Content available at: https://www.ipinnovative.com/open-access-journals

IP Indian Journal of Library Science and Information Technology

Journal homepage: https://www.ijlsit.org/

Original Research Article

Application of blockchain technology in data security

Pratima Verma[1], Bal Ram[2*]

[1]Dept. of Computer Science, Gurukul Kangri Vishwavidyalaya, Haridwar, Uttarakhand, India
[2]Dept. of Library, Wadia Institute of Himalayan Geology, Dehradun, Uttarakhand, India

ARTICLE INFO

Article history:
Received 18-06-2024
Accepted 05-07-2024
Available online 03-08-2024

Keywords:
Data
Blockchain
Data security
Cybersecurity
Cryptography
Decentralization

ABSTRACT

Blockchain technology has revolutionised how data is stored, managed, and secured. Its decentralised, transparent, and immutable nature presents unique advantages for data security. This paper delves into the application of blockchain technology in enhancing data security, exploring its fundamental principles, mechanisms, real-world applications, benefits, and challenges. By examining case studies across various industries, this paper aims to demonstrate the transformative potential of blockchain technology in securing data and protecting against cyber threats.

1. Introduction

Blockchain technology is rapidly transforming the landscape of data security. By moving away from centralised systems, blockchain offers a robust and tamper-proof approach to data protection. The rapid digitisation of information and the exponential growth of data generation has necessitated robust security mechanisms. Traditional centralised systems are increasingly vulnerable to data breaches, unauthorised access, and cyberattacks. Blockchain technology, first conceptualised in 2008 with the introduction of Bitcoin, offers a decentralised approach to data management and security, potentially addressing many limitations of conventional methods.

2. Overview of Blockchain Technology

The paper's primary objective is to investigate blockchain technology's application in data security. This includes understanding its core principles, exploring various security features, and analysing its application in different sectors to safeguard data integrity and confidentiality.

Blockchain technology is widely used to improve data security in many different fields. It is used to secure wireless sensor data in IoT networks, ensuring privacy and preventing theft.[1] Additionally, blockchain-based systems enable secure data sharing for IoT applications, focusing on data privacy, anonymity, and accountability without needing trusted parties.[2] In the healthcare sector, blockchain-based decentralised security (BCDS) with Crypto-Proof of Stake (CPoS) is proposed to protect personal health records from unauthorised access and key leakage, thereby ensuring data integrity and authentication.[3] Additionally, blockchain-inspired mechanisms are integrated into secure sensor data processing systems to provide access control, immutability, and protection against unauthorised modifications, thereby improving the overall security and integrity of the data.[4] Additionally, the Access Control Enabled Blockchain (ACE-BC) framework leverages attribute encryption and access control mechanisms to improve security and data privacy in sharing security information networks, thereby improving data privacy and efficiency.[5]

[*] *Corresponding author*.
E-mail address: balrammlis@gmail.com (B. Ram).

https://doi.org/10.18231/j.ijlsit.2024.008
2582-1555/© 2024 Author(s), Published by Innovative Publication.

Blockchain technology is important for improving data security measures through various innovative methods. For example, the Access Control Enabled Blockchain (ACE-BC) framework uses attribute encryption techniques and access control mechanisms to enhance data security in Cybersecurity Information Sharing (CIS).[6] Similarly, the blockchain-based decentralised security (BCDS) model uses proof-of-stake (CPoS) and master node key aggregation policy (MNKAP) to authenticate and protect sensitive data in the pool securely. Personal health record (PHR).[7] Additionally, using blockchain to secure access logs will ensure the integrity and reliability of outsourced data by leveraging its security and immutability features.[8] The erasable blockchain model of hierarchical access control improves data security by allowing data owners to specify access policies and control changes through attribute-based encryption and the chameleon hashing technique, ensuring efficient and secure data sharing.[9] These approaches demonstrate how blockchain technology significantly enhances data security measures in various applications.[10]

2.1. Definition and history

Blockchain is a distributed ledger technology that enables secure, transparent, and tamper-proof record-keeping. Each block contains a list of transactions and is cryptographically linked to the previous block, forming a chain. The decentralised nature of blockchain means that no single entity controls the entire network, enhancing security and trust.

2.2. Core components

1. *Decentralisation:* Unlike centralised databases, blockchain works on a peer-to-peer arrangement, where each member (hub) includes a duplicate of the complete blockchain.
2. *Immutability:* Information cannot be changed or erased once information is composed to a blockchain. This permanence is accomplished through cryptographic hashing and agreement instruments.
3. *Transparency:* All communications on a blockchain are observable to all contributors, certifying transparency and responsibility.
4. *Consensus mechanisms:* Numerous processes (e.g., Proof of Work, Proof of Stake) achieve compromise among nodes, authenticating and locking communications.

2.3. Blockchain types

1. *Public blockchain:* Open to anyone; participants can read, write, and audit the blockchain.
2. *Private blockchain:* Restricted access; only authorised participants can engage with the blockchain.
3. *Consortium blockchain:* Controlled by a group of organisations; access is shared among a consortium of entities.

3. Security Features of Blockchain

3.1. Cryptographic hashing

Each block in a blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. The hash function ensures data integrity by producing a unique output (hash) for any given input. Any alteration in the data would result in a different hash, signalling to tamper.

3.2. Consensus mechanisms

Blockchain systems utilise agreement components to approve exchanges and maintain the ledger's judgment. Well-known agreement calculations incorporate:

1. *Confirmation of work (PoW):* Diggers unravel complex scientific issues to approve exchanges and make modern pieces. This preparation requires critical computational control, making it expensive and troublesome to control.
2. *Verification of stake (PoS):* Validators are chosen based on the cryptocurrency they hold and are willing to "stake" as collateral. This strategy is more energy-efficient than PoW.
3. *Delegated proof of stake (DPoS):* Participants vote for a small number of delegates to validate transactions on their behalf, combining elements of both PoW and PoS.

3.3. Decentralisation and distributed ledger

Blockchain's decentralised architecture eliminates the need for a central authority, reducing the risk of a single point of failure. Data is replicated across multiple nodes, ensuring that the data remains secure even if some nodes are compromised.

3.4. Smart contracts

Shrewd contracts are self-executing contracts with the terms composed explicitly into code. They consequently implement and execute assertions when predefined conditions are met. This mechanisation diminishes the hazard of human blunder and extortion.

4. Applications of Blockchain in Data Security

4.1. Secure data storage

Blockchain provides a secure method for storing data across a distributed network. This decentralisation ensures that data is not stored in a single location, reducing the risk of data breaches and unauthorised access.

4.2. Data integrity and verification

The immutability and transparency of blockchain make it ideal for ensuring data integrity. Any changes to the data are visible to all participants, making it easy to detect and prevent tampering. Blockchain can be used to verify the authenticity of data, ensuring that it has not been altered since its creation.

4.3. Identity management

Blockchain technology can enhance identity management systems by providing a secure, decentralised way to store and verify identities. Users can have greater control over their personal information, reducing the risk of identity theft and fraud. Blockchain-based identity management systems can provide:

1. *Decentralised identifiers (DIDs)*: Unique identifiers created, owned, and managed by individuals.
2. *Self-sovereign identity:* Individuals have full control over their identity information without relying on a central authority.

4.4. Secure transactions

Blockchain technology can secure financial and non-financial transactions by providing a transparent and immutable record of all transactions. This ensures that transactions are accurately recorded and can be verified by all parties involved. Applications include:

1. *Cryptocurrencies:* Secure digital currencies (e.g., Bitcoin, Ethereum) that use blockchain for transaction validation.
2. *Supply chain:* Tracking and verifying the movement of goods through the supply chain to ensure authenticity and prevent fraud.

4.5. Regulatory compliance and auditing

Blockchain's transparency and immutability make it a valuable tool for regulatory compliance and auditing. Organisations can use blockchain to maintain accurate records of transactions, ensuring compliance with legal and regulatory requirements. Auditors can verify data and transactions on the blockchain, reducing the risk of fraud and errors.

4.6. Health data security

In the healthcare sector, blockchain can securely store and share patient records, ensuring they are only accessible to authorised personnel. This can enhance patient privacy, data security, and care coordination.

4.7. Intellectual property protection

Blockchain can be used to protect intellectual property by providing a secure and transparent record of ownership and rights. Creators can timestamp and register their work on the blockchain, ensuring their rights are protected and verifiable.

5. Case Studies

5.1. Healthcare: MedRec

MedRec, developed by MIT, is a blockchain-based system for managing electronic medical records. It provides a secure, decentralised way to store and share patient data. Patients have control over their data and can grant access to healthcare providers as needed. This enhances data security, patient privacy, and interoperability among healthcare systems.

5.2. Supply chain management: IBM Food Trust

IBM Food Trust uses blockchain technology to enhance transparency and traceability in the food supply chain. Recording every step of the supply chain on a blockchain ensures that data about the origin and movement of food products is accurate and tamper-proof. This improves food safety, reduces fraud, and enhances consumer trust.

5.3. Financial services: Ripple

Ripple is a blockchain-based payment protocol enabling secure, fast, low-cost cross-border transactions. Using a decentralised network of validators, Ripple ensures the security and integrity of transactions. Financial institutions can use Ripple to reduce the cost and complexity of international payments while enhancing security.

5.4. Digital identity: uPort

uPort is a blockchain-based identity management system that provides users a secure and decentralised way to manage their digital identities. Users can create and control their identities, granting access to their information as needed. This enhances privacy and security while reducing the risk of identity theft and fraud.

6. Challenges and Limitations

6.1. Scalability

One of the biggest challenges of blockchain innovation is versatility. As the number of exchanges increases, the measure of the blockchain develops, driving slower exchange times and higher costs. Arrangements such as shading, off-chain exchanges, and layer-2 conventions are being created to address these issues.

6.2. Regulatory issues

The use of blockchain technology is subject to regulatory scrutiny. Different jurisdictions have different regulations regarding data privacy, security, and financial transactions. Navigating these regulatory frameworks can be complex and hinder blockchain solutions' widespread adoption.[11]

6.3. Energy consumption

Blockchain networks that use Proof of Work (PoW) consensus mechanisms consume significant energy. This raises environmental concerns and has led to exploring more energy-efficient alternatives such as Proof of Stake (PoS) and other consensus algorithms.

6.4. Interoperability

Interoperability between different blockchain networks and existing systems is a significant challenge. Ensuring seamless communication and data exchange between various platforms is essential for the widespread adoption of blockchain technology.

6.5. Security risks

While blockchain technology offers robust security features, it is not immune to risks. Potential vulnerabilities include:[12]

1. *Smart contract bugs:* Errors in smart contract code can be exploited, leading to security breaches.
2. *51% attacks:* A single entity can manipulate the blockchain if it controls more than 50% of the network's computational power.
3. *Private key management:* The security of blockchain relies on the protection of private keys. Loss or theft of private keys can lead to unauthorised access and loss of assets.

7. Future Prospects

7.1. Advancements in consensus mechanisms

Future developments in consensus mechanisms, such as Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT), aim to improve blockchain networks' efficiency, scalability, and security. These advancements can make blockchain technology more sustainable and widely adopted.

7.2. Integration with emergent technologies

Integrating blockchain with new technologies such as artificial intelligence (AI), the Internet of Things (IoT), and quantum computing can improve data security. For example, blockchain can provide a secure and transparent framework for communication and data exchange between IoT devices.

7.3. Standardisation and interoperability

Efforts to develop standardised protocols and frameworks for blockchain technology can enhance interoperability between different blockchain networks and existing systems. This can facilitate broader adoption and integration of blockchain solutions across various industries.

7.4. Enhanced privacy solutions

Innovations in privacy-preserving technologies, such as zero-knowledge proofs and homomorphic encryption, can enhance the privacy and confidentiality of data on the blockchain. These solutions can address privacy concerns and enable secure data sharing.

7.5. Regulatory developments

As blockchain technology evolves, regulatory frameworks will likely adapt to address its unique challenges and opportunities. Clear and consistent regulations can provide a conducive environment for the growth and adoption of blockchain solutions.

8. Conclusion

Blockchain technology offers significant potential for enhancing data security across various industries. Its decentralised, immutable, and transparent nature provides robust mechanisms for protecting data against unauthorised access and tampering. While scalability, regulatory issues, and energy consumption need to be addressed, ongoing research and development efforts will likely overcome these hurdles. The future of blockchain technology in data security is promising, with the potential to transform how data is stored, managed, and protected.

9. Source of Funding

None.

10. Conflict of Interest

None.

References

1. Hsiao SJ, Sung WT. Enhancing cybersecurity using blockchain technology based on IoT data fusion. *IEEE Internet Things J*. 2023;10(1):486–98.
2. Wu T, Wang W, Zhang C, Zhang W, Zhu L, Gai K, et al. Blockchain-based anonymous data sharing with accountability for internet of things. *IEEE Internet Things J*. 2023;10(6):5461–75.
3. Deepika KM, Sanjay HA, Murthy M. Blockchain-based decentralized security using crypto-proof of stake for securing sensitive personal health care records. *Adv Eng Software*. 2022;173:103235.
4. Zhao W, Aldyaflah IM, Gangwani P, Joshi S, Upadhyay H, Lagos L. A blockchain-facilitated secure sensing data processing and logging system. *IEEE Access*. 2023;11.
5. Alharbi A. Applying access control enabled blockchain (ACE-BC) framework to manage data security in the CIS system. *Sens*. 2023;2023(6):3020.

6. Manogaran G, Alazab M, Shakeel PM, Hsu CH. Blockchain assisted secure data sharing model for internet of things based smart industries. *IEEE Trans Reliability*. 2022;71(1):348–58.
7. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on internet of medical things. *Pers Ubiquit Comput*;28:59–72.
8. Benkhaddra I, Kumar A, Bensalem ZE, Hang L. Secure transmission of secret data using optimization-based embedding techniques in blockchain. *Expert Syst Appl*. 2023;211:118469.
9. Sifah EB, Xia Q, Agyekum KO, Xia H, Smahi A, Gao J. A blockchain approach to ensuring provenance to outsourced cloud data in a sharing ecosystem. *IEEE Syst J*. 2022;16(1):1673–84.
10. Pal SK, Ram B. Applications of modern tools and technology in library services. Biotech Books; 2017.
11. Ram B, Yadav S, Singh KK. Application of cloud computing in library services. In: 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services; 2018. p. 75–8.
12. Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access*. 2017;p. 1–9.

Author biography

Pratima Verma, Research Scholar

Bal Ram, Librarian https://orcid.org/0000-0001-6749-9334

Cite this article: Verma P, Ram B. Application of blockchain technology in data security. *IP Indian J Libr Sci Inf Technol* 2024;9(1):51-55.