Anti-Money Laundering (AML) System using Blockchain Technology

Research Paper

Anti – Money Laundering(AMl) System using Blockchain Technology

Tejus Sharma
UG Student, CSE
Chandigarh University
21bcs3050@cuchd.in

Ritvik Kumar
UG Student, CSE
Chandigarh University
21bcs3058@cuchd.in

Sachin Pal
UG Student, CSE
Chandigarh University
21bcs3057@cuchd.in

Dushant Chaudhary
UG Student, CSE
Chandigarh University
21bcs3003@cuchd.in

BACHELOR OF ENGINEERING IN

COMPUTER SCIENCE ENGINEERING

ANTI MONEY LAUNDERING SYSTEM USING BLOCKCHAIN TECHNOLOGY

ABSTRACT: In this paper, we aim to dispel some myths about new blockchain technologies and cryptocurrencies, especially Bitcoin, as tools with primarily negative connotations and potential locations for a variety of criminal activities, including cases of money laundering where money has been obtained dishonestly and illegally. The technique of correlated variations, the comparable and normative approach, genetic, structural, and functional analyses, and other methodologies were all used to achieve this. The majority of the article is devoted to providing an overview of distributed ledger technology, also known as a distributed book of records technology, which forms the foundation of the blockchain and its most well-known application, the Bitcoin. We also had to discuss the Ethereum blockchain, which expands the potential uses of Bitcoin and, therefore, increases the possibility of misuse of this technology, particularly given its fundamental principle of anonymity. This is the second-most significant development in this field of technology. The blockchain and cryptocurrencies have not significantly aided the channels of illicit money laundering, especially those not connected to serious crimes like drug trafficking and terrorism, as we have demonstrated in this article, despite the absence of adequate national and international regulatory frameworks. This study's main contribution is a categorization of potential money laundering techniques, particularly the use of non-exchangeable tokens known as NFTs (Non-Fungible Tokens), whose current popularity may be related to a potential new money laundering approach. We come to the conclusion that rather than being afraid of the Bitcoin, we should accept it as a necessary component of a peaceful and prosperous future because the Bitcoin offers the human race new perspectives on issues other than money laundering, which had existed to the same extent even before the invention of the Bitcoin..

Keywords: *The Bitcoin, money laundering, Distributed Ledger Technologies, algorithm, the Ethereum*

1. Introduction

The rapid pace of technological advancements has outpaced the ability of our traditional institutions, including the legal system, to adapt and keep up with these changes. This sentiment was expressed by Larry Page, the CEO of Google.

Current national laws aiming at giving citizens legal certainty, as one ofthe main concepts of law, are increasingly at odds with the dynamic expansion of the technology sector, which is becoming

The emergence of Blockchain technology has the potential to significantly transform our understanding of legal standards and challenge traditional concepts within the field of law. One area where this impact can be observed is in the realm of judicial jurisdiction and the protection of citizens' rights and interests, which are guaranteed by legal frameworks. The notion of territoriality, where a state exercises its authority over events occurring within its boundaries, is central to this discussion (Ferreira, 2021, pp. 2-3).

The introduction of Blockchain technology raises questions about achieving legal certainty when utilizing this innovative system. Blockchain operates on a supranational and decentralized model, relying on algorithmic validation of information for financial and other transactions, without relying on built-in regulatory principles. This characteristic of Blockchain can potentially create conflicts with national civil law systems, which are built upon clear and coherent legal norms. Understanding and navigating this phenomenon can be challenging due to the disruptive nature of Blockchain technology and its potential implications for established legal frameworks.

Cryptocurrencies have become a new phenomena in the global financialsystem in recent years. Since a mystery person or entity using the alias Satoshi Nakamoto released the first decentralised cryptocurrency, Bitcoin, into the hacker community in 2009, the total amount of cryptocurrencies in circulationand the variety of different types.

The value of cryptocurrencies has significantly risen. The market value of all cryptocurrencies is currently above two trillion dollars, with Bitcoin and Ethereum accounting for half of that total.

via mining, astute trading on digital stock markets, and launching businesses on platforms that raise startup funding via initial coin offers (ICO), cryptocurrencies are becoming into a significant source of revenue. Businesses from a wide range of industries are taking part in the development of cryptocurrency markets, either directly or indirectly. These businesses include cryptocurrency stock exchanges and exchange offices (VCE - Virtual Currency Exchange), as well as retailers, financial institutions, video game developers, and computer manufacturers. The expansion of these marketplaces has led to a number of businesses, like Tesla, Microsoft, and Facebook, adding cryptocurrencies to their investment portfolios. Due to the potential that

cryptocurrencies and distributed ledger technology (or "DLT") have, regulated financial institutions (or "FIs") are confronted with substantial operational and regulatory issues.

The fight against money laundering and terrorist financing is of utmost importance (Holman & Stettner, 2018, p. 26). When it comes to the bitcoin ecosystem, there are significant differences compared to previous Internet-based systems, particularly regarding the level of centralization. The decentralized nature of peer-to-peer networks in cryptocurrencies like Bitcoin enables owners to bypass important controls within the global Anti-Money Laundering (AML) system. This creates challenges for existing AML regimes that rely on Know-Your-Customer (KYC) and customer identification procedures (CIP) since the potential for mutual anonymity among counterparties hinders their effectiveness, as noted by Holman and Stettner (2018).

DLT is one of several technological ecosystems that lacks clear responsibility frameworks. Who will be held responsible for the harm caused by the occurrence when users suffer losses of hundreds of millions of dollars, as occurred in the VCE Live Coin hack in December 2020? This topic is difficult to talk about since DLT is fundamentally a technology without any built-in legal constraints. Smart contracts serve as a typical example in this situation because they are created on a decentralised platform with an anonymous administrator, managed by a self-executing algorithm without the possibility of revocation, and treated by the law similarly to any other traditional contract or signature.

To really understand the role that cryptocurrencies play in the processes that make it possible to launder money that has been gained illegally, it is essential to understand the DLT on which cryptocurrencies are produced and maintained. We attempt to debunk myths regarding cryptocurrencies, namely Bitcoin, and emerging blockchain technology in this essay.

negative affiliations and provide opportunity for a range of crimes, including the washing of money earned dishonestly and illegally. To do this, the technique of correlative variations, the analogous and normative method, the method of correlative variations, and genetic, structural, and functional studies were all used.

.

2. The term blockchain

The foundation of blockchain technology is the algorithm's ability to reach agreement in a decentralised network without relying on a third party to verify or complete the transaction. Therefore, blockchain technology not only fixes a few systemic technological faults but also significantly improves how society views "trust," "authority," and "consensus." If it prevents anybody from having particular control over the network and the transactions that take place in it, the mathematical technique becomes a neutral (trustless) instrument for any imaginable application, boosting relationships between individuals. A "blockchain" is simply a collection of linear, immutable, and irreversible "blocks" that have been cryptographically hashed and serve as a record of transactions. Decentralised DLT technology is used to verify and preserve this linear history of time-stamped events. Network nodes "witness" transactions and agree on which ones are regular via a consensus "Proof of Work" process. Blockchain is referred to as a "trust machine" because it can achieve agreements on transactions algorithmically rather than via the external mediation of a third party or an authority (Vigna & Casei, 2018). In this hypothetical scenario, cryptographic evidence1 facilitates agreement and assures record authenticity.

where the code serves as a stand-in for the law, the mediator, the institution, or the authority. Transactions occur directly between participants in this way, avoiding financial agencies. Most importantly, the process by which money is created is determined and carried out by an immutable protocol rather than by state or government action. Bitcoin's ongoing success and disruptive power that completely changed the financial sector are demonstrated by the fact that it was the first to expose the fundamental fallacy of Modernity, which was founded on the Keynesian and Marxist ideas "that government needs to manage the money supply" (Ammous, 2018, p. 136). The code is created to mine Bitcoin, determining the weight of mining and regulating the pace of cash emission.

The capacity to verify something with absolute mathematical certainty is known as cryptographic proof. This is what Satoshi Nakamoto means when he refers to an electronic system that relies on cryptographic evidence rather than trust in his Bitcoin White Paper. Instead of relying on a source's or an individual's word, mathematical probability is used to verify data integrity. A timestamp can be added to a record to show when it was created. You can create a linear history of records that have been demonstrated to be secure by hashing them all together into a "chain" or "tree" that refers to the preceding record's hash output, or "a new block in the chain" (Nakamoto, 2008).

According to Ammous (2018, p. 219), Bitcoin can be viewed as a technology that uses processing power to convert electricity into accurate records. As a result, miners

receive cryptocurrency in exchange for their investment in processing power (hardware) and electricity. In fact, Bitcoin has grown to be the world's biggest dedicated computer network by charging for processing power. In this approach, a portion of the online community develops a liquid currency that competes with established fiat currencies created and managed by governments. Over the past ten years, hundreds of legitimate cryptocurrencies and thousands of tokens have been developed in the aftermath of Bitcoin, many of them with really innovative concepts and prosperous economic enterprises Mining is a crucial process in the production of Bitcoin. It utilizes a Proof of Work-based consensus mechanism, which aims to deter potential attackers by providing rewards. Essentially, mining involves a competition among participants to verify transactions. In the crypto-economy, where decentralized or distributed protocols play a key role, economic dynamics and incentives are integrated into network security engineering. Miners solve computational problems and receive payment for their efforts, with a new problem being solved approximately every 10 minutes. The total number of Bitcoins in circulation, set to reach 21 million by around the year 2201, also impacts the rate of Bitcoin generation within the network.

Contrary to common perception, the "consensus" achieved through the mining process is essentially a settlement driven by incentives. Its validity is determined by arbitrary attempts to leverage computational power rather than through discussions, agreements, predefined notions of justice, or objective truths. The fairness of the consensus algorithm, or more precisely, its legitimacy, does not rely on subjective judgments or predetermined principles but instead operates based on probability and the collective agreement of online computers (Brekke, 2019).

Public key cryptography makes sure that the communication cannot be read by anyone other than the intended receiver and cannot be intercepted. A set of keys is created via cryptographic hashing, one of which can encrypt (the public key) and the other of which may decode (the private key, which is kept a secret). Messages sent to the owner are encrypted using the public key, and the owner decrypts the messages using the private key (Brekke, 2019). Bitcoin's major objective is to create a network without the need for trust in any authorities, third parties, or intermediaries, which it views as a security vulnerability, extra expense, and potential uncertainty.

One of the less well-known features of the Bitcoin design is Proof of Work. It is a type of cryptographic proof that makes use of hashing. The "work" that nodes in the Bitcoin network mustperform enables them to validate the transactions that are being monitored, arrange those transactions into blocks, and submit those blocks to the SHA-256 hashing process to get a legitimateoutput. Mining is a term used to describe the computer "work" of hashing transaction data in orderto identify a legitimate exit.

3. Basic characteristics of blockchain sensibility

Google, Facebook, Amazon, and Apple are now able to connect the entire worldunder their control thanks to the Internet. Global connectivity will be made possible through blockchain, with participant control. Ethereum by Jon Choi, 2017. Decentralisation . Decentralisation, which is a component of network culture, refers to dispersed networks that are impervious to all types of government censorship and control. It's sometimes referred to as disintermediation. Peer-to- peer systems, like Bitcoin, are composed of network users that speak directly to one another on a technical level. They don't exist in peer-to-peer networks, unlike server-to-client topologies, where servers store and transmit material to various clients. Decentralisation as it is defined by blockchain network protocols differs significantly from decentralisation as an ethical, political, social, or economic aimor concept that a given protocol may or may not embrace.

Openness. No organisation in a decentralised system may prevent users from connecting to the network, which expressly defines the idea of neutrality in opposition to established organisations.

Trust. There is some scepticism in open, decentralised systems. It is preferable to keep the amount of required trust as low as possible in order to achieve perfect mistrust and security. Relationships built on trust may never be totally certain of their outcome. Bitcoin is totally based on verification and not at all on trust, claims Ammous (2018).

Immutability. The chain of blocks has to be immutable for Bitcoin to function independently and without intervention from any outside authority. Immutable code, which runs exactly as it is written, is the concept's basis. The Proof of Work consensus protocol's immutability provides assurance that the consensus on the network's state cannot be changed arbitrarily.

Privacy. Both people and organisations may

interact with one another completely anonymously using computers. The capacity to selectively disclose oneself to the world online through encryption is known as privacy. This is critical at a time when mass monitoring is being used on the Internet as an infrastructure, which is limiting the degree of freedom. In the case of Bitcoin, which employs a peer-to-peer payment mechanism, the whole network keeps track of transactions rather than a third party, making all transactions completely public. The computers themselves remain anonymous in a system that is so blatantly transparent.

Anonymity. Because it was formerly believed to be anonymous, Bitcoin was notoriously used as a payment mechanism for the "Darknet" and online criminal marketplaces. However, the trade may now be tracked and the transaction deanonymized. In order to prevent this and obscure the trail with "dirty" coins, coin mixers are used to "mix" transactions so they cannot be easily traced to individual owners. Additionally, cryptocurrencies like Z-Cash, Monero, and the majority of others have increased anonymity built into them. recently Nim, which were created explicitly for anonymity purposes, thanks to improved cryptography and zero-knowledge proofs.

4. Ethereum blockchain and tokenization

With the advent of blockchain 2.0, or Ethereum, the idea of decentralisation has undergone a full upheaval. With the help of this idea, theEthereum Blockchain has made it possible for transactions to involve any kindof value, not only money. Ethereum is a multipurpose blockchain that may beused for a variety of purposes. Three aspects, including the idea of smart contracts, WEB3.0, a new stage in the development of the Internet, and decentralised autonomous organisations (DAO), show the contribution madeby the Ethereum blockchain.

Computer programmes known as "smart contracts" are capable of upholding the terms of a contract between two parties without the assistance of a third party. Like a standard contract, smart contracts have the ability to set rules and, when certain conditions are fulfilled, automatically enforce those rules using code. Smart contracts are self-executing, unremovable, and have irreversible interactions. They created the potential for corporate management and contract law to be automated. The blockchain's dependability is ensured by the process used to verify and add transactions.

Smart contracts in the Ethereum network require transaction costs, known as "gas," to be paid in Ether (ETH). This makes Ether the foundational currency of the Ethereum blockchain.

The emergence of Web 3.0, a decentralized web built on blockchain technology, enables the development of decentralized applications (dApps) that operate in a distributed manner, free from censorship or outages.

Decentralized autonomous organizations (DAOs) are entities that follow protocols expressed as computer programs called smart contracts. These smart contracts govern their behavior in a way that benefits stakeholders. DAOs leverage token ownership rights, contractual obligations, and business logic to create wealth and influence for token holders, allowing them to make decisions with real power.

One of the key advantages of the Ethereum blockchain is its ability to facilitate the creation of unique tokens that exist and operate on the network (Ali & Bagui, 2021, p. 53). Unlike currencies and cryptocurrencies that represent value, tokens provide specific rights to their owners, which can be related to the issuer or used for recording ownership of assets. This process of encrypting rights on the network is known as "tokenization." Creating tokens on the blockchain doesn't require starting from scratch; existing blockchains like Ethereum offer templates, such as ERC (Ethereum Request for Comment) standards, that publishers can use to create their own tokens. Tokens can be classified into three categories based on their functionality: investment tokens, utility tokens, and currency tokens.

Blockchain technology is commonly utilized in Initial Coin Offerings (ICOs), where companies offer tokens to the public in exchange for funds, similar to an initial public offering (IPO) in traditional markets. ICOs often occur at the early stages of a project. Notably, platforms like Telegram and EOS raised significant funds through ICOs, highlighting the popularity of this fundraising method.

Once tokens are created, they can be promoted and sold by the issuer, providing various benefits to online communities. It is customary for issuers to publish a "white paper" outlining the project's details. Smart contracts play a vital role in facilitating ICO investments, allowing investors to participate in token sales.With individuals all across the globe, he may exchange the cryptocurrency in his digital wallet for new tokens. Particularly Twitter is used extensively in the marketing campaign.

The ERC-20 standard makes it simple to create, use, and trade tokens based on Ethereum. Anyone

may construct an ERC, but the inventor must accurately define the standard in order to win the online community's support for their business proposal.

With the help of the ERC-721 protocol, unchangeable tokens may be produced. In accordance with this standard, every token has a distinct owner, cannot be replaced, and can be tracked online individually. These are the so-called NFTs (Non-Fungible Tokens), which have recently entirely changed the cryptocurrency sector and have a market capitalization of over $600 billion.

The Base Security Token, or ERC-1462, is an extension of the ERC-20 standard and is noteworthy because it satisfies the demands of the Financial Institution (FI) in terms of the legal obligations in the financial markets. ERC-1462 guarantees adherence to securities regulations and legal enforcement. According to Ali and Bagui (2021, p. 54), ERC 1426 also has KYC (Know Your Customer) and AML (Anti Money Laundering) rules as well as the capability to lock tokens and prohibit their transfer in the event of a legal dispute.

The token-based economies are sustained by a mechanism that pays for its maintenance, which explains why the models of the centralised Internet infrastructure are now in use. Blockchain establishes a user economy apart from strong financial systems and institutions that enforce their own laws and only act in their own best interests when manipulating financial markets. Organisations and communities become economically viable thanks to blockchain. The intimate relationship between economic theories and technical breakthroughs is the cornerstone of cryptoeconomics. The blockchain protocol design contains a number of economic issues that might possibly have political implications.

5. Key terms in AML processes

Cryptocurrencies are a form of virtual currency that serves as a digital asset with multiple functions. They can act as a store of value, a medium of exchange, and a unit of account. Unlike "fiat currency," which refers to national currencies, and "e-money," which represents digital fiat currency, virtual currencies lack the legal status of being recognized as a national means of payment (Holman & Stettner, 2018).

Virtual currencies can be categorized as either convertible (having the same value as fiat money) or non-convertible (restricted for use within specific platforms or communities, such as tokens in video games). They can also be centrally administered, like Bitcoin and Ethereum, or decentralized, where control is governed by code (2018, p. 26). Bitcoin, as an example, is a typical convertible and decentralized virtual currency that utilizes cryptographic principles to secure transactions in the absence of traditional intermediaries like banks.

Bitcoin was the first cryptocurrency to be introduced and remains the most well-known, but numerous other cryptocurrencies have since been created with different features and purposes. According to Statista, as of March 2022, there were 10,397 cryptocurrencies in active use worldwide (Statista, 2022). Increasingly, cryptocurrencies are seen as a form of crowdfunding and a legal procedure comparable to Initial Public Offerings (IPOs). However, it's important to note that initial coin offerings (ICOs), which employ cryptocurrencies to raise capital for investments, often run afoul of securities laws and other financial regulatory frameworks.

It's worth noting that cryptocurrency regulations and perceptions may differ across jurisdictions, and it's crucial to consult the specific laws and guidelines applicable in your jurisdiction or seek professional advice when dealing with cryptocurrencies..

6. The cryptocurrency and money laundering industries

Cryptocurrencies are appealing to all players who seek to trade a value outside of the legal financial system, in particular to money launderers, due to the anonymity and dispersed data storage that make transaction activities on blockchain exceedingly difficult to monitor. One of three methods may be used to buy a cryptocurrency. The first technique is known as mining, which necessitates the use of specialist hardware tools called "rigs" that are intended for the task. There are accessible both solitary mining rigs and "farms" with hundreds or even thousands of units. They are virtually lawful everywhere since they don't truly show illegal conduct. One further option is to use a legal bank account to make a purchase and transfer fiat money, use stock exchanges or VCE, or, after completing verification, make a cash purchase from a cryptocurrency ATM. The third method is buying or offering goods or services on a legitimate or illegitimate market. These goods and services can be against the law. The act of concealing financial assets allows for their usage without disclosing how illegally they were obtained. According to Kolachala, Simsek, Ababneh, and Vishwanathan (2021), "there are generally three stages in money laundering: placement, in which illicit money enters the system, layering, in which its sources are obscured, and integration, in which the illicit money is made to appear legal." A piece of code that specifies use guidelines, records transactions, and controls the creation and purchase of cryptocurrencies must be created in order to create a new form of money. The creator and issuer of the

virtual currency, such as the Canadian-Russian blockchain developer Vitalik Buterin for Ethereum or the enigmatic Satoshi Nakamoto for Bitcoin, is referred to as the administrator. Its whole functioning is controlled by publicly available open-source software. Code modifications are only possible with each link's support. As a result, the cryptocurrency serves just as a tool for the platform issuing it to actualize its larger purpose. It is neutral in this regard. The business concepts that drive cryptocurrencies are often created by a group of young scientists and inventors. Supporting programmes have been created in addition to the cryptocurrency's originator and administrator to make the system easier to access and utilise. Virtual Currency Exchange (VCE), a trading platform, allows commission-based exchanges of cryptocurrency to cryptocurrency and cryptocurrency to fiat with VCE or third parties. A crypto wallet, which might be software or a USB stick, allows one to store and transfer bitcoin..

.

7. Money laundering mechanisms by using cryptocurrency market

Cryptocurrency markets may be subject to a variety of criminal and financial behaviour. However, rather than on the blockchain or its infrastructure, the bulk of these illegal activities occur in the ecosystem of cryptocurrency issuers, VCEs, and wallets that provide users' access to blockchain. To buy and sell bitcoin using VCE, one needs a bank account in order to transmit fiat money (USD) to an exchange office in return for bitcoins. Additionally, a bank account is credited with the appropriate amount of fiat money whenever Bitcoins are bought at VCE. The bank is aware of the identity of the account owner and every transaction they have made, providing a comprehensive picture of the scope of the account owner's company. If the amount of trade is large and transactions are frequent, the bank alerts the account owner to governmental agencies for money laundering control. Owners of illicit funds use Bitcoin traders' services to avoid this issue. Such modern money laundering practises may hinder the expansion of the private sector and the promotion of entrepreneurship, as well as contribute to economic instability on a national and international level (Bjelajac, 2011). the knowledge of illegal behaviour If obtained money could be "laundered" via cryptocurrencies, especially Bitcoin, the social cohesion of a society would be destroyed by the increase of gaming and crime (Bjelajac, 2017). Due to the anonymity and complexity of transactions made through VCE, as well as the use of Bitcoin mixers, cryptocurrency traders, and other tools for hiding the trail of illegally obtained funds, corruption, one of the biggest problems facing modern democracies, thrives in these environments (Bjelajac, 2015). Many commercial enterprises have created instruments for assessing criminal activity on the Bitcoin network and are experts in deanonymizing Bitcoin transactions. As a result, terrorist organisations have been dissuaded, and current forensic investigations have not revealed a wide strategic purpose on the partof terrorist organisations to access anonymous online financial transactions and employ Bitcoin mixers like CoinJoin and DarkWallet.

7.1 Bitcoin trader

A bitcoin trader is an individual who frequently engages in large-scale transactions involving the buying or selling of bitcoins for cash, often at a high commission rate of up to 15% of the transaction value. These transactions typically involve the transfer of funds from a centralized exchange (VCE) to the trader's bank account, despite the absence of any explicit business activities conducted in bitcoin.

Bitcoin traders typically utilize online forums or platforms to connect with potential buyers and sellers of bitcoins. The bitcoins involved in these transactions are often obtained through various forms of criminal activity, including illegal gambling, the sale of illicit weapons, drug-related activities, cybercrime, and hacking services. In the money laundering process, the bitcoin trader acts as an intermediary for criminals, facilitating the conversion of illicit funds into a more easily transferable and less traceable form.

To carry out the transaction, a public location with free Wi-Fi and a large population, where both parties feel safe, is chosen for the meeting between the bitcoin seller and the trader. In these face-to-face encounters, online bitcoin transactions occur rapidly and nearly instantly. Once the seller sends the bitcoins directly to the trader's cryptocurrency wallet, the trader receives the agreed-upon cash equivalent from the sale, completing the deal. Shortly after selling bitcoins on the VCE and transferring the fiat money to their bank account, traders swiftly withdraw the cash.

By engaging in this process, the bitcoin trader fulfills their demand for cash and can subsequently purchase bitcoins of questionable origin once again. Such traders are generally regarded as criminals who facilitate money laundering activities, particularly if their involvement leads to substantial sums of fiat currency. Law enforcement agencies are responsible for investigating these illicit activities. The need for bitcoin traders would diminish if bitcoin were widely accepted as a means of payment for various goods using private cryptocurrency wallets, as this would eliminate the need for intermediaries and allow for the mystery of bitcoin's origin to remain intact..

7.2 Bitcoin mixer

Bitcoin mixers, also known as mixing services, are online services that aim to obfuscate the origins and transaction history of Bitcoin. By utilizing a mixer, users can make their Bitcoin transactions more private and anonymous. The mixer achieves this by mixing the

user's Bitcoin with other coins from a reserve pool maintained by the mixing service provider, such as Bitcoin Laundry.

Bitcoin's blockchain is a public ledger where all transactions are recorded. This transparency allows anyone to trace the history and origin of Bitcoin transactions. However, when using a mixer, the transaction history becomes invisible and irretrievable. The mixer replaces the user's bitcoins with coins from the reserve pool, making it difficult to trace the ownership and previous transactions of the mixed coins.

The primary purpose of a Bitcoin mixer is to enhance privacy and anonymity. While there are legitimate reasons for individuals to desire privacy in their financial transactions, such as protecting personal information and preventing potential targeted attacks, it's important to note that criminals also exploit mixers to launder illicitly obtained funds. By mixing their "dirty" money with other bitcoins, criminals attempt to obscure the source of their funds and make them appear legitimate.

However, it's crucial to recognize that the use of mixers itself is not inherently illegal. Many individuals and businesses may have legitimate reasons to use mixers, such as protecting their financial privacy or preventing targeted surveillance. Mixers provide a means to enhance privacy, but they can also be misused by those engaging in illegal activities.

It's important to adhere to local laws and regulations regarding financial transactions and to use services like Bitcoin mixers responsibly and within the bounds of the law..

7.3 Bitcoin conversion and its investment into

The introduction of NFT (non-fungible token) tokens on the Ethereum blockchain has opened up a new avenue for money laundering. NFT tokens represent the unique value of digital and physical assets, such as artwork and virtual property in the Metaverse, which can be converted into fiat currency by selling them on the open market. This process presents several steps that facilitate the laundering of illicit funds:

1. Criminals acquire Bitcoins through illegal means and convert them into Ether through a centralized exchange (VCE). The Ether is then transferred to a virtual wallet.
2. An anonymous account is created on a platform like OpenSea, which specializes in trading NFT tokens.
3. A high-value NFT, ranging from small to significant amounts, is chosen for purchase. For example, the NFT art piece "Everydays: the First 5000 Days" by Beeple was sold for a substantial amount.
4. The transaction takes place using virtual wallets, similar to legitimate transactions on authorized platforms.
5. After the NFTs are sold, the "laundered" Ether returns to the crypto wallet, is exchanged for fiat currency on the VCE, and then withdrawn in smaller amounts or from different accounts into a legitimate bank account.
6. NFTs on platforms like OpenSea can be exchanged for other NFTs and resold multiple times, creating a complex trail of transactions that makes it challenging to trace the flow of funds.
7. The ability to divide a large sum of Bitcoins into smaller quantities of NFTs within a virtual wallet provides an additional opportunity for laundering illicit funds.

In summary, the process described above illustrates how NFTs can be utilized to launder illicit money, as the multiple transactions and conversions involved make it difficult to track the origin and movement of the funds.

7.4 Money laundering typologies

Cryptocurrencies can be utilized for money laundering through various methods, including the following:

1. Withdrawing large amounts of fiat currency in cash from bank accounts without a legitimate reason or receiving substantial non-cash payments in fiat currency from the sale of virtual currencies on Virtual Currency Exchanges (VCE). These frequent and significant transactions without proper justification may indicate potential money laundering activities.

2. Engaging in anonymous transactions by purchasing virtual currencies through unidentified sellers on websites. The buyer pays in cash, often in a public setting, using a high transaction fee in exchange for Bitcoins. If the transaction lacks convincing legal or economic justification and involves an amount greater than what the seller typically requires for personal needs, it raises suspicion of potential money laundering.

3. Utilizing "mixer" services before or after selling Bitcoins. These services aim to obfuscate the transaction history and origins of the Bitcoins, making it challenging to trace the funds back to their original source. The use of mixers can be an indicator of attempts to launder money through cryptocurrency transactions.

4. Laundering "dirty" money by repeatedly buying and selling Non-Fungible Tokens (NFTs). In this scenario,

individuals who acquired Bitcoins through illegal means invest their funds in NFTs, thereby obscuring the trail of illicitly obtained funds. The continuous purchase and sale of NFTs can help launder and conceal the origins of the "dirty" money.

It is important to note that these methods can be ndicative of potential money laundering activities when used in suspicious circumstances. However, legitimate and legal transactions involving cryptocurrencies also exist, and it is essential to adhere to local laws and regulations when engaging in cryptocurrency-related activities.

7.5 State of global regulations on preventing moneylaundering – Regulatory approach of the USA

Under US federal law, cryptocurrencies can be classified in various ways, such as money, securities, or commodities (Allen & Overy, 2018). In the United States, the regulation of the cryptocurrency market primarily revolves around centralized exchange offices, also known as Virtual Currency Exchanges (VCEs). The Financial Crimes Enforcement Network (FinCEN) issued guidelines in 2013 that defined "virtual currency" as a form of value that serves as a substitute for traditional currency.

As a result, individuals or businesses involved in managing, exchanging, or utilizing virtual currencies through VCEs are categorized as Money Service Businesses (MSBs) and are subject to regulations outlined in the Bank Secrecy Act. It's important to note that FinCEN distinguishes between administrators and exchangers of virtual currencies and those who solely use them for purchasing goods and services. Furthermore, the law exempts companies that engage in buying and selling cryptocurrencies for their own operational requirements or on behalf of software developers who do not manage stock markets.

It's worth mentioning that the aforementioned legislation does not explicitly classify independent software engineers who create cryptocurrencies, promote them on their websites, and directly sell them to clients (e.g., through an Initial Coin Offering or ICO) as physical individuals under the Act.

Please note that cryptocurrency regulations may vary across jurisdictions, and it is essential to consult the specific laws and guidelines applicable in your jurisdiction or seek legal advice when engaging in cryptocurrency-related activities..

8. Conclusion

Although it is true that people use Bitcoin and other cryptocurrencies to launder money gained illegally, this practise is no more significant than other types of money laundering. The prejudice against cryptocurrencies and the crypto industry is mostly a result of the general public's ignorance of these incredibly complex and technically unclear fields. Since its inception, one of the biggest misconceptions about Bitcoin has been that it would provide the ideal form of payment for terrorists and criminals. The transaction log for Bitcoin is open, available anywhere, and unchangeable. Since every transaction will be recorded as long as Bitcoin is in use, the blockchain structure is not the best long-term solution for masked identities. This implies that using Bitcoin for any crime that includes a victim is not advised for criminals. Its pseudonymous nature suggests that even many years after a crime has been committed, addresses may be used to authenticate identities (Ammous, 2018). The hoopla around Bitcoin as a completely anonymous mode of payment has led to the exposure and imprisonment of several criminals, especially online drug dealers and child pornographers. Bitcoin has the potential to facilitate "crime without victims," in which the absence of victims discourages authorities from identifying the "criminal." This means that although crimes without victims, like online gambling and trying to hide one's assets, are likely to use Bitcoin in order to evade discovery, the same cannot be true for crimes like murder and terrorism. As indicated by the large number of drug buyers discovered by competent authorities, drug dealing over the internet using Bitcoin is likely driven more by addicts' desire than by common sense. According to Ammous (2018), while Bitcoin may provide a sense of freedom to criminals, it doesn't necessarily make committing crimes easier. One example of a crime that heavily relies on Bitcoin is ransomware, where attackers gain unauthorized access to computers and encrypt victims' files, demanding payment in Bitcoin to unlock them. It is important to understand that Bitcoin itself should not be feared but rather recognized as a part of a promising and peaceful future. It creates new opportunities for humanity but also presents challenges, which extend beyond the issue of money laundering that existed even before the emergence of Bitcoin.

References

1. Ali, M., & Bagui, S. (2021). Introduction to NFTs: The Future of Digital Collectibles. *International Journal of Advanced Computer Science and Applications*, *12* (10), pp. 50–53. Downloaded 2022, March 16 from https://thesai.org/Downloads/Volume12No10/Paper_7-Introduction_to_NFTs_The_Future_of_Digital_Collectibles.pdf
2. Ammous, S. (2018). *The bitcoin standard: the decentralized alternative to central banking*. John Wiley & Sons
3. Bitcoin Laundry. (n.d.). *Welcome to Bitcoin Laundry*. Downloaded 2022, March 10 from https://bitcoin-laundry.net/#whymix

4. Bjelajac, Ž. (2011). Pranje novca kao faktor ekonomske destabilizacijeu nacionalnim međunarodnim razmerama [Money laundering as a factor of economic destabilization in national and international measures]. *Poslovna ekonomija*, *5* (2), pp. 151–170
5. Bjelajac, Ž. (2012). Pranje novca kao prepreka afirmaciji preduzetništvai razvoju privatnog sektora u Republici Srbiji [Money Laundering as an Affirmation of Barriers to Entrepreneurship and the Development of the Private Sector in Serbia]. *Poslovna ekonomija*, *6* (1), pp. 347–371
6. Bjelajac, Ž. (2015). Korupcija kao izazov savremenog demokratskog društva [Corruption as a Challenge of Modern Democratic Society]. *Kultura polisa*, *12* (26), pp. 43–57
7. Bjelajac, Ž. (2017). Patološko kockanje i kriminal [Patological GamblingandCrime]. *Kultura polisa*, *14* (34), pp. 185–20
8. Brekke, J. K. (2019). *Disassembling the Trust Machine*: *Unpublished doctoral dissertation thesis*, Durham University, Geography Department. Downloaded 2022, March 17 from http://distributingchains.info/ wpcontent/uploads/2019/06/DisassemblingTrustMachine_Brekke2019. pdf
9. Ferreira, R. (2021), *The new blockchain technology applied to the State of Law*. Downloaded 2022, March 16 from https://www.academia. edu/65125909/The_new_Blockchain_Technology_ applied_to_the_ State_of_Law
10. Holman, D., & Stettner, B (2019). *Anti-money laundering regulationof cryptocurency: U.S. and global approaches*. ICLG – Anti-moneyLaunering Lows and Regulations. Downloaded 2022, March 10 from https://www.allenovery.com/germany/-/media/sharepoint/publications/ publications/en-gb/documents/aml18_allenovery.pdf
11. Kolashal, K., Simsek, E., Ababneh, M., & Vishwanathan, R. (2021). SoK: Money Laundering in Cryptocurrencies. *In: The 16th International Conference on Availability, Reliability and Security (ARES 2021)*, (pp. 1– 10), Vienna, Austria, https://doi.org/10.1145/3465481.3465774
12. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Downloaded 2022, March 15 from https://bitcoin.org/bitcoin.pdf
13. *Statista*. *Number of cryptocurrencies worldwide from 2013 to February 2022*. Downloaded 2022, March 15 from https://www.statista.com/ statistics/863917/number-crypto-coins-tokens/
14. Vigna, P., & Casey, J.M. (2018). *The truth machine. The blockchain andthe future of everything.* St. Martin's press