MEASURES TO CURB THE CYBER MENACE RELATED TO CRYPTOCURRENCIES

KIRUTHIKA D[1], **Dr. KESAVAMOORTHY RENGANATHAN**[2]

[1]Research Scholar, VIT School of Law, VIT, Chennai-600010, India

[2]Associate Professor, VIT School of Law, VIT, Chennai-600127, India.

Email ID: [1] kiruthikaadv@gmail.com [2]kesavamoorthy.r@vit.ac.in

ABSTRACT

Advancements in technology have affected modern society in numerous areas, including communication, education, commerce, and so on. Cryptocurrencies in general and Bitcoin in particular are the most discussed topics of recent times. Cryptocurrencies are considered to be a subset of virtual currencies which are electronic in nature; protected by cryptography and used for peer to peer transaction payment. The acceptance given to cryptocurrencies across various industries and among various countries is steadily increasing due to the decentralised concept which operates free of central banks. In spite of the use of cryptography providing additional security, like any other business zone, cryptocurrencies are also prone to cyber-attacks. Cryptocurrencies are considered to be the criminal's heaven. The paper identifies the central features of cryptocurrencies i.e., decentralisation, untraceability, anonymity that forms the main drawback inviting cyber criminals to this zone. The paper further research the various cyber risks and reports the incidence of several record of ransomware attacks, account takeover, phishing, hacking and other security violations of cryptocurrencies. The paper located the diverse measures taken by the Indian Government towards handling of these cyber crimes like framing new Rules under Section 70 B (6) of the Information Technology Act, 2000 in the form of Cyber Security Directions, etc. The authors suggest various cyber security measures to curb the menace and discuss the use of Artificial Intelligence with its scope in combating these identified cyber risks.

Keywords: *Cryptocurrencies, Cyber risk, Cyber security, AI, Safety mechanism.*

1. INTRODUCTION

Advancements in technology have affected modern society in numerous areas, including communication, education, commerce, and so on. These advancements have brought incredible benefits; they have also provided opportunities and motivation for various forms of crime. The pace of technological change is such that law and policy are subject to continuous challenge. The growth of technology in the world has had an influence on human beings, especially in relation changes in attitudes that consider technology to be a goal, rather than a tool. The technology change, especially in the field of information technology has not have been balanced by legal instruments. The negative impact of rapid technological development is seen in changes in human behaviour, which tend to be criminal. One such area is cryptocurrencies.

Cryptocurrencies in general and Bitcoin in particular are the most discussed topics of recent times. Cryptocurrencies are considered to be a subset of virtual currencies which are in electronic form; protected by cryptography and used for peer to peer transaction payment. By their very definition, crypto means, "hidden," and "not acknowledging openly" [1]. In the words of Satoshi Nakamoto, "crypto currency is purely a peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution" [2].

The acceptance given to cryptocurrencies across various industries and among various countries is steadily increasing. The survey shows that 4% of employees in United States of America quit their employment because of their gains from crypto investments [3]. El Salvador, Central American country planned to build the world's first Bitcoin City which is funded by bitcoin backed bonds [4]. The Time Magazine is going to hold one of the cryptocurrencies on its balance sheet [5]. There are few theatres which are ready to accept cryptocurrencies as payment for the movie thickets [6]. Many National Football League stars made their announcements in accepting cryptocurrencies as their salary [7]. The Crypto Market hit its highest market cup of 3 Trillion Dollars in the first half of November, 2021 [8].

In India nearly 15 million to 20 million investors invested 400 billion rupees in cryptocurrencies in India in November, 2021 [9]. India ranks 2nd position in terms of Global Cryptocurrencies Adoption Index for the period from July 2020 to June 2021 from 11th position for the earlier period [10]. It is evident that masses support the cryptocurrencies. There is massive adoption of cryptocurrencies by masses due to the decentralised concept which operates free of central banks.

The threats associated with the crypto world are decade long story. Long story short threats grew along the crypto's wide acceptance over the years. Cryptocurrencies are considered to be the criminal's heaven. Incidence shows the record of ransomware attacks, account takeover, phishing, hacking and other security violations of cryptocurrencies. Victim assistance and compensation is of a great question. Thus, it is high time to research on this grey and emerging area so as to support the growing trade and business in cryptocurrencies to overcome the cyber threats. There is need to look and trace out the effective crypto cybersecurity protocol in place and suggest safety mechanisms.

The Research Methodology of the study mainly depends on the collection of primary and secondary sources from books, journals, websites, case laws and such other sources. This study uses analytical, critical, comparative and other necessary methods to deduce the conclusion and to make out the findings of the study and to provide the suggestions.

There are various literatures on the different aspects of cryptocurrencies which identifies different cyber crimes. However this study deep dives in to the plethora of materials and areas of research to bring all the cybercrimes under one roof. This study has exhaustive coverage of the topics under the cryptocurrencies, which runs to the length and breadth of the topics. The research is comprehensive one and well documented, first of its kind. This study critically examines the topic in detail, enhancing the knowledge and improves the comparative study in the area under various headings.

2. WHAT IS CRYPTOCURRENCY?

Cryptocurrencies are on the verge of replacing national currencies such as the US Dollar, Indian Rupee, Euro, Canadian Dollars, and more. This is because cryptocurrencies have started to become very viable alternatives to traditional currency. Cryptocurrency is a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow, as well as to control the creation of additional units of the currency [11]. Cryptocurrencies are extremely complex code systems or algorithm that encrypts sensitive data transfers. Cryptocurrencies do not have a physical form like paper money or coins. We cannot hold them physically, but we can buy things with them [12]. Former versions of digital currencies were strictly centralized, whereas these new forms of cryptocurrency are decentralized in nature [13]. Because most cryptocurrencies are not regulated by national governments, they are considered as alternative currencies [14] mediums of financial exchange that exist outside the bounds of State monetary policy.

Bitcoin is widely regarded as the first modern cryptocurrency. In the year 2007, Satoshi Nakamoto- a pseudonymous person or group [15], started working on the Bitcoin concept. On October 31st 2008, he released his white paper entitled *"Bitcoin: A Peer-to-Peer Electronic Cash System"* [16]. Since then, there have been other decentralized cryptocurrencies released by several parties. There is a plethora of cryptocurrencies worldwide, including Bitcoin, Ethereum, Primecoin and many theoretical ones have been proposed. Thousands of crypto currencies exist, and more spring into being every month. As on April 2018, there were 1614 types of crypto currencies in existence and but in November 2021, the number turned to be 14933 [17]. Due to this huge flow of crypto currencies the world now is turning to be a world of coins. Block chain inherently challenges to replace all forms of central authority with a decentralized, peer-to-peer, and open source trust protocol. The history of crypto currency is still happening as we speak, because there are always more developments to come [18].

In order to understand what makes cryptocurrencies different from the traditional currencies, one should look into the distinguishing traits of cryptocurrencies. The main characteristics of cryptocurrencies are its volatility; security; non-repudiability; user anonymity; fast and global; transparent; controlled supply cap, etc.

The one word philosophy of cryptocurrencies is decentralisation. Decentralization is the idea that individuals or groups of individuals can interact and transact with each other without needing third parties to validate, monitor, police or regulate these interactions. Satoshi Nakamoto describes a cryptocurrency network as that "timestamps transactions by hashing them into an ongoing chain of hash-based proof of work, forming a record that cannot be changed without redoing the proof of work." In this way, he summed up the form and operation of what came to be called "block chain," a system crucial to bitcoin and subsequent cryptocurrencies. Bitcoin's block chain technology is essentially a decentralized ledger. Thus, it is the transformation from paperless system to human less system. All crypto currencies are block chain, but not all block chain are crypto currencies [19].

The block chain is self-sustaining, peer to peer distributed database ledger technology for managing and recording transactions with no central regulatory and ownership involvement. It is like an online bank ledger, open to both parties in a transaction. Every single transaction in cryptocurrency is encrypted. Once that encrypted transaction takes place, it is added as a "block". The block chain has complete information about different users. A block chain is a continuously growing list of records, as blocks, which are linked and secured using cryptography. Block chain is a distributed ledger system, which is distributed across many computers within the system. The validation of transactions in the network is done as cryptocurrency mining which is a process in which transactions for various forms of cryptocurrency are verified and added to the block chain digital ledger. The cryptocurrency wallet is a protective digital wallet in digital era used to store, send, and get digital currency.

3. FEATURES OF CRYPTOCURRENCIES ATTRACTING CYBER RISKS

In order to understand what makes crypto currencies vulnerable to cyberattacks, one should look into the traits of crypto currencies. The main characteristics of crypto currencies attracting the cyber criminals are as follows:

3.1 Decentralization

Bitcoin's block chain technology is essentially a decentralized ledger. A lot of the crypto currencies available today are built on the block chain technology introduced by Bitcoin. This means that they are decentralized and run on several computers worldwide [20]. They are not owned or controlled by any organization or government. Thus, it is the transformation from paperless system to human less system [21]. They can only go out of use if they do not offer enough value to make them publicly acceptable. Because of this functionality where no single point of control exists, an enormous amount of computational power is required to maintain the network.

3.2 User Anonymity

The design of the block chain that most crypto currencies use ensures that the identities of users are protected. The user identity is never written to the block chain. Transactions are usually carried out on public addresses and not on names or any other detail that can uniquely identify the user. Although it is possible to see which addresses were involved in a transaction, it is not possible to see who the addresses belong to, from just viewing the information on the block chain. This is one characteristic of crypto currencies that has made them very popular.

Several crypto currencies now exist and more are being built every day. A lot of them do not gain public acceptance because their use case is limited or the developers cannot sustain the effort required to support them, but now and then we see one that gains wide acceptance and goes on to become an established currency.

3.3 Unregulated Market

Most nations have now no longer genuinely decided the legality of bitcoin, who prefer instead to take a wait-and-see approach. The major legal obstacle in the recognition of cryptocurrencies is the class to which it can be categorized. There is an identity crisis in cryptocurrencies. Whether is it a financial instrument; is it equivalent to cash; is it a security or is it an intangible asset/commodity. This categorization is much needed before bringing in regulations on cryptocurrencies. However, as in November 2021, El Salvador is the only country that acknowledges bitcoin as legal tender, being the first country to open its doors completely to Bitcoin will assist in enhancing its economy. Some nations have not directly assented to the legal use of bitcoin with the aid of enacting a few regulatory oversights [22]. Since the crypto market is an unregulated market which keeps it out for the stakeholders to exploit the resources at uneven cost.

The above features of cryptocurrencies and the unregulated market form the place of heaven for the cyber criminals to show off their talents.

4. CYBER THREATS ASSOCIATED WITH CRYPTOCURRENCIES

In spite of the use of cryptography providing additional security, like any other business zone, cryptocurrencies are also prone to cyber-attacks. Blockchain was supposed to be secured than the traditional transactions. However, the hackers had other ideas by investing time and brilliance they could crack the tough nuts to open access to the millions. Thus, it is high time to research on this grey and emerging area so as to support the growing trade and business in cryptocurrencies to overcome the cyber threats. Some of the cybercrimes connected with cryptocurrencies are:

4.1 Cryptocurrency Jacking

The recent cyber risk that emerged in cryptocurrency is the crypto jacking. It is defined as using the device unknowingly or without the knowledge of the owner for mining cryptocurrencies. In cryptocurrency jacking, the computer power is harnessed for the own gains of the hackers. This is done by installing a harmful program or snippets of code that secretly gets access to the device and start using the computational power for mining the cryptos [23]. The increase in access to computational power would facilitate the more access to the cryptocurrencies by way of mining. Jacking could also affect the productivity of the devices and compromises other data stored in the devices [24].

4.2 Crypto Ransomware

Ransomware is now one of the common malware from cryptovirology. There had been multiple cases of ransom involving cryptocurrencies. It threatens to publish the user’s personal data which they have gained unlawful access to through a virus. It is the way of extorting money through the encryption of the files by installing harmful program and demanding ransom. Ransom is demanded generally in the form of cryptocurrencies itself. The ransomware gives specific instructions to be followed and compel the victims to make the payment within a short span of time. They also block access to the data and the account until the ransom amount demanded is paid in full or parts. The most recent example is Colonial Pipeline, an American oil pipeline operator that paid hackers nearly $5 million in ransom [25].

4.3 Malware

Malware results in disruption or damage to the device and give rise to unauthorised access to a device which also includes wallet accounts, exchanges, etc. Crypto malware employs certain harmful codes or application to attack the devices. Malware poses a great threat on the security and integrity of the system. It further affects the performance of the system and steal the computational power of the system thereby increase the wear and tear [26].

4.4 Crypto Phishing

Phishing is often done through the deceptive links sent through E-Mails, short message services, through other digital messaging services. Through the phishing link the accounts and credentials of the user will be gained full access. Thus, compromising the security and breach will eventually lead to the loss of crypto assets of the users.

4.5 Account Takeover

The cyber criminals gain control of the user’s account and thereby access the private information like the password, PIN, username, etc. They get access either through the employment of malware, phishing or data available on the dark web. This account takeover is an identity theft. Upon getting the access to the accounts, the criminals withdraw cryptocurrencies from the account or change the login credentials of the account so that the users are denied with access. Most cases, the users do not have the knowledge that their accounts are being compromised until the damage is done [27].

4.6 DeFi Rug Pulls

DeFi stands for Decentralized Finance. DeFi removes the third party involved in the financial transactions. DeFi enables a practice called as Rug Pulls. Smart contracts are one such example of rug pulls. Smart contracts lock the funds in the form of cryptocurrencies for a particular span of time and upon the expiry of the contract or upon the attainment of a specific limit, certain programming functions are employed to steal the funds [28].

4.7 Other Risks

The user's information given in the trading platform by way of registration forms are compromised and get sold in the dark web for monetary benefits. The cyber criminals use the false social media account to contact the crypto users and directly ask for cryptocurrencies from followers. The criminals further go forward and send blackmailing emails demanding for cryptocurrencies or for sharing of private keys. Hackers commit initial coin offering scams by forming fake websites and directing the users to deposit cryptocurrencies into compromised wallet.

5. STEPS TAKEN BY INDIA IN HANDLING THESE CYBER CRIMES

Currently the stand of Indian Government seems neutral and undecided on regulating cryptocurrencies. The then Finance Minister in his Union Budget-2018 speech said, "the government does not consider crypto currencies as legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system"[29]. In April 2017, the Government formed a nine member Interdisciplinary Committee under the chairmanship of Dinesh Sharma, Special secretary in the Economic Affairs Department. The Committee had representatives from the Department of Economic Affairs, Department of Financial Services, Department of Revenue, Ministry of Home Affairs, IT Ministry, Reserve Bank of India, NITI Aayog and State Bank of India. The Committee was mandated to take stock of the current status of virtual currencies both in India and globally; examine the present global regulatory and legal structures governing virtual currencies; suggest measures for tackling the issues related to virtual currencies including issues like consumer protection, money laundering etc and examine other relevant issues related to virtual currencies [30]. On 2nd August, 2017, the Committee submitted its report to the Department of Economic Affairs. The Committee had proffered to ban cryptocurrency.

Apparently, unsatisfied with the report, the Government had formed a high level Inter-Ministerial Committee under the Chairmanship of Subash Chandra Garg on November 2, 2017 to study cryptocurrencies on a global level and further to provide recommendations for its regulation. This Committee had submitted its report in July, 2019 recommending a blanket ban on cryptocurrencies in India with a draft Bill namely Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019. The Government of India had maintained silence over this recommendation of the Committee and in February 2021 the Government introduced The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 whereby creating a facilitative framework for the construction of the Official Digital Currency namely the Central Bank Digital Currencies to be issued by the Central Bank of India [31] and banning all the private cryptocurrencies in the country. But this Bill could not be passed before the Parliament in the Winter Session.

Meanwhile in 2013 and 2018, the Reserve Bank of India issued an advisory to public not to buy and sell virtual currency Bitcoins. [32] The Indian central bank has issued a couple of official warnings on bitcoin [33]. The Central Bank, however, has barred Indian financial institutions from working with crypto currency exchanges and other related services. [34] Several Writ Petitions were filed before various High Courts of the country seeking the issue of a writ of mandamus for directing the stakeholders to declare all virtual currencies, websites and mobile applications facilitating and dealing with virtual currencies as illegal and ban [35] and further to regulate the flow of bitcoins by constituting a committee of experts to consider the prohibition regulation of cryptocurrencies [36]. The Hon'ble Supreme Court of India in March, 2020 by its decision in *Internet and Mobile Association of India vs. Reserve Bank of India [37]*, wherein a three judge bench of the Apex Court had set aside the circular issued by the RBI that prohibited any entity from providing banking services to anyone dealing with virtual or cryptocurrencies.

India’s Computer Emergency Response Team (CERT-in), which is overseen by the Ministry of Electronics and Information Technology has issued a new set of rules under Section 70 B (6) of the Information Technology Act, 2000 in the form of Cyber Security Directions dated 28th April, 2022 [38]. The new rules inter alia also mandate that virtual asset service providers, virtual asset exchange providers and custodian wallet service providers shall maintain all the information they have gathered as a part of the know your customer process and records of financial transactions for a period of five years. For the purpose of KYC, the RBI directions 2016 [39], SEBI circular dated 24th April, 2020 [40] and Department of Telecom notice dated 21st September, 2021 [41] mandated procedures as amended from time to time shall be followed. With respect to transaction records, accurate information shall be maintained in such a way that individual transaction can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses of accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred. Failure to comply shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both. These directions or new rules are effective after 60 days from the date on which it is issued.

India still does not have any Data Protection Law focusing cryptocurrencies. Recourse shall be taken to the Indian Penal Code, 1860 in case of extortion under Sections 383 to 387 and Sections 415 to 420 of the IPC stipulates provisions in relation to cheating. If any person, which may also include a virtual currency exchanges or business, fraudulently induces a deceived person to deliver any property to any person and that act causes or is likely to cause damage to the deceived person, such person can be penalized under Sections 417 and 420 of the IPC. Other legislations like the Unlawful Activities (Prevention) Act, 1967 for punishment for raising funds for terrorist Act [42] and the Information Technology Act, 2000 for punishment for cyber terrorism [43], identity theft [44] and impersonation [45] may be taken as recourse in the absence of any specific regulation or legislations for cryptocurrencies transactions.

At the international level various measures were taken in combating the crimes that take place using virtual currencies. In June 2015, the Financial Action Task Force came up with a “Guidance for a Risk Based Approach to Virtual Currencies” [46]. Project Titanium was launched in 2017 to support law enforcement agencies to investigate and mitigate crime and terrorism that involves virtual currencies and underground market transactions with Interpol as one of the prime partner [47]. Several online games get connected with virtual currencies. Deep connection between dark web and cryptocurrencies was investigated. In the latest case of *AA v Persons Unknown [48]* the English High Court has considered the criminal misuse of cryptocurrencies.

The current stand of the Indian Government is that “Yes” to Blockchain Technology and “No” to cryptocurrencies. The Indian Government is still watching out for the working of virtual currencies. Thus, there exists a trichotomy on cryptocurrencies regulation among the Reserve Bank of India, Indian Government, and Indian Judiciary.

6. ARTIFICIAL INTELLIGENCE IN TACKLING CYBER RISK ASSOCIATED WITH CRYPTOCURRENCIES

The scope of Artificial Intelligence (AI) in combating cyber risk associated with cryptocurrencies is firstly, Detection where AI is employed by way of behavioral analysis to identify abnormal traffics in the crypto transactions. The largest transaction in the crypto network is analyzed by way of multiple sub-graphs through which different characteristic behaviors of the transaction is identified. These transaction patterns reflect general practice among users and any deviation from the same would lead identify the suspicious behavior. Secondly, Prediction where AI identifies the vulnerable code and improves the defenses against the attacks. Thirdly, Response where AI automates the creation of virtual patches for a detected threat or developing new protection mechanisms in real-time. U.S. specialty retailer Avenue deployed a machine learning-based solution to differentiate between normal and abnormal behavior to combat bot attacks, shutting down bot-triggered anomalous behavior like stolen credentials or unauthorized purchases on customer accounts [49].

Deanonymization is needed to detect the fraud in crypto transactions which can be done by finding doubtful behavior in the transactions. AI can be put into force to achieve the deanonymization through two approaches. They are by way of clustering or classification [50]. The various techniques like supervised learning, unsupervised learning, deep learning and graph analysis are used to reduce the level of anonymity in the network system and helps in identifying the real world participants [51]. AI can be utilized to find the identity under the transaction of crypto player. Crypto network holds important details about the miners, their instruments, networks and patterns. Through these details, AI can trace the attacks and doubtful activities.

AI can be used within the system of cryptocurrencies to tackle the cyber security issues. It can be employed in network system for monitoring the anomalies, identification of vulnerable code and to produce defensive patches in case of an attack. This evaluation can be carried out by AI in seconds rather than taking days. AI can help to identify and prioritize relevant aspects of the data, computation, information classification, and other security factors [52]. AI can enhance awareness, respond in real time, and get better cybersecurity.

A combined research and law enforcement partnership was made in the European Union in the year 2017 between agencies and academic institutions from The Netherlands, Germany, Spain, Finland, Austria, and the UK, setting up the “Titanium” project, (Tools for Investigation of Transactions in Underground Markets). Through this project anomaly detection and machine learning techniques were developed as a solution for investigations relating to criminal and terrorist acts using cryptocurrencies on the internet [53].

7. CYBER SECURITY MEASURES TO CURB THE MENACE

Cyber security is a leading national problem. Studies say that cybercrimes related to cryptocurrencies are likely to increase. Kaspersky’s report, titled ‘Cyberthreats to financial organisations in 2021’, warns that cases of fraud involving the world’s largest digital asset are expected to rise next year [54]. The investigating agencies in India still remain a step behind the technology when it comes to cybercrimes connected with cryptocurrencies. Unlike traditional currencies and other assets, we do not have any legislation or guidelines governing cryptocurrencies and adding to it the user anonymity leaves the law enforcement clueless. Thus, the investigating agencies must be trained in this regard and technically sound experts need to be part of the law enforcement in our country. Until then appropriate cybercrime consultant’s services shall be taken. Profiling of the dealer, traders, individual holders and exchanges must be done.

Like any other business entities to protect themselves against losses, crypto related companies shall go for insurance coverages. The need for crypto related insurance is in need of the hour. Cyber liability insurance is in place to certain extend in the market and crypto related risks policies should come up more in future. These policies should cover the risks associated with cryptocurrencies like ransome payments, jacking, phishing, malware, etc.

The cyber criminals easily hide their real identities on the crypto platforms and thereby transform the asset they get in cyber space into traditional currencies. Therefore, the solution to this is locating an effective crypto cybersecurity protocols and controls. The enforcement of certain norms on network participants such as norms supporting information exchange and governing access to the network is critical for ensuring the security of the network. Along with this the users of cyberspace and especially the crypto users should take extra cautious with the applications and the websites that they access and have a sound knowledge about the security features of the platform. The attackers usually don’t touch upon if there lies a high level of cybersecurity protection.

The companies or exchanges that provide the cryptocurrencies services should come up with cybersecurity controls. Like how we use a diamond to cut another diamond, likewise the block chain technology which forms the base for the working of cryptocurrencies shall be used to come up with cybersecurity protocols such as:

- The company’s crypto should replace the third party transaction vendors so that all transactional data between two peers remains encrypted. This will ensure the level of security for the company to keep its records open in public sphere.

- The company's app need to be biometric login enabled and use AI to detect fraudulent activity.
- The company should store wallets and passwords in a secure database and should ensure that the employees undergo a strict background check so as to ensure the assets remain safe.
- The company shall deploy decentralised storage methods, Internet of Things devices, extensive public ledge systems and encryption methods to ensure safety.

8. CONCLUSION:

A regulatory environment that is dense with these new technologies is a very different place to an environment that relies on compliance with norms that are either legally or morally expressed or simply implicit in custom or practice. Like how a diamond is used to cut another diamond, likewise one technology should be used to overcome the challenges posed by another technology. Just because the contemporary technologies are beyond the reach of traditional laws, negating such innovation may not be the right solution. The taboos attached to the advent of advanced technologies must be thrown away.

The use of the internet and other networked services clearly creates jurisdictional questions about the most appropriate place in which legal proceedings should be brought. Although not all countries will agree on the most appropriate ways to respond to crimes of this nature, there are some issues that require urgent investigation, and on these all countries should arguably, agree. There is need for the collaboration between technology developers or computer science scientists and law makers to bridge the existing gap that arises due to the mismatch. It is the need of the hour to balance the independence of an open system with the crime prevention and law enforcement. The dealings of cryptocurrencies are still a grey area in most of the countries and especially in India. The present and future status of stakeholders of cryptocurrencies needs to be answered. As we all can witness that the cybercrime associated with cryptocurrencies are rising steadily, there is an urgent need to bring the cryptocurrency exchanges under regulation and monitoring mechanism.

REFERENCES:

[1] The Cryptocurrency Freedom Philosophy, ASTOUNDING ELEMENTS, (Aug. 2, 2022, 7.07am), http://www.astoundingelements.com.html

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System , BITCOIN, https://bitcoin.org/bitcoin.pdf.

[3] Shomik Sen Bhattacharjee, Cryptocurrency Profits Encouraging Employees in US to Quit Low-Paying Jobs: Survey, GADGETS 360, (Aug. 7, 2022, 11.20am), https://gadgets.ndtv.com.

[4] Caitlin Ostroff, El Salvador to issue 'bitcoin bond' in 2022, THE WALL STREET JOURNAL, (Aug. 4, 2022, 2.13pm), https://www.livemint.com.

[5] Eliza Gkritsi, Time Magazine to hold ETH on Balance Sheet as Part of Galaxy Digital Metaverse Deal, COIN DESK, (Aug. 2, 2022, 4.20pm), https://www.coindesk.com.

[6]AMC Theatres will now accept cryptocurrency Shiba Inu as mode of payment, THE INDIAN EXPRESS, (Aug. 3, 2022, 9.11pm), https://indianexpress.com.

[7]Adam Teicher, Kansas City Chiefs' Sean Culkin becomes 1st NFL player to convert entire salary to Bitcoin, ESPN, (Aug. 5 , 2022 , 8.20pm), https://www.espn.com.

[8]Pawan Nahar, Crypto market m-cap hits $3 trillion mark; will the frenzy continue?, THE ECONOMIC TIMES, (Aug. 6, 2022 , 11.40pm), https://economictimes.indiatimes.com.

[9] India seeks to block most cryptocurrencies in new bill, government says, CNBC, (Aug. 3, 2022 , 12.20pm), https://www.cnbc.com.

[10]Sowmya Ramasubramanian, India ranks second in Chainalysis's 2021 Global Crypto Adoption Index, THE HINDU, (Aug. 7, 2022 , 11.20pm), https://www.thehindu.com.

[11]Usman Chohan, Cryptocurrencies: A Brief Thematic Review, SSRN, (Aug. 2, 2022, 8.20pm), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330.

[12]So what's the story behind Cryptocurrency, SUCCESS RESOURCES, (Aug. 9, 2022, 12.20pm), https://successresources.com/cryptocurrency-history.

[13]The History of Cryptocurrency, CRYPTOCURRENCY ARMY, (Aug. 4, 2022, 1.15pm), https://www.cryptocurrencyarmy.com/cryptocurrency-explained/the-history-of-cryptocurrency

[14] Brian Martucci, What Is Cryptocurrency- How It Works, History & Bitcoin Alternatives, MONEY CRASHERS, (Aug. 7, 2022,1.15pm), https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/.

[15] Bernard Marr, A Short History Of Bitcoin And CryptoCurrency Everyone Should, (Aug. 4 ,2022, 9.15pm), https://www.forbes.com/sites/bernardmarr.

[16] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, BITCOIN, https://bitcoin.org/bitcoin.pdf.

[17] Today's Cryptocurrency Prices by Market Cap, COIN MARKET CAP, (Aug. 6 ,2022 , 11.15am), https://coinmarketcap.com/.

[18]Team Koinex, A brief history of cryptocurrency, MEDIUM (Aug. 3, 2022, 4.30 pm), https://medium.com/koinex-crunch.

[19] Sanjay Mehta, The Story Of Cryptocurrency, BlockChain And ICOs In India Is Still At A Preamble Level, INC 42, (Aug. 7, 2022, 11.30 pm), https://inc42.com/resources/cryptocurrency-blockchain-icos/.

[20]What properties/aspects of cryptocurrency make them usable, replace or supplement traditional currency?, QUORA, (Aug. 3, 2022, 2.40 pm), https://www.quora.com/in/What-properties-aspects-of-cryptocurrency-make-them-usable-replace-or-supplement-traditional-currency.

[21] Sanjay Mehta, The Story Of Cryptocurrency, BlockChain And ICOs In India Is Still At A Preamble Level, INC 42, (Aug. 6, 2022, 4.50 pm), https://inc42.com/resources/cryptocurrency-blockchain-icos/.

[22]Zagorsky. L, Bitcoin is now 'legal tender' in El Salvador – here's what that means, THE CONVERSATION, (Aug. 8, 2022, 2.20 pm), https://theconversation-com.cdn.ampproject.org,

[23]Ray Li, What is cryptojacking?, HACKERBITS, (Aug. 5, 2022, 7.50 am), https://hackerbits.com/programming/what-is-cryptojacking/.

[24]Crypto-jacking-what’s really going on inside your computer?, HACKERNOON, (Aug. 1, 2022, 2.30 pm), https://hackernoon.com/crypto-jacking-whats-really-going-on-inside-your-computer-eca62d2bafcf.

[25]Crypto-Ransomware, F-SECURE, (Aug. 7, 2022, 11.40 pm), https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml.

[26]Kevin Y. Huang , Security 101: The Impact of Cryptocurrency-Mining Malware, TRENDMICRO, (Aug. 3, 2022, 7.20 am), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware.

[27]Account Takeover Fraud (ATO), FRAUD.NET, (Aug. 3, 2022, 8.30 am), https://fraud.net/d/ato-account-takeover/.

[28] Joe Liebkind, Beware of These Five Bitcoin Scams, INVESTOPEDIA, (Aug. 5, 2022, 6.30 pm), https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp.

[29] Vivina Vishwanathan, Cryptocurrency not legal tender in India, but blockchain gets new life in Budget 2018, LIVE MINT, (Aug. 2, 2022, 1.45 pm) https://www.livemint.com.

[30]Government to ban cryptocurrencies from its payments system, GK TODAY, (Aug. 8, 2022, 9.50 pm) https://currentaffairs.gktoday.in/tags/dinesh-sharma-committee.

[31]Rajeev Kumar, Cryptocurrency Bill 2021: Crypto Bill not on Lok Sabha’s revised list of business today, FINANCIAL EXPRESS, (Aug. 2, 2022, 4.20 pm) https://www.financialexpress.com/money/cryptocurrency.

[32]RBI cautions users of Virtual Currencies, RESERVE BANK OF INDIA, (Aug. 6, 2022, 2.30 pm) https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=39435.

[33]RBI cautions users of Virtual Currencies, RESERVE BANK OF INDIA, (Aug. 3, 2022, 11.20 pm) https://www.rbi.org.in.

[34]Prohibition on dealing in Virtual Currencies (VCs), RESERVE BANK OF INDIA, (Aug. 6 2022, 2.45 pm) https://rbi.org.in/Scripts.

[35]Siddharth Dalmia vs Union Of India, WP (C) No. 1071 of 2017.

[36] Dwaipayan Bhowmick vs Union Of India, WP (C) No. 1076 of 2017.

[37]Internet and Mobile Association of India vs. Reserve Bank of India, 2020 SCC Online SC 275.

[38] No. 20(3)/2022-CERT-In Government of India, Ministry of Electronics and Information Technology (MeitY), CERT, (Aug. 9, 2022, 3.55 pm), https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[39] Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, RESERVE BANK OF INDIA, (Aug. 9, 2022, 2.45 pm), https://m.rbi.org.in//Scripts/BS_ViewMasDirections.aspx?id=11566

[40] Clarification on Know Your Client (KYC) Process and Use of Technology for KYC, SECURITIES AND EXCHANGE BOARD OF INDIA, (Aug. 3, 2022, 1.35 pm) https://www.sebi.gov.in/legal/circulars/apr-2020/clarification-on-know-your-client-kyc-process-and-use-of-technology-for-kyc_46565.html

[41] The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC), DEPARTMENT OF TELECOMMUNICATIONS, (Aug. 9, 2022, 9.47 am) https://dot.gov.in/access-services/subscriber-verification

[42] Unlawful Activities (Prevention) Act, 1967, § 17, No. 37 Acts of Parliament, 1967 (India).

[43] Unlawful Activities (Prevention) Act, 1967, § 66F, No. 37 Acts of Parliament, 1967 (India).

[44] Unlawful Activities (Prevention) Act, 1967, § 66C, No. 37 Acts of Parliament, 1967 (India).

[45] Unlawful Activities (Prevention) Act, 1967, § 66D, No. 37 Acts of Parliament, 1967 (India).

[46]Guidance for a Risk-Based Approach to Virtual Currencies, FATF, (Aug. 9, 2022, 6.50 pm), https://www.fatf-gafi.org/documents/documents/guidance-rba-virtual-currencies.html.

[47] Tools for the Investigation of Transactions in Underground Markets, INTERPOL, (Aug. 6, 2022, 9.50 pm), https://www.interpol.int/en/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Project-Titanium

[48]AA v Persons Unknown., [2019] EWHC 3556 (Comm).

[49] Costa Estevao, Artificial Intelligence in Cybersecurity: The Benefits and Challenges, CENGN (Aug. 8, 2022, 11.50 pm) https://www.cengn.ca/information-centre/innovation/artificial-intelligence-in-cybersecurity-the-benefits-and-challenges/

[50] Faridha sabry, Cryptocurrencies and Artificial Intelligence: Challenges and Opportunities, IEEE Access, (Aug. 9, 2022, 10.15 am) https://ieeexplore.ieee.org/iel7/6287639/8948470/09200988.pdf

[51] Turner Brian Adam, et all, Analysis Techniques for illicit Bitcoin Transactions, Frontiers (Aug. 11, 2022, 9:30pm), https://www.frontiersin.org/articles/10.3389/fcomp.2020.600596/full

[52] ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: OPPORTUNITIES AND CHALLENGES TECHNICAL WORKSHOP SUMMARY REPORT A report by the NETWORKING & INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT SUBCOMMITTEE and the MACHINE LEARNING & ARTIFICIAL INTELLIGENCE SUBCOMMITTEE of the NATIONAL SCIENCE & TECHNOLOGY COUNCIL (March 2020).

[53] Titanium: Tools for the Investigation of Transactions in Underground Markets, (Aug. 15, 2022, 11:10am) https://www.titanium-project.eu/

[54] Chetana Belagere, Bitcoin-related crimes likely to go up: Report-Anonymity allows criminals to misuse system: Kaspersky study , INDIAN EXPRESS, (Aug. 5, 2022, 4.30 pm), https://www.newindianexpress.com/states/karnataka/2020/dec/08/bitcoin-related-crimes-likely-to-go-up-report-2233200.html.