EasyChair Preprint

№ 4995

Abuses of Blockchain and Cryptocurrency in Dark Web and How to Regulate Them

Shiv Hari Tewari

February 21, 2021

Abuses of blockchain and Cryptocurrency in dark web and how to regulate them

By:

SHIV HARI TEWARI (M.Tech.(CSE) BIT, Mesra)

Email: tewarishivhari999@gmail.com

Abstract

The blockchain technology is a distributed ledger system where it is distributed among the users who does the transactions using this technique, it first came in trend after the sudden rise in the value of bitcoin in 2017 and then people get to know about this blockchain system and its working, it provides anonymity and security both to the user and that is why crypto currencies like Bitcoin and now Monero are using the blockchain method to ensure the safe, secure and untraceable transactions. Anonymity and security are like two edges of the same sword, they can be used for the great purposes like protecting the privacy of people, fostering, freedom of speech etc on the other hand they can be misused for the illegal activities happening over the internet like cyber terrorism and perpetrators often go unaccounted for their acts. Where there are many qualities of blockchains there are also some downsides too, because of increased security and anonymity it worked as a fuel for the dark web users to illicit transactions and do the illegal activities on the dark web. In this paper we have shown what are the downsides of blockchain, how the transaction happen on the dark web happens and how we can regulate and track the illegal activities on the dark web using regulated and sovereign backed crypto currencies.

What is Blockchain

Blockchains are originally the database of collection of blocks containing the details of transactions between the two parties. It is basically a system of recording information in a way that makes it difficult or impossible to change, hack or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block contains the number of transactions and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant’s ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT).

So, blockchain is a kind of DLT in which transactions are recorded with an immutable cryptographic signature called “Hash”.

The picture below shows the properties of DLT and why it is useful for today's database security.

Some of the major properties that makes it more useful for secure transactions are, anonymity of the users who done the transactions, its distributed nature and time-stamping.

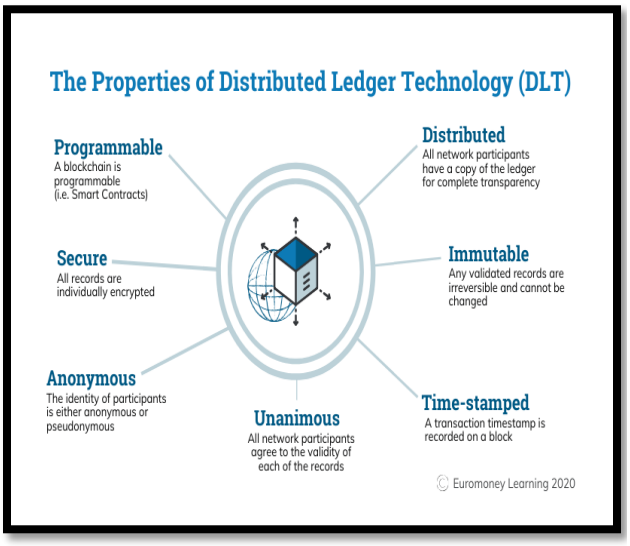

Fig. 1: Properties of Blockchain

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

As we can see the blockchain technology is not only secure but it also maintains the anonymity of its users and completes the transaction in stipulated time and stores all the details of the transactions.

Why it became famous overnight:

There have been so many attempts to create the digital currency but they all failed miserably as they weren't reliable and there was a trust issue in all of them, for example if someone is created a cryptocurrency named "X" now can we trust that they won't give themselves a million "X" or steal our millions of "X" for themselves.

The bitcoin was designed to solve this issue by using a specific type of database called a blockchain. Most normal databases, such as an SQL database, have someone in charge who can change the entries (e.g. giving themselves a million X dollars). Blockchain is different because nobody is in charge; it's run by the people who use it. What's more, bitcoins can't be faked, hacked or double spent, so people that own this money can trust that it has some value.

Hence in a nutshell blockchain is reliable, secure and it is originally devised for the digital currency or cryptocurrency like Bitcoin but tech community has find its some other

uses because it maintains anonymity of its users and known for the secure transactions.

Since it maintains the anonymity of its users, it has turned into a weapon for those who want to perform some illegal task over the internet or we can say the dark net.

What is Bitcoin:

Bitcoin[9] is a decentralized digital crypto currency that relies on cryptography algorithms and a peer-to-peer network to manage a fully distributed ledger without a central authority.

Unlike the traditional banking system, the absence of a central authority means that financial activities have remained under a pseudonym. Bitcoin users can generate multiple ac-counts (i.e., public addresses) with corresponding verifiers of the ownership (i.e., private keys) to send/receive bitcoins (BTCs) through a wallet software, which makes a payment as well as manages key pairs. Thus, payments in Bitcoin can be transferred over the Bitcoin network without revealing the real identities of the participants involved in each transaction.

Payment in Bitcoin starts by broadcasting a transaction over the Bitcoin network by Bitcoin users. Suppose that Alice sends BTCs to Bob. Alice's wallet software first searches unspent transaction outputs(UTXOs) that contain amounts of BTCs and conditions to spend corresponding BTCs. Each UTXO can be spent on other Bitcoin addresses as an input in a new trans-action. If Alice has authentication information (i.e., private keys) to ensure ownership of Bitcoin addresses having valid UTXOs, Alice's wallet software creates a transaction signed by her private keys and broadcasts it over the Bitcoin network. Bitcoin users can transfer arbitrary valid public addresses to receive/send BTCs with other users, but the address reuse is not recommended for privacy and security reasons.

After receiving a transaction request, Bitcoin nodes first check whether the requested transaction is cryptographically acceptable (valid) and register the transaction into the Bitcoin Mempool if it is verified. For creating a new Bitcoin block, Bitcoin nodes collate a set of transactions from the Mempool, form them into a

block, then perform PoW to solve a

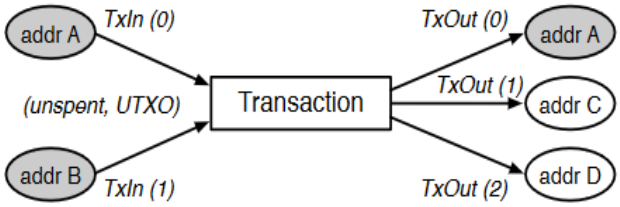

Fig.2: An example of a Bitcoin transaction between Alice and Bob. The gray and white ovals indicate the public Bitcoin addresses owned by Alice and Bob respectively.

mathematical equation, called a mining process. If a Bitcoin node solves the math problem and it is verified by other Bitcoin nodes, the new block is finally linked to the Bitcoin Blockchain.

Figure-2 illustrates an example transaction in which Alice sends BTCs to Bob and sends back the remainder of the BTCs to Alice. This Bitcoin transaction consists of a list of inputs (T x In), which are referenced to Alice's public addresses (the gray oval) connected to unspent transaction outputs (U T XO),and a list of outputs (T xOut) - the destination public addresses belonging to Alice and Bob. In this example, Alice transfers certain BTCs to Bob's public addresses (addr CandD).Since the total input value should equal the total output valueaccording to the Bitcoin protocol, Alice sends the rest of theBTCs back to the same address, used inT xIn(0).

What is dark web:

The dark web[20] 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.

What kind of people access the dark web:

The dark web resonates with a large number of people, however, the chief among them are those who use it for the illegal trades. A study in 2014 at Portsmouth discovered that the most solicited content on the dark web is child pornography and the next on hierarchy is drugs and unlicensed arms. It is also discovered that people used it purchase the illicit information and even for renting the hitman to kill someone. [15]

As per our study we have found some of those websites, one of them is **besamafia** which is used to hire a hitman and there is website named **doxtor** which sells the product which

was created by Apple but didn't launch in the market. There many more websites like them available on the dark net market and these websites uses bitcoin as their payment interface and PGP key for communication.[14]

Now the question raises here, "is dark web only devoted to dark activities?" the answer is no, for example wikileaks, it is a platform devoted to whistleblowing and it allows individuals upload classified information incognito to the appropriate agencies. In addition to this, the dark web has also helped people in China access certain sites which are otherwise inaccessible.

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.

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) fulfillment.

Advertisement:

Advertising illegal products or services on the Dark Web requires different approaches from promoting legal products or services through the Surface Web since traditional search engines do not index content on the Dark Web. If a dark website is created to promote sales, then this information must be registered with a directory service provided on the Dark Web (e.g., a hidden service directory through Tor). This registration is then advertised to potential visitors by posting access information (e.g., onion domains) on the Surface Web(e.g., SNS and forums). An alternative approach is to advertise dark websites on general purpose Dark Web search engines (e.g., Ahmia[1] and Haystak[5]) or market platforms (e.g., Silkroad[11] and Dream Market [6]).

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.

Negotiation:

To proceed with a transaction, a buyer must confer with a seller about the deal regarding shipping method, price, customizing services, and payment methods. These details vary according to the type of product or service. For example, porn dealers receive money from a buyer and send a pass-code for accessing a porn archive. In contrast, hacking service providers might require additional details, such as the type of hacking services requested and general information about targets. Typically, guidelines for information needed are included with the seller's sales information.

Payment:

Payment through the Dark Web commonly hasthe two following options depending on the existence of a third party who mediates transactions between the buyers and sellers. Transacting parties without a third-party mediator make agreements to receive and send fees directly where sellers provide a cryptocurrency address to the buyers for collecting fees. Escrow is available to overcome uncertainty in the credentials of transacting parties since established service providers tend to have a higher reputation. Escrow service providers support an automated payment system to buyers and charge service fees to the sellers.

Fulfillment:

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).

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.[14]

- 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.

The Blockchain technology and the dark web:

A blockchain is a decentralized public ledger which keeps immutable records of the transactions on the network. This record is stored across several users (decentralization) and this adds to the level of security and reliability.

One real importance of the blockchain[20] technology as it pertains to the dark web is the finance. Research was carried out on six different drug markets and the daily volume of transaction was found to be about $650,000. On the average, it recorded a daily transaction between $300,000 and $500,000.

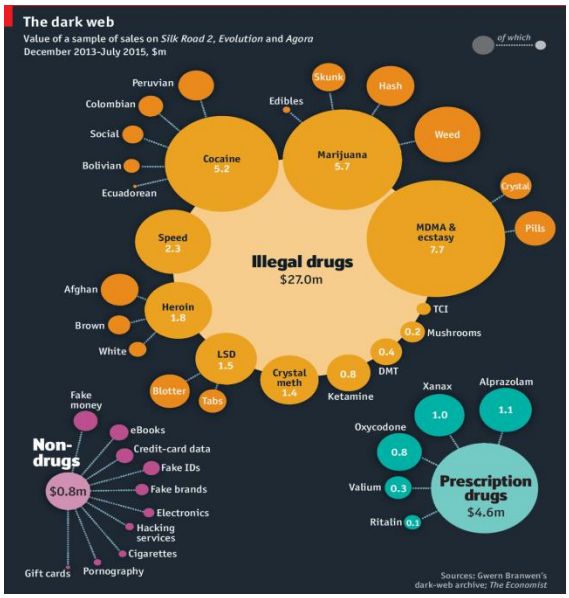

Fig.3 : use of dark web in different areas

When we compare this to the amount of transactions handled by Bitpay, a payment processor which facilitates the conversion of Bitcoin into fiat currency, the difference is clear. The largest merchant of Bitpay struggles to bring in $500,000 in a day.

We can then safely conclude that cryptocurrencies are important to the burgeoning of the dark web.

Today, we are facing two up-to-date techniques for hiding identity: (i) Dark Web and (ii) Cryptocurrency. The Dark Web leverages anonymous routing techniques (e.g. Tor) to conceal the user's identity. While the

Dark Web was first proposed to support the freedom of the press and guarantee open discussions without political pressure, it is also misused for malicious purposes, such as advertising harmful content and command-and-control servers (C&C).

So we can see how blockchain technology has fueled the dark net transactions and immune it from the people who can trace it and can shut down the whole network.

Now the question rises here is what kind of cryptocoins or cryptocurrency are used in the dark web and why they can't be traced.

We can say bitcoin is one of the cryptocurrency which is used over the dark web for transactions apart from the bitcoin there are others like litecoin, monero and dash but bitcoin is popular among them, now the other question is why they are so untraceable, according to interpol "despite of having all the tools to trace the transactions but on the dark net there is no means we can trace the data over the dark web and only few them get caught" others just slip away because there are privacy policies of cryptocurrency (bitcoin and monero) which makes their transaction untraceable than the others.

Cloudy and untraceable cryptocurrencies, particularly Bitcoin, are the primary means of payment. A recent report by Chainalysis, a leading crypto-payment analytic firm, has shown that Bitcoin transactions happening in the dark web grew from an estimated **$250 million in 2012** to **$872 million in 2018**, with a projected **$1 billion in 2019**. [13] [14]

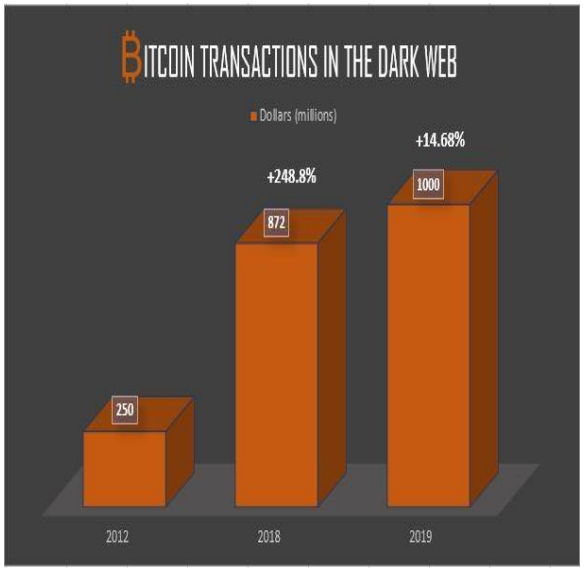

Fig. 4: Bitcoin transaction in dark web

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.[17]

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**,[14] which we have implemented 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.

Data Collection Overview:

MFScope[14] 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.

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.[16]

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.

Hence this is how the 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.

Why cryptocurrency is so much used on the dark web:

Since Blockchain[15] set out to solve the issue of centralization. With the decentralized blockchain technology, so much can be achieved with this technology and this is the bedrock of cryptocurrency. There are two major features of the blockchain technology and these are:

1. Anonymity
2. Security

Because of the property of anonymity one can be able to execute the transactions without leaving the trace and it might come off as superfluous at first, but if we dig deeper, it becomes extremely beneficial to illicit cryptocurrency addresses and apart from the bitcoin new currencies like Monero have features like stealth addresses which generates address for receiving illicit funds. These

addresses are traceable but cannot be traced back by the original owner.

Now in the context of security , there is a large sale in the dark web from the pornography to purchase of illegal drugs and these transactions are quite expensive to fund and don't allows any delays. The dealers require a safe and reliable means of getting their illicit funds over and only one currency can allow for this which is cryptocurrency.

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.

Ways to regulate the transactions happening on the dark web:

First and the most common way is to allot a crypto wallet to the client who wants to buy the cryptocoins or cryptocurrency, it is an encrypted electronic device which allows the keeper to do the transactions using cryptocoins and keeps track of all of the transactions. Each wallet will have a public key visible to anyone. But it can be operated by only a person who has a private key. Transactions on the cryptocoin network are usually anonymous.[18]

When people send cryptocoins to each other, someone has to keep account of who spent how much at what time. In case of flat money (or paper money) it is done by banks (known as Trusted Third Parties, for which they charge a commission).But in case of Crypto coins, it is registered on a ledger called BlockChain[15] (with nil or minimal fees).

Second method which can be used to regulate the activities over the dark web is known as controlled blockchain method.

Bitcoin is a peer-to-peer based cryptocoin which is not backed by

any commodity and (unlike flat money) carries no sovereign guarantee whatsoever.

Regulated and Sovereign Backed Cryptocurrencies (RSBC)[19], on the other hand are government backed cryptocurrency a kin to paper currency, but in digital form. In this system, the cryptocoins (known as Nation Coins) are backed by Sovereign Guarantee.[19]

They are run on a highly secure Controlled BlockChain (referred to as CBC) in which Sovereign backed Cryptocurrencies will be transacted without any hassles. NationCoins are completely managed by the Sovereign Authority i.e. the Government.

This system is based on the K-Y Protocol. The K-Y Protocol is a set of rules and instructions to implement the Regulated and Sovereign Backed Cryptocurrency (RSBC) system.

A Controlled Blockchain is different from a BlockChain . A Block Chain is permission less Distributed Database, whereas a Controlled BlockChain will be Permission Based. The permission for access and operation being provided by the Sovereign Authority.

A Controlled Block Chain (CBC) resulting from the K-Y Protocol has several money and non-money uses. In its complete form, it will have a wide spectrum of applications ranging from banking, taxation, and contracting to space research, automation and public services. And it can be used to effectively regulate the Deep Web.

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.[18][19]

Illegal Racketeers run anonymous websites on the Dark Web where people can order for any illegal items they want. This is possible because of the advent of Cryptocoins which are more advanced than Bitcoin in maintaining anonymity. Take for example, Monero. Monero is a cryptocoin which uses a technique called Ring Signatures. Ring

Signatures make Monero highly resistant to De-anonymization. In cryptography, a ring signature is a kind of digital signature executed by any member of a set of users, each one of whom has keys. A message having a ring signature is signed by someone in that certain set of people. In a ring signature, it is mathematically impossible to determine whose key was used to create the signature. There is no manner in which to unmask the anonymity of a signature. Monero thus presents an opaque Blockchain. This greatly amplifies and enhances financial anonymity to the extent that even miners do not know where the money is going or the nature of its contents. Crypto currencies like Bitcoin and now Monero have given a huge boost to the dark web and it has make the dark web much more immune in the context of anonymity. This is evident by the mushrooming of anonymous websites like SilkRoad.

But all that will change by introducing RSBCs. In fact, we can regulate the Dark Web if governments implement the K-Y Protocol.

Now imagine a scenario where RSBCs are in vogue. Bitcoin is converted not to Dollars but to USCoins (the NationCoin form; the digital avatar of the US Dollar).These USCoins go into a wallet that is already registered under some verified name. Thus the persons giving and accepting illegally earned Bitcoins can be easily traced by de-anonymization. In case of currencies like Monero, transaction identities can betraced at the point where there is an interface between Monero and NationCoins. The system will know who is who. By tracing transactions and analyzing patterns, the Government can find out who is funding terrorist activities and who is financing drug smuggling.[19]

Thus by the use of the regulated and sovereign blockchain (RSBC) we can easily trace the users and their activities happening over the web and all the transaction they have done over the internet or we should say the dark net.[17][18]

Imagine a scenario where 200 sovereign states maintain their own NationCoins. Hard cash transactions will be greatly reduced. People will have to transact using RSBCs. In fact, there will not be enough paper currency to fund illegal activities. All payments will have to be done by RSBCs. There will hardly be any unaccounted money. Illegal trade will be quickly identified in real-time as

the identities of parties involved in the activities will be known through their NationCoin wallets. The quantum of money circulating in the Deep Web will also be known, thus enabling the Government to tax and regulate the Deep Web.

Conclusions:

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(regulated and sovereign blockchain(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)[18][19] 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

[1] Ahmia, https://ahmia.fi/.

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

[3] bitcasino, https://bitcasino.io/.

[4] Cryptopay, https://cryptopay.me.

[5] Dream Market, http://n3mvkmkqb3ry4rbb.onion.

[6] Fresh Onions, http://zlal32teyptf4tvi.onion.

[7] Y. Akdeniz, “Anonymity, democracy, and cyberspace,”Social

Research:An International Quarterly, vol. 69, no. 1.

[8] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun,"Evaluating user privacy in bitcoin," in International Conference on Financial Cryptography and Data Security (ICFCDS 2013).

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system."[Online]. Available: http://bitcoin.org/bitcoin.pdf.

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

[11] Silk Road Market, http://silkroad7rn2puhj.onion/

[12] Blockchain.com, https://www.blockchain.com.

[13] What is dark market, https://www.thebalance.com/what-is-a-dark-market-391289.

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

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

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

[17] Hegadekatti, Kartik and S G, Yatish, 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

[18] Hegadekatti, Kartik and S G, Yatish, The K-Y Protocol: 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

[19] G. Wood, "Ethereum: A secure decentralized transaction ledger," 2014.[Online]. Available: https://bit.ly/2hhPViV

[20] Immunity on the dark web as a result of blockchain technology: https://codeburst.io/immunity-on-the-dark-web-as-a-result-of-blockchain-technology-6693eb087bdd