Multidisciplinary Journal of Akseprin Indonesia
Website : https://jurnal.akseprin.org/index.php/MJAI/about
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)

ISSN 3025-0129 (online)
Pages 01-08, Vol. 2, No. 3, 2024

Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

Blockchain Technology for the Internet of Things and Future Cyber Security

Ahmed Mohammed[1], Rawaa Mohammed Abdul[2]
[1,2] Mustansiriyah University Baghdad, Iraq

ABSTRACT

The purpose of this study is to make an attempt at doing a full survey of blockchain technology by describing its structure in addition to several consensus methods. They also investigate the difficulties and potential benefits associated with the Internet of Things and cyber security. In addition, they investigate potential future developments that the technology may accommodate in the next few years. The Internet of Things (IoT) aims to create a vast network of devices that generate and share data to enable intelligent interactions between people and their surroundings. The IoT is open, heterogeneous, and dynamic and might speed up real-time applications. These traits raise security, privacy, and trust issues. Thus, these issues limit IoT technology adoption. On the other side, Cybersecurity keeps unwanted people from getting into digital devices, networks, and data. This makes it less likely that data will be stolen or changed. It is about methods, processes, and routines that are carefully made to protect personal information and stop hacking. Cybersecurity has grown a lot because of cyberattacks. Cybersecurity tools include filters, encryption, secure passwords, and systems that look for threats and tell people what to do about them. Workers must learn how to do these things. The integration of blockchain technology with the Internet of Things (IoT) and cyber security serves to mitigate risks and enhance capabilities. This article presents a comprehensive analysis of blockchain security risk categories, drawing upon the intersection of Internet of Things (IoT) and cybersecurity challenges. Additionally, this study investigates the unique dangers and weaknesses associated with blockchain technology, as well as the security solutions designed to mitigate these risks. The use of blockchain technology in the domains of Internet of Things (IoT) and cyber security is advantageous owing to its attributes of openness, auditability, consistency, and security.

Keywords: Blockchain; Cybersecurity; Internet of Things.

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)

Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

INTRODUCTION

The contemporary worldwide market necessitates enhanced production efficiency, advanced military capabilities, and intelligent infrastructure for residential, industrial, and urban sectors. The proliferation of the Internet of Things (IoT) has resulted in a heightened need for IoT devices; nevertheless, these devices are not without their limits [1]. These constraints include the generation of substantial volumes of data, energy consumption concerns, and challenges pertaining to trust and security. The advent of blockchain technology, first proposed by the inventor of Bitcoin, Nakamoto, has facilitated the execution of transactions that are characterized by enhanced security, immutability, and verifiability. The BC-IoT system, which is a decentralized and user-friendly database, is used for the purpose of executing transactions [2]. The Internet of Things (IoT) refers to a networked infrastructure including linked equipment capable of autonomously exchanging data, hence enhancing operational efficiency, productivity, and safety. Nevertheless, the proliferation of internet-connected devices on the Internet of Things (IoT) gives rise to security concerns, as these devices become potential targets for exploitation by malicious actors. The issue of interoperability arises in the context of Internet of Things (IoT) devices since they engage in unauthorized data sharing. Blockchain technology effectively mitigates the challenges by rectifying inherent faults in centralized systems, mitigating the risk of server failures, and minimizing the potential for single-point errors. The precise mechanism of transmitting agreement remains a subject of continuing research, whereas blockchain networks demonstrate adaptability and security via the use of cryptographic techniques [3].

. E-commerce has raised data security vulnerabilities, placing online firms in danger, particularly those that provide tickets, trip reservations, and financial transactions to suit customer demand. Online companies must adopt cybersecurity measures to combat cybercrime and promote its benefits. Despite substantial financial expenditures and meticulous cybersecurity efforts by organizations, persistent hackers assault corporate operations, infiltrating critical data and damaging organizational components. These attacks interrupt networks and traffic by targeting data storage devices and applications. Blockchain technology streamlines business procedures and protects firm data [4]. Cybersecurity and IoT are similar technologies. Blockchain technology speeds up data and security improvements and typically involves hackers. Blockchain reduces cybersecurity risks by encrypting data, authenticating ownership, and assessing validity. Its decentralized data ledger protects data but exposes platform flaws, As well as Blockchain consensus algorithm detects and fixes data weaknesses, improving data quality and communication. Encryption and digital signatures protect linked devices from hacking [5].

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)

Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

A significant number of surveys dealing with blockchain, internet of things, and cybersecurity are now available. However, there are not enough comprehensive studies in the existing body of research that investigate in a single article the intersection of IoT-based blockchain technology and cybersecurity-based blockchain technology. Additionally, there are not enough studies that investigate the actual use of blockchain technology in the fields of IoT and cybersecurity. In this section, we present a short review of many survey papers relevant to the usage of blockchain technology in current applications. These papers were published between the years 2017 and 2023 and cover a range of topics related to the use of blockchain technology in modern applications.

Devulkar and Awwad review Blockchain and IoT technologies, examining integration, challenges, and potential applications. [6]. Ferrag analyzes IoT blockchain protocols, compares methodologies, and compares safe technologies. [7]. Tanwar et al. explore blockchain technology and IoT security challenges, examining recent developments in IoT security research using blockchain-related methodologies and technologies. [8]. Bhutta et al. analyze Blockchain's evolution, architecture, development frameworks, security, consensus techniques, and cryptographic primitives, highlighting future paths and research problems. [9]. Ali et al discuss state-of-the-art activities in secure IoT ecosystem, focusing on blockchain basics, decentralized networks, and challenges faced by centralized models. They discuss industry and academic breakthroughs [10]. Atlam et al discuss IoT and blockchain integration, highlighting advantages and potential solutions. They introduce blockchain as a service for IoT, AI integration, and future research directions. [11]. Krichen et al. explore blockchain's applications in banking, healthcare, information systems, wireless networks, IoT, smart grids, government services, and military, addressing challenges and potential improvements. [12].

Chen et al. divided research into four sections: access control, data security, trustworthy third party, and automated payment, focusing on blockchain's role in IoT systems and potential applications in academics and engineers [13]. Guru et al discuss blockchains, construction, and consensus techniques, highlighting their limitations and potential applications in smart healthcare, smart grid, and financial systems. They discuss data breaches, denial of service attacks, and challenges. [14]. D. Guru et al compares blockchain's tradeoffs, describes its taxonomy and design, compares consensus processes, and examines scalability, privacy, interoperability, energy consumption, and regulatory difficulties. This study also discusses blockchain's future [15]. Alzoubi et al. analyze peer-reviewed literature on Blockchain-IoT integration issues, identifying solutions and highlighting outstanding issues for future developments [16]. P.Karthikeyan and S.Velliangiri discuss IoT security in blockchain-based applications across industries, addressing security issues and eBusiness models, and assisting researchers in developing secure IoT applications [17]. Qamar and Zardari discuss IoT's

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)
Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

challenges, including sensitive data, privacy, and security, and explore blockchain and IoT's potential to overcome flaws and maximize benefits. [18]. Alkhateeb et al. conducted a literature review on hybrid blockchains, focusing on security, transparency, and efficiency in various industries. They found advantages and problems in cloud, fog, telecom, and edge computing [19]. Ghuli et al. propose a peer-to-peer technique for identifying IoT device ownership in the cloud, using Genesis as the device's producer and blockchain for device ownership transfer without third parties. [20]. Aggarwal et al. discuss IoT with blockchain, its characteristics, architectural layout, and potential solutions for real-world issues [21]. The following sections are organized as follows: Section 2 describes Block chain background. Section 3 presents the internet of things, and Section 4 presents the cyber security discussion. Finally, Section 5 the conclusions and future work.

RESEARCH ELABORATIONS

In his 1982 dissertation, David Chaum introduced a technique that had similarities to a blockchain. As per the findings of reference [2], the individual expressed a desire to develop a technique for safeguarding the integrity of document timestamps. In 1992, Haber, Stornetta, and Dave Bayer made the inclusion of Merkle trees into the protocol. The protocol's efficiency was enhanced by the consolidation of several documents into a unified block and the use of document hashing to ensure the integrity of the documents [2]. The decentralized blockchain was conceived by Satoshi Nakamoto in 2008. The use of hash algorithms inside timestamp blocks has effectively reduced the need for document signing, hence enhancing the concept. The design implemented bitcoin technology in the subsequent year. In 2016, a worldwide conference was established by trade organizations specializing in Business Continuity (BC). Blockchains, often known as BCs, refer to a kind of decentralized ledger consisting of cryptographically linked data blocks. As stated by the source referenced as [24], every block comprises a cryptographic hash of the preceding block, a timestamp, and transaction data. The process of hashing and encoding transactions results in the creation of a Merkel tree for every block. Each block inside a blockchain has a cryptographic hash that serves the purpose of connecting it to the preceding block. The blocks are interconnected in a chain-like formation. The iterative methodology assesses both the preceding block and the genesis block. Each transaction inside a system is associated with a hash value, a previous hash value, and a set of data [5]. The peer-to-peer (P2P) network functions as a decentralized ledger, overseeing the management of the blockchain (BC). The communication and verification of new blocks among nodes is facilitated using a protocol. The safety of blockchain records is ensured by their immutability. Blockchain (BC) is a technique for fault-tolerant distributed computing. Satoshi included blockchain technology into Bitcoin, so establishing it as the pioneering digital

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)
Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

currency effectively addresses the issue of double spending without reliance on a centralized server or trusted intermediary.

A-immutability: After being committed to the blockchain, data cannot be altered, thus the term "immutability." Blockchain (BC) data is immutable and cannot be altered. This is because a transaction must be approved by all nodes in the network before it can be recorded. As a result, this verification procedure strengthens anti-corruption measures and fosters openness . B-Decentralization refers to the absence of a central controlling authority or individual. The network is decentralized because of a collective of nodes responsible for its maintenance. Therefore, given the absence of a governing body, it is possible to directly access the system and store various items such as cryptocurrency and documents [6]. C- Boosting security: No one can modify network attributes to her benefit when the BC removes the central authority. Cryptography protects the system using complicated mathematical procedures and an attack firewall. These mathematical procedures provide a single length, which changes all hash IDs whenever the data changes. D- Distributed ledger: - Information on the parties involved in a transaction may be found in a distributed ledger. Because the ledger is hosted on the network, all users contribute to its upkeep, and anybody may verify the accuracy of its entries at any time. E- Consensus: - Consensus algorithms are the fundamental basis of blockchain technology. Every block has a consensus mechanism that aids the network in reaching choices. Consensus refers to the method through which a group of active nodes on a network make decisions.

A- public blockchain: It is an open distributed ledger, thus anybody may join onto the BC platform and become a certified node. It lets nodes and users check transactions, validate records, prove work as an incoming block, and mine. Bitcoin and Ethereum are BC networks. B- Private blockchain Because it is a closed network, it requires authorization to use, BC network members. The governing organization controls security, permissions, and accessibility. Thus, private BC are like public ones but have a tiny network. Voting, digital identification, access ownership, etc. [3]. C- Consortium blockchain: Unlike private BCs, it is semi-decentralized and runs several organizations. Nodes may cycle to multiple institutions. BC, community and government organizations, and banks are utilized for information exchange and mining. Energy Web Foundation, R3, etc. D- hybrid Blockchain: It permits one to have a private ear-based system and a public system without authorization. A hybrid network lets users decide who may access BC's data and share just a piece of it. Hybrid systems are secure, flexible, and transparent. Dragonchain is hybrid BC.

The Internet of Things (IoT) is a network of connected devices with sensors and processors that exchange data. In populated metropolitan areas, small-scale IoT sensors can monitor vehicle movement and provide recommendations. Security measures must be designed

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)
Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

to counter potential attackers. Various ad hoc IP protocols, such as NFC, Bluetooth, IEEE 802.15.4, Wi-Fi, ZigBee, and 6LoWPAN, are identified as potential communication methods between devices. The Internet of Things (IoT) has the potential to simplify daily life across a variety of application domains based blockchain.

RESULTS AND DISCUSSIONS

A decentralized, peer-to-peer Blockchain Platform for Industrial Internet of Things (BPIIoT) may improve Cloud-based Manufacturing (CBM) production security. CBM operators modify manufacturing equipment. BPIIoT uses blockchain smart contracts for upon-demand manufacturing equipment and service customers sign smart contracts. BPIIoT integrates shop floor equipment into cloud-based settings, boosting decentralized and peer-to-peer production software. Distributors must trust IoT component makers. Product completion demands confidence.

IoT healthcare applications and services continuously monitor patient healthcare requirements. Healthcare might benefit from cloud data. Smart hospital technologies protect health records while Highdimensional images need more bandwidth. Decision fusion may reduce accuracy due to rounding errors in raw sense data analyses, which rely on sensor processing. More-powerful sensor network gateways improve data fusion. Decision fusion is sensor-driven, and data fusion monitors require electricity to deliver high-dimensional data. Radio signals need more power than CPUs

Blockchain technology could enable smart cities due to IoT proliferation, generating data through core and edge networks. Peripheral devices have low capacity and low processing, while mining nodes have high capacity. Edge nodes and centralized servers provide key services and boundaries in blockchain-based smart cities. Dispersed work may increase flexibility and reduce assaults, but edge node breaches must be isolated. Smart cities face challenges in latency, bandwidth, safety, privacy, and scalability

Blockchain technology distinguishes smart houses from conventional IoT homes. The British Columbia smart home system has an Access power List (ACL) that provides the user control over anything in her property. The miner produces a shared key so devices may communicate, following the owner's restrictions. The British Columbia smart home system receives minimal IoT data. It also protects data security, availability, and privacy against DDoS assaults.

There are benefits to building Blockchain based IoT applications. Blockchain technology can improve the Internet of Things (IoT) ecosystem by ensuring data security and accuracy. It decentralizes the system, allowing devices to connect through servers. Blockchain records are straightforward, preventing human overwriting, and IoT-based applications can

Multidisciplinary Journal of Akseprin Indonesia ISSN 3025-0129 (online)
Website : https://jurnal.akseprin.org/index.php/MJAI/about Pages 01-08, Vol. 2, No. 3, 2024
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)

Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

exchange information securely [3]. In contrast Due to limited processing capability, PoW, PoS, and vote-based consensus protocols are inappropriate for the Internet of Things (IoT). The consensus process slows transactions, making it inappropriate for real-time IoT situations. Most IoT devices are deployed on cloud servers

CONCLUSIONS

This study surveys blockchain technology, its structure, and consensus methods. It explores the challenges and potential benefits of the IoT and cyber security. IoT aims to create a vast network of devices for intelligent interactions, but security, privacy, and trust issues limit adoption. Blockchain technology has facilitated transactions with enhanced security, immutability, and verifiability. Cybersecurity aims to protect personal information and prevent hacking. Blockchain technology mitigates these challenges by encrypting data, authenticating ownership, and assessing validity.

ACKNOWLEDGEMENTS

Please acknowledge collaborators or anyone who has helped with the paper at the end of the text.

REFERENCES

[1] Dwivedi, Vimal, Mubashar Iqbal, Alex Norta, and Raimundas Matulevičius. "Evaluation of a Legally Binding Smart-Contract Language for Blockchain Applications." Journal of Universal Computer Science 29, no. 7 (2023): 691.

[2] R. boomsom, Vichayanan, Muhammad Saleem Korejo, Javed Ali, and Uthen Thatsaringkharnsakun. "Blockchain-Enabled Internet of Things (IoT) Applications in Healthcare: A Systematic Review of Current Trends and Future Opportunities." International Journal of Online & Biomedical Engineering 19, no. 10 (2023).

[3] Abu Jahid, Mohammed H. Alsharif, Trevor J. Hall, “The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap,” Journal of Network and Computer Applications, Volume 217,2023.

[4] Deepika, P., and R. Agusthiyar. "A Systematic Review of Security Solutions for IoT Smart Environment with Defense Methods and Mitigation against Various Attacks–Brief Review." Harbin Gongcheng Daxue Xuebao/Journal of Harbin Engineering University 44, no. 8 (2023): 77-104.

[5] Al-Qahtani, Abdulrahman Saad Saeed A. "Towards Knowledge-Based Economy: Assessing the Ecosystem and Value Creation Drivers Through Cybersecurity, Intangible

Multidisciplinary Journal of Akseprin Indonesia
Website : https://jurnal.akseprin.org/index.php/MJAI/about
e-mail : akseprin@gmail.com or mai@akseprin.org
PUBLISHER: Akademi Sertifikasi Profesi Internasional (AKSEPRIN)
ISSN 3025-0129 (online)
Pages 01-08, Vol. 2, No. 3, 2024
Received: 2023-08-09 Revised: 2023-10-19 Accepted: 2023-11-01 Published: 2024-09-30

Assets and Blockchain Technology in Qatar." PhD diss., Hamad Bin Khalifa University (Qatar), 2023.