Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Volume III, Issue II, July 2021

A Survey on Blockchain Technology in IoT for Security

Soumya Bajpai[1], Kapil Sharma[2]
[1]Research Scholar, Amity University, Gwalior, M.P., India, soumyabajpai2013@gmail.com
[2]Associate Professor, Amity University, Gwalior, M.P., India, ksharma@gwa.amity.edu

Abstract— **The Internet of Things, i.e. IoT, has advanced dramatically in recent years. By integrating IoT and the Internet, heterogeneous intelligent devices may process real-time data and conduct transactions. However, IoT's security dependability and privacy are significant roadblocks to its progress. Consensus mechanisms, Decentralization, smart contracts and data encryption are all elements of Blockchain that are suited for developing IoT systems to avoid possible attacks and reduce overall transaction costs. Blockchain can improve IoT security performance by acting as a decentralized and transparent database platform. Although blockchain technology can provide us with more dependable and convenient services, the security risks and problems associated with this novel technology are also an optimal strategy that we must consider.**

Keywords— **Blockchain, Decentralization, Internet of things.**

I. INTRODUCTION

Blockchain is a decentralized and immutable transaction ledger in which each transaction is inextricably connected to the one before it. Operation in untrusted decentralized contexts may be safeguard by both the record of transactions and decentralized consensus on the authenticity of the transaction record, which is the fundamental function of the Blockchain. The first application of Blockchain is Bitcoin it's a type of digital currency based on blockchain technology that can be used to exchange items on the internet like money. People may now employ blockchain technology in a variety of fields and services, including the financial market, IoT, elections, medical care, and storage and supply chain, thanks to the success of Bitcoin. Blockchain technology has the potential to resolve IoT's most pressing security concerns, notably those related to data integrity and dependability [1]. Software applications can use Blockchain to broadcast and record transactions/events in a secure and distributed (peer-to-peer) way.

A) The basic concept of Blockchain

Blockchain technology is a multi-field infrastructure building that includes cryptography, algorithms, mathematics, and economic models, merging peer-to-peer networks and employing distributed consensus algorithms to tackle classic distributed database synchronization problems [2].

Blockchain is quickly gaining traction and is being utilized for various applications, including mobile wallets, distributed storage, and online platforms. Recording events (such as temperature, moisture, or location changes) and constructing tamper-resistant ledgers that are only accessible by particular parties, such as specified actors in a supply chain, are possible uses of Blockchain in IoT.

The IoT security need may met using Blockchain technology [3]. The following notable Blockchain characteristics can help ensure IoT applications' integrity and hence improve IoT security [4].

Decentralized:- The essential characteristic of Blockchain is that it does not require a centralized node to record, store, or update data; instead, data may be recorded, stored, and updated in a distributed manner.

Transparent: - The blockchain system's data record is transparent to each node, and it is also transparent when updating the data, which is why Blockchain can be trusted.

Integrity: Blockchains are capable of storing transactions in a permanent and verifiable manner. The integrity and non-repudiation of transactions can be guaranteed by the signatures of the senders in transactions. Blockchains' hash chain structure prevents any recorded data from being modified, even in part. Blockchain consensus techniques can ensure that records are accurate and consistent.

Anonymity:- To maintain anonymity and privacy, blockchains might employ changing public keys as users' identities. Many IoT apps and services, especially those that require private identities and privacy, find this appealing.

Immutable:- Any records will be reserved indefinitely and cannot be modified unless more than 51 percent of the nodes are taken over at the same time.

Open Source:- Individuals may use blockchain technology to construct any application they want, and most blockchain systems are accessible to everyone. Records can be checked openly, and people can use blockchain technology to construct any application they desire.

Fault Tolerance:- Blockchains are intrinsically decentralized systems with a diverse set of members, according to the network mentioned above layer. These participants' activities are influenced by the information and incentives accessible to them. When a newly broadcast transaction is received, each node in the decentralized blockchain network has the choice to accept or ignore it. Once the majority of the nodes agree on a single state, consensus can be reached. As a consequence, defects in a small number of nodes are unlikely to affect the public ledger's status, and will be recoverable when the consensus state is updated.

Attack Resistance:- Blockchain, on the other hand, is built on a decentralized P2P network and can resist tampering. Tampered nodes are unable to inject fraudulent transactions or blocks into the chain as long as each node in the network retains a copy of the Blockchain. As a result, the Blockchain's record integrity is guaranteed.

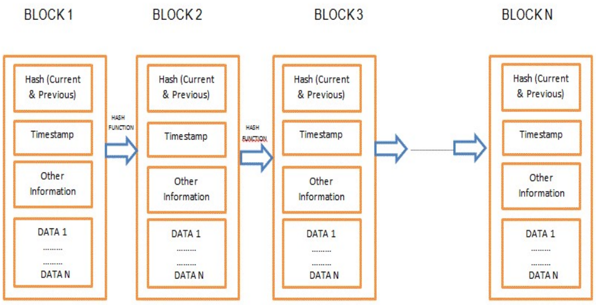

Fig. 1. Block chain Structure

II. Blockchain Features for IoT: Applications

i) Data is uploaded by a huge number of end devices in IoT networks, which are data-centric. As a result, IoT attacks on networks and systems are a possibility.
ii) Sensory data in an IoT system might be personal or sensitive [5], for example, medical IoT or it may come from national applications, such as the IoT-based smart grid [6] and nuclear power plant. The data's integrity and privacy are critical. Blockchain is thought to hold the answer to data integrity, resolving security, and dependability problems in IoT networks. Beyond bitcoin, Blockchain has attracted a lot of attention for other IoT applications (e.g., supply chain management and smart city), because to its assured data integrity.
iii) The accuracy of sensory data: Blockchain-powered IoT networks have two types of data: Blockchain-related data, such as transaction fee, account, balance, and IoT-related data, such as sensory data. As with other conventional Blockchain applications, the Blockchain-related data may be checked based on prior transactions, for example, the expenditure must be less than the account balance.

B) Working of a Blockchain

The following are the key functioning processes of Blockchain:
1) The transmitting node logs new data and broadcasts it to the rest of the network.
2) The receiving node examined the message against the data it received, and if it was accurate, it was saved to a block.
3) To the block, every receiving node in the network applies a proof of work (PoW) or proof of stake (PoS) method.
4) After the consensus method is completed, the block is added to the chain, and every node in the network accepts it, allowing the chain to grow indefinitely.

C) Consensus Algorithm

The consensus algorithm is a technique that ensures that all blockchain nodes agree on the same message ensures that the newest block has been appropriately added to the chain, guarantees that the message stored by each node is the same, and protects against malicious attacks. There are two types of algorithm:-

i) Proof of Work (PoW)

A proof of work is a piece of data that is difficult to generate (costly or time-consuming) yet simple to verify by others and meets particular criteria. Producing a proof of work can be a random and low-probability procedure, requiring a lot of trial and error on average before producing a legitimate proof of work. Bitcoin uses the Hashcash proof of work system.

Mining is the process of computing PoW. Each block contains a random value called "Nonce" in the block header; by modifying this nonce value, PoW must create a value that makes the block header hash value smaller than a previously determined "Difficulty Target." Difficulty refers to the amount of time it takes for a node to calculate a hash value that is smaller than the goal value.

Miners must produce a proof of work that covers all of the data in a block for it to be acknowledged by network members. The difficulty of this job has been tweaked to limit the network's ability to produce new blocks to one every 10 minutes. Because successful generation has such a low probability, it's impossible to forecast which worker computer in the network will be able to create the next block [7]

ii) Proof of Stake (PoS)

Proof of Stake does not require expensive processing resources because the Proof of Work approach wastes a lot of electricity and computer resources. The resource that is compared in Proof of Stake is the amount of Bitcoin a miner has - someone who owns 1% of Bitcoin may mine 1% of the Proof of Stake blocks" [7]

D) Types of a Blockchain

Three types of blockchain technology can be distinguished.

i) A public blockchain :-allows anybody to review and verify transactions, as well as participate in the consensus process. Bitcoin and Ethereum, for example, are both public blockchains.

ii) Consortium blockchains: This implies that the node with authority may be chosen in advance, and it generally has business-to-business relationships. The information in the Blockchain can be open or private, and it is classified as partially decentralized. R3CEV and Hyperledger are both consortium blockchains.

iii) Private Blockchain: Nodes will be restricted; not every node will be able to join in this Blockchain, and data access will be controlled by tight authority.

E) IoT involved Blockchain

IoT devices would join the Ethereum blockchain and participate in basic Blockchain tasks such creating raw sensory transaction records, validating transactions, and even mining blocks [8]. In Blockchain-IoT networks, three virtual roles, namely, full node, light node , and miner, must be maintained.

Miners are the most in demand for storage and compute since they mine transactions into blocks and store all blocks. Full nodes store all blocks, including block headers and content, but they do not participate in block mining. Complete nodes require massive storage and a particular amount of computing.

In Blockchain networks, IoT end devices act as light nodes. For access control and audit, IoT devices can create private keys on their own or register with a certificate authority (CA). Light nodes, which store block headers and create transactions but do not mine blocks, can be enabled by the Simplified Payment Verification (SPV) technology.

F) Blockchain as a Service for IoT

Blockchain provides a service layer (120, 122) that may be used to interact with common IoT architectures, such as the four-level design described in Section 3. This structure is often made up of three virtual roles: sensor, agent, and miner .

IoT sensors capture sensory data and use Blockchain agents to communicate with Blockchain services. The sensors aren't involved in any Blockchain functionality. The agents can convert the obtained sensory data into transactions and send them to the Blockchain network.

Miners, who constitute a peer-to-peer network, carry out the Blockchain's basic job of confirming transactions and mining transactions into blocks.

III. *(A)*CHALLENGES OF APPLYING BLOCKCHAIN IN IOT APPLICATIONS

Blockchains are currently designed to operate on P2P homogenous networks. However, the peculiarities of IoT, such as end device resource limitations compared to the high performances computer servers or desktop devices, restrict Blockchain from being used directly for IoT. The use of Blockchain on IoT devices is fraught with difficulties.

i) Computation

For light-weight IoT devices, Blockchain activity is costly. Some complex cryptographic methods employed in privacy-preserving Blockchains. In Blockchain, a complete node must validate and search every block and transaction, which may be a significant burden for resource-constrained IoT devices. IoT devices are unable to perform PoW like consensus algorithms. The Bitcoin network as a whole can do roughly 1019 hashes per second. A modern graphics processing unit (GPU) can do around 107 hashes per second [9].

ii) Storage

The cost is too high to be useful in IoT applications. Big data is generated by the Internet of Things. Because every block in an n-node Blockchain network is copied n times, the overall quantity of data in Blockchain driven IoT might be tremendous.

iii) Communication

Blockchain nodes necessitate regular data transfers and exchanges. This is because Blockchain is based on a peer-to-peer network that constantly exchanges data in order to preserve consistent records, such as for the most recent transactions and blocks.

iv) Energy

Some IoT devices are intended to run for a long period on a single charge of the battery. An IoT gadget, for example, is meant to consume 0.3 mWh per day and last at least 5 years when powered by a 600 mWh CR2032 battery ([134).

v) Mobility and partition of IoT

The wireless network may be separated into two modes: infrastructure mode, in which network infrastructures (base stations) transmit all packets, and ad-hoc mode, in which the network does not rely on pre-existing structures and each node passes data to other node[10].

vi) Blockchain Performances

IoT device mobility may jeopardize Blockchain performance. The mobility of devices in an infrastructure-based wireless network can lead to an increase in signaling and control messages. Network partitioning, on the other hand, separates wireless ad-hoc networks into separate portions when mobile nodes move in different ways [11].

vii) Latency and capacity

Blockchain's high latency is utilized to assure consistency in decentralized Blockchain networks. For many IoT applications, the latency that Blockchain is known for is untenable. For example, Bitcoin's 10 minute block confirmation time is too long for delay-sensitive IoT applications like car networks.

B) Security Discussions on Blockchain-based IoT Applications

Despite the fact that Blockchain is known to be tolerant of the Byzantine Problem, it still has unresolved security vulnerabilities that would persist in Blockchain-based IoT networks.

i) Privacy

Due to the fact that transactions are supposed to be openly observed and confirmed by all peers, Blockchain might suffer from privacy challenges, including user privacy and data confidentiality.

Users privacy: The one-to-many mapping between a physical user and virtual identities may be formed based on a transaction graph (162, 163, 164), and the identity of a physical user may be conjectured [12].

Untraceability and unlinkability should be achieved by fully anonymous electronic cash. Bitcoin is pseudo anonymous rather than completely anonymous. In newer Blockchains, improved encryption technologies safeguard user privacy. Hawk aimed to overcome the privacy issue of smart contracts on public Blockchain by employing cryptographic primitives, like as zero-knowledge proofs, to automatically construct an efficient cryptographic protocol. A statement may be confirmed using zero-knowledge proof without any more information than the statement itself. In addition to public-key based signatures, zero-knowledge proof has been utilized in Zerocoin, Zerocash, Provisions, [13] and other projects to establish anonymous proof of ownership.

ii) Identity and Device Management

Owners of IoT devices should be aware of their devices' identities and vice versa. Peers are specified by their public addresses in contemporary public Blockchains, such as Bitcoin and Ethereum, which can be formed independently without previous communication to the others In Blockchains, a physical node might be viewed as several virtual nodes, according to [14]. Peers must be permitted to access the Blockchain network in the case of private Blockchains. As a result, blockchains require identity management as a core necessity.

iii) Access Control

Blockchain enables IoT devices to design their own access control policies and assume complete ownership of their own data as a distributed system, reaching device democracy. Programmable smart contracts are one technique that may be used to create access control [15].

IV. Security Issues

The security of Blockchain, like that of any other system, is determined by the security of its underlying software and hardware implementation, as well as the protocols and messages that it requires to function. Furthermore, while consensus is seen as a tool to assure fairness and confidence in an untrustworthy system, it also serves as a target for would-be attackers. Furthermore, because all transactions are public, there is a risk of privacy leakage. Furthermore, due to the Blockchain's immutability, any unlawful blocks will remain for the duration of the Blockchain.

A) Selfish Mining and Majority Attack

After applying the consensus method and confirming a block in the chain, transactions in blockchains are typically regarded immutable. Nonetheless, majority assaults can be carried out if the attacker has control of more than 50% of the Blockchain's miners. In this instance, the entire process of adding blocks to the chain might be hijacked, resulting in the introduction of possibly erroneous blocks.

B) Anonymity and Confidentiality

Blockchain allows users to conduct transactions in an anonymous manner. Nonetheless, because the transactions are publicly, identifiable indicators that might identify users' identity and private information may still exist. Transactions, for example, may be connected to IP addresses to provide even more information about a user, and third-party programmes may follow a person's many personas, currencies, and data.

C) Blockchain Misuse

In addition to the risk for privacy exposure owing to the particular of distributed ledger, we must also consider, as with other systems, the misuse of Blockchain in general, outside of its intended usage. The usage of encryption secure systems, in particular, enables security for both benign and criminal users.

D) Fork Problems

One issue is the fork issue. The fork issue is linked to the decentralized node version and agreement during software upgrades. It's a critical problem since it touches on so many aspects of Blockchain.

E) Blockchain Scale

As Blockchain grows, data becomes larger and larger, making the loading of stores and computation more difficult. It takes a long time to synchronize data, while data continues to expand, posing a significant difficulty for clients while using the system [3].

F) Blockchain Data Confirmation Over Time

Compared to standard online credit card transactions, which often take 2 or 3 days to confirm, bitcoin transactions only take approximately 1 hour to confirm. This is far better than the norm, but it's still not good enough for what we want. The Lightning Network is a solution to this problem.

G) Issues with Current Regulations

The characteristics of a decentralized system will weaken the central bank's ability to control economic policy and the amount of money, making governments wary of blockchain technologies. Authorities must investigate this new issue and formulate new policies quickly, or else market risk will arise.

H) The Problem of Integrated Costs

Of course, changing an existing system comes with a high cost in terms of both time and money, especially when it comes to infrastructure. We must ensure that this creative technology provides economic benefits and meets regulatory standards and bridges the gap between conventional and modern organizations, since it frequently encounters difficulties from existing internal organizations.

V. Future Direction

This section discusses how to improve Blockchain's security, scalability, and capacity for future large-scale, high-volume IoT applications. The Blockchain for IoT application design would also take into account the unique characteristics of IoT networks, such as their enormous scale, intrinsic segmentation, imperfect network connection, non-trivial topology, non-zero propagation time, and heterogeneity.

A) Sharding

Sharding Blockchain is a new way for processing transactions in parallel. The block production pace of Blockchain may be considerably increased in this way. Early sharding concepts, such as focused solely on transaction processing and maintained a single public Blockchain.

B) Side Chain

Aside from the ubiquitous nature of IoT networks, certain IoT devices, such as those placed on aeroplanes, transcontinental trains, and ships, can travel long distances. The integrity of the data supplied by these IoT devices, such as the erosion of aircraft components, is just as critical, if not more so, than data supplied by static IoT devices [16].

C) Consensus on the Internet of Things

Data-centric IoT-Blockchain applications would benefit from specifically built consensus mechanisms for diverse purposes. Instead of checking transaction syntax, the consensus protocol might be constructed to obtain data consensus by validating transaction data. Due to the network topology a high density, sensor observations are highly linked in the space domain.

D) Blockchain Editable

Because a big number of IoT devices continue to record a high number of events over time, the storage capacity of IoT devices can be quite limiting for the explosively rising size of a Blockchain ledger. Since the genesis block in 2009, the total size of Bitcoin, which records financial data, has expanded to 149 terabytes by December 2017.

VI. Conclusions

There's no denying that Blockchain has been a popular concept in recent years. While there are certain issues to be aware of, certain issues have already been addressed as new techniques evolve on the application side, becoming more stable and mature.

The latest Blockchain technologies were thoroughly examined, followed by a comparison of the technologies' applicability to IoT situations. For future efficient integration of Blockchain and IoT technologies, research areas were identified to increase Blockchains' capacity, security, and scalability.

This section discusses how to improve Blockchain's security, scalability, and capacity for future large-scale, high-volume IoT applications. The Blockchain for IoT application design would also take into account the unique characteristics of IoT networks, such as their enormous scale, intrinsic segmentation, imperfect network connection, non-trivial topology, non-zero propagation time, and heterogeneity.

The government must enact legislation to address this technology, and businesses must be prepared to accept blockchain technology in order to avoid it having a significant influence on the present system.

While we benefit from the advantages that blockchain technology provide, we must also be aware of the potential for negative impact and security risks.

References

[1] M. Merkx, "VAT and blockchain: Challenges and opportunities ahead," EC Tax Rev., vol. 28, no. 2, pp. 83–89, 2019.

[2] E. Oswald, M. F. Eds, and D. Hutchison, Advances in Cryptology – EUROCRYPT 2015. 2015.

[3] R. Kuhn and T. Weil, "Strengthen the Internet of," no. August, 2017.

[4] I. C. Lin and T. C. Liao, "A survey of blockchain security

issues and challenges," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653–659, 2017, doi: 10.6633/IJNS.201709.19(5).01.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[6] W. Chin, W. Li, and H. Chen, "08067688," no. October, pp. 70–75, 2017.

[7] W. Gao, W. G. Hatcher, and W. Yu, "2018 27th International Conference on Computer Communication and Networks (ICCCN).," no. i, 2018.

[8] X. Wang et al., "Survey on blockchain for Internet of Things," Comput. Commun., vol. 136, pp. 10–29, 2019, doi: 10.1016/j.comcom.2019.01.006.

[9] M. Galan, "Decentralized Application Platform Ethereum," 2016, [Online]. Available: https://is.muni.cz/th/436304/fi_m/Dimplomovka_galan.pdf.

[10] M. Lauridsen, I. Z. Kovács, P. Mogensen, M. Sørensen, and S. Holst, "Coverage and capacity analysis of LTE-M and NB-IoT in a rural area," IEEE Veh. Technol. Conf., vol. 0, pp. 2–6, 2016, doi: 10.1109/VTCFall.2016.7880946.

[11] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's INTRAnet of things to a future INTERnet of things: A wireless- and mobility-related view," IEEE Wirel. Commun., vol. 17, no. 6, pp. 44–51, 2010, doi: 10.1109/MWC.2010.5675777.

[12] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," 2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017, 2017, doi: 10.1109/ICCCN.2017.8038517.

[13] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," Proc. - IEEE Symp. Secur. Priv., pp. 397–411, 2013, doi: 10.1109/SP.2013.34.

[14] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini, "CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT," IEEE Int. Conf. Commun., 2017, doi: 10.1109/ICC.2017.7996641.

[15] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang, "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network," IEEE Access, vol. 7, pp. 106043–106052, 2019, doi: 10.1109/ACCESS.2019.2929919.

[16] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014, 2014, pp. 230–234, doi: 10.1109/SOCA.2014.58.