A SEMINAR REPORT ON

"Cryptocurrency Crime: Emerging Risks and Strategies"

SUBMITTED TO

SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
FOR THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE ACADEMIC YEAR 2024-25
Of

THIRD YEAR OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ENGINEERING

Submitted By

Student Name: Pranjal Londhe
Roll No: 31

UNDER THE GUIDANCE OF

Prof. Darshana Bhamare
(Department of Artificial intelligence
and Machine Learning)

ISBMCOE, Nande

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING
ISBM COLLEGE OF ENGINEERING,
Pune-412115

SAVITRIBAI PHULE PUNE UNIVERSITY
A.Y.2024-25

CERTIFICATE

This is to certify that the Seminar Report entitles

"Cryptocurrency Crime: Emerging Risks and Strategies"

Submitted By

Student Name: Pranjal Londhe **Roll No: 31**

Is a a bonafide student of the institute and the work has been carried out by him/her under the supervision of **Prof. Darshana Bhamare** and it is approved for the partial fullfillment of therequirement of Savitribai Phule Pune University, for the Third Year degree of Artificial Intelligence and Machine Learning Engineering.

Prof.Darshana Bhamare	**Prof.Kirti Randhe**	**Dr.P.K.Srivastava**
Guide	HOD	Principal

Date : _____

Place:ISBM College of Engineering,Pune

Pune(Maharashtra)

Abstract

The rapid evolution of cryptocurrency has ushered in a new era of financial innovation, yet it has also attracted an array of criminal activities that exploit its decentralized and pseudonymous nature. This report examines the emerging risks associated with cryptocurrency crime, encompassing fraud, money laundering, ransomware, and other illicit activities. As digital currencies gain traction, the sophistication of criminal tactics continues to evolve, presenting significant challenges for regulatory bodies, law enforcement, and financial institutions.

The report begins by providing a comprehensive overview of the current landscape of cryptocurrency crime, highlighting recent trends and statistics that underscore the urgency of addressing these issues. Notably, the rise of decentralized finance (DeFi) platforms and non-fungible tokens (NFTs) has created new opportunities for illicit actors to engage in fraudulent schemes. Additionally, the report explores how the anonymity afforded by blockchain technology can complicate the tracing of illicit funds and the identification of offenders.

Further, the analysis delves into the various types of crimes associated with cryptocurrencies, detailing the mechanisms employed by criminals. For instance, phishing attacks and social engineering tactics are prevalent in cryptocurrency fraud, often leading to significant financial losses for individuals and organizations. The report also discusses the role of ransomware attacks, where hackers demand cryptocurrency payments, exacerbating the challenge for victims and law enforcement alike.

Keywords

Cryptocurrency, Crime, Fraud, Money Laundering, Ransomware, Decentralized Finance, Regulation, Blockchain Technology, Security, Risk Management, Compliance, Law Enforcement, Cybersecurity, Financial Innovation, Digital Economy.

ACKNOWLEDGEMENT

First and foremost, I would like to thank to my guide of this seminar, **Prof. Darshana Bhamare** for the valuable guidance and advice. She inspired me greatly to work in this seminar. Her willingness to motivate me contributed tremendously to my seminar work. I would also like to thank her for showing me some example that related to the topic of my seminar.

Apart from our efforts, the success of any seminar depends largely on the encouragement and guidelines of many others. So, i take this opportunity to express my gratitude **to Prof. kirti Randhe** Head of Department of Artificial Intelligence and Machine Learning Engineering, ISBM College Engineering, Nande who has been instrumental in the successful completion of this seminar work.

The guidance and support received from all the members who contributed and who are contributing to this seminar work, was vital for the success of the seminar. I am grateful for their constant support and help.

Pranjal Londhe

Roll no :31

(T.E. AIML)

CONTENTS

Acknowledgments **2**

Abstract **1**

1 Introduction **3**

1.1 Overview 3

1.2 Customer Review Analysis 4

1.2.1 Advantages 4

1.2.2 Challenges 4

1.2.3 Applications 4

1.3 Deep Learning 5

2 Literature Survey **6**

3 Motivation **8**

4 Problem Definition and Objectives **9**

4.1 Problem Definition 9

4.2 Objectives 9

5 MATERIALS AND METHODS **10**

6 Results **12**

6.1 Dataset 12

6.2 Results 14

7 Conclusion and Future Work **17**

7.1 Future Work 17

8 References **19**

CHAPTER 1 : INTRODUCTION

1.1 Overview

The advent of cryptocurrencies has revolutionized the financial landscape, introducing decentralized and digital forms of currency that offer various benefits, including increased transaction speed, lower fees, and greater privacy. However, the rapid growth and popularity of cryptocurrencies have also made them an attractive target for criminal activities. As digital currencies continue to evolve, so do the strategies employed by criminals, leading to a surge in cryptocurrency-related crimes. This report aims to explore the emerging risks associated with cryptocurrency crime and propose strategies for mitigating these threats. Understanding these dynamics is crucial for stakeholders, including investors, regulators, and law enforcement agencies, to safeguard the integrity of the cryptocurrency ecosystem and protect users from potential harm.

As more individuals and institutions engage with cryptocurrencies, the associated risks are becoming increasingly pronounced. Fraudulent schemes, such as Ponzi schemes and phishing attacks, have proliferated, targeting both novice investors and seasoned traders. Moreover, the anonymity offered by cryptocurrencies has facilitated significant challenges for law enforcement, particularly in combating money laundering and ransomware attacks.

This report will explore the emerging risks posed by cryptocurrency-related crimes and propose effective strategies for mitigating these threats. Understanding these dynamics is essential for regulators, law enforcement, and investors to foster a safer and more secure cryptocurrency ecosystem. Through comprehensive regulation, enhanced security measures, and public education, stakeholders can work collaboratively to address the risks and uphold the integrity of the digital financial system.

1.2 Customer Review Analysis

As the cryptocurrency market continues to expand, user experiences and feedback provide valuable insights into the emerging risks and strategies associated with cryptocurrency crime. Analyzing customer reviews reveals several key themes that highlight the concerns and percep- tions of users in this evolving landscape.Customer reviews serve as a crucial feedback mechanism for identifying the emerging risks associated with cryptocurrency crime and the strategies needed to address them. By understanding user concerns and experiences, stakeholders can develop more effective security measures, educational resources, and regulatory frameworks, ultimately enhancing the safety and integrity of the cryptocurrency ecosystem.

1.2.1 Advantages

- Focusing on cryptocurrency crime helps raise awareness among users about potential risks, empowering them to make informed decisions and recognize scams.
- The recognition of emerging risks encourages exchanges and platforms to adopt advanced security measures, protecting users' assets and fostering greater trust in the ecosystem.
- Training law enforcement agencies on cryptocurrency technologies and crime detection strengthens their ability to investigate and combat financial crimes effectively.

1.2.2 Challenges

- The inherent anonymity of cryptocurrencies makes it difficult for law enforcement to trace transactions and identify perpetrators, complicating crime prevention and investigation efforts.
- Cybercriminals continuously adapt their tactics to circumvent security measures, making it difficult for exchanges and platforms to keep up with emerging threats.
- The decentralized nature of cryptocurrencies complicates oversight and accountability, as there is no central authority to enforce regulations or provide guidance.

1.2.3 Applications

1. Development of AI-driven tools to identify and flag potential fraudulent activities in real-

time, helping users and exchanges prevent scams.

2. Tools to monitor trading activities across exchanges for unusual patterns, helping detect potential market manipulation or fraudulent schemes.
3. Platforms that facilitate open communication between cryptocurrency projects and their users, promoting transparency and building trust

1.3 Deep Learning

Deep learning offers powerful applications in combating cryptocurrency crime by leveraging advanced algorithms to enhance detection and prevention strategies. By analyzing vast datasets, deep learning models can identify fraudulent transactions by recognizing patterns that deviate from typical user behavior, allowing for real-time alerts on suspicious activities. Natural language processing techniques enable these models to detect phishing attempts by analyzing the language and context of communications, thereby protecting users from scams. Additionally, deep learning can process blockchain transaction data to spot anomalies indicative of money laundering or organized crime. Predictive analytics powered by historical data helps forecast potential criminal trends, allowing stakeholders to implement proactive measures. Furthermore, sentiment analysis of social media can provide early warnings of market manipulation, while automated reporting systems streamline compliance with regulatory requirements. However, challenges such as data privacy concerns, model bias, and the need for continuous updates to counteract evolving criminal tactics must be addressed. Overall, the application of deep learning significantly enhances the ability to safeguard the cryptocurrency ecosystem against emerging risks.

CHAPTER 2 : LITERATURE SURVEY

1. Nature of Cryptocurrency Crime

Researchers have classified cryptocurrency crimes into several categories, including fraud, money laundering, ransomware, and cyberattacks. Studies by Zohar (2015) and Fujimoto(2020) emphasize the unique characteristics of cryptocurrencies that facilitate these crimes, such as anonymity and lack of regulation.

2. Fraud and Scams

Numerous studies detail the prevalence of fraud in the cryptocurrency space, including Ponzi schemes and ICO scams. A notable paper by Li et al. (2021) analyzes the psycho- logical factors that lead investors to fall victim to these schemes, highlighting the need forimproved investor education.

3. Money Laundering Techniques

Research by Foley etal. (2019) investigates how cryptocurrencies are used in money laun- dering, focusing on techniques such as mixers and the use of multiple exchanges to obscure transaction trails. The study underscores the challenges regulators face in tracking illicitfunds across borders.

4. Ransomware Attacks

The rise of ransomware attacks demanding payment in cryptocurrencies is well-documented. A study by IBM (2021) outlines how cybercriminals leverage the anonymity of cryptocur- rencies to extort victims, emphasizing the need for robust cybersecurity measures.Other studies emphasize the importance of international cooperation to address cross-border challenges.

5. Regulatory Responses

Literature on regulatory approaches is varied, with scholars like Arner etal. (2017) advo- cating for a balanced regulatory framework that protects consumers while fostering inno- vation. Other studies emphasize the importance of international cooperation to address cross-border challenges.Other studies emphasize the importance of international coopera- tion to address cross-border challenges.

6. **Blockchain Analysis Tools**
   Several papers discuss the development of blockchain analysis tools designed to detect and investigate cryptocurrency crime. Research by Chainalysis (2020) demonstrates how these tools can trace illicit transactions and assist law enforcement in prosecuting offenders.

7. **Deep Learning and AI Applications**
   Recent studies highlight the potential of deep learning and artificial intelligence in com- bating cryptocurrency crime. For example, research by Kwon etal. (2022) illustrates how machine learning algorithms can enhance fraud detection and anomaly recognition in transaction data.

8. **Public Awareness and Education**
   Literature also stresses the importance of public awareness campaigns to educate users about the risks of cryptocurrency investment. Studies indicate that informed users are less likely to fall victim to scams and fraud.

9. **Community-Driven Approaches**
   Some research explores the role of community engagement in identifying and reporting sus- picious activities. This approach, highlighted by experts like Lummis (2021), can enhance overall security within the cryptocurrency ecosystem.

10. **Future Directions**
    Emerging research suggests a need for interdisciplinary approaches combining technology, law, and social sciences to address the complexities of cryptocurrency crime. Scholars advocate for ongoing collaboration between academia, industry, and regulators to adaptto the rapidly evolving landscape.

CHAPTER 3 : MOTIVATION

The motivation behind exploring "Cryptocurrency Crime: Emerging Risks and Strategies" stems from the rapid growth and adoption of cryptocurrencies in recent years. As digital currencies gain popularity, they have simultaneously attracted a diverse range of criminal activi- ties, posing significant challenges to users, regulators, and law enforcement.Increasing Incidence of Crime: Reports of fraud, hacking, money laundering, and other illicit activities related to cryptocurrencies have surged. This alarming trend necessitates an in-depth analysis to iden- tify and address the emerging risks associated with digital currencies.Protecting Investors and Users: Many individuals are entering the cryptocurrency market without sufficient knowledge of its risks. By highlighting these dangers and providing strategies for mitigation, we can better protect users from falling victim to scams and fraudulent schemes.Regulatory Imperatives: As governments and regulatory bodies seek to establish frameworks for cryptocurrency use, under- standing the criminal landscape is crucial. Effective regulation can help foster a safer environ- ment for legitimate cryptocurrency activities while deterring criminal behaviors.Technological Evolution: The rapid advancements in blockchain technology and associated tools present both opportunities and challenges. Exploring how these technologies can be leveraged to combat crime is vital for maintaining the integrity of the cryptocurrency ecosystem.Cryptocurrency crime is not confined by borders. Understanding its global nature and the collaborative efforts required to address it is essential for creating comprehensive strategies that can be implemented worldwide.Addressing the risks associated with cryptocurrency crime is crucial for promoting public trust in digital assets. A secure and transparent environment is necessary for broader adoption among individuals and institutions.The complexities of cryptocurrency crime call for interdis- ciplinary collaboration among technologists, law enforcement, regulators, and academics. This report aims to foster dialogue and share insights that can lead to more effective crime prevention strategies.

CHAPTER 4 : PROBLEM DEFINITION AND OBJECTIVES

Problem Definition

As the cryptocurrency market continues to expand, it faces an increasing array of criminal activities that exploit its unique characteristics, such as decentralization, anonymity, and rapidtransaction capabilities.

4.1 Objectives

- Identify and Analyze Risks: To systematically identify and analyze the various types of crimes associated with cryptocurrencies, including fraud, money laundering, ransomware, and cybersecurity threats.
- Identify and Analyze Risks: To systematically identify and analyze the various types of crimes associated with cryptocurrencies, including fraud, money laundering, ransomware, and cybersecurity threats.
- Identify and Analyze Risks: To systematically identify and analyze the various types of crimes associated with cryptocurrencies, including fraud, money laundering, ransomware, and cybersecurity threats.
- Explore Technological Solutions: To investigate the role of advanced technologies, includ- ing deep learning and blockchain analysis tools, in detecting and preventing cryptocurrency crime.
- Foster Collaboration: To emphasize the need for collaboration among stakeholders—includingregulators, law enforcement, industry players, and academia—to develop comprehensive strategies for combating cryptocurrency crime.
- Provide Strategic Recommendations: To offer actionable strategies and best practices for mitigating risks, enhancing security measures, and promoting a safer cryptocurrency ecosystem.

CHAPTER 5 : MATERIALS AND METHODS

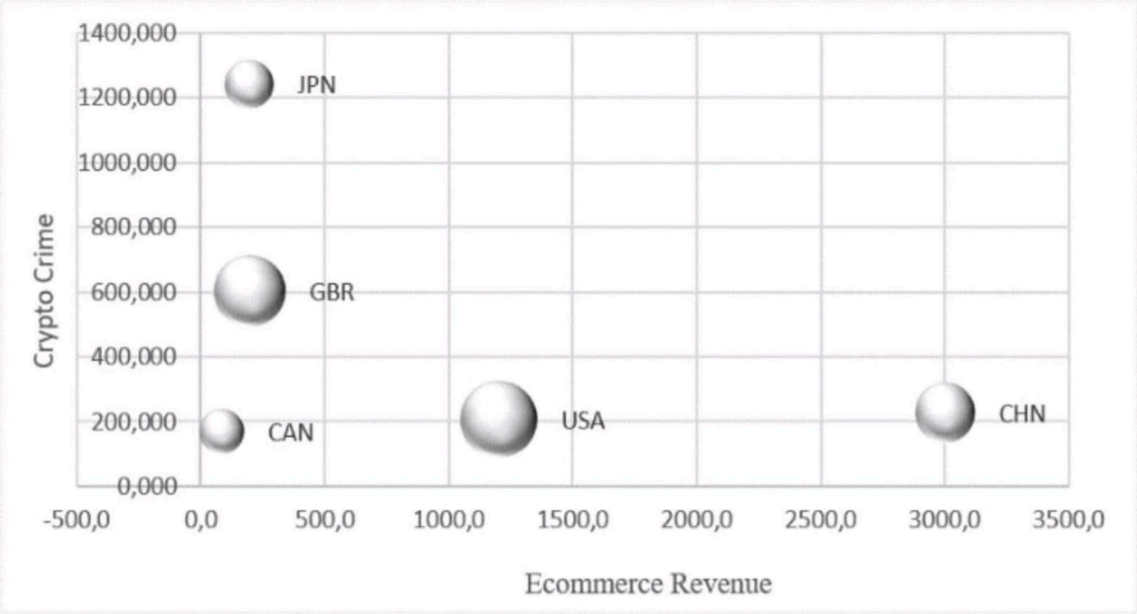
A. THE RISK OF THE CRYPTOCURRENCY: THE DANGERS OF THE BENEFITS

The rapid rise in the popularity of cryptocurrency, a digital payment system secured by cryp- tography, has transformed how people conduct transactions. Operating on a decentralized, peer-to-peer network, cryptocurrencies allow users to send and receive funds without relying on traditional financial institutions. This system offers advantages such as anonymity and ease of transferring large sums, making it appealing for both legitimate users and cybercriminals. As cryptocurrencies become more integrated into various sectors, including well-known brands and popular marketplaces, they simultaneously attract illicit activities, posing significant risks to users. The Dual Nature of Cryptocurrency Cryptocurrency's advantages stem from its foun- dational technology, which enables secure and anonymous transactions through digital wallets and exchanges. While these features enhance user convenience, they also facilitate criminal activities. The lack of government regulation and oversight provides a fertile ground for cyber- criminals to exploit these systems, leading to an increase in cyberattacks, fraud, and other illegal activities. Current data protection technologies often fall short in safeguarding users from infor- mation leaks and cyber threats, leaving individuals vulnerable. Rising Threats and High-Profile Incidents Recent incidents underscore the escalating risks associated with cryptocurrency. In September 2023, CoinEx, a Hong Kong-based cryptocurrency exchange, suffered a cyberattack resulting in a loss of 70*million.*

Similarly, high-profile breaches involving prominent figures in the cryptocurrency space, such as the Ethereum co-founder, have led to significant financial losses through phishing attacks. The November 2023 theft of 26*millionfromKronosResearchand*54.7 million from KyberSwap further illustrates the challenges faced by both users and platforms in maintaining security. Moreover, fraudulent applications, such as a fake Ledger Live app in the Microsoft Store, haveled to substantial user losses, totaling at least 768*,* 000*.*

The emergence of fake accounts impersonating blockchain security organizations highlights the sophistication of cybercriminals, who generate significant income through deception. The Evolving Landscape of Cybercrime Cybercriminals continuously refine their methods alongside

advancements in technology. Techniques such as cryptojacking—unauthorized use of devices for cryptocurrency mining—are becoming more prevalent. According to "The 2023 Crypto Crime Report" by Chainalysis, cryptocurrency-related crime reached unprecedented levels in 2022, with illegal transactions surging. This alarming trend necessitates urgent attention from users, regulators, and industry stakeholders. reached 20.1*billioncomparedto*18 billion in 2021. These estimates are only preliminary and do not take into account the profits from non-cryptocurrency crime where cryptocurrency was used as a form of payment. For example, revised estimates for 2021 were 4*billionhigherthanpreviousfigures.*



Almost 15 years ago, the official recognition of Bitcoin as a digital currency and payment sys- tem took place. Since then, the use of cryptocurrency has rapidly spread worldwide. However, along with the benefits for its users, transparency and uncontrolled cryptocurrency transactions have provided criminals with the opportunity to use them as fake internet money, particularly in the Deep Web for transactions related to drugs, weapons, pornography, and other prohibited goods. Cryptocurrency crime expands with the growth of the cryptocurrency market, asserting its criminal reputation. It is impossible to determine a typical criminal profile for a crypto- criminal: it can be anyone, from a novice teenager to groups of experienced hackers. However, some countries have much more developed cryptocurrency crimes than others. Therefore, re- search on detecting subtle correlations between different factors associated with cryptocurrencies and their impact on the level of cybersecurity worldwide is relevant.

CHAPTER 6 : RESULTS

6.1 Dataset

6.1.1 DATA SET AND PRELIMINARY DATA PREPARATION FOR CORRESPONDENCE :

The issue of studying the main risks of using cryptocurrencies is important for the personal and financial security of individual users, businesses, governance, and cybersecurity of countries around the world. Therefore, it is important to study various aspects related to the risk factors of the cryptocurrency environment. To establish the implicit relationships between the individ- ual dimensions of the cryptocurrency environment discussed in Sections III-A-III-C, which are not obvious due to the specific methodology of their calculation.

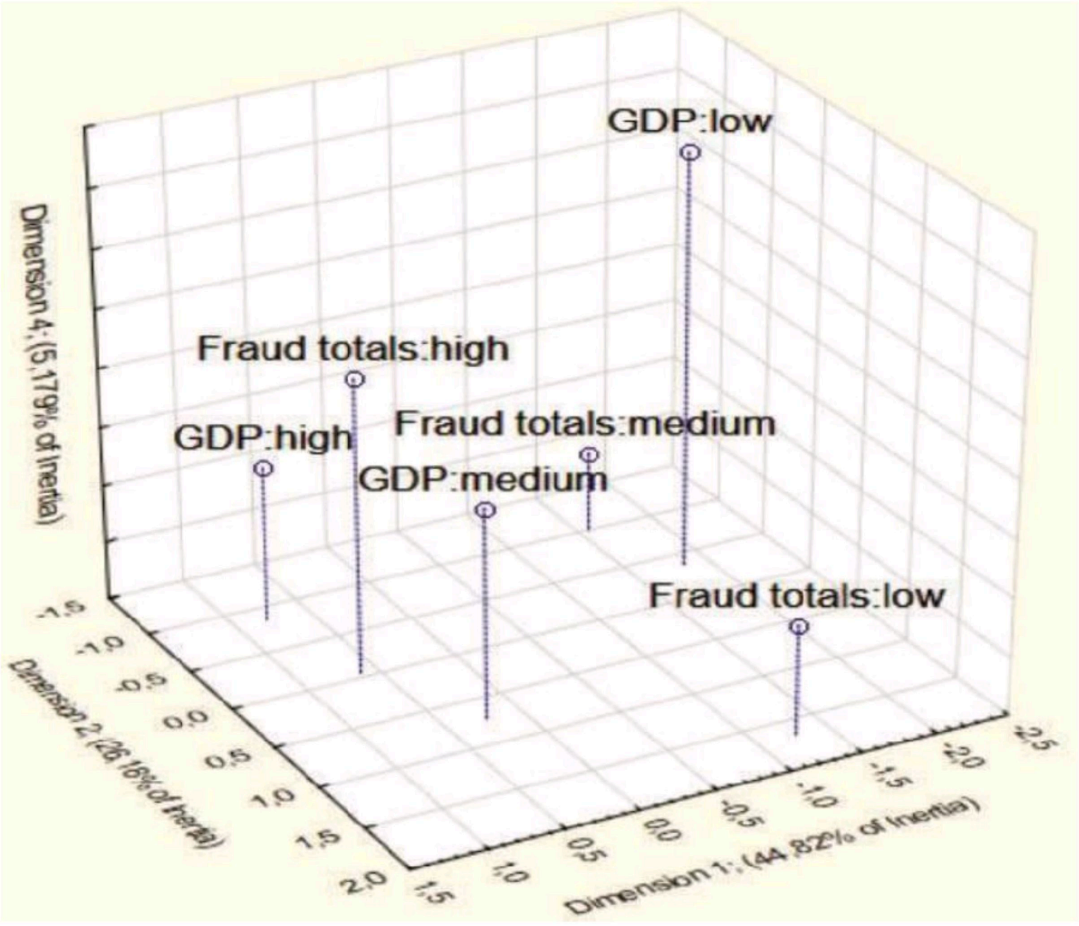
In particular, in the GCAI, countries with the same Index score have different Index ranks . These features require ad- ditional research. To establish the implicit relationships between fraud cryptocurrency crime totals, NCSI, GCAI, DDL, and GDP , a correspondence analysis was conducted between the following pairs of indicators: fraud cryptocurrency crime totals, and GDP, fraud cryptocurrency crime totals and DDL; fraud cryptocurrency crime totals and GCAI; fraud cryptocurrency crime totals and NCSI; NCSI and GCAI. Correspondence analysis is an exploratory analysis that al- lows you to build a visual association model between categories of two nominal variables. The correspondence table of the variables under study is an image in a multidimensional space. Its rows and columns represent points and calculate the distances between them. The goal of cor-respondence analysis is to find the space of the lowest dimensionality in which the data points representing the categories of the original variables can be reproduced with maximum accuracy Such unique insights can only be obtained through correspondence analysis.

	Country	GCA	NCSI	DDL
AFG	Afghanistan	147	12,99	19,50
ALB	Albania	85	62,34	48,74
DZA	Algeria	47	33,77	42,81
ATG	Antigua and Barbuda	145	11,69	57,10
ARG	Argentina	15	63,64	60,43
ARM	Armenia	89	35,06	55,06
AUS	Australia	41	66,23	77,61
AUT	Austria	84	85,71	75,76
AZE	Azerbaijan	74	63,64	54,78
BHS	Bahamas	127	20,78	65,10
BHR	Bahrain	133	57,14	65,17
BGD	Bangladesh	17	67,53	33,11
BRB	Barbados	148	19,48	73,10
BLR	Belarus	44	53,25	62,33
BEL	Belgium	81	18,18	37,10
BEN	Benin	80	58,44	25,83
BOL	Bolivia	79	31,17	42,09
BIH	Bosnia and Herzegovina	126	28,57	49,31
DWA	Botswana	144	29,87	41,96
BRA	Brazil	9	51,95	59,11
BRN	Brunei	153	41,56	67,50
BGR	Bulgaria	58	74,03	62,06
CHM	Cambodia	30	23,38	34,59
CMR	Cameroon	42	32,47	28,28
CAN	Canada	19	70,13	75,96
CHL	Chile	68	59,74	61,44
CHN	China	11	51,95	62,41
COL	Colombia	32	53,25	52,08
COD	Congo, Dem. Rep.	130	5,19	18,91
CIV	Cote d'Ivoire	65	44,16	33,54
	Croatia	102	83,12	64,63
HRV	Cuba	136	16,88	29,10
CUB	Cyprus	123	66,23	68,83
CYP	Czech Republic	62	90,91	69,21
CZE	Denmark	112	84,42	82,68
DNK	Dominican Republic	71	71,43	45,21
DO	Ecuador	43	53,25	45,57
EC	Egypt	35	57,14	46,93

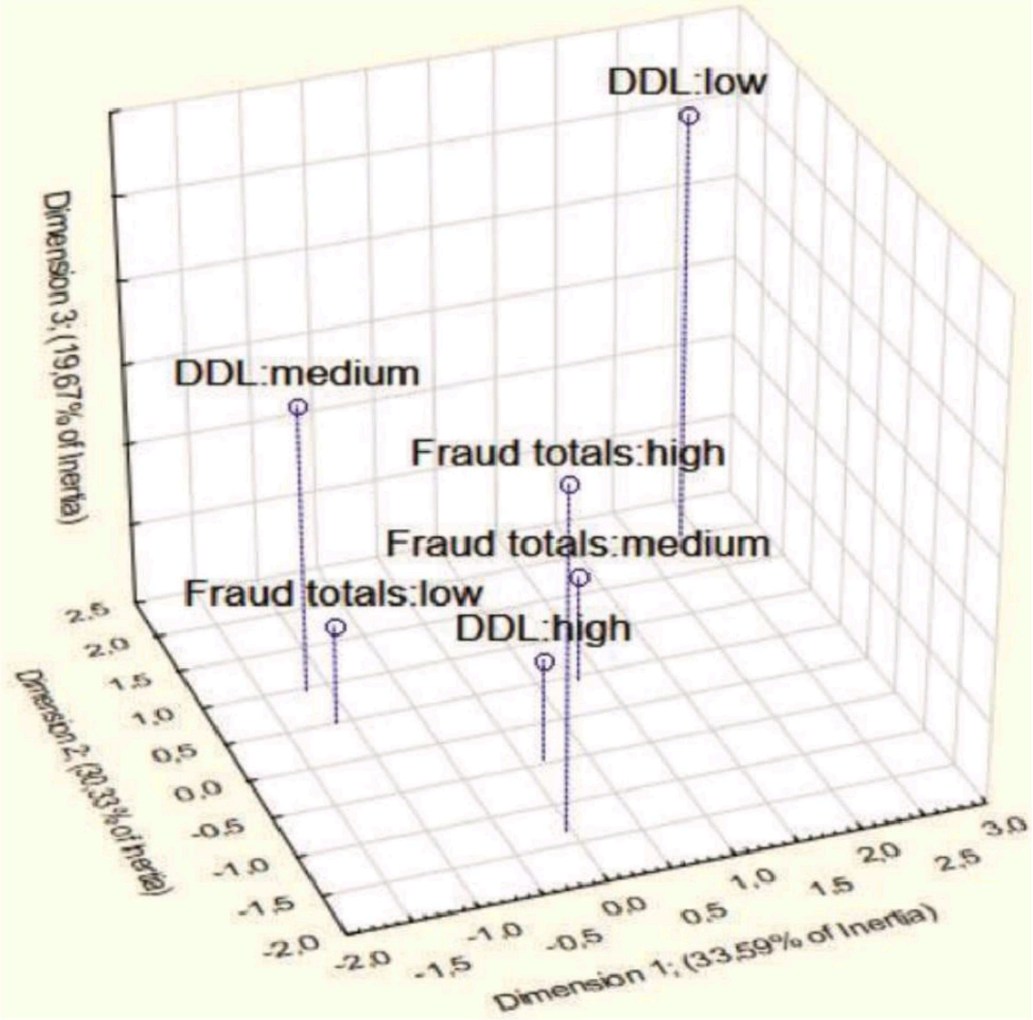
The values of the National Cyber Security Index (ranging from 1.30 to 94.81), Digital Devel- opment Level (ranging from 11.30 to 82. 93), GDP (in the range of 241 and 22939581 *million*), fraud cryptocurrency assets crime totals (in the range of 4 and 2269521 *thousands*)*and* Global Crypto Adoption Index score (in the range of 0 to 1), which are unevenly distributedamong countries

6.2 Results

For a quality representation of the highlighted categories of variables, fraud cryptocurrency crime totals, and GDP, four dimensions are needed. The first dimension in this case FIGURE . The 3D plot of column coordinates of fraud cryptocurrency crime totals and GDP. “extracts” 44.82the third – 23.82increases the “extracted” inertia to 100An objective assessment of the proximity of empirical and theoretical distributions in the analysis of correspondence is the 2-test. In our case, the significance level p-level < 0.01. Therefore, the obtained results of the correspondence analysis are statistically significant. The number of degrees of freedom df = 25, 2 e = 210.47. 20 (0.01;25) = 44.3. 2 e > 2 0 . This means that the expected values are sufficiently close to the observed ones.



we can conclude that there are correlations between a low level of Fraud total and a medium level of GDP, between a high level of Fraud total and a low level of GDP, and between the medium level of Fraud total and medium level of GDP for the countries under study. Thus, there is no obvious connection between the level of economic development of a country and thelevel of cryptocurrency fraud.



For a quality representation of the crosstab table values of the variables fraud c cryptocurrency crime totals and DDL, four dimensions are needed. The first dimension, in this case, “extracts” 33.59and the third – 19.67increases the “extracted”inertia to 100

CHAPTER 7 : CONCLUSION AND FUTURE WORK

This report has outlined the various types of cryptocurrency crimes, explored the chal- lenges posed by emerging technologies, and emphasized the necessity for collaborative efforts among regulators, law enforcement, and industry stakeholders. Effective risk assessment, user education, and the implementation of advanced technological solutions are vital to protecting users and maintaining the integrity of the cryptocurrency ecosystem.This report has outlined the various types of cryptocurrency crimes, explored the challenges posed by emerging technologies, and emphasized the necessity for collaborative efforts among regulators, law enforcement, and industry stakeholders. Effective risk assessment, user education.

This report has outlined the various types of cryptocurrency crimes, explored the chal- lenges posed by emerging technologies, and emphasized the necessity for collaborative efforts among regulators, law enforcement, and industry stakeholders. Effective risk assessment, user education, and the implementation of advanced technological solutions are vital to protecting users and maintaining the integrity of the cryptocurrency ecosystem.

7.1 Future Work

- Enhanced Regulatory Frameworks: Research into best practices for creating regulatory frameworks that balance consumer protection with innovation is essential. This includes examining international cooperation to address the borderless nature of cryptocurrencycrime.
- Advanced Technological Solutions: Continued investment in advanced technologies, such as machine learning and AI for fraud detection, can significantly improve the ability to identify and respond to criminal activities in real-time.
- User Education and Awareness: Developing comprehensive educational programs to raise awareness about the risks associated with cryptocurrency and best practices for security can empower users to protect themselves against scams and fraud.

- Collaboration and Information Sharing: Establishing platforms for information sharing among industry stakeholders, regulators, and law enforcement can enhance the collective ability to combat cryptocurrency crime.
- Longitudinal Studies on Crime Trends: Conducting longitudinal studies to track trends in cryptocurrency crime will provide valuable insights into emerging threats and the effec- tiveness of implemented strategies.
- Behavioral Research: Exploring the psychological factors that lead individuals to engage in or fall victim to cryptocurrency crime can inform preventive measures and educationalinitiatives.
- Ethical Considerations: As technology evolves, ethical considerations surrounding privacy, surveillance, and the balance between security and personal freedoms must be addressed.

REFERENCES

[1] E. Saiedi, A. Broström, and F. Ruiz, "Global drivers of cryptocurrency infrastructure adop- tion," Small Bus. Econ., vol. 57, no. 1, pp. 353–406, Jun. 2021, doi: 10.1007/s11187-019- 00309-8.

[2] P. Weichbroth, K. Wereszko, H. Anacka, and J. Kowal, "Security of cryptocurrencies: A view on the state-of-the-art research and current developments," Sensors, vol. 23, no. 6, p. 3155, Mar. 2023, doi: 10.3390/s23063155.

[3] O. Kovalchuk, M. Masonkova, and S. Banakh, "The dark Web worldwide 2020: Anonymous vs safety," in Proc. 11th Int. Conf. Adv. Comput. Inf. Technol. (ACIT), Sep. 2021, pp. 526–530.

[4] O. Kovalchuk, M. Shynkaryk, M. Masonkova, and S. Banakh, "Cybercecurity: Technology vs safety," in Proc. 10th Int. Conf. Adv. Comput. Inf. Technol. (ACIT), Sep. 2020, pp. 765–768.

[5] J. Reed. (2022). Cryptocurrency-related Crime Boomed in 2022. [Online]. Available: https://securityintelligence.com/news/cryptocurrency-relatedcrime-boomed-2022/

[6] World Economic Forum. (2023). Global Risks Report 2023. [Online]. Available: https://www.weforum.org/publications/global-risks-report- 2023

[7] M. Majeed, K. S. Ofori, G. K. Amoako, A.-R. Alolo, and G. Awini, "The rise of blockchain applications in customer experience," in Advances in Marketing, Customer Relationship Management, and E-Services. Hershey, PA, USA: IGI Global, Nov. 2023, doi: 10.4018/978-1-6684-7649-9.

[8] X. Yang, "Blockchain-based financing," U.S. Patent 20 200 294 140 A1, Sep. 17, 2020.

[9] Y. Xinxin, "Block chain-based method and device for distributing copyright income of works," Taiwan Patent TWI 701 619 B, Aug. 11, 2020.

[10] (2023). 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All- Time Highs Amid Surge in Sanctions Designations and Hacking. [Online]. Available: https://www.chainalysis.com/blog/2023-cryptocrime- report-introduction

[11] BCS. (2023). The Biggest Cyber Attacks of 2023. [Online]. Available: https://www.bcs.org/articles-opinion-and-research/the-biggest-cyberattacks- of-2023

[12] A. Greubel, D. Andres, and M. Hennecke, “Analyzing reporting on ransomware incidents: A case study,” Social Sci., vol. 12, no. 5, p. 265, Apr. 2023, doi: 10.3390/socsci12050265.

[13] J. A. G. Hernández, P. G. Teodoro, R. M. Carrión, and R. R. Gómez, “Crypto-ransomware: A revision of the state of the art, advances and challenges,” Electronics, vol. 12, no. 21, p. 4494, Nov. 2023, doi: 10.3390/electronics12214494.

[14] A. Alqahtani and F. T. Sheldon, “A survey of crypto ransomware attack detection methodologies: An evolving outlook,” Sensors, vol. 22, no. 5, p. 1837, Feb. 2022, doi: 10.3390/s22051837.

[15] Bank for International Settlements. The Crypto Ecosystem: Key Elements and Risks. Ac- cessed: Dec. 14, 2023. [Online]. Available: https://www.bis.org/publ/othp72

[16] M. C. Şcheau, S. L. Crăciunescu, I. Brici, and M. V. Achim, “A cryptocurrency spec- trum short analysis,” J. Risk Financial Manage., vol. 13, no. 8, p. 184, Aug. 2020, doi: 10.3390/jrfm13080184.

[17] S. Kapoor. Cybercrimes in E-Commerce. Ijser.org. Accessed: Dec. 14, 2023. [Online]. Avail- able: https://www.ijser.org/researchpaper/ Cybercrimes-in-E-commerce.pdf

[18] C. Davison, P. Akhavan, T. Jan, N. Azizi, S. Fathollahi, N. Taheri, O. Haass, and M. Prasad, “Evaluation of sustainable digital currency exchange platforms using analytic mod- els,” Sustainability, vol. 14, no. 10, p. 5822, May 2022, doi: 10.3390/su14105822.

[19] D. Sanz-Bas, C. del Rosal, S. L. N. Alonso, and M. Á. E. Fernández, “Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain,” Laws, vol. 10, no. 3, p. 57, Jul. 2021, doi: 10.3390/laws10030057.

[20] L. P. Krishnan, I. Vakilinia, S. Reddivari, and S. Ahuja, “Scams and solutions in cryptocur- rencies—A survey analyzing existing machine learning models,” Information, vol. 14, no. 3,p. 171, Mar. 2023, doi: 10.3390/info14030171.

[21] K. Zhao, G. Dong, and D. Bian, “Detection of illegal transactions of cryptocurrency basedon mutual information,” Electronics, vol. 12, no. 7, p. 1542, Mar. 2023, doi: 10.3390/elec- tronics12071542.