Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Internet of Things-enhanced blockchain technology: an overview of advancements and prospects

Atheer Alaa Hammad[1]*

[1]Ministry of Education, Anbar Education Directorate, AL ANBAR, IRAQ.

*Corresponding Author: Atheer Alaa Hammad

DOI: https://doi.org/10.55145/ajest.2024.03.02.06
Received May 2024; Accepted July 2024; Available online July 2024

ABSTRACT: Through a systematic review of the literature, this study provides a comprehensive summary of the latest findings on the acceptance and application of blockchain technology in supply chain management. It was founded on a comprehensive analysis of thirty studies published in prestigious journals. The need for secure, decentralized AI systems to thwart potential cyberattacks is growing as AI is increasingly used in cybersecurity. The ideal choice for enhancing the security and privacy of AI systems is blockchain technology (BT), due to its immutable and decentralized data storage properties. This comprehensive literature review focuses on the integration of decentralized IT with cybersecurity. It provides a comprehensive BT and IoT cybersecurity taxonomy to get you started. This work contributes to a more sophisticated understanding of the integration between BT and IoT by demonstrating compelling results that highlight the benefits of these connections for cybersecurity. These findings are coupled with the potential cybersecurity advantages and difficulties of IoT. It also addresses the beneficial uses of blockchain-enabled IoT to solve cybersecurity problems. Finally, this paper addresses future directions for blockchain-based cybersecurity research across a range of sectors, including industry, agriculture, IoT, and health.

Keywords: Blockchain, Artificial intelligence, Cybersecurity, Privacy &IoT technology

1. INTRODUCTION

Blockchain has revolutionized areas that were hitherto unforeseen. Today's blockchain technology has multiple areas to impact and continues to see development in cutting-edge areas with multiple applications. The journey of blockchain began on October 31, 2008 when a research paper titled “Bitcoin: A Peer-to-Peer (P2P) Electronic Cash System” appeared, written by an anonymous Satoshi in 2008. The brief pointed to the realization of a purely electronic cash system via the internet peer-to-peer exchange [1] .In order to give patients better care, diagnostics have grown in popularity in the majority of healthcare sectors due to the rising standards of healthcare services. Here, an individual's medical data can be monitored through the use of an electronic health record (EHR). Digital medical records are kept up to date for medical facilities using an electronic health records system. In today's world, when patients want instant access to their medical records, enterprise-level data systems are utilized to share medical papers along with other networking operations. There are numerous integrity, management, and security-related problems with the electronic health records system. Concerns remain, though, regarding patient privacy and security in their medical records. They find it difficult to keep up with the vast volume of healthcare data that is created electronically. Blockchain technology, a productive way to store health information[2]. A network of uniquely identified linked objects that adheres to an addressing standard and has embedded technology that can intersect and sense its surroundings to gather data and communicate with it is known as the Internet of Things. Blockchain and the Internet of Things (IoT) are quickly emerging technologies that are easily integrated and used in a variety of services, particularly in applications related to industry, agriculture, and health monitoring systems (HMS). Using IoT every smart device has a processing and storage capability that allows it to examine the physical data gathered and send it to a central storage location for additional computations. Because storage needs to include data processing, security, single point of failure, and trust, it is challenging. By combining Blockchain technology with the Internet of Things, such issues can be lessened[3].

2. Literature review

In 2024 Wang, F., Gai, Y et al. [4] By examining the user's unique digital identity characteristics and massive data management chains, the researchers proposed redesigning blockchain information security. This work advances and unifies multiple domains, such as computer science for information security, data management, and social psychology of trust, through the NOPI paradigm. It looks into the relationships between blockchain laws, big data, network trust, and information security as well as user identification. Both dynamic security measures and cooperative blockchain management processes are presented. The digital social security governance framework will be significantly enhanced by the CPS-based Zero Trust approach. Digital governance will improve big data classification and sharing, as well as digital and intelligent modernization and alter organizations (governments, enterprises, and other entities) and the Metaverse (Metaverse systems). Additionally, high-level initiatives and global economic cooperation will obtain a promotion. growth in quality.

In 2024 Ren, Z., Yan, E. et al[5]. They suggested a distributed KMS based on blockchain technology and a zero-knowledge proof CP-ABE system. centralized key management by authorized entities, ineffective key distribution and administration, lack of key validation, and limited scalability and expensive on-chain expenses in blockchain networks are some of the problems that attribute-based cryptosystems based on blockchain are trying to solve. Next, a thorough examination of the algorithmic and blockchain security of the recommended approach Better trade-offs between functionality, security features, and computational and storage overhead are provided by the suggested approach. It provides practical solutions to existing issues in attribute-based cryptosystems based on blockchain technology. The blockchain ciphertext access control algorithm needs to be improved.

In 2024 Zhang, Z., Yu, G., Sun, C. et al. [6] In this paper, researchers offer a Trust-Based DRL (TBDD) with the goal of dynamically changing node allocation and reducing the risk of collusion attacks. These kinds of systems must carefully balance security and scalability considerations. Deep Reinforcement Learning (DRL) is particularly effective in two domains: multidimensional optimization and complex, dynamic systems. Productivity is increased while network security is upheld. Targeted repartitioning against potential threats and node type differentiation are achieved by TBDD through an extensive trust evaluation system. By increasing node mobility frequency, spreading nodes equitably among shards, enhancing tolerance to dishonest nodes, and balancing the risk of fragmentation, the TBDD framework secures the network. Extensive evaluations confirm that TBDD works better at reducing cross-trade transactions and distributing partition risks than traditional partitioning strategies based on trust, community, and randomness.

In 2024 Luo, F., Huang, R. et al. [7] For agricultural IoT systems with different cryptographic configurations, researchers in this system developed blockchain-based multi-domain authentication to address issues with certificate management and key assurance. To increase cross-domain batch verification's adaptability, an algorithm for batch verification employing batches is proposed. Batch sizes can be changed with this method based on certain tasks. Unlike single-chain design, HBMA is obviously well-suited for large-scale agricultural IoT applications covering numerous domains. Analysis of cross-domain device behavior should provide insights into how to improve the blockchain's PBFT consensus mechanism. The hybrid blockchain paradigm that this system adopts facilitates cross-domain collaboration between agencies that manufacture agricultural goods and monitor safety.

In 2024 Wang, X., Zhang, H., Wu, H. et al. [8] They proposed an architecture for federated learning based on multilayer clustering (BMFL). Which enables the exchange of a large set of data within the Industrial Internet of Things (IIoT) thanks to federated learning (FL), which enables data owners to train neural networks collectively without sharing local data. In order to maintain the hash of the relevant block header and during change management of the encryption key on the main blockchain, we use BMFL chameleon hashing technology. we can use a blockchain model to record the parameters of this global model and divide the groups into the participants based on the training tasks. Experimental results show that the proposed BMFL exhibits more accurate and stable convergence behavior than the classical FL algorithm, which indicates that the additional time required for key cancellation is reasonable.

In 2024 Zheng, W., Wang, X., et al.[9] They proposed a two-layer architecture called S-DAG, which combines a sharded blockchain and a DAG blockchain. The sharded blockchain manages transactions inside the building's Internet of things network, while the DAG blockchain keeps track of the headers from the sharded network. The segmentation approaches now in use are not adequate to handle the complexity of 3D data requests and the variability in edge node performance in Internet of Things architecture. This leads to issues such as overheated parts and subpar data searches. The findings show that compared to earlier options, the suggested strategy is more suitable for developing IoT data management. It is predicated on the creation of a 3D-Merkle tree block structure to facilitate 3D data searches and an adaptive load balancing algorithm (ABLA) to sporadically divide the network.

In 2024 Ismail, S., Nouman, M., et al. [10] Researchers introduced a comprehensive security architecture for IoT sensor networks that is based on blockchain technology and machine learning (ML). Two modules make up the framework: one for machine learning detection and the other for blockchain prevention. The two fundamental tactics in the blockchain prevention module are identification and trust management. Identity management ensures that unauthorized entities are prohibited from performing any actions by handling node registration and authentication with a lightweight smart contract (SC). To maintain credibility and trust across sensor nodes throughout the network, a lightweight SC is employed in trust management. Keep an eye on the node's lifetime and prior actions.

In 2024 García-Valls, M. et al. [11] The CoTwin middleware architecture serves as a framework to facilitate the creation and optimization of a DT model in a cyber-physical system made up of multiple interconnected cells. Thanks to the framework, cells may do a wide range of tasks, including loading new models, accessing and retraining previously taught models, and using them for prediction as necessary. The framework supports popular languages and platforms and is built on a language-neutral UML architecture. To provide the necessary capabilities to deal with models on the blockchain cooperatively, a set of components has also been designed with concern separation.

In 2024 Ghani, M. A. N. U., She, K et al. [12] They put forth a strategy that integrates Blockchain technology, microbatch aggregation, and Generative Adversarial Networks (GANs) in a way that addresses the crucial issues of data integrity and privacy preservation in programmes that use facial recognition. High-quality and realistic synthetic face images have been produced with the self-attention mechanism-enhanced privacy-preserving GAN (PPSA-GAN) architecture, fulfilling strict privacy requirements with remarkable results. Strict benchmarking on the CelebA dataset produced state-of-the-art results, with PPSA-GAN outperforming previous approaches with an astounding 35.50 Fréchet starting distance and 13.99 starting score. Additionally, the equivalent values of 0.947, 0.938, 0.943, and 0.948 indicated that the F1-score, recall, and precision criteria were met.

In 2024 Alsaeed, N., Nadeem, F. et al. [13] They proposed a novel architecture for Internet of Medical Things (IoMT) device collective authentication. The group authentication system is implemented in four steps: setup, registration, secret creation, and authentication. The suggested architecture for group authentication blends fog computing powered by blockchain, Efficiency and scalability are improved by the use of Shamir's secret sharing (SSS) approach with elliptic curve cryptography (ECC). The proposed architecture was simulated using the Ethereum platform and the Solidity programming language; its performance was evaluated using the Hyperledger Caliper tool. Simulation tests showed that the suggested framework could authenticate IoMT devices at 400 transactions per second throughput with an average latency of 0.5 seconds. Modern blockchain-based authentication methods were contrasted with the suggested framework, and the latter performed better in terms of throughput and latency.

In 2024 Alsaeed, N., Nadeem, F. et al. [14] A novel architecture for group authentication in Internet of Medical Things (IoMT) systems has been created by researchers. Solidity was utilized as the programming language, and the Hyperledger Caliper tool was employed to simulate and assess the performance of the suggested system on Ethereum. The suggested architecture for IoMT device authentication performed well in simulation tests, achieving a throughput of 400 transactions per second with an average delay of 0.5 seconds. The suggested framework outperformed other cutting-edge blockchain-based authentication methods when tested against them, according to the results, in terms of throughput and latency.

In 2024 Dong, Y., Li, Y. et al. [15] They displayed a prototype of a decentralized blockchain system with editing and access control features. It has been successfully demonstrated by researchers looking into the interoperability of different systems that redactable features and access control may be implemented to a consortium blockchain. The consortium blockchain system operates through the following five processes: initialization, user registration, data uploading, data access, and data organization. Combining editing with access control makes this feasible.

In 2024 Chen, J., Pu, C., Wang, P., et al. [16] Provide a decentralized management framework based on blockchain that enables TSN's ECNs to independently communicate with one other. Researchers created TECChain, a blockchain-based architecture, to handle edge collaboration and related processes for EC in TSN. Delegation (DPoD) and proof-of-dilligence (PoD) consensus approaches are established to address the consensus problem in TECChain. Two interval-based consensus procedures were presented by scientists using the high-precision synchronous clock basis of TSN: sequential decision making based on DPoD (S-DPoD) and sequential fault tolerance based on DPoD (BFT-DPoD), respectively. The results show that the recommended algorithms perform better than the others in terms of security, transactions per second (TPS), and energy efficiency. A comparison study shows that S-DPoD performs better than BFT-DPoD in terms of consensus success rate, byzantine fault tolerance, and interactive message consumption. greater TPS and quicker transaction verification times.

In 2024 Guo, H., Liang, H., Huang, J et al. [17] We present a new system that can manage non-fungible tokens (NFTs) individually and in large quantities, and allows for the simultaneous trading of fungible tokens. Token bridges that accept multiple token standards, such as ERC20, ERC721, and ERC1155, and offer cross-chain storage have been developed by researchers. By utilizing Ethereum and its test network, which demonstrates a notable reduction in cross-chain token step transfer time by roughly half, waiting times and handling costs can be reduced. This strategy demonstrates cost- and efficiency-effectiveness.

In 2024 Fan, J., Liu, D., Tang, G et al. [18] Content delivery networks, or CDNs, have reinvented the way that end users' IoT devices exchange storage and bandwidth. The IoT devices of end users function as miniature caching servers with this innovative CDN solution for intelligent share processing. Using Ethereum's smart contracts as a foundation, smart sharing develops a safe and open transaction platform. The findings demonstrate how the Smart Sharing framework may help CDN providers, end users, and content suppliers alike. Smart sharing can benefit content producers (CPs), content delivery network (CDN) providers, and owners/end users of Internet of Things (IoT) devices.

In 2024, Asaithambi, S., Ravi, L., Devarajan, M., et al.[19] Researchers have developed an enterprise blockchain e-commerce platform based on the PoA consensus procedure for generating and approving new blocks in the system. SMB ecosystem participants have emphasized the need of e-commerce security and privacy. Use an accumulated

validators number (AVN) and a pseudo random number generator (PRNG) to validate the new block. Ensure that each block in the distributed ledger is permanently timestamped and stored there. VM nodes mutually delegate all institutions on the network under the private PoA-based blockchain protocol, which also protects data integrity. The proposed consensus mechanism is characterized by strong traceability, non-repudiation, and resilience to known security threats.

In 2024 Sultan, N. H., Kermanshahi, S. K. et al. [20] A dynamic multi-client searchable symmetric encryption (SSE) method has been proposed by researchers for the Internet of Things. Dynamic file addition and removal are possible with little privacy loss thanks to the system's effective forward and backward privacy achieved by combining the BitMap index with additional symmetric encryption algorithms. Additionally, the owner can grant access to several clients to their encrypted data through the method's usage of a tree-based block key distribution approach. By leveraging the benefits of the Chameleon hash function, customers' access credentials are deleted at a minimal cost.

In 2024 Liu, L., Ma, Z., et al.[21] Researchers have created a smart blockchain system that allows for the use of incentive mechanisms to authenticate environmental, social, and governance (ESG) reports. The first stage simplifies the audit selection process and is based on artificial intelligence. Particularly when using deep learning and clustering techniques, it is possible to link environmental, social, and governance (ESG) reporting audit assignments to validators whose prior performance demonstrates that they are the most qualified for the task. The "Veri-Green" VCG auction mechanism's second stage will improve the validation process even more. Offering a strategic advantage, the VCG mechanism produces the most economically efficient results. The blockchain will be utilized to store the verified ESG certification, and "Veri-Green" will be employed in the selection of qualified auditors. When comparing blockchain-enabled verification certificate storage to conventional third-party auditing techniques, it is clear that environmental, social, and governance (ESG) reporting verification systems have made significant progress. Once verified, an ESG report's intrinsic security, transparency, and immutability guarantee that it presents an unquestionable and trustworthy picture of its veracity.

In 2024 Kumari, D., Parmar, A. S.,[22] Finding a workable and appropriate way to store massive amounts of medical data has piqued the interest of many experts, particularly when it comes to cloud storage with centralized structures. Nevertheless, there are several difficulties in putting cloud-based storage architecture into practice, including data ownership, failure tolerance, interoperability with other platforms, as well as worries about privacy and security. Therefore, a reliable architecture needs to be created in order to overcome all of these limitations.The suggested HealthRec-Chain design uses the Interplanetary File System (IPFS), a distributed file system technology, to automatically store encrypted health records with Java-enabled GPG encryption to provide high-level security and privacy. An experimental setup inside a pre-planned simulated situation serves as an illustration of the multi-layered technique of HealthRec chains.

In 2024 Lakshmanan, M., Mala, G. A.,[23] The researchers recommended using a blockchain-connected system to securely and extremely verifiably store patient health data. The optimal key is generated by the most sophisticated position-based Coot and Penguins search optimization method (MP-CPeSOA). Heterogeneity is addressed by the polynomial interpolation approach, which estimates values between two data points. Euclidean distance, concealment ratio, preservation ratio, correlation between the original and restored data, and patient health data security are all taken into account by the aim function. The digitally signed generated key in the model the researchers devised provides the highest level of security for the patient's medical records.

In 2024 Shahidinejad, A., Abawajy, J. [24] Patients can obtain ongoing care from several institutions with the assurance of guaranteed authenticity and traceability of authentication records after only one registration on a cloud server. The researchers conducted experimental evaluations using ARM and Hyperledger Fabric and provided both formal and informal verification of the proposed protocol in order to provide useful insights into security and performance. The most recent medical consortium authentication methods were examined in this research, along with their drawbacks, and an efficient blockchain-based solution that can withstand known attacks was then presented.

In 2024 Pei, H., Yang, P., Li, W.[25] For monitoring our general health and assisting medical professionals with patient care, the Internet of Medical Things, or IoMT, is crucial. Proxy Re-Encryption is a secure data sharing technique that researchers suggest combining with Blockchain technology to enable safe data exchange in the Internet of Medical Things (PRE-IoMT). IoMT data is shared via the BlockChain-based Proxy Re-Encryption (PRE) protocol. To enable secure IoMT data transfer between DO and DU, public and private keys must be generated during the key distribution stage. The proxy must be re-encrypted using the ID hash value following data exchange. In order to ascertain whether the ciphertext has changed the pairing mechanism, the researchers devised a technique to analyze the ciphertext of IoMT data using the CS.

Reference and researcher	Method	Third-Party	With/without Blockchain	Notes
[4] In 2024 Wang, F., Gai, Y et al.	Studying the attributes of a user's precise digital identity and big data management chains, reshaping blockchain information security.	no	With	high-level initiatives and global economic cooperation will get an upgrade. Growth in quality
[5] In 2024 Ren, Z., Yan, E. et al	They suggested a novel distributed KMS and zero-knowledge proof CP-ABE system based on blockchain technology. In order to overcome the difficulties that blockchain-based attribute-based cryptosystems face,	no	With	Better balances between computational and storage overhead, security features, and functionality are offered by the suggested solution.
[6] In 2024 Zhang, Z., Yu, G., Sun, C. et al.	The researchers demonstrated a trust-based DRL (TBDD) system that is intended to dynamically modify node allocation and mitigate the danger of collusion assaults.	IoT	With	Trust and ideal data flow are partially resolved by integrating sharded blockchain with IoT, but not fully.
[7] In 2024 Luo, F., Huang, R. et al.	They suggested HBMA, or blockchain-based multi-domain authentication for intelligent agricultural Internet of things networks. The CLC method will be used to investigate inter-IoT networks.	Internet of agricultural things	With	Organizations that monitor safety and produce agricultural products may work together across domains more easily thanks to the hybrid blockchain paradigm that this solution uses.
[8] In 2024 Wang, X., Zhang, H., Wu, H. et al.	They suggested an architecture for federated learning based on multilayer pooling (BMFL). A larger range of data can be shared by the Industrial Internet of Things (IIoT) thanks to federated learning (FL), which enables data owners to train neural networks together without sharing local data.	Industrial Internet of Things (IIoT)	With	It is necessary to solve the problem of model overloading time to improve the efficiency of the overall solution.

[9] In 2024 Zheng, W., Wang, X., et al.	They suggested a two-layer architecture known as S-DAG, which combines a DAG blockchain with a sharded blockchain.	IoT for the building	With	Parts overheating is effectively prevented by ABLA, while data query efficiency is marginally increased by 3D-Merkle trees.
[10] In 2024 Ismail, S., Nouman, M., et al.	To safeguard IoT sensor networks, researchers proposed an integrated security framework that combines blockchain technology with machine learning (ML).	Internet of Things	With	To guarantee the dependability and integrity of the network, consensus and transaction validation must be accomplished via a fault-tolerance mechanism.
[11] In 2024 García-Valls, M. et al.	The CoTwin middleware concept is showcased as a collaborative platform for creating and refining a DT model within a cyber-physical system including several interconnected cells.	no	With	Setting a maximum limit on the time behavior of individual processes is not feasible.
[12] In 2024 Ghani, M. A. N. U., She, K et al.	They put forth a methodology that addresses the crucial issues of preserving data integrity and privacy in facial recognition applications by combining Blockchain technology, microbatch aggregation, and Generative Adversarial Networks (GANs) in a synergistic manner.	Face recognition	With	The effectiveness of the algorithm in differentiating between actual and fake facial photos needs to be confirmed by researchers.
[13] In 2024 Alsaeed, N., Nadeem, F. et al.	They put up a fresh paradigm for collaborative authentication for IoMT (Internet of Medical Things) systems. There are four steps involved in implementing the	Internet of Medical Things (IoMT).	With	The suggested architecture ought to be more safe and impervious to potential assaults involving authentication. It is also observed that when the

	group authentication system: setup, registration, secret creation, and authentication.			number of submitted transactions rises, the average latency of the suggested framework stays within a fairly small range.
[14] In 2024 Alsaeed, N., Nadeem, F. et al.	The elliptic curve cryptography (ECC), Shamir's Secret Sharing (SSS) method, and blockchain-based fog computing techniques are combined in this proposed group authentication system.	Internet of Medical Things (IoMT).	With	When the quantity of submitted transactions rises, the average latency of the suggested framework stays within a relatively small range, suggesting that it facilitates scalability in the IoMT system.
[15] In 2024 Dong, Y., Li, Y. et al.	With editing and access control features, they put forth a decentralized blockchain system prototype.	no	with	Effective control over the dissemination of false information and unlawful access to information is made possible by the decentralized consortium blockchain technology.
[16] In 2024 Chen, J., Pu, C., Wang, P., et al.	Establish a decentralized management system based on blockchain to enable ECNs in TSN to collaborate autonomously.	no	With	Researchers need to be extremely cooperative managers since every node actively and voluntarily engages in the cooperation management process, but every node is an autonomous and self-serving agent.
[17] In 2024 Guo, H., Liang, H., Huang, J et al.	They have unveiled a new framework that can process non-fungible tokens (NFTs) individually and in batches, and it can also enable the simultaneous trade	no	With	By using federated learning, the researcher must intend to strengthen the security and privacy

	of fungible tokens.			assurances of this system.
[18] In 2024 Fan, J., Liu, D., Tang, G et al.	By leveraging distributed caching servers, a content delivery network (CDN) seeks to shorten the time it takes for material to reach end consumers. Large-scale caching server deployment and upkeep are highly costly.	IoT	With	In order to scale a CDN, no caching servers need to be deployed. End users can benefit from faster and less expensive content from nearby IoT devices; content providers (CPs) stand to get more cash from increased content views.
[19] In 2024	A blockchain-integrated enterprise e-commerce platform has been created by researchers, and it uses the PoA consensus process to build and approve new blocks in the system.	E-Commerce	with	It is necessary to enhance user authentication for the PoA distributed ledger. All newly produced blocks in the system are approved by validator blocks.
[20] In 2024	A dynamic multi-client searchable symmetric encryption (SSE) method has been proposed by researchers for the Internet of Things.	Iot	With	It presumes a trustworthy service supplier. adding new features including multi-keyword search and connected keywords, as well as extending the system to incorporate a malevolent service provider.
[21] In 2024 Liu, L., Ma, Z., et al.	In order to use incentive mechanisms to validate environmental, social, and governance (ESG) reports, researchers have developed a smart blockchain system.	AI	With	To confirm and enhance the researchers' practical solution in real-world environmental, social, and governance (ESG) reporting scenarios, extensive field studies must be carried out. It entails working

				with business partners to test the Veri-Green system and get input for ongoing enhancements.
[22] Kumari, D., Parmar, A. S.	Researchers have suggested storing and exchanging private medical records and photos using a patient-centric system called HealthRec-Chain.	Health	without	The feasibility of HealthRec-Chain is demonstrated by the development of a specially tailored Ethereum dashboard for performance tracking.
[23]In 2024 Lakshmanan, M., Mala, G. A.	The researchers suggested using a blockchain-connected system to securely store patient health data with strong verifiability. The most advanced position-based Coot and Penguins search optimization algorithm (MP-CPeSOA) produces the optimal key Health.	Health	with	The maximum level of protection for the patient's medical records
[24] Shahidineiad, A., Abawajy, J.	A blockchain-based authentication mechanism that greatly boosts the efficiency of computing, communication, and storage utilization on the blockchain while simultaneously thwarting potential assaults has been presented by researchers.	Health	Whit	Efficiency is increased in terms of communication and processing overhead. With this protocol, the blockchain's processing and storage overhead is significantly decreased.
[25] in 2024 Pei, H., Yang, P., Li, W.	To improve the security of data sharing in PRE-IoMT, they specifically suggested a novel method for proxy re-encryption data sharing. They achieved this by introducing identity	IoMT	with	It can successfully stop ciphertext kept on the cloud server from being altered.

	hashing at the key generation stage to accomplish the mapping between the public key and user identity.			

3. Blockchain and IoT-BIM integration for data

IoT defined by IBM Internet of Things, or IoT, is referred to a growing range of Internetconnected devices which captures or generate a large amount of information daily. From consumer wearables toindustry set machines that have sensors on their manufacturing equipment. This network includes the supply chain and other n-vehicle components[26].

Integrating Blockchain technology with the Internet of Things (IoT) is a concept that holds huge potential across various industries. Blockchain, a decentralized and secure ledger system, and the Internet of Things, a network of interconnected devices, together address critical challenges of data integrity, security, and trust in the digital ecosystem. Integrating these technologies provides a transparent, tamper-resistant layer for IoT data transactions Devices generate a significant portion of data, and ensuring the integrity of this data is crucial[27]. Blockchain achieves this by creating a decentralized, distributed ledger where every data transaction is recorded in a secure and immutable way. This not only enhances the reliability of the data, but also creates a transparent and auditable trail. Furthermore, Blockchain technology facilitates secure and automated smart contracts, enabling a self-executing contract based on pre-defined conditions. From an IoT perspective, this means that devices can autonomously participate in transactions or exchanges, operated according to pre-defined parameters without the need for intermediaries. This not only reduces transaction costs, but also enhances the efficiency and speed of IoT operations[28]. Using Blockchain with IoT is particularly important in sectors such as supply chain management, healthcare and cybersecurity, where trust, transparency and data integrity are of paramount importance. As research into this integration deepens, the potential for creating robust and secure IoT ecosystems using blockchain technology has become increasingly clear, paving the way for a new era of decentralized and trustworthy digital interactions[29]. The evolution of dynamic supply chains into off-site manufacturing offers a unique and compelling opportunity to adjust to shifts in market demand. That being said, new challenges and perspectives for improving workflows in logistics and production as well as increasing efficiency and process optimization are also brought about by this paradigm shift[30].

4. Description of the blockchain

Blockchain is defined as a distributed data structure (or) public ledger Introduced by Satoshi Nakamoto in 2008 as an important technology that underpins Bitcoin. Bitcoin is known as a cryptocurrency or digital currency in blockchain technology [1]. Blockchain is a public ledger that records all transactions with a growing list of records and is confirmed by the nodes participating in the blockchain [31]. It is solved by consensus and double-spending in a peer-to-peer network using a public-key cryptography algorithm [32]. Blockchain contains a series of blocks that contain data that records and stores a Bitcoin transaction. Each transaction has a set of rules to verify the transaction. The blockchain block will not disappear and change at a later time [33]. Blockchain is a series of blocks that stores a set of transactions for each node. Blockchain grows with additional blocks, represents a public ledger and stores all transaction history To create blockchain information systems, many blockchain consortia have been formed. Despite the potential of the blockchain information systems that have been created, only a few have succeeded in reaching the market[34]. In fact, due to the high complexity of the system and the lack of knowledge about how to design a system that meets the needs and provides value to all stakeholders, blockchain consortia have frequently lost their focus. As a result, stakeholders have had difficulty realizing the full potential of blockchain information systems. Previous research has shown that blockchain systems present organizational and technical problems[35].

There are some basic mathematical equations and concepts used in blockchain technology:

1. Hash Functions

A hash function H takes an input m and produces a fixed-size string h : $h = H(m)$

Where:

- m is the input message,
- h is the hash output (digest).

2. Proof of Work (PoW)

In PoW, miners find a nonce n such that the hash of the block header combined with the nonce is less than a target value T:

$H(Block\ Header + n) < T$

where:

- $Block\ Header$ includes the previous block hash, Merkle root, timestamp, etc.
- n is the nonce,
- T is the target difficulty.

Digital Signatures (Elliptic Curve Digital Signature Algorithm - ECDSA)

ECDSA is used for signing transactions and verifying signatures.

Signing

Given a private key d and a message hash z

Choose a random integer k from $(1, n-1)$,

Calculate the point $(x1, y1) = k . G$,

Compute $(r = x\_1 \bmod n)$,

Compute $(s = k\^{-1}(z + r\ cdot\ d) \bmod n)$.

The signature is (r, s).

3. Verification Given a public key Q message hash z and signature (r, s):

Compute $(w = s\^{-1} \bmod n)$,

Compute $(u\_1 = z\ cdot\ w \bmod n)$ and $(u\_2 = r\ cdot\ w \bmod n)$,

Calculate the point $(x\_2, y\_2) = u\_1\ G + u\_2 . Q$

Verify $(r\ equiv\ x\_2 \bmod n)$.

4. Merkle Trees A Merkle tree is a binary tree that is used to efficiently and securely verify the integrity of large sets of data.

Leaf Nodes

Each leaf node is a hash of a transaction

$L\_i = H(T\_i)$

Parent Nodes

Each parent node is a hash of its two child nodes:

$P\_i = H(L\_\{2i\} + L\_\{2i + 1\})$

5. Block Hash

A block is valid if its hash is less than the target value. The block hash is calculated as:

$(Block\ Hash) = H\ (Block\ Header)$

where:

- (text{Block Header}) includes the previous block hash, Merkle root, timestamp, nonce, etc.

6. Difficulty Adjustment

The difficulty of finding a valid block is adjusted to ensure a consistent block generation time. The new difficulty $D\ \ new$ is adjusted based on the actual time $T\ \ actual$ taken to generate the blocks and the desired time $(T\_\{text\{desired\}\}$:

$D\_\{text\{new\}\} = D\_\{text\{old\}\}$ times frac $T\_\{text\{desired\}\} T\_\{text\{actual\}\}$

where:

$D\_\{text\{old\}\}$ is the current difficulty,

$T\_\{text\{desired\}\}$ is the target block time,

$T\_\{text\{actual\}\}$ is the actual time taken to mine the blocks.

These equations and concepts are fundamental to the operation and security of blockchain technology, ensuring data integrity, secure transactions, and decentralized consensus.

Mechanisms of Consensus: Different consensus algorithms have their own formulas, such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). Equations include probability distributions, stake calculations, and voting mechanisms.

These equations and concepts form the basis of blockchain technology, which enables safe, transparent, and decentralized systems for a variety of applications beyond bitcoin, including voting, supply chain management, and healthcare.

5. Conclusion

Because so many sensors are used in healthcare applications, networks connected to the Internet of Things (IoT) need to be securely connected. Sensitive sensor data may include extremely private information such as vital signs, clinical notes, medical diagnoses, and patient health data, to name just a few. The introduction of blockchain technology is currently viewed as an innovative way to achieve significant scalability, data integrity, and privacy because it ensures consensus and confidence across systems. This article provided a clear comparison of several IoT journals based on many studies. This study will help scientists and academics learn more about blockchain applications and offer recommendations for the best ways to safeguard privacy.

Future Work Improved consensus is an important issue in Blockchain network. The networks connected to the Internet of Things (IoT) must be securely connected and the ability to create a secure and effective digital mix between the combination of blockchain technology, the Internet of Things and e-commerce.

FUNDING

None

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.
[3] T. R. Gadekallu et al., "Blockchain for the metaverse: A review," arXiv preprint arXiv:2203.09738, 2022.
[4] F. Wang, Y. Gai, and H. Zhang, "Blockchain user digital identity big data and information security process protection based on network trust," Journal of King Saud University-Computer and Information Sciences, vol. 102031, 2024.
[5] Z. Ren, E. Yan, T. Chen, and Y. Yu, "Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof," Journal of King Saud University-Computer and Information Sciences, vol. 101969, 2024.
[6] Z. Zhang et al., "TBDD: A New Trust-based, DRL-driven Framework for Blockchain Sharding in IoT," arXiv preprint arXiv:2401.00632, 2024.
[7] F. Luo, R. Huang, and Y. Xie, "Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks," Journal of King Saud University-Computer and Information Sciences, vol. 101946, 2024.
[8] X. Wang, H. Zhang, H. Wu, and H. Yu, "Dual-blockchain based multi-layer grouping federated learning scheme for heterogeneous data in industrial IoT," Blockchain: Research and Applications, vol. 100195, 2024.
[9] W. Zheng et al., "Data management method for building internet of things based on blockchain sharding and DAG," Internet of Things and Cyber-Physical Systems, 2024.
[10] S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, "Towards a lightweight security framework using blockchain and machine learning," Blockchain: Research and Applications, vol. 5, no. 1, p. 100174, 2024.
[11] M. García-Valls and A. M. Chirivella-Ciruelos, "CoTwin: Collaborative improvement of digital twins enabled by blockchain," Future Generation Computer Systems, 2024.
[12] M. A. N. U. Ghani et al., "Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition," Journal of King Saud University-Computer and Information Sciences, vol. 102036, 2024.

[13] N. Alsaeed, F. Nadeem, and F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing," Future Generation Computer Systems, vol. 151, pp. 162-181, 2024.
[14] S. Rashidibajgan and T. Hupperich, "Utilizing blockchains in opportunistic networks for integrity and confidentiality," Blockchain: Research and Applications, vol. 5, no. 1, p. 100167, 2024.
[15] Y. Dong, Y. Li, Y. Cheng, and D. Yu, "Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption," High-Confidence Computing, vol. 4, no. 1, p. 100168, 2024.
[16] J. Chen, C. Pu, P. Wang, X. Huang, and Y. Liu, "A blockchain-based scheme for edge–edge collaboration management in time-sensitive networking," Journal of King Saud University-Computer and Information Sciences, vol. 36, no. 1, p. 101902, 2024.
[17] H. Guo et al., "A framework for efficient cross-chain token transfers in blockchain networks," Journal of King Saud University-Computer and Information Sciences, vol. 101968, 2024.
[18] J. Fan, D. Liu, G. Tang, K. Wu, and X. Shao, "Intelligent edge CDN with smart contract-aided local IoT sharing," High-Confidence Computing, vol. 100225, 2024.
[19] S. Asaithambi et al., "Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs," Egyptian Informatics Journal, vol. 25, p. 100444, 2024.
[20] N. H. Sultan et al., "Securely sharing outsourced IoT data: A secure access and privacy preserving keyword search scheme," Ad Hoc Networks, vol. 158, p. 103478, 2024.
[21] L. Liu, Z. Ma, Y. Zhou, M. Fan, and M. Han, "Trust in ESG Reporting: The Intelligent Veri-Green Solution for Incentivized Verification," Blockchain: Research and Applications, vol. 100189, 2024.
[22] D. Kumari et al., "HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data," Computer Networks, vol. 110223, 2024.
[23] M. Lakshmanan, G. A. Mala, and K. M. Anandkumar, "Highly secured EHR management system based on blockchain technology with digitally signed authentication using data sanitization and polynomial interpolation," Biomedical Signal Processing and Control, vol. 87, p. 105412, 2024.
[24] A. Shahidinejad, J. Abawajy, and S. Huda, "Untraceable blockchain-assisted authentication and key exchange in medical consortiums," Journal of Systems Architecture, vol. 103143, 2024.
[25] H. Pei, P. Yang, W. Li, M. Du, and Z. Hu, "Proxy re-encryption for secure data sharing with blockchain in Internet of Medical Things," Computer Networks, vol. 110373, 2024.
[26] R. Brandín and S. Abrishami, "IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing," Automation in Construction, vol. 159, p. 105266, 2024.
[27] X. Liang et al., "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 468-477.
[28] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, pp. 1575-1578.
[29] A. Khatoon, "A blockchain-based smart contract system for healthcare management," Electronics, vol. 9, no. 1, p. 94, 2020.
[30] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for eHealth data access management," in 2017 fourth international conference on advances in biomedical engineering (ICABME), 2017, pp. 1-4.
[31] C. Celli, National identity in global cinema: How movies explain the world. Springer, 2016.
[32] N. P. De Leon et al., "Materials challenges and opportunities for quantum computing hardware," Science, vol. 372, no. 6539, p. eabb2823, 2021.
[33] F. Bob et al., "Is kidney stiffness measured using elastography influenced mainly by vascular factors in patients with diabetic kidney disease?" Ultrasonic Imaging, vol. 40, no. 5, pp. 300-309, 2018.
[34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," p. 21260, 2008.
[35] H. Jin, S. Dong, X. Dai, Y. Cai, and J. Xiao, "Dispatcher: Resource-aware nakamoto blockchain via hierarchical topology and adaptive incentives," Distributed Ledger Technologies: Research and Practice, vol. 3, no. 2, pp. 1-20, 2024.