Page 781 - 791 **DOI:** *https://doij.org/10.10000/IJLMH.119180*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Blockchain Technology: A Disruption to the Financial Risks of Phishing Attacks in India

ARKAJIT DEBNATH[1] AND DR. RAGHUNATH CHAKRABORTY[2]

ABSTRACT

The development of financial applications inside the newly growing Digital Financial Ecosystem in India has increased the possibility for cybercrime. As a result, offenders have increased their misleading tactics in order to deal with the evolving digital landscape in India. The growing number of phishing attacks in India is a striking illustration of the fact that the system itself serves as a fertile ground for cybercriminals. This article will provide an illustration of the mechanism behind blockchain technology and the potential to serve as a model for promoting transparency and digital identification among consumers as well as the benefits of utilising the technology within the financial ecosystem. This paper will also discuss the compatibility of the technology within the peripherals of Digital India. This would allow for the maintenance of a financial management system that is free from identity theft and other illicit methods such as phishing. In terms of the infrastructure requirements and the vision of the government bodies that are prescribed, the utilisation of such a technology is both exhaustive and comprehensive. In addition, the study will assess the presence of blockchain technology in a variety of government models that are not based in India in order to present a clear picture of the likely future of the Indian Financial System.

Keywords*: Digital India, Phishing, Blockchain Technology, Fintech, Compatibility.*

I. INTRODUCTION

Digitalisation not only encompasses the lifestyle of the masses rather they infiltrated the nerves of the mass population of India. In Indian Ayurveda there is a famous proverb that "if you want to kill a poison, you need a poison"; so, in Indian context the poisonous impact of digitalisation can be minimised by the poison of blockchain technology that perhaps stood as a pivot of this paper. But the relevant question in this regard lies with the compatibility of the blockchain technology within the legal framework is a rising question in the Indian Financial System. The compatibility of blockchain technology with a nation's economic framework depends on the capacity of the nation to harness that technology in order to bring out the most productive output. The recent trends in the cyber-attacks within the fetters of financial ecosystem of India

[1] Author is a Research Scholar at ICFAI Law School, ICFAI University Tripura, India.
[2] Author is an Assistant Professor, ICFAI Law School, ICFAI University Tripura, India.

 [ISSN 2581-5369]

clearly depict the prevalence of multifarious financial accessibility complexities. The Financial system is expeditiously promoting the digitalisation at a grass-root level, yet the legislative framework to implement smooth functioning of the same digital financial ecosystem is almost two decades older. The volatile nexus of comprehensive legislative framework with the fast-growing digital market is resulting into a gap enabling the virtual perpetrators to embezzle the financial data at a larger level. The blockchain technology erupts as a prominent advancement in the digital realm which could change the meagre landscape of financial risk management in India.

The blockchain technology is an advanced database mechanism which allows the transparent information sharing within a network. It constructs a centralised digital ledger enabling exchanges between multiple parties in a secure and efficient manner. This centralised mechanism provides a secure setup for the financial to carry out the smooth financial transactions within the state as well as cross border transactions. The secure outreach of the blockchain technology will also help in fighting crimes like phishing, spear-phishing, whereby the perpetrators target the customers and use social engineering methodologies in order to take financial gains. The figure below will elaborate the functioning and the modus-operandi of the blockchain technology with regard to the financial transactions from one party to the other.

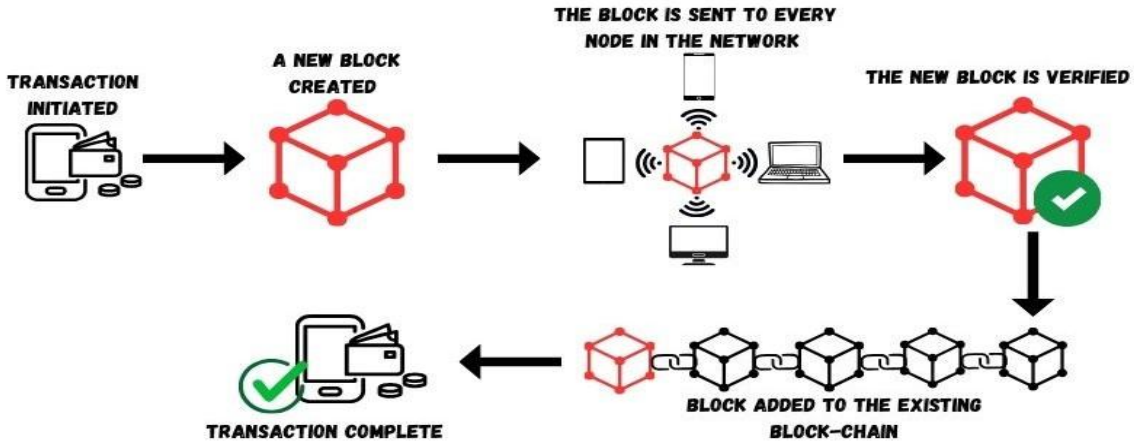

Fig: Self-made by the author

The blockchain technology is equipped with a mechanism which would give every user a digital identity and every transaction which has been done by that identity will be recorder in a manner such that it forms a chain-like structure taking it back to the origin. The Fig. depicts the journey

of a transaction within a blockchain technology framework. the transaction is first initiated by the party and then a separate block is created symbolic to the fresh transaction and therein after the freshly created block is sent to the network nodes for verification. The verification process will ensure the consensus of the parties resulting in the attachment of a separate block to the existing block chain referring to a successful transaction. This procedure will ensure the historical background of the transaction and the records of the initiator will be saved in a non-removable system of chains interlinked with each transaction. The blockchain model, initially introduced as an architectural model for crypto currencies that eventually expanded its dimensions to multiple facets of productivity. The blockchain technology in the present day is used in various sectors such as Energy, Finance, Media and Entertainment. This technology has offered a dynamic shift in the interoperability between sectors like Money Transfer, Healthcare, Logistics and even Government works. The equipped use of blockchain technology can enhance the transparency and the operability of the departments and provide the users with a smoother approach. The founding stone on which the blockchain technology is standing is the concept of transparency.

II. BLOCKCHAIN TECHNOLOGY: A BARRIER TO VEHEMENT FINANCIAL RISKS

Blockchain is a transformative innovation catalysing a paradigm shift in the realm of data security and data integrity. Notwithstanding it conceived as an architectural framework for cryptocurrencies such as Bitcoin but moulded its nascent nature and has now developed into a flexible technology with applications spanning various sectors, including cyber security (Swan, 2015)[3]. Elementarily, blockchain is a decentralised distributed ledger technology which securely records transactions over a network of computers in a tamper-resistant and transparent manner (Nakamoto, 2008)[4]. The pertinent utility of blockchain technology lies with the efficient modus operandi of the harnessing process that constitutes the forming of transaction or block that is cryptographically linked to the preceding one forming a chronological chain of blocks[5]. It ensures that one transaction cannot be altered retroactively, enhancing data integrity and trust in the system that acted as beneficial, in order to ascertain the source of inception regarding a deceptive financial transaction. The decentralised nature of the blockchain eliminated the need of intermediaries or central authorities enhancing the resilience among attacks. Pertaining to the

[3] MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 11 (2015).
[4] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, April 29, 2024, https://bitcoin.org/bitcoin.pdf (2008)
[5] Gaoqi Liang et al., Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks,IIEEE Transactions on smart grid, 10, 3162-3173 (2019), April 25, 2024, https://ieeexplore.ieee.org/document/8326530

 [ISSN 2581-5369]

efficacy of blockchain technology, it emerged as a promising solution for the proliferation of cyber security concerns and also to rebut the attacks like phishing by leveraging the inherent properties of decentralisation, transparency and immutability. The incorporation of blockchain technology into e-financial services has the potential to improve the efficiency of financial accessibility and financial confidentiality by diminishing the financial susceptibility.[6]

III. BLOCKCHAIN TECHNOLOGY: A PAUSE TO DEADLY FINANCIAL RISK OF PHISHING ACTIVITIES

Financial risks and money laundering are not interchangeable words but they are conjointly interpreted in its layman sense. Finance is mostly connected by the people with that of money as money is not a matter of accumulation of luxury in Hindu culture rather the Indians adore the money as a blessing of goddess Laxmi. Furthermore, as per the dictum of Arthashastra, one of the safest ways of securing the hard-earned money is to diversify the money. In the present Scenario, the entire diversification of money has been carried out by investing the money in Bank Accounts, share markets, mutual funds etc. The substantial investment takes place through the financial applications installed in the mobile phones of millions of Indian consumers. Mostly the financial applications have been owned and regulated by the private fiduciaries but the transition took place when the central government comes in with the mega campaign of "Digital India". The initial prosperity of Digital India took place through the linkage of bank accounts of millions of pensioners of India, but the irony lies with the fact that the initial consumers of Digital India that is, Pensioners are the most vulnerable tech users. Thereafter, the epidemy of deceptive financial transactions has been strengthened by the data breaches and data misappropriation of financial data by the cyber intruders prominently through voice calls and seeking the credentials of ATM Cards, Credit Cards, Bank Accounts of the innocent consumers. This modus operandi eventually titled as "Phishing Attacks" sprouted its roots rapidly and emerged as a Gigantic poisonous tree especially in the era of Big Data.

Although the practice of phishing was a pre-existent, the umbrella of Digital India served as a platform for the perpetrators to enhance their social engineering skills and simultaneously and upgrade their Digital Game with the infrastructural development of the state since the government initiated the digitalisation of the economy holding the hands of the Digital India Initiative. In the current scenario India is a growing digital economy and simultaneously the

[6] Tița Raluca-Florentina, *The Utility of Blockchain Technology in the Electronic Commerce of Tourism Services: An Exploratory Study on Romanian Consumers*, 14 SUSTAINABILITY 943, 2 (2022), https://doi.org/10.3390/su14020943.

hub of cyber threats like Phishing[7]. Multiple approaches have been taken under consideration to mitigate the financial frauds and the high rising magnitude of the crime but subsequently the perpetrators find an escape resulting in the financial loss of millions. Therefore, a robust mechanism in order to combat the crime of phishing is the need of the hour. The mechanism has to be of such nature that the origin, tracks and the whereabouts of a released fund could be traced back within a system[8]. The blockchain technology offers several capabilities like enabling the creation of a decentralised identity management systems where users maintain a control over their own digital identities and personal data.

IV. BLOCKCHAIN TECHNOLOGY ADDRESSING IDENTITY THEFT: A MAJOR PHISHING WEAPON IN INDIA

The blockchain technology eliminates any intermediaries or centralised repositories of sensitive information which may lead to a data breach and thus, enhances the privacy of the user. This mechanism is helpful in order to eliminate the concept of identity theft which is the common precursor to maximum phishing attacks. The blockchain based authentication mechanisms such as digital signatures and public key cryptography enhances the security mitigating any threat of spoofing or impersonating. With the help of the cryptographic principles and the decentralised mechanisms blockchain technologies ensure a peer-to-peer interaction along with a chain of authentic traces of the previous transactions minimising the reliance on trusted third-party applications or fintech apps that are susceptible to compromise the financial data entrusted to them. As blockchain technology gains popularity, the concerns over the financial security of blockchain transaction networks have escalated. Phishing scam detectors serve to safeguard potential victims and foster a more robust blockchain ecosystem. Phishing scam detection is typically defined in existing works as a process of classifying nodes by utilising graph embedding methods like random walk or graph neural network (GNN) to understand the probable traits of users. However, these detectors face significant complexity issues as a result of the extensive scale of blockchain transaction networks.

Identity management is one of the key factors which make the blockchain technology safer than the traditional centralised financial system. In this system the users retain the full control over their digital identities in a systematic manner. Each user possesses a unique cryptographic key pair consisting of a public key which serves as their digital identifier and private key. Using this

[7] Rasha Zieni et al., *Phishing or Not Phishing? A Survey on the Detection of Phishing Websites*, 11 IEEE ACCESS 18499-18599 (2023), May 02, 2024, https://doi.org/10.1109/access.2023.3247135.
[8] *Phishing Attacks and Anti Phishing Techniques*, 2024 INT'L RSCH. J. MODERNIZATION ENG'G TECH. & SCI., May 02, 2024, https://doi.org/10.56726/irjmets48484.

crypto key, the users can authenticate themselves without the help of any third-party application controlling or mishandling their information. The decentralised nature of blockchain technology enhances the resilience of identity management system to mitigate phishing attacks. The identity management model makes sure that each transaction involving identity verification or authentication is encrypted in the blockchain from both peers in a tamper resistant manner providing a immutable audit trail of user interactions. With the use of verifiable credentials and Decentralised Identifiers (DIDs) the users can assert their identity in a privacy preserving manner minimising the risk of over sharing. The users in the blockchain technology are provided with a private key and a public key, the public key serves as their digital identifier and the private key grants access to their identity and the associated data within. The users can smartly use those keys and determine the information which are to be shared and which are not to the other verified user in the other end. This methodology of providing information within a peer-to-peer protected system will definitely solve the problem of people falling victim to the phishing attacks where the identity of the other user is not known and it is taken as leverage by the perpetrators resulting in the ultimate loss and no recovery. In a nutshell it can be assessed that the identity management model within the blockchain technology empowers the individuals with strong control over their information enhancing the security through cryptographic mechanisms. There are multiple instances which serve as real time examples as to how the blockchain technology has helped in combating the phishing attacks in various nations.

V. FINANCIAL RISKS MANOEUVRED THROUGH PHISHING ATTACKS IN INDIA

Phishing is one of the prevalent cyber threats continues to pose significant challenges to individuals, businesses and institutions worldwide. Phishing is defined as the practice of masquerading as a trustworthy entity to obtain sensitive information such as usernames, passwords and financial data[9], phishing attacks exploit the human vulnerabilities rather than the technical weaknesses through various social engineering techniques. These attacks are often arrived via e-mails, instant messaging, social media, voice calls, enticing the unsuspecting victims to divulge confidential information or click on malicious links. The anatomy of Phishing involves components orchestrated to deceive and manipulate users. The attackers primarily craft messages or websites that closely resembles legitimate communications from reputable sources employing sophisticated techniques to mimic logos, branding and language[10]. The meticulous

[9] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems 581-590 (2006)

[10] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd Symposium on Usable Privacy and Security 88-99 (2006).

deception aims to project a sense of trust and urgency among the recipients compelling them to act impulsively without testing the authenticity of such communication. The phishing attack models work on certain psychological triggers such as Fear, Curiosity or greed to manipulate the human behaviour in order to achieve the optimum result from the social engineering techniques applied by the perpetrators[11]. The emotional turbulence among the recipients overrides the logical reasoning and overlooks the warning signs and divulge sensitive information hastily. A phishing mail purporting to be from a financial institution may warn a person for an unauthorised transaction urging them to verify their account details in order to cancel or revert the transaction. The consequences of the phishing attacks can be severe encompassing financial loss, identity theft, repetitional damage, compromised data confidentiality[12]. Despite highlighted awareness and cyber security measures phishing remains a persistent threat due to the adaptability and evolving sophistication. It is the onset of crisis when the actual vulnerability in regard to phishing is actually visible. During the time of COVID 19 when the remote working was the new culture, there has been a substantial spike in the number of phishing attacks in India. Since India is a prominent service provider in various sectors, the remote working culture and the dependency of the people at large has resulted in a seven-fold spike in the phishing statistics[13]. The Indian Computer Emergency Response Team (CERT-In) managed a total of 1,391,457 occurrences related to cyber security in the year 2022. The Cert-In 2022 Annual Report revealed that there were 653 security warnings, 38 advisories, and 488 vulnerability notes published in the country last year, providing up-to-date information on the newest cyber threats and vulnerabilities. The survey additionally identified a surge in phishing assaults, malware attacks, and insecure services. India witnesses a wide variety of phishing attacks in the last few years due to upsurge in the digitalisation of the financial ecosystem and the rising magnitude of transactions through fintech applications. In terms of the nature of cyber assaults in the past two years, there was a significant rise in phishing attacks (230%), malware attacks (45%), and vulnerable services (20%) in 2022 compared to 2021. The number of phishing attacks has tripled in 2022 compared to the previous year, increasing from 523 incidents in 2021 to 1,714 incidents in 2022. The number of vulnerable service instances rose from 728,276 in 2021 to 875,892 in 2022, while the number of malware attacks climbed

[11] Hong, J., & Kim, Y., Emotion in action: the effect of additive fear and anger on the endorsement of phishing e-mails. In Proceedings of the 2013 conference on Computer supported cooperative work 447-456 (2013)

[12] Markus Jakobsson & Steven Myers,Phishing and Countermeasures: Understanding the Incresing problem of Identity Theft, May 04, 2024, (2006), https://api.semanticscholar.org/CorpusID:166691459.

[13]B. W. Team, 1.39 million cyberattacks handled in 2022, phishing attacks rise: Cert.In, May 04, 2024, https://www.business-standard.com/india-news/1-39-million-cyberattacks-handled-in-2022-phishing-attacks-rise-cert-in-123111500614_1.html

 [ISSN 2581-5369]

from 1,489 in 2021 to 2,164 in 2022. The statistics purely portray the nature of vulnerability which India possesses while regulating the digitalisation initiated by the Digital India initiative.[14]the blockchain technology is a mechanism which has the potential to amplify the financial security in the digital realm and provide with a secure and transparent mechanism for the consumers in India.

VI. IMPETUS OF BLOCKCHAIN TECHNOLOGY IN MAJOR COUNTRIES

The Blockchain Technology is a new and innovative method of handling the sensitive data and the integration of such a methodology in full swing is a challenge for any government, but looking at the benefits and the security it provides several countries have adopted blockchain technology in their data management modules[15].

Singapore has emerged as a leading proponent of blockchain technology within Southeast Asia. The Singapore Government has invested in research and development initiatives to explore the innovative application of the technology in various sectors including Finance, healthcare and even supply-chain management[16]. The Singapore Government has also initiated the process of incorporating the blockchain technology in to the banking sector developing the sector in a secured manner[17]. Recently the Monetary Authority of Singapore (MAS) and the industry stake holders have collaborated to develop Project Ubin, a blockchain based platform for interbank payments and settlements[18]. The leverage of blockchain technology has reduced the susceptibility of Singapore's Banking system to phishing attacks and fraudulent activities. This step is a milestone into fostering a greater amount of confidence among the consumers and the businessmen[19].

Switzerland has also emerged as a prominent hub for the blockchain innovation due to the favourable economic system and environment among the blockchain start-ups and enterprises

[14] Ibid.

[15] Purnendu Bikash Acharjee et al., Securing International Law Against Cyber Attacks through Blockchain Integration, 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, 2676-2681 (2023), May 04, 2024, https://www.semanticscholar.org/paper/Securing-International-Law-Against-Cyber-Attacks-Acharjee-Kumar/3d24998ce3ff6d300ebdb077b7831406f9d3969f

[16] Singapore Government, Blockchain, May 04, 2024, https://www.tech.gov.sg/technologyareas/infrastructure-and-services/blockchain,(2020)

[17] YIN XIA LOH ET AL., *The Implementation of Blockchain Technology in Malaysia and Singapore Financial Industry*, *in* 2023 16TH INTERNATIONAL SYMPOSIUM ON COMPUTATIONAL INTELLIGENCE AND DESIGN (ISCID), (2023), May 04, 2024, https://doi.org/10.1109/iscid59865.2023.00038.

[18] Ho, J., Leong, T. C., & Wong, C. H., Project Ubin: SGD on Distributed Ledger. Monetary Authority of Singapore. https://www.mas.gov.sg/-/media/mas/projectubin/project-ubin--sgd-on-distributed-ledger.pdf (2017)

[19] SAREH ROTABI & OMAR ALI, *Applications of Blockchain Technology for a Circular Economy with Focus on Singapore*, *in* BLOCKCHAIN TECHNOLOGIES FOR SUSTAINABILITY 151-168 (2021), May 05, 2024, https://doi.org/10.1007/978-981-16-6301-7_8.

from around the world[20]. The Swiss Government is taking multiple initiatives in order to foster the blockchain market by initiatives such as the Crypto Valley Association with supervises the collaboration between the industry players, academia and the government[21]. Switzerland has positioned itself at a front foot of blockchain adoption, harnessing the technology with its potential to enhance cyber security and combat phishing attacks.

Estonia is another prominent example of a country who has actively adopted blockchain technology to bolster cybersecurity resilience. Estonia has implemented blockchain based solutions to secure digital identities and streamline administrative processes[22]. The country's E-Residency program which allows individuals to establish and manage business remotely is based on blockchain technology and in order to ensure integrity and authenticity of the identities. Estonia has practically mitigated the risks of identity theft and fraudulent activities thereby enhancing the trust on digital ecosystem and reducing incidents of phishing attacks targeting individuals and businessmen.[23]

VII. CHALLENGES OF BLOCKCHAIN TECHNOLOGY: IN INDIAN CONTEXT

Blockchain technology and the innovations associated with it has always been Novel and un-entertained by the government in India despite the fact that the growing economy and the fintech market in India has thrived in the recent few years. The growing fintech industry in India has given access to instant online payment methods and fund transfers with the click of a button and simultaneously has become one of the breeding grounds for cybercrimes such as phishing. The primary challenge which India is facing in regard to the introduction of blockchain technology within its economic system is the lack of infrastructure, regulatory uncertainties and technological limitations. In order to introduce a system like blockchain, the harnessing of the system with a proper regulatory body and set of rules are a mandate in order to get the best possible outcome of the system. One of the important obstacles to blockchain adoption in India is the lack of a clear regulatory framework governing the rules of the blockchain system[24]. The

[20] Maurer, R. Blockchain and the law: What is the impact of the General Data Protection Regulation on the blockchain? In J. M. Lehmann & C. M. Witt (Eds.), Distributed Ledger Technology: The Science of the Blockchain 145-160, May 05, 2024, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, (2018).
[21] Crypto Valley Association. (n.d.). About. https://cryptovalley.swiss/about/
[22] Randviir, A. (2017). The development of e-government in Estonia. In Proceedings of the 16th European Conference on e-Government, Academic Conferences International Limited. 631-637 (2017)
[23] Dita Aulia Salma & Fahlesa Munabari, Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia, Deviance Jurnal Krimunology, (2023), May 05, 2024, https://pdfs.semanticscholar.org/7297/e9d18343724a80ed0a1e508ceb41747ffee0.pdf?_gl=1*16tqjze*_ga*MTc3NjY2MDQwOC4xNzE0NDUyNDA1*_ga_H7P4ZT52H5*MTcxNTYzMjkwMS4xMC4wLjE3MTU2MzMwNDIuNDcuMC4w .
[24] *Blockchain Technology in India – Challenges and Opportunities*, 8 INT'L J. RECENT TECH. & ENG'G 32-36, (2019), May 06, 2024, https://doi.org/10.35940/ijrte.d1038.1284s319.

Reserve Bank of India has adopted a cautious approach towards crypto currencies and block chain technology expressing concerns about their risk to financial stability and consumer protection (Reserve Bank of India, 2018)[25]. India also faces significant technological challenges in implementing the blockchain technology even though the country has a vibrant technological ecosystem and a pool of skilled developers the blockchain technology requires robust infrastructure and interoperability standards[26].

The complexity of India's Financial sector, characterized by diverse regulatory requirements, legacy systems and fragmented market participants present additional hurdles to blockchain adoption. The financial institutions must navigate through a labyrinth of regulations governing data privacy, cybersecurity, and financial transactions, making it challenging to implement blockchain solutions that comply with the regulatory needs[27]. The recent development in the fintech arena in the form of UPI payments has indulged the people in a separate form of financial economy which would directly contradict with the blockchain methodology[28]. The data fiduciaries in India will not be allowing a system which would refrain the third parties to gain access to the consumer data like blockchain. Despite such challenges India has taken steps to explore the blockchain technology to combat fraud and digital identity management[29]. The NITI Aayog's National Strategy for Blockchain and RBI's exploration of central bank digital currencies demonstrate India's recognition of blockchain's transformative potential in enhancing the financial inclusion and promoting economic growth[30]. The monetary Association of Singapore has adopted a robust mechanism in order to implement the blockchain technology in in five different phases executed in a multi-layer facet which would which bring down the transactions within a blockchain regulated ecosystem for transparency even at a cross border level.

VIII. CONCLUSION

In conclusion it can be said, while blockchain technology holds immense potential for revolutionizing India's financial sector and enhancing cyber security, the widespread adoption

[25] Reserve Bank of India, Press Release: RBI cautions users of Virtual Currencies against Risks, May 06, 2024, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=42424 (2018)
[26] NITI Aayog, National Strategy for Blockchain. Government of India. (2018)
[27] KPMG, Blockchain in India: A forward-looking approach, May 06, 2024, https://home.kpmg/in/en/home/insights/2020/10/blockchain-in-india.html (2020)
[28] *Blockchain Technology and It's Applications in E-Governance Services*, 8 INT'L J. RECENT TECH. & ENG'G 5795, (2019), https://doi.org/10.35940/ijrte.d8599.118419.
[29] SUMAIYA & AJAY KUMAR BHARTI, *A Study of Emerging Areas in Adoption of Blockchain Technology and it's Prospective Challenges in India*, *in* 2019 WOMEN INSTITUTE OF TECHNOLOGY CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING (WITCON ECE), (2019), https://doi.org/10.1109/witconece48374.2019.9092935.
[30] NITI Aayog, NITI Aayog enters into agreement with IET U.K. to further blockchain technology in India. Government of India, May 06, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=1740547 (2021).

 [ISSN 2581-5369]

of this technology is facing a backlash due to the high infrastructural needs. The mechanism of blockchain technology ensures the transparency within a financial transaction creating a separate block for each transaction and attaching it with the previously existing chain. This mechanism will be highly beneficial in order to mitigate cyber threats especially phishing attacks since the attacks are primarily based on the anonymity of the attackers and the vulnerability of the victims. The social engineering techniques and the veil of identity theft will be removed with the tracing and verification of every transaction for the consensus of the parties. The blockchain technology will also ensure the identity verification of the parties using the technology eradicating the very concept of identity theft. The digitalization of the economy has provided access of the consumer data to multiple data fiduciaries and the mishandling of the data by any fiduciary results in a Big Data breach. India needs to adopt Blockchain technology within the financial ecosystem in order to provide consumers with data independence and a peer-to-peer recorder transaction chain which would be tractable whenever necessary. The rising magnitude of cyber-crimes within the financial sector in India are depicting the cyber vulnerability of the state with regard to the risk management of the technological infrastructure and the financial security of the consumers. Major countries in the world like Switzerland, Singapore and Eutopia have internally incorporated the blockchain technology within their financial system making it more secure and a successful attempt at cyber-attack mitigation. The technology required in order to harness the capability of blockchain technology is the primary sector where India should be working so that a risk-free financial management atmosphere is available to the consumers. Referencing the technology used in projects like Ubin will would help India harness the power of Blockchain technology and utilise it to its full potential not only within the financial system but also in sectors like administration and healthcare. The milestones which are achieved by several other nations with regard to the implementation of blockchain technology within the parameters of the financial system are a case study for the Indian Financial Ecosystem which would flourish with such a transparent mechanism equipping the consumers to trace down their hard-earned money in the prescribed system. It is an observation that India should adopt the Singapore model for blockchain technology harnessing and along with the aid and supervision of the government bodies, ensure a working model for the financial risk management. The financial inclusion boom in India has enhanced the ambit of Internet of Things as a result, the risk management is the primary need of the consumer base in the current financial scenario.

*****

 [ISSN 2581-5369]