DEEP INTO THE DARK WEB: THE PRIMROSE PATH OF BITCOINS

SATHIABAMA S*

ABSTRACT

The growth in the nucleus of information technology is quick as a wink with the wide enlargement in the number of internet users. Like how every human being has a dark part of the life, the internet also has a gloomy evil behind it. This is the "Dark Web" which cannot be accessed through the normal search engines but requires the usage of special software. Though the Dark Web, on one hand, protected the anonymity of vulnerable people online, it remained as the dawn of an era to the abuse of technology leading to cybercrimes. The financial transactions made to avail anything in the dark web are through digital currencies of the most popular bitcoins. But, the legal field is not able to govern the dark part of the web due to the shield of anonymous searches. Hence the Courts are unable to consider digital evidence from such a part where there is no jurisdiction. At this juncture, this paper would bring out the illegality of using the dark internet and bitcoins, thereby argues to criminalize anyone who gains access to it. So, it is high time to cut off the expanding thread of players online.

I. INTRODUCTION

The Internet is the window to look into the whole world containing both pleasant and unpleasant things. It is in the hands of the viewer whether to see the good or the bad. Some are interested in the bad part of it which creates harm to the rest or many times even results in danger. Though it is unfortunate that the window is not able to hide the bad things from the viewers, the law can take a step forward to criminalize those people who do so, thereby preventing a future disaster that might result. Around 4,208,571,287 people in the world are Internet users among 7,634,758,428 of the population according to the statistical data as on June 30, 2018.[1] When such is the case with the world, 462,124,989 persons are Internet users from India which is 34.1% of the Indian population as on December 31, 2017.[2] This shows the rate at which usage of the Internet has been growing which signifies *digital revolution* and a limitless borderless expansion.[3] It

* The Author is a Final Year B.A., LL.B (Hons.) Course student at the Tamil Nadu National Law University (TNNLU), Tiruchirappalli.

[1] Internet World 'Internet Users in the World by Regions Stats' <https://www.internetworldstats.com/stats.htm> accessed 26 November 2018.

[2] Internet World 'Internet Users in Asia by Regions' <https://www.internetworldstats.com/stats3.htm#asia> accessed 26 November 2018.

[3] Karnika Seth, Computers, Internet and New Technology Laws (1st rev Edn, Lexis Nexis 2013).

also has given rise to the need for updating the cyber laws throughout the globe. These Internet users make use of search engines like Google, Yahoo, Bing, and others to access the available data. But certain sites are inaccessible through standard search engines and are intentionally hidden. The masked part of the Internet is the *Dark Web* which serves as a platform for those Internet users who intends to surf as anonymous, as it not only provides protection for unauthorized users but also usually includes encryption[4]to prevent monitoring.[5] It can be accessed only through special software such as Tor (The Onion Router), Onion. City, Onion.to, Not Evil, I2P (The Invisible Internet Project), etc.

The Researchers at King's College London found that out of all these, 57 percent of the sites designed for Tor popularly known as .onion sites open doors for criminal activity which includes drugs, illicit finance, and extreme pornography.[6] The Tor browser was created by the US Naval Research Laboratory[7] in the mid-1990s allowing intelligence operatives to exchange information completely in an anonymous manner.[8] Later, Tor was released into the public domain for anyone to use.[9] As part of their strategy for secrecy, their reasoning was simply that the more people using the system, the harder it would be to separate the government's own messages from the general noise.[10] Tor spread widely and is a critical part of the dark web today.[11] But this anonymity has attracted a lot number of people who wanted to keep their activities secret.[12] The Research concluded that more than 50% of what is hosted on the website contained illicit and

[4] Encryption is a secure method of communication where only the people communicating can access messages sent. Eavesdroppers, such as cyber-criminals and hackers, telecoms and Internet providers or governments or even the law-enforcement agencies cannot read communications. Even the company that built and runs the service cannot access messages, and hence cannot easily cooperate with authorities who request these exchanges. Madhumita Murgia, 'WhatsApp adds end-to-end encryption: What is it and what does it mean for you?' (Telegraph, 6th April 2016) <http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/> accessed 26 November 2018.

[5] Michael Chertoff and Tobby Simon, 'The Impact of the Dark Web on Internet Governance and Cyber Security' (2015) 6 CIGI <https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf> 26 November 2018.

[6] Cara McGoogan, 'Dark web browser Tor is overwhelmingly used for crime, says study' (*The Telegraph*, 2 February 2016) <http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/> accessed 26 November 2018.

[7] 'Inception' (*Tor*) <https://www.torproject.org/about/torusers.html.en> accessed 26 November 2018.

[8] iWonder, 'What is the Dark Web and is it a threat?' (*BBC*) <http://www.bbc.co.uk/guides/z9j6nbk#zcxvrdm> accessed 26 November 2018.

[9] ibid.

[10] ibid.

[11] ibid.

[12] ibid.

illegal material.[13] The normal search engines provide access to around 5% of the content on the web only[14].

In the past, Tor had been used by the Journalists to communicate with the whistle-blowers and activists.[15] However, the illegal content and the criminal activities in the dark outweighed anything else. This remains as a platform to sell illicit goods including weapons, drugs, trade in both physical and proprietary information, make illegal financial transactions, and promote paedophilia, gambling and also aid in carrying on terrorism.[16] The Assassination Market is an interesting place where people bet on the date of death of others.[17] There is something popular in the dark net called the "Hidden Wiki" which promotes contract killing, money laundering services, cyber-attacks and also provide instructions to make explosives.[18] Some sites also enable human experimentation with the help of homeless people.[19] One can also order on the darknet to rob something which one is not able to afford.[20] It also plays the role of a hacker's market to sell the credit card numbers, Social Security Numbers and other personal data which they have hacked already to the interested buyers.[21]

One might wonder how anything could be bought or sold in the dark web. Any transaction in the darknet is made through digital currencies. Bitcoins remain to be the most popular digital currency running around the dark Internet. It was also affirmed by the study made by two professors at the Department of War Studies at King's College London.[22] Daniel Moore, a cyber-threat intelligence engineer in the Department of War Studies wrote, *"Bitcoin is the most common currency employed in all Tor hidden-services trade"*.[23] One of the reasons for its popularity is that bitcoins

---

[13] McGoogan (n 6).

[14] Lesly Stahl and Shachar Bar-On, 'New Search Engine Exposes the Dark Web' (CBS News, February 2015) <https://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/> accessed on 26th November 2018.

[15] Explainer: what is the dark web? (*The Conversation*, 13 August 2015) <http://theconversation.com/explainer-what-is-the-dark-web-46070> accessed 26 November 2018.

[16] McGoogan (n 6).

[17] ibid.

[18] ibid.

[19] ibid.

[20] ibid.

[21] Daniel Ingevaldson, 'What's lurking in the Deep End of the Internet?' (*Wired*) <https://www.wired.com/insights/2015/03/whats-lurking-deep-end-internet/> accessed 26 November 2018.

[22] Michael del Castillo, 'Bitcoin Remains Most Popular Digital Currency on Dark Web' (*CoinDesk*, 21 March 2016) <http://www.coindesk.com/bitcoin-remains-most-popular-digital-currency-on-dark-web/> accessed 26 November 2018.

[23] ibid.

are used globally and it also maintains anonymity in the web, unlike the payments which are made by credit cards and PayPal by which the user can be traced back.[24] Hence the dark web also sets a threshold for the bitcoins to play around making transactions easier and non-regulation by Law or Government.

The unique relation between dark web and usage of bitcoins is their anonymity which links them together leading to more and more crimes in the virtual world. The usage by unknown users remains as a shield from the interference of Laws in the large worldwide digital market. This paper would enlighten on the concept of regulation by Law thereby reducing the crimes in the virtual market and protect vulnerable people within the cloak. It also would in parallel concentrate on the primrose path of bitcoins into the dark web which is dangerous to many using the web. In the current world of digital generation, the Internet should only remain as a boon and not as a bane which is usually the most debated topic all over the globe. It should be made known to people how worse or dangerous it could become while using the dark web. Hence it is high time for the Law to take action in order to prevent a greater harm to the society.

II. LAWLESSNESS IN THE CROOKED DARK NET

It is popularly said that law can do anything except changing a man into a woman and vice versa. But, the dark web is the forum into which the law has not been able to intervene because of the shield of anonymity. This enables the dark market to soar high without the intervention of law into its business. However, this Chapter would give an insight into the stand of law in the United States and India for dark web crimes.

A. Position in the United States of America

A talk about the dark web without involving the news of the famous *"Silk Road" (Dread Pirate Roberts[25])* is incomplete. It was created by Ross Ulbricht aged 29, on January 2011 and is the most sophisticated and extensive criminal marketplace on the dark web, and served as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually all

[24] Dean, 'Dark Markets: How to Buy Things from the Deep Web's Black Markets' (*Cryptorials*, 11 July 2015) <http://cryptorials.io/dark-markets-how-to-buy-things-from-the-deep-webs-black-markets/> accessed 26 November 2018.

[25] Alois Afilipoaie and Patrick Shortis 'Silk Road: After being closed twice, can the brand ever rise again?', (GDPO Situation Analysis, January 2015) <https://www.swansea.ac.uk/media/GDPO%20SA%20silk%20rd%20rise%20again.pdf> accessed on 26th November 2018.

varieties, were bought and sold regularly by the site's users.[26] It had thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to more than 100,000 buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions.[27] However, the law enforcement agencies from the period of November 2011 to September 2013 made more than 60 individual undercover purchases of controlled substances from Silk Road vendors.[28] The anonymity in Silk Road was maintained in two principal ways of operation through Tor network and a Bitcoin-based payment system.[29] Finally after a four week trial, on February 5, 2015, Ross was convicted by U.S. District Judge Katherine B. Forrest on the following seven offences (counts) under Rule 7(c)(1) of the Federal Rules of Criminal Procedure, (1) distributing narcotics[30], (2) distributing narcotics by means of the Internet[31], (3) conspiring to distribute narcotics[32], (4) engaging in a continuing criminal enterprise *("CCE or the Kingpin Statute"[33])*, (5) conspiring to traffic in false identity documents[34], (6) a computer hacking conspiracy[35], (7) a money laundering conspiracy.[36] He was ordered with life sentence prison term as well as to forfeit $183,961,921.[37] The Judge also said, *"There must be no doubt that lawlessness will not be tolerated. There must be no doubt that no one is above the law - no matter one's education or privileges. All stand equal before the law. There must be no doubt that you cannot run a massive criminal enterprise and because it occurred over the Internet minimizing the crime committed on that basis"* which proves clearly that even though there was no presence of regulation of law which is an important element for any Court to consider, the Judge ruled against the crimes committed in the case as they were very cruel to the society.

But later in the case of *United States of America v. Alex Levin[38],* where a search warrant called Network Investigative Technique (the "NIT Warrant") was issued, the same was held to run afoul

[26] 'Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison' (*FBI*, 29 May 2015) <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison> accessed 26 November 2018.

[27] ibid.

[28] ibid.

[29] ibid.

[30] Federal Rules of Criminal Procedure, 21 U.S.C. §§ 841 & 846.

[31] ibid.

[32] ibid.

[33] Kingpin Statute, 21 U.S.C. § 848(a).

[34] The Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[35] ibid.

[36] 18 U.S.C. § 1956(h); United States of America v. Ross William Ulbricht 31 F.Supp.3d 540 (S.D.N.Y. 2014

[37] ibid.

[38] Criminal Action No. 15-10271-WGY (D. Mass. 20 April 2016).

of section 636(a) of the Federal Magistrate's Act, 1968 and Rule 41(b) of the Federal Rules of Criminal Procedure which laid jurisdictional limitations on the power of Magistrate Judges. Hence, the Court concluded that the NIT Warrant was issued without jurisdiction and was *void ab initio*. It followed that the resulting search was conducted as though there was no warrant at all. Since warrantless searches were presumptively unreasonable, and the good-faith exception was also inapplicable, the evidence was excluded. However, the current status of bitcoins is that it cannot be considered as a property since they are neither things in possession nor things in action.[39] This is implied from the case of *Armstrong DLW GMBH v. Winnington Networks Ltd*[40] which held that digital tokens that can survive only in the electronic form cannot be the subject of possession. This ruling of the courts in England and Wales, therefore, do not identify bitcoins as property.[41]

B. Position in India

The out bust of Silk Road was an eye-opener to the world in knowing about the dark web and its illegal activities. India is also a growing IT hub to go illegal with such activities. Hence, not much of the news about the usage of darknet in India has been disclosed. But there are certain cases in places like Bengaluru and Andhra Pradesh where dark web users exist. The Telangana State cybercrime cops who are like the FBI were on a mission to survey the dark side of the Internet after knowing the information that there were several Indian customers of Silk Road.[42] A Cybercrime official said, *"Absolute anonymity and encrypted data are the main features here. It's not at all easy to track users. However, we are examining ways to build surveillance capabilities."*[43] In their struggle to capture darknet users, the cops came across two strange teenage suicides in Hyderabad in 2015, which were later found that the teenagers had used Tor in their computers and had watched several suicide videos.[44] Hence, the cops were of the perception that they must have got inspired after subscribing to it.[45] A Cybercrime official from Cyberabad had an opinion that *"Activities on Tor can*

[39] Dave Michels, 'You may not actually own your Bitcoin - legal expert' (*The Conversation*, 24 November 2018) <https://theconversation.com/you-may-not-actually-own-your-bitcoin-legal-expert-107307> accessed 27 November 2018.

[40] [2012] EWHC 10 (Ch.).

[41] Michels (n 40).

[42] K.K. Abdul Rahoof, 'Hyderabad criminals in Deep Web' *Deccan Chronicle* (India, 10 January 2016) <http://www.deccanchronicle.com/150615/nation-crime/article/hyderabad-criminals-deep-web> accessed 27 November 2018.

[43] ibid.

[44] ibid.

[45] ibid.

be punished under the Information Technology Act, 2000. The moment people clinch deals for illegal goods and services on Deep Web they are liable for legal consequences, both civil and criminal."[46]

Further, there was another case in Hyderabad which dealt with the buying of contraband from China by the Sahu brothers, Mayank Kumar Sahu and Piyush Sahu.[47] The Task Force police, along with Anti-Narcotics Cell (ANC) and sleuths of the Central Crime Station (CCS), had arrested them and taken them into custody to know more about the people involved in similar crimes and also to know how they operated.[48] Here the officials were of the idea that the only way to combat is through regulating the delivery system.[49] But there are also other crimes which are carried out without the use of delivery of goods on the dark web. There were also similar cases in Bengaluru which involved buying of drugs on the dark web through bitcoins.[50] Pavan Duggal, a Mumbai based cyber law expert was of the idea that *"Only a few are actually aware of this. There are no laws in the darknet. The levels of anonymity cannot be regulated. It is hard to even collect incriminating electronic evidence. It is unfortunate that we have not even begun thinking in this direction yet."*[51] This serves as a yardstick for the Researcher to think in that direction which will help to combat dark web crimes and prevent the misuse of anonymity.

Therefore the position in the *Armstrong case* applies to the United States of America and India, where the degree of legal protection is unclear.[52] It can be implied that bitcoins cannot be considered for evidence if they are not recognized as property and thus would take any criminal case to its worse situation when its evidence is missing or not marked by the Court of law. The laws in the above two countries are neither regulating the dark web nor its crimes. This serves as the platform for virtual criminals to grow crooked in the dark web by carrying on illegal activities. But nothing should be above the law. Law should always have a control over anything in the

---

[46] ibid.

[47] Mahesh Buddi, 'Drug peddlers the first 'deep web' arrests in Telangana, AP' *Times of India* (India, 18 December 2015) <http://timesofindia.indiatimes.com/city/hyderabad/Drug-peddlers-the-first-deep-web-arrests-in-Telangana-AP/articleshow/50229361.cms> accessed 27 November 2018.

[48] ibid.

[49] ibid.

[50] Aritra Sarkhel, 'The deep, dark side of web! How people are getting drugs, guns delivered at doorstep' *The Economic Times* (India, 27 July, 2016) <http://economictimes.indiatimes.com/industry/tech/internet/the-deep-dark-side-of-web-how-people-are-getting-drugs-guns-delivered-at-doorstep/articleshow/53407720.cms> accessed 27 November 2018.

[51] Saba Firdaus, 'Surfing the dark net for drugs' *The Hindu* (India, 13 July 2015) <http://www.thehindu.com/news/cities/bangalore/surfing-the-dark-net-for-drugs/article7414381.ece> accessed 27 November 2018.

[52] Michels (n 40).

society. That part of the society which is free from the regulation of law will lead to chaos. Some might misconstrue this to be a protection of privacy or freedom to enjoy oneself in the virtual world, but the reality will not end up so.

III. THE MERRYMAKING GAME OF BITCOINS

The dark web transactions are made through electronic money and the most preferred is the Bitcoin. It is a decentralized digital currency also known as crypto currency created by a person, Satoshi Nakamoto in 2008.[53] It can be used to purchase items both electronically and locally using the bitcoins stored in one's Bitcoin wallet.[54] This process is very transparent and it is governed through one's private and public keys which maintain the anonymity of the buyer and seller of any transaction.[55] Accordingly, section 42 of the Information Technology Act, 2000 imposes an obligation on the subscriber of the electronic signature to maintain complete confidentiality of his or her private key and if the same is compromised, the subscriber is under an obligation to inform the certifying authority.[56] The keys help in concealing the real name of the owner of the bitcoins as it only reveals the public address which the owner wants to show to others. Hence it is very clear that the flow of bitcoins in e-commerce is not regulated by anyone like the decentralization of Internet activity.

This allows the bitcoins to play in the dark web which also requires deregulation and anonymity so as to carry on any activity without getting webbed into any law. People are more susceptible to commit crimes by using bitcoins in the dark web when they are completely concealed within the blanket of anonymity. Very recently a man named Minnesota was charged with felony second-degree intentional homicide in the slaying of his wife, Amy Allwine in the month of November 2016 and he was called for trial on February 13, 2017.[57] This was a pre-planned plot to kill his wife in South Washington at their home. The accused initially tried to hire a hit man in the dark web to murder his wife which had failed.[58] Later after the failure of the first attempt, he has

[53] Carter Graydon, 'What is Bitcoin?' (*Cryptocoins news*, 10 September 2014) <https://www.cryptocoinsnews.com/bitcoin/> accessed 27 November 2018.

[54] ibid.

[55] ibid.

[56] Seth (n3) 166.

[57] Snejana Farberov, 'Husband is charged with shooting dead his wife then trying to disguise her death as a suicide by staging her body with a handgun 'after failed murder-for-hire plots paid for with bitcoins on Dark Web" (*Mail online*, 18 January 2017) <http://www.dailymail.co.uk/news/article-4133592/Man-charged-slaying-wife-pretending-killed-self.html> accessed 27 November 2018.

[58] ibid.

bought a gun in the dark web by making the payment in bitcoins.[59] He then shot dead his wife after poisoning her and made it look like a suicide scene.[60] While three police agencies were involved in investigating the case, Sgt. Randy McAlister of the Cottage Grove police said *"the Dark Web distinguishes the case from more common murder cases. The Internet factor has required more time for the investigation."*[61] Hence, the improvement of technology in the Internet activity has been a difficulty and a negative means to achieve things.

Further, there was another case of an illegal Bitcoin exchange *Coin.mx* which was run by Anthony Murgio of 33 years of age along with his father Michael Murgio and laundered cash for Internet criminals including drug dealers, and facilitated extortion schemes.[62] It also marked the massive bank hack which was one of the biggest thefts of customer data ever that stole information from more than 100 million people, according to prosecutors.[63] He was held guilty on January 9, 2017, and was sentenced to a year of probation, 200 hours of community service and a $12,000 fine thereby avoiding jail.[64] The unanimity in all the Bitcoin crimes is that it is committed by youngsters who had passed out their degrees and are involved in this activity having the notion that they can gain more money.

The Bitcoins were not only used in the dark web, but its usage in itself has led to fraud after the demonetization scheme in India. It was the time when Indians bought bitcoins at a premium of 35% from local Bitcoin exchanges.[65] Hence the Reserve Bank of India reminded the users by issuing a public notice in the month of February 2017 that the crypto currency or any businesses related to it were not authorized and were not subjected to consumer protection laws.[66] India's Central Bank, despite having the agenda to embrace digital payments and financial technologies do not permit Bitcoin as legal tender.[67] It has also installed a new *"Payments Regulatory*

---

[59] Lester Coleman, 'Minnesota Murder Plot leads to Dark Web Investigation' (*Cryptocoins news*, 20 January 2017) <https://www.cryptocoinsnews.com/minnesota-murder-plot-leads-to-dark-web-investigation/> accessed 27 November 2018.

[60] ibid.

[61] ibid.

[62] Lester Coleman, 'Bitcoin Exchange Coin.mx Criminal Case Sees Murgio Senior Evade Jail' (*Cryptocoins news*, 1 February 2017) <https://www.cryptocoinsnews.com/bitcoin-exchange-coin-mx-criminal-case-sees-murgio-senior-evade-jail/> accessed 27 November 2018.

[63] ibid.

[64] ibid.

[65] Samburaj Das, 'Bitcoin Fraud is Becoming Frequent says Indian Crime Branch Official' (*Cryptocoins news*, 6 March 2017) <https://www.cryptocoinsnews.com/bitcoin-fraud-becoming-frequent-says-indian-crime-branch-official/> accessed 27 November 2018.

[66] ibid.

[67] ibid.

Board" that will oversee and handle digital payment gateways which had become hugely popular in India post-demonetization but will not be including Bitcoin under the revised set of Fintech-friendly regulations[68].[69] Therefore, the Indian scenario does not recognize the use of bitcoins in the e-commerce industry. But its usage has not come to a halt completely which allows virtual criminals in the digital market to commit even more crimes than before taking a primrose path which the general public is not realizing as a *prima facie* case.

IV. THE LAW OUGHT NOT TO WAIT FOR THE FUEL TO BE ADDED TO THE EVIL

The virtual crimes resulting through the dark web has only been increasing since its start. This has been violating the laws of all countries even if it is out of the regulation of those laws. However, the law is not static and has to update itself to the changing needs of the people. The Researcher argues that law cannot be waiting until something very severe occurs to the society. The only way to control virtual crimes is by way of enforcement of laws thereby making corresponding amendments to the existing laws. All the countries in the world at any time can amend their domestic laws accordingly so as to regulate the operation of the dark web. The following are the measures put forth by the Researcher to combat dark web crimes with respect to Indian laws.

A. Amendment to the Information Technology Act, 2000

The Central Government has the power to make rules to carry out the provisions of the IT Act under section 87 of the Act. It should frame rules to regulate and control the dark web in such a way that it will be used only for that purpose for which it was created. The purpose was to maintain Government's communication in a secret place like the dark web. So it should be used for that instead of the usage which results in the commission of offenses. The new rule should direct the Government to use various techniques like Network Investigative Technique (NIT)[70]

[68] India has historically had cautious regulations on financial activity and with the advent of Fintech as a sector have been cautiously evolving its policies to tap into the potential while attempting to balance the need for the right amount of oversight with the need to facilitate new entrants and technology to ensure greater availability, choice and most importantly better financial inclusion in the country. 'Fintech India' (*MAPE Advisory Group*, June 2016) <http://mapegroup.com/pdf/mape-fintech-2016.pdf> accessed 27 November 2018.

[69] Das (n 66).

[70] It is a computer program designed to reveal the IP address of the user and it has been used by FBI to hack systems. Forrest Stroud, 'Network Investigative Technique (NIT)' (*Webopedia*)

and Memex[71] which expose dark websites. Once the location is exposed by using the technique, the law has no concern about the line of jurisdiction. Hence when the jurisdiction is set forth, all the corresponding provisions should be made applicable to the rules framed to regulate the dark web. Therefore, amending the IT Act is the first step to control the dark web.

B. Amendment to the Reserve Bank of India Act, 1934[72]

Section 22 of the RBI Act provides a monopoly to issue bank notes to the Reserve Bank of India. This also includes bitcoins as electronic money which is similar to real cash. Initially, the RBI released a notice cautioning the users of virtual currencies including bitcoins to be at risk.[73] Hence there should a regulatory mechanism in issuing these so as to avoid anonymity and future risk. It can be made possible by allowing the Non-Banking Financial Institutions in India which are governed by Non-Banking Financial Company (NBFC) Regulations to regulate the same.[74] For this purpose, section 22 of the RBI Act should be amended accordingly providing for issuing and exchanging of digital currencies including bitcoins by Non-Banking Financial Institutions.

C. Corresponding Amendment to the Code of Criminal Procedure, 1973, the Indian Penal Code, 1860 and the Indian Evidence Act, 1872

Sections from 93 to 101 under Cr.P.C which are relating to search warrants are in the context of the property of persons. In the present scenario, the exposure techniques such as Network Investigative Technique (NIT) and Memex which reveals dark websites should be issued as warrants by the Courts once there is a suspicion of a crime committed using the dark web. This will enable the respective authorities to hack the particular website and system to find the IP address thereby knowing the location of the user. This *hack warrant* is similar to the search warrant issued to police officers. However, all the processes can be carried on only when there is a

<http://www.webopedia.com/TERM/N/network-investigative-technique-nit.html> accessed 27 November 2018.

[71] A powerful new search engine developed by DARPA, the U.S. military's Defence Advanced Research Projects Agency with the help of the inventor Chris White. Memex goes far beyond the realm of traditional search engines and gives law enforcement a powerful new tool to search the "dark web", where criminals buy, sell, and advertise in the illegal weapons trade and sex trafficking. *'New search engine exposes "dark web"'* (n 14).

[72] Hereinafter referred as "RBI Act".

[73] 'RBI cautions users of Virtual Currencies against Risks' (RBI, 24 December 2013) <https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/IEPR1261VC1213.PDF> accessed 27 November 2018.

[74] Seth (n 3) 167.

suspicion of a virtual crime relating to the dark web which is like every other crime which can be taken cognizance only when it comes to the notice of the police. Accordingly, the Cr.P.C provisions should be amended and similarly, the provisions of IPC should also be amended to include punishment for the commission of dark web crimes granting a higher degree of punishment than usual as such commission would generally result in a collective breach of many provisions. Moreover, even when the jurisdiction is not sure the Courts should be in a position to order punishment if any of the offenses had been committed like in the case of the *Silk Road*. Therefore, amendment to the provisions of Cr.P.C and IPC would create fear in the minds of the people thereby serving as a preventive measure from using the dark web. The corresponding evidence collected through the hack warrant should be considered as electronic evidence under section 3 of the *Indian Evidence Act (IEA), 1872* and the same should be admissible under sections 65A and 65B of IEA which should also be amended accordingly.

V. CONCLUSION

With the huge uprising of global markets, the digital market has become one of the most significant tools to involve people's corrupted minds in gaining pleasure and money. This set alights the fire in them to commit any crime in order to achieve anything in the world. The dark web has been the place for such people to fulfil their gains where they can roam around as unknown persons provided they can enjoy a little more than others if they own digital currencies especially bitcoins. When everything is unknown, the jurisdiction of all the activities is also unknown which is where the law is stuck up and not able to regulate it. But lawlessness or lack of jurisdiction should not stand as a bar to punish any criminal which will not serve justice to the aggrieved in the society. Therefore, the lousy conglomeration of Dark Web and the bitcoins is proving to be a dirty foul play in the virtual universal market. Further, the role of bitcoins along with the dark web makes it more difficult to find any piece of evidence related to the crime. Therefore, the law should take cognizance of the dark web crimes at the earliest to avoid a greater harm for which the Researcher has proposed few measures such as an amendment to IT Act, RBI Act, Cr.P.C, IPC and IEA by the Legislature. These measures would decrease the dark web crimes if at least not *in toto* which itself would create a sense of fear in the minds of the people to prevent the same. Therefore, the objective of the IT Act in regulating electronic commerce and that of the criminal major Acts in granting punishment and serving justice will be fulfilled. This would improve the safe browsing of the Internet by regulating it by the law of the land.

****