IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, September 2026
Impact Factor: 8.2

Exploring Blockchain as a Cybersecurity Tool: Essential Concepts, Potential Use Cases, and Obstacles

Babali Rai[1] and Minal Mandwe[2]
Department of Computer Science,
Tilak Maharashtra Vidyapeeth, Kharghar
[1]rai.babali@gmail.com

Abstract : *The exponential growth of digital information in the modern age presents a formidable challenge for organizations and institutions. As cyber threats targeting individuals, businesses, and governments continue to escalate, the security and accessibility of critical data are increasingly vulnerable. Blockchain, an innovative technology rooted in cryptography and decentralized systems, offers a potential remedy for these security concerns. As a potential solution to security issues, Blockchain technology, which is grounded in cryptography and distributed systems, presents a promising approach. By utilizing encryption methods and digital signature techniques, a Blockchain-based infrastructure can provide protection for various Internet of Things devices that are susceptible to attacks, including networked temperature controllers, intelligent doorbell systems, surveillance equipment, and other exposed peripheral units. This paper examines the various ways in which Blockchain technology can mitigate cyber threats and enhance data protection. While traditionally associated with cryptocurrencies such as Bitcoin, the discussion will also explore broader Blockchain applications, address potential obstacles, and consider future prospects in this field.*

Key Words: Bitcion, Blochchain, Cruptography, Distributed Ledger Technology (DLT), digital signature techniques,IoTA, Ethereum

1. INTRODUCTION

Blockchain:

The term "Blockchain" is derived from the combination of two words, "block" and "chain," which refers to a technology that stores data in blocks and interlinks them in a chain to enable transparent information sharing across a network for ensuring consistency (Amazon.com). A block represents a record or unit of data, which may contain various data types of information such as quantity, price, address, and so on. As the asset is transferred from one owner to another, these blocks are linked together to form a chain. This chain comprises the specifics of each transaction, including the time and order in which they occurred.It makes use of Distributed Ledger Technology (DLT) to save records in a ledger format, where each member of the network has a copy of the record and all completed transactions are shared among all parties (. By utilizing DLT, Barclays (London, England) uses Blockchain technology to improve security during fund transfers.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, September 2026
Impact Factor: 8.2

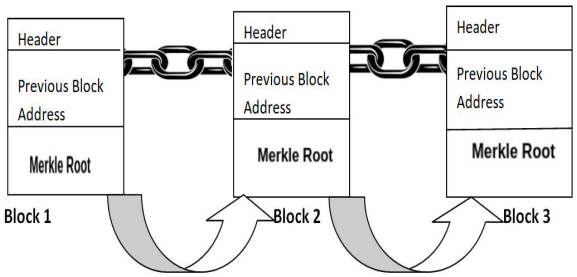


Fig: BlockChain Common Structure

Blockchain technology is commonly used in the cryptocurrency system to provide secure and decentralized transactions. It ensures that data is immutable, which means that transactions are permanently stored and accessible to everyone on the network(Alex. R. Mathew,2019).

Due to the lack of a single point of failure, a single user cannot alter any transaction record in blockchain technology. Who has access to the data depends on the participants. Blockchain networks are usually classified into two categories, Public and Private, based on accessibility(ibm.com). These categories specify who is permitted to participate, how they can obtain access to the network, and other details. Public blockchains allow for the use of internet-connected computers to validate transactions, while private blockchains are restricted and use identity to grant access to selected members. Bitcoin is a well-known example of a public blockchain technology, while private blockchains are typically created and managed by organizations for their exclusive use. These networks employ a process called "selective endorsement" to grant permission to join the network.

Every member of the public blockchain can freely view every individual's data in transactions, which raises security issues and makes it necessary for businesses to carefully monitor what information is made publicly available. Businesses are implementing cybersecurity based on blockchain.Blockchain technology and cybersecurity combined can solve a lot of public network security issues.This helps in tracking assets within business networks. Contrary to traditional database systems, blockchain technology overcomes several challenges, and its adoption is increasing in various industries.Cybersecurity: In today's digital age, safeguarding sensitive data has become a daunting task for organizations, as they frequently transfer information online through various devices and internet connections (Role of Blockchain in Cybersecurity, geeksforgeeks). With the growing reliance on technology, cybersecurity has emerged as the most effective solution to defend against cyber threats and malicious software that could compromise valuable digital assets.

II. BLOCKCHAIN IN CYBERSECURITY AS A NEW WEAPON:

In today's digital era, the increasing volume of digital data poses a significant challenge to businesses and institutions. With the growing risk of cyber threats, the confidentiality and availability of sensitive data are at stake. In light of these risks, protecting sensitive data has become a top priority for organizations. To address this challenge, blockchain and cybersecurity solutions work together to secure our digital world from external threats.To reduce the possibility of data manipulation, the blockchain stores data in the form of a decentralized digital ledger. This is accomplished by using cryptography techniques to encrypt the data. Conversely, cybersecurity refers to a framework intended to defend information, data, networks, and devices against outside threats. In the realm of cybersecurity, Blockchain functions as a triad model that guarantees security by upholding the principles of Confidentiality, Integrity, and Availability.

Blockchain employs the hash encryption technique to ensure the confidentiality of data stored in the ledger. This method makes it difficult for unauthorized individuals to access the information. To further enhance security, Blockchain utilizes various algorithms and IETF/RFC key process management system, which prevent external access to the data. By doing so, Blockchain ensures that only authorized individuals can access the data within the network.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, September 2026
Impact Factor: 8.2

Blockchain operates on a distributed ledger technology (DLT) system, which is a decentralized data management network where every member can transparently access and view records and transactions. This ensures a high level of data integrity and fosters trust among all stakeholders.

Data availability is the final pillar of Blockchain technology. This means that data must be accessible at all times when needed, which enables organizations to function seamlessly and eliminates downtime. This can be achieved through Blockchain technology as data is stored in a distributed ledger format rather than a centralized one.

Blockchain & Cryptography:

Cryptography is an essential component of the Blockchain that safeguards the integrity of data by ensuring its security. It is a critical technology for securing data and ensuring data integrity, confidentiality, and availability for secure communication. By converting plain text into cipher text using various algorithms, cryptography plays a vital role in protecting data and maintaining the confidentiality of information (Cryptography and its Types,geeksforgeeks, Feb, 2025). The use of cryptography is crucial for maintaining the security and integrity of data in the digital age.Blockchain utilizes two methods to safeguard data: cryptography and hashing. Cryptography is employed for the encryption and decryption of text or data. It comes in two forms: symmetric and asymmetric. Cryptography is of utmost importance for public blockchain networks as data is accessible to all members, thus necessitating secure measures.Hashing, on the other hand, is a process that converts data or information into an unreadable, unalterable text. This method is also important for securing data in blockchain systems. While the techniques may differ, their goal is the same: to ensure the security and integrity of data in blockchain networks.

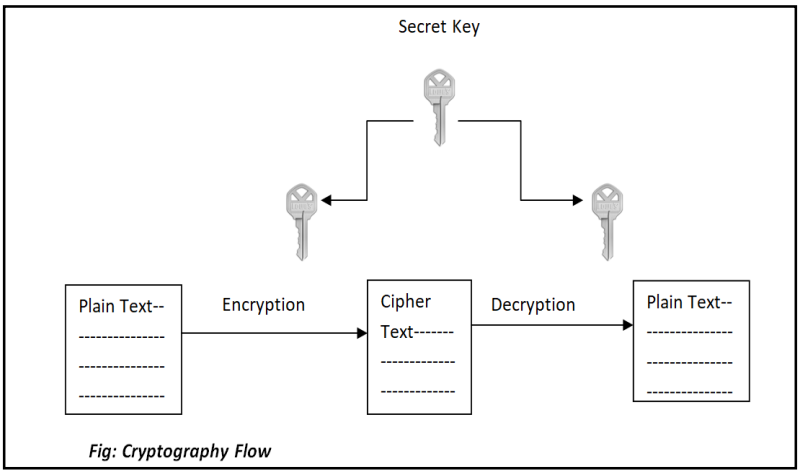


Fig: Cryptography Flow

Blockchain and Cryptocurrency: Cryptocurrency is a digital currency that functions as a medium of exchange. It employs a digital ledger to facilitate transactions involving money, properties, or intellectual assets among authorized users.it does not rely on banks for verification of any transaction ,it is peer-to-peer system to send or receive payments instead of being physical money around the entire world. Unlike other currencies there is no need to convert money from one currency to other for international fund transfer.

Cryptocurrency is a type of digital currency that serves as a medium of exchange (Jaya Vaidhyanathan, Aashika Jain ,2023). It employs a digital ledger to conduct transactions involving money, properties, or intellectual assets between authorized users. The main advantage of cryptocurrency is that it eliminates the need for banks to verify transactions, as it operates on a peer-to-peer system for sending and receiving payments ,it is not controlled by any government. Additionally, cryptocurrency is not limited by physical borders, making it a convenient option for international fund transfers without the need for currency conversion.One of the most widely used and popular cryptocurrencies, such as Bitcoin and Ethereum, employ Blockchain technology for secure, transparent transactions, as well as for the easy identification of crypto buyers and sellers in the cryptocurrency market.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, September 2026 Impact Factor: 8.2

Applications of Blockchain Technology and Practical Uses (Security concerns) Over the past few years, our world has witnessed the rapid emergence of new technologies that have transformed our lives. Today, it is nearly impossible for us to imagine a world without the likes of Google and other social media apps(Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). The invention of Blockchain has been a game-changer, booming the world with its remarkable features such as decentralization, automation, transparency, and immutability.There are a wide range of industries in which these components can be used, leading to numerous use cases. These are, in our opinion, the most relevant blockchain use cases for businesses, organizations, and governmental bodies.

1. Upholding loyalty and copyright in the film industry:

The use of blockchain technology in the film and entertainment industries can offer secure and transparent transactions to ensure fair and justifiable royalties and credits to every artist. Blockchain platforms can be utilized to program and automate the payment of contracts on time and in the correct amount (consensys). For online and international payments, various cryptocurrencies like Bitcoin can be employed. The elimination of third-party intermediaries allows creators and artists to sell their products directly in a blockchain-based digital marketplace.

2. Securing IoT with blockchain: IOTA(Internet of Things Applications)

The Internet of Things (IoT) is a cutting-edge technology that allows for the integration of devices such as Smart Homes, Hospitals, Banks, smart cars ,smart farming and Education systems with 5G networks. This connection provides a secure and swift means of transmitting and receiving data, resulting in the creation of tamper-resistant records for shared information and transactions (Tanweer Alam,2019).

IoT devices seamlessly connect people, places, and things, offering ample opportunities for value creation and fostering innovative and rapid growth towards success. These devices are equipped with various chips and sensors to transfer data over networks and transform valuable information into action, ultimately influencing business processes to pave the way for new ways of working and untapped opportunities in today's competitive marketplace.

At the outset, IoT systems faced sluggish performance due to two primary reasons. Firstly, the large and cumbersome chips used in IoT devices contributed to the slowdown, and secondly, all the devices were connected to a single centralized server. Consequently, data collected from these chips were stored on this centralized server/database(ibm.com , Benefits of IoT and blockchain).

. However, by incorporating Blockchain technology into IoT devices, these challenges have been resolved, resulting in enhanced security and transparency for IoT devices. Instead of centralized server now through blockchain Data collected form IoT devices are stored on different decentralized systems, hence improve security and less chance of failure and less prone to inconsistency. With blockchain technology, data collected from IoT devices is now stored on several decentralized systems rather than centralized servers, improving security and reducing the likelihood of failure and inconsistency.

IoT uses blockchain's primary feature, immutability, to guarantee data integrity, while its transparency feature allows users to monitor the status of connected devices.Blockchain technology facilitates user and device authentication within the network, thereby fostering trust among all parties involved in IoT processes.

3. Cryptocurrency, Bitcoin , and Blockchain:

Cryptocurrency is a digital payment system that utilizes blockchain technology. This payment method operates on a peer-to-peer basis and does not require the involvement of any third party to verify transactions. Cryptocurrency gets its name from the cryptography system used to secure transactions on the network. Bitcoin was the first cryptocurrency, introduced in 2009 by Satoshi Nakamoto, and remains a popular choice for trading and profit generation. Businesses can also use blockchain technology to enhance their operations and processes. Businesses can consider Blockchain technology as the next-generation software to enhance and revolutionize their processes.

Cyber Security in Blockchain Possible Challenges and their respective alternatives:

Blockchain technology's distributed and highly encrypted nature provides enhanced security against cyber attacks. The technology incorporates numerous safety features, including cryptography, identity controls, and robust data protection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, September 2026
Impact Factor: 8.2

measures to ensure authorized access and maintain confidentiality. However, despite these safeguards, the blockchain market still faces potential risks from malicious actors(Tejas Rasane, Sairaj Sarde,Omkar Lakade, 2023). As hacking methods become increasingly advanced, organizations continue to encounter challenges when integrating Blockchain into their cybersecurity strategies. This article examines common risks linked to Blockchain and presents best practices for protecting each element of the Blockchain ecosystem. Followings are the same:

Weaknesses in Smart Contract Systems: Despite their innovative nature, smart contracts are susceptible to various vulnerabilities. Malicious actors can take advantage of flaws or mistakes in the programming of smart contracts to misappropriate assets, alter information, or potentially disrupt the entire system(Sanjiv Cherian,Mar 25, 2024). For instance, in April 2020, dForce experienced a huge $24 billion loss due to an attack that used the callback feature of the ERC-777 token to falsify transaction notifications.

Solution: Mythril is an Ethereum smart contract security analysis tool. At HITBSecConf 2018, it was first presented. A variety of security flaws are detected by Mythril, such as owner-overwrite-to-ether-withdrawal and integer underflows(Mythril Docs ,2019). The Ethereum Virtual Machine's (EVM) bytecode can be examined using the Mythril12 security analysis approach. By examining input records, it can assist in determining probable reasons when program flaws are discovered.

Sybil attacks: a well-known type of cyber exploitation that has found a new home in blockchain technology (Old vulnerabilities, new platform). These attacks take place when malevolent actors fabricate several false identities in an attempt to overrun, control, or interfere with a system, usually with the intention of weakening authority(Anastasiya Novikava,Jul 3, 2024). Sybil attacks were first noticed in peer-to-peer networks, but they have now spread to blockchain settings. Attackers use a large number of fraudulent nodes spread throughout the network in the context of blockchain, which allows them to block connections and transactions, take over the network, and carry out 51% attacks (i.e., malicious actors control more than half of a blockchain's functions and then dominate the ledger functions) (Ananda Krishna,2025).

Solutions: More secure consensus techniques like Proof-of-Stake (PoS) or Byzantine Fault Tolerance (BFT) can be used to reduce the risk of 51% assaults. These alternate techniques improve network security and offer more resistance against majority attacks. Thankfully, for Sybil attacks are typically simple to identify. They typically impact blockchain operators that have inadequate monitoring and validation procedures. Make sure you have strong authentication procedures in place for each node.

Man-in-the-middle (human) attacks: Attackers are likely to steal users' Blockchain assets.Attackers may intercept data transfer to alter its destination and contents, as well as steal secret keys.These activities might recycle data from legal senders that are difficult to identify.

Solution: To safeguard data and lessen threats, users must employ strong encryption and privacy keys.In order to preserve data privacy and resilience, blockchain offers safe protocols and independently verifies all transaction and data information.

III. FUTURE SCOPES

Companies are simultaneously managing their legacy infrastructure and exploring new computational models to revolutionize entire industries using innovative tools like blockchain for enhanced security. The implementation of blockchain technology is still in its early stages, and potential challenges are being investigated. Nevertheless, blockchain is gaining widespread adoption across various organizations, driving innovation and transforming our daily interactions with technology. Consequently, it is anticipated that blockchain technology will continue to flourish in the future.

IV. CONCLUSION

Blockchain technology has gained significant popularity for data security due to its decentralized nature and use of cryptography. Its unique structure and design have led to numerous applications. However, as blockchain adoption

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, September 2026
Impact Factor: 8.2

grows and data volumes increase, it faces several challenges, including scalability issues, security concerns, privacy risks, and the need for high-performance computing devices. To address these challenges, various solutions and techniques have been implemented, such as Mythril, encryption, cryptography, and decentralization. Improving blockchain security requires increased awareness of vulnerabilities to develop better network solutions. Despite these obstacles, blockchain technology offers potential solutions for safeguarding digital infrastructure, suggesting a promising future for blockchain and cybersecurity.

REFERENCES

1. Amazon Web Services. (n.d.). What is blockchain? AWS
2. IBM. (n.d.). What is blockchain? IBM
3. IBM. (n.d.). What is blockchain security? IBM Blockchain Security
4. GeeksforGeeks. (n.d.). Role of blockchain in cybersecurity. GeeksforGeeks
5. GeeksforGeeks. (n.d.). Cryptography and its types. GeeksforGeeks
6. Forbes Advisor. (n.d.). What is cryptocurrency and how does it work? Forbes Advisor
7. Consensys. (n.d.). Blockchain use cases: Media and entertainment. Consensys
8. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
9. Rasane, T., Sarde, S., & Lakade, O. (2023). [Title of the article not provided]. Journal of Emerging Technologies and Innovative Research (JETIR). JETIR article PDF
10. Mathew, A. R. (2019). [Title of the article not provided]. International Journal of Engineering and Advanced Technology (IJEAT), 9(1). IJEAT article PDF
11. Alam, T. (2019). Blockchain and its role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(1), 10–13. ResearchGate
12. IBM. (n.d.). Blockchain for the Internet of Things (IoT). IBM
13. Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. Journal of Network and Computer Applications, 163, 102635. https://doi.org/10.1016/j.jnca.2020.102635
14. Novikava, A. (2024, July 3). Blockchain security issues. NordLayer. NordLayer
15. Cherian, S. (2024, March 25). Blockchain network security challenges and solutions. Microminder. Microminder
16. Mythril. (2019). About Mythril. Read the Docs. Mythril documentation
17. Krishna, A. (2025). Blockchain security issues. Astra Security. Astra Security