https://doi.org/10.51483/IJCCR.3.1.2023.78-88

ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal
of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper **Open Access**

Ways to Regulate the Abuses of Blockchain and Cryptocurrency Over the Dark Web

Shiv Hari Tewari[1]*

[1]Assistant Professor, Sunstone Eduversity, India. E-mail: tewarishivhari999@gmail.com

Article Info

Volume 3, Issue 1, June 2023
Received : 14 January 2023
Accepted : 21 May 2023
Published : 05 June 2023
doi: 10.51483/IJCCR.3.1.2023.78-88

Abstract

The blockchain technology operates as a distributed ledger system, where users engage in transactions utilizing this method. It gained popularity following the sudden surge in the value of bitcoin in 2017, which led to widespread awareness of blockchain and its functioning. This technology offers both anonymity and security to users, making it attractive for cryptocurrencies like Bitcoin and the more recent Monero, as it ensures secure, untraceable transactions. Anonymity and security can serve beneficial purposes, such as protecting individuals' privacy and fostering freedom of speech. However, they can also be exploited for illicit activities, including cyber terrorism, where the perpetrators often evade accountability. While blockchains possess numerous positive qualities, they also have downsides. The heightened security and anonymity they provide have fueled illegal transactions and activities on the dark web. In this review paper, we explore the research conducted on the dark web and cryptocurrencies. We highlight the drawbacks of blockchain, the process of transactions on the dark web, and propose regulatory measures and the use of government-backed cryptocurrencies to monitor and curb illegal activities on the dark web.

Keywords: *Dark Web, Blockchain, Cryptocurrency, Regulation, Illicit activities, Anonymous transactions, RSBCs*

1. Introduction

In recent years, the Dark Web has emerged as a clandestine digital landscape where illicit activities thrive, fueled by the anonymity provided by blockchain technology and cryptocurrencies. The decentralized and secure nature of blockchain has facilitated anonymous transactions, making it a preferred platform for illegal trades, including drug trafficking, weapon sales, and cybercrime. As the Dark Web continues to evolve, it has become crucial to explore effective strategies for regulating the abuses of blockchain and cryptocurrency within this hidden realm.

This research paper aims to investigate and propose ways to curb the misuse of blockchain and cryptocurrency on the Dark Web. By analyzing the current state of affairs and the challenges associated with regulating this underground ecosystem, we seek to shed light on potential solutions that can mitigate the negative impact of these technologies on society.

* *Corresponding author: Shiv Hari Tewari, Assistant Professor, Sunstone Eduversity, India. E-mail: tewarishivhari999@gmail.com*

The first section of this paper delves into the unique features of blockchain technology, emphasizing its decentralized nature and the advantages it offers to users seeking anonymity. We examine the use of cryptocurrencies like Bitcoin and Monero, which have become prevalent forms of digital currency on the Dark Web, enabling untraceable transactions. Additionally, we explore the implications of the Dark Web's growth and the rise of anonymous websites that facilitate illegal activities.

Next, we delve into the concept of Regulated and Sovereign Backed Cryptocurrencies (RSBCs) as a potential solution for controlling illicit transactions on the Dark Web. The K-Y Protocol, a set of rules and instructions, serves as a foundation for implementing RSBCs and enabling traceability in the digital realm. We explore how RSBCs can leverage controlled blockchains to enhance transparency, identify the parties involved in illegal activities, and effectively regulate the Dark Web.

Furthermore, we examine the potential impact of implementing RSBCs on the Deep Web ecosystem. By envisioning a future where multiple sovereign states issue their own NationCoins, we explore how this system can significantly reduce unaccounted money and enable real-time identification of illegal trade. Additionally, the ability to tax and regulate the Deep Web could be enhanced through the tracking of money circulation.

This research article contributes to the ongoing discourse surrounding the regulation of blockchain and cryptocurrency misuse on the Dark Web. By examining the unique challenges posed by this hidden realm, we provide insights into potential approaches to address these issues effectively. It is our hope that this study will stimulate further discussions and inspire concrete actions toward establishing a safer and more accountable digital landscape.

2. Literature Review

The misuse of blockchain and cryptocurrency on the Dark Web has become a growing concern in recent years. This section provides an overview of existing research and literature related to the regulation of these technologies within the hidden realm.

Martin *et al.* (2017) explores the structure and functioning of Dark Web marketplaces, highlighting the prevalence of illicit activities such as drug trade and weapon sales. It emphasizes the need for effective regulation to curb the abuses facilitated by blockchain and cryptocurrency.

Alex *et al.* (2019) examining the challenges of regulating cryptocurrency transactions, this research proposes a decentralized framework that balances the need for privacy and law enforcement. It discusses the potential application of this framework to mitigate illicit activities on the Dark Web.

Sean *et al*. (2019) focusing on the issue of money laundering through Bitcoin, this study investigates the patterns and techniques used to obfuscate illicit flows. It emphasizes the importance of effective regulation and cooperation between law enforcement agencies and cryptocurrency service providers.

Xinyu *et al.* (2018) highlights the potential risks to anonymity posed by social network profiling. It discusses how combining social network data with blockchain transactions on the Dark Web can de-anonymize users, emphasizing the need for improved privacy protection mechanisms.

Svenja (2020) examines the regulatory frameworks for cryptocurrencies worldwide. It discusses different approaches to regulation, including licensing, taxation, and Know Your Customer (KYC) procedures, and highlights the importance of international cooperation in addressing Dark Web abuses.

Aaron (2018) investigates the intersection of cryptocurrency and cybercrime, including its impact on the Dark Web. It analyzes case studies and provides insights into the challenges faced by law enforcement agencies in tracking and combating illegal activities facilitated by blockchain technology.

Manoharan *et al*. (2020) exploring the manipulation of prices on Dark Web marketplaces, this research sheds light on the financial aspects of illicit transactions. It emphasizes the need for effective regulation to deter price manipulation and ensure fair market practices.

Dirk *et al.* (2019) examines the legal and regulatory challenges posed by cryptocurrencies, including their implications for combating money laundering, terrorist financing, and other illicit activities. It provides insights into the complexities of regulatory approaches and the need for international coordination.

3. Definition of Blockchain

Blockchain is a collection of blocks that store transaction details between two parties. It is designed to ensure the integrity and security of the recorded information, making it difficult or nearly impossible to alter or tamper with the system. In simple terms, a blockchain is a digital ledger system that records transactions. This ledger is duplicated and distributed across a network of computers, forming a decentralized database known as Distributed Ledger Technology (DLT). Each block in the blockchain contains a certain number of transactions, and whenever a new transaction occurs, it is added to the ledger of every participant. One of the key features of blockchain is its decentralized nature, where multiple participants manage the database. This distributed approach enhances security and prevents a single point of failure. Additionally, every transaction on the blockchain is secured with an unchangeable cryptographic signature called a "Hash."

DLT offers several important properties that make it valuable for ensuring secure transactions. Firstly, it provides anonymity to users involved in transactions, protecting their identities. Secondly, its distributed nature ensures that no single entity has complete control over the system, enhancing security. Lastly, the inclusion of timestamps in the blockchain enables precise tracking and verification of transaction history.

Figure 1 below illustrates the properties of DLT and demonstrates why it is beneficial for ensuring database security in today's digital landscape.

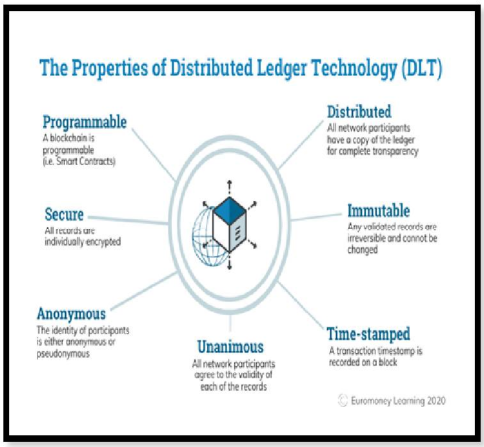
The Properties of Distributed Ledger Technology (DLT)
Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block
© Euromoney Learning 2020

Figure 1: Properties of Blockchain

Which means if one block in one chain is changed then it would be immediately apparent it had been tampered with? If intruders want to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions.

4. Relation of Blockchain with the Cryptocurrencies

There have been numerous attempts to create digital currencies in the past, but they all faced significant failures primarily due to their lack of reliability and issues of trust. For instance, if someone were to create a cryptocurrency called "X," there would be doubts about whether we can trust them not to grant themselves an excessive amount of "X" or potentially steal the existing "X" belonging to others.

Bitcoin was developed to address this trust problem by utilizing blockchain technology. Unlike traditional databases like SQL, where there is a central authority capable of altering entries (such as granting themselves a million X dollars), blockchain operates differently. It is decentralized and managed by the users themselves. Additionally, bitcoins cannot be counterfeited, hacked, or spent twice, ensuring that those who own this currency can trust its value.

In essence, blockchain is a reliable and secure system originally designed for digital currencies like Bitcoin. However, the tech community has discovered additional uses for it due to its ability to maintain user anonymity and facilitate secure transactions. While the anonymity provided by blockchain has its benefits, it has also become a tool for individuals engaged in illegal activities on the internet, such as the dark net.

5. What is Bitcoin

Bitcoin is a decentralized digital cryptocurrency that operates through cryptographic algorithms and a peer-to-peer network, allowing for a fully distributed ledger without the need for a central authority (Akdeniz, 2002).

Unlike traditional banking systems, the absence of a central authority in Bitcoin ensures that financial activities remain pseudonymous. Users can generate multiple accounts, known as public addresses, along with corresponding ownership verifiers called private keys, to send and receive bitcoins (BTC) using wallet software. This software facilitates payments and manages key pairs, enabling transactions over the Bitcoin network without revealing the real identities of the participants involved in each transaction.

To initiate a payment in Bitcoin, a user broadcasts a transaction over the Bitcoin network. For example, if Alice wants to send BTC to Bob, her wallet software searches for unspent transaction outputs (UTXOs) containing the desired BTC amounts and spending conditions. Each UTXO can be used as input in a new transaction, allowing Alice to spend the BTC on other Bitcoin addresses. If Alice possesses the necessary authentication information, such as private keys confirming ownership of the Bitcoin addresses with valid UTXOs, her wallet software creates a transaction signed with her private keys and broadcasts it on the Bitcoin network. Bitcoin users can transfer BTC to any valid public address for receiving or sending, although address reuse is not recommended for privacy and security purposes.

Upon receiving a transaction request, Bitcoin nodes verify the cryptographic validity of the transaction and add it to the Bitcoin Mempool if it passes verification. When creating a new Bitcoin block, nodes gather a set of transactions from the Mempool, arrange them into a block, and engage in a mining process to solve a mathematical equation known as Proof of Work (PoW). If a node successfully solves the math problem and the solution is verified by other nodes, the new block is then linked to the Bitcoin Blockchain.

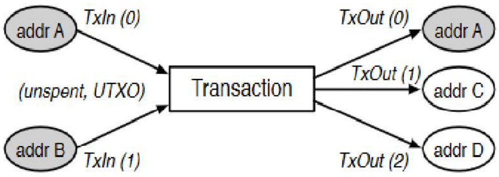

Figure 2: An Example of a Bitcoin Transaction Between Alice and Bob. The Gray and White Ovals Indicate the Public Bitcoin Addresses Owned by Alice and Bob Respectively

Figure 2 depicts an example transaction where Alice sends BTC to Bob and returns the remaining BTC to herself. The transaction includes a list of inputs (Tx In) referencing Alice's public addresses connected to unspent transaction outputs (UTXO) and a list of outputs (Tx Out) representing the destination public addresses belonging to Alice and Bob. In this scenario, Alice transfers a specific amount of BTC to Bob's public addresses (addr C and D). As per the Bitcoin protocol, the total value of inputs must match the total value of outputs, which is why Alice sends the remaining BTC back to the same address used in Tx In(0).

6. What is Dark Web

The dark web (Hegadekatti *et al.*, 2016) also known as the dark net or deep web is a place where questionable activities used to run. The dark web in itself is several times bigger than the general indexed net(also called the surface web) which is known to us over time. This means that it is not visible on the search engines like google and bing.

7. What Kind of People Access the Dark Web

The dark web attracts a significant number of individuals, but the primary users are those engaged in illicit activities. A study conducted in 2014 at Portsmouth revealed that the most sought-after content on the dark web includes child pornography, followed by drugs and unlicensed weapons (https://www.darpa.mil/program/memex). Furthermore, it was discovered that people utilized the dark web to acquire illicit information and even hire hitmen for criminal purposes. Based on our research, we have come across certain websites on the dark net market. One example is **besamafia**, which serves as a platform for hiring hitmen. Another website, called **doxtor**, offers products created by Apple that were not officially released in the market (Hegadekatti *et al.*, 2016). These are just a few examples among many similar websites found on the dark net market. These websites typically utilize bitcoin as a payment method and employ PGP keys for communication.

However, it is important to note that the dark web is not solely dedicated to illegal activities. For instance, platforms like **WikiLeaks** provide a means for individuals to anonymously share classified information with relevant authorities for whistleblowing purposes. Additionally, the dark web has also facilitated access to certain websites for individuals in China, where such sites may be otherwise inaccessible.

8. Encryption and Anonymity on the Dark Web

Most users on the dark web make use of sophisticated encryption technologies. One example is the use of Virtual Private Networks (VPNs) which keep the activities on the internet safe and private. The conventional routing of the VPN is prone to traffic analysis and this can reveal the origin of this traffic, information about the transmission, and the destination.

9. The Criminal Ecosystem of Dark Web

The procedures for how an illegal underground transaction involving the Dark Web and cryptocurrency operates, which consists of five steps: (i) advertisement; (ii) discovery; (iii) negotiation; (iv) payment; and (v) fulfilment.

10. Advertisement

Promoting illegal products or services on the Dark Web requires different strategies compared to promoting legal products or services on the Surface Web. This is because conventional search engines do not index content on the Dark Web. To advertise sales on a dark website, the information must be registered with a directory service available on the Dark Web, such as a hidden service directory through Tor. The registration details are then shared with potential visitors by posting access information, such as onion domains, on the Surface Web platforms like social networking sites and forums. Another approach involves advertising dark websites on general-purpose Dark Web search engines like Ahmia (https://ahmia.fi/) and Haystak (https://cryptopay.me), or market platforms such as Silkroad (BitcoinWiki,Addressreuse) and Dream Market (http://zlal32teyptf4tvi.onion).

11. Discovery

Buyers follow similar approaches from the leads of a seller's advertisement strategies, such as discovering entry points to suppliers selling illegal offerings through communities or Dark Web search engines. Also, buyers may share access information with other buyers directly.

12. Negotiation

In order to initiate a transaction, the buyer needs to communicate with the seller to discuss various aspects of the deal, including shipping methods, pricing, customization options, and payment methods. The specific details can vary depending on the type of product or service being offered. For instance, in the case of pornography dealers, the buyer would provide payment and receive a pass-code to access a porn archive. On the other hand, hacking service providers may require additional information such as the specific hacking services requested and general details about the targets. Typically, the seller's sales information will include guidelines outlining the necessary information required for the transaction.

13. Payment

Payment methods on the Dark Web typically fall into two categories based on the involvement of a third party intermediary in facilitating transactions between buyers and sellers. When no third-party mediator is present, the transacting parties establish agreements to directly send and receive payments. In such cases, sellers provide buyers with a cryptocurrency address to collect the fees. Alternatively, escrow services are utilized to address uncertainties regarding the credibility of transacting parties. Established service providers with a solid reputation offer escrow services, which involve an automated payment system for buyers and service fees charged to sellers.

14. Fulfilment

As the final step, sellers fulfill orders similar to e-commerce services of the Surface Web by sending physical products via an agreed delivery method (e.g., drugs and weapons), providing online services (e.g., hacking and illegal content) or performing criminal activities in real-world environments (e.g., targeted assassinations).

15. Tor Networks

Tor networks use virtual tunnels, however, these tunnels do not connect the client directly to the servers. What happens is that a relay point in the Tor network is created and this is able to circumnavigate the traffic analysis. It is achievable thanks to three distinct properties (Silk Road Market).

- The relay point is not privy to the entire path of the circuit.
- The encryption of each relay is unique.
- The connections are terminated after a while to preclude long-term observation.

In view of these, a system which offers similar or even superior advantages has been proposed the blockchain technology.

16. The Blockchain Technology and the Dark Web

A blockchain is a distributed and transparent ledger that maintains unchangeable records of transactions within a network. These records are shared among multiple users, which enhances security and dependability. Regarding the dark web, one significant aspect of blockchain technology(Hegadekatti *et al.*, 2016) is its impact on financial transactions. A study conducted on six different drug markets revealed a substantial daily transaction volume of approximately $650,000. On average, the daily transactions ranged between $300,000 and $500,000.

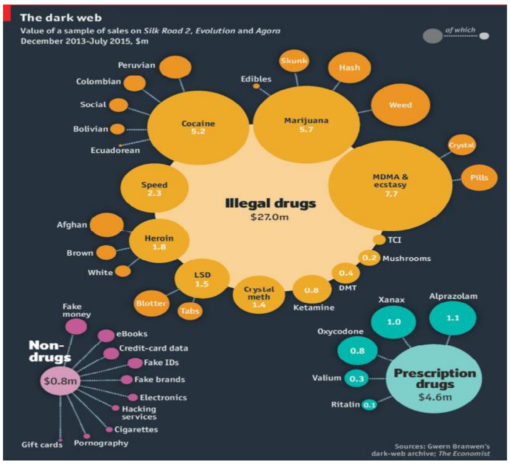

Figure 3: Uses of Dark Web in Different Areas

When comparing the transaction volumes of Bitpay, a payment processor that facilitates the conversion of Bitcoin into traditional currency, it becomes evident that there is a significant disparity. Even the largest merchant using Bitpay struggles to generate $500,000 in daily transactions. This highlights the importance of cryptocurrencies in the context of the expanding dark web.

Currently, two contemporary techniques for concealing identity are prevalent: (i) the Dark Web; and (ii) Cryptocurrency. The Dark Web utilizes anonymous routing methods, such as Tor, to hide users' identities. While initially envisioned to support press freedom and open discussions without political influence, the Dark Web has also been misused for malicious activities, including the promotion of harmful content and command-and-control servers (C&C).

Blockchain technology has played a pivotal role in facilitating transactions on the dark web and shielding it from scrutiny and potential shutdowns. The question arises as to which cryptocurrencies are commonly used in the dark web and why they are difficult to trace. Bitcoin stands out as one of the preferred cryptocurrencies for transactions on the dark web, alongside others like litecoin, monero, and dash. However, Bitcoin enjoys greater popularity. The reason for their traceability challenges lies in the privacy policies of these cryptocurrencies, particularly bitcoin and monero, which render their transactions difficult to trace compared to others.

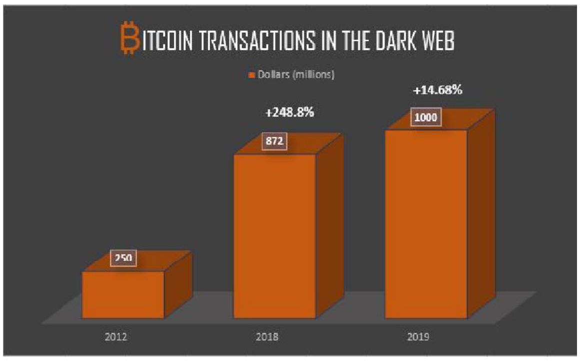

Figure 4: Bitcoin Transaction in Dark Web

Cloudy and untraceable cryptocurrencies, notably Bitcoin, are the primary form of payment on the dark web. A recent report from Chainalysis, a leading crypto-payment analytics firm, revealed that Bitcoin transactions on the dark web increased from an estimated $250 mn in 2012 to $872 mn in 2018, with a projected amount of $1 bn in 2019 (Dream Market; Fresh Onions).

17. Collection of Cryptocurrency Addresses used in the Dark Web

Despite the wide attention and dark web law enforcement and research community, no one could reach any conclusions that why there is so much illicit transaction over the dark web and why the security agencies cannot trace them (MFScope).

Since there are many researchers who already have a lot of efforts to study and analyze the dark web deeply, to facilitate them there is a platform called MFScope (Silk Road Market) which we have applied to know the details about the previous illicit transactions happened on the dark web. This platform mainly of two major components; first one is ***data collection***, in this part it collects the illicit cryptocurrency addresses from the dark web. Second major part is ***analysis***, in this part it analyzes the cryptocurrency addresses and tracks their illicit money flows.

18. Data Collection Overview

MFScope (Silk Road Market) starts by collecting seedonion addresses from Tor hidden service search engines such as Ahmia and FreshOnions. From the collected seed addresses, MFScope crawls text contents and traverses onion links on visited dark websites until there are no more links to traverse. From the crawled websites, MFScope extracts cryptocurrency addresses and performs preprocessing to filter out invalid or unnecessary addresses. Then get labeled whether such collected crypto currency addresses are indeed used for selling illegal goods and services.

19. How the Transactions Happen (the Dark Wallet)

According to Cody Wilson who conceived the dark wallet "I want a private means for black market transactions and it's just a money laundering software"

The method used by the dark wallet uses for the transaction in the dark web is called "Coin Mixing" and hence the dark wallet also known as coin mixer (What is dark market). Crypto currency mixing systems such as SmartMixer or Dark Wallet are a primary instrument of money laundering used by criminals active in the dark web and seeking anonymity. Dark Wallet was created in 2014 by Amir Taaki and Cody Wilson (who also created the first 3D printed gun), and it's an open source bitcoin platform designed to render its users anonymous and to obfuscate bitcoin transactions. One of its principal uses is coin mixing.

What coin mixing does is combine a user's transaction with that of other random users who happen to be making separate transactions through the system at the same time. It joins the bitcoins of the two or more users and mixes them together so as to conceal their origin. The user can instruct the software to pay the seller in cut up chunks of the original price (0.4 + 0.2 + 0.1 instead of the 0.7 bitcoins) or at a delayed date that they can set. This makes it extremely difficult for an outside party to determine who made a particular transaction.

In recent years, a number of competitor wallets have emerged including Anonymix, Wasabi Wallet, and SmartMixer. In May of last year, BestMixer.io, which worked similarly to Dark Wallet, was shut down by Europol with the aid of the Dutch tax services on the premises of money laundering. It's the first case of its kind. Thus it is the way transactions and launderings of bitcoins happen in the dark web and this is one the reasons why we cannot trace it using our usual sources. So, we have seen till now what is the blockchain, how cryptocurrencies like bitcoin are used for transaction using blockchain and how bitcoin transaction is much secure because of blockchain, but there are also some downside of blockchain technology like we have seen earlier it provides DLT which makes anonymity property too immune that people use this technology over the dark web for their illegal works.

20. Why Cryptocurrency is so Much Used on the Dark Web

Blockchain technology emerged as a solution to the problem of centralization (https://www.darpa.mil/program/memex). Its decentralized nature enables a wide range of possibilities, forming the foundation of cryptocurrencies. Two key features define blockchain technology:

1. Anonymity

2. Security

Anonymity plays a crucial role as it allows for transactions to be conducted without leaving traces. While this may initially seem unnecessary, a deeper understanding reveals its significant benefits for illicit cryptocurrency transactions. Emerging currencies like Monero offer features such as stealth addresses, which generate addresses for receiving illicit funds. These addresses can be traced to a certain extent but cannot be linked back to the original owner.

Security is of utmost importance, especially in the context of the dark web where various transactions take place, ranging from pornography to the purchase of illegal drugs. These transactions involve substantial amounts of funds and require a secure and reliable method without any delays. Cryptocurrency emerges as the sole currency capable of meeting these requirements. It provides a safe and efficient means for dealers to transfer their illicit funds.

Now the question rises here is, *"if the dark web is this much worse, are there any ways to stop or trace the activities happening over dark web?"*

To answer this question first we need to understand that cryptocoins are based blockchain technology and that means no third party(even the government) can intervene between them, which means there will be no traces of that some illicit transaction happened over dark net and only the two parties which are involved in the activity knows about the transaction.

Hence we can say till now there is no way we can completely stop an illicit transaction happening on the dark web or take control of that, but there are few ways to regulate the activities and keep track of that.

21. Ways to Regulate the Transactions Happening on the Dark Web

The primary method is to assign a crypto wallet to individuals interested in purchasing cryptocoins or cryptocurrencies. This encrypted electronic device enables users to conduct transactions using cryptocoins and maintains a record of all transactions. Each wallet possesses a public key visible to everyone, but only the owner with the private key can operate it. Transactions within the cryptocoin network generally maintain anonymity (https://pideeco.be/articles/dark-web-and-money-laundering/).

When individuals transfer cryptocoins to one another, there must be a record of who spent how much and when. In traditional currency systems, such as fiat money or paper money, this responsibility falls on banks, which act as Trusted Third Parties and charge commissions for their services. However, in the case of cryptocurrencies, these transactions are recorded on a ledger known as the Blockchain (Blockchain.com), typically with negligible or minimal fees.

The second approach to monitor activities on the dark web is referred to as the controlled blockchain method. Bitcoin, a peer-to-peer based cryptocoin, lacks backing from any physical commodity and does not possess a sovereign guarantee, unlike traditional fiat currencies.

In contrast, Regulated and Sovereign Backed Cryptocurrencies (RSBC) (https://pideeco.be/articles/dark-web-and-money-laundering/) are government-supported cryptocurrencies that resemble digital versions of paper currency. Within this system, the cryptocoins, known as Nation Coins, are backed by a Sovereign Guarantee (https://pideeco.be/articles/dark-web-and-money-laundering/). Transactions involving these currencies take place on a highly secure Controlled Blockchain (referred to as CBC), ensuring smooth and secure transactions. NationCoins are fully managed by the Sovereign Authority, meaning the government holds control over their operations.

The RSBC system operates based on the K-Y Protocol, which encompasses a set of rules and instructions for implementing the Regulated and Sovereign Backed Cryptocurrency system (https://pideeco.be/articles/dark-web-and-money-laundering/).

A Controlled Blockchain, in contrast to a traditional Blockchain, is a permission-based distributed database. Access and operation permissions are granted by the Sovereign Authority, distinguishing it from the open nature of a regular Blockchain. The implementation of the K-Y Protocol results in a Controlled Blockchain (CBC) that serves various purposes beyond financial transactions. It has a broad range of applications, including banking, taxation, contracting, space research, automation, and public services. Moreover, it can effectively regulate activities on the Deep Web.

22. Ways to Discern the Identity of Bitcoin Wallet Holder

In reality, it is possible to discern the identities of Bitcoin wallet holders by a process known as de-anonymization. Off late Bitcoins are under surveillance and can be de-anonymized. This effectively renders the anonymous transactions traceable. Computer scientists associate activities with Bitcoin wallet usage. Even geographically pinpointing the user is possible. But it may take time and will most probably be retrospective (https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314; https://pideeco.be/articles/dark-web-and-money-laundering/).

Illegal operators operate anonymous websites on the Dark Web, providing a platform for the purchase of illicit items. The rise of advanced Cryptocoins, such as Monero, has enabled enhanced anonymity on these platforms. Monero utilizes Ring Signatures, a cryptographic technique that prevents de-anonymization, making it difficult to determine the origin of a signature. This level of anonymity is reinforced by Monero's opaque Blockchain, amplifying financial secrecy even among miners. The increased use of Cryptocurrencies like Bitcoin and Monero has significantly boosted the Dark Web's anonymity, evident through the proliferation of platforms like SilkRoad (MFScope; https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314).

However, the introduction of Regulated and Sovereign Backed Cryptocurrencies (RSBCs), implemented through the K-Y Protocol, has the potential to regulate the Dark Web. Imagining a scenario where RSBCs are in widespread use, Bitcoin could be converted into NationCoins like USCoins, and transactions would occur through registered wallets, allowing for easier traceability and de-anonymization. Even with currencies like

Monero, transaction identities could be identified at the interface between Monero and NationCoins, enabling governments to trace illegal activities, such as funding terrorism or drug smuggling (https://pideeco.be/articles/dark-web-and-money-laundering).

In this way, the implementation of Regulated and Sovereign Blockchains (RSBCs) would facilitate the tracing of users and their activities, including transactions conducted on the Dark Web (MFScope; https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314). Consider a future where each sovereign state has its own NationCoins, reducing reliance on physical cash transactions. With RSBCs becoming the primary means of payment, unaccounted money would diminish, and the identities of parties involved in illegal activities would be known through their NationCoin wallets. Real-time identification of illicit trade would be possible, and the circulation of money within the Deep Web could be tracked, enabling taxation and regulation by governments (https://pideeco.be/articles/dark-web-and-money-laundering).

23. Conclusion

The blockchain technology has got many aspects and it provides anonymity and security of the level which cannot get breached or traced by any third party, since it cannot get traced nobody could get to know the activities happened over the blockchain and because of its distributed ledger technology only those who were involved in the activities knows about it. As anonymity increased, it increased the illegal online activities and made dark web much more immune than ever, it also gave birth to the concept of crypto currencies like bitcoin and Monero. It also increased the use of dark web and illicit transactions happened over there. There is no solution found till now and the only solution we have can be used to regulate the transactions over the deep web and to trace back the activities happened there. This technology (RSBC) is a kind of advancement in the blockchain systems and introduces the concept of de-anonymization where one has to convert their crypto coins into the NationCoins (crypto currency of the particular nation) (https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314; https://pideeco.be/articles/dark-web-and-money-laundering/) by which we can know about the person who has crypto wallet and where is the crypto coins spent and so that can track the illicit transactions and illegal activities happening over the dark net.

Thus this is how we can at least have the details of the activities running on the deep web and we can track the illegal activities happened there.

References

Ahmia, https://ahmia.fi/

Akdeniz, Y. (2002). Anonymity, Democracy, and Cyberspace. *Social Research:An International Quarterly*, 69(1), 223-237.

Alex, Pentland *et al.* (2019). Anonymity and Law Enforcement: A Decentralized Framework for Cryptocurrencies.

Androulaki, E., Karame, G.O. , Roeschlin, M., Scherer, T. and Capkun, S. (2013). Evaluating User Privacy in Bitcoin. in International Conference on Financial Cryptography and Data Security (ICFCDS 2013).

Barnett, G. and Jiang, K. (2016). Resilience of the World Wide Web: A Longitudinal Two-Mode Network Analysis. Social Network Analysis and Mining, 6, 1-105.

Bcoin-cli, https://github.com/bcoin-org/bcoin/wiki/CLI.

bitcasino, https://bitcasino.io/

BitcoinWiki, Addressreuse. [Online]. Available: https://bit.ly/2LRWVCS

Blockchain.com, https://www.blockchain.com.

Cryptopay, https://cryptopay.me.

Aaron Higbee (2018). The Role of Cryptocurrency in Cybercrime. *Computer Fraud & Security*, 2018(7), 13-15. doi: https://doi.org/10.1016/S1361-3723(18)30064-2

Dirk A. Zetzsche *et al*. (2019). Legal and Regulatory Challenges of Cryptocurrencies. DOI:10.2139/ssrn.3018534

Dream Market, http://n3mvkmkqb3ry4rbb.onion.

Fresh Onions, http://zlal32teyptf4tvi.onion.

Hegadekatti, Kartik. and Yatish, S.G. (2016). The K-YProtocol: The First Protocol for the Regulation of Crypto Currencies (E.G.- Bitcoin) (February 13, 2016).Available at SSRN: https://ssrn.com/abstract=2735267 or http://dx.doi.org/10.2139/ssrn.2735267

https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314

https://pideeco.be/articles/dark-web-and-money-laundering/

https://www.darpa.mil/program/memex

Manoharan, Ramar *et al*. (2020). DarkWebMarket Price Manipulation. https://github.com/topics/darknet-markets

Martin, Dittmann *et al.* (2017). Dark Web Marketplaces: Structure, Functioning, and Abuse Potential.

MFScope; https://www.darknetstats.com/mfscope-a-novel-platform-for-identifying-illegal-crypto-transactions-on-the-dark-web/

Nakamoto, S. (2019). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

Sean, Foley. *et al*. (2019). Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. https://www.fdd.org/analysis/2018/01/10/bitcoin-laundering-an-analysis-of-illicit-flows-into-digital-currency-services/

Silk Road Market, http://silkroad7rn2puhj.onion/

Svenja, Heikenfeld. (2020). Regulating Cryptocurrencies: Analyzing the Global Regulatory Framework. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

What is Dark Market, https://www.thebalance.com/what-is-a-dark-market-391289.

Wood, G. (2014).Ethereum: A Secure Decentralized Transaction Ledger. [Online]. Available: https://bit.ly/2hhPViV

Wu, P. and Li, S. (2011) .Layout Algorithm Suitable for Structural Analysis and Visualization of Social Network. *Journal of Software,* 22, 2467-2475. http://pub.chinasciencejournal.com/JournalofSoftware/18611.jhtml https://doi.org/10.3724/SP.J.1001.2011.03896

Xinyu, Xing *et al*. (2018). Anonymity Loves Company: A Threat to Online Anonymity via Social Network Profiling.

Cite this article as: Shiv Hari Tewari (2023). Ways to Regulate the Abuses of Blockchain and Cryptocurrency Over the Dark Web. *International Journal of Cryptocurrency Research,* 3(1), 78-88. doi: 10.51483/IJCCR.3.1.2023.78-88.