Analysis and Comparison of Different Blockchain Algorithms in IoT Security

Monika Parmar¹, Neeraj Kumar², Harsimran Jit Kaur¹, Abha Sharma⁴, Sandhya Sharma⁵, Mamatha Sandhu⁶

¹ Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India. e-mail: monika.parmar@chitkarauniversity.edu.in
² Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India. e-mail: neeraj.kumar@chitkarauniversity.edu.in
³ Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. e-mail: harsimran.kaur@chitkara.edu.in
⁴ Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India. e-mail: abha.sharma@chitkarauniversity.edu.in
⁵ Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India. e-mail: sandhya.sharma@chitkarauniversity.edu.in
⁶ Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. e-mail: mamatha.sandhu@chitkara.edu.in

abha.sharma@chitkarauniversity.edu.in

Abstract. Internet of things (IoT) and Blockchain are two advancements that are picking up notoriety since the hour of their creation. Sooner rather than later, IoT is going to impact everything we use in our daily lives. As the utilization of this innovation expands, the danger to misuse it likewise increments. Existing advancements are insufficient to manage this. Along these lines, Blockchain has risen as a successful answer for understanding the security issues identified with IoT. Information put away in Blockchain is permanent and can't be changed very effectively. Likewise, the information is added to the block only after it is affirmed by everybody in the system, and in this manner, it is permitting secure exchanges. The individuals who approve the exchanges or transactions and include them in a block are known as miners or excavators. In this article, a detailed overview of the different Blockchain algorithms that are being used for IoT security has been explored. Also, an attempt has been made to provide a detailed overview regarding Blockchain which can act as a reference for the researchers who wish to pursue research in the Blockchain domain.

Keywords: IoT, Blockchain, Security, Proof of work (PoW), Proof of elapsed time (PoET), Proof of stake (PoS).
1. Introduction

IoT comprises gadgets that create, process, and share the huge amount of safety-critical, security information private delicate data, and consequently are engaging focuses of different digital cyber-related issues [1]. Some latest networkable gadgets, that comprise the IoT, consume very less energy and are quite lightweight. These gadgets must commit a large portion of their accessible energy and calculation for executing center application usefulness, making the errand of moderately supporting privacy and security very challenging. Conventional security strategies will in general be costly for IoT regarding energy utilization and handling overhead [2]. Additionally, so many threat security structures are profoundly centralized and are accordingly not essentially appropriate for IoT. To ensure client protection, existing strategies frequently either uncover boisterous information or deficient information, which may frustrate some IoT applications from offering customized services [3]. Subsequently, IoT requires a lightweight, adaptable and protection defend. The Blockchain innovation that supports Bitcoin the primary cryptocurrency framework [4] can defeat previously mentioned challenges because of its appropriated, secure, and private nature. It generally creates a decentralized system and eliminates the need for central servers and usually provides peer-to-peer interaction. It is a decentralized database that records each exchange made on a system. It has a record appropriated over a system of hubs. This system can be open or private. Blockchains permit distributed exchanges, disposing of the need for central servers. This innovation essentially has four components namely Consensus, Record, Cryptography, and Smart agreement. Consensus provides the PoW and checks the activity in the systems or networks. The record provides the total subtleties of transactions inside networks. Cryptography makes sure that all information in record and systems gets encrypted and just approved clients can decode the data. A smart agreement or contract is utilized to confirm and approve the members of the network. While the blockchain tools have tremendous capability to create powerful internet communication networks. Next, there's a big question about scalability. Bitcoin block size is set to 1 MB, and around every 10 minutes, a block is created. More blocks, therefore, mean huge storage capacity and reduced system propagation speed. It would also lead to a significant centralization as users want such a large blockchain to stay. Thus, the trade-off between safety issues and block size is becoming a problem. Miners will cover their produced blocks in the future to get more profits. Therefore, some approaches to this dilemma need to be put forth. Researchers have revealed that security compromise in blockchain can also occur even though consumers only make a transaction with their private key and public key. The user's real IP address could even be tracked. You could also monitor the actual IP address of the user. The existing algorithm of consensuses like PoS or PoW faces some major issues. For instance, PoW consumes much more resources. These issues must be dealt with through the advancement of blockchain technology.
2. SEGMENTS OF BLOCKCHAIN
Blockchain principally has four segments which are as following:

2.1. System of Nodes
All the hubs or nodes associated with the web, keep up whole exchanges or transactions made on a Blockchain organize cooperatively and the validness of exchange is checked via a protocol. At the point when another exchange happens, its records are added to the record of past exchange which is well known as 'mining'. Different nodes present on the system, confirm the proof of work. Independent nodes produce and register authentic transactions into the circulated or distributed record. Neither a focal authority nor a believed outsider is important to approve exchanges. All hubs or nodes of the Blockchain work together to keep up a consistency of the record. Every hub runs a customized mechanism, called consensus. This is the procedure by which hubs concede to how to refresh the Blockchain because of a lot of transactions. Accomplishing consensus guarantees most of the hubs or nodes in the system have approved a similar arrangement of transactions. The objective of distributed or circulated consensus is to keep the records of an adequate system peer correctly at a generally granular time scale. The Consensus guard against malevolent peers that can disturb the trustworthiness of the record by (a) retroactively altering transactions; (b) performing semantically unpermitted exchanges or (c) blocking the acknowledgment and booking of correct transaction demands.

2.2. Dispersed database framework
The database is made out of data blocks and is replicated to each hub of the framework. Each block has a rundown of exchanges, a timestamp, and the data which connects to the past block.

2.3. Common Record
The record is made freely accessible and is ethical which is refreshed each time an exchange or transaction is made. The heart of the ledger or record is generally the cryptographic hash, a statistical
algorithm that maps the data with the variable size to the fixed-size string. All transactions named A, B, C, D are hashed as H(A), H(B), H(C), H(D), and after that they get aggregated into successive hashes as H(hA|hB), H(hC|hD) to constitute a Merkle tree.

Figure 2. Connecting block transactions to block header

The top hash, or the Merkle tree root, is incorporated into the block header. This has been depicted in figure 1.

2.4 Cryptography
Data is limited by a cryptosystem which makes it difficult for unapproved clients to access or alter it.

3. MECHANISMS PROVIDING CONSENSUS IN BLOCKCHAIN
The mechanisms involved in providing the consensus are as following:

3.1 Proof-of-Work (PoW)
It is the broadly known system for building up consensus. In PoW, a solitary node can give its decisions to other hubs or nodes, which can be thusly approved by different hubs in the system. If a node attempts to submit a block then it should likewise confirm the work is performed, which is a computationally troublesome errand. PoW gives extraordinary system dependability [5]. Be that as it may, PoW is especially exorbitant in light of the computational assets consumed. "Diggers or Miners" are boosted to
take part to gain a crypto monetary reward, which is given for the generation of a successful block. The basic flowchart for PoW has been shown in Figure 2.

![Flowchart of PoW](image)

**Figure 3. Proof for POW [6]**

### 3.2 Proof-of-Stake (POS)

It is like a PoW. The hubs or nodes are compensated after creating a block. But just a couple of hubs can take part in this stage [7]. Surely, the following generator hub is deterministically chosen dependent on the collected wealth (i.e., the "Stake"). The digging or mining procedure for a Blockchain dependent on POS is typically alluded to as "forgery". The innovation that propelled POS was PeerCoin. POS tends to make the mechanism of consensus virtual. In POW, cryptographically puzzles are solved by the miners or excavators. In POS, rather than excavators, there are validators. The validators lock up a portion of their Ether as a stake. Following that, the validators wager on the blocks that they feel will be added close to the chain. At the point when the block gets included, the validators get a block reward concerning their stake.

### 3.3 Proof of Burn (PoB)

In this, validators usually burn coins by sending them to a location where they are unrecoverable. By sending the coins to an inaccessible location, validators win a benefit to mine on the framework or system. The more coins miners consume or burn, the better are their odds of being chosen to mine the
following block [8]. While PoB is a fascinating option in contrast to PoW, this algorithm squanders assets/resources unnecessarily. It is additionally scrutinized that mining influence goes to the individuals who are happy to burn more cash.

### 3.4 Proof of Capacity (PoC)

In this, validators should invest their hard drive space as opposed to putting resources into costly equipment or consuming coins [9]. The more the hard drive space validators have, the better are their odds of getting chosen for mining the subsequent block and acquiring the reward for a block. A brief analysis of some of the commonly used consensus algorithms has been demonstrated in table 1.

### 3.5 Proof of Elapsed Time (PoET)

It is one of the most attractive algorithms for consensus that pick the subsequent block fairly. It is generally utilized in permission Blockchain systems. In PoET, each validator on the system gets a reasonable opportunity to make his block.

| Consensus Algorithms | PoW          | PoS            | PoET                | BFT       |
|----------------------|--------------|----------------|---------------------|-----------|
| **Type of Blockchain** | Permissionless | Either Permissionless or Permissioned | Either Permissionless or Permissioned | Permissioned |
| **Rate of Transaction** | Low          | High           | Medium              | High      |
| **Need of Token** | Required      | Required        | Not Required         | Not Required |
| **Participation Cost** | Yes          | Yes            | No                  | No        |
| **Peer Network Scalability** | High         | High           | High                | Low       |
| **Model** | Not Trusted   | Not Trusted     | Not trusted          | Semi –trusted |
| **Tolerance** | Around 25%   | Depend on the algorithm used | Not Known            | Around 33% |
Different consensus algorithms have different advantages and disadvantages. Based on the application, different algorithms can be used and are illustrated in the below heads.

**Figure 4. Illustration of algorithms based on Applications**

- **Monitor Node Identity:** In terms of choosing a main for every round, PBFT requires understanding the identification of every mining node, whereas Tendermint has to understand the evaluators to choose a proposer in that period. The peers can freely access the data for Proof of Work, Proof of Stake, Proof of Burn, and Distributed Proof of Stake.

- **Saving Energy Resources:** In Proof of work, the mining node uniformly hashes the data block header to get to the expected value. Consequently, the energy that is required to produce has achieved an enormous scale. As far as Proof of Stake and Distributed Proof of Stake is concerned, the mining node now hashes the data block to scan for the desired point, however, the work has been significantly reduced so the objective function is built to be restricted.

- **Adversary's Accepted Strength:** Generally, the requirement for one to take access to the system is known to be fifty-one percent of total hash capacity. But malicious nodes mining strategy in PoW networks could help miners earn more profit by twenty-five percent of total hashing power. Tendermint and PBFT are equipped to take care of up to thirty-three percent of the deficient nodes.

- **Instances of Algorithms:** The famous cryptocurrency Bitcoin is based upon Proof of Work, but Peercoin is the latest cryptocurrency that is based actually on peer-to-peer Proof of Stake. Besides, Hyperledger is based on PBFT to arrive at an agreement also known as the consensus protocol. Ripple incorporates protocol Ripple whereas Tendermint creates the same. Bitcoin is centered on PoW whereas Peercoin is the latest cryptocurrencies of the peer-to-peer PoS.

**Advances on consensus algorithms:** Performance, protection, and usability imply a successful consensus algorithm. There are so several gaps in the latest accepted consensus algorithms. New protocol mechanisms are there to resolve the issues related to blockchain. PeerCensus's concept is to disentangle block formation and confirmation of communication to improvise the pace of agreement. A new mechanism approach for ensuring the block is produced at a reasonably stable speed is also proposed. The elevated block creation pattern is defined to compromise the security of Bitcoin. Thus,
to overcome this issue, the (GHOST) chain selection rule is recommended. GHOST measures the divisions and the mining node will select the best to adopt instead of the fastest system.

4 SELECTING BLOCKCHAIN FOR SECURING IoT

Blockchain innovations are capable of securing the IoT based gadgets. IoT based gadgets can be designed to make use of the open services of Blockchain. IoT framework authorizes IoT gadgets to safely discover other gadgets, encrypting machine-to-machine exchanges/transactions utilizing appropriated key administration strategies [10, 11]. To guarantee security, care ought to be taken during the bootstrapping of an IoT gadget onto a specific Blockchain administration or service. Some features need to be considered while considering Blockchain technology for securing IoT devices and these features are Scalable IoT discovery, trusted communication, authentication of messages, IoT updates and configuration, secure firmware update, and image distribution.

5. CONCLUSION

Associations executing IoT arrangements keep on encountering difficulties recognizing security advancements and approaches adequate to mitigate one of kind dangers to IoT applications. Blockchain innovation vows to assume a significant job in catering to these difficulties. In this article, an attempt has been made to summarize various consensus algorithms used in Blockchain. A comparative analysis has also been made in Table 1 which is depicting that different consensus algorithms possess different features and each algorithm can be utilized as per the requirement of the user. IoT is one of the greatest innovations that the world has witnessed. With the development of extremely fast networks and intelligent devices, IoT is getting popularity all around the world. But sadly, IoT gadgets are increasingly

![Figure 5. Features of Blockchain for Securing IoT devices](image-url)
inclined to assault and unfit to secure themselves. The various properties and qualities of the Blockchain featured to expel the issues in IoT have been discussed in this paper.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in the internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[2] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[3] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013, pp. 23–27.
[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[5] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst.,20(4):398–461, November 2002.
[6] Ghimire, S., and Selvaraj, H., 2018, December. A survey on bitcoin cryptocurrency and its mining. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE.
[7] Vasin, Pavel. “Blackcoin’s proof-of-stake protocol v2.” (2014)
[8] Sultan, A., Mushtaq, M.A., and Abubakar, M., 2019, March. IoT security issues via blockchain: a review paper. In Proceedings of the 2019 International Conference on Blockchain Technology (pp. 60-65).
[9] K. Christidis and M. DevetsikIoTis, (2016) 'Blockchains and Smart Contracts for the Internet of Things,' IEEE Access, vol. 4, pp. 2292—2303.
[10] Yu Zhang and Jiangtao Wen (2015), 'An IoT electric business model based on the protocol of bitcoin'. ICIN. IEEE, pp. 184–191.
[11] M Banerjee, J. Lee, and K. K. R. Choo (2018), 'A Blockchain future for the internet of things security: a position paper,' Digit. Commun. Networks, vol. 4, no. 3, pp. 149–160.