THE NEW MONEY LAUNDERING MACHINE THROUGH CRYPTOCURRENCY: CURRENT AND FUTURE PUBLIC GOVERNANCE CHALLENGES

Llambi Prendi [*], Daniel Borakaj [**], Klarida Prendi [**]

* *Corresponding author*, University Aleksandër Moisiu of Durrës, Durrës, Albania
Contact details: University Aleksandër Moisiu of Durrës, Lagjia 1, Rr. Currilave, 2001 Durrës, Albania
** University Aleksandër Moisiu of Durrës, Durrës, Albania

OPEN ACCESS

How to cite this paper: Prendi, L., Borakaj, D., & Prendi, K. (2023). The new money laundering machine through cryptocurrency: Current and future public governance challenges. *Corporate Law & Governance Review, 5*(2), 84–91.
https://doi.org/10.22495/clgrv5i2p9

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 17.02.2023
Accepted: 25.08.2023

JEL Classification: G3, G28, K24, M4
DOI: 10.22495/clgrv5i2p9

Abstract

The purpose of this paper is to examine the role of cryptocurrency in facilitating money laundering and identify different methods and services that send funds through numerous addresses or businesses to obscure their origins using cryptocurrency. The methodology for conducting this research is qualitative. A literature review that involves a systematic and rigorous approach to identifying, analyzing, and synthesizing existing research on the use of cryptocurrency as a money laundering instrument has been taken into consideration. We identified in the first selection more than 150 research papers published between 2002 and 2021. Our results show that cryptocurrency is used in money laundering schemes, including the purchase of cryptocurrencies by criminal networks using illicit proceeds and the use of cryptocurrencies to transfer funds. The biggest issue facing virtual currency currently is that the same attributes that attract legitimate users, such as anonymity, as well as speed and global reach, also attract criminals. Money laundering has had devastating social implications for societies. Our research helps to focus attention on the problems of using cryptocurrency in money laundering practices and possible interventions by the authorities in the form of regulation.

Keywords: Blockchain Technology, Cryptocurrency, Financial Crimes, Governance Challenges, Virtual Currency

Authors' individual contribution: Conceptualization — L.P. and K.P.; Methodology — K.P.; Formal Analysis — L.P. and K.P.; Investigation — L.P., D.B., and K.P.; Resources — L.P.; Writing — Original Draft — L.P.; Writing — Review & Editing — L.P., D.B., and K.P.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

A cryptocurrency is a digital or virtual currency that is used as an alternative to traditional money and is safe because it uses encryption technologies, which makes it impossible to double-spend (Frankenfield, 2023a). Cryptocurrencies do, however, come with a number of hazards and difficulties. Cryptocurrencies, for instance, can have a very variable value, making them a risky investment (Europol, 2021a).

Frankenfield (2023a), explain that not all e-commerce sites accept cryptocurrency payments, even though many cryptocurrencies are decentralized networks built on blockchain technology and may be mined or bought from exchanges. Around 2,000 cryptocurrencies are currently available on the market, allowing users to send virtual money worldwide in exchange for products, services, and other types of value (U.S. Department of Justice, 2020).

The most commonly used and valuable cryptocurrency is bitcoin. Bitcoin was created in 2008 by Satoshi Nakamoto with the publication of an article titled "Bitcoin: A Peer-to-Peer Electronic Cash System". The name Satoshi Nakamoto is an alias and the identity of the person or persons behind this invention is currently unknown.

Bitcoin is a virtual currency created to be used as money. Money is defined as any item or medium of exchange that is centralized, widely accepted, and recognized, and that facilitates the exchange of goods and services. Like money, bitcoin can be defined as a medium of exchange, as a payment method for goods and services, and as a payment method for the services of labor and other factors. This electronic money is not generally acceptable because it is not decreed money but is a form of payment outside the control of any one person or institution.

Peer-to-peer technology enables bitcoin to function without a central authority or banks; the network as a whole handles transaction management and the issuance of bitcoins[1].

Bitcoin has changed the way of thinking about money because the limited amount of this currency makes it a currency that offers the security of purchasing power, perhaps more secure than traditional money itself (Frankenfield, 2023b).

Other 9 popular cryptocurrency that has large market capitalization are ethereum, tether, BNB, USD coin (USDC), XRP, Binance USD (BUSD), cardano, dogecoin, and polygot.

The market capitalization may fluctuate over time due to the number of shares outstanding. This is especially true in cryptocurrency, where new tokens or coins are issued or minted regularly (Fernando, 2023). Bitcoin has a market capitalization of $442,254,419,953 which is 24 times higher than the gross domestic product (GDP) of Albania (GDP = 18.26 billion) or almost equal to the GDP of Nigeria (GDP = 440,833.58 billion) (The World Bank, n.d.-a, n.d.-b). This market capitalization created by these virtual currencies constitutes a very large monetary value which also attracts criminal groups to exercise their illegal activity. One common type of criminal activity associated with e-money is fraud. Criminals may use stolen identities or credit card information to make fraudulent purchases or money transfers. In addition, criminals may use e-money platforms to launder money or finance illicit activities, such as terrorism or drug trafficking (Brito, 2013). The usage of virtual currencies in money laundering operations has increased, and many organized criminals relied on them as a typical payment during the COVID-19 pandemic (Europol, 2021a). Governments and banking organizations have taken a number of actions to combat e-money-related criminal activities. These steps could include anti-money laundering (AML) regulations, which attempt to stop money laundering and the financing of terrorism, as well as Know Your Customer (KYC) standards, which force financial firms to confirm the identity of their clients (Douma, 2016).

Anti-money laundering (AML) refers to a set of regulations and procedures designed to prevent the use of financial systems for money laundering or terrorist financing (Custers et al., 2020).

The purpose of this article is to identify various methods that use cryptocurrency to send funds through multiple addresses or businesses to conceal their origins. We will verify that cryptocurrency is used in money laundering schemes in a variety of ways, including the purchase of cryptocurrencies by criminal networks using illicit proceeds and the use of cryptocurrencies to transfer funds. We will investigate the possible interventions by the authorities in the form of regulation. Mostly we will focus on bitcoin.

The findings of the studies show us that virtual currencies are involved in criminal activities, based on this the development of a legal framework for cryptocurrencies is suggested. The methodology of this work is qualitative and we will try to answer the following questions:

RQ1: What are the methods of cryptocurrency money laundering?

RQ2: What are dark web marketplaces?

RQ3: What are the features that facilitate the use of bitcoin in money laundering mechanisms?

RQ4: Is further bitcoin regulation necessary?

The rest of this paper is structured as follows. Section 2 reviews the relevant literature. Section 3 analyses the methodology that has been used to conduct empirical research. Section 4 analyses the results, we will deal with some cases involving the use of cryptocurrency in illegal activities such as money laundering, fraud, drug trafficking, etc. Section 5 concludes the paper.

2. LITERATURE REVIEW

Revenue in the cryptocurrencies segment has reached around US$42 billion in 2023 and is expected to show an annual growth rate of 14.36% by 2027. User penetration will be 3.8% in 2023 and is expected to hit 4.4% by 2027 (Statista, n.d.).

Bitcoin was the first decentralized virtual currency to emerge in 2009. While previous virtual currencies used centralized entities as intermediaries, this new currency gained popularity due to the absence of third parties in transactions (Europol, 2021b).

Since then, cryptocurrencies have grown in popularity as a means of payment, investment, and fund transfer. The problem with these electronic currencies was that they were not regulated by laws. Law enforcement was not prepared for this type of economy created by cryptocurrency. Criminal groups, seeing these currencies as an advantage against them, began to use these currencies on the dark web as part of fraud and extortion schemes (Europol, 2021a) to use for their benefit, criminal groups use this service to exchange these electronic currencies in fiat currency, real currency, or national currency. The degree of anonymity of cryptocurrencies can vary depending on whether their associated blockchain is public or private. A public ledger that records the history of all verified transactions also prevents double-spending and counterfeiting by cryptographically recording each transaction. Transactions in non-public or private blockchains are more difficult to trace or attribute (U.S. Department of Justice, 2020).

According to the U.S. Department of Justice (2020), different authors have expressed opinions for/against the use of cryptocurrency. Cryptocurrency has the potential to minimize transactions, reduce

[1] https://bitcoin.org/en/

corruption and fraud, avoid inflation in fiat currencies, and in the future facilitate "micro-payments", providing enterprises with the opportunity to sell low-cost goods and services and creating new access to markets. Cryptocurrency can also limit national governments' ability to regulate their economies through monetary policy, they are not secure to invest, engage in financial transactions related to criminal activity, take part in money laundering, or shield otherwise legitimate activity from tax, reporting, or try and hide legal activity from tax, reporting, as well as other legal requirements, and commit crimes directly involving the cryptocurrency marketplace its own, such as snatching cryptocurrency from exchanges.

Money laundering is the process of concealing the source of criminal proceeds to use them to carry out legal or illegal activities later on.

When an illegal action creates significant profits, the individual or group engaged must find a means to spend money without bringing attention to the primary activity or the individuals involved in creating such earnings. Criminals achieve this by hiding sources, changing the form, or moving the money to an inconspicuous location. For that reason, money laundering is frequently a derivative process that is preceded by illegal activity (Wells, 2013).

Steps taken to launder money are not, in themselves, illegal. But since money laundering requires that the wealth itself be derived from crime, exposing money laundering activities is essential to the fight against these crimes themselves. Money laundering is considered the lubricant of the crime machine, affecting and harming today's societies.

Empirical research in the field of accounting and finance was conducted by Guidara (2022). This paper identifies the importance of developing the legal framework for digital currencies as well as the importance of market actors to reduce the risk of money laundering. According to Guidara (2022), banks play a very important role in reducing money laundering.

The use of cryptocurrency in criminal activities, although it does not occupy a significant weight in the economy of these activities, has become a concern due to its significant growth in recent years (Europol, 2021b). The use of cryptocurrency by criminal groups let us understand that these groups are becoming very sophisticated and difficult to identify. Large money laundering networks have precisely adopted electronic money and are offering these criminal groups their services (Statista, n.d.). The degree of use of cryptocurrency in criminal activities is difficult to identify.

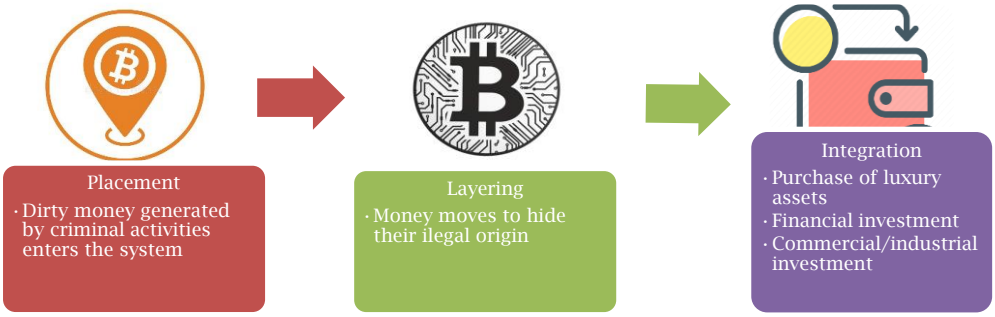
There are three phases of money laundering:

1) *Placement:* At this stage, dirty money generated by criminal activities enters the system. Money can enter the system through casinos, banks, restaurants, supermarkets, taxi companies, etc. According to Forgang (2019), placing large amounts of illicit cash into the financial system for the first time is the riskiest stage of money laundering for the money launderer. Such high risk makes the unique attributes of the crypto economy more attractive.

2) *Layering:* It is the stage where money moves to hide its illegal origin. Some of the many methods of layering are electronic fund transfers to/from offshore bank accounts, or between countries. The crypto economy offers money launderers new opportunities for layering. One common method of layering involving cryptocurrencies is "chain hopping". Chain hopping can obfuscate the origins of a transaction and make it near impossible to track (Cochrane, 2020).

3) *Integration:* When the above stages are passed, the money is considered clean. So when this money reaches the third stage, it is impossible to distinguish whether the money is legal or not.

Figure 1. Money laundering stages (placement, layering, and integration)



Lots of authors have the same results, to prevent money laundering through cryptocurrencies, governments must take measures by sensitizing the population through education and the creation of laws to regulate this market.

Sicignano (2021) attempted to analyze the relationship between bitcoin and money laundering in Italian law in his paper. He explains that virtual money would be a Trojan horse rather than a tool for criminals and money launderers. Money launderers who invest a significant amount of money in bitcoin risk being caught.

Weber et al. (2019) have made a study about the legal and illegal activities that can be carried out through bitcoin. They used a very wide database to classify these transactions.

According to Hillman (2020), with the use of cryptocurrencies, transactions of any size can be completed quickly and without the involvement of a central government or financial institutions. The increased number of corruption issues including cryptocurrencies, this global phenomenon cannot be ignored and anti-corruption measures should be taken. The players are choosing to use the new

technology for illegal activities. Numerous instances of corrupt behavior involving cryptocurrencies have been documented, including fraud, market manipulation, exchange theft, ransomware attacks, black market deals, and financing for terrorism. For those looking to avoid paying taxes, which for a long time profited from a lack of effective tax regulation, cryptocurrencies have also become very popular.

According to United Nations (n.d.), money laundering using cryptocurrency creates a large money laundering scheme with thousands of transfers at a low cost and executes it using a computer script. Two types of technologies related to cryptocurrencies can be used for money laundering: 1) privacy coins, cryptocurrencies that offer a higher level of anonymous blockchain transactions, and 2) mixer, a service that transfers coins while making the connection between the source and destination of the fund impossible to trace. As a result, it is almost impossible to connect the funds to their source.

3. RESEARCH METHODOLOGY

The objective is to investigate the possibility of using cryptocurrency in money laundering practices and possible interventions by the authorities in the form of regulation.

Two methods were used for conducting the literature review in this paper.

Systematic review: A systematic review comprises an in-depth investigation of the body of prior research using predetermined search criteria. Usually, several databases are searched in the search process. The studies are subsequently evaluated and chosen depending on how well they address the study issue.

Narrative review: A narrative review uses a less formal method to summarize the body of literature. Less attention is placed on the methodical search and selection of studies and more emphasis is placed on giving a thorough overview of the available research on the subject (Grant & Booth, 2009).

This paper develops these methods for conducting a comprehensive and systematic literature review as well as qualitative interpretation. First, from 2002 to 2021, the authors retrieved lots of relevant scientific publications in English on the topic. We have studied publications from several sources like Scopus which contain the most relevant and high-impact publications, Web of Science databases which is a larger database of indexed publications that includes high-impact conference proceedings, and other sources. Therefore, the database combination provides a comprehensive overview of scientific developments in the field. We will conclude by gathering facts from diverse sources and debating the outcomes of various approaches to the use of cryptocurrency as a money laundering instrument.

A total of 150 publications were gathered and checked for duplicates, yielding a preliminary selection of 100 papers. The authors then refined the initial selection by manually screening titles and abstracts for compliance with the main topic of the use of cryptocurrency in money laundering. The compliance check consisted of four sequential closed-ended questions:

1) *Is the publication about cryptocurrency?*

2) *Is the role of cryptocurrency significant in the publication?*

3) *Is the publication about the use of cryptocurrency in money laundering and other criminal activities?*

4) *Is the publication about the regulations in the cryptocurrency market?*

If the answer to any question was "no", the publication was excluded from the final selection. Conversely, all the publications included in the final selection answered "yes" to all four questions. After the content compliance check, the final selection consisted of 35 publications.

Following that, we quantitatively evaluated the metadata of the final selection of publications. The number of publications, type (journal or conference paper), and year published, the total number of citations, first-author country of affiliation, and keywords were all examined. The analyses aimed to identify general trends related to the publications on the use of cryptocurrency in money laundering in the last 20 years. Then, we developed a qualitative content analysis of the final selection based on the abstracts and full-text reading when needed to categorize the publications into distinct primary and secondary content groups and approach types. The qualitative content assessment aimed to expose the main subjects already covered by the literature, the density of knowledge in each category or subcategory, and its most relevant existing knowledge gaps.

The findings of the studies that were reviewed emphasized the importance of developing a legal framework for cryptocurrency. This paper consults the original reports published by the European Central Bank and other sources such as articles and books written by economists, journalists, and various universities. Cryptocurrencies are relatively new, and to this day, experts around the world are still arguing and giving opposing opinions. We will try to find different treatments for the same questions to compare and analyze them.

Two other methods that would be suitable for conducting the research are meta-analysis and scoping review. A meta-analysis involves a statistical analysis of the results of multiple studies and a scoping review involves a preliminary assessment of the available literature (Grant & Booth, 2009).

4. ANALYSIS AND FINDINGS

Money laundering is crucial to all financially motivated crimes because criminal groups can use their illegally earned money. Virtual currencies have been used in many illegal activities such as money laundering, illegal purchases, ransomware payments, investment scams, cybercrime, etc. (Europol, 2021).

Money laundering and criminal activity using cryptocurrency are likely to occur through several methods.

4.1. The use of cryptocurrencies for criminal purposes

Several cases of the use of cryptocurrencies for criminal purposes are described below.

Case 1: Exchanges and money laundering

Criminals can convert paper money into cryptocurrency using a bitcoin exchange, and then participate in a variety of bitcoin-based transactions or purchases to hide the criminal origin of the money.

BTC-e has been used in criminal activities processing more than 4 billion dollars from 2011 to 2017 by a Russian citizen. Alexander Vinnik was charged with running a black market bitcoin exchange that assisted in the laundering of billions of dollars. Ransomware fraud, identity theft, drug trafficking, and public corruption are just a few examples of illegal activities that Vinnik has carried out using BTC-e. The website served 700,000 customers worldwide.

Case 2: Mexican drug lords

Criminals can sell illegal goods or services by being paid in bitcoins, eventually converting them into regular currency, and then finance transactions and purchases designed to hide their illegal source. Cryptocurrencies are increasingly being used to launder drug trafficking proceeds. Several agencies are in charge of investigating and prosecuting cases involving online marketplaces and virtual currency trafficking.

The U.S. Government charged six Chinese citizens in October 2020 for allegedly participating in the laundering of cartel funds using cryptocurrencies. Mexican drug cartels were increasingly using Chinese crypto channels for money laundering at the time. This system has become more convenient for cartels to use because it simplifies the money laundering process. Approximately $2.8 billion in bitcoin has been transferred from criminal entities to exchanges binance and huobi (50%) and another cryptocurrency (50%) (Vassanelli, 2022).

Case 3: Fraudulent cryptocurrency investment (Ponzi scheme using cryptocurrency)

Fraud is the most commonly reported act when using cryptocurrency. Scams are unavoidable when money is involved. The same is true for cryptocurrency (Hetler, 2023).

Criminals were duping people into investing in a Ponzi scheme by using the social media platform Vitae.co and the website Vitaetoken.io. This investment scam has affected over 223,000 people from 177 countries. A total of €1.1 million in cash, €1.5 million in cryptocurrencies, and 17 luxury vehicles were seized. This is an example of cryptocurrency being used in an investment scam. Before the price bubble bursts, the criminals flee with a large portion of the cryptocurrency and convert it to other currencies[3].

Case 4: The fraudulent trading scheme

Europol dismantled criminals involved in investment fraud and money laundering in May 2021. The criminal network established various online trading platforms that advertised substantial profits from investments in high-risk options and cryptocurrencies. They advertised trading platforms on social media and manipulated software to show the fictitious gain, inciting the victim to invest more. The total amount of victims defrauded in Europe was estimated to be €30 million (Europol, 2021b).

Case 5: QQAAZZ criminal network

Cybercriminals are individuals or teams of people who use technology to commit criminal activities on the internet.

Since 2016, it is estimated that the QQAAZZ network has laundered or tried to launder millions of euros in stolen funds. The QQAAZZ network opened and managed large numbers of corporate and personal savings accounts at banks all over the globe to receive funds from malicious hackers who stole money from victims' accounts. The money was then relocated to other QQAAZZ-controlled savings accounts and occasionally converted to cryptocurrency via "tumbling" services designed to conceal the whereabouts of the funds. The QQAAZZ members obtained these bank accounts by creating and registering dozens of shell corporations that engaged in no legitimate business activity using both legitimate and fraudulent Polish and Bulgarian identification documents (Europol, 2020).

Case 6: Ransomware payments

Ransomware is a kind of malicious software or malware that prevents access to computer files, systems, or networks and requires a ransom to regain access. The Federal Bureau of Investigation (FBI) states that incidents of ransomware attacks can result in costly disruptions to operations, as well as the loss of important information and data. The emergence of bitcoin and other cryptocurrencies has been closely associated with the development of ransomware, with ransom payments usually being facilitated in these digital currencies (Custers et al., 2020). WannaCry resulted in the hackers receiving a bitcoin ransom of £108,000 which they have now withdrawn.

In 2017, the hackers who initiated the WannaCry ransomware attacks began withdrawing money from three bitcoin wallets. To unlock files that had been held hostage by the malware, victims were requested to pay a ransom of between $300 and $600. It was estimated that approximately 230,000 computers worldwide had been affected by WannaCry. Between July 24 and August 3, the hackers withdrew more than £18,000 in bitcoin from the three wallets and transferred the funds to Shapeshift.io to convert bitcoins into monero, intending to make the transfer of funds untraceable (Gibbs, 2017).

4.2. Dark web marketplaces

The use of the dark web has created real dangers related to money laundering for virtual currencies. The dark web is a term used to refer to a collection of web pages that exist on an encoded network and are inaccessible via conventional search engines or browsers. Almost all dark web sites use the "Tor" encryption tool to conceal their identity (Chertoff, 2017).

According to estimates, cryptocurrency-related transactions on dark web marketplaces have reached a total of €1.5 billion (US$1.7 billion) in 2020 (Europol, 2022).

When a dark web merchant makes a transaction, it is usually in the virtual currency bitcoin. But to use that money, the merchant needs to convert it into real currencies, so it can be more easily spent or invested in something else. Some "cash out" sellers advertise their service directly on the dark web. They

[3] Europol helps Belgian and Swiss authorities unravel Vitae Ponzi scheme.

secretly send pounds or euros in the mail and receive bitcoins in return.

It is not prohibited to use Tor to browse the internet. Your IP address and browsing history can be hidden for free, and doing so is legal. But a lot of people who use Tor do so because they want to remain anonymous while engaging in illegal activity (Coble, 2015). About 55% of dark web content is legitimate, according to Terbium Labs, a provider of data about the dark web. While some users use the dark web as a haven for illegal activities, others use it to protect their right to privacy (Sherman, 2022).

Case 7: Criminal services online.

The FBI was able to identify and apprehend a nurse who hired a hitman thanks to the blockchain analysis they conducted. The virtual currency bitcoin was used to pay for the murder. A nurse from Illinois who admitted sending $12,000 in bitcoin to the website Sicilian Hitmen International Network was given a 12-year prison term. She had intended to have her boyfriend's wife murdered (Popper, 2020).

The most famous dark web site related to the use of bitcoin has been Silk Road. Silk Road was an online black market and the first modern dark web marketplace, better known as a platform for selling drugs. The website began operations in February 2011 and was shut down on October 11, 2013, following the arrest of its founder Ross Ulbricht. The FBI confiscated over 144,000 bitcoins. The simplest way to explain Silk Road would be to call it the "eBay of illegal drugs". During two and a half years of operation, the "eBay of illegal drugs" made more than US$1 billion in transactions, according to the FBI (Kopfstein, 2013). All Silk Road users used bitcoins as a payment method. Silk Road functioned as an intermediary for buyers and sellers, without knowing each other. This was the main reason to use bitcoin as payment money. The buyer would send the coins to the platform, where they would be held until the order reached its destination by mail. When the buyer received the order, then the money was transferred to the seller. Silk Road kept a commission for this service (Brito, 2013).

4.3. The use of bitcoin for money laundering

"Bitcoin is frequently mischaracterized as an anonymous currency" (Antonopoulos, 2014, p. 201). For instance, PayPal keeps track of each transaction and connects each user's virtual account to their bank account. Bitcoin lies somewhere in the middle. "Using data analysis, you can link between addresses to form a broad and comprehensive picture of someone's spending habits" (Antonopoulos, 2014, p. 201). It is relatively easy to link the identities of bitcoin addresses (Antonopoulos, 2014).

Although all transactions' public keys are stored on the blockchain, they are not linked to any particular person's identity. Security professionals, on the other hand, refer to it as pseudonymous privacy, similar to publishing books under a pen name. As long as the nickname is not connected to you, you can maintain your privacy. But the "trick" becomes obvious the moment someone links to one of your books. The author makes public the entirety of their writing under the alias. Bitcoin has been characterized as offering pseudo-anonymity and generating sufficient obfuscation to permit users to dispute charges (Duhaime, 2019).

There are several solutions to enable more anonymity. Mixing services (also known as "tumblers") enable bitcoin users to cover their tracks. Not all transactions using mixers are illegal, but mixers provide an attractive tool for criminals. Bitcoin tumbling, also known as bitcoin mixers or bitcoin scrubbers are processes that use a third-party service to break the connection between a bitcoin address that sent coins and the address they were sent to. It is possible to send bitcoins there, pay a commission for this service, and receive other bitcoins. The only downside is the fact that the company doing the shuffling has the transaction records, even though they claim they delete them as soon as the transaction is complete, they can keep track of where the coins went. Legitimate users face the risk of having "contaminated" coins or more precisely, bitcoins from an illegal source sent to their wallet by a mixing service. Because of alternative currencies, it becomes possible to complicate transactions even more.

Cryptocurrency exchanges, with the participation of various virtual bitcoin alternatives, increase the overall level of anonymity and complicate the tracking of user actions.

The second benefit of using bitcoin is that users can send each other financial instruments without the involvement of a third party, avoiding the involvement of banks or other financial institutions. To prevent money laundering, banks, and other businesses must report suspicious activity and "restrict the ability of criminals to transfer value without inspection" (Stokes, 2013, p. 4).

The third risk relates to "the speed and simplicity of carrying out Bitcoin transactions" (Stokes, 2013, p. 4). In addition to enabling a significantly simpler payment structure known as "smurfing" to avoid suspicion, the electronic process enables the electronic currency to complete international transactions in fewer than 10 minutes.

4.4. Further necessary bitcoin regulation

The question is more concerned with how people use money than with whether it is physical or digital. However, special requirements might be required if the use of digital currency itself makes investigations and enforcement agencies more challenging (European Central Bank, 2012).

The biggest risk that an unregulated currency poses is a speculative attack (Douma, 2016). A speculative attack on a currency is when investors believe that the value of a currency is overvalued and therefore, they sell this currency in anticipation of its decline and buy another currency, investors engage in what is called "short selling". Short selling occurs when an investor sells assets he does not own by borrowing them and agrees to repurchase them in the future.

The bank loses money when the attacker buys the currency back from it. The value of the currency just keeps declining and becoming unstable if a bank is unable to defend itself from a speculative attack. Banks can rely on the Central Bank of their nation to defend against speculative assaults. Because they have foreign reserves that can be borrowed during uncertain times, central banks can fend off speculative attacks (Langdale, 2023).

What if a bitcoin investor chooses to attack a currency? The Central Bank will have to purchase bitcoins from an online exchange. Since

the International Monetary Fund (IMF) will not have bitcoins in reserve and there is no way to obtain them, the Central Bank is unable to turn to the IMF for assistance.

The IMF is therefore constrained in its ability to intervene if a private cryptocurrency like bitcoin is used to attack a value of a currency through what is known as a "speculative attack". If bitcoin becomes a significant medium of exchange for international trade, speculative attacks using it could seriously harm the global economy unless the IMF finds a way to stop them (Plassaras, 2013).

The European Central Bank has been dispatching the dangerous message that anyone can create their own virtual currency without a license by leaving bitcoin unregulated. The anonymity that bitcoin offers is one of its biggest benefits as well as one of its biggest drawbacks. A setting is created where criminals can hide their tracks by using an anonymous peer-to-peer payment system in an unregulated currency. Regulation is essential because unregulated currencies enable criminals to remain undetected and carry out their illicit activities. "Special requirements may be required if the use of digital money itself complicates investigations and law enforcement" (Plassaras, 2013, p. 6).

5. CONCLUSION

Authorities are mainly worried about the potential for financial fraud that bitcoin provides as well as the economic and social repercussions of this use. At the moment, the biggest problem with bitcoin is that the same characteristics that attract legitimate users, such as confidentiality, and international reach, also attract criminal activity. Regulators must now concentrate primarily on how virtual currency should be categorized within the framework of the anti-money laundering (AML) program.

To establish legal guidelines for using cryptocurrencies as a payment system, it is not enough that Interpol already has a department dedicated to crimes committed through the use of virtual currencies, such as bitcoin. Other institutions must be established globally. The regulation of this market is a global emergency and the possibility of removing it from circulation, or even labeling it as illegal, as some countries (Russia and China) have threatened, is likely to be impossible due to the decentralized virtual network that bitcoin works. We cannot say that cryptocurrency is very problematic, although crime relies on them to exercise their activity; non-virtual currencies have the same problem. We must emphasize the regulation of these laws which evidence criminal activity. Paper money can be used to buy and sell drugs and money laundering as well; paper money can be stolen, not from a digital wallet, but from a physical wallet; even non-virtual currencies can be used for tax evasion purposes. Paper money, like bitcoin, can be used in illegal transactions, but we do not consider decommissioning paper money at all. We can only prohibit its use for illegal purposes. Electronic money offers a large number of potential benefits. Governments must be careful not to stifle these innovations. Electronic money is the future of currencies and we must prepare in such a way as to create the right infrastructure to function. Legislators' interests in the detection and prevention of money laundering would advance if intermediaries, like exchangers and fund transmitters, were required to maintain records and alert authorities to suspicious activity, just like regular financial institutions.

In this paper, we talk about what these discoveries mean for law enforcement and how bitcoin laundering chains might be broken. In several different cases, we showed how cryptocurrencies are used in illegal activities. All these cases serve individuals to understand the ways of fraud as well as governments to design policies against money fraud.

Very little information is available on money laundering with other cryptocurrencies and this research has relied on some cases mostly involving bitcoin.

Further study is required to develop software tools that are specially designed for examining all ledgers for the possibility of money laundering. Such software must have the ability to recognize patterns in accounts that are suggestive of money laundering. More study is needed on methods that allow users to be recognized.

REFERENCES

1. Antonopoulos, A. M. (2014). *Mastering bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media, Inc.
2. Brito, J. (2013, November 18). *Beyond silk road: Potential risks, threats, and promises of virtual currencies*. Mercatus Center at George Mason University. https://www.mercatus.org/research/federal-testimonies/beyond-silk-road-potential-risks-threats-and-promises-virtual
3. Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy, 2*(1), 26–38. https://doi.org/10.1080/23738871.2017.1298643
4. Coble, C. (2015, September 28). *Is it illegal to use the Tor network?* [Blog post]. FindLaw. https://www.findlaw.com/legalblogs/law-and-life/is-it-illegal-to-use-the-tor-network/
5. Cochrane, B. (2020, November 8). *Cryptocurrency viewed through the three stages of money laundering* [Post]. LinkedIn. https://www.linkedin.com/pulse/cryptocurrency-viewed-through-three-stages-money-brendan/
6. Custers, B. H. M., Oerlemans, J.-J., & Pool, R. (2020). Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice, 28*, 121–152. https://brill.com/view/journals/eccl/28/2/article-p121_121.xml
7. Douma, S. (2016). *Bitcoin: The pros and cons of regulation* [Master's thesis, Leiden University]. Leiden University Student Repository. https://studenttheses.universiteitleiden.nl/handle/1887/42104
8. Duhaime, C. (2019). The role of anti–money laundering law and compliance in fintech. In J. Barberis, D. W. Arner, & R. P. Buckley (Eds.), *The RegTech Book*. https://doi.org/10.1002/9781119362197.ch36
9. European Central Bank. (2012). *Virtual currency schemes*. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
10. Europol. (2020). *20 Arrests in QQAAZZ multi-million money laundering case*. https://www.europol.europa.eu/media-press/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case

11. Europol. (2021a, December 7). *European Union serious and organised crime threat assessment (SOCTA) 2021: A corrupting influence: The infiltration and undermining of Europe's economy and society by organized crime*. https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
12. Europol. (2021b, May 11). *Trading scheme resulting in €30 million in losses uncovered. Trading scheme resulting in €30 million in losses uncovered.* https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-%E2%82%AC30-million-in-losses-uncovered
13. Europol. (2022, January 26). *Cryptocurrencies: Tracing the evolution of criminal finances*. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances#downloads
14. Fernando, J. (2023, March 16). Market capitalization: How is it calculated and what does it tell investors? *Investopedia*. https://www.investopedia.com/terms/m/marketcapitalization.asp
15. Forgang, G. (2019). Money laundering through cryptocurrencies. *Economic Crime Forensics Capstones*. https://digitalcommons.lasalle.edu/ecf_capstones/40
16. Frankenfield, J. (2023a, April 5). What is bitcoin? How to mine, buy, and use it. *Investopedia*. https://www.investopedia.com/terms/b/bitcoin.asp
17. Frankenfield, J. (2023b, April 21). Cryptocurrency explained with pros and cons for investment: Learn what you need to know before you invest in a virtual currency. *Investopedia*. https://www.investopedia.com/terms/c/cryptocurrency.asp
18. Gibbs, S. (2017, August 3). WannaCry: Hackers withdraw £108,000 of bitcoin ransom. *The Guardian*. https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom
19. Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x
20. Guidara, A. (2022). Cryptocurrency and money laundering: A literature review. *Corporate Law & Governance Review, 4*(2), 36–41. https://doi.org/10.22495/clgrv4i2p4
21. Hetler, A. (2023, April 19). 10 Common cryptocurrency scams in 2023. Some of the latest scams involve rug pulls, Ponzi schemes, and phishing. *TechTarget*. https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams
22. Hillman, H. D. (2020). *Money laundering through cryptocurrencies: Analysing the responses of the United States and Australia and providing recommendations for the UK to address the money laundering risks posed by cryptocurrencies* [Doctoral thesis, University of the West of England]. UWE Bristol Research Repository. https://uwe-repository.worktribe.com/output/4234061/money-laundering-through-cryptocurrencies-analysing-the-responses-of-the-united-states-and-australia-and-providing-recommendations-for-the-uk-to-address-the-money-laundering-risks-posed-by-cryptocurrencies
23. Kopfstein, J. (2013, October 3). How Ebay of illegal drugs came undone. *The New Yorker*. https://www.newyorker.com/tech/annals-of-technology/how-the-ebay-of-illegal-drugs-came-undone
24. Langdale, J. (2023). Money laundering in Australian casinos. *Journal of Money Laundering Control, 26*(7), 99–109. https://doi.org/10.1108/JMLC-09-2022-0136
25. Popper, N. (2020, March 4). Can you really hire a hit man on the dark web. *The New York Times*. https://www.nytimes.com/2020/03/04/technology/can-you-hire-a-hit-man-online.html
26. Plassaras, N. (2013). Regulating digital currencies: Bringing bitcoin within the reach of the IMF. *Chicago Journal of International Law, 14*. Advance online publication. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419
27. Sicignano, G. J. (2021). Money laundering using cryptocurrency: The case of bitcoin! *Athens Journal of Law, 7*(2), 253–264. https://doi.org/10.30958/ajl.7-2-7
28. Statista. (n.d.). *Number of identity-verified cryptoasset users from 2016 to November 2022*. https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/
29. Stokes, R. (2013). Anti-money laundering regulation and emerging payment technologies. *Banking & Financial Services Policy Report, 32*(5), 1–10.
30. Sherman, P. (2022, December 7). Is Tor legal? Understand the legal consequences of using Tor. *VPN Overview*. https://vpnoverview.com/privacy/anonymous-browsing/is-tor-legal/
31. The World Bank. (n.d.-a). *GDP (current US$) — Albania*. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=AL
32. The World Bank. (n.d.-b). *GDP (current US$) — Nigeria*. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=NG
33. United Nations. (n.d.). *Money laundering through cryptocurrencies*. https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html
34. U.S. Department of Justice. (2017, July 26). *Russian national and bitcoin exchange charged in 21-count indictment for operating alleged international money laundering scheme and allegedly laundering funds from hack of Mt. Gox* [Press release]. United States Attorney's Office, Northern District of California. https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged
35. U.S. Department of Justice. (2020). *Cryptocurrency: Enforcement framework* (Report of the Attorney General's cyber digital, task force). https://www.justice.gov/archives/ag/page/file/1326061/download
36. Vassanelli, E. (2022, November 18). Money laundering and cryptocurrencies: A case study of Mexican drug cartels. *Crossfire KM*. https://www.crossfirekm.org/articles/money-laundering-and-cryptocurrencies-a-case-study-of-mexican-drug-cartels
37. Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019, August). *Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics* [Paper presentation]. KDD '19 Workshop on Anomaly Detection in Finance, Anchorage, the USA. https://arxiv.org/pdf/1908.02591.pdf
38. Wells, M. (2013). *Technology in the fight against money laundering in the new digital currency age.* Thomson Reuters. https://www.readkong.com/page/technology-in-the-fight-against-money-laundering-in-the-new-6952847