Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 12. Issue.01, PP. 12-25, June 2024
https://doi.org/10.22555/pjets.v12I1.1121
E-ISSN 2224-2333
P-ISSN 2222-9930

Cryptocurrency Crimes: A Systematic Literature Review of Bitcoin's Role in Illicit Activities

Dr. Dodo Khan[1], Hira Farman [2], Saif Hassan[3], Moomal Seelro[4], Muhammad Hussain Mughal[5]
[1]Thar Institute of Engineering, Sciences and Technology, NED University of Engineering and Technology, Karachi, Pakistan
[2] Iqra University Karachi, Pakistan
[3,4,5] Department of Computer Science, Sukkur IBA University,

[*]Corresponding author: *dodo.khan@neduet.edu.pk*

Abstract:

Bitcoin is the most successful cryptocurrency with the highest market capitalization of up to 53%. Due to its pseudonymous mechanism, bitcoin is being utilized in a variety of illicit activities. It is noticed that around US$72 billion of unlawful activities per year involve Bitcoin. In this study, a systematic literature review is conducted on the illicit use of Bitcoin, and the measures required to counter the illicit activities using Bitcoin. In this work, authors have managed to select 45 research articles published during 2018-2022. The synthesis of selected articles revealed that bitcoin is proliferating in darknet markets. It is used to make payments for criminal activities such as drug trafficking, money laundering, human trafficking, pornography, ransomware, and other criminal activities like contract killers, Ponzi schemes, and terrorism financing. According to the findings from this study, out of 45 research articles, 24.4% of articles claim that Bitcoin has been used in drug trafficking whereas 17.7% believe that people use Bitcoin for money laundering. Moreover, Blockchain identity flexibility, dissociative anonymity, and a lack of deterrence encourage users to perform illegal activities. At present, the research community is actively involved in proposing and designing innovative approaches to counter the illicit use of Bitcoin. However, these solutions are unable to stop the misuse of Bitcoin.

Keywords: *Bitcoin, Cryptocurrency, Illicit, Review,*

I. INTRODUCTION

Blockchain technology is the most talked-about technology of the twenty-first century [1]. It is one of the most disruptive technologies, with the potential to change businesses in a variety of sectors. According to a World Economic Forum [2] study, blockchain will account for 10% of global GDP by 2027. Furthermore, it has served as the core technology behind various cryptocurrencies, including Bitcoin. Bitcoin was invented by Satoshi Nakamoto in 2008 and is the most successful cryptocurrency [3]. Aside from Bitcoin, there are already over 7,000 active cryptocurrencies worldwide. Bitcoin, on the other hand, has the most market capitalization of up to 53%. The primary motive for the invention of cryptocurrencies is egalitarianism, or the avoidance of central authority such as the financial system or the government. Cryptocurrencies are characterized as alternative money that is decentralized and partly private [8]. Bitcoin uses cryptographic algorithms and peer-to-peer networks controlled by a totally distributed ledger with no central authority [3]. Anonymizing a Bitcoin user's identity is accomplished by using the hashed value of the public key with the digital signature technique [1].

Due to its pseudonymous nature, bitcoin is being utilized in a variety of unlawful illegal activities including to sell or buying illicit narcotics [5] on the dark web. It is also being used in money laundering, human trafficking, funding

terrorism, and child exploitation pornography. Moreover, almost one-quarter of Bitcoin users and half of Bitcoin transactions are involved with illegal behavior [4]. Bitcoin is involved in about US$72 billion of criminal activities every year, which is comparable to the size of the illegal drug markets in the United States and Europe [4]. Dark web market sales surged by 70% in 2019 alone, totaling more than USD$790 million every year. Thus, this caught the attention of researchers and law enforcement agencies. However, authorities across the globe are facing challenges to track down illegal acts and the criminals behind them.

In this study, the authors conducted a systematic literature review (SLR) on the illicit activities utilizing cryptocurrency (bitcoin). Firstly, extensive research was conducted on how cryptocurrency (bitcoin) is employed in illicit activities and the factors associated with it. Secondly, identifying different types of illegal activities where Bitcoin is used, and thirdly, we investigate the possible measures to counter the illegal activities in Bitcoin. This research shall assist law enforcement authorities in identifying crimes and tracking down the criminals who perpetrated them.

The rest of the paper is arranged as follows. Section 2 describes the survey methodology, while Section 3 examines the consolidated papers. Section 4,5,6 responds to the research questions, and lastly, section 7 discusses the conclusion.

II. SURVEY METHODOLOGY

This SLR followed the recommended reporting guidelines for systematic reviews and meta-analyses (PRISMA) [5]. A systematic literature review is defined as the process of understanding and evaluating existing research articles on a particular research subject and area of interest. This section describes our review methodology, which incorporates Kitchenham [5] described stages. Initially, publications were identified from several sources, and then duplicate and irrelevant articles were screened by reading the title, abstract, and then the complete text. Figure 1 depicts the whole process used in this SLR. The following section discusses every step in detail. This SLR consists of a formulation of research questions, eligibility criteria for identifying the most relevant articles, and information sources, a paper search technique, and data extraction procedures.

A. Need for Systematic Review

There are numerous research articles on the illicit use of cryptocurrency (bitcoin) are available. However, there is still a need for a comprehensive analysis of the illicit use of Bitcoin and the strategies to prevent or to timely detect illegal activities. As such this study looks at the illegal usage of bitcoin, as well as how the research community is assisting law enforcement agencies in identifying cryptocurrency related to unlawful acts to take legal action.

B. Research Question

What are the major illicit activities that have taken place using cryptocurrency (Bitcoin): The purpose of this SLR is to deeply investigate the illicit use of Cryptocurrency (Bitcoin). Thus, the goal of RQ-1 is to examine all pertinent academic research papers and data in order to identify the majority of illegal activities and scams involving Bitcoin and their crucial influence on law enforcement.

How cryptocurrency (Bitcoin) is used for illicit activities and what are the major factors associated with it: This question aims to review all relevant studies from academic research to identify probable processes of illicit use of cryptocurrency (bitcoin) and properties of cryptocurrency that support illicit crimes and list down major cryptocurrency fraud took place glo ally.

What are the innovative strategies the research community has proposed to detect illicit usage of Bitcoin: This question seeks to uncover how researchers around the world have attempted to detect or identify illicit crimes related

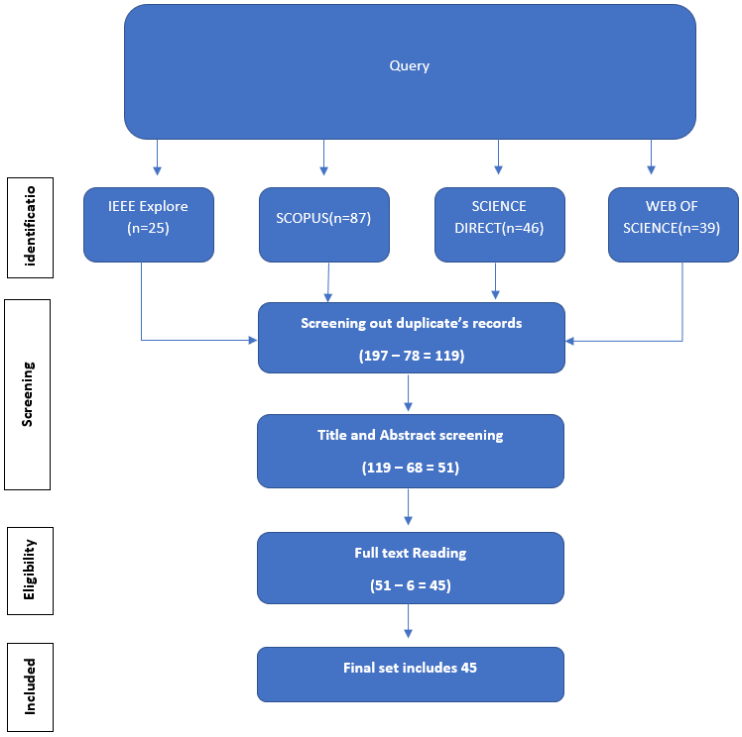

Figure 1: The methodology for this SLR

to cryptocurrency (bitcoin). This SLR is looking at research that provided concrete solutions that were then implemented, simulated, or formally demonstrated.

C. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were used to verify that selected studies on SLR were acceptable, and these are contributing to answering the research question provided in this SLR. We only choose research articles from (conferences and journals) authored in English and published between 2018 - 2022. Furthermore, only publications that meet any of the research questions are considered for inclusion in the present study. We excluded articles published in languages other than English since we couldn't comprehend them. The inclusion and exclusion criteria employed in this SLR are shown in Table 1.

D. Information and Data Sources

This research focuses on the cryptocurrency (bitcoin). Therefore, we relied on computer science related literature. Significant and concentrated computer sciences databases, as well as interdisciplinary resources, were searched. The articles were acquired from the following sources. These sources provide the most comprehensive coverage of high-quality publications, such as ISI- and Scopus- indexed articles [6] [5].

- Scopus
- Science Direct
- IEEE explores
- Web of Science

Table 1: List inclusion and exclusion criteria.

	Article Inclusion Criterian
1	**The study must be original research work instead of a review or a survey paper.**
2	**The papers are focusing on cryptocurrency illicit activities (directly or indirectly) and highlighting the relevant reasons/factors.**
3	**Papers proposing a feasible solution aiming to solve the blockchain/cryptocurrency illicit method (method, technique, model, and framework).**
4	**The proposed solutions have been evaluated (implemented, simulated, and formal proof).**
5	**The papers are published in peer-reviewed journals/conference journals.**
6	**The papers should only be in English language.**
7	**Published in between 2018-2023**
8	**Directly or indirectly address the research question**

E. Search Process

PRISMA activity requirements [5], demand predefined search procedures to prevent biasness during article searches. Therefore, our search procedures were created to perform a specific literature search using the internal search engines of the aforementioned publishing portals. Our search string keywords were identified via a series of exhaustive test searches. Keywords are "bitcoin, cryptocurrency, illicit activities, crime, illegal activities, law enforcement agencies"

F. Screening Process

To ensure that every article that has been searched is relevant to the study objectives, the incremental technique has been utilized. The first thing we do is to check the downloaded papers for duplicate articles that were collected from various data sources. The titles of all publications were then carefully screened to exclude those that were unrelated to the study topics. However, oftentimes it could be difficult to determine the relevance from the paper's title alone. This necessitated a more thorough review of each paper's abstract before deciding whether to accept it. It was essential to assess each article for its applicability to the RQs using the inclusion and exclusion criteria we had already established. The initial search returned a total of 197 articles. Only 119 articles were left after excluding duplicates and papers that weren't written in English. After looking at the abstracts and keywords of all 119 articles, we found 51 that were relevant to our study. After that, we looked at the full texts of these articles and chose 46 of them. Figure 1 shows the total number of papers that were found, processed, and found to be suitable for this SLR study.

G. Data Extraction

Based on the PRISMA activity criteria, an Excel sheet was created to perform the data collection procedure. The form was created to collect the necessary information from the articles in relation to the RQs. The form was divided into three sections: the characteristics/ of the chosen articles, the technical element of illicit activities, and the quality rating of the selected papers. All articles that passed the quality evaluation had data retrieved from them. The goal was to correctly capture just the necessary information from the papers. The quality evaluation was carried out in accordance with the standard PRISMA principles. It should be noted that the form's legitimacy is required to assure the authenticity of the data obtained. As a result, the form was carefully verified on 5 randomly chosen publications by performing data extraction and the form changed iteratively.

III. DISCUSSION CONSOLIDATED PAPER

The analysis of selected 45 published articles is discussed in this section. It delves into the study trend of bitcoin publishing for unlawful operations, as well as ways for dealing with such issues. To adequately answer the study questions, the data acquired throughout the data extraction procedure was properly collated, and demographic data was evaluated. Figure 2 depicts a year-by-year breakdown of the chosen articles. The growing interest in academic study on unlawful activities of bitcoin has resulted in an increase in the number of publications throughout the years. It should be highlighted that the bulk of academic studies on Bitcoin addressing illegal activities occurred between 2021 and 2022.

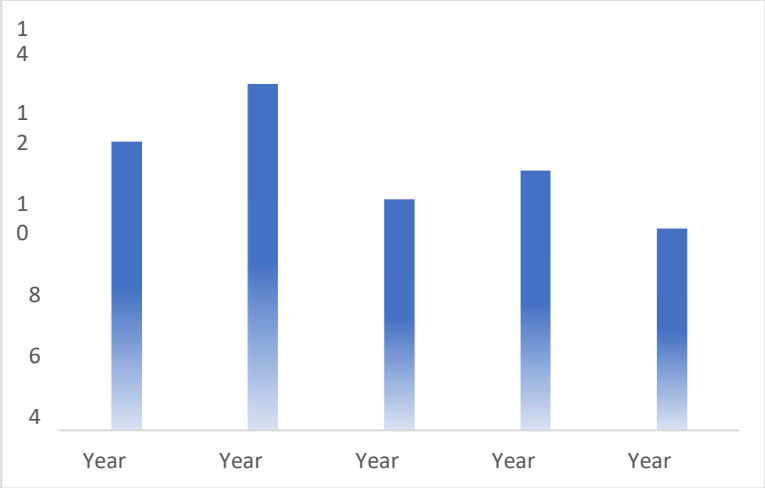

Figure 2: Shows the number of selected articles published in each year.

In 2018, the number of published articles discussing the illicit use of Bitcoin stood at 7. By 2022, this figure had risen to over 10 articles. Concurrently, blockchain technology started significantly impacting various sectors, prompting scholarly interest in exploring its potential criminal applications.

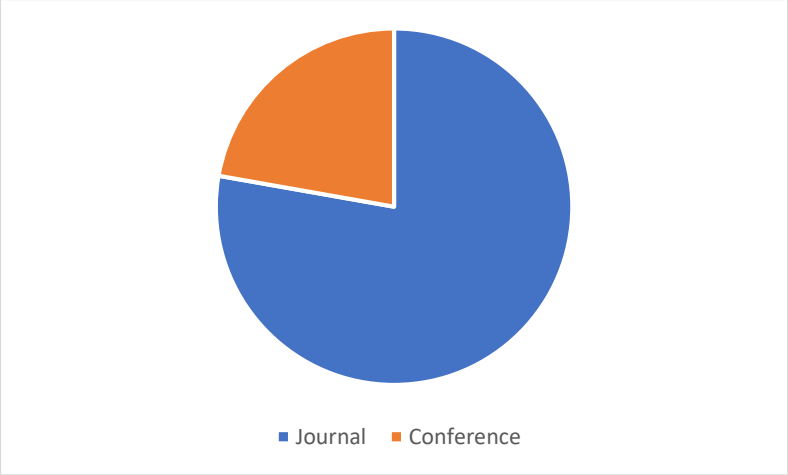

Figure 3: Figure illustrates the distribution of selected papers

Figure 3 illustrates the distribution of publication types among the selected papers in this systematic literature review (SLR). Analysis reveals that the majority of publications addressing the illicit use of Bitcoin were disseminated through academic journals, comprising 35 out of 45 articles, while 10 articles were presented in conference proceedings. Figure 4 depicts the statistical distribution of the chosen publications geographically. Russia leads with eight articles, followed by the United States with six publications (published in academia or industries). Furthermore, China is the fourth top nation with five papers, closely followed by Italy with four papers, and Switzerland, Australia, India, and Canada with one, two, and three papers, respectively. This report illustrates the scholarly community's interest in Bitcoin in illicit activity

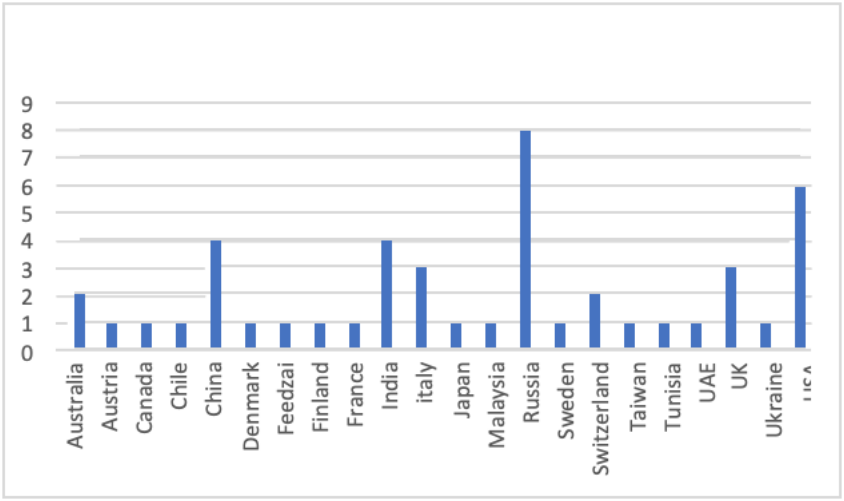

Figure 4: The global distribution of chosen papers is analyzed

IV. WHAT ARE MAJOR ILLICIT ACTS TAKING PLACE USING CRYPTOCURRENCY (BITCOIN)

In this internet era, numerous crimes and illicit activities are associated with the online world. Although blockchain technology, particularly cryptocurrency, is a new and trending development, it is frequently used for illegal activities. Its inherent anonymity makes it nearly impossible to trace.

Table 2 highlights the major illicit acts along with the relevant citations, which include financial scams, human trafficking, pornography, drug trafficking, money laundering, ransomware, financing terrorism, criminal activities, and blackmail.

Figure 5 shows the list of illegal activities related to cryptocurrency derived from this SLR. Table 2 illustrates the list of illegal activities with the relevant citations. Drug trafficking (Illicit drugs) is the most-discussed illicit activity, with more than ten papers exploring blockchain's role in drug trafficking or techniques to combat drug trafficking. After drug trafficking, money laundering (tax evasion) is the subject of almost ten research publications as a prominent topic of emphasis for the academic community. Criminal activities concerning Bitcoin were covered in 8 articles (Contract killers, Bitcoin tumbler, Cybercrime, darknet market) [46][47]. Six articles examined financial fraud (Ponzi schemes, counterfeit apparel, financial sanctions), followed by human trafficking, pornography (sextortion), ransomware, funding terrorism, and blackmail (The theft of cryptocurrencies to kidnapping).

Table 2: The list of illicit activities related to Bitcoin

Financial Scam	**[7-11]**
Human trafficking	**[12]**
Pornography	**[7, 12]**
Drug trafficking	**[12-21]**
Money laundering	**[4, 11, 12, 22-25]**
Ransomware	**[7, 11, 12, 26, 27]**
Financing terrorism	**[8, 27, 28]**
Criminal activity	**[7, 12, 25, 29-31]**
Blackmail	**[7, 11]**

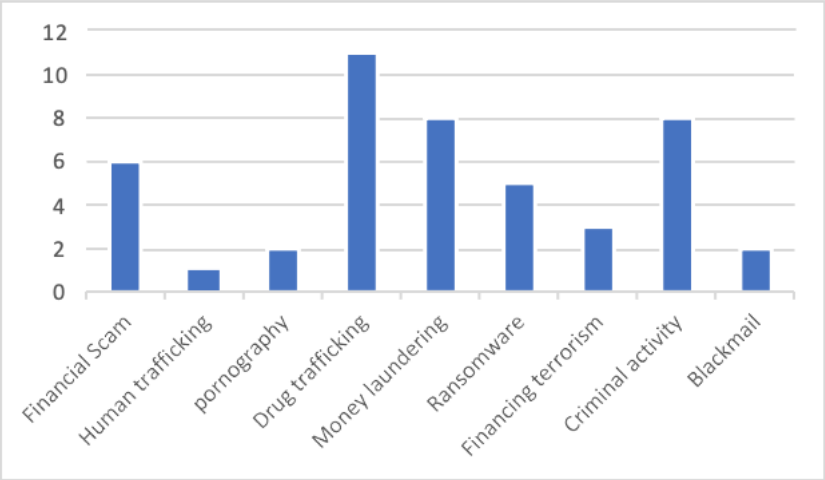

Figure 5: Bitcoin related illicit activities

A. Financial Scam

Crypto scams have moved to the skies during COVID-19 [7] [8]. It is said that between 2020 and 2021, Americans lost $80 million in financial scams (cryptocurrency fraud schemes), and the Federal Trade Commission (FTC) received over 7,000 complaints from customers related to financial scams in crypto investment [10-11].

B. Human Trafficking

The dark web is primarily a marketplace where users use covert websites to offer services related to human trafficking, such as the trafficking of organs and sex [32]. The US Department of State [12] reports that there were 118,932 victims of human trafficking in 2019. It has also been discovered that most traffickers jump between accounts and sites on the dark web to elude law enforcement monitoring.

C. Pornography

It has been discovered that the use of cryptocurrencies, such as bitcoin, to pay for commercial pornography [7][12], abuse, and/or exploitation of goods and/or services [33].

D. Drug Trafficking

Through the use of cryptocurrencies like Bitcoin and Ethereum, drug traffickers and users may buy and sell narcotics on the dark web [34] [32]. The United States (DEA, FBI, and IRS), the United Kingdom (National Crime Agency), Germany, Denmark, Moldova, Australia, and Ukraine work together to shut down the biggest drug black market on the Internet, according to research released by Europol in January 2021 [35]. Furthermore, around 4,650 Bitcoins.

E. Money Laundering

One of the biggest obstacles to maintaining a functional financial system is money laundering [12][22][25]. The process of hiding the source of illegal funds, such as revenues from crime, through a convoluted web of transactions, including cryptocurrency transactions, is known as money laundering. The majority of scholars currently hold the view that money laundering is the world's most lucrative kind of criminal activity [4]. According to expert estimates, every year, between $150 billion and $500 billion obtained through illicit means are transferred into legitimate financial circulation worldwide.

F. Ransomware

Ransomware is a type of virus, or malicious software [7] [11], that threatens users by preventing access to important data until a bitcoin ransom is paid [36]. Cryptocurrencies have reportedly been used as payment in kidnappings [37]. 2020 saw the discovery of 304 million ransomware infections globally, a 62% increase over 2019 and the second-highest number since 2016. Law enforcement and public safety are now seriously threatened because of the massive ransom.

G. Financing Terrorism

Cryptocurrencies are sometimes accused of being a great tool for terrorists. Because Bitcoin and other alternative currencies are fully anonymous [8][27][28], they are very difficult to track down[48][49]. However, whether they are ideal for funding terrorists is debatable. The extant literature examines many sources of financing. It emphasizes, in particular, that terrorists depend on both legal and criminal financial sources. Stock market and real estate investments, as well as salary, are examples of legal sources. Robbery, theft, kidnappings, and drug trafficking are common methods of obtaining illegal funds.

H. Criminal Activity

You may hire a hitman to kill someone else on a number of underground websites [9]. For instance, in May 2016, a White-hat hacker going by the handle "bRpsd" is said to have helped the FBI capture many hitmen by breaking into the "Besa Mafia" website on the dark web and revealing confidential data, including user accounts and correspondence with clients [29][30]. Hitmen and clients were linked via this clandestine website, with the price of a murder job purportedly ranging from $5,000 to $200,000 USD.

V. HOW CRYPTOCURRENCY (BITCOIN) IS USED FOR ILLICIT ACTIONS AND WHAT ARE THE SUPPORTING FACTORS

Cryptocurrencies represent a decentralized form of currency [8]. Bitcoin, the pioneering digital cryptocurrency introduced by Satoshi Nakamoto, operates on blockchain technology, employing cryptographic algorithms and peer-to-peer networks without central oversight [3]. Transactions on the Bitcoin network are validated by a network of peer-to-peer nodes based on trust. To anonymize a user's identity, transactions are completed using a hashed value of the public key generated through digital signature techniques [1]. This allows payment transactions to occur on the Bitcoin network without revealing the identities of the involved parties.

Cryptocurrencies have increasingly become associated with facilitating illicit activities [7]. As cryptocurrencies gain acceptance, they are utilized for online transactions involving unlawful goods such as drugs and human trafficking, contributing to the rise in criminal activities [11]. Among cryptocurrencies, Bitcoin is particularly prevalent in the cybercriminal realm, especially on the dark web, where large volumes of Bitcoins are exchanged [29]. Reports suggest that a significant portion of Bitcoin users and transactions are linked to illegal conduct, with estimates indicating approximately US$72 billion of criminal activity annually, comparable to the scale of illegal drug markets in the United States and Europe [51] [38]. Current prominent forms of cryptocurrency-related crime include blackmail, financial schemes such as sextortion, money laundering, and ransomware attacks [39] [40].

Bitcoin has provided opportunities for criminals to defraud numerous individuals through various schemes, including Ponzi schemes, drug trafficking, and money laundering. Instances of Ponzi schemes involving cryptocurrency have garnered attention from law enforcement agencies worldwide. For example, the creator of Bitcoin Savings and Trust was accused of defrauding investors of over $7 million worth of Bitcoin through a Ponzi scheme[52] [11]. Similarly, an Indian bitcoin expert was arrested for orchestrating a Ponzi scheme valued at nearly $300 billion [41]. The Silk Road, an illicit online marketplace that exclusively accepted Bitcoin transactions, was a significant operation in the realm of illegal activities [42]. Following its takedown by the Federal Bureau of Investigation (FBI), it was reported that the creator had facilitated approximately US$1 billion in illicit transactions within a brief period. Platforms like AlphaBay and Hansa, two of the largest dark web markets, utilized Bitcoin for transactions involving a wide range of illegal goods and services, including narcotics, hacking tools, human trafficking, and fraudulent services [29]. Furthermore, counterterrorism experts express concerns about the widespread use of cryptocurrencies due to their global accessibility, decentralization, transaction speed, and perceived lack of regulation [43] [44]. Cryptocurrencies have the potential to facilitate money laundering techniques, such as through online gambling and e-commerce transactions [45]. In May 2017, a wave of crypto ransomware attacks targeted hospitals, schools, and businesses across more than one hundred countries, including Spain, Russia, and the United Kingdom, demanding Bitcoin as a ransom [11].

The space transition approach [29] was utilized to examine criminal incidents associated with Bitcoin, identifying components conducive to illicit operations such as drug trafficking, extortion, Ponzi schemes, and money laundering. Factors such as "identity flexibility," "dissociative anonymity," and a perceived lack of deterrence were found to facilitate illicit activities involving Bitcoin. Additionally, the data indicates that perpetrators often met their accomplices in physical locations and executed their crimes in the digital realm, and vice versa, supporting the validity of the space transition theory. It's noteworthy that not all cryptocurrency-related crimes occur exclusively online; for instance, cases involving human trafficking and tax evasion may utilize Bitcoin earnings.

VI. WHAT ARE THE INNOVATIVE STRATEGIES THE RESEARCH COMMUNITY HAS PROPOSED TO DETECT ILLICIT USE CARRIED OUT WITH BITCOIN

By using Bitcoin's anonymous mechanism, cryptocurrencies have emerged into a shelter for criminal activity (e.g., terrorism, drug smuggling, or human trafficking, ransomware, Money laundering)[52]. Every year, criminals launder billions of funds obtained through significant crimes, causing millions of people and economies to suffer. Because of Bitcoin's anonymous structure, ransomware operations seeking ransom in bitcoins and drug monitoring payments are also conducted in Bitcoin. Because cryptocurrency may be used to fund terrorists. As a result, it is critical to address this problem and identify money laundering, payment for drug trafficking, and Ponzi schemes. Table 3 list the publications addressing (detect) the illicit use (detect) of cryptocurrency (bitcoin) and or designing a platform to create a system to ensure the product's end-to-end traceability to address illicit drug issues.

Several studies in the literature mentioned various methods to identify illegal activity related to cryptocurrency. Machine Learning, according to researchers [53][22] may be used to detect these illegal actions. Research offers [8] Adaptive Stacked eXtreme Gradient Boosting (ASXGB), an adaption of eXtreme Gradient Boosting (XGBoost), to identify criminal activity (e.g., scams, terrorist funding, and Ponzi schemes) on cryptocurrency infrastructures, both at the account and transaction levels. Furthermore, cryptocurrency might be seen as a risk because it may be used to purchase

guns or explosives on the dark web. To mitigate this risk, governments should pass legislation allowing for covert remote web searches of digital devices. This might aid in the detection of e-wallets used to fund terrorists.

Furthermore, due to the enormous number of transactions and the data format of bitcoins, it is very difficult to identify money laundering activities. Many strategies for detecting money laundering in the traditional banking system have been presented in various studies. In one study [24], researchers presented a framework for converting Bitcoin's international data into a data frame comparable to that of a bank's user database, which is utilized by certain current state-of-the-art intelligent systems to identify abnormal clusters of transactions and user activity[54]. As a result, resolving this issue may immediately decrease crime and terrorist activity. Another research [26] focused on ransomware and conducted a large-scale investigation of Bitcoin ransom payments, transfers, and victim migrations. The findings of this study may assist authorities in better understanding ransomware operations in Bitcoin.

Over the last several years, there has been a considerable increase in the number of pharmaceutical drug frauds, resulting in the poisoning of thousands of patients, untreated diseases, and early deaths. Detecting counterfeit drugs is a difficult task that poses a risk to the healthcare system. Unfortunately, the healthcare system and government lack proper audibility and transparency of drug origin. The consequences include fake drugs and a loss of trust. According to the findings, pharmaceutical companies may use blockchain to comply with future track-and-trace laws in the pharmaceutical business[55]. It may also help to decrease counterfeiting and corruption in the pharmaceutical supply chain. Many academics have used Blockchain and presented various remedies to the long-standing counterfeit medication problem. Initially, a study proposal [14] was presented along with a prototype of Blockchain-based medicine traceability from production to pharmacies. Following its execution, the prototype demonstrated its usefulness. In addition, another study [16] uses Ethereum blockchain decentralized off-chain storage to enable efficient medicine tracking from doctor's prescription to patient consumption. Furthermore, smart contracts protect data provenance and give all parties a secure and immutable transaction history. Another researcher [18] used IoT devices to monitor and trace medicines. As a result, the system has investigated blockchain for the security of IoT devices and the elimination of counterfeiting. In India, researchers [19] used blockchain to permanently eliminate the counterfeit medication issue by strengthening the supply chain. It will increase transaction transparency by tracing a medicine from the extraction of raw ingredients to the patient using the drug.

VII. CONCLUSION

Bitcoin is the first public Blockchain application, and it captured the highest market capitalization. Bitcoin is used in a wide range of illicit activities because of its pseudonymous mechanism. This study (SLR) is focused on the illegal use of Bitcoin in various applications. The authors managed to consolidate 45 articles from major computer science databases on illicit usage of cryptocurrency (Bitcoin). The analysis of these articles revealed that Bitcoin is used to make payments for human trafficking, pornography, drug trafficking, and ransomware on the dark web. Moreover, drug trafficking is the most discussed illicit activity in literature, followed by money laundering and ransomware. The identity flexibility, dissociative anonymity, and a lack of deterrence encourage users to perform illegal activities using Bitcoin. The finding also revealed that researchers around the world have proposed innovative strategies to counter unlawful acts carried out with Bitcoin. However, there is no state of art solution so far. As a result, there is an urgent need for cutting-edge solutions to combat the illicit use of bitcoin.

Table 3: List of publications and techniques to detect illicit activities

	Year	Country	Citation	Technique
1	**2021**	**Taiwan**	**[31]**	**A blockchain-based architecture improves transparency and custody of digital evidence during criminal investigations.**
2	**2022**	**France**	**[14]**	**An architecture based on blockchain " ChainDrugTrac", for the tracing and detection of counterfeit medical products.**
3	**2021**	**Tunisi a**	**[16]**	**This is an end-to-end (patients- doctor's prescription) product tracking system for the drug to ensure product safety and eliminate counterfeits**
4	**2019**	**India**	**[19]**	**Blockchain technology tracks medicine transactions from raw ingredients to the patient, ensuring quality assurance.**
5	**2020**	**Feedzai**	**[22]**	**Unsupervised anomaly detection techniques fall short of identifying the illegal patterns present in an actual dataset of Bitcoin transaction data.**
6	**2019**	**India**	**[24]**	**A framework for converting Bitcoin data into bank databases and using it on intelligent systems to detect anomalous clusters of transactions.**
07	**2020**	**USA**	**[4]**	**Our investigation indicated that most Bitcoin laundering services do not involve law enforcement.**
08	**2022**	**China**	**[26]**	**An analysis of Bitcoin victims' movements, ransom transfers, and payments. This survey found that most ransomware perpetrators prefer to distribute the ransom across many firms instead of utilizing Bitcoin mixers for payment.**

VIII. FUTURE RESEARCH DIRECTION

Future research on Bitcoin and illicit activities should focus on designing better methods to detect and track suspicious transactions, studying the effectiveness of current regulations in stopping illegal uses, and using machine learning to find and predict patterns of illegal activity. Additionally, examining how decentralized exchanges affect the traceability of Bitcoin and exploring ways for international law enforcement to collaborate in combating Bitcoin-related crimes are crucial areas of study.

CONFLICT OF INTEREST

There is no conflict of interest between all the authors

REFERENCES

[1] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," Applied Sciences, vol. 11, no. 20, p. 9372, 2021.

[2] D. Shift, "Technology tipping points and societal impact," in World Economic Forum Survey Report, available at: http://www3. weforum. org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015. pdf (last accessed 20.08. 2018), 2015.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.

[4] J. Crawford and Y. Guan, "Knowing your bitcoin customer: Money laundering in the bitcoin economy," in 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE), 2020: IEEE, pp. 38-45.
[5] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical report, ver. 2.3 ebse technical report. ebse, 2007.
[6] M. Das, X. Tao, and J. C. Cheng, "BIM security: A critical review and recommendations using encryption strategy and blockchain," Automation in construction, vol. 126, p. 103682, 2021.
[7] J. Choi et al., "A Large-Scale Bitcoin Abuse Measurement and Clustering Analysis Utilizing Public Reports," IEICE TRANSACTIONS on Information and Systems, vol. 105, no. 7, pp. 1296-1307, 2022.
[8] D. Vassallo, V. Vella, and J. Ellul, "Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies," SN COMPUT. SCI., vol. 2, no. 3, pp. 1-15, 2021.
[9] C.-L. Chen et al., "An Anti-Counterfeit and Traceable Management System for Brand Clothing with Hyperledger Fabric Framework," Symmetry, vol. 13, no. 11, p. 2048, 2021.
[10] F. Cozzi, "Will blockchain technologies strengthen or undermine the effectiveness of global trade control regulations and financial sanctions?," Global Jurist, vol. 20, no. 2, 2020.
[11] S. Kethineni and Y. Cao, "The rise in popularity of cryptocurrency and associated criminal activity,"
[12] Int. Crim. Justice Rev., vol. 30, no. 3, pp. 325-344, 2020.
[13] M. Taleby Ahvanooey, M. X. Zhu, W. Mazurczyk, M. Kilger, and K.-K. R. Choo, "Do Dark Web and Cryp tocurrencies Empower Cybercriminals?," in International Conference on Digital Forensics and Cyber Crime, 2022: Springer, pp. 277-293.
[14] L. Almaqableh et al., "Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can," Int J Inf Manage, p. 102488, 2022.
[15] E. K. Kambilo, H. B. Zghal, C. G. Guegan, V. Stankovski, P. Kochovski, and D. Vodislav, "A blockchain-based framework for drug traceability: ChainDrugTrac," in Proceedings of the 37th ACM/SIGAPP Sympo sium on Applied Computing, 2022, pp. 1900-1907.
[16] K. Moeller, R. Munksgaard, and J. Demant, "Illicit drug prices and quantity discounts: A comparison be tween a cryptomarket, social media, and police data," Int. J. Drug Policy, vol. 91, p. 102969, 2021.
[17] R. Mars, J. Youssouf, S. Cheikhrouhou, and M. Turki, "Towards a Blockchain-based approach to fight drugs counterfeit," in TACC, 2021, pp. 197-208.
[18] N. Saxena, I. Thomas, P. Gope, P. Burnap, and N. Kumar, "Pharmacrypt: Blockchain for critical pharma ceutical industry to counterfeit drugs," Computer, vol. 53, no. 7, pp. 29-44, 2020.
[19] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, and P. Lund, "Blockchain: A solution for improved traceability with reduced counterfeits in supply chain of drugs," in 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS), 2020: IEEE, pp. 1-5.
[20] A. Kumar, D. Choudhary, M. S. Raju, D. K. Chaudhary, and R. K. Sagar, "Combating counterfeit drugs: A quantitative analysis on cracking down the fake drug industry by using blockchain technology," in 2019 9th international conference on cloud computing, data science & engineering (Confluence), 2019: IEEE, pp. 174-178.
[21] A. Mikhaylov and R. Frank, "Illicit payments for illicit goods: noncontact drug distribution on Russian online drug marketplaces," Global Crime, vol. 19, no. 2, pp. 146-170, 2018.
[22] J. Demant, R. Munksgaard, D. Décary-Hétu, and J. Aldridge, "Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime," Int. Crim. Justice Rev., vol. 28, no. 3, pp. 255-274, 2018.
[23] J. Lorenz, M. I. Silva, D. Aparício, J. T. Ascensão, and P. Bizarro, "Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity," in Proceedings of the First ACM International Conference on AI in Finance, 2020, pp. 1-8.
[24] R. Barone and D. Masciandaro, "Cryptocurrency or usury? Crime and alternative money laundering tech niques," Eur. J. Law Econ., vol. 47, no. 2, pp. 233-254, 2019.

[25] S. Samanta, B. K. Mohanta, S. P. Pati, and D. Jena, "A framework to build user profile on cryptocurrency data for detection of money laundering activities," in 2019 International Conference on Information Tech nology (ICIT), 2019: IEEE, pp. 425-429.
[26] J. R. Hendrickson and W. J. Luther, "Cash, crime, and cryptocurrencies," The Quarterly Review of Econom ics and Finance, vol. 85, pp. 200-207, 2022.
[27] K. Wang et al., "A large-scale empirical analysis of ransomware activities in bitcoin," ACM Transactions on the Web (TWEB), vol. 16, no. 2, pp. 1-29, 2021.
[28] H. Lee and K.-S. Choi, "Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework," Victims & Offenders, vol. 16, no. 3, pp. 363-384, 2021.
[29] F. M. J. Teichmann, "Financing terrorism through cryptocurrencies–a danger for Europe?," J. Money Laund. Control, 2018.
[30] S. Kethineni, Y. Cao, and C. Dodge, "Use of bitcoin in darknet markets: Examining facilitative factors on Bitcoin-related crimes," Am. J. Crim. Justice, vol. 43, no. 2, pp. 141-157, 2018.
[31] S. K. Taylor, A. Ariffin, K. A. Z. Ariffin, and S. N. H. S. Abdullah, "Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets," in 2021 3rd International Cyber Resilience Conference (CRC), 2021: IEEE, pp. 1-5.
[32] F.-C. Tsai, "The Application of Blockchain of Custody in Criminal Investigation Process," Procedia Com puter Science, vol. 192, pp. 2779-2788, 2021.
[33] S. Kaur and S. Randhawa, "Dark web: a web of crimes," Wireless Personal Communications, vol. 112, no. 4, pp. 2131-2158, 2020.
[34] B. R. da Cunha, P. MacCarron, J. F. Passold, L. W. dos Santos, K. A. Oliveira, and J. P. Gleeson, "Assessing police topological efficiency in a major sting operation on the dark web," Scientific reports, vol. 10, no. 1, pp. 1-10, 2020.
[35] A. ElBahrawy, L. Alessandretti, L. Rusnac, D. Goldsmith, A. Teytelboym, and A. Baronchelli, "Collective dynamics of dark web marketplaces," Scientific reports, vol. 10, no. 1, pp. 1-8, 2020.
[36] M. T. Ahvanooey, M. X. Zhu, W. Mazurczyk, M. Kilger, and K.-K. R. Choo, "Do Dark Web and Crypto currencies Empower Cybercriminals," in 12th EAI International Conference on Digital Forensics & Cyber Crime (EAI ICDF2C 2021), Singapore, 2021.
[37] W. Feng, Y. Wang, and Z. Zhang, "Can cryptocurrencies be a safe haven: a tail risk perspective analysis," Applied Economics, vol. 50, no. 44, pp. 4745-4762, 2018.
[38] C.-R. Attacks, "The New Form of Kidnapping (2015)," URl: https://blog. trendmicro. com/crypto- ransom ware-attacks-thenew-form-of-kidnapping.
[39] S. Foley, J. R. Karlsen, and T. J. Putniņš, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?," The Review of Financial Studies, vol. 32, no. 5, pp. 1798- 1853, 2019.
[40] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, "Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem," in Proceedings of the 1st ACM conference on advances in financial technologies, 2019, pp. 76-88.
[41] P. Xia et al., "Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams," in 2020 APWG Symposium on Electronic Crime Research (eCrime), 2020: IEEE, pp. 1-14.
[42] K. Bangera, "Mastermind of a bitcoin [BTC] Ponzi scheme worth over $300 Billion arrested in India. 2018. Retrieved April 6, 2018," ed, 2018.
[43] S. Okyere-Agyei, "The dark Web–A Review," 2022.
[44] A. Brill and L. Keene, "Cryptocurrencies: The next generation of terrorist financing?," Defence against ter rorism review, vol. 6, no. 1, pp. 7-30, 2014.
[45] D. Takedown, "Authorities Shutter Online Criminal Market AlphaBay," ed, 2017.
[46] V. C. W. Group, "Regulating virtual currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering," ed: Ministere des finances et des comptespublics.[In ternet] Raspoloživo na: http …, 2014.

[47] Slattery, T. (2014). Taking a bit out of crime: Bitcoin and cross-border tax evasion. Brook. J. Int'l L., 39, 829.

[48] Wootton, A. R., Drabble, L. A., Riggle, E. D., Veldhuis, C. B., Bitcon, C., Trocki, K. F., & Hughes, T. L. (2019). Impacts of marriage legalization on the experiences of sexual minority women in work and commu nity contexts. Journal of GLBT Family Studies, 15(3), 211-234.

[49] Wootton, A. R., Drabble, L. A., Riggle, E. D., Veldhuis, C. B., Bitcon, C., Trocki, K. F., & Hughes, T. L. (2019). Impacts of marriage legalization on the experiences of sexual minority women in work and commu nity contexts. Journal of GLBT Family Studies, 15(3), 211-234.

[50] Tundis, A., Nemalikanti, S., & Mühlhäuser, M. (2021, August). Fighting organized crime by automatically detecting money laundering-related financial transactions. In Proceedings of the 16th International Confer ence on Availability, Reliability and Security (pp. 1-10).

[51] Ali, M. (2024). The Application of General and Criminal Confiscation Laws in Bankruptcy Cases in Indo nesia and Australia. Pakistan Journal of Criminology, 16(2).

[52] Khan, D., Jung, L. T., Hashmani, M. A., & Waqas, A. (2020, January). A critical review of blockchain consensus model. In 2020 3rd international conference on computing, mathematics and engineering technol ogies (iCoMET) (pp. 1-6). IEEE.

[53] Khan, D., Jung, L. T., Hashmani, M. A., & Cheong, M. K. (2022). Empirical performance analysis of hy perledger LTS for small and medium enterprises. Sensors, 22(3), 915.

[54] Khan, D., Memon, M. M., Hashmani, M. A., Simpao, F. T., Sales, A. C., & Santillan, N. Q. (2023). A Critical Review on Blockchain Frameworks for Dapp. International Journal of Technology Management and Infor mation System, 5(1), 1-10.

[55] Memon, M. M., Hashmani, M. A., Simpao, F. T., Sales, A. C., Santillan, N. Q., & Khan, D. (2023). Block chain in Healthcare: A Comprehensive Survey of Implementations and a Secure Model Proposal. Proceed ings of the Pakistan Academy of Sciences: A. Physical and Computational Sciences, 60(3), 1-13.