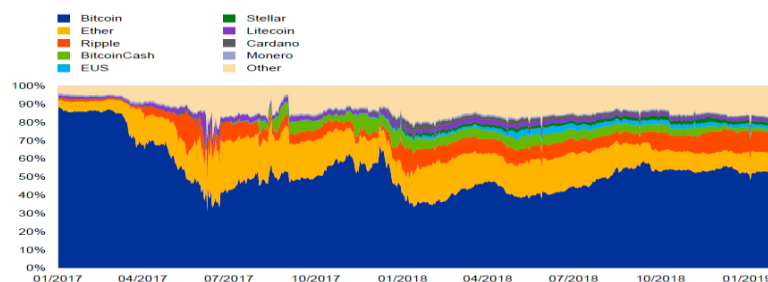


Figure 3: Percentage of the total market capitalization of crypto-assets (Bitcoin market share in crypto-assets is currently at 54%) (ECB, 2019)

2.1. Risks Related to Bitcoin

According to the investigated information and studies, it can be said that scientific research on cryptocurrencies in general and Bitcoin, in particular, is relatively rare. Despite this, some studies shed light, directly or indirectly, on the threats of Bitcoin, as follows:

- Some risks may arise from cryptocurrencies in general and Bitcoin in particular. HSE (2014) study concluded that there are a set of challenges arising from the use of Bitcoin, such as the fluctuation of the currency price, and problems related to security. Moreover, an overview was given on the extent to which these currencies can be used in the practice of various criminal activities, in order to help the security authorities and the judiciary learn more about this technology to implement the law in all countries.
- Moreover, in terms of business ethics, it was found that the use of cryptocurrencies poses great risks to both users and regulators, especially since it is a new technology that does not comply with the old legal framework. (Aljohani, 2017) took a look at what the future might hold for these decentralized currencies. In addition to the possibility of using them in criminal operations such as money laundering, financing terrorist operations, trafficking in illegal goods, and finally, risks related to the organization process.
- Furthermore, there are some legal and regulatory dilemmas, and some economic risks concentrated in destabilizing financial markets and affecting price stability in the market (Nian, et al., 2015)
- In a performed research by (Kaushal, Bagga & Sobti, 2017) to recognize security threats and probable attacks on Bitcoin wallets, the study established that regardless of the advantages that Bitcoin enjoys in terms of encryption and security, not the whole Bitcoin wallets are safe against all types of potential attacks.
- One of the important points to cause negative effects and impacts of Bitcoin is the attacks of hackers, as some characteristics in Bitcoin made it an attraction for fraudsters. It was found that many Bitcoin exchanges were closed, as there are nearly half of the number of those exchanges were closed in the period between (2010-2015), and the main reason for its closure was the successive attacks on it by hackers, which incurred heavy losses (Moore, Christin & Szurdi, 2018).

3. BITCOIN AND FINANCIAL CRIMES

In the former 15 years, after publishing the white paper of bitcoin in Oct 2008, the total number and value of cryptocurrencies have grown exponentially. The developer community has made remarkable technical enhancements in an effort to make currencies (particularly bitcoin) as scalable and secure as potential.

The swift rise of bitcoin and further cryptocurrencies has led to the proliferation of innovative and new forms of financial crimes as well. Financial crime is recognized as any associated crime with finances such as money laundering, tax evasion, theft, fraud, and terrorist financing committed by an organization, a person, or a set of individuals (Houben & Sniers, 2018). This has created a massive crisis for organizations, persons, and financial establishments. Furthermore, these crimes are an ever-changing threat to governments, businesses, and people around the globe. New trends arise every year as criminals look for novel means to exploit the financial scheme's vulnerabilities (Jung & Lee, 2017).

3.1. Money Laundering

Money laundering is identified as a technique used by criminals to conceal the origin of illegally obtained funds, frequently through wire transfers, to authentic banks or companies deprived of regulation or enforcement agencies' interference (Zali & Maulidi, 2018). This manner encompasses the operation of having unlawful money, which has numerous negative effects on the economy, upsurges crimes and corruption, and weakens and affects financial institutions negatively (Arafeen, Arifeen & Ahmed, 2016). In line with Gjoni, Gjoni & Kora (2015), the term "money laundering" dates back to the 20th century, when criminals utilized business-related laundry to launder large quantities of illicit income from controlled entities. Money laundering was described as gaining unlawful money and "laundering" it to make it lawful (Anderson & Anderson, 2015). Moreover, money laundering was characterized as a secondary crime, when it is prearranged by expert criminals and is committed in a specific geographical region, finally influencing the financial and economic stability of the nation (Masjedi, 2015).

The trend of money laundering is increasing every year as it includes numerous methods such as money laundering based on trade, bulk cash smuggling, wire transfers, offshore property buildings, payments through credit cards, cash transactions, and transferring money digitally (Qureshi, 2017). The UN Office on Crime and Drugs predicted that money laundering accounts for 2% to 5% of worldwide GDP, or \$0.8 to \$2 trillion annually. It was stated that money laundering has social costs that reinforce further crimes such as terrorist financing, arms trafficking, smuggling, and drug trafficking (Qureshi, 2017). It is remarkable to realize that money laundering is a continually complicated evolving field. Consequently, governments and financial institutions have enacted a series of rules and regulations to identify money laundering practices, combat, and prevent them if possible.

A case was announced on Feb 27, 2020, in which, CipherTrace stated that New York-headquartered MY Safra Bank (MYSB) has been recognized for its anti-money laundering monitoring and practices of the bank's clients on Jan 30, 2020 (Clegg, 2020). This practice has involved virtual OTCs, Bitcoin ATM operators, cryptocurrency exchanges, and further crypto-associated dealings. The bank was accused of insufficient due diligence on its transactions and clients,

shortage in investigating, and lack of client due diligence. The bank's lack of know-your-customer (KYC) practices and shortcomings in its BSA rules and anti-money laundering prohibited the bank from properly recognizing associated transactions with cryptocurrencies that result in money laundering for clients. While the bank was not penalized for the lack of rules, it was forced to apply the relevant regulations and laws to identify suspicious accounts in the future.

Three months later, the bank's board of directors was to appoint a team of compliance committees to oversee and supervise the compliance program of the bank, monitor training programs to educate the staff below the BSA and coach them to monitor and detect suspicious actions properly. Moreover, they had to create SAR file policies and advance an organization-wide BSA/AML risk evaluation (Clegg, 2020). Six months after this announcement, the Bank was enforced by authorities to have an experienced and qualified BSA Officer and relevant personnel to properly recognize and verify clients who wish to exchange, sell, buy, or manage cryptocurrencies.

3.2. Cybercrime

Cryptocurrencies currently is the most prevalent payment method on the dark web since they enable purchasers and traders to stay anonymous. Hence, with the rising technology utilization in the financial field, cybercrime is a remarkable financial crime trend currently. There are numerous cybercrime categories in which, cybercriminals are exploiting cryptocurrencies (specifically Bitcoin). They comprise Bitcoin exchange hacks, crypto-jacking, DDoS extortion, and ransomware (Carlisle, 2017).

3.2.1. Hacking. Bitcoin is a very attractive goal itself for cybercriminals. Hacking is the activity of illegal programmers who try to hack into digital devices such as PCs, tablets, smartphones, and whole networks. Upon accessing these schemes directly, they can perform administrative tasks. For instance, because of hacking, in 2022 alone, numerous blockchains' "bridges" that provide users with an easier and "safer" way to move assets between these blockchains were hacked and millions of dollars were stolen through locking in these bridges. In 2018, more than \$1 billion was stolen (in the shape of cryptocurrencies) from exchanges and further global platforms. Fraud and attacks that have factually targeted conventional payment schemes, fiat currencies, and banks have currently been reformed to comprise cryptocurrencies (Carlisle, 2017). With the increasing malware numbers and phishing actions targeting enterprises and crypto-investors, attacks on numerous crypto assets such as individual crypto wallets or crypto exchanges are becoming common (routine).

3.2.2. Phishing. it could be defined as the unlawful assortment of private (personal) data, such as online banking passwords and usernames or passphrases of blockchain wallets employing social engineering, chat-support forums, and fraudulent websites. Phishing sites regularly copy reputable and lawful websites' appearance (such as banks) and ask clients to "log in" to these fake

websites. Upon logging on to this fraudulent website, the clients are effectively providing scammers with their bank access data to use it (Cipher Trace, 2021).

3.2.3. Theft identification. From the term, criminals can employ unknown citizen's credentials to compel crimes on their behalf. The data is attained from purchased or phishing scams on the dark web.

3.2.4. Ransomware. It is considered one of the major historical trends in cybersecurity. It is designed to extract money from users through encrypting their data. It is malicious software (a kind of malware) that threatens to spread information, block data access, or PC schemes. This malware usually shows a message on the screen proposing to restore access after paying a ransom by the victim. Cybercriminals usually request payment in a digital currency form (like bitcoin). Hence, tracking down hackers is almost impossible. The busiest ransomware attacks year was 2017, with NotPetya and WannaCry notorious ransomware outbreaks wiping out numerous huge institutions. Furthermore, the bitcoin price rose from under \$1,000 to around \$20,000 in this year, hitting a greatest high of \$19,800 on Dec 2017 (Cipher Trace, 2021).

3.2.5. DDoS extortion. DD4BC (Bitcoin DDoS) was a prominent set doing numerous activities through employing DDoS technology in the form of ransomware, which appeared in 2014 for the first time and was caught in 2016 by Europol. In Oct 2019, the fraud Fancy Bear Group (4) sent ransom requests to financial institutions and banks around the globe that were threatened by DDoS attacks. In specific cases, cybercriminals have executed minor DDoS attacks to test their skills and confirm the threat, without observing major follow-up attacks.

3.3. Fraud

Another key financial crime trend is fraud which comprises crimes such as:

3.3.1. Insider trading. This crime occurs when a person possesses, by virtue of his position, valuable information that is not available to the public and uses that information to buy, sell, or "tip-it-off" financial assets to third parties to exploit that data for their own benefit (Cipher Trace, 2021; Mukherjee, Larkin & Corbet, 2022).

3.3.2. Ponzi systems. It is a presented fraud form as an opportunity for investment. Nonetheless, the investors' funds are not invested anywhere. This system (Ponzi) pays out profits to initial investors with the taken money from newer investors. They frequently promise stable and greater returns to attract further investors to the program (Mukherjee, Larkin & Corbet, 2022)

3.3.3. Pig butchering. Scammers, posing as greatly efficient cryptocurrency traders, entice victims with so-called cryptocurrency investments through offering fake profits and providing fictitious returns to promote further investments. These programs are frequently executed through romance scammers where the scammer spends time to gain the victims' trust to convince them to invest in a fake

platform of Bitcoin offering a "profit". Finally, the scammer takes all funds and disappears after a while.

3.3.4. Crimes linked to cryptocurrency. Upon growing of cryptocurrencies, the frequency of related financial crimes will grow as well, such as fraud cryptocurrency-jacking and unlawful actions like human trafficking, weapons, and drugs (Mukherjee, Larkin & Corbet, 2022).

3.3.5. Financial Terrorism Funding. Terrorism financing has become a major alarm for financial establishments and regimes around the globe as terrorist administrations collect cryptocurrencies or fiat money to execute their operations and launch attacks (Cipher Trace, 2021).

3.3.6. Synthetic identity fraud. Imitation identity is a mix of fabricated and true data. Real data is frequently attained through phishing attacks or bought on the dark web. Fraudsters can make fake identities through utilizing legal SSNs (Social Security Numbers) along with fake PII (Personally Identifiable Data).

3.3.7. Further fraud patterns. These comprise fraud on social media, misleading online marketplaces, compromising Business emails, etc.

In brief, financial crime is an ever-evolving risk impacting governments, businesses, and individuals around the globe. Novel yearly emerging trends as criminals look for novel methods to exploit the financial scheme's vulnerabilities. Through remaining informed with proactive steps, establishments can help lessen the influence of financial crime and make a more secure and safer financial scheme for the whole community (Cipher Trace, 2021).

4. ECONOMIC IMPACTS

Cryptocurrencies threaten the economy of countries, especially industrial ones, for several reasons, the most important of which is the increase in their economic importance so that they become the main mechanism for settling payments, especially international exchanges, and the fear of capital flight from them to encrypted virtual currencies, and the possibility of exposing them to heavy losses. Nonetheless, in light of the fact that these currencies are not official and have no legal framework regulating it, it is likely that a collapse will arise in the economy of specifications and investors regarding the currencies collapse.

The US government estimates that bitcoin-related financial crimes generate hundreds of billions of dollars a year (US Department of the Treasury, 2022). Most of these transactions are related to corruption, organized crimes, cybercrimes, and fraud. These crimes yield most of the illegal money in the US, which enters the financial system and affects the nation's economy (Mugarura, 2016). The US is an attractive destination for illicit capital obtained abroad (US Department of the Treasury, 2022). Financial crimes destructed the economy through distortions in the artificial growth of price, consumption, and impact growth rates negatively (Gjoni, Gjoni & Kora, 2015).

Beqiri and Beqiri (2018) established similar conclusions in which, the financial crimes associated with bitcoin have an adverse impact on government budgets, reducing tax revenues and customer inflows. This reduction in the government budget diminishes the scope for capital and public investments, which ultimately leads to damaging economic growth. Moreover, the authors pointed out that privatizing a country is counterproductive, as money launderers often use privatization to carry out unlawful transactions and discredit the country. In addition, money laundering's negative reputation reduces reasonable international chances while global crimes increase, which affects the development and economic growth of the nation (Sarigul, 2013). These severe consequences directly impact the economy through affecting sincere businesses, as lawful transactions become less attractive to overseas investors, who suspect that all companies are intricate in money laundering (Gjoni, Gjoni & Kora, 2015).

With the increase in generated money by these crimes, this process impacts the nation's economy negatively due to instability and disruptions, resulting in the collapse of financial markets, a decline of the private sector, weakened state control over economic strategies, and lower regime revenues (Masjedi, 2015). Money launderers found novel means for money laundering while emerging monetary centers are left defenseless due to unmanaged regulation (FATF, 2018). Fostering corruption and bribery by these crimes diminishes the state's economy, as it is the main obstacle to lifting individuals out of poverty and suffering through the extortion of public resources (Ahmed, 2019). Therefore, one of the most important economic costs is the damage to the country's reputation and its worldwide significance in terms of progress and development (Arafeen, Arifeen & Ahmed, 2016).

5. Crime Prevention And Control

In view of the increasing importance of the various financial risks of Bitcoin and its control by the regulatory authorities, it is necessary to reduce and control the risks of exchanged transactions using the cryptocurrency (Bitcoin) through several procedures as follows (Dwyer, 2022)

5.1. Monitoring Financial Transactions

The anonymity of cryptocurrencies makes it impossible for financial institutions to identify the real beneficiary of financial transactions that take place in those currencies. Nevertheless, advanced and modern information technology systems can use the systems and algorithms that have been developed to identify patterns and behaviors that indicate suspicion of money laundering and threats. Furthermore, identifying other financial disclosure by giving the necessary alert indicators, as in the case in dealing with financial movements that take place within the channels of the official financial system, then and in the event that an account is identified and linked to a criminal suspicion; the general-recorded movements can be used to build a powerful law enforcement intelligence system (Cipher Trace, 2021; Lachtar, 2020).

5.2. Developing International Standards and Local Legislation

Critics pointed out that anonymity is an impediment to combating Bitcoin-related risks and financial crimes. Nonetheless, cryptocurrencies in their true form - at least in theory - have the components that enable them to identify the customer or suspicious financial movements that reveal fraud and theft. In order to overcome this, a system must be found to identify customers on a large scale when opening electronic wallets. That is, global rules for KYC requirements must be established and agreed upon by all actors in the financial industry, in addition to the development of legislation governing this.

5.3. Regulation of Cryptocurrency Exchanges

The organization of platforms that offer cryptocurrencies in exchange for fiat currencies is subject to regulation, while other platforms that exchange cryptocurrencies with each other are difficult to regulate since they do not accept fiat currencies. Nonetheless, a concerted international effort such as the Financial Action Task Force would be very effective in setting the necessary standards to combat crimes related to cryptocurrency exchanges within their own platforms (Cipher Trace, 2021; Dwyer, 2022).

Conclusion:

By tracking and examining Bitcoin, we find that the design of that currency resulted in the emergence of a set of newly emerging characteristics, such as decentralization, pseudonymity, non-retroactive transactions, and others. These characteristics led to the emergence of many risks, represented in the fluctuation of the price of Bitcoin, exposure to fraud and tax evasion, and the use of it in illegal transactions such as trafficking in drugs, smuggled goods, and money laundering. Moreover, it is used in financing terrorist operations and smuggling money abroad through online transfers, and other threats that affect individuals, institutions, and even countries.

Despite the property of encryption algorithms and confirmation of transactions by miners, Bitcoin has proven to be vulnerable to fraud and theft, which poses some security challenges and raises many criminal concerns. Moreover, it is possible that with the increase in dealing with bitcoins, it will become more attractive to professional hackers, especially since these transactions are never retracted after they are confirmed. The feature of decentralization and the pseudonym – privacy, and secrecy - and the inability to track criminal activities, made this currency a suitable tool for criminals and delinquents of the law, as well as the basic currency used in black market activities, especially via the Internet. This made it widely known in what is known as the trade of Black E-commerce and opened the door wide to illegal activities, such as drug trafficking, financing of killings, money laundering, and others. Furthermore, it was

a major factor in attracting terrorist organizations, especially in the part related to financing their activities.

This undoubtedly poses dilemmas and a huge challenge for governments, as it undermines the ability of countries to impose their control over economic policies, which may negatively affect the economic stability of countries. The idea of not controlling Bitcoin is a frightening idea for governments, which prompted many countries to ban that currency. Nonetheless, banning or imposing restrictions on it to limit its use in illegal activities in general and for any other purpose, may not limit the spread of Bitcoin, especially since the governments of those countries will not be able to fully activate that ban. But it undoubtedly annoys those who deal with it, especially if they want to convert it into an official currency - such as the dollar.

Bibliography:

- Ahmad, S. (2019). Corruption and money laundering. *International Journal of Government Auditing*, 29–30. Available at: http://intosaijournal.org/site/wp-content/uploads/2019/04/INTOSAI-Journal-Spring-2019_Corruption-and-ML-Nexus_SAI-Pakistan.pdf
- Aljohani, A. (2017). Bitcoin: Technology, Economics and Business Ethics. University of Ottawa, Ontario, Canada. Available at: <https://bitly.cx/3sHO>
- Anderson, M. & Anderson, T. (2015). Anti-money laundering: history and current developments. *Journal of International Banking Law and Regulation*, 30(10), 521–531.
- Arafeen, Q., Arifeen, N. & Ahmed, M. (2016). Money laundering in Pakistan-its effects and negative outcomes. *International Journal of Advance Engineering and Research Development*, 3(4), 109–111.
- Beqiri, V. & Beqiri, N. (2018). Negative effects on the domestic economy caused by money laundering. *International Journal of Knowledge*, 27, 87–92.
- Böhme, R. et al. (2015). Bitcoin Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213–238
- Carlisle, D. (2017). Virtual Currencies and Financial Crime Challenges and Opportunities. Royal United Services Institute (RUSI). Available at: <https://bitly.cx/BDIS>
- Cipher Trace. (2021). Cryptocurrency Crime and Anti-Money Laundering Report. Available at: <https://bitly.cx/8L7dO>
- Clegg, P. (2020, Feb 27). OCC hits New York based bank with first-ever enforcement action. CipherTrace. Available at: <https://bitly.cx/PTv11>

- Dwyer, GP. (2022). "Regulation of cryptocurrencies". In Corbet, Shaen (ed.). Understanding Cryptocurrency Fraud. The challenges and headwinds to regulate digital currencies. Boston/Berlin: De Gruyter. pp. 201-204
- ECB. (2019, June). Crypto-assets – trends and implications. European Central Bank, Eurosystem. Available at: <https://bitly.cx/EZOZR>
- Faridi, O. (2019, Aug 13). \$4.3 billion lost due to cryptocurrency crimes: Cipher trace report. Ethereum World News. Available at: <https://bitly.cx/8vF>
- FATF. (2018). Annual Report 2017-2018 [Report]. Financial Action Task Force. Available at: <https://rb.gy/yh0kef>
- Fries, T. (2021, Sept). Africa's crypto market has grown by \$105.6 billion in the last year World. World Economic Forum. Available at: <https://ln.run/WVGuK>
- Gjoni, M., Gjoni, A. & Kora, H. (2015). Money laundering effects [Paper]. International Conference on Management, Business and Economics, Durres, Albania. Available at: <https://ln.run/tQqds>
- Holtmeier, M. & Sandner, P. (2019). The Impact of Crypto Currencies on Developing Countries. Frankfurt School Blockchain Center. Available at: <https://shorturl.at/UHghJ>
- Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament's Special Committee. Available at: <https://rb.gy/7lnr5s>
- HSE. (2014). Risks and Threats of Virtual Currencies. Leesburg Pike: Homeland Security Enterprise. Available at: <https://rb.gy/vrr46c>
- Jung, J. & Lee, J. (2017). Contemporary financial crime. Journal of Public Administration and Governance, 7(2), 88–97.
- Kayal, P. & Rohilla, P. (2021). Bitcoin in the economics and finance literature: a survey. SN Business & Economics, 1(88), 1 – 21
- Kaushal, P., Bagga, A. & Sobti, R. (2017). Evolution of bitcoin and security risk in bitcoin wallets. International Conference on Computer, Communications and Electronics (Comptelix). pp. 172-177
- Kethineni, S. & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 1–20.
- Lachtar, N., et al. (2020). A Cross-Stack Approach towards Defending Against Cryptojacking. IEEE Computer Architecture Letters, 19(2), 126–129.
- Lansky, J. (2018). Possible state approaches to cryptocurrencies. Journal of Systems Integration, 9(1), 19–31.

- Litchfield, A., & Herbert, J. (2018). Resolv: Applying cryptocurrency blockchain methods to enable global cross-platform software license validation. *Cryptography*, 2(2), 1–24.
- Masjedi, E. (2015). Electronic money laundering and data mining methods in investigating money laundering prevention. *International Academic Journal of Science and Engineering*, 2(10), 29–46.
- Moore, T., Christin, N. & Szurdi, J. (2018). Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology*, 18(4), 1-16
- Mugarura, N. (2016). Uncoupling the relationship between corruption and money laundering crimes. *Journal of Financial Regulation and Compliance*, 24(1), 74–89.
- Mukherjee, S., Larkin, C. & Corbet, S. (2022). Cryptocurrency Ponzi schemes. In Corbet, Shaen (ed.). *Understanding Cryptocurrency Fraud. The challenges and headwinds to regulate digital currencies*. Boston/Berlin: De Gruyter. p.118.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at: <https://rb.gy/eq07bp>
- Qureshi, W. (2017). An overview of money laundering in Pakistan and worldwide: causes, methods, and socioeconomic effects. *University of Bologna Law Review*, 2(2), 300–345.
- Sarigul, H. (2013). Money laundering and abuse of the financial system. *International Journal of Business and Management Studies*, 2(1), 287–301.
- US Department of the Treasury. (2022). National Money Laundering Risk Assessment. Available at: <https://rb.gy/ddk4dz>
- Zali, M. & Maulidi, A. (2018). Fighting against money laundering. *BRICS Law Journal*, 5(3), 40–63.