Bjelajac Željko*
https://orcid.org/0000-0003-4953-8779
Bajac B. Momčilo**
https://orcid.org/0000-0003-2115-6373

UDK: 004.738.5:(343.53:336.741.1)
Original scientific paper
DOI: 10.5937/ptp2202021B
Received: 07.05.2022.
Approved on: 17.06.2022.
Pages: 21–38

BLOCKCHAIN TECHNOLOGY AND MONEY LAUNDERING

ABSTRACT: In this paper, we want to break down certain prejudices against new blockchain technologies and cryptocurrencies, especially the Bitcoin, as instruments having mostly negative connotations and representing an opportunity for various criminal activities, including the cases of money laundering where money has been acquired in unethical and illegal ways. According to that aim, there were applied the methods of genetic, structural and functional analysis, the method of correlative variations, as well as the analogous and normative method. A significant part of the paper is dedicated to an introduction to DLT – (Distributed Ledger Technologies), i.e. a distributed book of records technologies, on which the blockchain and its most important exponent – the Bitcoin – rests. Also, we had to touch upon the second most important contribution to this technology, namely the Ethereum blockchain, which expands the perspectives opened by the Bitcoin, and thus the possibilities for misuse of this technology, primarily due to its constitutive principle of anonymity. In the paper, we have shown the fact that despite inadequate legislation, both nationally and globally, the blockchain and cryptocurrencies have not significantly supported the paths of illegal money laundering, especially not related to serious crimes, in particular drug trafficking and terrorism. We mostly see the contribution of this paper in the typologization of possible

* LLD, Full Professor, The University of Business Academy in Novi Sad, The Faculty of Law for Commerce and Judiciary in Novi Sad, Serbia, e-mail: zdjbjelajac@gmail.com
** PhD, Associate Professor, UNION Nikola Tesla University in Belgrade, The Faculty of Management, Sremski Karlovci, Serbia, e-mail: momcilo.bajac@famns.edu.rs

money laundering procedures, especially by using the NFT (Non-Fungible Tokens), non-exchangeable tokens whose hype, in last two years, might be the result of a perceived opportunity for a new way of money laundering. We conclude that we should not be afraid of the Bitcoin, but it should be accepted as an integral part of a peaceful and prosperous futurity for it opens new perspectives for humanity burdened with bigger problems than money laundering, which had existed to the same degree even before the appearance of the Bitcoin.

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

1. Introduction

Our old institutions, like the law, haven't evolved to keep pace with the rate of change (brought about by technology).

Google CEO Larry Page

The dynamic growth of the technology industry, which is becoming decentralized and global, is increasingly at odds with current national legislations aimed at providing people with legal certainty, as one of the primary principles of law.

The emergence of new technology called Blockchain can radically modify the way we think about legal norms and redesign basic concepts of law. Especially those concerning the issue of jurisdiction of courts "to guarantee the defence of the rights and interests of citizens, protected by law", and the issue of territoriality "in which the State exercises its power by attributing internal jurisdiction to facts that happen under its territory" (Ferreira, 2021, pp. 2–3), so legal certainty could be achieved when using this new technology. Blockchain's feature, as a supranational decentralized concept of algorithmic validation of information (financial and other transactions without built-in regulatory principles), to come into conflict with national civil law systems, in which the Law refers to clear and coherent norms, makes it difficult to understand this phenomenon.

In recent years, cryptocurrencies have emerged as a new phenomenon in the global financial system. Since the first decentralized cryptocurrency, Bitcoin, was released into the hacking community by a mysterious person or an entity under the pseudonym Satoshi Nakamoto in 2009, the total value of cryptocurrency in circulation and the variety of different types of

cryptocurrencies have increased dramatically. At the time of writing this paper, the global market capitalization of cryptocurrencies has exceeded two trillion dollars, half of which goes to Bitcoin and Ethereum.

Cryptocurrencies are becoming a very important source of wealth through mining or skilful trading on virtual stock exchanges, as well as starting businesses on platforms that gather start-up capital through the Initial Coin Offer (ICO). There is also a wide range of companies that are directly or indirectly involved in the development of cryptocurrency markets, such as cryptocurrency stock exchanges and exchange offices (VCE – Virtual Currency Exchange) and companies in retail, banking, video games and computing sectors. The growth of such markets has increased the interest of investors so many include cryptocurrencies in their investment portfolios (Tesla, Microsoft, Facebook).

"For regulated financial institutions ("FIs"), the opportunities presented by cryptocurrencies and distributed ledger technology ('DLT') are tied to significant operational and regulatory challenges" (Holman & Stettner, 2018, p. 26), the most significant being the fight against money laundering and terrorist financing. Key aspects of the cryptocurrency ecosystem differ from previous Internet-based platforms, primarily in terms of the degree of centralization. The decentralized Peer-to-Peer network allows owners of Bitcoin and other cryptocurrencies to avoid key control factors in the global Anti-Money Laundering (AML) regime. "The potential for mutual anonymity among counterparties can frustrate the Know-Your-Customer ('KYC') and customer identification procedures ('CIP') on which existing AML regimes depend" (Holman & Stettner, 2018, p. 26).

Most technological ecosystems, such as DLT, do not have special liability regimes. Who will be responsible for the damage caused by a situation in which users are damaged for hundreds of millions of dollars, as in the case of hacking of VCE Live Coin in December 2020? Given that DLT is just a technology that does not have coded principles of law in it, this question is not easy to answer. A classic example, in this case, are smart contracts that the law treats like any classic contract or signature, and are created on a decentralized platform, with an anonymous administrator, run by a self-executing algorithm without the possibility of revocation.

To understand the real place of cryptocurrencies in the processes that enable the laundering of illegally acquired money, it is necessary to get acquainted with the DLT on which they are created and maintained. In this paper, we want to break down prejudices against new blockchain technologies and cryptocurrencies, especially Bitcoin, as instruments that have mostly

negative connotations and represent an opportunity for various criminal activities, including laundering of money acquired in unethical and illegal ways. To that aim, the methods of genetic, structural and functional analysis, the method of correlative variations, as well as the analogous and normative method were applied.

2. The term blockchain

Blockchain technology is based on the ability of the algorithm to reach consensus in a decentralized network without resorting to external authority to testify and conduct the transaction. As such, blockchain technology not only solves some technical aspects of the system but also touches on very important societal issues of "trust", "authority" and "consensus". If the mathematical algorithm allows no one to have special control over the network and the transactions that take place in it, then it acquires the status of a neutral (trustless) mechanism for any potential application, facilitating connections between people. More precisely, a "blockchain" is an immutable irreversible linear chain of cryptographically hashed "blocks" on which transactions are recorded. This linear history of time-stamped events is verified and stored in a decentralized DLT-based manner, and network nodes "witness" transactions and reach consent on which transactions are considered regular through a consensus "Proof of Work" algorithm. The ability to reach consensus on transactions algorithmically, and not through the external mediation of an authority or a third party, gives blockchain the name "trust machine" (Vigna & Casei, 2018). In this case, the code replaces the law, intermediary person, institution or authority, and cryptographic evidence[1] ensures the authenticity of the record and organizes consensus. In such a way, transactions take place directly between participants, bypassing the control of financial institutions, and most importantly, the very creation of money is determined and executed through an immutable protocol, and not through government or state intervention. In fact, Bitcoin was the first to break the basic deception of Modernity, based on Keynesian and Marxist ideas "that government needs to manage the money supply" (Ammous, 2018,

[1] Cryptographic proof is the ability to prove something with mathematical certainty. This is what, in his Bitcoin White Paper, Satoshi Nakamoto means by an electronic system based on cryptographic evidence instead of trust. Data integrity is checked by mathematical probability, not by trusting an authority or someone's word. Add a timestamp and it can be proven when a given record was made. Hash them together into a "chain" or a "tree" referring to the hash output of the previous record, and you have a linear history of proven secure records, "a new block in the chain" (Nakamoto, 2008).

p. 136), which proves its continued success and disruptive power that caused a turmoil in the world of finance. The creation of Bitcoin by mining is built into the code which, by determining the weight of mining, dictates the pace of currency emission. "Bitcoin can thus be understood as a technology that converts electricity to truthful records through the expenditure of processing power" (Ammous, 2018, p. 219), whereby it generates cryptocurrency as a reward to miners for the money invested in processing power (hardware) and electricity consumed. By monetizing the processing power, Bitcoin has in fact become the largest single-purpose computer network in the world. This way, a part of the internet community creates a currency that is liquid and parries traditional fiat currencies issued and controlled by states. Hundreds of respectable cryptocurrencies and thousands of tokens have been created in the wake of Bitcoin over the last decade, with very creative ideas and successful business ventures behind them.

Mining is one of the most important activities in creating cryptocurrencies. It is in fact a transaction verification competition in which incentives aim to deter potential attackers from the system, through a consensus-based process of the Proof of Work.[2] This implies the introduction of economic dynamics, i.e. cryptocurrency in network security engineering, an area of crypto-economy that relies on incentives for decentralized or distributed protocol designs. The difficulty of the computer problem that miners solve is set so that it is solved on average every ten minutes, and for their "work" miners are rewarded with cryptocurrency. At the same time, this determines the rate of Bitcoin creation in the network, until a total of 21 million Bitcoins are in circulation, which will happen in the middle of the 22nd century. The "consensus" reached by the consensus algorithm should not be misunderstood as a kind of agreement on the truth of the event, but rather as an incentive-driven settlement, the truth of which is decided by random attempts to consume CPU power. The "fairness" of the consensus algorithm, or rather its legitimacy, does not lie in negotiations, the consensus of opinion or some notion of justice or objective truth, but in coincidence and large numbers that create an operational consensus of computers online (Brekke, 2019).

[2] Proof of Work is one of the lesser-known aspects of bitcoin architecture. It is a form of cryptographic evidence, which uses hashing. Nodes in the Bitcoin network must do some "work" which allows them to verify the transactions being tracked and then group them into blocks and let them pass through the SHA-256 hashing algorithm to produce a valid output. This computer "work" of hashing transaction data to find a valid way out is called *mining*, which is associated with gold mining.

Public key cryptography ensures that the message cannot be intercepted and can only be read by its authorized recipient. Cryptographic hashing is used to create a set of keys: one that can encrypt (the public key) and the other that can decrypt (the private key that is kept a secret). The public key encrypts messages sent to the owner; the owner then uses the private key to decrypt the messages (Brekke, 2019). The main goal of Bitcoin is to build a network without the need to trust any authority, third party or intermediary, which it perceives as a security weakness, unnecessary cost and potential uncertainty.

3. Basic characteristics of blockchain sensibility

The Internet has enabled Google, Facebook, Amazon, and Apple to connect the world under their guardianship. Blockchain will enable the connection of the world under the guardianship of the participants.

Jon Choi, Ethereum, 2017.

Decentralization. Decentralization is part of the network culture and involves distributed systems resistant to any form of control, censorship or extinguishing by any authority. We can also call it disintermediation. Technically, peer-to-peer systems such as Bitcoin are made up of network participants who communicate directly with each other. Unlike server-to-client models, where servers hold and deliver content to different clients, they do not exist in peer-to-peer networks. There is an important difference between decentralization conceived in blockchain network protocols and decentralization as an ethical, political, social or economic goal or principle that such a protocol may or may not support.

Openness. In a decentralized system, no entity can prevent individuals from joining the network as it is possible with traditional institutions, thus specially constituting the idea of neutrality.

Trust. Decentralized and open systems imply a certain level of mistrust. It is ideal to reduce the amount of needed trust as much as possible, approaching complete distrust and security. Relationships based on trust never have an absolute degree of certainty of outcome. Bitcoin is 100% based on verification and 0% on trust (Ammous, 2018, p. 174).

Immutability. The Bitcoin chain of blocks must be immutable, to function autonomously outside the control of any external authority. It is based on the idea of immutable code that is performed exactly as it is written. Immutability ensures that the consensus on the state of the network, reached by the consensus protocol on Proof of Work, cannot be changed arbitrarily.

Privacy. Computer technology provides the opportunity for individuals and groups to communicate with each other in a completely anonymous way. Privacy is the power to selectively reveal yourself to the world online with the help of cryptography, which is especially important at a time when the Internet is being used as an infrastructure for mass surveillance and narrowing the field of freedom. In case of Bitcoin, which operates on a peer-to-peer payment system, instead of a third party keeping records of transactions, the entire network does so, making all transactions completely public. To preserve privacy in such a radically transparent system, the computers themselves remain anonymous.

Anonymity. Anonymity is closely related Bitcoin was initially considered anonymous and infamously became a means of payment for "Darknet" and Internet black markets. However, the transaction can be tracked today until the moment of exchange and be deanonymized at this time. To avoid that and to cover the trail with "dirty" coins, coin mixers are used to "mix" transactions so that they cannot be traced directly to certain owners. Also, advanced cryptography and zero-knowledge proofs have developed currencies with much stronger anonymity, such as Z-Cash, Monero and more recently Nim, which have been developed specifically for anonymity purposes.

4. Ethereum blockchain and tokenization

What has completely revolutionized the concept of decentralization is the launch of the Ethereum blockchain, or blockchain 2.0. With this concept, the Ethereum Blockchain has expanded the possibility of transactions to all types of value, not just monetary transactions. Ethereum is a general-purpose blockchain that can have different types of applications running on it. The contribution made by the Ethereum blockchain is reflected in three things: first, the concept of smart contracts, second, a new stage in the evolution of the Internet, namely WEB3.0, and third, decentralized autonomous organizations (DAO).

Smart contracts are computer programs that are able to enforce the terms of an agreement between the parties without the need for human coordination or intervention. Smart contracts can define rules, like a regular contract, and automatically enforce them with code when pre-defined conditions are met. Smart contracts are self-executing, cannot be deleted, and interactions with them are irreversible. They opened the possibility of automating aspects of contract law and business management. The way transactions are verified and added to the blockchain guarantees its reliability. Execution and verification

of smart contracts require transaction fees paid in ETH, which is called "gas". Ether (ETH) is therefore the original coin of the Ethereum platform and the Ethereum blockchain.

Through WEB 3.0 (decentralized WEB), which is on blockchain, therefore fully distributed to a huge number of computers, it is possible to create decentralized applications (dApps) that run in a distributed way without the possibility of censorship or downtime.

And finally, decentralized autonomous DAO organizations are organizations that operate through rules coded as computer programs, already described above, as smart contracts. Based on these rules, they perform actions for the benefit of shareholders. DAO is a computer algorithm that applies ownership rights over tokens, contractual obligations, and business logic rules. Token owners accumulate power and capital by founding organizations with their own money and thus have real decision-making power.

However, one of the most important advantages of Ethereum blockchain platform is "its ability" for everyone "to create unique tokens" that exist and run on Ethereum blockchain (Ali & Bagui, 2021, p. 53). Unlike currencies and cryptocurrencies, which represent a value, tokens give their owner special rights or rights in relation to the issuer or record the ownership of property. Encryption of these rights over the blockchain is called "tokenization". You do not need to create a blockchain from scratch to create tokens. Instead, some existing blockchains, such as Ethereum or LimeChain, provide templates that allow the publisher to create their tokens. The Ethereum blockchain uses ERC (Ethereum Request for Comment) standards. There are three categories of tokens based on their functionality: currency tokens, aid tokens, and investment tokens.

Initial Coin Offers (ICOs) typically use blockchain technology to offer so-called "tokens" that can give different rights to their owners. The company publicly issues crypto tokens in exchange for funds that resemble an initial public offer (IPO), in which the company offers securities to the public on the stock market. Unlike (IPO), ICO usually happens in the very early stages of a project. In 2018, the Russian platform and social network Telegram, with its ICO offer and GRAM token, collected $1.7 billion from investors around the world, while the EOS decentralized platform on the blockchain raised $4.2 billion in the same year.

As soon as the publisher finishes creating the token, the tokens can be advertised and sold. Each token issuer offers a certain value to Internet communities. It is a common market practice for an issuer to publish the so-called "white paper" on its website. Using smart contracts, any investor

around the world can exchange cryptocurrencies stored in his crypto wallet for new tokens. The advertising campaign relies primarily on social media channels, especially Twitter.

ERC-20 the standard allows easy creation, use and exchange of tokens based on Ethereum. ERC can be created by anyone, but it is up to the creator to clearly explain the standard to get the support of the internet community for their business idea.

The ERC-721 standard allows the creation of unexchangeable tokens. In this standard, each token is special and irreplaceable, has individual ownership and can be tracked separately online. These are the so-called NFT (Non-Fungible Tokens), which have revolutionized the crypto market in the last few years with a capitalization of over six hundred billion dollars.

ERC-1462, Base Security Token extends the ERC-20 standard and is interesting because it meets the requirements of the Financial Institution (FI) from the point of view of legal regulations in financial markets. ERC-1462 ensures compliance with securities and legal enforcement. ERC 1426 also includes KYC (Know Your Customer) and AML (Anti Money Laundering) regulations, and the ability to lock tokens and restrict their transmission due to a legal dispute (Ali & Bagui, 2021, p. 54).

Token-based economies are enabled by a system that pays for its maintenance, thus technically and economically disrupting the existing centralized Internet infrastructure models. Blockchain makes organizations and communities economically sustainable, thus creating a user economy independent of massive financial systems and institutions that impose their own rules and manipulate financial markets only in their interest. Cryptoeconomics is based on the inseparable relationship between economic concepts and technology. Blockchain protocol design encodes a set of economic ideas, which may eventually have political repercussions.

5. Key terms in AML processes

A cryptocurrency is a form of virtual currency, a digital representation of value that has several different functions: (1) medium of exchange (2) unit of account (3) storehouse of value. What distinguishes virtual currency from "fiat currency" as the national currency and "e-money" which is the digital representation of fiat currency, is the lack of legal status of the national means of payment (Holman & Stettner, 2018, p. 26). Virtual currencies can be convertible (equivalent to fiat currency) or non-convertible (tokens in video games or online communities), while administration can be centralized

(admin-controlled) or decentralized because it manages code such as Bitcoin and Ethereum (2018, p. 26). According to this taxonomy, Bitcoin is a typical convertible, decentralized virtual currency that uses cryptographic principles in transactions in the absence of intermediaries that guarantee the validity of the transaction, such as banks. Bitcoin, which was launched in early 2009, is the oldest and most well-known cryptocurrency, and many variations with different characteristics and purposes have been created since then. According to the Statista portal, in March 2022, there were 10,397 cryptocurrencies worldwide (Statista, 2022). Cryptocurrencies are increasingly accepted as a means of raising capital, as a variant of "crowdfunding", and similar to the already existing legal mechanism IPO (Initial Public Offer). The use of cryptocurrencies to raise capital for investment purposes through ICOs is very often in conflict with applicable securities laws and other financial regulatory regimes.

6. Money laundering and cryptocurrencies business

Due to the anonymity and distributed data storage, transaction activities on blockchain are very hard to follow, which makes cryptocurrencies attractive to all actors who wish to exchange a value outside the legal financial system, primarily to money launderers.

You can obtain a cryptocurrency in three ways: the first one is through mining by having hardware equipment, the "rigs" specially constructed for this purpose. There are individual rigs or "farms" for mining of hundreds or even thousands of rigs. They are mostly legal in all countries because they themselves do not present a criminal activity. Another way is by purchasing through stock markets or VCE, by transferring fiat currency from a legitimate bank account, or by purchasing at a crypto ATM for cash, with previous authentication. The third way is by selling/purchasing of product or service on the legal or black market. Such products and services could be illegal.

Money laundering means that financial property is being hidden so it could be used without revealing illegal activities through which it was gained. "Broadly, there are three stages in money laundering, *placement*, in which illicit money enters the system, *layering*, in which its sources are obfuscated, and *integration* in which the illicit money is made to appear legal" (Kolachala, Simsek, Ababneh, & Vishwanathan, 2021, p. 2).

To create a new cryptocurrency, it is necessary to develop a code that establishes rules for its use, keeps the book of records and manages issuance and purchase of cryptocurrency. The administrator of the virtual currency is

a person or an entity that creates and issues virtual currency into circulation, such as the anonymous Satoshi Nakamoto is for Bitcoin, or Vitalik Buterin, a Canadian-Russian blockchain developer, is for Ethereum. After released into circulation, it runs on an open-source software that manages all of its functions. A change in code is possible only with the consensus of all participants in the chain. Therefore, the cryptocurrency itself is neutral, it is merely an instrument of a broader concept of the platform that emits it. Oftentimes original and creative business ideas with a team of young scientists and innovators can be found behind cryptocurrencies.

Besides the creator and the administrator of cryptocurrency, supporting applications have been developed to ease the access to and the use of the system.

- A crypto wallet is a software application or a USB stick that enables the owner to store and transfer cryptocurrency.
- Virtual Currency Exchange (VCE) is a platform for trading that, with a commission fee, enables exchanges of crypto-crypto and crypto-fiat with VCE or third parties via VCE.

7. Money laundering mechanisms by using cryptocurrency market

The cryptocurrency markets are potentially vulnerable to a wide spectre of criminal activities and financial crime. However, most of these criminal activities do not occur on the very blockchain and its infrastructure but in the surrounding ecosystem of cryptocurrencies' issuers, VCE and wallet, which support consumers' access to blockchain.

To buy and sell Bitcoin through VCE one needs a bank account to transfer fiat currency (USD) to an exchange office, in exchange for Bitcoins. Also, when Bitcoins are being sold at VCE, equivalent value in fiat currency is being transferred to a bank account. The identity of the account owner and all of their transactions are known to bank, which creates a clear picture about the scope of trade of person in question. In case the scope of trade is large and transactions are made often, the bank reports the account owner to government institutions for money laundering control. To avoid this scenario, owners of dirty money use services of Bitcoin traders.

Such modern tendencies in manners of money laundering can be a factor in an economic destabilization of national and international dimensions (Bjelajac, 2011), as well as an obstacle to affirmation of entrepreneurship and private sector's development (Bjelajac, 2012). The knowledge that illegally

obtained money could be "laundered" by using cryptocurrencies, primarily Bitcoin could significantly contribute to an expansion of gambling and crime in a community that would break its social cohesion (Bjelajac, 2017). Anonymity and complexity of transactions through VCE, use of Bitcoin mixers, cryptocurrencies traders and other mechanisms of hiding the trail of illegally obtained money is fertile ground for complicating the phenomenon of corruption as one of the biggest challenges of modern democratic society (Bjelajac, 2015). A number of private companies is specialized in the deanonymization of Bitcoin transactions and developing tools for analyzing illegal activities on the Bitcoin network. This has discouraged terrorist groups, so present forensic investigations have not shown a broad strategic intention of terrorist groups to access anonymous online financial transfers and use Bitcoin mixers, such as CoinJoin and DarkWallet.

7.1. Bitcoin trader

A Bitcoin trader is a person who buys or sells Bitcoins for cash with a big commission fee (up to 15% of transaction value), taking on the risk to be recognized by the investigative authorities because of frequent transactions that always end in large amounts being transferred from VCE to their bank account, even though there are no business activities that they visibly charge in Bitcoins to other persons. Bitcoin seller and Bitcoin buyer get into contact through a web forum or platform. These Bitcoins almost always come from illegal activities of all kinds, such as arms dealing, drugs, cybercrime, hacking services, child pornography, gambling, etc. In such cases Bitcoin trader represents the connecting link in the process of money laundering for criminals. Bitcoin seller and Bitcoin trader then meet in a public space with free Wi-Fi and where both parties feel secure because of the number of people present there. Bitcoin transaction is done very quickly, almost instantaneously, at that place over the internet. The seller transfers Bitcoins directly into the crypto wallet of the trader, after what the trader gives the seller the agreed equivalent value in fiat currency in cash. At this point, the transaction is finished. After selling Bitcoins on VCE and transferring fiat currency to their public bank account, traders immediately withdraw money in cash (Wisser, 2021). This way, the trader secures their need for cash so they could again buy Bitcoins of suspicious origin. Bitcoin trader that corresponds to the aforementioned profile will generally be considered criminal trader that aids criminals by facilitating the process of money laundering. As long as large amounts of cash in fiat currencies are the end result of such trade, actor will be accessible

to the investigative authorities. Only if Bitcoin were broadly recognized as a means of paying for other products through anonymous crypto wallets, its origin would remain unknown and there would be no need for Bitcoin traders.

7.2. Bitcoin mixer

Bitcoin mixer is an online "mixing service" of Bitcoin with the aim to hide the trail of its origin, with a compensation fee of up to 3,5% of the total Bitcoin amount. Thanks to the constitutive principle of transparency, all Bitcoin transactions on blockchain are public so it is possible to track their history and origin. By using a mixer, history of transactions becomes invisible and cannot be reconstructed. A mixer is designed so that Bitcoins received after "mixing" come from a reserve fund of the mixing service provider, such as Bitcoin Laundry, which completely and permanently hides the identity of the owner even from the most trained forensic investigators. "Bitcoin Laundry is here to help you keep your bitcoin transactions anonymous and private. When you mix bitcoin with us, we exchange the bitcoins you send us with coins from our reserve pool that can't be traced to your identity or your previous transactions. To be extra safe we also offer options to delay your payout and send it to multiple addresses. We keep our fees low and reserve pools large to make sure we can always give you the best possible Bitcoin mixer service" (Bitcoin Laundry, n.d.). Since there are legitimate reasons for using "mixers", their work is not against the law, and therefore their services are being abused by criminals for laundering "dirty" money.

7.3. Bitcoin conversion and its investment into NFT tokens

Another possibility for money laundering appeared with the emergence of the previously described NFT tokens on Ethereum's blockchain. NFT tokens are non-fungible tokens that represent a unique value of both digital and physical things, mostly artwork, ownership on Metaverse and many other digital values that can eventually be turned into fiat currencies by selling them on the market. The mechanism functions as follows: Bitcoins obtained through illegal actions of any kind or purpose are converted into Ether on the VCE, which is then deposited in the virtual wallet. A platform for trading in NFT tokens, such as OpenSea, is visited and an anonymous account is opened there. One of the NFTs is chosen in value from 1 to 70 million USD (e.g. NFT digital art photograph by an anonymous author Beeple, "Everydays: the First 5000 Days", was sold for 69,3 million dollars). Purchase is done from a virtual

wallet, as on every other legal platform, which then makes the transaction completed. With the final sale of NFTs, "laundered" Ethers return to the crypto wallet, are sold on the VCE for fiat currency, which is then withdrawn from a legal bank account in many smaller amounts or from different accounts. On the OpenSea platform, NFTs can be sold countless times and exchanged for other NFTs, which leads to the loss of trail of money invested after several cycles. Particularly the possibility to divide a large amount of Bitcoins in a virtual wallet into many small amounts of NFTs presents an exceptional opportunity for laundering "dirty" money.

7.4. Money laundering typologies

Consequently, there are four types of possible money laundering by using cryptocurrencies:

1. Possible money laundering could be indicated by frequent withdrawals of larger amounts of fiat currency in cash from bank accounts, without any obvious necessity, in combination with frequent non-cash receipts of large amounts in fiat currency to bank account, which originate from sale of virtual currencies on the VCE.
2. Buying virtual currencies – when a buyer anonymously offers their services over the internet websites to an unknown seller, then in a public space pays in cash the equivalent of Bitcoins with a high commission fee, without convincing legal or economic explanation for the reason for the transaction, in an amount that exceeds average private necessities of the seller (Wisser, 2020).
3. Buyer or seller use Bitcoin "mixer" services before or after selling Bitcoins.
4. Owner of illegally obtained Bitcoins invests into NFT and through many cycles of purchasing and selling NFTs hides the trail of "dirty" money.

8. State of global regulations on preventing money laundering – Regulatory approach of the USA

For the purposes of the US federal law, cryptocurrency may be considered differently, as a currency, security or a commodity (Allen & Overy, 2018). Framework for regulation of AML in the field of cryptocurrencies in the USA is most developed for centralized exchange offices, VCE. In 2013, FinCEN (Financial Crimes Enforcement Network) published guidelines, where it

is concluded that "virtual currency" is a form of "value that substitutes for currency" and that exchange offices or specific persons who administrate, exchange or use virtual currencies are therefore qualified as Money Service Businesses (MSB), regulated by the Bank Secrecy Act (Allen & Overy, 2018). It is important to emphasize that FinCEN made a distinction between those who only use virtual currency for buying commodities and services and those who exchange and administrate virtual currency, whereby they exempted from the law companies that purchase and sell cryptocurrencies for their own needs or for the needs of software programmers who also do not manage stock markets. This Act did not define the position of independent software developers as physical persons who create cryptocurrencies, which they then promote on their websites and sell directly to the consumers (e.g. like ICO).

9. Conclusion

Use of Bitcoin and other cryptocurrencies for laundering illegally obtained money is a fact, but no more significant than other types of money laundering. Much prejudice that exists about cryptocurrencies and crypto economy is a result of insufficient informing and knowledge about these truly complex and technically unclear categories for most people. One of the most frequent misconceptions about Bitcoin from its inception is that it would be an excellent currency for criminals and terrorists. Bitcoin's book of records on transactions is public, globally available and unchangeable. It will have records of every transaction as long as Bitcoin is functioning, so blockchain structure is not ideal for hiding one's identity in the long run. This means that for any crime that indeed has a victim it would not be recommendable for criminals to use Bitcoin. Its pseudonym nature signifies that addresses can be connected to true identities, even many years after a crime was committed (Ammous, 2018). Many criminals, but mostly online drug dealers and child pornography traders, have been identified and arrested because they got caught up in the hype about Bitcoin as a completely anonymous means of payment. Bitcoin can be useful in enabling "crime without victims", where the absence would not motivate investigative authorities to establish the identity of the "criminal". Therefore, it may be expected that crimes without victims, such as online gambling and avoiding control over one's capital, will use Bitcoin in hopes of never being identified, but the same cannot be claimed about murder and terrorism. Drug dealing over the internet by using Bitcoin most probably occurs more because of the addicts' desire than common sense, which is proved by a large number of drug buyers identified by competent

authorities (Ammous, 2018). In other words, Bitcoin will most probably increase the feeling of freedom for criminals, but it would not necessarily facilitate committing crimes. One type of high profile and high-profit crime, which used Bitcoin to a large degree, is ransomware, such as for example, CerberRansomware: a method of unauthorized access to computers that codes victims' files, "locks" them in folders and releases them only if the victim pays the required amount, usually in Bitcoins. Bitcoin is not something to be afraid of but something that should be accepted as a part of a peaceful and prosperous future, something that opens new perspectives to the entire mankind, which has far greater problems than money laundering that existed in the same proportions even before Bitcoin.

Bjelajac Željko
Pravni fakultet za privredu i pravosuđe, Univerzitet Privredna akademija u Novom Sadu, Srbija

Bajac B. Momčilo
Fakultet za menadžment,Univerzitet UNION Nikola Tesla u Beogradu, Sremski Karlovci, Srbija

BLOKČEJN TEHNOLOGIJE I PRANJE NOVCA

REZIME: U ovom radu želimo da razbijemo predrasude prema novim blokčejn tehnologijama i kriptovalutama, posebno Bitkoinu, kao instrumentima koji imaju pretežno negativne konotacije i predstavljaju priliku za razne kriminalne aktivnosti, uključujući i pranje novca stečenog na neetički i nezakonit način. U tom cilju, primenjene su metode genetičke, strukturne i funkcionalne analize, metoda korelativnih varijacija, kao i analogna i normativna metoda. Značajan deo rada je posvećen upoznavanju sa DLT – (*Distributed Ledger Technologies*), odnosno tehnologijama distribuirane knjige zapisa, na kojima počiva blokčejn i njegov najznačajniji eksponent – Bitkoin. Takođe smo morali da se dotaknemo i drugog najznačajnijeg doprinosa ovoj tehnologiji, a to je Ethereum blokčejn, koji proširuje perspektive koje je otvorio Bitkoin, a time i mogućnosti za zloupotrebe ove tehnologije, pre svega zbog njenog konstitutivnog principa anonimnosti. U radu smo pokazali da i pored neadekvatne zakonske regulative, kako na nacionalnim tako i na globalnom nivou, blokčejn i

kriptovalute nisu u značajnoj meri potpomogle puteve nezakonitog pranja novca, pogotovo ne u vezi sa teškim krivičnim delima, posebno trgovinom narkoticima, kao i sa terorizmom. Doprinos ovoga rada najviše vidimo u tipologizaciji mogućih postupaka pranja novca, pogotovo korišćenjem NFT (*Non Fungible Tokens*), nerazmenljivih tokena čiji hajp u poslednje dve godine može biti i rezultat uočene prilike za novi način pranja novca. Zaključujemo da se ne treba plašiti Bitkoina, već ga treba prihvatiti kao sastavni deo mirne i prosperitetne budućnosti, jer otvara nove perspektive čovečanstvu opterećenom većim problemima od pranje novca, koje je u istim razmerama postojalo i pre pojave Bitkoina.

Ključne reči: *Bitkoin, pranje novca, Distributed Ledger Technologies, algoritam, Ethereum.*

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 destabilizacije u 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 preduzetništva i 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 Gambling and Crime]. *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 regulation of cryptocurency: U.S. and global approaches*. ICLG – Anti-money Launering 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 and the future of everything.* St. Martin's press