Novi Ekonomist
Vol 18(2), Year XVIII, Issue 36, july – december 2024.
ISSN 1840-2313 (Print) 2566-333X (Online)
DOI: 10.69781/NOEK202436035

Submitted: 23.10.2024.
Accepted: 21.11.2024.
Scientific Article
UDK: 343.9.024:336.741.1

MONEY LAUNDERING USING CRYPTOCURRENCIES

Marijana Joksimović
Alfa BK University, Faculty of Finance, Banking and Audit, Belgrade, Serbia
joksimovicmarijana80@gmail.com
ORCID: 0000-0002-5939-5137

Marija Paunović
University of Kragujevac, Faculty of Hotel Management and Tourism, Serbia University „MB", Faculty of Business and Law, Belgrade, Serbia
majap@rcub.bg.ac.rs
ORCID: 0000-0001-5216-0039

Stevica Dedjanski
Faculty of Social Sciences, University of Business Academy in Novi Sad, Belgrade, Serbia
stevica.dedjanski@fdn.edu
ORCID: 0000-0002-5144-3675

This paper is part of the results of research on project U 01/2023 Green economy in the era of digitization, Faculty of Finance, Banking and Auditing, Alfa BK University. This research is supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia by the Decision on the transfer of funds to finance the scientific research work of teaching staff at faculties in 2024, No. 451-03-65/2024-03 of 26 January 2024.

Abstract: *This paper examines the growing issue of money laundering through cryptocurrencies on a global scale. Criminals use digital assets to launder illicitly obtained funds, converting them into cryptocurrencies to obscure the origins of the money. Unlike traditional financial systems, decentralized finance (DeFi) platforms lack mechanisms to freeze or block funds from suspicious sources, presenting a unique challenge for law enforcement. However, the blockchain underlying cryptocurrencies allows for the tracking of transactions across DeFi protocols, making it possible to trace asset movement, albeit with difficulty due to complex methods criminals use to mix and transfer funds across multiple wallets. The study employs official data from financial institutions between 2019 and 2023, using time-series analysis to forecast money laundering trends under both optimistic and pessimistic scenarios. The paper concludes by highlighting the ongoing efforts by regulatory bodies to strengthen measures aimed at preventing cryptocurrency-related money laundering.*

In order to draw adequate conclusions, the data used in the paper are official data from financial institutions relevant to money laundering. The time series used in the paper includes data related to the period from 2016 to 2023 and the forecast model based on optimistic and pessimistic scenarios is constructed.

Key words: *Money laundering (ML), Blockchain technology, Cryptocurrency, Anti-money laundering and Fraud.*

JEL classification*: C02, F00, F30, F31, G18, G23, G28, O32, O38*

1. INTRODUCTION

The previous year, 2023, was the year of recovery of cryptocurrency, i.e. the system of Decentralized Finance (DeFi). In December alone, 721 DeFi projects with around 4M wallet addresses were recorded. Fraud in the DeFi system continues to raise concerns, both in terms of money laundering and other types of fraud in the system. Thus, over $500 million was stolen from various protocols in the first quarter of this year, according to the research paper CryptoCrime Reports. (Chainalysis, 2024)

Money laundering using cryptocurrency involves converting illegally obtained funds into digital assets to conceal their illicit origins. Unlike centralized systems, where there is an option to freeze funds coming from suspicious or illegal sources, the DeFi system generally does not have this option. On the other hand, blockchain can track assets moving through DeFi protocols to their next destination, unlike centralized systems. However, criminals often use complex methods to mix and transfer funds across various wallets to obfuscate the transaction trail. This makes it challenging for law enforcement agencies to track and investigate these activities. As a result, regulatory bodies are continuously working to implement stricter measures to prevent money laundering through cryptocurrencies.

2. METHODOLOGY AND LITERATURE

In academic literature, there is a lack of papers dealing with money laundering specific to DeFi. Time series analysis can use time series of cryptocurrency transaction data to identify anomalies and patterns that indicate money laundering. As a starting point for addressing this question, and in order to draw adequate conclusions, the data used in the paper are official data from financial institutions relevant to money laundering. The time series used in the paper include data related to the period from 2016 to 2023. To perform an AML check on cryptocurrencies, autors use compliance tools provided by blockchain analytics like Chainalysis, Elliptic, or CipherTrace.

There are several methods of laundering cryptocurrency money. The first method of laundering cryptocurrency money involves the use of so-called money mules or smurfs who help cryptocurrency money launderers to make a certain income.

A money mule is usually a person who transfers cryptocurrency funds on behalf of the money launderer in order to make a certain income. Money launderers usually use numerous money mules and also break up and divide large funds so that they are not easily detected. Cryptocurrency money launderers apply the same principle and also use money mules.

To prevent money laundering in cryptocurrency, regulatory authorities and platforms can implement various measures:

1. Know Your Customer (KYC) verification: Require users to provide identification documents for verification before using the platform.
2. Anti-Money Laundering (AML) policies: Implement robust AML policies to monitor transactions and report suspicious activities to relevant authorities.
3. Transaction monitoring: Use advanced technology to track and analyze transactions for any unusual patterns that may indicate money laundering.
4. Compliance frameworks: Follow regulatory guidelines and standards to ensure legal compliance and prevent illicit activities.
5. Educate users: Raise awareness about the risks of money laundering in cryptocurrency and encourage users to report any suspicious activities.

By implementing these measures, cryptocurrency platforms can help combat money laundering and protect the integrity of the financial system. (Joksimović, M., Peković, D., & Stamenovic, M., 2024). Blockchain technology (Bjelobaba et al, 2022; Paunović, M., Joksimovic, M. & Doganjić, J., 2023), can be leveraged for anti-money laundering (AML) efforts in several ways:

1. Transparency and immutability: Blockchain's transparent and immutable nature allows for the tracking of transactions, making it easier to identify suspicious activities.
2. Smart contracts: Smart contracts can be used to automate AML processes such as transaction monitoring and compliance checks.
3. Identity verification: Blockchain can facilitate secure and decentralized identity verification, making it harder for criminals to engage in money laundering activities.
4. Data sharing: Blockchain networks can enable secure data sharing among financial institutions and authorities, improving collaboration in detecting and preventing money laundering.
5. Tokenization: Tokenization of assets on the blockchain can streamline AML compliance by providing a clear record of ownership and transaction history.

By utilizing blockchain technology in AML efforts, financial institutions and regulatory authorities can enhance the effectiveness of their anti-money laundering measures and improve the overall integrity of the financial system. To perform an AML check on cryptocurrencies, authors use compliance tools provided by blockchain analytics like Chainalysis, Elliptic, or CipherTrace. These tools can help analyze transactions to detect potential money laundering activities and ensure compliance with Anti-Money Laundering (AML) regulations.

3. RESEARCH RESULTS

Reports from organizations such as the Financial Action Task Force (FATF), the United Nations Office on Drugs and Crime (UNODC) and Federal Bureau of Investigation, (FBI'S), Internet Crime Complaint Center the authors give in the paper. These reports often provide insights into cryptocurrency-related crime and anti-money laundering efforts. Additionally, resources from blockchain analytics like Chainalysis or CipherTrace can offer detailed analyses of cryptocurrency crime trends and AML practices in the industry.

One of the biggest cryptocurrency-related money laundering cases in the world is the Mt. Gox scandal. Mt. Gox was a major Bitcoin exchange based in Japan that filed for bankruptcy in 2014 after losing approximately 850,000 Bitcoins, worth over $450 million at the time, due to hacking and mismanagement.

The incident resulted in allegations of money laundering, fraud, and the loss of funds for many investors.

The in the world is the OneCoin scam. OneCoin was promoted as a legitimate cryptocurrency by its founders but was later exposed as a Ponzi scheme. The scam reportedly defrauded investors of billions of dollars worldwide through false promises and deceptive marketing tactics (Chainalysis, 2023). Several individuals associated with OneCoin have been arrested and face legal action for their involvement in the fraud. On the Table 1 authors show total cryptocurrency laundering by year 2016 to 2023, by billions $.

Table 1. Total cryptocurrency laundering by year 2016 to 2023, by billions $

Year	Bilion $
2016	1.5
2017	4.9
2018	3.3
2019	11,8
2020	8,5
2021	14,2
2022	23,8
2023	22.2

Source Authors from available data

A look at Table 1 shows a decrease in CML in 2023 compared to 2022. Part of this decline can be attributed to an overall decrease in the volume of crypto transactions, both legitimate and illegitimate.

On the Table 2 authors show Total value leaving illiciti wallets and arriving at conversion services including off-ramps by year 2019 to 2023, by billions $

Table 2. Total value leaving illiciti wallets and arriving at conversion services including off-ramps by year 2019 to 2023, by billions $

Year	Bilion $
2019	10.1
2020	9
2021	18
2022	30
2023	24

Source: *Money Laundering and Cryptocurrency Report*, Annual Crypto Crime Reports, 2023.

Table 3. Crime types with cryptocurrency Nexus SAD in 2023

Crime Type	Currency
Investment	32. 094
Tech Support	8.719
Personal Data Breach	8.716
Extortion	8.630
Confidence/Romance	3.749
Government Impersonation	2.266
Non-payment/Non-Delivery	810
Phishing/Spoofing	667
Advanced Fee	649
Data Breach	592
Employment	581
Other	369
SIM Swap	300
Lottery/Sweepstakes/Inheritance	137
Identity Theft	133
Credit Card/Check Fraud	119
Ransomware	108
Overpayment	90
BEC	70
Real Estate	60
Harassment/Stalking	39
Malware	27
Botnet	13
Crimes Against Children	11
Threats of Violence	6
IPR/Copyright and Counterfeit	4

Descriptors These descriptors relate to the currency used in the crime and the IC3 uses them for tracking purposes only. They are available only after another crime type has been selected	
Cryptocurrency	43.653
Cryptocurrency Wallet	**25.815**
LOSSES Regarding Ransomware adjusted losses: this number does not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victims directly reporting to FBI field offices/agents	
Cryptocurrency	**3.809.090.856**
Cryptocurrency Wallet	**1.778.399.729**

Source: FBI'S, Federal Bureau of Investigation, *Cryptocurrency Crime Report 2023.* Internet Crime Complaint Center

During 2023, IC3, Internet Crime Complaint Center, received complaints regarding cryptocurrency trading from over 200 countries that had trading abuses. We see on Table no 4. Top 5 countries by complaint Count in 2023 in $, and Table no 5. Top 5 countries by complaint Losses in 2023 in $.

Table 4. Top 5 countries by complaint Count in 2023 in $

Country	**Complaints**
United States of America	57.762
Canada	1.236
United Kingdom	962
Nigeria	841
India	840

Source: FBI'S, Federal Bureau of Investigation, *Cryptocurrency Crime Report 2023.* Internet Crime Complaint Center

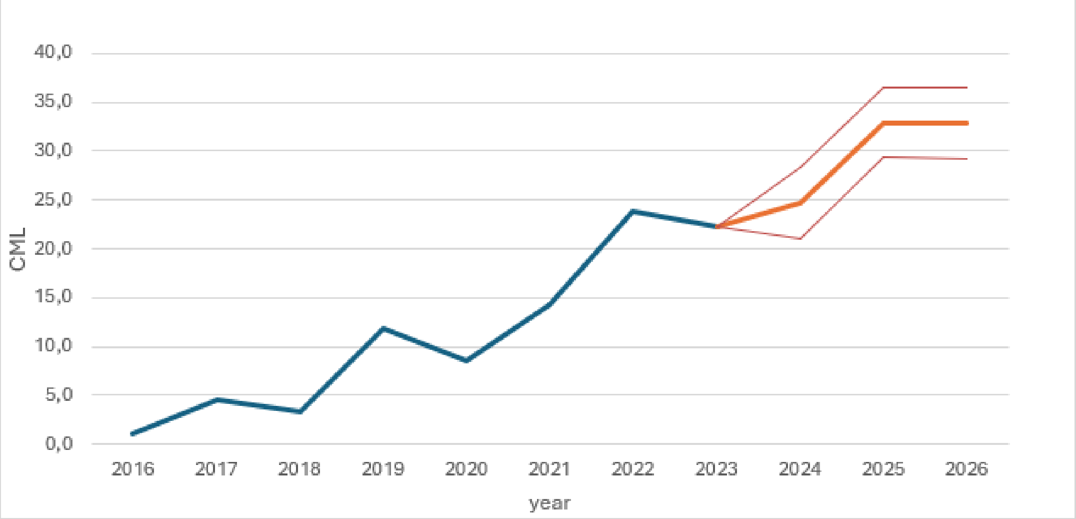
Table no 5. Top 5 countries by complaint Losses in 2023 in $

Country	**LOSSES**
United States of America	4.809.737.956
Cayman Islands	195.663.025
Mexico	126.994.051
Canada	72.080.498
United Kingdom	59.367.008

Source: *FBI'S, Federal Bureau of Investigation,* Cryptocurrency Crime Report 2023. *Internet Crime Complaint Center*

In the next Graph is shown the forecast of time series for the next 3 years.

Graph 1. Forecast analysis of MLC



Sours: Authors calculation

The chart shows the forecast for CML based on data collected from 2016 to 2023. In this period, there is a steady increase in CML, which means that transactions related to money laundering have grown significantly in this period. The graph shows predictions under two scenarios: optimistic and pessimistic. The optimistic scenario (lower line) forecasts that CML could increase to approximately 29.3 billion USD by the end of 2026. The pessimistic scenario (upper line) suggests CML could reach 36.6 billion USD in the same period. Both projections are based on a 95% confidence interval, meaning there is a 95% chance that the actual values will fall within these ranges.

The projections indicate a significant rise in the value of money laundering activities by 2026, depending on the scenario. In both cases, the expected growth is considerable, signaling increased activity related to money laundering in the coming years.

In the following text on Table 6, a description of the biggest money laundering scams is given, classified by continent.

Table 6. The biggest money laundering cryptocurrency fraud in the world, classified by continent

Continent	**The biggest money laundering cryptocurrency fraud**
Europe	One of the biggest money laundering cryptocurrency frauds in Europe is the case of BitClub Network. BitClub Network was a Ponzi scheme that operated from 2014 to 2019, defrauding investors of hundreds of millions of dollars. The founders of BitClub Network were charged with running a fraudulent investment scheme that involved false promises of high returns on investments in bitcoin mining operations. The case highlighted the importance of conducting due diligence and being cautious when investing in cryptocurrency-related opportunities.
Asia	One of the notable cases of cryptocurrency-related fraud in Asia is the $850 million Bitfinex scandal involving the loss of funds from one of the largest cryptocurrency exchanges. In this case, it was alleged that Bitfinex used Tether, a stablecoin pegged to the US dollar, to cover up losses. The scandal raised concerns about money laundering and market manipulation in the cryptocurrency industry.
America	One of the biggest money laundering and cryptocurrency fraud cases in America involved the Bitfinex and Tether scandal. In this case, it was alleged that Tether, a stablecoin issuer, and Bitfinex, a major cryptocurrency exchange, engaged in fraudulent activities to cover up losses and manipulate the price of Bitcoin. The New York Attorney General's office accused them of hiding around $850 million in losses. This case highlighted concerns about transparency and regulatory compliance in the cryptocurrency industry.
Australia	One notable case in Australia involving money laundering and cryptocurrency fraud is the one related to the Australian dark web drug trafficking operation known as "Silk Road." This case involved illegal activities conducted on the dark web, including the sale of drugs and money laundering using cryptocurrencies. The Australian authorities have been actively working to combat such criminal activities and increase regulations to prevent money laundering and fraud in the cryptocurrency space.
Africa	One of the biggest cryptocurrency-related money laundering cases in Africa involved Mirror Trading International (MTI), a South African company that was accused of operating a Ponzi scheme that defrauded investors of hundreds of millions of dollars. MTI attracted investors with promises of high returns through automated cryptocurrency trading but was later revealed to be a fraudulent

	operation. South African authorities have been investigating the case and taking action against those involved in the scheme.
Antarctic	There haven't been any reported cases of significant money laundering cryptocurrency fraud in Antarctica. Antarctica is a continent dedicated to scientific research, and its population consists mainly of researchers and support personnel. Fraudulent activities like money laundering are highly unlikely in such a controlled and monitored environment.

Sours: Authors from available data

CONCLUSION

As cryptocurrencies become more popular, there is a possibility that money laundering using cryptocurrencies could increase in the future. However, regulatory bodies and law enforcement agencies are working to develop measures to prevent and detect such activities. It's crucial to stay informed about regulations and best practices when dealing with cryptocurrencies to mitigate the risks associated with money laundering. What is prevention for money laundering cryptocurrency?

Preventing money laundering in cryptocurrencies involves implementing various measures, including:

1. Know Your Customer (**KYC) Procedures**: Require users to verify their identities to deter illicit activities.
2. **Anti-Money Laundering (AML) Compliance**: Implement AML controls and procedures to monitor and report suspicious activities.
3. **Transaction Monitoring**: Regularly monitor transactions for any irregularities or suspicious patterns.
4. **Risk-Based Approach**: Assess the risks associated with different transactions and clients to tailor preventive measures accordingly.
5. **Compliance with Regulations**: Stay updated with regulatory requirements and ensure compliance with local laws and guidelines.
6. **Blockchain Analytics**: Use blockchain analysis tools to track and investigate transactions on the blockchain.
7. **Training and Awareness**: Educate employees and users about money laundering risks and prevention measures.

By combining these prevention strategies, individuals and businesses can help combat money laundering in the cryptocurrency space. Based on the data presented in the paper, it can be concluded the money laundering process that their future is still expected, both on the national and global market.

REFERENCES

[1] Bjelobaba G, Paunovic M, Savic A, Stefanovic H, Doganjic J, Miladinovic Bogavac Z. (2022). Blockchain Technologies and Digitalization in Function of Student Work Evaluation. Sustainability. 2022; 14(9):5333. https://doi.org/10.3390/su14095333

[2] Chainalysis, (2023), Crypto Crime Report 2023, from: https://go.chainalysis.com/2023-crypto-crime-report.html

[3] Chainalysis, (2024), Crypto Crime Report 2024, from: https://go.chainalysis.com/2024-crypto-crime-report.html

[4] FATF, (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, Paris, France, from: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

[5] FBI'S, Federal Bureau of Investigation, (2023) *Cryptocurrency Crime Report 2023.* Internet Crime Complaint Center, http://www. FBI.gov

[6] IMF, (2023), The IMF and the Fight Against Money Laundering and the Financing of Terrorism, from: http://www.imf.org

[7] Joksimović, M., Peković, D., & Stamenovic, M., (2024) The importance of artificial intelligence in the fight against money laundering, The Second International Scientific Conference "Challenges of Digitalization in the Business World"Belgrade, November 23th 2023, Alfa

BK University, ISBN 978-86-6461-068-1, p.p.300-306.

[8] Joksimović, M., Vukčević, N., & Jovanović, L. (2023), The impact of cryptocurrencies on the environment and the increased risk of money laundering and the financing of terrorism at the micro and macro level, International Scientific Conference Green Economy In the Function of Solving Global Environmental Problems, Scientific and Professional Society for Environmental Protection Ecologica, Belgrade, Book of Apstract, p.30

[9] Joksimovic, M., Mitrovic, R. & Joksimovic, D. (2018) Money laundering and the financing of terrorism: the role of offshore business, Scientific Journal of Stanislaw Staszic University of Applied Sciences in Pila, Journal Progress in Economic Sciences, p-ISSN 2300-4088 e-ISSN 2391-5951, NR 5(2018) Pila, DOI: 10.14595/PES/05/014, Published: 2018-10-09 in Piła, Poland, p.p. 213-232

[10] Muminović, S. & Ljubić, M. (2013) Prevencija pranja novca u Srbiji – iskustva i izazovi, Revizor, 16(61), Institut za ekonomiku i finansije, Beograd, str. 9-23

[11] Ljubić, M. & Pavlović, V. (2016), The Role of the Accounting Profession in Prevention and Detection of Financial Statement Fraud, Academy of Criminalistic and Police Studies, International Scientific Conference “Archibald Reiss Days” 10-11. mart 2016. Reiss 2016, Academy of Criminalistic and Police, pp. 87-100

[12] Paunović, M., Joksimovic, M. & Doganjić, J. (2023), Blockchain as basis for ecosystem model insurance in international business, International Scientific Conference Green Economy In the Function of Solving Global Environmental Problems, Scientific and Professional Society for Environmental Protection Ecologica, Belgrade, Book of Apstract, ISBN 978-86-89061-17-8 p. 172.