

BlockChain Technology and Money Decontaminating

Dr Anitha K¹, Sasi Priya S², Affreen A³

¹Associate Professor, Department of Information Technology, Arunai Engineering College, Tiruvannamalai Tamilnadu, India
Email: ani16ram@gmail.com

^{2,3} UG Students, Department of Information Technology, Arunai Engineering College, Tiruvannamalai Tamilnadu, India
Email: psasi5703@gmail.com², affreena03@gmail.com³

Abstract:

Blockchain is considered to be the top emerging fields in the current scenario. It is considered to be one of the most secure technologies to keep data safe. A block chain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. In this paper, we want to break down certain narrow mindedness against new blockchain technologies and crypto currencies, exclusively the Bitcoin, as it has mostly undesirable immoral including cases of money decontaminating where money has been acquired in unprincipled and illicit 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. 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 illicit money decontaminating, especially not related to solemn misconducts.

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

I. INTRODUCTION

Blockchain technology, considered to be one of the most secure technologies to keep data safe, is constructed on blocks of data. Blockchain technology is fast, public, cheap, easy to use, transparent and programmable technology that allows for the transfer of information and/or financial possessions instantaneously from one part of the world to another. Blockchain expertise can comprise any type of data and the link among individually block and the next is called a chain because the blocks are linked in a method that cannot be altered. The information is recorded in the blockchain, it becomes infeasible to alter it i.e. immutability. Used for storing bank records or transactions. To understand this first understand what is stored in a single block. Each block

contains three types of info, the data, its hash, and a pointer to the hash of the previous block. For example, bitcoin stores information about the transactions of bitcoins, such as the sender, the receiver, and the amount of bitcoin that is transferred. The hash of the block is a unique identifier. Each block’s hash will be different based on the data that is stored in it, so if the data gets changed the hash also changes. The addition of the previous block’s hash is the main reason behind the success of blockchain technology and this is also why the alteration of data kept in the blockchain develops impracticable. If one wants to change the blockchain by altering the data kept in a block, this will also central to alteration in the hash of the block, which will accordingly not match with the hash that is in its next block, causing a chain reaction. So, any alteration in a single block will

overturn the whole blockchain. We repetitively see new applications based on blockchain technology and we will get more familiar with them as they become part of our daily lives. Blockchain technology has the potential to upgrade any system that requires a third-party regulatory authority that serves to define the authenticity of any changes that will take place in the system. A digital ledger was announced that would be spread to each node present in the blockchain to keep track of all the transactions that were taking place in an organization. The development of bitcoin has radically changed the concept of money and currency Bitcoin is the first-ever form of a digital asset or money that not only has no backing or intrinsic value but also no centralized issuer or controller. This is where the nodes were not only keeping track of the transactions, but they could also program and execute software, hence taking the name of smart contracts. It more resourceful for many more applications. 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.

II. BASIC CHARACTERISTICS OF BLOCKCHAIN SENSIBILITY

- A. Decentralization:** In blockchain, decentralization refers to the transfer of control and decision-making from a centralized entity to a distributed network. Decentralized networks strive to reduce the level of trust that participants must place in one another, and frighten their ability to exert authority or control over one another in ways that degrade the functionality of the network. Technically, peer-to-peer systems such as Bitcoin are made up of network participants who communicate directly with each other.
- B. Openness:** In a decentralized system, no entity can prevent individuals from joining the network as it is possible with outdated establishments, thus specially constituting the idea of detachment.
- C. Trust:** Decentralized and open system implies mistrust. It secures the chain using specific protocols. Validating the transactions and blocks for tamper

proofing. Bitcoin is 100% based on verification and 0% on trust.

- D. Immutability:** The Bitcoin chain of blocks must be immutable. It is based on the idea of immutable code that is performed exactly as it is written that can't be changed arbitrarily.
- E. Privacy:** Privacy is the power to selectively reveal yourself to the world online. 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 an intermediary 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.
- F. Anonymity:** Cryptocurrency transactions are recorded on a blockchain, which is generally public. At the same time, crypto trades are not necessarily linked to an identity, which provide a bit of anonymity for the users.

III. ETHEREUM BLOCKCHAIN

The concept of decentralization is revolutionized by the launch of the Ethereum blockchain, or blockchain 2.0. With this concept, the it has expanded the possibility of transactions to all types of value, not just monetary transactions. Ethereum is a all-purpose blockchain that can have different types of applications running on it. The contribution made by this 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). The technology enables functionality beyond digital currency, such as decentralized applications and smart contracts. The developer community is one of the largest. The Ethereum platform processes transactions faster than Bitcoin. Ethereum services are open by default – you just need a wallet. These are free and easy to set up, controlled by you, and work without any personal info. Ethereum is a blockchain and distributed platform designed for multiple uses. Ethereum is a decentralized blockchain platform that establishes a peer-to-

peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority.

The Ethereum blockchain is powered by its native cryptocurrency — an ether (ETH)— and enables developer to create new types of ETH-based tokens that power dApps through the use of smart contracts. The most common ETH-based cryptocurrencies are built on the ERC-20 token standard.

IV. KEY CONCEPTS OF AML PROCESS

A cryptocurrency is a form of computer-generated currency has several functions: (1) medium of exchange (2) unit of account (3) storehouse of value. It distinguishes virtual currency from “fiat currency” as the countrywide currency and “e-money” which is the digital representation of fiat currency. Computer-generated currencies can be adaptable (equivalent to fiat currency) or non-adaptable (tokens in video games or online communities), while administration can be centralized(admin-controlled) or decentralized as it manages code such as Bitcoin and Ethereum. 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 wide-reaching (Statista, 2022).

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 rules. Cryptocurrencies are considered to be an increasingly means of raising capital.

V. MONEY DECONTAMINATING AND CRYPTOCURRENCIES BUSINESS

Owing to the anonymity and circulated data storage, transaction happenings on blockchain are very tough to follow, which makes cryptocurrencies good-looking to all performers who wish to exchange a value outside the legal financial system, mainly to money launderers. Obtaining a cryptocurrency in three ways: the first one is done 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. Another way is by acquiring through stock markets or VCE, by transferring fiat currency from a sincere 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. “Broadly, there are three stages in money laundering; placement, in which illicit money enters the system, layering, in which its sources are complicated, and integration in which the illicit money is made to appear legal”. A change in code is possible only with the compromise 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. 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. Bitcoin conversion and its investment into NFT tokens.

VI. MONEY DECONTAMINATING MECHANISM BY USING CRYPTOCURRENCY MARKET

The cryptocurrency marketplaces are theoretically exposed to a wide spectre of criminal activities and financial crime. 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 A number of private companies is specialized in the deanonymization of Bitcoin transactions and developing tools for analysing illegal activities on the Bitcoin network.

a. Bitcoin Trader A Bitcoin agent is a person who buys or vends Bitcoins for money with big commission fee analytical establishments frequent dealings that always end in large amounts being transported from VCE to their bank account Bitcoin seller and Bitcoin consumer get into connection through a web forum or stage. These Bitcoins almost always come from illicit actions of all kinds, such as arms dealing, cybercrime, hacking services, gambling, etc. Bitcoin contract is done very quickly, almost rapidly, at that place done the internet. The seller transfers Bitcoins straight into the crypto wallet of the trader, after what the trader stretches the seller the agreed corresponding value in fiat currency in cash. At this point, the transaction is ended traders nearly extract money in cash.

b. Bitcoin Mixer Bitcoin connections on blockchain are civic so it is likely to trail their past and beginning. Bitcoin mixer is a working "mixing service" of Bitcoin with the goal to hide the trail of its origin, with a reward fee of up to 3,5% of the total Bitcoin sum. By using a mixer, past of dealings develops unseen and cannot be rebuilt. "Bitcoin Laundry is here to aid you save your bitcoin transactions nameless and remote. To be additional safe we also offer options to stay your payout and lead it to several addresses. Since there are genuine reasons for using "mixers", their work is not

in contradiction of the law, and therefore their facilities are being abused by prisoners for filtering "dirty" money.

c. Bitcoin conversion and its investment into NFT tokens Additional option for money laundering seemed with NFT tokens on Ethereum's blockchain. NFT tokens are non-fungible tokens that signify a exclusive value of both numeral and corporal things, mostly creation, possession on Metaverse and many other digital values that can finally be turned into fiat currencies by vending them on the market. On the Open Sea platform, NFTs can be vended countless periods and swapped for other NFTs, which mains to the loss of trail of money capitalized after several cycles. Mainly the possibility to divide a large amount of Bitcoins in a near wallet into many small amounts of NFTs offerings an exceptional chance for laundering "dirty" money.

VII.STATE OF GLOBAL REGULATIONS ON PREVENTING MONEY LAUNDERING

"Virtual currency" is a procedure of "worth that alternates for currency" and that exchange offices or exact persons who manage, exchange or use practical currencies. It is significant to underline that FinCEN made a difference between those who only use computer-generated currency for purchasing commodities and facilities and those who exchange and manage virtual currency. This Act did not describe the position of independent software developers as carnal persons who create cryptocurrencies, which they then encourage on their websites and vend straight to the consumers.

VIII.CONCLUSION

One of the furthestmost average misconceptions about Bitcoin from its commencement is that it would be an excellent currency for criminals and extremists. Bitcoin's book of records on dealings is civic, worldwide existing and unchangeable. For any crime that indeed has a victim it would not be recommendable for criminals to use Bitcoin. Bitcoin can be useful in enabling "crime without victims", where the nonappearance would not motivate exploratory 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 expectations of never being identified, but the same cannot be demanded about murder and terrorism. Bitcoin will most possibly increase the feeling of freedom for criminals, but it would not essentially facilitate committing crimes. Bitcoin is not somewhat to be afraid of but something that should be accepted as a part of a peaceful and well-off future, something that opens new outlooks to the entire mankind, which has far greater problems than money laundering that existed in the same scopes even earlier Bitcoin.

IX. REFERENCES

- [1] Ammous, S. (2018). *The bitcoin standard: the decentralized alternative to central banking*. John Wiley & Sons.
- [2] Bitcoin Laundry. (n.d.). *Welcome to Bitcoin Laundry*
- [3] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*
- [4] Statista. *Number of cryptocurrencies worldwide from 2013 to February 2022*
- [5] Holman, D., & Stettner, B (2019). *Anti-money laundering regulation of cryptocurrency: U.S. and global approaches*. ICLG – Anti-money Laundering Laws and Regulations.

[6] 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)*

[7] Bjelajac, Ž. (2011). [Money laundering as a factor of economic destabilization in national and international measures]. *5 (2)*, pp. 151–170

[8] Bjelajac, Ž. (2012). [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

[9] Vigna, P., & Casey, J.M. (2018). *The truth machine. The blockchain and the future of everything*.

[10] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Downloaded 2022, March 15 from <https://bitcoin.org/bitcoin.pdf>