

Proof of ability (PoAb) : An energy efficient and secure blockchain consensus algorithm for IoT devices

Amit Chaurasia [†]

Vijay Shankar Sharma ^{*}

Sandeep Kumar Sharma [§]

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Atul Srivastava [‡]

Department of Computer Science and Engineering

Amity School of Engineering and Technology

Lucknow 226028

Uttar Pradesh

India

Anuradha Pillai [@]

Department of Computer Science and Engineering

Symbiosis Institute of Technology

Pune 412115

Maharashtra

India

Abstract

In this paper we present a novel consensus algorithm PoAb: Proof of Ability. The consensus algorithm is based on the ability of the node to mine the transaction that is based on the shares of transaction mined by that node, and the resources available for the mining of the transaction. This consensus algorithm requires less computational overhead, it is secured from 51% attack and there is no requirement of energy hungry hardware computation.

[†] E-mail: amit.chaurasia@jaipur.manipal.edu

^{*} E-mail: vijayshankar.sharma@jaipur.manipal.edu (Corresponding Author)

[§] E-mail: sandeep.sharma@jaipur.manipal.edu

[‡] E-mail: atul.nd2@gmail.com

[@] E-mail: anuradha.pillai@sitpune.edu.in

For implementation Hyperledger fabric is used for the implementation of SHA3 algorithm which makes the hashing faster. PoAb is required for the selection of the miner from the pool of p2p network nodes, which takes the capability of the node to mine the block.

Subject Classification: Primary 93D50, Secondary 68M25.

Keywords: Consensus algorithm, Blockchain, IoT, Energy, Hash rate, 51% attack.

1. Introduction

In recent years, Blockchain has garnered significant appeal due to its decentralisation capabilities. In simple terms Blockchain provides a distributed ledger that does not require any centralized authority for its functioning and allows the safety of transactions and data. A blockchain is a linear sequence of blocks, each containing data and a cryptographically safe hash of that data. The information in each of these blocks may contain anything from a financial transaction to a smart contract to a digital currency.

The strength of the blockchain is its decentralization. A blockchain relies on peer groups of computers rather than managed by a single computer. The security of the blockchain relies on computers interconnected to each other known as nodes. Blockchains are immutable i.e. Fig. 1 represents the block that is uploaded and it is quite impossible to modify or delete the block since if the hash of one block is changed then the entire subsequent hashes will get changed signaling the change in the network. The Blockchain sphere is not just limited to cryptocurrency, which is termed as Blockchain 1.0, it is extended to healthcare, supply chain management and voting systems etc. which is termed as Blockchain 2.0, the foundation is to be built to make blockchains more scalable and interoperable to support more complex decentralized applications which is termed as Blockchain 3.0. The approaches and solutions that make the industry meet the business demands are termed Blockchain 4.0. And to manage all this requires a privacy and trust-based model, which is provided by blockchain. However, there are various challenges that exist with the deployment of blockchain into industry [4], [13]. The challenges for blockchain and industry integration is scalability, security, interoperability, complexity and energy consumption. This paper focusses on the energy consumption issues, as the energy consumed by the Bitcoin mining currently is 160 terawatt-hours annually which is more than the total electricity consume by the entire Argentina. One Bitcoin transaction

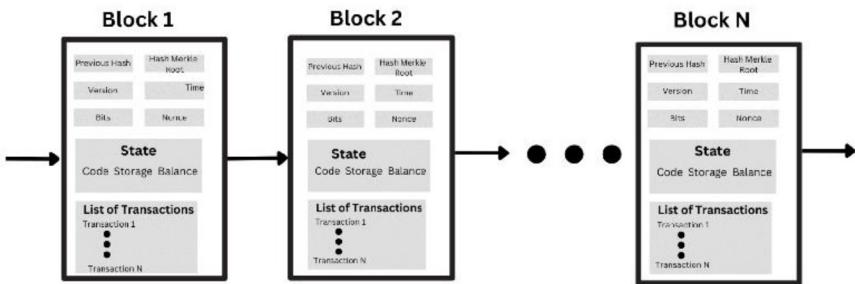


Figure 1
Blockchain Architecture

requires an average of 1200 kWh of energy which is equivalent of 100, 000 transactions done by VISA [14].

2. Related Work

The study of the data benefits the industry in a variety of ways, including increased productivity, cost reductions, the development of necessary skills, and effective decision-making.

In a decentralized system, consensus algorithms determine a conventional agreement. The problem with the consensus algorithm is that it should be more scalable and utilize less energy. IoT devices are tiny, and their features consume a small amount of electricity another issue related to PoW consensus algorithm, it suffers from 51% attack, in which the pool who acquires 51% of the total mining resources will have the more chances to mine the block. Consequently, an energy-efficient and secure consensus algorithm is required for IoT devices.

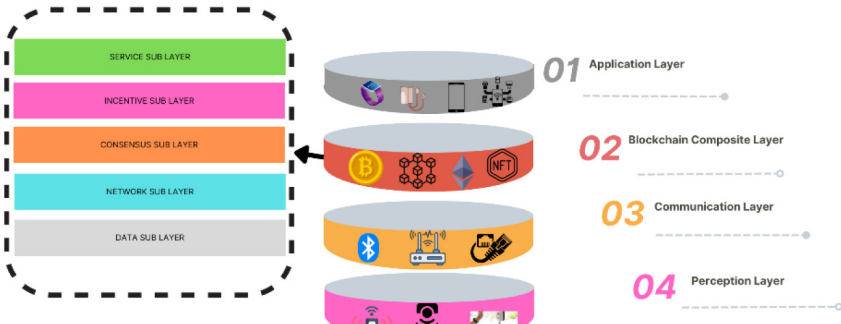


Figure 2
Blockchain-IoT Layered Architecture

Table 1
Comparison of different Consensus Algorithm

Type	Ref.	Consensus Algorithm	Pons	Cons
Proof of Work	[8]	Proof of Work (PoW)	PoW is resilient to Sybil attacks, in which an adversary generates several counterfeit identities to dominate the network.	PoW networks are susceptible to 51% assaults, whereby a singular entity.
	[10]	Proof of Meaningful Work (PoMW)	Decreased Wastage of Energy	Assault using more than half of the processing er available
	[1]	Hybrid PoW (HPoW)	Robust protection against Sybil attacks and double spending	hybrid models can introduce centralization risks
	[7]	Proof-of-Worktime (PoWT)	PoWT is time-based component can make attacks on the network more difficult	PoWT may face scalability challenges,
	[13]	Delayed Proof-of-Work (dPoW)	dPoW allows for trust less interoperability between blockchains.	dPoW suffers from the scalability issue, since it involves the anchoring transactions.
	[3]	Equitable chance Energy Saving (ePoW)	ePoW seeks to provide a more equitable chance for all participants to contribute to the consensus process and earn rewards.	The cost of maintaining hardware and software is high as comparison
	[11]	Semi-synchronous PoW (SSPoW)	SSPoW improves the scalability issue by allowing faster block generation as comparison to PoW.	SSPoW suffers from generation of fork blocks.

Contd...

Proof-of-Stake	[2]	Leased Proof of Stake (LPoS)	PoS is significantly more energy-efficient compared to Proof-of-Work () consensus mechanisms. Instead of relying on computational er and energy-intensive mining.	PoS lead to the centralization if a group holds the most wealth in the cryptocurrency.
	[6]	Secure Proof of Stake (SPoS)	SPoS is the energy efficient PoS, it uses the notion of nothing at stake and avoids the miners to expend high computational resources.	SPoS suffers from the centralization system if the validator is chosen from a small number of users.
	[5]	Aurand/Hybrid PBFT	Hybrid PBFT which increases the security and on top that an additional consensus mechanism adds up an extra layer of security.	Hybrid PBFT suffers additional computational overhead.
	[12]	Delegated Proof of-Stake (DPoS)	DPoS achieve faster confirmation time for block generation, helps in the scalability issue related to network.	It controls the network, potentially the security is compromised by gaining more influence over the network
	[9]	Proof of Stake Time (PoST)	collateral acts as a deterrent against malicious behaviour, as validators risk losing their stake if they validate fraudulent transactions or produce invalid blocks.	PoST may be vulnerable to long-range attacks,

The issue related to frame consensus mechanism for Internet of Thing devices in the distributed system requires less energy dissipation and scalability. As the number of devices/sensors are huge in numbers for an IoT infrastructure as mentioned in the Fig. 2, the scalability is of greater importance. The algorithm also requires solving consensus in an energy efficient manner as the IoT devices are driven by small power backup. There are some solutions based on hierarchical consensus which can efficiently resolve energy consumption, but still scalability is the curse. In quorum-based consensus algorithm scalability is managed but the issue of energy

consumption pertains. There are methods by which the management of data can be used for optimizing the resources for energy efficiency. These steps are data compression, data aggregation and optimized routing. These steps potentially increase the battery life and decrease network idealization and enhance the consensus algorithm capability.

3. Objectives and Motivation

The use of IoT devices has been gaining popularity over recent years; the industry is equipping their products with IoT devices, e.g. IoT based fans, switches, vehicles and gadgets. On other side of the coin the blockchain3.0 is also about to become the next blooming technology after the advent of internet/WWW. Hence, the applications where blockchain and IoT are leveraged together will have an edge over the existing decentralized application. This will help in securing the captured data associated with sensors, efficient channelization of resource sharing and removing the control of centralization system. But the integration of blockchain technology and IoT have limitations of its own, such as scalability where the IoT devices are enormous in numbers and their communication with each other, another limitation associated with IoT, is that it is equipped with devices which runs on less electrical power. But in blockchain technology the consensus mechanism requires a lot of energy to commit the transactions. So, the need for scalable and energy-efficient consensus algorithm to bring the convergence of IoT and blockchain together.

The Consensus algorithm helps in ensuring the same state for all the nodes in an IoT infrastructure, i.e. all the nodes in the network should concur on a particular value or decision. The system involves the message passing system in which the nodes share the messages for the consensus mechanism. As mentioned in Fig. 3 and Table 1 there are basically two classifications of consensus or fault tolerance the first one is crash fault tolerance, and another is byzantine fault tolerance. The first one is related to concur in the peer-to-peer networking if the system/node malfunction/crashes whereas the latter is based on if the system/node acts maliciously.

The examples of BFT consensus are Istanbul Byzantine Fault Tolerance (IBFT) and Practical Byzantine Fault Tolerance (PBFT), whereas examples for CFT consensus are Paxos and Raft. In Paxos the consensus is made based on message passing, phased in two stages i.e. prepare and accept. Raft is a more efficient consensus mechanism based on leader selection, where the leader is responsible for all consensus related communication.

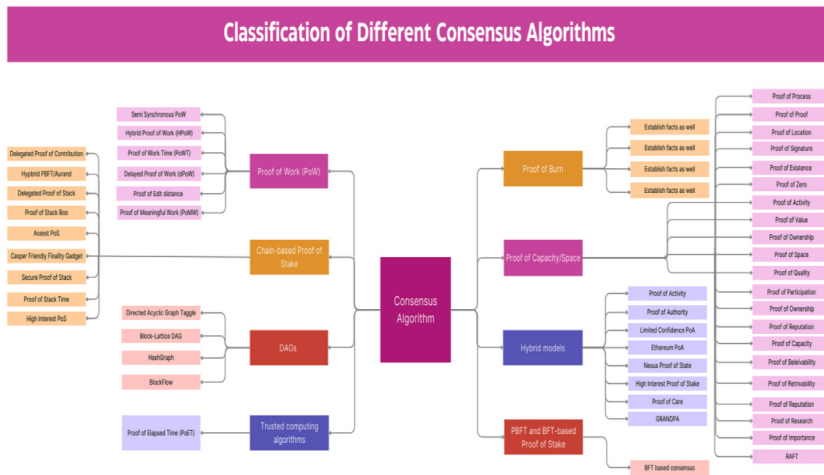


Figure 3

Classification of Different Consensus Algorithm

The PBFT is based on three phase consensus mechanisms, i.e. Pre-prepare, Prepare and Commit. For the pre-prepare step the block is broadcast with the proposer's block, the validators verify proposer's validity and sequence number, in the next step the validator broadcast the proposal's block to all validators, the validators want to receive at least $2F+1$ prepare messages from other validators (F is number of faulty nodes). In the next step the validator sends the commit message to all the validators and in turn if the validator receives $2F+1$ message.

4. Implementation and Results

For the implementation of the Proof-of-Ability consensus algorithm on top of the Hyperledger Fabric. The implementation for the selection requires input i.e. block id (ID), resources for the mining of transactions (MiB, the number of transactions have been mined by the node (NoP) and the number of candidate nodes. The reason for using the Hyperledger fabric is that it supports the Secure Hash Algorithm family 3 i.e. SHA256, which is around 50% faster than its counterpart Keccak256 and it is also very resilient to brute force attack.

The hash of the above information is compared with the target value set, and this hash value found to be greater than the target value then the ID is broadcast, the process is waiting for the candidacy from the other

nodes if the number of the candidate nodes are greater than 20 the number of Target value is updated. The next process includes the voting mechanism to choose the leader for the mining.

Algorithm 1

Algorithm for generating Consensus using Proof of Ability

Input: ID, CiB, NoP, CoN

Output: Consensus

```

1: procedure Consensus_PoAb(ID, CiB, NoP, CoN)
2: if hash(ID + CiB + NoP > Target) then
3: broadcast "ID"
4: waiting for process (p1)
5: receive the candidacies from all nodes.
6: send each received candidacy to all the candidate nodes.
7: if (CoN > 20) then
8: update(Target), failed consensus and broadcast, select new Target,
9: goto 2
10: end if
11: if (CoN < 6) then
12: waiting (p2)
13: end if
14: if (CoN ≥ 6 && CoN ≤ 20) then
15: new result = 0
16: p = 1
17: sort(NoP)
18: while result = 0 do
19: result ← (blocknumber + CoN = 1(Id) mod (CoN + 1))
20: p ← p + 1
21: end while
22: endif
23: end procedure

```

The graph is plotted for the transaction time to mine the transaction for the three-consensus algorithm proof-of-authority (PoA), Proof-of-Work (PoW) and Proof-of-Ability (PoAb). As the number of transactions are increased per block, the amount of amount of transaction time is also increased, but to process transactions the state-of-the-art PoAb requires less time to process the transaction in Fig. 4.

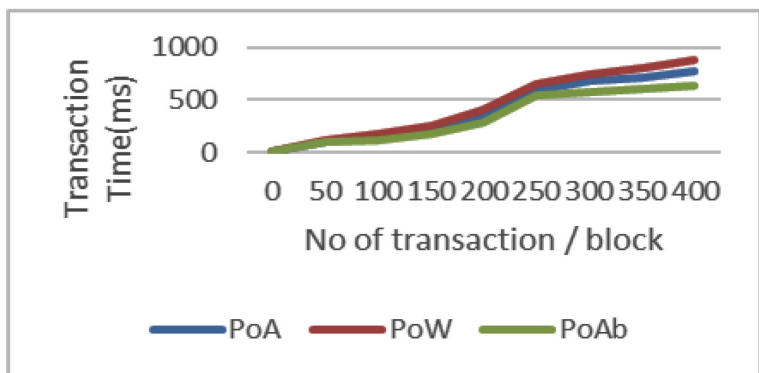


Figure 4
Blockchain Evolution

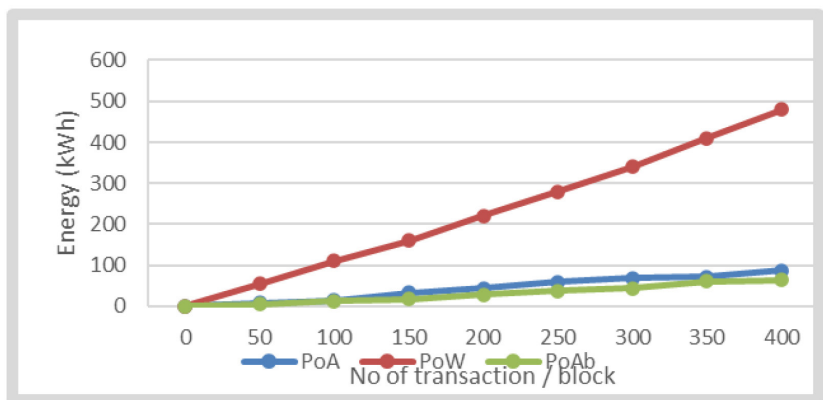


Figure 5
Blockchain Evolution

The energy consumption is plotted in Fig. 5, where the energy consumption is very high in terms of PoW but the energy consumption is comparable for PoA and PoAb. After comparison the PoAb consensus algorithm outperforms PoA by 29.46% in average energy consumption.

5. Discussion and Conclusion

Energy, Security against 51% attack and Fast execution of transaction for a block is an important aspect for any blockchain application. And when it comes to the processing for IoT applications the consensus

algorithm should not be hardware hungry. In this direction this article introduces a novel energy efficient consensus algorithm for the IoT devices which requires less energy and time for processing the transaction. This will reduce the computation time for the miners and the selection for the leader for mining is based on the ability of the node to process the transaction. The ability of the node to process is underlined by fractions of transactions already processed by that node, the computational capacity to mine the node are considered. This simple algorithm makes the selection of the leader in the consortium an easy task. This algorithm achieves fast transaction processing, and the energy consumption is also less by 29% as compared to PoA. Although this algorithm suffers from the issue of dominance by one node if most of the node is processed most of the transactions and has most computational capacity, but in terms of IoT consortium the probability to achieve this scenario is very less.

References

- [1] N. A. Akbar, A. Muneer, N. El Hakim, and S. M. Fati, "Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensususes," *Future Internet*, vol. 13, p. 285 (2021).
- [2] S. Hattab and I. F. T. Alyaseen, "Consensus algorithms blockchain: A comparative study," *International Journal on Perceptive and Cognitive Computing*, vol. 5, pp. 66–71 (2019).
- [3] C. W. Hsueh and C. T. Chin, "E: Solving blockchain problems economically," in *2017 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, San Francisco, CA, USA: IEEE, pp. 1–8 (2017).
- [4] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for industry 4.0: A literature-based review," *Blockchain: Research and Applications*, vol. 2, p. 100027 (2021).
- [5] S. Johnson, P. Robinson, and J. Brainard, "Sidechains and interoperability," *arXiv preprint*, arXiv:1903.04077 (2019).

- [6] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*, Santa Barbara, CA, USA: Springer, pp. 357–388 (2017).
- [7] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652 (2021).
- [8] B. Laurie and R. Clayton, "Proof-of-work proves not to work; version 0.2," in *Workshop on Economics and Information Security* (2004).
- [9] W. Li, S. Andreina, J. M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*, Springer, pp. 297–315 (2017).
- [10] P. Rani and R. Bhambay, "A comparative survey of consensus algorithms based on proof of work," in *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 1*, Springer, pp. 261–268 (2022).
- [11] S. M. S. Saad and R. Z. R. M. Radzi, "Comparative review of the blockchain consensus algorithm between proof of stake (PoS) and delegated proof of stake (DPoS)," *International Journal of Innovative Computing*, vol. 10 (2020).
- [12] D. Stone, "Delayed blockchain protocols," *arXiv preprint*, arXiv:1804.06836 (2018).
- [13] D. Su, L. Zhang, H. Peng, P. Saeidi, and E. B. Tirkolaee, "Technical challenges of blockchain technology for sustainable manufacturing paradigm in Industry 4.0 era using a fuzzy decision support system," *Technological Forecasting and Social Change*, vol. 188, p. 122275 (2023).
- [14] J. Tuwiner, "61 Bitcoin Energy Consumption Statistics (2023)," *Buy-BitcoinWorldwide*.

Received October, 2024