IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology: Revolutionizing Cybersecurity

Tanushree Parmar[1]
Assistant Professor
Computer Science
(Techno India University, Kolkata)

Ekta Chandak[2]
Assistant Professor
Management
(Techno India University, Kolkata)

Abstract

E-commerce applications are being used in distributed networks more and more these days. Numerous benefits come with these apps, such the ability to shop online from multiple locations. Offloading application data from user devices to servers creates numerous research hurdles for the sake of simplicity. This study provides a thorough examination of the most widely used blockchain security applications and finds peer-reviewed literature that aims to use blockchain technology for cyber security. Blockchain technology offers several features including immutability, integrity, trackability, and decentralization. This paper presents the blockchain architecture and elucidates the concept, attributes, and necessity of blockchain technology in the field of security. It makes an effort to draw attention to how blockchain is influencing the direction of cryptocurrency, cyber security, and IoT adoption. This essay outlines the benefits of blockchain technology over traditional systems and justifies its necessity in a number of technological domains. According to our research, new blockchain applications can benefit greatly from the Internet of Things (IoT), networks, machine learning, public-key cryptography, web apps, certification programs, and the safe storing of personally identifiable information (PII).

Keywords: Blockchain, Cybersecurity, Distributed Ledger Technology (DLT), Smart Contracts

1. Introduction:

Our way of life has altered as a result of the Internet. Its use to share our opinions, interact virtually on social networking sites, enjoy digital entertainment, market, and even purchase and sell has enhanced every minute of our lives. Organizations should take deliberate action if they wish to benefit from the newest Internet technology. E-commerce is one of the most important areas on which a business may concentrate. The age of E-commerce is revolutionary, constantly expanding and altering the traditional methods of managing business. It also serves as the foundation for new global corporate ventures. Electronic kinds of software serve as the cornerstone of e-commerce.

Our everyday lives now cannot function without the internet, and the needs for online services are only getting bigger. The global e-commerce platform has been significantly impacted by the digital world. For a variety of network users, online business platforms offer flexibility and convenience from various stores (Balaji N, 2019). For instance, using the internet platform makes it simple to complete the registration and transaction processes. Because of this, cyberattacks are spreading very quickly around the globe.

Blockchain: Under the pseudonym Satoshi Nakamoto, a creator published concepts for the distributed ledger technology known as Blockchain and the digital money known as Bitcoin in 2008 (Nakamoto, 2008). The decentralized underlying technology of bitcoin ensures data integrity and accountability by encrypting the data. As a result, the technology is becoming more popular and widely used across numerous industries. It builds a distributed database that is impervious to unauthorized access by recording and encrypting the data in a series of back-linked blocks of information (Wang, 2020). Additionally, smart contracts emerged as a key component of blockchain technology. It's a self-enforcing contract that regulates who can access data storage nodes on behalf of two or more parties (Alam Khan, Asif, Ahmad, & Alharbi, 2020).

This technology is regarded as a great technological achievement in recent history. Its foundations include several types of software, the science of cryptography, and disruptive computing. It is described as the series of online transactions recorded on numerous computers connected to a peer-to-peer network as a shared ledger (An introduction to blockchain in ecommerce, 2019). The World Economic Forum claims that blockchain has the potential to develop into a robust transactional instrument that boosts user empowerment, lowers corruption, and enhances trust (Shaping the Future of Technology Governance: Blockchain and Distributed Ledger Technologies, 2020). Consequently, the largest danger to the future of e-commerce platforms is now the security of network design (Apau, Korenteng, & Gyamfi, 2019).

Cybersecurity: The process of protecting networks, computers, servers, mobile devices, electronic systems, and data from hostile intrusions is known as cyber security. It is often referred to as electronic information security or information technology security. The word can be categorized into a few basic categories and is used in a range of contexts, including business and mobile computing. (Kaspersky). Operational security includes decisions and processes for managing and protecting digital assets. This covers the permissions people have when they connect to a network and the guidelines that specify where and how information can be exchanged or kept.

Disaster recovery and business continuity refer to how a company handles a situation, like a cyber-security incident, that causes it to lose operations or data. Plans for disaster recovery outline how the business will rebuild its information and operations to fully function after an event. The technique a company employs to attempt to continue operating in the event that certain resources are unavailable is known as business continuity. The process of safeguarding a computer network against trespassers, be they malevolent actors or malicious software is known as network security (Kemmerer, 2003).

The goal of application security is to defend software and hardware from intrusions. Through compromise, the data that an application is designed to secure could be accessed. Good security begins in the design stage, long before a program or device is used. Information security procedures protect data integrity and privacy during transmission and storage (Jang-Jaccard & Nepal, 2014).

2. Distributed Ledger Technology

A digital asset transaction recording system called distributed ledger technology (DLT) simultaneously records the transaction and all of its details in multiple places. Unlike conventional databases, distributed ledgers do not have a central data repository or administrative functions.

DLT refers specifically to the technology architecture and protocols that enable concurrent access, validation, and updating of the records that comprise distributed ledgers. It runs on a computer network that connects multiple nodes, objects, or places (Lemieux & Bravo, Introduction: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part I), 2021).

Every node in a distributed ledger processes and validates every item, producing a record of every item and reaching an agreement on its accuracy. Both dynamic data, like financial transactions, and static data, like registries, can be recorded in a distributed ledger.

2.1 How Do Distributed Ledgers Function?

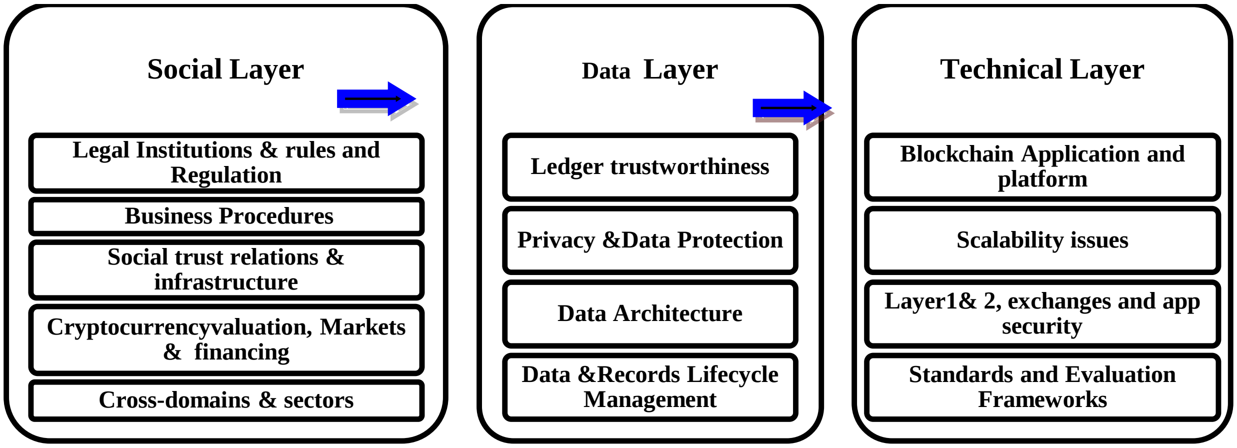
The decentralization principles underpin the operation of DLT. DLT functions on a peer-to-peer (P2P) network, where numerous nodes store, validate, and update the ledger concurrently, in contrast to conventional centralized databases. This lowers the possibility of a single point of failure and does away with the requirement for a central authority.

Digital data is first replicated throughout the network of nodes in the process. Every node processes new update transactions on its own and keeps an exact duplicate of the ledger. Every participating node uses a consensus method to identify the accurate ledger version in order to guarantee consensus. The revised ledger is distributed to every node after a consensus is obtained, guaranteeing correctness and synchronization (Lemieux & Wang, Conclusion: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2), 2021).

DLT stores data securely via cryptography, and only authorized users are able to access it thanks to cryptographic signatures and keys. Additionally, the technology produces an immutable database, meaning that once data is saved, it cannot be removed and that any revisions are preserved indefinitely for future generations to see.

With this architecture, record-keeping is moved from a single authoritative site to a decentralized system where all relevant entities can read and edit the ledger, marking a substantial change in the way information is gathered and shared. All other entities may therefore observe who is utilizing and making changes to the ledger. Because of DLT's openness, participants have a high degree of trust in one another, and the possibility of fraud in the ledger is all but eliminated. Consequently, DLT eliminates the necessity for the ledger's users to depend on a dependable central authority or an external, third-party supplier to fulfill that function and serve as a safeguard against tampering (Farahani, Firouzi, & Luecking, 2021) .

The full potential of blockchain technology in the digital transformation of the public sector necessitates a framework for technology design and implementation that starts with areas where social trust needs to be improved. In order to support the goal of trust, officials should think about what data must be collected and stored in the blockchain (as well as what should not be collected and stored there). This should be followed by thinking about the blockchain protocols, architectures, and other technical factors that provide the required capabilities.


Social Layer
Legal Institutions & rules and Regulation
Business Procedures
Social trust relations & infrastructure
Cryptocurrencyvaluation, Markets & financing
Cross-domains & sectors
Data Layer
Ledger trustworthiness
Privacy &Data Protection
Data Architecture
Data &Records Lifecycle Management
Technical Layer
Blockchain Application and platform
Scalability issues
Layer1& 2, exchanges and app security
Standards and Evaluation Frameworks

Three Layer trust model of DLT **(Lemieux & Wang, Conclusion: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2), 2021)**

A new "Three Layer" design and implementation paradigm is needed for this approach. It consists of three layers:

- The Data layer is the ledger itself as a "immutable" store of transactional data/records, including considerations of data usability, privacy, and security, authenticity, reliability, integrity, etc.;
- The Technical layer is the technology stack, which includes distributed ledger protocols, consensus mechanisms, architectures, peer-to-peer networks, data storage, etc.;
- The Social layer is made up of human actors and social aspects like user incentives and motivations, culture, levels of digital literacy, access to technology, etc.; By employing this tactic, adoption of blockchain technology and distributed ledger technology in government digital transformation is facilitated.

3. Feature of Blockchain and Cybersecurity on E-commerce platform:

With the use of technology, government agencies can handle and secure massive volumes of data more effectively and safely. Improved data management is guaranteed, and private data is protected from theft and fraud. Digital currency applications for countries are another possible use case for blockchain technology. Blockchain and cybersecurity complement each other since blockchain uses cryptographic techniques to ensure data integrity while enhancing cybersecurity.

Block-by-block data connections provide an immutable ledger that is resistant to manipulation.

Even Blockchain can take the place of cyber security because of the decentralized strategy; there is less chance of censorship, manipulation, or unauthorized changes to domain data because no one entity can control the entire system.

The use of Domain Name Systems (DNS) is made safer and less susceptible to cyber attacks by blockchain technology. Blockchain applied to improve cybersecurity in IoT, data storage and sharing, network security, private user data, navigation and utility of World Wide Web (Wertz, 2019).

The purpose of cybersecurity measures is to shield data from unwanted access. Blockchain, on the other hand, aims to offer immutability and transparency. Data is transparent and impervious to tampering once it is added to the blockchain and cannot be removed.

3.1 Improvement of Public Trust using Blockchain:

The Blockchain solution's biggest effects on e-commerce are in the areas of public loyalty and trust. The majority of previous research on trust-related issues concentrated on blockchain technology's capacity to impose rules and regulations without requiring arbitrary authority (Ramachandiran R., 2018). By integrating a blockchain network into the business's database system, the suggested method can guarantee customers of e-commerce platforms' trust. Data transparency is facilitated by the company's integration of blockchain technology with its database system, which allows all stakeholders—including suppliers, clients, and e-commerce platform providers—to examine their own information. Ultimately, it improves consumers' privacy and confidentiality on e-commerce platforms, which in turn surely boosts their loyalty and faith in the company that created it (Alam Khan, Asif, Ahmad, & Alharbi, 2020).

3.2 Increase Data Security through Blockchain Technology

According to a different study led by Alex R. Mathew, traditional data management systems' security is susceptible to cyberattacks. The study addresses concerns such as the use of a single, independent security system that is vulnerable to attacks like DDoS (Distributed Denial of Service), in which hackers target a single security system, throw it out of commission, and then go on to collect important personal data. This study also discusses the centralized nature of currently used data management systems (Mathew, 2019). The analysis comes to the conclusion that the single point of failure or compromise in the present data management system is its greatest weakness and suggests using blockchain because of its robust architecture. Only two parties are able to read and alter the shared data blocks since each block is hashed before being connected to the next node, making it impossible for third parties to access the data and rendering it useless in the event of a leak. According to (Mathew, 2019), security researchers found that Blockchain technology may be able to overcome security gaps that exist now but are not covered by the security mechanisms in place.

Michelle Drolet also concluded in its research that there are many reasons behind the increase in data security using blockchain that is because of its decentralized, encryption and validation process and virtual impossibility to hack (Drolet, 2018).

4. Why blockchain needed for Cybersecurity?

Data breaches are becoming increasingly important for people and organizations trying to protect their security and privacy as cyberattacks are becoming more and more common. According to the research, the number of data breaches had risen at an unanticipated rate. In 2016, there were 36.6 million data breaches; by 2017, that number had risen to 197.6 million, setting a new high record with 446.5 million data exposure issues the following year (Xuan, Alrashdan, & Al-Maatouk, 2020). Due to their vulnerability to ransomware attacks, small businesses are also affected by data breaches at the same time as larger corporations. Using the stolen data, the attackers threatened and demanded ransom from the companies. For instance, in 2016 Uber settled the data breach issue by paying the hacker $100,000 to remove the stolen data (Gimenez-Aguilar, De Fuentes, Gonzalez-Manzano, & Arroyo, 2021).

Customer loyalty and public trust will be jeopardized by company data breaches since consumers value their data privacy, particularly when it comes to transaction history and personal Blockchain Technology in E-commerce Platform information. In March 2018, there was an unauthorized database access to Under Armour's online shop system, resulting in the breach of over 150 million customers' encrypted passwords, emails, and usernames (Dennis & Disso, 2019).

With 200 million users globally, the online video game Fortnite also suffered from an assault that revealed user information and allowed hackers to listen in on player conversations (Alon Boxiner, 2019). According to the news, cyberattacks are becoming more frequent on internet platforms, and in order to prevent businesses from losing out, they must be controlled and monitored. Businesses that rely on e-commerce should use blockchain technology to secure their extremely sensitive data and effectively lower the risk of data breaches (Shaverdian, 2019).

There are few chart diagram showing data breaches on different E-commerce platform.

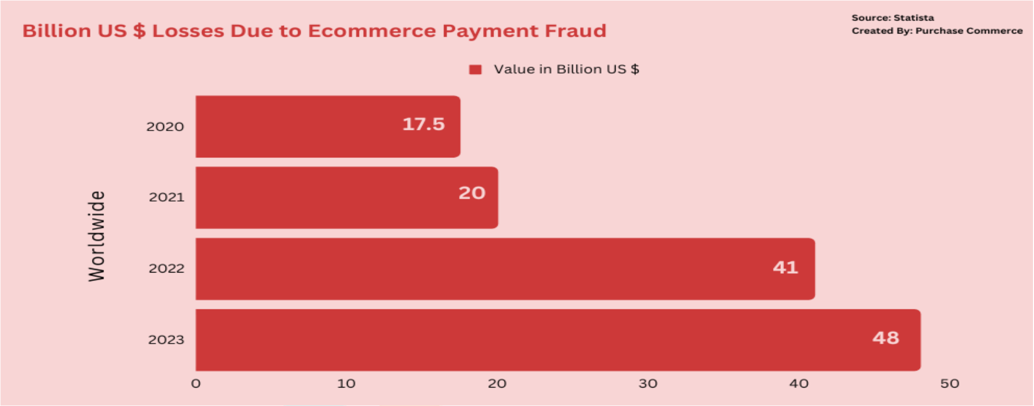


Figure 1. This graph, from Statista, shows the Billion US$ losses due to E-commerce payment fraud, from 2020 to 2023 (The data is worldwide – the figures in million US dollars) .

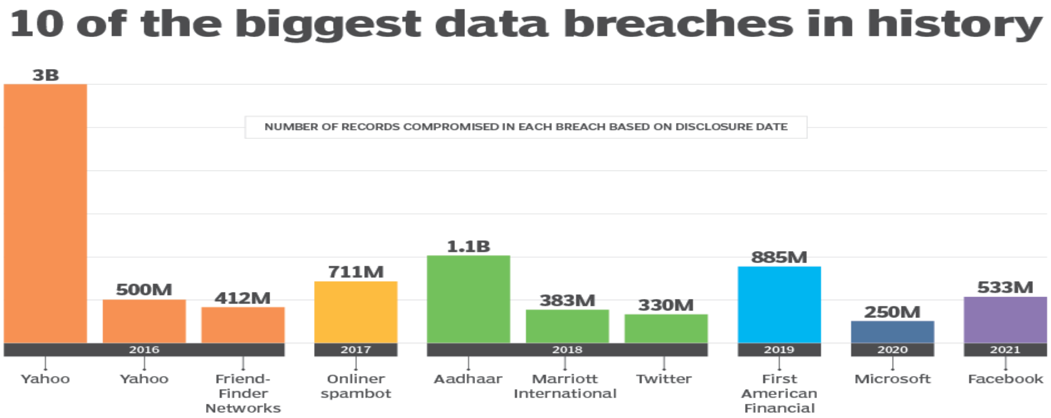


Figure 2. This graph indicate Data Breaches from 2016-2021 (Tech Target Security)

5. Key features of Blockchain Technology impacting Cybersecurity

In light of the difficulties and vulnerabilities presented by the decentralized nature of blockchain, these techniques include defending against ransom ware attacks and other malicious actions in addition to preventing unauthorized access and data alteration (Maleh, Shojafar, Alazab, & Romdhani, 2020).

5.1 Decentralized

Decentralized is a key idea in blockchain technology that affects cybersecurity profoundly. In contrast to conventional systems, which depend on a central authority for data management and control, blockchain functions through a decentralized architecture. Multiple network nodes or computers store and verify data in a decentralized blockchain network. Because blockchain is dispersed, there isn't a single point of failure, which protects it against cyberattacks. Because the data is saved and verified by other nodes in the network, it is secure even in the event that one node is compromised.

There are several advantages to blockchain's decentralized architecture in terms of cybersecurity. First off, by doing away with the requirement for a central authority—which is susceptible to cyberattacks—security is increased. Second, since each financial transaction is verified by consensus among the involved nodes, it guards against illegal access and data manipulation. Blockchain technology ensures the security and integrity of digital assets and transactions by preventing unauthorized alteration of data recorded on the blockchain. It is a useful cybersecurity solution in a variety of industries due to its decentralized structure and reliance on a network of nodes.

5.2 Collaborative Agreement

A key idea in blockchain technology is the collaborative consensus process, which guarantees agreement among users in a decentralized network. In order to achieve this cooperative agreement, consensus protocols are essential since they offer a means of transaction validation and verification. Blockchain networks can come to an agreement on the legitimacy and sequence of transactions without depending on a central authority thanks to consensus mechanisms. The blockchain ledger's correctness and integrity are guaranteed via collaborative consensus, which involves numerous nodes or participants in the validation process (Farahani, Firouzi, & Luecking, 2021).

5.3 Strong Encryption Practices

Blockchain networks can offer strong defense against cyberattacks and illegal access by implementing cutting-edge encryption methods. Public key cryptography is a crucial encryption method used in blockchain networks. Each user or participant in this approach needs a set of unique keys, a public key and a private key. While the private key is kept private and is used for decryption, the public key is shared freely and is utilized for encryption. Blockchain networks are capable of validating configuration changes, authenticating devices, and securing communication channels through the use of public key cryptography. A transaction that a user starts is signed using their private key, which functions as a digital signature or authenticity check. Using the user's public key, other network users can then confirm the transaction.

5.4 Immutable Records

A fundamental component of blockchain technology is immutable records. By guaranteeing that data cannot be changed or tampered with once it is posted to the blockchain, they significantly increase data security. The utilization of cryptographic hashing methods makes this possible (An introduction to blockchain in ecommerce, 2019). A transaction or piece of data is hashed and merged with other transactions when it is added to a blockchain. As a result, a distinctive string of characters is produced, serving as a digital fingerprint for that particular data block. The word "blockchain" refers to the sequence of connected blocks that this fingerprint is subsequently stored in.

5.5 IoT Protection

I.T. In the context of blockchain technology, protection is essential to improving cybersecurity. The likelihood of cyberattacks and security lapses increases with the proliferation of Internet of Things (IoT) devices. These gadgets, which include industrial gear and smart home appliances, have few security safeguards, making them easy targets for hackers. Blockchain technology can offer improved security features to shield Internet of Things devices from these kinds of online attacks. IoT devices may efficiently verify and encrypt data communications, guaranteeing the integrity and secrecy of the information shared, by utilizing the decentralized nature of blockchain technology. In blockchain-based solutions, the use of digital signatures and access management rules offers an additional layer of security against manipulation or unauthorized access (Lemieux

& Wang, Conclusion: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2), 2021).

5.6 Preventing DDoS Attacks

DDoS assaults overload a target system or network with traffic, making it unusable for authorized users. Due to their one focus point, traditional centralized systems are susceptible to these kinds of attacks. However, a domain name system (DNS) that is based on blockchain technology has the ability to significantly increase security and lessen these kinds of attacks. In a distributed ledger, the domain registration data is kept in a blockchain-based DNS. By doing this, the DDoS attack's singular target is eliminated. The distributed architecture of blockchain networks distributes the load among several nodes. Because of this, it is more difficult for attackers to take down one node and cause systemic disruptions (Kemmerer, 2003).

5.7 Data Privacy

When it comes to blockchain technology, data privacy is crucial. While there are many advantages to blockchain, such as immutability and transparency, there are also worries about private and sensitive data being exposed. Organizations can use permissioned blockchain networks, which restrict access to vetted members, to allay these worries. An organization's permissioned network allows them to manage who has access to the blockchain. This guarantees that viewers or participants in transactions can only be authorized people or entities. By providing rights based on criteria like identity verification or particular roles within the network, privacy of sensitive data is preserved (Drolet, 2018).

5.8 Smart Contract Security

In the blockchain ecosystem, smart contract security is crucial because it guards against potential risks and weaknesses that bad actors could take advantage of. The main goals of smart contract security are to locate and eliminate any threats, weaknesses, and flaws in smart contracts. Finding flaws in the code requires careful testing, auditing, and code review. Furthermore, standard libraries, access control mechanisms, and input validation are examples of best practices that can be used to strengthen the security of smart contracts (Demirkan, Demirkan, & McKee, 2020).

6. Blockchain Has the Potential to Change Cybersecurity:

Blockchain strengthens authentication through the use of collaborative consensus techniques and a distributed ledger. This network eliminates the requirement for a central authentication authority by having various participants validate and verify transactions. By lowering the possibility of identity theft and impersonation, this improves the security of authentication procedures.

Blockchain also has the ability to strengthen data encryption, increase privacy, and enable safe threat intelligence exchange between enterprises. It changes data integrity, transparency, and trust. Sensitive information is protected by immutability, which makes vital data verifiable and impervious to manipulation. Decentralization spreads information and control, lowering risks and boosting resilience **(how blockchain could revolutionize cybersecurity)**.

Additionally, it enhances identity management, granting users greater autonomy and lowering reliance on centralized service providers. By automating security procedures, smart contracts lower error rates and guarantee constant protocol adherence.

Real-time monitoring is made possible by blockchain's transparency, which also promotes accountability for unauthorized modifications and helps audits. An unchangeable record of transactions ensures the integrity of components and items, which is beneficial for supply chain security. But there are obstacles, like issues with scalability and interoperability **(forbestechcounci, 2022)**.

Not with standing these obstacles, blockchain's capacity to resolve problems and offer unmatched security improvements underscores its potential to completely transform cybersecurity procedures and norms inside enterprises.

7. Blockchain Cybersecurity Challenges and Drawbacks

To properly use blockchain technology and maintain strong security standards, individuals and organizations must be aware of these issues (Zheng, Xie, Dai, Chen, & Wang, 2018).

7.1 Scalability Issues

One significant disadvantage of blockchain technology for cybersecurity is its scalability. More processing power is required to maintain and validate transactions as the network grows. This makes it inappropriate for high-volume or real-time applications due to decreased throughput and greater latency. Resolving the scalability issue is essential to blockchain's broad adoption in cybersecurity (Dennis & Disso, 2019).

7.2 Privacy Concerns

It is a common misconception that blockchain technology is completely anonymous, however it is not. Pseudonymous transactions are linked to particular addresses rather than individual identities. Nonetheless, there are instances in which transactions can be linked to specific people. Privacy concerns may arise from this, especially if private or sensitive information is involved. One difficulty that must be addressed in the context of blockchain cybersecurity is striking a balance between the requirements of privacy and transparency (blockchain the weapon for cybersecurity)**.**

7.3 Regulatory and Legal Frameworks

Due to the constantly changing regulatory environment surrounding blockchain technology, there may be difficulties and uncertainties with regard to legal frameworks and compliance. For blockchain technologies to satisfy the needs of diverse industries and countries, certain rules and laws are required. Lack of these standards can lead to ambiguity and prevent blockchain from being widely used in cybersecurity procedures (Maleh, Shojafar, Alazab, & Romdhani, 2020).

7.4 Smart Contract Vulnerabilities

Self-executing contracts on the blockchain called "smart contracts" can pose particular cybersecurity difficulties. They can facilitate automated and efficient transactions, but they are also vulnerable to code attacks and vulnerabilities. Smart contracts may contain bugs or vulnerabilities that can be used to gain unauthorized access or cause financial losses. Effective risk mitigation requires strong security mechanisms and code audits (Lemieux & Bravo, Introduction: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part I), 2021).

7.5 Energy Use

Blockchain networks need a lot of energy and processing power to mine and validate transactions, especially public proof-of-work networks like Bitcoin. Concerns over blockchain technology's environmental impact have been brought up by its energy footprint. To overcome these issues, finding energy-efficient alternatives to consensus algorithms or sustainable solutions is crucial.

8. How will Blockchain affect Cybersecurity in the Future?

Blockchain technology is predicted to have a big impact on cybersecurity in the future. The immutability and decentralization of blockchain technology can strengthen security protocols and offer strong defense against online attacks.

Blockchain improves system resilience by removing the requirement for a central authority and decentralizing control, which lowers the possibility of single points of failure. Bad actors find it challenging to alter or tamper with data stored on a blockchain network due to its decentralized structure. Furthermore, the immutability of blockchain guarantees that information recorded on the network cannot be removed or changed, making it a reliable and impenetrable source of data. There is a great deal of room for growth and progress in blockchain cybersecurity in the future. Blockchain technology will surely become increasingly important in improving cybersecurity procedures as it develops (Demirkan, Demirkan, & McKee, 2020).

Access management is a key area where blockchain technology may be further linked with cybersecurity. Because of its decentralized structure and capacity to function as a digital ledger, blockchain offers safe, impenetrable access control methods that lower the possibility of illegal access to private information. Furthermore, transactions can be made private and securely using blockchain-based technologies, doing away with the need for middlemen and centralized authority.

The capacity of blockchain technology to produce immutable and auditable records of cyberthreats and attacks is another important advantage for cybersecurity.

9. Conclusion

The examination carried out on the cybersecurity dimensions of blockchain technology has yielded encouraging results and perspectives. Because blockchain is decentralized, there is less chance of a single point of failure and more system resilience, which makes it harder for malicious actors to alter or tamper with data. Blockchain's immutability guarantees the accuracy of data stored, making it a reliable and impenetrable source of information.

One important aspect of blockchain technology is smart contracts, which improve security by automatically enforcing certain rules and circumstances. This lowers the possibility of fraud and illegal access. The report also emphasized how blockchain technology may be used to counteract changing cyberattacks. Security experts can examine attack pathways and create preventive security measures thanks to its public and auditable record of malicious activity.

The investigation found well-known authors, citation networks, and publishers in the subject of blockchain development. It also emphasized the nations that are actively working to promote blockchain technology. In addition, the distribution of vulnerabilities and the corresponding scores obtained from the Common Vulnerability Scoring System (CVSS) were analyzed, offering important insights into the regions that need attention and mitigation activities. These results contribute to our understanding of blockchain technology's impact on cybersecurity and its potential as a useful remedy.

10. **Bibliography**

Alam Khan, F., Asif, M., Ahmad, A., & Alharbi, M. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society* , 55.

An introduction to blockchain in ecommerce. (2019). Retrieved february 5, 2020, from Inviqa: https://inviqa.com/blog/introduction-blockchain-ecommerce.

Apau, R., Korenteng, F., & Gyamfi, S. (2019). Cyber-Crime and its Effects on E-Commerce. *Journal of Information* , 39-59.

blockchain the weapon for cybersecurity. (n.d.). Retrieved from www.encora.com: https://www.encora.com/insights/blockchain-the-weapon-for-cybersecurity

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting . *Journal of Management Analytics , 2* (7), 189-208.

Dennis, R., & Disso, J. P. (2019). An analysis into the scalability of bitcoin and ethereum. *Third International Congress on Information and Communication Technology: ICICT 2018* ., (pp. 619-627). LONDON.

Drolet, M. (2018, June 05). *4-reasons-blockchain-could-improve-data-security*. Retrieved from www.csoonline.com: https://www.csoonline.com/article/565578/4-reasons-blockchain-could-improve-data-security.html

forbestechcounci. (2022, 03 04). Retrieved from www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/?sh=5150a2643a41

Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems* , 91-118.

how blockchain could revolutionize cybersecurity. (n.d.). Retrieved from www.smartdatainc.co: https://www.smartdatainc.com/blogs/how-blockchain-could-revolutionize-cybersecurity/

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences , 80* (5), 973-993.

Kaspersky. (n.d.). Retrieved from Resourse-center: https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

Kemmerer, R. A. (2003). Cybersecurity. *International Conference on Software Engineering, IEEE Proceeding* , 705-715.

Lemieux, V. L., & Bravo, M. (2021). Introduction: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part I). *Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers* , 1-20.

Lemieux, V. L., & Wang, C. (2021). Conclusion: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2). *Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers* , 129-163.

Maleh, y., Shojafar, M., Alazab, M., & Romdhani, I. (2020). Blockchain for cybersecurity and privacy: architectures, challenges, and applications. In y. Maleh, M. Shojafar, M. Alazab, & I. Romdhani, *Blockchain for cybersecurity and privacy: architectures, challenges, and applications.*

Mathew, A. R. (2019). Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology (IJEAT) , 9* (1).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* .

Shaping the Future of Technology Governance: Blockchain and Distributed Ledger Technologies. (2020). Retrieved February 5, 2020, from World Economic Forum: https://www.weforum.org/platforms/shaping-the-futureof-technology-governance-blockchain-and-distributed-ledger-technologies.

Shaverdian, P. (2019). Start with trust: utilizing blockchain to resolve the third-party data breach problem . *66 UCLA L. Rev.* , 1242.

Tech Target Security. (n.d.). Retrieved from www.techtarget.com: https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them

Xuan, T. M., Alrashdan, M. T., & Al-Maatouk, Q. (2020). Blockchain technology in E-commerce platform . *International Journal of Management* , 1688-1697.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services , 14*, 352-375.