Page 1128 - 1136 **DOI:** *https://doij.org/10.10000/IJLMH.119799*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Role of Blockchain Technology in Enhancing Cybersecurity

SALONI YADAV[1]

ABSTRACT

In today's digital world, where technology has become an integral part of our daily lives, Cybercrime and Cybersecurity attacks are hardly seen to be out of news, everyday there are hundreds and thousands of cases which are registered, this threat is not only limited to India but growing globally, With the rapid adoption of digital payment systems, the growth of e-commerce, and the increasing penetration of online services, people and businesses are becoming more exposed to cyberthreats. Although Advancement in digital technology have increased productivity, but they have also created new opportunities for hackers to take advantage of. Traditionally, security in cyberspace has been designed using systems with a central structure and control, however these systems are vulnerable to hacking. Centralized databases are vulnerable to single points of failure and can be exploited by malicious actors targeting to leverage vulnerabilities, thus creating the essential need for advanced cybersecurity safeguards, in this context blockchain technology has emerged as a solution to enhance cybersecurity. Blockchain provides an alternative, less-travelled route to increased security that is far less welcoming to attackers. Blockchain technology has the ability to transform cybersecurity especially in areas that deal with sensitive information because of its decentralized, transparent, and immutable nature. This study aims to explore the potential benefits of blockchain technology for enhancing cybersecurity. The goal of this study is to provide a comprehensive understanding of how blockchain technology may enhance cybersecurity and lessen cyberthreats.

Keywords: *Blockchain Technology, Cybersecurity, Decentralized, Immutability, transparency.*

I. INTRODUCTION

Cybersecurity is basically securing your data in the virtual world, in virtual world we do lot of transactions and information exchange, always there is an element of risk where the external element can enter into your channel and tamper your data. Centralized systems have been common targets for cyberattacks thus there arises a need for more advanced system to deal with it and it is when blockchain technology came into play, Blockchain technology is seen as

[1] Author is a Student at School of Legal Studies, Babu Banarasi Das University, Lucknow, India.

 [ISSN 2581-5369]

an ultimate gamechanger in the world of cybersecurity. Blockchain technology is not a replacement for AI, ML & DL techniques as AI, ML& DL is the Ist line of defence for our cybersecurity, the main aim is to protect our data from cyberattacks but in case even after that they manage to get in, thus we need to initiate second line of defence i.e. Blockchain technology. Blockchain technology is the technology on which bitcoin is based basically a technique to store information through decentralised manner, it has emerged as a promising solution to address the growing concerns of cybersecurity. It plays a crucial role in the digital world of security with its decentralised and tamper proof structure. The principal advantage of blockchain is its use of a distributed ledger. Every transaction here is locked, encrypted and verified by a network of systems thus creating a strong defence for digital data ensuring data integrity.

II. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain can be loosely translated as several cryptographically chained blocks.[2] Blockchain is a particular type or subset of so-called distributed ledger technology ("DLT"). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. Blockchain is a mechanism that employs an encryption method known as cryptography and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure to which data can only be added and from which existing data cannot be removed that takes the form of a chain of "transaction blocks" , which functions as a distributed ledger.[3] In a blockchain, the data is structured in the form of blocks, a block is just a digital storage unit that holds the data each block is made up of three main things-

- First the data or information stored in the block
- Second each block has its fingerprint known as hash, block is linked and secured by hashes using cryptography based on available hashing algorithms, every created block will have a unique hash id although cryptography has its drawback but hashing algorithms proves to offer highest degree of security against hacking.[4]
- Third each of these block stores the fingerprint of the block before it

[2] Alex. R. Mathew, *Cyber Security through Blockchain Technology*, 9 IJEAT 3821, 3821- 3824 (2019).
[3] World Bank Group (H. Natarajan et al.), *Distributed Ledger Technology (DLT) and Blockchain*, FinTech Note No. 1 (2017), https://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf .
[4] Joseph Meynard G. Ogdol et al., *Enhancing Cybersecurity Through Blockchain Technology*, 3 J-HERD 2 (2018).

Every user on a blockchain network has a set of two keys. A private key, which is used to create a digital signature for a transaction, and a public key, which is known to everyone on the network. A public key has two uses: 1) it serves as an address on the blockchain network and 2) it is used to verify a digital signature / validate the identity of the sender.[5]

The unique thing about this is that if anyone try to tamper with the data, then the hash of the block will change & if the hash of one block changes, the hash of next block will also change and then eventually the entire blockchain will be destroyed. For this reason, it is next to impossible to alter or tamper with the data in a blockchain because once a block is defined and becomes part of the blockchain it cannot be altered after that.

ROLE OF MINERS

The people who are connected to the blockchain through their computers are known as nodes. The operation of a blockchain network involves nodes collaborating to achieve consensus on the addition of new blocks. This consensus process ensures that the network agrees upon the validity of transactions.[6] New information may only be added if a majority of computers in the network approve it after acceptable evidence is supplied that the information, which is sent cryptographically, is accurate.[7]

III. KEY FEATURES OF BLOCKCHAIN TECHNOLOGY

DECENTRALIZED CONTROL: One of the unique characteristics of blockchain technology is its decentralized control,[8] because of its decentralized nature, it eliminates the need to trust in the third party and does not have a single point of failure. this feature of Blockchain technology makes it resilient against attacks since authenticity cannot be compromised by just one point of trust. By enabling direct communication between several participants, blockchain reduces weak points, removing opportunity for people to commit embezzlement and theft.

IMMUTABILITY: Blockchain's immutability is examined for its part in protecting data integrity, providing an unchanging historical record that acts as a barrier to data alteration and

[5] European Parliament, *Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion: Report on Cryptocurrencies and Blockchain* (July 5, 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

[6] Vinod Kumar Uppalapu & Dr. Ajay Agarwal, *Enhancing Cybersecurity through the Utilization of Blockchain Technology*, 13 IJRIM, 20, 19-25 (2023).

[7] Atharva Deshmukh et al., *Blockchain Enabled Cyber Security: A Comprehensive Survey*, in Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI) (Jan. 25-27, 2022, Coimbatore, India).

[8] Emanuel Ferreira Jesus et al., *A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack*, Security & Communication Networks, 2, 2-27(2018).

manipulations.[9] Once information is stored in blockchain than no compromise can be done with the data. Immutability is more than just a deterrent mechanism, it is also an active protector of information integrity highly valued by industries where data sacrosanct cannot be negotiated, like in critical infrastructure and financial systems.[10] If the information in any block changes, so will its hash. A spiral effect will result from this, where the hashes of the blocks that follow will become invalid. For this reason, blockchain transactions are unchangeable.

TRANSPARENCY: transparency of the blockchain's ledger led to greater trust among the users. All transactions are traceable by all network members and, after confirmation, cannot be changed anymore. This transparency is essential for developing trust in digitally mediated interactions, especially when strict audit trails are needed.[11]

AUTHENTICITY: Hashes are widely used as a mechanism to sign text files or data files to prevent tampering. To supply authenticity to each message, users are mandated to give a Private Key to be used by the Hashing Algorithm. The user's Private Key is a unique key that is only known by the user and is used to encode the message, it is found to be mathematically irreversible using the resulting hash message.[12] there is an order of dependency between blocks that can be used to ensure the integrity of the whole Blockchain.[13] Thus ensuring the integrity and origin of the message.

CONSENSUS PROCESS: Blockchain's collaborative consensus process eliminates yet another conventional flaw. Without a central authority, it can keep an eye out for anomalies, malicious activity, and false positives. It is possible to trick one eye, but not all of them.[14]

ENCRYPTED COMMUNICATION: Through encryption and digital signatures, a blockchain system can shield connected thermostats, smart doorbells, security cameras, and other vulnerable edge devices, making certain that information exchanged between them is private, impenetrable, and available to authorized users only.[15]

PUBLIC & PRIVATE KEY SECURITY: digital signature in blockchain enable data authenticity and verification, by signing data blocks with a private key, the blockchain ensures

[9] Huma Jamshed et al., *Survey on Vulnerabilities in Blockchain's Smart Contracts*, 20 JISR-C, 13, 10-14(2022).
[10] Onyekachi Kingsley Igbokwe, *Enhancing Cybersecurity Through Blockchain Technology: A Review* (Dec. 2023) DOI:10.13140/RG.2.2.36577.68969.
[11]N. Kolokotronis et al., *Secured by Blockchain: Safeguarding Internet of Things Devices*, 8 IEEE Consumer Electronics Mag. 3, 28 (2019).
[12] Ogdol, *supra* note 3.
[13] Mathew, *supra* note 1.
[14] Yogesh Shelke, *Rethinking Cybersecurity Through Blockchain*, Infosys, https://www.infosys.com/insights/cyber-security/cybersecurity-blockchain.html.
[15] *Id.* at 5.

that only authorized parties can create or modify data, while anyone with the public key can verify its authenticity.[16]

CHRONOLOGICAL RECORD: Every data entry or transaction is time-stamped and appended to a block, which is then confirmed and sealed via a consensus process. This greatly streamlines audit processes and increases trust in the system's dependability by providing auditors with an unquestionable record of all actions.[17]

IV. IMPLEMENTING BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY

Cybersecurity refers to the process of safeguarding computer systems and networks against malicious cyberattacks that seek to steal money or private information by gaining unauthorized access to, altering, or destroying digital data.[18] Cybersecurity is not merely a matter of protecting data; it's about preserving trust in our digital interactions.[19] This is where blockchain technology can be used as a solution as Blockchain Technology is protected with the help of ledgers with the cryptographic keys. It is managed by a network of nodes, or computers, as opposed to traditional databases, which are governed by a single authority. Since changing the blockchain would require the consent of the majority of network participants, its decentralized structure makes it extremely resistant to fraud and cyberattacks.[20] Thus attacking & manipulating data is going to be extremely difficult because if one wants to alter or do fraud in the blockchain it would need the majority of at least 51%, but realistically to hack 51%of the computers on the network is not that possible because all of them are decentralised and thus they will have to be hacked individually at their locations. The greater the number of nodes, the more difficult this is to do the bigger the blockchain, the more secure it is.

DATA INTEGRITY: one of the significant advantages of blockchain technology is its ability to ensure data integrity with the help of its core features such as decentralization, immutability and transparency, each block in a blockchain contains a cryptographic hash of the previous block, which, along with the data stored within the block, creates a chain of

[16] Danny Pehar, *How Blockchain Revolutionizes Data Integrity And Cybersecurity*, Forbes, (Jan 17, 2024) , https://www.forbes.com/councils/forbestechcouncil/2024/01/17/how-blockchain-revolutionizes-data-integrity-and-cybersecurity/.
[17] *Id* at 6.
[18] Mohan Vishal Gupta, *A Study on Cyber Security Using Blockchain Technology*, 11 IJFANS ,428 (2022).
[19] *Cybersecurity with Blockchain Solutions*, Blockchain Council (Jan. 16, 2025), https://www.blockchain-council.org/blockchain/blockchain-in-cybersecurity.
[20] *The Role of Blockchain in Preventing Identity Theft in Digital Transactions*, The Palos Publishing Co. (2025), https://palospublishing.com/the-role-of-blockchain-in-preventing-identity-theft-in-digital-transactions/.

secure, immutable records.[21]

FRAUD PREVENTION: The technology presents promising solutions for fraud prevention and identity theft. By embracing distributed data storage, blockchain safeguards against unauthorized access and modification of data.[22]

MINIMIZING DATA BREACH RISKS: In a traditional database system data is stored through centralized servers that can be easily targeted by the hackers but in a blockchain technology data is stored in a decentralised manner since no central authority controls the data manipulation with the data is difficult and data is distributed across a network of nodes, this ensures that breaches in a few computers do not compromise the rest of the network's data.[23]

DATA SAFETY: Blockchain technology ensures data security through an integrated system whereby it collects, arranges, stores, and disseminates information in different blocks thus ensuring data safety, once data has been added to the network, no one can alter the data set either by adding or deleting it [24]

IDENTITY VERIFICATION: Unlike traditional systems that rely on centralized databases, blockchain-based verification employs a distributed ledger where information is stored across multiple nodes, every piece of identity data is encrypted and linked using cryptographic methods, ensuring its immutability and transparency.[25]

These were some of the areas I talked about the scope of blockchain technology extends far beyond this, the features of blockchain technology makes it really helpful to prevent data manipulation, minimizing data breach risks and thus ensuring cybersecurity.

V. KEY AREAS WHERE BLOCKCHAIN TECHNOLOGY CAN BE A BIG ADVANTAGE

HEALTHCARE SECTOR: Due to increase in cyberthreats, the privacy and security of data is a big concern as healthcare data of any person is a very sensitive information that needs to be protected, Blockchain technology can be used in the healthcare industry to store data blocks that are not publicly accessible but that authorized personnel can access, recover, or verify. A timestamp and cryptographic signature can be used to authenticate the blocks,

[21] Abbas Aljuboori & Abbas Khudhair Abbas, *Blockchain Technology and Its Issues: Types, Applications, Challenges, and Future Directions*, 10 J INFORM SYSTEMS ENG, 103 (2025).
[22] Uppalapu, *supra* note 5.
[23]Uppalapu, *supra* note 5.
[24] Sriram V. P. et al., *Enhancing Cybersecurity Through Blockchain Technology*, in Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications 17 (2023).
[25] Arthur, *A Comprehensive Guide to Blockchain Identity Verification*, PreciseHire (Dec. 30, 2024), https://precisehire.com/guide-to-blockchain-identity-verification/.

guaranteeing their incorruptibility and source traceability.[26]

SMART CONTRACTS: Smart contracts are digital contracts that are executed by themselves when precise circumstances are met, Smart contracts in the contemporary blockchain automatically perform functions of all kinds, thus substituting intermediaries to facilitate trustless foreign remittance.[27] Blockchain components like smart contracts, applications, APIs, digital assets, and wallets must be tested for access control, authentication, data security, and business logic validation, as a result, individuals in the permissioned chains feel more confident.[28]

COMBATTING CORRUPTION: The following excerpt, from a report by the World economic Forum (2020, p.4), provides an example of how blockchain could address corruption problems:[29]

"[..] blockchain provides the unique combination of permanent and tamper-evident record-keeping, transaction transparency and auditability, automated functions with 'smart contracts', and the reduction of centralized authority and information ownership within processes. These properties make blockchain a high potential emerging technology to address corruption."

EDUCATION FIELD: Blockchain technology can be used efficiently in the education industry to manage results while assuring reliability and openness, thus preventing forgery as once the result is uploaded by the institution no changes can be made.

TAMPER PROOF ELECTIONS: In our country where election results are always questioned blockchain technology can be of great use ensuring the reliability of the results, Sierra Leone was the first time a country has used Blockchain technology in a national election, Agora has developed a voting system for Sierra Leone that dramatically reduces the chances of an election being rigged.[30]

VI. CHALLENGES ASSOCIATED WITH BLOCKCHAIN TECHNOLOGY

SCALABILITY: Scalability is one of the biggest challenges associated with blockchain as more transactions are conducted in the network, so does the size of the blockchain increase,

[26] Ajitesh Kumar et al., *A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security Against Cyberattacks in Healthcare*, **22** Sensors, 5921 (2022).
[27] Anwar Mohammed, *Blockchain and Cybersecurity: Applications Beyond Cryptocurrencies Enhancing Cybersecurity*, **3** JBDS, **1**(2022).
[28] Shelke, *supra* note 13.
[29] Silvia Semenzin et al., *Blockchain-Based Application at a Governmental Level: Disruption or Illusion? The Case of Estonia*, **00** Pol'y & Soc'y **0**, 1 (2022).
[30] African Enterprise, *Sierra Leone First in the World to Use Blockchain Technology in Election*, African Enterprise (2025), https://africanenterprise.ca/story/sierra-leone-first-world-use-blockchain-technology-election/.

thus resulting in potential performance problems and increased storage demand.[31]

HIGH ENERGY CONSUMPTION: high energy consumption of the blockchain proof of-work consensus systems is one of its major drawbacks Blockchains using Proof of Work (PoW) consensus mechanisms, like Bitcoin, have been dogged by charges of high power use. The PoW process requires miners to solve complex cryptographic puzzles in order to verify transactions, which consumes enormous computational power and therefore large amounts of energy.[32]

TRAINED EXPERTS: Blockchain-driven cybersecurity solutions require a workforce with the necessary skills. As blockchain technology is dealing with complex process that requires knowledge of its practicality and theory, we need trained workforce skilled in the field of blockchain.

INTEROPERABILITY: Integration of blockchain technology with existing cybersecurity systems can be complex, potentially causing compatibility issues, In a diverse cybersecurity landscape with various platforms and protocols, ensuring seamless communication and data exchange between different blockchain implementations becomes crucial.[33]

VII. RECOMMENDATIONS

EDUCATION & TRAINING PROGRAMS: Invest in training programs to bridge the skills gap in blockchain and cybersecurity. Offering educational initiatives for professionals and students can create a pool of talent proficient in both domains, fostering successful blockchain adoption.[34]

INVESTMENT IN RESEARCH AND DEVELOPMENT: Blockchain technology in the field of cybersecurity is a new concept, investment in Research and development can be helpful in better implementation of technology to prevent cybercrimes research must be focused to overcome challenges such as scalability and interoperability.

VIII. CONCLUSION

From above discussion one thing is clear that blockchain technology is not a buzzword it can be used against the cybercriminals effectively, its inherent characteristic of decentralization, immutability and transparency makes its different from traditional protection systems which are more vulnerable to cyber attackers, cybercrimes are increasing on a rapid rate with every

[31] Igbokwe, *supra* note 9.
[32] Aljuboori, *supra* note 20.
[33] Dr. K K Ramachandran, *Blockchain Technology for Enhancing Cybersecurity in India*, 2 IJBT ,9, 9-20 (2024).
[34] *Id.*

 [ISSN 2581-5369]

new day cyberfraudsters found new ways to commit crime thus to protect our data blockchain technology could be really helpful as of now this technology i.e. integration of blockchain with cybersecurity is in its early stages, developers need to design enhanced versions to handle operations more effectively, this technology can be a great help to most of the industries whether it's healthcare sector, government sector, businesses all will be benefited especially fields where data security is most important.

blockchain technology is not free from challenges such as scalability, high energy consumption and many more and to improve this we need more systematic research in this field collaboration of private and government institutions together can provide best results as we move forward in an increasingly complex and digital landscape, the unique features of this technology can work as a powerful toolkit for building more secure digital environment.

The question is no longer that *"Can blockchain help in cybersecurity, but it is that how we can use it at its best to achieve the greater potential that this technology can provide."*

*****

 [ISSN 2581-5369]