Bit by Bit leading to Dark

Sonal Sodhani[1] and HarshitChitlangia[2]

1. Abstract

Developed by an anonymous programmer, Bitcoin is a global cryptocurrency and a system for digital payment. It is a decentralized currency as it operates without a single administrator; the transactions take place directly between the users minus any intermediaries. Whereas, the term deep Web is used to denote a class of content on the Internet that, for various technical reasons, is not indexed by search engines. The dark Web is a part of the deep Web that has been intentionally hidden and is inaccessible through standard Web browsers.

Considering the difference in darkweb and visible web, and the anonymity linked with both the bitcoins and the darkweb, it is important to develop tools that can effectively handle it. Bitcoins when combined with the darkweb has the potential to host an increasingly high number of malicious services and illegal activities.

In this paper, the authors try to provide a broader understanding of the bitcoins and the darkweb, and also of their impact when used together. Also, the authors delve in examining the scope of law with regard to the use and regulation of darkweb and bitcoins, across the globe, in the light of the various legal and practical problems being faced by the policy makers in formulating strategies, policy or laws for governing and regulating such anonymous entity, without violating the privacy of the users.

Key Words:

Bitcoins, Cryptocurrency, Darkweb, Information Technology Act 2000, TOR.

2. What are Cryptocurrencies and Bitcoin?

A cryptocurrency is a computerized digital money that utilizations cryptography for security. It is also known as virtual currency. Cryptocurrency is a type of digital currency that is intended to be secure and anonymous. Cryptocurrency is associated with the use of cryptography. Cryptography is the process of converting legible data and information into an almost uncrackable code, to track purchases and transactions. Cryptocurrency is an approach to secure communications, data, information and

[1] ***Student, New Law College, Bharti Vidhyapeeth Deemed University, Pune.***
[2] ***Student, Amity University, Ranchi***.

money online. It has developed in the computerized and digital era with components of mathematical hypothesis and computer science.

Bitcoin is a cryptographic, computerized and experimental currency introduced to the advanced digital world in 2009. It is alluded to as a "peer-to-peer, electronic payment system". Unlike the standard type of money, it is in virtual frame and can be utilized to make payments online and also in physical stores. The Bitcoin system is private, however with no customary money and finance related institutions engaged in transactions. Unlike previous digital currencies that had some central controlling individual or entity, the Bitcoin network is totally decentralized, with all parts of transaction performed by the users of the framework.

3. Working of Bitcoin system: Blockchain Algorithm

Basically, bitcoin is a snippet of codes based on blockchain algorithm. Each Bitcoin and each user is encoded with a unique identity, and every transaction is recorded on a decentralized open public ledger, also known as blockchain, that is visible to all the systems on the network yet does not reveal any personal information about the involved parties. Bitcoin is a currency which is based on digital signatures. The owner transfers Bitcoins to the recipient by signing the hash of the previous transaction and public key of the recipient.

Cryptographic techniques empower special users on the bitcoin network, known as miners, to assemble blocks of new transactions and compete to confirm that the exchanges are substantial and valid—that the purchaser has the amount of Bitcoin being spent and has transferred that amount to the dealer's account. For providing this service, miners that effectively verify a block of transaction are remunerated by the network's controlling computer algorithm with some newly created Bitcoins.

This decentralized management of this blockchain algorithm is the distinguishing technological quality of Bitcoin as it settles the so-called double spending issue (i.e., spending through money you don't own by use of fraud or forging) and the attendant need for a trusted third party, to check the integrity of electronic transactions between a purchaser and a vender. Blockchain technology could have implications not only for the customary and traditional paymentsystem but rather perhaps also for a wide range of transactions (e.g., stocks, bonds, etc.) in which records are stored digitally.

4. What is Darkweb?

Internet has two sides – the visible and the invisible side. The visible side of the Internet incorporates sites that can be found through an ordinary search, while the invisible side — the Deep Web — incorporates those networks and sites that cannot be accessed through general means. Dark Web is a small portion of this Deep Web.

The Dark Web is that segment of the Deep Web that has been deliberately hidden and is out of reach through standard web browsers. Dark websites serves as a platform for Internet users for whom secrecy and anonymity is essential, since they provide protection from unauthorized users, and also include encryption to avoid and prevent monitoring.[3]

A relatively known source for content on the Dark Web is found in the Tor network. The Tor network is an anonymous network that can only be accessed with a special web browser, which is termed as the Tor browser.[4] First to appear as The Onion Routing (TOR) project in 2002 by the US Naval Research Laboratory, it was a technique for communicating on the web secretly. Another network, I2P, gives a lot of similar features that Tor does. Be that as it may, I2P was intended to be a network inside the Internet, with traffic remaining contained in its borders.

Like any technological innovation, from pencils to cell phones, anonymity can be utilized for both good and bad. Users who fear economic or political retaliation and retribution for their actions swing to the Dark Web for protection. But, there are also those users who exploit this online anonymity to utilize the darkweb for illicit illegal activities, like,terrorism funding, controlled substance trading, illegal financial transactions, identity theft, etc.[5]

5. Working of Tor browser and Darkweb

Internet anonymity is ensured when Internet Protocol (IP) addresses cannot be followed or tracked. Tor client software routes Internet traffic through a worldwide volunteer network of servers, concealing user's information and eluding any activities

[3] Michael Chertoff and Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, GLOBAL COMMISSION ON INTERNET GOVERNANCE (Feb., 2015), https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf (on Mar. 18, 2018, 11:58 am).

[4] *Clearing Up Confusion – Deep Web vs. Dark Web*, BRIGHTPLANET (Mar. 24, 2009), https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/ (on Mar. 08, 2018, 05:45 pm).

[5] *An Introduction to the Digital Black Market, or as also known, the Dark Web*, NETSPARKER, https://www.netsparker.com/blog/web-security/introduction-digital-black-market-dark-web/ (on Apr. 05, 2018, 05:03 pm).

of monitoring. This makes the Dark Web quite appropriate for cybercriminals, who are always trying to hide their tracks.

Onion routing is a technique for anonymous communication over a network. Messages are repeatedly encrypted and encoded, and later is sent through several network nodes, called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to reveal routing instructions and guidelines, and sends the message to the next router, where the same procedure is repeated.[6] This technique keeps intermediary nodes from knowing the origin, destination and contents of the message.

6. Bitcoin and Darkweb : an amalgam

Bitcoin has twofold effect on the working of darkweb. While on one hand, bitcoins and other cryptocurrencies have proven to be effective in encouraging illegal and illicit trade, on the other hand, has helped in detection of illegal activities because of the public nature of the blockchain.

The blend of TOR for secret communications and bitcoin for covert payments has led to the proliferation of darknet markets. Similar to the way PayPal propelled EBay, the secured, decentralized, and anonymous nature of bitcoins has assumed an essential part in the success of darknet markets.

Two things rule the dark web black market today: drugs and financial fraud. The former only required the presence of two systems to flourish explosively in the way that it did – an anonymous cryptocurrency like bitcoin, and an anonymizing proxy system. Financial fraud, however, required these and one more factor in the blend to complete its trifecta – an approach to keep scraping financial information to dupe. While malware trading was nothing new, a radical new age of black market warez gained the limelight.

Many a times, bitcoins are associated with the illegal and nefarious activities on the 'dark web,' like illicit purchase of weapons, and terrorism funding. This was because network members could be anonymous or pseudonymous i.e., not completely unknown – due to various identifying information like network (IP) addresses and public keys – however not clearly linked to a genuine and real identity. Hence, it becomes difficult for regulators and counterparties to hold any user accountable, and

[6]*Onion Routing*, GEEKS FOR GEEKS, https://www.geeksforgeeks.org/onion-routing/(on Apr. 01, 2018, 04:47 pm).

enforce legal, tax and contractual obligations. Albeit a tangential example, the huge amount of assets and resources it took for the U.S. Federal Bureau of Investigation (FBI) to trace the mastermind behind 'Silk Road' (the scandalous 'darkweb' trade), bears testimony to this. Further, when the blockchain is deployed in regulated ventures and industries, KYC prerequisites and various reporting obligations like anti-money-laundering for illegal tax evasion and anti-terrorist-funding are triggered. These are difficult to meet when exchanges and transactions are on blockchains, at least in the formblockchains are commonly being used today.

Despite the fact that bitcoin has been used broadly in illegal activities, some contend that the blockchain really makes it easier for law enforcement to distinguish illegal activities, in spite of the currency's anonymity. It has been reported that by linking bitcoin wallets with transactions on darkweb, 125 Tor users were unmasked by the researchers of Qatar University, Doha.[7]

The paradox of bitcoin is that its associated data creates a measurable trail that can suddenly make one's whole financial history a public information. The challenge is that the Bitcoin network is intended to blur the correspondence amongst transactions and IP addresses. All Bitcoin users are associated with peer-to-peer network over the Internet. Data stream between their systems like gossips in a crowd, spreading rapidly until everybody has the data—with nobody but the originator knowing who spoke first.

This bitcoin is safe from robbery and theft, as long as users never reveal their private keys. But, as soon as a Bitcoin is spent, the forensic trail starts. It was reported that by 2013, millions of dollars' worth of Bitcoins were being exchanged and swapped over Silk Road for illegal drugs and stolen identity cards.[8]

7. Forecasting Legal Issues

i) Privacy

Most Internet protection and privacy laws deal with a situation where a site or an app gathers personal data from an end user. The IT Act[9], for example, directs and

[7]Chris Stokel-Walker, *Dark web users are easy to unmask through their bitcoin use,* NEW SCIENTIST (Feb.1, 2018), https://www.newscientist.com/article/2160066-dark-web-users-are-easy-to-unmask-through-their-bitcoin-use/ (on Apr. 1, 2018, 12:01 pm).

[8] John Bohannon, *Why criminals can't hide behind Bitcoin,* PEKING UNIVERSITY (Mar. 9, 2016, 9:00 AM), http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin (on Mar. 15, 2018, 02:55 pm).

[9] Information Technology Act, 2000.

regulates the collection, use, disclosure, and exposure of sensitive personal information or data by a body corporate which owns, controls or operates computer resource.[10] So even though members and participants would have these standard Internet privacy rights, such rights will probably not reach out and extend to the blockchain in light of the fact that there is no centralized organisation that collects data. On the off chance that we take a look at the IT Act's language (Section 43A), protection and privacy on the blockchain would likely not be available on the grounds that there is no single "body corporate" is collecting data and "own[ing], control [ling] or operat[ing]" a computer resource (unlike what a customary web service does, for example). Rather, data is imparted to all blockchain members and participants, and control is decentralized. Enterprise deployment of business and commercial blockchain technology may accordingly hope to address these security concerns, consolidating protection and privacy by design.

ii) Cybersecurity

On the off chance that high esteem value transactions and records will be moved to the blockchain, cybersecurity becomes essential. Data breach are being declared every day, and the Ethereum DAO hack demonstrates that the usage and implementation of blockchain technology isn't dependable and is not infallible (despite the fact that the basic underlying technology is broadly recognized to be robust, powerful and secure). For example, members' private keys (put away and stored on their gadgets/devices or potentially on the cloud) can open up and unlock their entire possessions and holdings, making private keys a clear target, and often a single point of failure. The existing gauge on information security and data protection, for example, the IS/ISO/IEC 27001 standard that the Rules say, will usually not be sufficient for the blockchain, in light of the fact that they were not designed according to its decentralized nature.

iii) Complications due to Irreversibility

In an ordinary circumstance, the cheated and defrauded parties could approach courts, administrative and regulatory bodies (in India, one could approach the RBI under the Banking Ombudsman Scheme), or third party gatekeepers (like banks) to either

[10] Section 43A, IT Act, read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(a) reverse the fraud, or (b) get compensation. In blockchain transactions, however, (a) deceitful and fraudulent transactions can't be switched or reversed by any central party, and (b) it is difficult and troublesome for courts to follow and trace the wrongdoer, and to uphold and enforce a judgment.

iv) Regulating TOR

The most significant Dark web policy issue is regulating Tor. The Darkweb couldn't exist without anonymising technology. There is nothing inherently criminal about use of Tor for anonymity, however there is no clear way to sort the offenders from the innocent users if they are for the most part anonymous. It is hard to consider somebody responsible for their activities if their identity is unknown, and it is difficult to unmask one individual without having the capability to deanonymise every other person using Tor.

v) Jurisdictional questions

The Internet itself has brought up several issues and questions on the most proficient method to decide when a given jurisdiction's law would administer or govern a given situation. In case of an ultra-decentralized technologylike the blockchain, the difficulty with respect to these jurisdictional questions is amplified. This is because there are no identifiable 'hosts' or 'administrators' or ‘operators’ as there are for common ordinary websites and apps. This makes identifying legal obligation and responsibility difficult. Also, servers for all theblockchain network are decentralized and likely spread all through the world, making it difficultto pinpoint where a breach or failure occurred.[11]

vi) Difficulty in evidence collection

Since the Dark Web is in flux, everything is very dynamic. Illicit commercial marketplace are moving locations consistently, making steady changes the naming and address schemes in the Dark Web. The information collected from the Dark Web two weeks back will no longer be relevant today.[12] So if a judge or an investigator needs to check a URL involved with a criminal case, they end up nowhere. So, one needs to archive and document everything, one needs to have

[11] BLOCKCHAIN AND THE LAW: THE UNCHARTED LANDSCAPE, CLYDE & CO.,https://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF (on Feb. 28, 2018, 10:25 am).

[12] Q&A: *Deep Web, Anonymity and Law Enforcement,* TREND MICRO INC. (Sept. 10, 2015), https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/qna-deep-web-anonymity-and-law-enforcement (on Mar. 5, 2018, 07:35 pm).

screenshots and the proofs are to be made with timestamps, so that the chain of contention cannot be broken.

7. Dark web and Bitcoin: legal status in India and abroad

Browsing dark web is neither legal nor illegal in India. Since there is no law or regulation applicable on browsing dark web within the territory of India, one cannot be imprisoned just for browsing the same. However, buying and selling of illegal products is a punishable offence under IT Act 2000.

However, no enactments and legislations exist in India to control illegal activities occurring on the dark web. The Information Technology Act 2000 represents the Indian law that convicts cybercrimes. Despite the fact that numerous cybercrimes are being reported in India, no prosecutionhave included illegal activities occurring on the darkweb. Alike India, in US, hacking is regulated by the Computer Fraud and Abuse Act (CFAA), which bans trespassing on, unauthorised accessing of, and damaging computers in interstate or international trade. The CFAA also bars trafficking, unapproved and unauthorised computer access, and computer espionage. These U.S. controls are consummately adequate to deal with hacking, yet they don't particularly handle the problem of anonymity on the web, and they are not really viable and effective beyond U.S. borders, from where most cybercrime against the U.S. is propelled.

However, various countries around the globe have been attempting to regulate the use of darkweb.China has made efforts to block access to Tor which can easily be seen with the coming of the 'Great Firewall'. China seriously considers the danger that Tor postures to their data control. In 2008, China blocked the Tor project's site in order to keep users from downloading the service. In 2009, China tried to obstruct the most part of public relay computers that Tor uses to anonymise users. Russia has attempted to deanonymise Tor for political purposes. On 2 August 2016, Russia's Federal Security Service started enforcing the accumulation and collection of encryption keys from Internet Service Providers (ISPs). A refusal to turn over keys could bring about a one million rouble fine ($15,000). Austria has made efforts to kill Tor traffic inside its border. One of the most dramatic policy actions was made by Austria in 2014. Authorities arrested a man who had made his computer a Tor relay, and held him responsible for 'contributing to the fulfilment and completion ' of a cybercrime perpetrated by another Tor user who had no association or connection with the arrested man, beyond the fact that the cybercriminal's

activity was routed through the arrested man's computer. The verdict has set a precedent of reference that it is conceivably illegal to operate a Tor exit relay in Austria.

The Reserve Bank of India (RBI) has been consistent in warning citizens of the hazard related with cryptocurrencies. In recent time a debate has risen within the country in the matter as to whether profits from crypto exchange ought to be taxed or not.

In a move to regulate the cryptocurrency market in India, Finance Minister ArunJaitley, recently, in his Budget speech of 2018 cleared that it isn't legal tender and its use will be discouraged. However, he said that the legislature will look at the use of blockchain technology. Amid the run-up to the financial budget, there have been discussions that the legislature could come up with a roadmap to manage and regulatethe cryptocurrency market.

The recent action of conducting survey by the Income Tax department over all the major trades has likewise triggered issuance of income tax demand notice by the department to the clients and users of these exchanges. There have been reports stating that few banks have frozen accounts suspected of having cryptocurrency trades and transactions in India, while the Registrar of Companies (ROC) has stopped enrolling companies intending to go about with such exchanges.[13]

The bitcoin's shadow was evident in the supply of money for the 2015 Paris terrorist attacks. The EU is keen to bring the bitcoin under control. The intergovernmental Financial Action Task Force in Paris announced in 2015 that some terrorist sites urged sympathizers to give in and donate bitcoins.[14]

US anti-terrorism officials are likewise anxious about the way how the Islamic State is accumulating a huge amount of dollars through bitcoins.[15]However, US Treasury classified bitcoin as convertible decentralized virtual currency, but Commodity Futures Trading Commission (CFTC) considers it as a commodity.Though, bitcoin is legal in Mexico, the New York state government has already passed a Bill denying and prohibiting bitcoin. Countries like Canada and Australia have brought the bitcoin under the domain of anti-money laundering and antiterrorism laws for regulations. Countries

[13]*SBI, four more banks suspend accounts of major Bitcoin exchanges in India*, BUSINESS STANDARDS (Jan. 20, 2018, 16:18 IST), http://www.business-standard.com/article/markets/sbi-four-more-banks-suspend-accounts-of-major-bitcoin-exchanges-in-india-118012000519_1.html (on Mar. 29, 2018, 6:47 pm).

[14]Atul Biswas and Bimal Roy, *Bitcoin, the new hawala*,THE ECONOMICS TIMES (Jun. 14, 2017, 11:21pm IST), https://blogs.economictimes.indiatimes.com/et-commentary/bitcoin-the-new-hawala/ (on Mar. 14, 2018, 02:35 am).

[15] Ibid.

like Bulgaria and Norway levies taxes on bitcoins as done for ordinary income. In countries like Cambodia, Nepal and Bangladesh bitcoin trading is not legal.

Controlling terrorist funding was one major reason behind Government of India's demonetisation activity. In the event that India neglects or fails to direct and regulate bitcoin, this may ironically turn into an easy method for subsidizing and funding terrorism. The government ought to have legitimate control over bitcoin in light of the interest of the economy and the security of the nation.

The recent development on the regulation of bitcoin can been seen in G20 Summit 2018. As per the recommendation made by France's Finance Minister, a public debate on bitcoin was held in the G20 Summit 2018, held in Argentina. The conclusion of the meeting is that a firm deadline of July 2018 has been given for recommendations to regulate cryptocurrencies globally.

8. Suggestions and Recommendations

Making policies to address the darkweb and the bitcoins require a comprehensive understanding of the advantages and dangers of anonymity and of an open internet. Rash and sweeping enactment can possibly infringe on civil liberties and can be a nightmare to implement. But again, not addressing to the darkweb and the utilization of bitcoins will enable illegal activities to persist unabated. It is difficult to regulate the Dark Web in isolation; any control must be pertinent to the internet as a whole and will thus influence Surface Web users, Deep Web researchers, and Dark Web criminals alike.

When new technologies emerge, the government must determine its part in regulating them. Technical advancements can change the ways our laws apply and necessitate new laws. The darkweb and the bitcoin are brand new topicsto numerous policy makers, and it is essential that they become informed before authorizing and enacting policies as opposed to learning from mistakes. Current laws on internet protection and cybersecurity are vaguely applicable on darkweb. There are no strong legislation to regulate it within legal structure. However, attempts are being made by countries to regulate the use of cryptocurrencies like bitcoin and furthermore to bring them within the ambit of judicial framework.

Some recommendations for regulation on working of darkweb and bitcoins are –

- **Use of CIPAV:** Computer and Internet Protocol Address Verifier (CIPAV) is a data gathering tool used by FBI to recognize and identify suspects who are disguising their location using proxy servers or anonymity services, like Tor. This technology permits

Tor activity to be flagged separately from general internet traffic. It does nothing to compromise the anonymity of users, yet it is useful in narrowing down inquiry and search parameters when the investigation is performed.

- **Web crawling:**Given the enormous size of deep web, it won't be practical for the authorities to physically visit every webpage and assess its content for possibly illicit nature. Web crawling can be utilized to crawl and index a huge number of such sites in short notice and can be programmed to report when certain catchphrases and keywords are detected. This makes findingthings on darknet easier.
- **Customer data monitoring:**If security organizations and agencies can tell individuals are going on darkweb, one can make inferences from it. This can be done without intruding the privacy of the users as just the destinations of web requests are to be observed and not who is connecting or interfacing with them.
- **Social site and hidden service monitoring:**Regular websites, for example, Pastebin, where links todarkweb are frequently posted must be kept under observation.
- **Semantic analysis:**Once adarkweb is discovered, it should be downloaded and its data should be stored in a database for future analysis.
- **Tracking down the bitcoin:** Though bitcoin is not associated with personal details of the holders, each bitcoin transaction is recorded in a public log with their wallet IDs. Bitcoin logs can be continuously monitored and observed for cues that can lead to a connection.
- **Encrypting the transmission layer:** The encryption policy should mandate that all providers of mass-market services transitionto secure encryption protocols, for example, SSL/TLS. This will include generating new set of encryption keys for each transaction and will guarantee forward secrecy. Encrypting the transmission layer will ensure that even if the user is exploited, his past transactions would stay secure and the level of potential harm and damage would be confined.
- **Updating the legal framework:**Update existing laws and regulations to deal with the proliferation of secured communication services. The government must support the development of research in cyber security and cryptographic tools. The laws should endorse constrains and prescribe limits on lawful access to encrypted communications that are proportionate and effective.

9. Conclusion

Technology is neither good nor bad, it is the users who make it act in either directions. The countries must rise to the challenge of authorizing policies that effectively strikes harmony between ensuring users' anonymity and avoiding illegal activities on the web. Countries around the globe have diverse positions on how best to handle the challenge of Tor. Given that international cooperation will be essential, governments must cooperate towards creating smart darkweb policies. The specific strategies for intervening on the darkweb must be deliberately and carefully considered. By learning from past mistakes, leaders can make policies that viably and effectively tends to address the challenges of tomorrow's internet.