NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

A detailed study of intersection of Cyber Security and Blockchain technology for robust security Decentralized Environments

Ms. Saloni S. Chauhan
CS and IT Department
Atmiya University
Rajkot, Gujarat

***Abstract*—** *The intersection of Blockchain technology and Cyber security has emerged as a key area of study in the field of decentralized environments. This research paper offers a detailed analysis of this intersection to shed light on the intricate dynamics and implications for strong security. After giving a summary of the core concepts of Blockchain technology, such as immutability and decentralization, the paper looks at how it might be used to enhance cyber-security procedures. A review of relevant literature thoroughly examines important topics such as cyber-security applications that use Blockchain technology, security enhancement in decentralized environments, and challenges in integrating Blockchain technology into cyber-security frameworks. The study also looks at future directions and research priorities, illustrating how cyber-security and Blockchain technology will evolve after 2021. By integrating information from multiplesectors.*

***Keywords*—** *Keywords: Blockchain, Cyber-security, Data Integrity, Authentication, Survey, Impact, Applications*

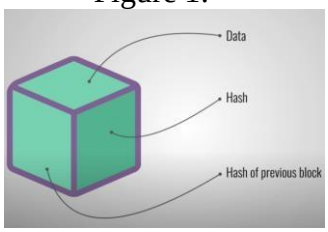
Introduction

A basic component of human society across a range of sectors, including personal, national, organizational, and global levels, is the demand for security. Security works to defend people, places, institutions, and countries against a range of dangers, vulnerabilities, and threats. The innate urge to establish a secure and stable environment for people, communities, and nations gives rise to the demand for security. It employs a multifaceted strategy that tackles societal, economic, digital, and physical security issues to create a society where people may live and prosper with confidence.

One of the evolving technologies now-a-days is Blockchain Technology which ultimately gave rise to Cryptocurrencies all over the world. The use of its spread veritably fleetly. Blockchain technology works as wonder when one can talk about the managing and storing huge public databases. One can define Blockchain as the it is a series of blocks which contains information of specific data, a specific hash value and hash value of preceding blocks that are being used in the series of chain. Blockchain technology uses the major two cryptography techniques likes Cryptography and hashing. For using the process of encryption and

decryption in p2p network which is used in between the blocks of information and data.
And hashing technique for securing the data from manipulation, alteration or from any upgradation.

Figure 1:



Blockchain uses the decentralized database, Peer-to-peer network which is used to store and manage records. Therefore, it can widely play a major role in following sectors, Cyber Security, Education, Healthcare, Digital money transactions, IOT management. And many others. In today's technological world, privacy and security have become critical for safeguarding consumers, companies, and communities from an extensive variety of online dangers. It assists in developing a safe, reliable, and reputable internet community in addition to eliminating the danger of monetary loss and reputation harm.

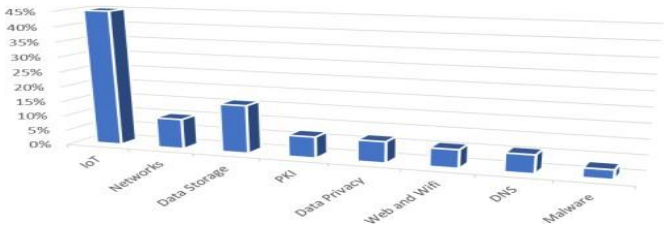
Cyber Security	The safeguarding of Cyber systems in opposition to Cyber threats are frequently. referred to as Cyber security.
Cyber Threats	Threat will exploit a Cyber Space.
Cyber Space	An assortment of interconnected computer networks that include services, computers, embedded controllers and processors, and stored data.
Cyber System	A Cyber system is an intricately linked network of digital elements, such as people, networks, software, hardware, and software.
Cyber Physical System	Actuators and sensors in a Cyber system allow it to control and react to physical entities.
Vulnerabilities	Weakness in a computer system is generally considered as the Vulnerabilities of that respected system.
Cyber Risk	Threat * Vulnerabilities is referred as the Cyber Risk.

LITERATURE REVIEW

By reading and analyzing the blog related to guide to hybrid Blockchain, benefits and use cases written by Dr. Ravi Chamria it is concluded that Performance rate of public Blockchain is very less while on other hand performance rate of private Blockchain and hybrid Blockchain is quite good. Because as discussed earlier private Blockchain and hybrid Blockchain is permission-ed type of technology. [2] From the journal of digital communications and networks it is observed that most uses and application of Blockchain technology and Cyber security is in IOT Devices and Data Storage.

Users	Percentage
IoT	45%
Networks	10%
Data Storage	16%
PKI	7%
Data Privacy	7%
Web and Wifi	6%
DNS	6%
Malware	3%

Decentralization	Eliminating the need of central authority Prevents unauthorized access and tempering of data.
IoT Protection	It uses the concept of digital signatures. Blockchain ensures the integrity and confidentiality of an IoT system.
Collaborative Consensus	It provides the mechanism od Validating and verifying order of transactions. Blockchain ensures accuracy and integrity in Collaborative Consensus
Preventing D-Dos attacks	As Blockchain technology uses the p2p network it is used to prevent d-dos cyber-attacks.
Strong Encryption Practices	Blockchain uses the strong cryptography techniques like hashing, public and private key concept and many more.
Data Privacy	Nodes are interconnected to more privacy compared to other technologies.
Immutable Records	More functionalities in types of Blockchain like hybrid which make it hard for records to change or alter.



[3] From reading and examining the article of externetworks it is concluded the following key advantages of integrating the Blockchain in Cyber security.

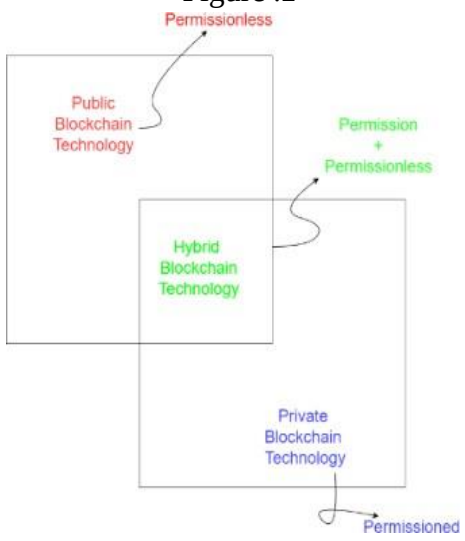
The introduction (2008) outlines the history of Blockchain technology's development and emphasizes its immutable and decentralized features as a possible cyber-security solution. examining Nakamoto's (2008) groundbreaking work on Bitcoin and highlighting the importance of immutability and decentralization in boosting security. In 2015, an examination of the intrinsic security advantages of Blockchain technology, such as the decrease in single points of failure and the bolstering of defenses against malevolent assaults. An analysis of the primary barriers to incorporating Blockchain technology into cyber-security frameworks, including issues with interoperability, scalability, and regulatory compliance. Analysis of the various applications of Blockchain technology in cyber security in 2016—from secure authentication techniques to reliable communication channels— was conducted. Evaluation of research priorities, with a focus on the necessity of interoperable standards, scalable solutions, and investigation of new applications of Blockchain technology in cyber-security. A review of the literature through 2021 that highlights ongoing research and the possibility of revolutionary security solutions at the nexus of Blockchain and cyber-security in the future. Immediately after 2021, there has been a growing body of research devoted to resolving the issues of privacy, scalability, and interoperability that arise when incorporating Blockchain technology into cyber-security frameworks. Furthermore, there has been an increasing focus on investigating new Blockchain applications in cyber-security contexts, like secure data sharing protocols and decentralized identity management. The regulatory ramifications and compliance need for blockchain-based

cybersecurity solutions have also been studied by researchers, with the goal of creating frameworks that comply with current standards. Current research endeavors are investigating novel strategies to surmount the constraints of conventional cybersecurity frameworks by means of incorporating. blockchain technology. The primary emphasis is on augmenting data safeguarding, authentication protocols, and threat intelligence dissemination in decentralized settings. Moreover, multidisciplinary research teams are forming to investigate the connections between blockchain technology and other cutting-edge innovations.

RELATION BETWEEN BLOCKCHAIN TECHNOLOGY AND CYBER SECURITY

The blockchain technology uses the peer-to-peer network that is p2p network. The p2p network gave new form to the concept of decentralized network. This type of Network is quite secure and useful.

Figure :2



There will be data blocks which contain the crucial information of the consumers or users. And one data block is connected to another, and that data block is further connected to another, and series go on and on. And this data block is known as the nodes of the chain. Therefore, here we can conclude that in p2p network the blocks of data are interconnected, Information on it is much more secure. Earlier the client server system architecture is in use but as it is less secure while on the other hand the p2p network provides a good amount of security and privacy to the data and consumers. Another useful functionality of p2p network is that if some attacker or hacker tries to temper any one data block. Then all the users will get to know that there is something wrong with the information or data. Also, by referring the article of blockchain council it also analyzed that most common and harmful cyber-attack like Dos/ D-dos attacks can also be prevented from the use of p2p network.[4] There are many types of blockchain technology but here we will discuss the 3 major types of the blockchain technology that is, • Private Blockchain • Public Blockchain • Hybrid Blockchain. As the number of cyber-attacks is increasing day by day. There is a requirement for strong technology which protects the confidentiality, integrity, and availability of resources. As we know today the most asset in one's life is data. Data plays a very crucial role in the information technology field. And revolutionary blockchain technology using very strong security mechanisms which is very difficult to breach or hack. Therefore, the rate of data breaches is also reducing with the rise of blockchain technology. Earlier when there was no integration of Blockchain in Cyber security the rate of attacks was quite high. Why so? Because earlier when one user wants to send any data or information to another user using a centralized database there will be every high chance for data to get misplaced, manipulated or any type of Cyber-attacks like man-in-the middle, phishing attack, dos attacks may take place. Therefore, the CIA can be threatened. But the Technology of Blockchain works wonders for the Cyber Security branch also. Blockchain uses the P2P network that is peer to peer network which is much more secure. Also, it uses the distributed database

which provides more security and privacy. Therefore, the rate of Cybercrimes decreases at a good rate. Therefore, one can conclude, the decentralized and transparent nature if Blockchain technology contributes to enhance the security in theCyber world.

CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Despite having a lot of advantages Blockchain technology also have some Cyber security challenges. Many attacks like Malleability attacks, double spreading attacks, 51% attacks, Wallet security attacks, smart control loophole attacks and system error attacks are still observed.[5] Out of the listed attacks the highest rate is observed in malleability attacks. Because cryptocurrencies have so many shortcomings, criminals can easily take advantage of them, as can their users. The enforcement of cryptocurrency fraud and scams has also been limited because of the challenges in identifying and prosecuting offenders, as well as the absence of laws and law enforcement experience pertaining to cryptocurrencies.[6] In total 65 real world Cyber-attacks, scams, and frauds in noted between the year of 2011 to 2019. Out of which 48 incidents is of hacking, 10 incidents is of scams and 7 incidents is of smart contract flaws.[7] Therefore we can conclude here that Security breach, human errors and agency problems are some of the major reasons due to which Cyber security challenges is observed in rising Blockchain technology.[8] The attacks will try to get full access over physical layer of system, will try to install malicious files inside an system, will try to get access of log files of systems, will analyses the network and try to gain passive access to an system, will try to impersonate the user or server etc. And the main motive behind doing this is steal cryptocurrency coins.[9] In 2015, the Financial Action Task Force revealed that Liberty Reserve's founders embezzled hundreds of millions of dollars from criminal organizations over a six-year period. Broader and deeper applications of blockchain may be limited by technical, scaling, and commercial issues. Modeling issues, risks and public perception, government regulations and personal data protection issues.[10] Block browsers are vulnerable to XSS attacks that can display untrusted transaction data. Block browsers and accounts are subject to XSS attacks that give users accesses. Manage your private keys and manage your accounts. Vulnerable encryption code can compromise Blockchain systems if a malicious user tampers with transaction data. More than 90% of Ethereum smart contracts have reused code, which may contain known vulnerabilities.[11].

Figure :3 [12]

Apart from challenges discussed above, there are many other securities, network, connectivity, scalability issues are also being observed in Blockchain technology.

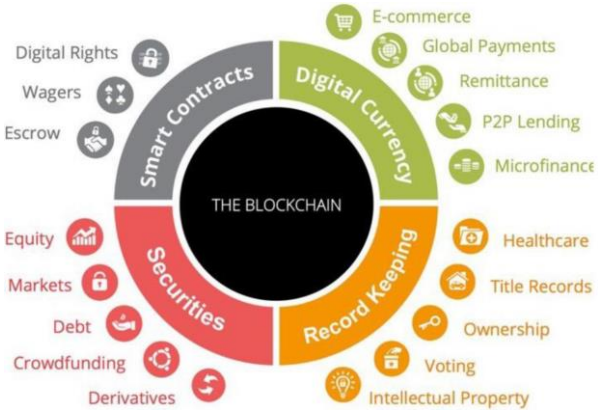
OPPORTUNITY IN BLOCKCHAIN TECHNOLOGY

Several characteristics of blockchain technology may speed up and secure transactions. Every device connected to a network has a distributed ledger.

It is encrypted for security and organized as a series of transactions. Because it is decentralized and disintermediated, transactions are validated by other networked computers that accept them rather than by a central authority. Because a block is either immutable or, at the very least, resistant to manipulation, it cannot be removed or changed. Because there is no need for a central authority and everyone can verify that a particular transaction is authentic and unaltered, transparency and trust are fostered.[13]

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

Figure: 4[14]



A. Blockchain technology in Smart Contracts

Smart contracts were first introduced by cryptographer Nick Szabo in 1994 with the intention of serving as a "computerised transaction protocol that executes terms of a contract" (Szabo, 1994).[15] Digital contracts that operate in computer network programming code are known as smart contracts. They make use of blockchain technology and the Ethereum platform. These contracts use blockchain technology to speed up the contracting process and prevent contract data loss.[16] Smart contracts lessen dependency on a single system. Ensuring that each party has a copy of the agreements and rules facilitates quick and easy communication between the parties. Additionally, it stops data loss. Since smart contracts and blockchains are interconnected, data manipulation is also a challenging task.[17]

B. Blockchain technology in Digital Currency

A fundamental component of most blockchain technologies is a token that can be used as a payment method. Some blockchains, like Bitcoin, classify the token as a cryptocurrency even though its primary use is as a payment method. The token enables users to conduct blockchain transactions by functioning as a "utility token" for other blockchains. For example, the Ethereum Virtual Machine, which acts as the Ethereum blockchain's runtime environment for smart contracts, accepts ether tokens as payment for processing. Whatever the circumstances, it is imperative to exchange digital currencies for government-issued ones.[18] Utilizing specialized devices such as ASICs, which execute complex hashing algorithms like SHA-256, has accelerated the creation of cryptocurrencies by increasing the rate at which hashes—which validate transactions—are generated.[19]

C. Blockchain technology in Record Keeping

When assessing the authenticity of records, it's also important to make sure the person claiming to be the creator is who they say they are. Authenticity therefore depends on demonstrating the identity of record creators as well as their agreement or capacity to participate in a process. To address this conflict, Weingärtner et al. suggest using a Self-Sovereign Identity (SSI), which is a decentralized identity under entity control that identifies the entity, or its representative, and that enables it to make identity-related claims that can be cryptographically validated—typically through the use of Verifiable Credentials.[20]

D. Blockchain technology in Securities

Platforms facilitating this
type of securities trading would be able offering advantages such as:

- Near real-time settlement (between milliseconds and minutes)
- Peer-to-peer delivery versus payment
- Round-the-clock uptime
- Auditability (transparency, UTXO model) [21]

CONCLUSION

Blockchain provides security and privacy to many domains. Blockchain Technology prevents attacks like dos and ddos attacks. But there are also other cyber-attacks are increasing which cannot be prevented by blockchain technology. Therefore, more efficient framework is required that can overcome the challenges of blockchain technology in future. Because in future the world needs both the technologies so more user-friendly framework which can detect and prevent the cyber-attacks that are being happening at increasing rate.

FUTURE WORKS

Need to explore the key advantages and disadvantages of blockchain technology which uses the cyber security framework. To do a detailed study of prevention and detection cyber security systems which can also prevent many cyber-attacks which are happening due to blockchain transactions.

REFERENCES

[1] https://www.youtube.com/watch?v=SSo_EIwHSd4

[2] https://www.zeeve.io/blog/guide-to- hybrid-blockchain-benefits-and-use- cases/#

[3] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), 147-156.

[4] https://www.blockchaincouncil.org/bloc kchain/blockchain-role-of-p2p-network/#:~:text=Because%20of%20P2 P%20networking%20capability,to%20traditional%20client%2Dserver%20systems

[5] Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. Human Behavior and Emerging Technologies, 2022, 1-11.

[6] Brown, A. K. (2023). The Criminal Side of Cryptocurrency. In Mainstreaming Cryptocurrency and the Future of Digital Finance (pp. 187-205). IGI Global.

[7] Alkhalifah, A., Ng, A., Kayes, A. S. M., Chowdhury, J., Alazab, M., & Watters, P. A. (2020). A taxonomy of blockchain threats and vulnerabilities. In Blockchain for Cybersecurity and Privacy (pp. 3-28). CRC Press.

[8] Charoenwong, B., & Bernardi, M. (2021). A decade of cryptocurrency 'hacks': 2011– 2021. Available at SSRN 3944435.

[9] HOUY, S., SCHMID, P., & BARTEL, A. (2023). Security Aspects of Cryptocurrency Wallets-A Systematic. ACM Comput. Surv, 1(1).

[10] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

[11] Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 1, 1-15.

[12] https://witscad.com/course/blockchainfundamentals/chapter/challenges-in-bct

[13] Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. Journal of Property, Planning and Environmental Law, 12(2), 129-145.

[14] https://nielit.gov.in/aurangabad/content/world-blockchain

[15] Bergquist, J. (2017). Blockchain technology and smart contracts: privacy-preserving tools.

[16] Fauziah, Z., Latifah, H., Omar, X., Khoirunisa, A., & Millah, S. (2020). Application of blockchain technology in smart contracts: A systematic literature review. Aptisi Transactions on Technopreneurship (ATT), 2(2), 160-166.

[17] Sekhar, S. M., Siddesh, G. M., Kalra, S., & Anand, S. (2021). A study of use cases for smart contracts using blockchain technology. In Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government (pp. 1823-1844). IGI Global.

[18] Routledge, B., & Zetlin-Jones, A. (2022). Currency stability using blockchain technology. Journal of Economic Dynamics and Control, 142, 104155.

[19] Maulana, A., & Putri, A. D. (2019, March). Development of digital currency technology. In Journal of

Physics: Conference Series (Vol. 1175, No. 1, p. 012205). IOP Publishing.

[20] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.

[21] Wall, E., & Malm, G. (2016). Using blockchain technology and smart contracts to create a distributed securities depository.