Indian Journal of Data Communication and Networking (IJDCN)
ISSN: 2582-760X (Online), Volume-3 Issue-1 December 2022

A Review on IoT Blockchain Technology

Neenu Kuriakose, Divya Midhunchakkaravarthy

Abstract: ***Our lifestyles are increasingly incorporating the Internet of Things. Every year, a growing number of gadgets gain connectivity and communication capabilities via the Internet. There are currently more than 400 million IoT devices in use worldwide, and by 2025, that number is anticipated to reach 1.5 billion. Keeping track of all IoT devices and figuring out which one to connect to in order to make service requests is getting more and more challenging. The device could also end up malfunctioning or performing poorly. We must determine the most effective method of data storage in order to provide the groundwork for how to build trust amongst devices.***

Keywords: IoT, Blockchain, Network

I. INTRODUCTION

IoT: What is it? In 1999, Kevin Ashton created the phrase "Internet of Things (IoT)" to describe supply chain management. IoT, according to his definition, is a network that links the Internet to physical objects [1]. However, as technology has developed, more definitions have been created in recent years to encompass more IoT applications. These definitions cover a wide range of uses, including transportation and healthcare. According to Gubbi et al., the Internet of Things (IoT) is a network of objects that collects data from the environment and the physical world and offers data transfer analytics and communication [1]. In this scenario, objects are gadgets that communicate with one another via Bluetooth, Wi-Fi, radio frequency identification, or other technologies [1]. IoT is defined as Objects that are Actively Participating in Information Sharing, Social Processes, and Business by the Cluster of European Research Projects [2]. They can communicate with one another, interact with the environment, and use other devices during this process [2]. Items include appliances, utilities, and sensors for air quality monitoring. IoT, on the other hand, is described by Forrester [3] as a smart setting that is utilised in public utilities, healthcare, and transportation. IoT creates infrastructures that can interact with their surroundings and are aware of it [3]. As a result, the system as a whole is more time-efficient.

Manuscript received on 15 July 2022 | Revised Manuscript received on 25 November 2022 | Manuscript Accepted on 15 December 2022 | Manuscript published on 30 December 2022.
*****Correspondence Author(s)

Neenu Kuriakose*, Ph.D. Scholar, Lincoln University College, Malaysia. E-mail: neenuannaa@gmail.com, ORCID ID: https://orcid.org/0000-0002-9942-2160

Dr. Divya Midhunchakkaravarthy, Associate Professor, Department of Computer Science, Lincoln University College, Malaysia.

II. LITERATURE REVIEW

IoT is divided into four key categories by Gubbi et al., including personal and household, business, utilities, and mobile devices [1]. Only the individual, household members, or carers with access to the healthcare applications have access to personal and home IoT information. In an enterprise setting, the data is accessible to the owners of the data and can be distributed to third parties on a judicious basis. IoT for utilities often uses the data for service optimisation rather than for customer service. Smart logistics and transportation are referred to as mobile IoT services by Gubbi et al. [1]. Sensors can be used to measure air pollution and forecast traffic jams. Atzori et al. performed a further division of IoT into various categories, classifying it into three distinct paradigms: Internet oriented in sense of middleware, things oriented as sensors, and semantic oriented as knowledge [4]. According to Gubbi et al. [1], the phrase "Internet of Things" (IoT) refers to a network or system of stationary and mobile devices that may connect with one another. However, we will refer to gadgets like laptops and smartphones that can switch between networks as mobile devices.

IoT became widespread in 2011, and by 2013 there were 9 billion connected devices. By the end of 2025, that number will rise to 24 billion, according to Gubbi et al. [1]. The volume of data that needs to be processed, the processing power of the majority of IoT devices, and the heterogeneity of devices within the same network become more challenging as the number of IoT devices increases yearly. Devices connected to the same network frequently employ many network protocols and communication techniques. There is a chance that one device will have a variety of alternatives for communication and data sharing with other devices, even when communication standards are established. To address these issues, it is necessary to develop better methods for storing and analyzing data that is being transferred [5].

IoT links people, computers, and other electronic devices with physical objects. Gubbi et al [1] example of how IoT might connect people in the medical industry with patient data involves a patient having a gadget that measures vital signs and sending the information to a doctor. Real-time data monitoring enables doctors to respond to patient symptoms. By identifying symptoms early and acting before a patient's condition worsens, this can lower inpatient expenditures [1]. Also, it can lessen the number of required doctor visits and notify medical staff in an emergency so that a patient can receive treatment as soon as possible.

III. BLOCKCHAIN

Data is kept in blocks owing to a technology called blockchain. Transaction data is permanently saved in blocks, which are files. These details include the list of transactions, the block size, the block header, and the counter. A cryptographic hash of the previous block is contained in each block. A person or people using the alias Satoshi Nakamoto invented the first blockchain implementation, which was Bitcoin. Under that heading, a white paper [6] was released in January 2008. Although Nakamoto claimed to be a man from Japan, there are suspicions that the paper's author is a native English speaker given the paper's excellent English [6]. Moreover, some claimed that it was jointly produced by Samsung, Toshiba, Nakamichi, and Motorola [7]. By using a few letters from each of the four names (Sa-Toshi Naka-Moto), the name Satoshi Nakamoto may serve as an abbreviation for those four businesses [7]. Another hypothesis is that Satoshi Nakamoto was actually Craig Wright, an Australian computer scientist and businessman. He offered the encryption key used in the initial Bitcoin transactions between Satoshi and Hal Finney in 2009 [8] as proof.

Bitcoin transactions are recorded in the public ledger known as Blockchain [6]. Transactions are kept in the digital ledger. A transaction, in general, is a verified occurrence that was recorded in a blockchain [6]. A transaction might include, for instance, transmitting cryptocurrency to another user. Each Bitcoin currency is represented as a chain of digital signatures; each owner adds their digital signature from the prior transaction and the new owner's public key to the end of the coin. A transaction in the Bitcoin blockchain is when one user transfers cryptocurrency to another user; the first transaction in the Bitcoin blockchain occurred in 2009 [9] between Satoshi and Hal Finney. Yet, a transaction can differ from blockchain to blockchain based on the blockchain's intended use. Blockchains used in finance often store bitcoin and money transactions; in contrast, a blockchain utilised in healthcare may store medical records. It verifies transactions using public-key cryptography by assuring that the digital signature originated from an owner's private key. Each distributed ledger comprises a connected block that creates a blockchain, which is where the data is kept. [10]

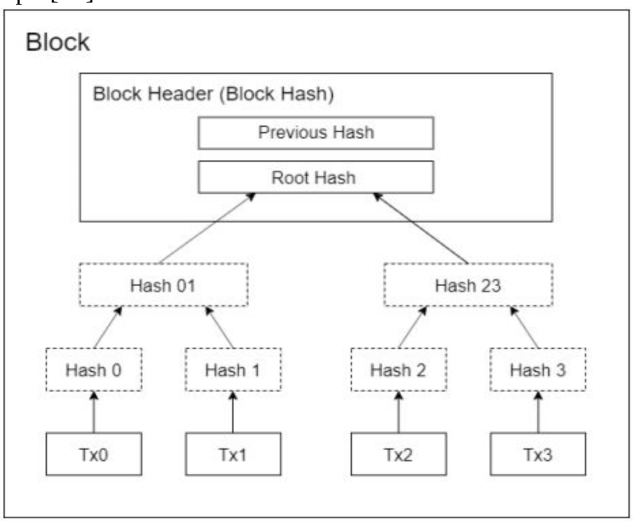

Figure 2.1: Merkle Tree-This figure shows a Markle Tree structure for one block in the blockchain. In this graph, four different text inputs are hashes in four different hash values, and then values are appended and hashed into parent nodes until the root. The root contains the hash values of all children. Based on [1].

Each block contains data inside a Merkle tree structure that has been hashed and encoded. Figure 2.1 depicts the structure of a Merkel tree. Every left node of a Merkle tree is labelled with the hashes of the data block, and the labels of its child nodes' cryptographic hashes are found on the right nodes of the tree. The result of a hash algorithm, also known as a message digest, is an alphanumeric string that has a predetermined length (number of bits) and is made from the transaction data [11]. SHA-256 is the most widely used hashing algorithm [12]. The Bitcoin protocol uses the SHA-256 algorithm, which was created by the National Security Agency (NSA) of the United States [13], to generate private keys and to conduct mining operations [6]. This hashing algorithm was chosen due to the hash's randomness, which means that by changing only one character, the hash will change entirely. Figure 2.2 displays the SHA-256 algorithm's randomness. Several hashing algorithms are employed in blockchains; for instance, the Darkcoin protocol makes use of the X11 hashing algorithm, which Evan Duffield created in 2014 [14].

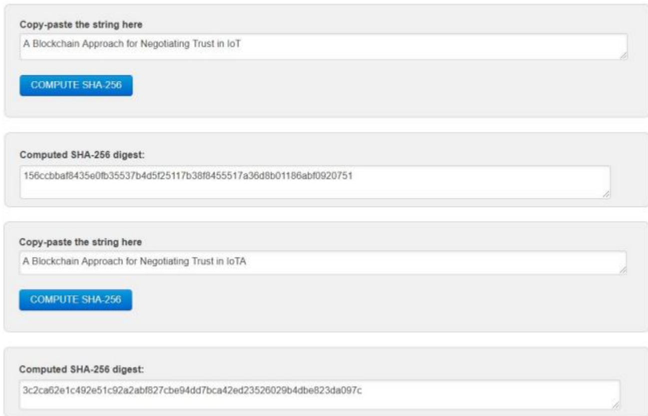

Figure 2.2: SHA-256 Hashing - The image demonstrates how adding a single character entirely alters the hash output, making it impossible to compare it to the original hash. We only added the letter "A" at the end of the image, so the output hash cannot be compared to earlier hash output [4].

The Merkle tree is employed for cryptographic functions like digital signatures and authentication. Full binary trees and infinite trees of one-time signatures are the two primary types of Merkle trees. The parent node's value in a complete binary tree is a one-way function of the values of its offspring. Each node in a tree that employs digital signatures with cryptographic functions has verification parameters that can be used to sign messages and to confirm the identity of the node's progeny [15].

IV. BLOCKCHAIN NETWORK TYPES

Blockchain networks come in two flavours: permissioned and permissionless. All nodes in a network can participate in permissionless blockchains, also known as public ones,

Retrieval Number: 100.1/ijdcn.F37190811622
DOI: 10.54105/ijdcn.F3719.123122
Journal Website: www.ijdcn.latticescipub.com

Published By:
Lattice Science Publication (LSP)

Indian Journal of Data Communication and Networking
IJDCN
Exploring Innovation
www.ijdcn.latticescipub.com

while only a limited number of nodes can participate in permissioned blockchains as validators or miners. Everyone can join in permissionless blockchain, which aids in protecting participants' anonymity. Using a public address and public and private keys that are not directly associated with the user's identity can help to maintain anonymity [6]. Anyone can start a Bitcoin mining operation or engage in Bitcoin trading, making it an example of a permissionless blockchain.

Permissioned blockchain offers decentralization, but there are limitations on who can participate in it. Ripple [16], for example, allows participation from anybody who registers, but other permissioned blockchains only enable approved users, frequently only those inside the network. Private blockchains are another name for permissioned blockchains. Being a hybrid permissioned blockchain where everyone can join, Ripple is seen as such. Certain validators do, however, serve as a centralized authority. Validators are frequently chosen by the network as trusted nodes, and anyone can apply to be one. Additionally, there are open-source public blockchains like Ethereum that let individuals create their own customized private blockchain. Private blockchains are primarily used in homes and businesses where data sharing is not allowed. Immutable records, anonymity, and real-time record changes are features common to most blockchain technologies [17]. Blockchain does not need a central authority and can be totally decentralized, in contrast to conventional database storage, which needs an administrator for "quality" control. Blockchains even include algorithms that can settle disputes when they arise without the intervention of a higher authority. These resolution procedures are frequently incorporated into consensus protocols, and they frequently settle two different types of disputes: disputes over the information contained within a block and disputes regarding blocks in a blockchain. A single point of failure, which affects the data's availability, is eliminated via decentralization. Users are unable to access the data when they need it when availability is compromised. Another security feature added by blockchain is the impossibility of easily changing data, which protects data integrity [17]. The blockchain also prevents double spending. Users can make multiple purchases using the same digital currency thanks to the double spending feature. Each coin in a blockchain is represented by a chain of digital signatures. A hash is digitally signed by each owner of a currency to transfer ownership. Receivers cannot check for double spending; they can only use their digital signature to demonstrate that they are the true owners of the coins. The traditional answer is a central authority that monitors for double expenditure. This solution places all of the trust in one company. Nakamoto [6] suggested the idea of a system where all transactions are publicly broadcast, and players need to agree on a transaction order in order to accomplish this without a trusted party. The server timestamps each transaction, and it publishes each transaction to everyone using the blockchain [6]. Bitcoin attempts to prevent double spending by requiring participants to agree on the sequencing of transactions. Another name for this agreement is consensus.

V. CONSENSUS

A consensus protocol represents agreement among distributed network nodes, devices, and users. Anyone can submit information on a public blockchain, but it is crucial that the network confirms it before adding it to the block that has been agreed upon. Due to the immutable ledger technology used by blockchain, where data contributed once cannot be changed later, inaccuracies in the data must be verified. To create a self-auditing system, nodes in the network must reach consensus on the same state of a blockchain. That block will be rejected and not added to the chain if consensus cannot be obtained. Every participant in this procedure is required to have two cryptographic key functions: a private key for signatures and a public key for other purposes. Before a new block is added to the blockchain, there are a series of checks that are done to make sure that a new block is valid. Each new block needs to contain a hash value of the previous block. Another criterion for a block to be valid is that the hash value of that block needs to be an under-targeted hexadecimal value. The targeted hexadecimal value is a predetermined value, and any hexadecimal number that is lower or equals to the targeted number is considered under the target. That is achieved by changing a nonce.

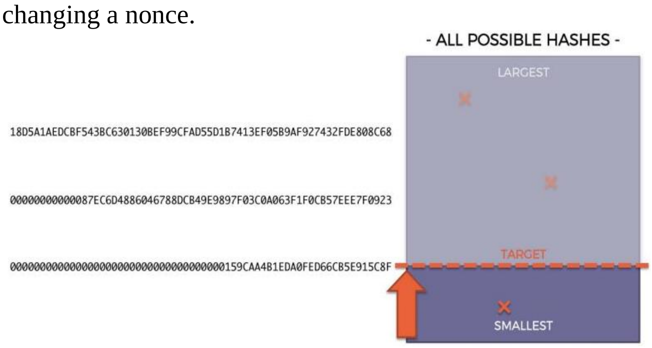

Figure 2.3: Cryptographic Puzzle Target - Miners must choose a hash value that is below the goal line in order to solve the cryptographic puzzle depicted in this picture [18]. The number adjacent to the target line is one of the acceptable solutions. The word "smallest hash "'s value is also taken into account when determining the answer to the problem.

Two different blocks may be added to the network's various nodes simultaneously on the same blockchain. Forking refers to this circumstance, and it is handled by carrying on until one portion of the network adds the following block before others. After the block is added, the network will be modified in accordance with the section of the longest blockchain. It is the same branch to which the new block is added. Digital signatures are used in blockchains that use crypto-currencies to authenticate users and stop double-spending in addition to ensuring that the blocks that are added are valid. Double-spending is avoided by time-stamping transactions and distributing them to all nodes. With Proof of Work, miners attempt to determine the header's hash value to verify data. PoW is typically linked to open-source, public blockchains that allow for open participation.

Bitcoin's proof-of-work (PoW) algorithm requires scanning data whose hash starts with a specific number of zero bits. Hashes with the desired number of leading zeros are displayed in Figure 2.3.

In section 2.2.3, the cause of this rise in CPU load is explained. The hashes for that block and all succeeding blocks must also be recalculated if an attacker wants to change anything inside a block. Because each new block contains the hash value of the previous one and because all blocks must have the proper hash values for the blockchain to remain intact, an attacker must change all blocks following the block they are attacking [6]. Figures 2.4(a) and (b) illustrate how a blockchain can be compromised when an attacker tries to alter the data contained within a block. Proof-of-Burn (PoB), in which miners burn some cryptocurrency, is an alternative to PoW through an unspendable address [12]. The address that cannot be spent is one that was generated at random and lacks a private key. Coins sent to that address cannot be accessed or used without a private key. Consensus techniques like Proof-of-Personhood (PoP) and Proof-of-Individuality (PoI) aim to protect anonymity. Binding these two identities results in PoP-tokens, which are used as anonymous credentials and maintain anonymity [6]. PoP is a consensus technique that links real-world and digital identities together using ring signatures and collective signing. PoI is being developed by Ethereum and is very similar to PoP [12].

The blockchain in Proof-of-Stake (PoS) operates under the presumption that users who have a larger stake are less likely to attack the network [12]. It requires participants to periodically demonstrate that they possess a certain level of wealth, typically expressed in the number of coins. Some people view this system as unfair because it provides the wealthiest users more control [12]. There are some instances where users with more senior accounts have more influence. In order to determine which users have the most influence, wealth and account age may occasionally be combined. Transaction as Proof-of-Stake (TPoS) is an additional PoS variant in which all nodes that produce transactions take part in the consensus. Because the block is selected from a pool of users who staked a set amount of cryptocurrency rather than through a mining process where miners compete for rewards, PoS is thought to utilise less energy than PoW [19]. Miners who wager money but do not win keep their wager. However, malicious miners will lose their stakes, and the network will have less faith in them. Staking is comparable to locking cash in a safe. Users are chosen at random after staking to prevent the richest person from always winning, but those who are not chosen will not lose their money.

The main distinction between Delegated Proof-of-Stake (DPoS) and PoS is that delegates are chosen rather than all participants with the highest stake casting a single vote, which speeds up the voting process. Delegates can also change the block and interval sizes. Delegates who are discovered to be dishonest may be replaced. Replacement typically occurs once daily or once weekly, depending on the blockchain. Voting is passed over by dishonest delegates until they are replaced [12]. Proof-of-Activity (PoA) builds on the concept of PoS based on the age and also considers how active each user is, reducing the power of inactive stakeholders. The age is calculated using the creation date of the account. The concept is based on Reddcoin's Proof-of-Stake-Velocity, where members with the highest exchange rates and money flows have more influence [12]. To fix the unfairness of PoS, which occasionally gives more power to passive users who also happen to have more stake, Proof-of-Activity (PoA) was proposed. Ownership and activity in the blockchain are both considered by PoA [20]. Reddcoin takes a similar stance to PoA in that it measures the velocity of currency, or how frequently money circulates in an economy and is used by users. The Proof-of-Stake-Velocity (PoSV) algorithm is used [21]. This is comparable to a churn rate, which is a measure of participant turnover in peer-to-peer networks [22].

VI. CONCLUSION

Blocks are where blockchain stores its info. The creator of the first blockchain went by the name of Satoshi Nakamoto. Although some blockchains use private ledgers to store data, the blockchain that powers bitcoin uses a public ledger for transactions. The blockchain for Bitcoin aims to maintain anonymity and has an immutable ledger. A blockchain uses a consensus protocol to validate the data that is stored; there are various types of consensus protocols, including Proof-of-Work, Proof-of-Stake, and Proof-of-Activity. Additionally, blockchains frequently employ the Byzantine Fault Tolerance algorithm, which requires 2/3 of all nodes to concur on the validity of the data to prevent attacks. Miners oversee processing transactions on blockchains like Bitcoin using their computing power, and in exchange, they are paid in bitcoins. Blockchains can be used in smart homes to record device-to-device transactions.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems, 29(7):1645–1660, 2013. [CrossRef]
2. Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelffl´e. Vision and challenges for realising the internet of things. Cluster of European Research Projects on the Internet of Things, European Commision, 3(3):34–36, 2010.

3. Jennifer B´elissent et al. Getting clever about smart cities: New opportunities require new business models. Cambridge, Massachusetts, USA, 2010.
4. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. Computer networks, 54(15):2787–2805, 2010. [CrossRef]
5. Floris Van den Abeele, Jeroen Hoebeke, Ingrid Moerman, and Piet Demeester. Integration of heterogeneous devices and communication models via the cloud in the constrained internet of things. International Journal of Distributed Sensor Networks, 11(10):683425, 2015. [CrossRef]
6. Satoshi Nakamoto. Bitcoin white paper, 2008.
7. Andriy Luntovskyy and Dietbert Guetter. Cryptographic technology blockchain and its applications. In The International Conference on Information and Telecommunication Technologies and Radio Electronics, pages 14–33. Springer, 2018. [CrossRef]
8. Michael Safi. Australian craig wright claims he is bitcoin founder satoshi nakamoto. https://www.theguardian.com/technology/2016/may/02/craig-wright-bitcoin-founder-satoshi-nakamoto-clai, May 2016.
9. Mobility report - internet of things forecast. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.
10. Nir Kshetri. Can blockchain strengthen the internet of things? IT professional, 19(4):68–72, 2017. [CrossRef]
11. Patrick Schueffel, Nikolaj Groeneweg, and Rico Baldegger. The crypto encyclopedia. Technical report, Growth publisher, 2019.
12. Tiago M Fern´andez-Caram´es and Paula Fraga-Lamas. A review on the use of blockchain for the internet of things. IEEE Access, 6:32979–33001, 2018. [CrossRef]
13. W Penard and T van Werkhoven. On the secure hash algorithm family. national security agency. Technical report, Technical Report, 2008
14. Evan Duffield and Kyle Hagan. Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proofofwork system. bitpaper. info, 2014
15. Free online sha-256 generator tool. https://www.freeformatter.com/sha256-generator.html.
16. Wang Xiaofei, Hong Fan, Tang Xueming, and Cui Guohua. Merkle tree digital signature and trusted computing platform. Wuhan University Journal of Natural Sciences, 11(6):1467–1472, 2006. [CrossRef]
17. David Schwartz, Noah Youngs, Arthur Britto, et al. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5:8, 2014.
18. Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy. Towards blockchain-based auditable storage and sharing of iot data. In Proceedings of the 2017 on Cloud Computing Security Workshop, pages 45–50. ACM, 2017. [CrossRef]
19. Hadelin de Ponteves and Kirill Eremenko. Udemy: Blockchain a-z: Learn how to build your first blockchain. https://www.udemy.com/course/build-your-blockchain-az/learn/lecture/9657368#overview.
20. Tiago M Fern´andez-Caram´es and Paula Fraga-Lamas. A review on the use of blockchain for the internet of things. IEEE Access, 6:32979–33001, 2018. [CrossRef]
21. Daniel Stutzbach and Reza Rejaie. Understanding churn in peer-to-peer networks. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, pages 189–202. ACM, 2006. [CrossRef]
22. Nikos Fotiou and George C Polyzos. Decentralized name-based security for content distribution using blockchains. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 415–420. IEEE, 2016. [CrossRef]

AUTHORS PROFILE

Ms. Neenu Kuriakose is currently pursuing PhD. Her areas of interest include Internet of Things (IoT), Machine Learning, Computer Security and Block-chain Technology. She has published 10+ papers in professional journals. She holds two patents, entitled as “Block-chain enabled intelligent IoT architecture with AI “and “Intelligent IoT based smart irrigation system using cloud computing.” She earned an Indian book of record in 2nd August 2021. Ms. Neenu received Best Research scholar award from novel research academy (2021) and Indo-Asia Best Researcher award in Computer Security era (2021). E-mail: nkuriakose@lincoln.edu.my, neenuannaa@gmail.com

Dr. Divya Midhunchakkaravarthy is an associate professor currently working at Lincoln university college, Malaysia as the Dean of Computer Science. Her areas of interest include Machine Learning, Computer Security and Block-chain Technology.