Advances in Machine Learning, IoT and Data Security

"Volume 1, Issue 1, Year 2024"

website: https://www.c5k.com

Research Article

Blockchain Technology for Securing Digital Information: Opportunities and Challenges

Mahafuj Hassan[1*], Md Azhad Hossain[1], Mohammad Zahidul Alam[2], Md Redwan Hussain[3], Jarin Tias Meraj[3]

[1]*Department of Business Administration, International American University, Los Angeles, CA 90010, USA*

[2]*Department of Information Technology, Westcliff University, Irvine, CA 92614, USA*

[3]*Department of Computer Science and Engineering, Daffodil International University, Birulia, Savar, Dhaka-1216, Bangladesh*

**Corresponding Author: mahafujhassan87@gmail.com*

ARTICLE INFO

Article history:
03 Jul 2024 (Received)
17 Aug 2024 (Accepted)
25 Aug 2024 (Published Online)

Keywords:
information security, blockchain, decentralization, timestamp, Cyber security.

ABSTRACT

Modern Internet technology has developed because of information security. The password mechanism, programmed mechanism, decentralized mechanism, and distributed mechanism. The Blockchain's mechanism offers a whole new angle for the advancement of Internet information security technologies. The mechanisms used to store and distribute information within a network are redefined by Blockchain technology. It is not necessary for participants to know one another or for third-party certifying agencies to take part. It uses distributed technology to record, transmit, and store information value transfer activities. It also uses an asymmetric cryptographic algorithm to prevent data tampering and forgery. Finally, it allows all participants to agree on the current state of blockchain data information. Additionally, the use of blockchain technology in identity identification, data protection, and network security is explained by a recent industry study. The development of information security technology will be greatly accelerated by blockchain technology, which will also have a significant influence on the field's overall growth.

DOI: https://doi.org/10.103/xxx @ 2024 C5K Research Publishing

1. Introduction

Blockchain technology, also known as distributed ledger technology, is a crucial component of Bitcoin: A Peer-to-Peer Electronic Cash System. It is the foundation for the construction of Bitcoin's data structure and transaction information encrypted transmission. Blockchain technology is driving a revolution in information security technology, playing a major role in the identification, certification, defending against DDoS attacks, ensuring data integrity and credibility, and actively promoting the healthy development of national information security(MEI & LIU, 2016).

Blockchain technology is a result of the integration of multiple existing technologies, such as a database, to maintain a unique and reliable database through a decentralized and trustful approach. It forms a new way of data recording, delivery, storage, and presentation, allowing anyone in the system to participate in the work of a data center. This technology removes the central control node by decentralizing and constructing a P2P self-organizing peer-to-peer network through a distributed method. It maintains the integrity, continuity, and consistency of data information through asymmetric password verification mechanisms, thereby enhancing the security of national informatization(MEI & LIU, 2016).

Blockchain technology is an evolutionary and scalable Internet protocol that uses a block-based chain data structure, open-source decentralized distributed architecture, asymmetric cryptographic mechanism, and flexible and controllable scripting. The blockchain database is an internet-distributed database technology that uses innovative blocks as data elements, connected into a chain through index information. The first block, a genesis block, was created by Nakamoto and each block chronologically records value exchange during its creation. The block structure contains the block header and block data, linking the previous block to the current block. The block data is validated value exchange information to ensure data integrity and consistency.

*Corresponding author: mahafujhassan87@gmail.com (Mahafuj Hassan)
All rights are reserved @ 2024 https://www.c5k.com, https://doi.org/10.103/xxx
Cite: Mahafuj Hassan, Md Azhad Hossain, Mohammad Zahidul Alam, Md Redwan Hussain, Jarin Tias Meraj (2024). Blockchain Technology for Securing Digital Information: Opportunities and Challenges. *Journal of Information Technology Management and Business Horizons*, 1(1), 1-XY.

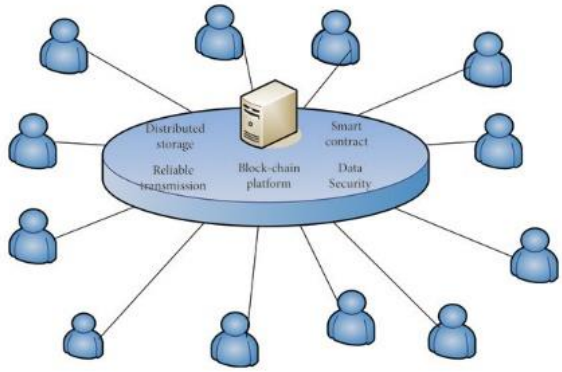

Fig. 1. Advantages of blockchain technology(Yang, 2022).

Blocks form a blockchain based on the value of the exchange agreement, with each block header containing the transaction information index of the previous block. The data index of the previous block forms the head of the block, and the data information forms the block data. A timestamp is affixed to form a blockchain end-to-end, ensuring the authenticity of the blockchain database. The blockchain database stores the complete data information from the genesis block to the latest block in a chain structure, allowing anyone to participate in the recording of any block. Blockchain technology is a decentralized system that operates on the principle of voluntariness, allowing all nodes to work together to maintain and update data. It uses protocol mechanisms to ensure that each node maintains its data information and verifies other nodes.

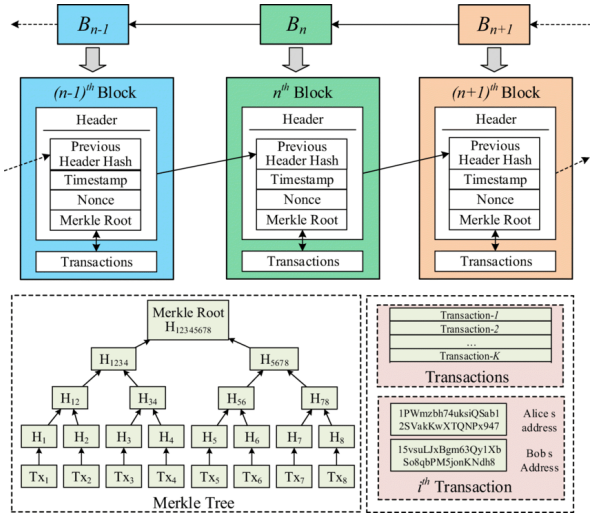

Fig. 2. Blockchain architechture.

The updated block data information relies on the fact that most nodes or all nodes in the network consider the data information correct or pass the comparison result, ensuring the authenticity of the record. It also establishes a distributed peer-to-peer network accounting system, allowing employees to participate in decentralizing accounting responsibilities. Data information is distributed and validated in distributed networks via an open source and decentralized distributed system, with new transaction information also distributed in a distributed structure(Liang Liu, 2018).

Blockchain technology validates the ownership of data information based on asymmetric encryption algorithms, with two keys required for encryption and decryption: a public key and a private key. The public key is open to the public, while the private key is only owned by the owner of the information. In a decentralized environment, a script is a programmable smart contract that all blockchain agreements need to agree on ahead of time. This script allows for flexibility in changing the conditions under which the value of the saved value is spent and adding value re-transfer conditions when sending the value.

The study makes the function of Blockchain technology for digital information more clear. Information security and blockchain security technology are also explained briefly.

2. Related Studies

In 1991, Stuart Haber and W. Scott Stornetta introduced Blockchain Technology, a computational solution for time-stamping digital documents. They developed a system using cryptography to store multiple documents in a Chain of Blocks. In 1992, Merkle Trees formed a legal corporation using this system, which became efficient. In 2004, Hal Finney introduced a system for digital cash called "Reusable Proof of Work," which helped solve the Double Spending Problem.(Dylan Yaga, 2019) In 2008, Satoshi Nakamoto conceptualized the concept of "Distributed Blockchain" in his white paper, which followed a peer-to-peer network of time stamping. This led to the development of Bitcoin, which was later recognized as a legal currency in 2017. In 2018, Bitcoin's value dropped to $3,800, and online platforms banned cryptocurrency advertising. In 2019, Ethereum network transactions exceeded 1 million per day, and Amazon announced the availability of the Amazon Managed Blockchain service on AWS. In 2020, Ethereum launched Beacon Chain in preparation for Ethereum 2.0, and in 2022, it shifted from a Proof of Work to a Proof of Stake consensus mechanism, reducing Ethereum's energy consumption by approximately 99.95%(*History of Blockchain*, 2023).

A study reviews existing blockchain-based solutions for Industry 4.0 applications, focusing on security and privacy. It discusses the merits and demerits of these approaches, as well as the challenges of interoperability and governance, providing a clear understanding for researchers and professionals(Shaik V. Akram, 2020). Another survey shows that Blockchain is increasingly used in various sectors, but many engineering and management challenges remain unaddressed. A special issue received 200 submissions, with 39 accepted articles. The first 36 articles cover supply chain, financial technology, IoT, smart city, healthcare, security, privacy, and consensus algorithms. The

findings aim to provide sustainable solutions for existing and future blockchain systems and platforms(Choo et al., 2020).

The research, Blockchain Technology for Security Issues and Challenges in IOT shows that the Internet of Things (IoT) enables research and engineering without human involvement, enabling interactions between machines and smart workers. Integrating blockchain technology with IoT can address security and privacy concerns, but also presents challenges like scalability. This study explores the advantages, design considerations, and potential applications of distributed ledger-based blockchain technology in IoT, focusing on specific issues unique to IoT and blockchain(Ruan, 2023).

3. Blockchain technology for cyber security

This study explores the application of blockchain technology in the field of information security.

3.1. Identity Authentication:

A key component of security that MIT is concentrating on is the use of blockchain technology for identity identification. Blockchain technology removes possible risks to central entities such as CAs by providing decentralized authentication. This method enhances network access performance by enabling users to authenticate certificates using transparent, decentralized sources. The first public key infrastructure (PKI) based on blockchain technology is the MIT CertCoin project, which uses distributed accounts with blockchain as a public key and domain name to replace centralized CAs. Additionally, Pomcor has made available a blockchain-based PKI solution that enables users to locally authenticate signatures and keys using blockchain copies. The IOTA project is rebuilding an entirely new identity management system without depending on outside CAs by using Tangle, a lightweight, scalable, and blockless distributed account. This method aims to protect legitimate users and ensure the security of network information.

Fig. 3. Identity authentication management for Blockchain technology.

3.2. Infrastructure Protection:

DDoS assaults double the potency of these attacks by launching attacks against one or more targets using numerous computers and C/S technologies. By taking advantage of flaws in the target system's network service function or by directly accessing its resources, they aim to compromise confidentiality, integrity, and usability. DDoS assaults have the potential to consume excessive amounts of service resources, and as computer and network technology advances, so does their destructiveness. Hackers typically target the DNS service, and blockchain technology is predicted to address this major vulnerability on the Internet. Blockchain-based DNS systems seek to replace HTTP and create a better web by doing away with arbitrary record tampering and hacker assaults. They do this by using the Ethereum blockchain and the IPFS.

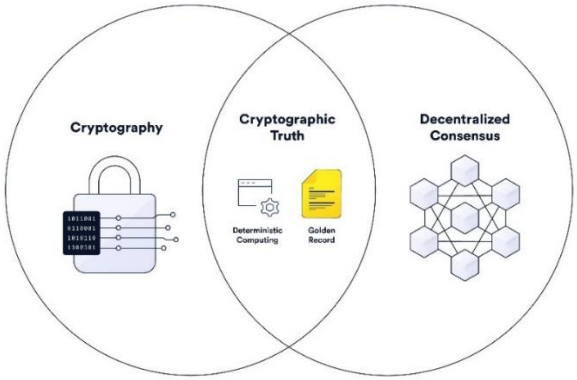

Fig. 4. Double layer data protection in Blockchain technology.

3.3. Data security:

Data security technology is crucial for protecting the integrity of data. Digital signatures, typically generated through cryptography, provide a set of data information representing the identity and integrity of the signer. However, the confidentiality of the private key is compromised, making digital signatures only valid for the original data. Blockchain technology can replace digital signatures with transparency, distributing evidence to multiple nodes and increasing the cost of tampering with data. GuardTime's KSI project uses blockchain technology to store hash tables of raw data and files, ensuring data integrity and transparency. This technology is particularly beneficial for organizations dealing with large amounts of sensitive data and frequent hacker attacks.

4. Challenges Faced by Blockchain Technology for Cyber Security

The section discusses the challenges that Blockchain Technology faces in terms of cybersecurity.

4.1. Hardware and Energy Consumption:

Blockchain is a decentralized alternative to traditional transaction systems, requiring offloading for scalability, interoperability, and sustainability. It allows offloading

of public key operations, increases transaction speed, and improves output accuracy. However, Bitcoin's energy consumption is 11 times higher than Ethereum's due to complex mathematical problems and transaction time.

4.2. Scalability:

Blockchain networks can handle large-scale transactions, but data processing services are crucial for scalable services. Cloud computing can provide on-demand resources for blockchain activities, enabling a highly scalable integrated system. However, many blockchains struggle to support countless users, leading to modest exchange rates and higher fees. Blockchain technology is crucial for EV applications with WSN infrastructure, but challenges include scalability, data security, and confidentiality.

4.3. Transaction likability:

Blockchain-related problems include transaction linkability and address tracking. Attacks against wallet addresses and transaction currency have been reported for cryptocurrencies such as ZCash and Bitcoin. These problems still exist even after more than 11 years have passed. Transparent addresses do not safeguard transaction value, and shielding addresses can delink them. Even with its anonymous feature, onion or garlic cast routing is susceptible to timing analysis attacks.

5. Conclusion

Blockchain technology describes a novel approach to trade that is predicated on important technologies including shared public accounts, decentralized coherence, and password security. Viewable permissions and appropriate controls. By recording and trading assets that are real and intangible, virtual and physical, it has the potential to drastically alter how our society creates and lives. It is not sufficient to see blockchain technology as an application for modern commerce. It streamlines corporate procedures and fosters accountability, openness, and trust. It will fundamentally alter how transactions are conducted on the Internet and impact the state of Internet information security technologies. During the development process, technology will unavoidably encounter some security concerns in its realization and implementation. However, it is anticipated that blockchain technology's novel approach to information exchange and storage would provide a ground-breaking remedy for the unregulated information security sector.

References

Choo, K.-K. R., Ozcan, S., Dehghantanha, A., & Parizi, R. M. (2020). Blockchain Ecosystem—Technological and Management Opportunities and Challenges. *IEEE Transactions on Engineering Management*, *67*(4), 982 - 987.

Dylan Yaga, P. M., Nik Roby, Karen Scarfone. (2019). Blockchain Technology Overview.

History of Blockchain. (2023). Geeksforgeeks. https://www.geeksforgeeks.org/history-of-blockchain/

Liang Liu, B. X. (2018). Research on Information Security Technology Based on Blockchain. the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis,

MEI, H., & LIU, J. (2016). Industry present situation, existing problems and strategy suggestion of blockchain. *Telecommunications Science*, *32*(11), 134-138.

Ruan, Z. (2023). Blockchain Technology for Security Issues and Challenges in IOT. 2023 International Conference on Computer Simulation and Modeling, Information Security (CSMIS), Buenos Aires, Argentina.

Shaik V. Akram, P. K. M., Rajesh Singh, Gehlot Anita, Sudeep Tanwar. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Wiley*.

Yang, B. (2022). [Retracted] Prevention of Business Risks of Internet Information Security Platforms Based on Blockchain Technology. *Computational Intelligence and Neuroscience*, *2022*(1), 7671810.