IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY AND ITS IMPACT ON CYBERSECURITY: AN ANALYSIS

Satyendra Kumar

Department of Computer Science, Security Architect at Accenture in Singapore.

ABSTRACT

Blockchain technology protects data through an integrated system that gathers, organises, stores, and distributes data in various chunks. Thus, this technology makes it possible to add the data to the network. No one can change the data set by adding or by erasing new data once it has been introduced to the network. Furthermore, modifications to a blockchain are permanently recorded in the database, this technology makes it easier to track and verify any changes that are made. This technology downloads its data on a regular basis, organising and storing a copy locally since it utilises numerous systems in a blockchain. It makes use of the cooperation of numerous performers and achievements in cryptography to locate the data faults and cyberattacks in advance by analysing the data documented. This technology has seen adoption in many areas, most notably in finance through the usage of cryptocurrencies, but the technology is viable in cybersecurity. This article examined many use cases of blockchain in the cybersecurity modules as envisioned by different researchers.

Keywords

Cloud computing, medical data, Triple level Encryption, hash function, patient privacy and security

I.Introduction

Blockchain is a decentralised, publicly available database on computers that tracks transactions as blocks. The ability of this ledger to be everlasting and to only allow authorised users access promotes a transparent storing of data [1-3]. Blockchain is a popular distributed ledger that enables the recording and tracking of transactions, which can be traced back to 1976 in a publication by Diffie titled "New Directions in Cryptography".

Cybersecurity is the act of safeguarding networks and systems from digital assaults that seek to gain entry, alter, or eradicate digital data with the intention of extorting money or sensitive information [4]. As our dependence on technology and data continues to grow, it becomes increasingly crucial to fortify security measures in order to safeguard digital data and transactions. Cyberattacks can be executed using various types of malicious software such as worms, spyware, backdoors, etc. [5]. Some commonly encountered forms of cyberattacks include Phishing, Man in the middle (MITM) attack, Distributed denial of service (DDoS) attack, Ransomware, and SQL injection attacks [6 & 7].

Blockchain presents an alternative route towards enhanced security, i.e., less commonly taken and not nearly as welcoming to cybercriminals [8]. This approach diminishes vulnerabilities, offers robust encryption, and validates data integrity and ownership more effectively. It can even abolish the necessity for certain passwords, which are often referred to as the weakest link in cybersecurity [9].

The primary benefit of blockchain is its utilization of a decentralized ledger [10]. By removing the most obvious targets, a distributed approach of infrastructure with public keys lowers numerous hazards related to centrally stored data [11]. Unless there is platform-level vulnerability, it is very hard for attackers to steal, corrupt, or change data because transactions are tracked across each node in the network [12, 13].

The collaborative consensus method used by blockchains eliminates another typical drawback. Without depending on a centralized authority, it may identify malicious behavior, abnormalities, and false positives [14]. Not any of them can be fooled, just one of them. This enhances authentication and safeguards data transmissions and record-keeping [15].

Blockchain does make use of encryption, one of the most significant cybersecurity techniques, while having many unusual aspects. In an internet of things (IoT) ecosystem, the decentralised ledger can leverage public key infrastructure to encrypt communication, check devices, confirm configuration updates, and identify private devices.

In the context of this research, the communication is the unprocessed and unprotected information that needs to be analyzed, which can come in the form of electronic mails or instant messages. To analyze the unprotected information, a hashing algorithm will be employed, a Hashing Algorithm is defined as a cryptographic algorithm that analyzes data and produces a distinct series of characters representing the data, numerous hashing algorithms are available that offer varying levels of security and require different computational capabilities. Hashes are widely utilized as a means to digitally sign text files or data files in order to prevent unauthorized modifications. In order to ensure the authenticity of each communication, users are required to provide a Personal Key to be used by the Hashing Algorithm. The user's Personal Key is a unique key that is exclusively known by the user and is employed to encrypt the communication, it is known to be mathematically irreversible using the resulting hash value. Once the communication is secured, it is added to the blockchain and distributed to other blockchain networks.

The Blockchain is an ever-growing list of records referred to as blocks that are interconnected and protected by hashes utilizing cryptography based on the available hashing algorithms. A hashed communication is the output of the newly created block in the updated blockchain where each created block will have a unique hash identifier that is appended to the final communication before it is transmitted to its intended recipient. Although cryptography has its limitations, this research includes the selection of a hashing algorithm that has been proven to offer the highest level of security against unauthorized access. By utilizing encryption and digital signatures, a blockchain system can protect connected thermostats, smart doorbells, security cameras, and other susceptible edge devices.

In addition, this technology can act as a defense against distributed denial-of-service (DDoS) attacks. The sole point that allows these attacks to succeed can be removed using a domain name system (DNS) protocol built on a blockchain [16–18]. A DDoS attack on the hosting infrastructure of one DNS host in 2016 caused a sizable chunk of the internet to go offline. Blockchain is a potentially effective cybersecurity technique since it is centred on building confidence in a dubious ecosystem. Although this ledger system is decentralised, members of the particular blockchain have free access to the data. Every member (or node) has access to all encrypted data related

to transactions that is recorded on their blockchain and can record, send, and read it. This procedure upholds a high standard of data integrity while simultaneously fostering confidence.

Essentially, Blockchain's distributed architecture prevents any single point of vulnerability or weak spot from exposing large datasets to risk. No password is required to access the transparent ledger. The ledger can create a single, impenetrable way of entry into any sensitive data by leveraging biometrics, such fingerprints and retina scans. The use of decentralised storage reduces the amount of data that may be compromised to almost nothing by ensuring that each block only holds a single piece of a much larger jigsaw. Finally, each node on the blockchain has access to the public record-keeping system, which makes it possible to detect prospective criminal attempts in real time. The special characteristics of blockchain, which put an extremely unbreakable barrier among a hacker and the data you provide, can help the cybersecurity business.

The common reviews of blockchain and cybersecurity are well-understandable in this section. The rest of this critique is structured in the following fashion. Section 2 provides an overview of the cybersecurity research in the blockchain. Section 3 outlines the general systems of the cybersecurity for blockchain. Section 4 relevant cases of the cybersecurity research for blockchain. The merits and applications of these approaches are discussed in Section 5. Lastly, Section 6 concludes the complete article with some suggestions.

II.OVERVIEW OF PRIVACY AND CYBERSECURITY IN BLOCKCHAINS

Numerous designing options and applications are available with blockchain technologies that can generally improve cybersecurity.

Challenges with blockchain

Governments and major institutions are both advocating for the adoption of a blockchain-powered cybersecurity system because they view it as the future. However, implementing this system is not as simple as updating an existing toolkit.

The connection between blockchain technology and cybersecurity is continuously evolving. Not all research proposals on smart contracts, decentralized storage, protecting edge devices, or digital identities align with industry needs. Without proper planning, the implementation of these proposals may become stimulating inconceivable, even. Below are several challenges that businesses may encounter when integrating blockchain into their cybersecurity strategy [21].

Distributed Blockchain for security

Distributed block chain technology digitalizes and disperses record-keeping across a network, so the process of verifying transactions no longer relies on a single central institution [22]. Distributed block chains are always decentralized but vary widely in permissions, sizes, roles, transparency, types of participants, and how transactions are processed [23]. A decentralized structure provides inherent security advantages because it eliminates the single point of failure [24].

Distributed block chain also consist of several inherent security features, namely encryption, private and public keys, contracts, identity controls and software-mediated agreement. These built-in features ensure data protection and integrity by authenticating transaction records, verifying access, demonstrating traceability, and preserving privacy.

By providing greater resilience, transparency, and encryption, these configurations strengthen the position of distributed block chains in terms of integrity, confidentiality, and availability [25-27]. However, distributed block chains are created and constructed by individuals, which means they are susceptible to human mistakes, biases, or vulnerabilities based on the specific use case, subversion, or malicious attack.

Background and traceability

Blockchain designs are fundamentally based on traceability and Visibility, however their security benefits might vary depending on the application. A digital decentralised ledger holds unchangeable records of parties' transactions and goods information in the context of a supply chain and throughout the lifespan of the product [28-30]. This decreases the risks of forgery and manipulation by any individual party. In financial scenarios, visibility and unchangeability of payment history decrease the necessity for a central intermediary. Blockchains can also enhance the security and confidentiality of transactions, namely money transfers and international payments.

Transactions between software and/or devices authentication

Blockchain transactions can be used for any verifiable interaction, not just financial transactions, such as aiding in the prevention of IoT device compromise. Validating software updates is a beneficial cyber health practice because of the widespread distribution of malicious "updates." Organisations can use blockchain hashing to verify updates, downloads, and patches with the product's developer. This also aids in thwarting supply chain attacks, especially since software and edge IoT devices are attractive targets for network penetration [5, 11, 13, and 16].

Continuity and availability

Decentralised infrastructure promotes resistance to attacks, fraud, and disruptions. This method reduces the vulnerabilities listed below.

- Distributed communication and information technology networks can reroute users and limit the exposure of user data in the event that a central database is compromised or goes offline.
- In an IoT environment, security decisions can be taken further away from the network's core by distributing operations and administrative oversight.
- Redundancy is aided by decentralising DNSes in the case of a DDoS assault.

Ownership confirmation

A tokenization method for preserving data format on the blockchain known as Proof of Ownership (POW) provides immutable proof of data ownership. It surpasses current record-keeping systems that depend on a centralized repository and a data owner [31].

It was difficult to demonstrate that one owned internet assets before digital ledgers. Even in the real world, millions of people lack access to trustworthy government identification or financial institutions. Deeds can be lost, credentials don't always hold up across borders, and credentials can be stolen. Non-fungible tokens (NFTs) allow artists to digital watermark their work [32]. The ability to produce an unalterable proof of legitimacy and ownership utilising cryptographic keys has various security advantages across numerous blockchain application scenarios, including the following:

- Owners of real estate can demonstrate their ownership and assign rights.
- Possessing the capacity to independently control their credentials of students, teachers, jurisdiction, and professionals can lessen the use of fake certificates.

- Manufacturers can affix NFTs to their products to guarantee authenticity, including luxury brands.
- By retaining full control over their media, creators can strengthen copyright defenses.

III.BLOCKCHAIN FOR CYBERSECURITY: A CASE-BASED APPROACH

The various existing security protocols simply cannot keep pace with the relentless and cunning attacks. In the present digital era, the significance of cybersecurity has increased. With the ever-growing dependence on technology and the internet, the risk of cyberattacks has significantly risen. In response, various remedies have been devised to aid in the protection against these dangers, including the utilization of blockchain technology. Initially developed as the underlying technology behind Bitcoin, blockchain technology has expanded its potential applications far beyond the realm of cryptocurrency [33, 46]. One domain where blockchain technology is now increasingly employed is in augmenting cybersecurity.

This technology possesses distinctive characteristics that render it suitable for safeguarding data and preventing cyberattacks [34]. For instance, the decentralized nature of blockchain implies that it is not governed by a solitary entity, thus making it more resilient against attacks. Furthermore, the utilization of cryptographic protocols and digital signatures ensures that data stored on a blockchain is highly secure and immune to tampering.

Technologies engaged in constructing blockchain-driven platforms and applications possess the capability for enhanced security; however, technologies are never the initial step. Security authorities must collaborate with product and platform creators to initially recognize the issues, connections, and compromises for novel security functionalities, and subsequently they can actively devise, assess, execute, and oversee them. Various cases for blockchain used in the enhancement of cybersecurity are drawn in below Figure 1.

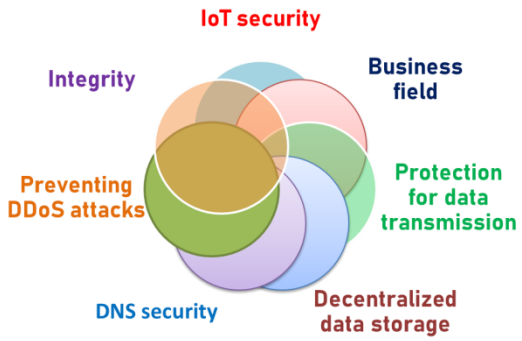

Fig. 1. General cases of blockchain-based cybersecurity

Looking at some of the problems with adopting blockchain technology for cybersecurity will also be discussed solutions. Overall, blockchain technology has a huge potential to improve cybersecurity, and as it develops, it is expected to play a bigger and bigger part in thwarting online threats. We will examine the impact of blockchain technology on bolstering Cybersecurity. We will delve into the different methods in which blockchain can be employed to safeguard information and thwart cyber threats, such as utilizing blockchain for authentication management, protected data retention, and encrypted correspondence [35]. The concepts mentioned in the above figure are explained in the upcoming sub-sections.

Integrity of data: In the majority of blockchain systems or distributed ledger technologies (DLT), the information is organized into blocks and each block consists of a transaction or a group of transactions [36]. Every fresh block links to all the preceding blocks in a cryptographic chain, making it extremely difficult to manipulate. In essence,

blockchain has the potential to enhance the security and authenticity of data by establishing a system where anyone can contribute and validate information. However, it is unfeasible to input inaccurate data as the validators will consistently detect it.

Data on blockchains cannot be modified because network nodes cross-check and expand on each other and necessitate agreement to authenticate transactions [37]. However, data off-chain can be tampered with. This is where on-chain signatures can facilitate novel blockchain use cases where security is of utmost importance. Distributed voting, health and scientific data cooperation among institutions, and decentralized metadata, which is progressively crucial for enhancing AI in cybersecurity of data reliability applications in which blockchain designs are emerging.

Protection of data transfer: By adopting encryption, data transmission will be shielded from unauthorised access.

Decentralized data storage: Data might be kept in a blockchain, which happens to be impenetrable and resistant to hacking, rather than on centralised systems that are subject to assault. Using blockchain technology, a decentralised and secure data storage system can be built [38].

IoT security: As AI and IoT are used more frequently, protecting data and systems from intruders has consistently been a top priority [39]. A feasible application used for sustaining cybersecurity in the IoT system uses blockchain technology to increase security by utilising device-to-device encryption to safeguard communication, management of keys mechanisms, and authentication.

DNS security: It connects domain names to their IP addresses, functions like a public directory. Over the years, hackers have made attempts to enter the DNS and take advantage of these links, crashing websites in the process [40]. The DNS can be stored with increased security because of the immutability and decentralised nature of blockchain technology.

Minimizing DDoS attacks: The most common assault is the DDoS attack, in which criminals attempt to interrupt service delivery by flooding the Internet with traffic. Blockchain has shown to be a successful defence against these attacks thanks to its immutability and cryptographic features [41].

The reliability of software downloads: In order to stop fraudulent software from infecting the devices, blockchain can be used to verify updates and installers [42]. In this case, hashes are stored in the blockchain and can be compared to new software IDs to confirm the validity of the download.

Business field: Blockchain improves the traceability, security, trustworthiness, and transparency of data exchanged around a business networks while generating new efficiencies that save costs [43]. Blockchain for business employs an open, unchangeable ledger that only members with authorization can view.

IV.RELATED RESEARCHES

Based on the relevant reviews conducted during the course of this study, it was discovered that works related to the field of Blockchain Technology focused on Cybersecurity have been investigated by other authors. In the research [44], examining the applications of Blockchain Technology, it was determined that blockchain technology has the potential to secure various areas such as the IoT (Internet of Things), Social Media Networks, and other industry sectors beyond computing such as Healthcare, Finance, and Marketing. This is further supported and indirectly validated, explored and successfully implemented blockchain technology [45] in digital supply chain systems while considering interoperability. The most recent study implemented blockchain

technology in the field of cybersecurity intrusion detection and found that blockchain technology is applicable for the purpose of detecting intrusions.

Phishing is one of the most widespread yet prevalent threats to Cybersecurity. Phishing is a type of cyber-attack where an attacker pretends to be reputable companies and/or institutions by copying authentic e-mail messages, instant messages, and/or websites in an effort to obtain sensitive data from victims like usernames, passwords, credit card information, and more [49]. Systems that utilize blockchain employ a network of multiple nodes where each member of the network has access to the most recent version of an encrypted ledger so they can verify a new transaction.

Previous research indicated that 50 percent of phishing is conducted via electronic mail [48]. Additionally, it was discovered that financial institutions and card issuers in the U.S (in 2003) incurred indirect losses nearly $1.2 billion, when approximately two million users divulged their information to counterfeit websites [49]. Conversely, investigations into fortifying data protection assert that Blockchain technology can securely store crucial information by implementing a considerable number of nodes. It is also contended that any application employing a Blockchain fosters trust in decentralized systems and ultimately advances cyber tranquility. Rather than entrusting your data to a Cloud Based Data Center, Blockchains have the capability to offer the same service while bolstering the security aspect.

Depending on the size and circumstances of the desired system, distributed ledgers can be employed extensively for various decentralized or peer-to-peer systems. However, the research validates Tapscott's hypothesis, and additional advancements (2016) in the technical execution of blockchain technology may be incorporated, leading to a higher utilization of network capacity for the suggested email server platforms during the dissemination of the revised ledger [46]. Nonetheless, there is a minor lag in the delivery of the emails.

It can be reasonably inferred that despite the usefulness of blockchain technology has been demonstrated in a broad range of practical uses such as cybersecurity. There has not been a real trial or at the very least a simulation carried out to examine the efficiency of blockchain technology. To tackle the identified shortcomings, this paper integrates the techniques in Blockchain Technology in an effort to further bolster Cybersecurity by enhancing current protocols to combat phishing and improving data security and integrity.

V.A POWERFUL TOOL FOR CYBERSECURITY: BLOCKCHAIN

The biggest threat to each trade, business, and corporation in the world is regarded as being posed by the massive and rapidly expanding underworld industry known as cybercrime. Blockchain in cybersecurity is widespread, and we've employed it as a new tool in the battle to safeguard and to safe our most sensitive information.

In Blockchain and banking concepts, Billions of dollars in financial transactions combined with outdated and centralized cybersecurity measures make the biggest banks frequent victims of hacking and fraud. In reality, the majority of global banks presently encounter cyber assaults on a daily basis, with cyber criminals concentrating on operational hazards. The initial implementers among Street banks employ blockchain technology to protect their crucial information. As stated in its yearly report, the more advanced phishing attacks specifically target staff members who possess authorization to classified data. The report proposes a multi-tiered security procedure to distribute risk - precisely what blockchain can offer.

In Integrity of cryptocurrencies and blockchain technology, DLT safeguards the authenticity of cryptos via encryption techniques and the dissemination of public data. The credibility of individuals' cryptocurrency transactions is guaranteed as they can track the movement of the digital currency back to its source. Encryption aids in managing the production of cryptocurrencies, thereby maintaining their stability.

In IoT security with blockchain, it is an expanding industry full of originality, imagination and, as a result, cybersecurity concerns. Nowadays, IoT products can be found in nearly every aspect of our lives. Everything is wirelessly connected, from robotic sprinklers to bike locks with bluetooth capabilities to smart kitchen equipment. There have been numerous reported IoT device breaches over the past few years will certainly rise given estimates that there will be more than 55 billion connected IoT devices by upcoming years.

One cybersecurity-related study discovered that might be bypassed by hackers for the safeguards in an implanted cardiac device, granting them the capacity to drain the battery and provide cardiac shocks that aren't appropriate. As the IoT device market continues to expand, the need for an improved form of cybersecurity grows as well. Blockchain offers a secure infrastructure for secure data transmission between devices without the involvement of hackers. IoT devices can provide trails for inspecting and tracing the registration and use of products thanks to decentralised control. Moreover, it was revealed that the camera was the target of hackers of an "intelligent" baby monitor by acquiring a basic IP address. The system was fully under the control of the hackers, allowing them to observe over the camera and eavesdrop on conversations.

In secured supply chains, DLT can be employed to establish a clear and dependable supply chain [45]. By tracing merchandise and their transfers on the distributed ledger, corporations can guarantee the authenticity of their products and confirm that no unauthorized modifications have occurred.

In Blockchain and medical records for patients, similar to banking, the healthcare sector faces a constant barrage of cyber assaults [50]. In reality, healthcare encounters twice the number of phishing emails and malware attacks compared to any other industry. New obstacles emerge regularly and now encompass cyber-attacks on IoT devices that are camouflaged using encrypted malware.

In addition to storing personal financial information, healthcare institutions like clinics, hospitals, and doctors' offices also have access to vital medical records. Cybercriminals are drawn to patient data because it sells for an expensive amount on the black market. Although credit card details are regularly stolen, contemporary technology typically quickly undoes any damage. It can be disastrous to reveal information such as social security numbers, full names, weights, heights, medications, and health issues of millions of patients. Hackers have previously extorted billions of dollars from clinics all across the world by threatening to reveal private information, and they will continue to do so until new technologies are introduced.

Blockchain might be the vitally important answer to an issue that poses serious risks to hospitals and their patients. Due to the decentralised nature of the DLT, only a small number of people [36] are allowed access to data that, when taken together, would make up a patient's whole health record. Only specific information made available to licenced healthcare practitioners’ guarantees that cybercriminals cannot access all identifiable aspects of an individual's medical record.

In Government regulations on cybersecurity and blockchain, the permeable security can be enhanced with blockchain. The whole system operates on secure encryption of data, effectively creating a wall between hackers and identifiable information. Encrypted data, distributed information storage, and publicly-accessible ledgers can establish a fresh set of government cybersecurity objectives [21, 26, 30, and 39]. Authorities would be able to rapidly detect potential breaches and track the tampered data back to its source. These governments and agencies,

in their efforts to be at the forefront of governmental blockchain adopters, are pioneering methods to incorporate DLT into everyday cybersecurity procedures.

In Military and defence data on blockchain, progress within the military and defense industries has resulted in some of the most significant technological advancements in the last hundred years [51]. Blockchain is regarded as a credible means of protecting data for military organizations, defense contractors, and aerospace firms that handle highly sensitive information [52].

The armed forces were at the forefront of developing the Internet to disseminate crucial and intricate data to geographically dispersed teams worldwide, and they devised GPS to enhance their understanding of military positioning. These military and defense enterprises utilize blockchain's encryption and decentralization techniques to enhance data security and optimize confidentiality.

Thus, from these above-declared blockchain with cybersecurity innovation for the digital era that will assist maintain adherence to the CIA (Confidentiality, Integrity, Availability) triads that of cybersecurity. However, the complicated nature of its execution may make application challenging.

VI.MERITS AND APPLICATIONS

The major benefits of this module are availability, confidentiality, integrity, responsibility, etc. and their applications are also discussed in detail.

Blockchain benefits

The Executives and technology professionals have expressed interest in the blockchain and cybersecurity combo despite probable obstacles. One-third of research report identified blockchain use in creating security solutions as the leading trend in cybersecurity. It placed higher than the rising need for cybersecurity employment, which was tied for third among all themes. The following are some of the reasons why blockchain technology is promising and how it should be managed:

Security for smart contracts: Data security, authentication, access control, and business logic must be validated for blockchain components such smart contracts, APIs, wallets, digital assets, and applications. As a result, permissioned chain participants are more confident.

Data security and confidentiality: The technology offers specific entry to transactions and data in the decentralized ledger with limited regulation. Additionally, blockchain does not provide cyber criminals with conventional data security objectives and the capability to undermine confidentiality obstacles. In general, this makes it more difficult to obtain or alter information in blockchain networks.

Management of the public key infrastructure: Digital signatures and asymmetric cryptographic keys are essential components of blockchain security. The public key termed as the digital identity for node participants throughout implementation. To securely encrypt, sign, and validate transactions, the private key is required for authorization. Blockchain asymmetric cryptography offers advantages comparable to those of conventional encrypted transactions.

The other recent merits involved are enhancing IoT hardware, preserving the integrity of crypto-currencies, safeguarding patient health information, protecting bank assets, protecting military and defence information, government cybersecurity procedures being updated, etc. With blockchain cybersecurity guiding the way,

industries throughout the board are embracing emerging technology that offers to increase online safety. Therefore, finding a trustworthy cybersecurity protocol is more crucial than ever.

Blockchain applications

The DLT applications already drive initiatives that depend on safety, regulated entry, responsibility, openness, and effectiveness. Security executives must comprehend the advantages and hazards of DLT's overall blueprint prior to deploying these scenarios and leveraging them to cultivate confidence in the virtual realm.

VII.CONCLUSION

Despite these advantages, companies should continue to adhere to security best practices, such as implementing limitations on rates, encrypting sensitive configuration files, and identifying and rectifying vulnerabilities in the development process. Many have mistakenly viewed its cryptographic foundation as the ultimate solution to security, resulting in a failure to implement the necessary security controls for trust in blockchain. The authors also noted that the perception of blockchain technology is often polarized, with some considering it inherently insecure while others view it as unhackable, when in reality, the truth lies somewhere in between.

The adoption of blockchain to boost cybersecurity has been gaining momentum globally. Enterprises now strive for increased transparency and protection in their networks and supply chains, even amidst an economic downturn. The digitization and robustness are crucial in a more challenging and uncertain world. Organizations aim to integrate confidentiality and effective management while ensuring security and transparency. Although the use of blockchain is still limited, the integration of blockchain and cybersecurity is not confined to the periphery. It is already recognized as a crucial tool in environments where security is of utmost importance.

Blockchain technology significantly contributes to improving cybersecurity. Blockchain technology offers a highly transparent and secure framework for data storage and transmission with its unalterable record, distributed storage, smart contracts, digital signatures, agreement mechanisms, and public key cryptography. Businesses and individuals may protect their data from hacker assaults and unauthorised access by utilising blockchain technology. Data is protected during transmission because to the decentralised nature of the blockchain network, which makes it difficult for hackers to access and alter data, and by means of digital signatures and public key cryptography.

The usage of blockchain-based systems can offer a potent answer to strengthen cybersecurity in today's digital environment, when cyber dangers are a continual worry. Although it is still in its infancy, blockchain technology has the power to completely transform the cybersecurity industry. We may anticipate a sharp decline in cyber risks and an improved secure digital environment as more companies and people use this technology.

Businesses can get the know-how to protect against data breaches from more active consulting services. Consultants work with firms to design thorough security plans that identify potential dangers and weaknesses in their structures and develop mitigation techniques for those risks. Additionally, ongoing support is provided to make sure that organisations are aware of the most recent cybersecurity risks as well as ensuring their security procedures continue to be effective. Businesses may feel secure knowing that their sensitive data is adequately protected and that their systems are secure thanks to these cybersecurity consulting services.

REFERENCES

1. Zhu, H., Wang, Y., Hei, X., Ji, W. and Zhang, L., 2018, October. A blockchain-based decentralized cloud resource scheduling architecture. In 2018 International Conference on Networking and Network Applications (NaNA) (pp. 324-329). IEEE.

2. Morgan, S., 2019. Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. Cybercrime Magazine, 10.

3. Karafiloski, E. and Mishev, A., 2017, July. Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies (pp. 763-768). IEEE.

4. Sandhu, K., 2021. Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges. Handbook of Research on Advancing Cybersecurity for Digital Transformation, pp.1-17.

5. Kimani, K., Oduol, V. and Langat, K., 2019. Cyber security challenges for IoT-based smart grid networks. International journal of critical infrastructure protection, 25, pp.36-49.

6. Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K., 2021. A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), pp.669-710.

7. Biju, J.M., Gopal, N. and Prakash, A.J., 2019. Cyber attacks and its different types. International Research Journal of Engineering and Technology, 6(3), pp.4849-4852.

8. Fadi, O., Karim, Z. and Mohammed, B., 2022. A survey on Blockchain and Artificial intelligence technologies for enhancing security and privacy in smart environments. IEEE Access, 10, pp.93168-93186.

9. Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. and Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, p.101660.

10. Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S.J.C.C., 2019. Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22, pp.14743-14757.

11. Pan, J. and Yang, Z., 2018, March. Cybersecurity challenges and opportunities in the new" edge computing+ iot" world. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 29-32).

12. Li, W., Su, Z., Li, R., Zhang, K. and Wang, Y., 2020. Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network, 34(6), pp.31-37.

13. Vashisht, S., Gaba, S., Dahiya, S. and Kaushik, K., 2022. Security and privacy issues in IoT systems using blockchain. Sustainable and Advanced Applications of Blockchain in Smart Computational Technologies, pp.113-127.

14. Hassan, M.U., Rehmani, M.H. and Chen, J., 2022. Anomaly detection in blockchain networks: A comprehensive survey. IEEE Communications Surveys & Tutorials.

15. Chithanuru, V. and Ramaiah, M., 2023. An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. Concurrency and Computation: Practice and Experience, p.e7724.

16. Shah, Z., Ullah, I., Li, H., Levula, A. and Khurshid, K., 2022. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 22(3), p.1094.

17. Alotaibi, B., 2019. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. IEEE Sensors Journal, 19(23), pp.10953-10971.

18. He, S., Ren, W., Zhu, T. and Choo, K.K.R., 2019. BoSMoS: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial Internet of Things. IEEE Internet of Things Journal, 7(2), pp.948-959.

19. Attaran, M. and Gunasekaran, A., 2019. Applications of blockchain technology in business: challenges and opportunities.

20. Mylrea, M. and Gourisetti, S.N.G., 2018, August. Blockchain for supply chain cybersecurity, optimization and compliance. In 2018 resilience week (RWS) (pp. 70-76). IEEE.

21. Hasanova, H., Baek, U.J., Shin, M.G., Cho, K. and Kim, M.S., 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), p.e2060.

22. Aste, T., Tasca, P. and Di Matteo, T., 2017. Blockchain technologies: The foreseeable impact on society and industry. computer, 50(9), pp.18-28.

23. Helo, P. and Hao, Y., 2019. Blockchains in operations and supply chains: A model and reference implementation. Computers & industrial engineering, 136, pp.242-251.

24. Athanere, S. and Thakur, R., 2022. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. Journal of King Saud University-Computer and Information Sciences, 34(4), pp.1523-1534.

25. Huang, J., Kong, L., Chen, G., Wu, M.Y., Liu, X. and Zeng, P., 2019. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), pp.3680-3689.

26. Vance, T.R. and Vance, A., 2019, October. Cybersecurity in the blockchain era: a survey on examining critical infrastructure protection with blockchain-based technology. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 107-112). IEEE.

27. Charla, G.B., Karen, J., Miller, H. and Chun, M., 2021, May. The Human-side of Emerging Technologies and Cyber Risk: A case analysis of blockchain across different verticals. In 2021 IEEE Technology & Engineering Management Conference-Europe (TEMSCON-EUR) (pp. 1-6). IEEE.

28. Ar, I.M., Erol, I., Peker, I., Ozdemir, A.I., Medeni, T.D. and Medeni, I.T., 2020. Evaluating the feasibility of blockchain in logistics operations: A decision framework. Expert Systems with Applications, 158, p.113543.

29. Subramanian, N., Chaudhuri, A. and Kayıkcı, Y., 2020. Blockchain and supply chain logistics: Evolutionary case studies. Springer Nature.

30. Kaushik, K., 2022. Blockchain enabled artificial intelligence for cybersecurity systems. In Big Data Analytics and Computational Intelligence for Cybersecurity (pp. 165-179). Cham: Springer International Publishing.

31. Wang, Y. and Kogan, A., 2018. Designing confidentiality-preserving Blockchain-based transaction processing systems. International Journal of Accounting Information Systems, 30, pp.1-18.

32. Cheong, B.C., 2022. Application of Blockchain-enabled technology: Regulating non-fungible tokens (NFTs) in Singapore. Singapore Law Gazette, January.

33. Miraz, M.H. and Ali, M., 2018. Applications of blockchain technology beyond cryptocurrency. arXiv preprint arXiv:1801.03528.

34. Muheidat, F. and Tawalbeh, L.A., 2021. Artificial intelligence and blockchain for cybersecurity applications. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 3-29). Cham: Springer International Publishing.

35. Aiden, M.K., Sabharwal, S.M., Chhabra, S. and Al-Asadi, M., 2023. AI and Blockchain for Cyber Security in Cyber-Physical System. In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications (pp. 203-230). Cham: Springer International Publishing.

36. Farahani, B., Firouzi, F. and Luecking, M., 2021. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177, p.102936.

37. Rathee, G., Sharma, A., Kumar, R. and Iqbal, R., 2019. A secure communicating things network framework for industrial IoT using blockchain technology. Ad Hoc Networks, 94, p.101933.

38. Shobanadevi, A., Tharewal, S., Soni, M., Kumar, D.D., Khan, I.R. and Kumar, P., 2021. Novel identity management system using smart blockchain technology. International Journal of System Assurance Engineering and Management, pp.1-10.

39. Sadik, S., Ahmed, M., Sikos, L.F. and Islam, A.N., 2020. Toward a sustainable cybersecurity ecosystem. Computers, 9(3), p.74.

40. Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. and Rong, C., 2019. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal, 6(5), pp.8114-8154.

41. Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), p.1333.

42. Deshmukh, A., Sreenath, N., Tyagi, A.K. and Abhichandan, U.V.E., 2022, January. Blockchain enabled cyber security: A comprehensive survey. In 2022 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

43. Korepin, V., Dzenzeliuk, N., Seryshev, R. and Rogulin, R., 2021. Improving supply chain reliability with blockchain technology. Maritime Economics & Logistics, pp.1-14.

44. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In Technology & Engineering Management Conference (TEMSCON), 2017 IEEE (pp. 137-141).

45. Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In proceedings of the 50th Hawaii international conference on system sciences.

46. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.

47. Benaddi, H. and Ibrahimi, K., 2020, October. A review: Collaborative intrusion detection for IoT integrating the blockchain technologies. In 2020 8th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE.

48. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586.

49. Litan, A. (2004). Phishing attack victims likely targets for identity theft.

50. Legaspi, J., 2019. Exploring the Cybersecurity Measures Healthcare Managers Use to Reduce Patient Endangerment Resulting from Backdoor Intrusions into Medical Devices (Doctoral dissertation, Colorado Technical University).

51. Kumar, S.S., Kumar, S.G., Chandraprabha, S., Shankar, B.M. and Kumar, S.S., 2021. Blockchain-Based Secured Data Management in Confidential Cyber Defence Applications. In Blockchain for Information Security and Privacy (pp. 177-191). Auerbach Publications.

52. Selimoglu, S.K. and Saldi, M.H., 2023. Blockchain Technology for Internal Audit in Cyber Security Governance of Banking Sector in Turkey: A SWOT Analysis. In *Contemporary Studies of Risks in Emerging Technology, Part B* (pp. 23-55). Emerald Publishing Limited.