Comparative Study Between Aura and Clique Blockchain-Based Proof of Authority Algorithms on Wireless Sensor Network

Delphi Hanggoro*, Jauzak Hussaini Windiatmaja*, Riri Fitri Sari *
Universitas Indonesia, Depok 16424, INDONESIA

Abstract

Using blockchain in Wireless Sensor Network (WSN) has solved the problems of centralized authority, heterogeneity, authentication, and security. However, no blockchain consensus is intended for WSN applications. Usually, permissioned blockchain is used to integrate into the WSN because of its fast transaction time and easy management member. This study compared two permissioned blockchains consensuses Proof-of-Authority algorithms named Aura and Clique to determine which algorithm is more appropriate for WSN. We compare the suitability of Aura and Clique algorithms, how they work on WSN topology and evaluate each algorithm's transaction speed and block drop. The result shows the transaction speed of Aura has a transaction time of 31.62ms, slower than Clique, which only requires 6.03ms for 100 transactions. Aura has no dropped blocks, whereas Clique has approximately 8 dropped blocks in the number of transactions. This happens because the Clique algorithm has a GHOST protocol that only stores the blocks proposed by one Leader. Aura has a longer transaction time, but Aura does not have discarded blocks. All data from WSN can enter the network. Thus, Aura is more suitable than Clique to apply to WSN.

Key Words: Wireless Sensor Network, blockchain, proof-of-authority, aura, clique.

1 Introduction

Blockchain technology is known as a secure distributed database. Other technologies needed the security advantage of blockchain, such as the Internet of Things (IoT) and Wireless Sensor Network (WSN). Yet, blockchain application to IoT and WSN has solved several problems, including centralized authority, heterogeneity, authentication, and security.

Some of the key challenges of blockchain integration on WSN are resource constraints and network architecture. To overcome resource problems, previous studies modified the consensus of existing public blockchains such as Proof-of-Work (PoW) [21] and Proof of Stake (PoS) [7] to reduce power and memory use on the sensor devices.

*delphi.hanggoro@ui.ac.id, jauzak.hussaini@ui.ac.id; riri@ui.ac.id

However, lately there are some new types of blockchain, such as private and consortium, which are intended for devices that have limited resources. The private type is more for personal use in a company, while consortium (permissioned) is more commonly used in several companies with the same business interest. According to Biswas et al. [5], permissioned blockchain is a type of blockchain that is intended for a business of two or more companies, network members can also be easily maintained. In addition, the permissioned blockchain does not consume enormous resources and has fast transaction times, which is suitable for IoT integration. Singh et al. [25] study reinforce the use of a permissioned blockchain, proved that the Proof-of-Authority (PoA) [24] consensus can be a lightweight solution for IoT smart homes.

Proof-of-Authority (PoA) is part of a permissioned blockchain developed and deployed on the Ethereum private network. The way Proof of Authority (PoA) works is by leveraging identity values, so block validators are not risking coins, but their own reputation. Therefore, the PoA blockchain is secured by an arbitrarily selected validation node as a trustworthy entity. Proof of Authority relies (PoA) on several block validators. This makes it a highly scalable system. Pre-approved participants who act as system moderators verify blocks and transactions. Networks that use PoA consensus do not require any mining activity. This type of consensus mechanism also does not require a lot of resources, so it is appropriate to be integrated into the WSN.

Furthermore, to answer the challenges of network architecture Alghamdi et al. [1] tried the solution of Bozorgi et al. [6] and Zhang et al. [29] to use the clustered network architecture on the WSN network which is assumed to be hierarchical routing algorithms as a solution for implementing blockchain on the WSN. The results of research by Alghamdi et al. [1] shows lower energy consumption than flat routing algorithm on large-scale WSN and have greater adaptability. In addition, Cui et al. [10] has also implemented clustered WSN in his research. Based on his research, clustered WSN has flexibility in the division of tasks so that each device has a specific task that does not burden other devices.

In Ethereum there are two different algorithms for PoA: Aura [2] and Clique [9], which have differences in the validation process and the number of block proposers (Leaders).

This study analyses the Aura and Clique algorithm's compatibility with WSN and evaluates the performance. Our contribution to this research is to compare the suitability of the Aura and Clique's works on WSN topology. Subsequently, we evaluate and compare the transaction speed and block drop on the Aura and Clique algorithm.

The rest of this research is structured as follows: Section 2 is the literature review of blockchain and consensuses, blockchain integration on IoT, and PoA details. Section 3 discusses the comparison method. Section 4 presents the results and discussions. Finally, Section 5 describes the conclusions.

2 Literature Review

2.1 Blockchain and Consensus Algorithm.

Blockchain is a distributed and decentralized data structure. Primarily, blockchain is used to record a digital transaction on a crypto network. "Bitcoin" [21] is the original application of the use of blockchain for digital currency which was developed by Satoshi Nakamoto in 2008. Bitcoin is formed by a Peer-to-Peer (P2P) network. Bitcoin does not require a central server to host the blockchain and store transaction history, unlike server-based systems. In contrast, bitcoin keeps a copy of the blockchain/ledger on all network members, thus forming a decentralized public ledger.

Each block consists of data that has been verified and then wrapped by a hash with a specific target. The block is linked to the previous block's hash, as shown in Figure 1. Once a block is created, it will be distributed to all nodes on the blockchain to form a decentralized blockchain.

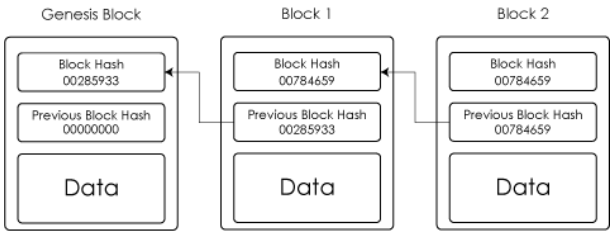


Figure 1: Blockchain recording mechanism

Blockchain security is made up of four technological features that ensure reliable and secure data services [28]:

(1) Distributed ledger: all network members share the same data, making tamper or change difficult. All members are responsible for monitoring legitimate transactions. (2) Authorization and asymmetric encryption: although every member can see data that has entered the network, every identity is properly encrypted and can only be accessed by the data owner, who can ensure identity privacy. (3) Smart contracts: are predefined codes that are trusted and tamper-proof; smart contracts will be executed automatically when certain conditions are met. (4) Consensus Algorithm: a key feature of blockchain, a consensus algorithm is a mechanism for all nodes on a blockchain network to agree on the data that will enter the network.

The consensus used in a blockchain system depends on the type of blockchain. There are three types of blockchain: Public, Private and Consortium.

2.1.1 Public Blockchain. Public blockchain is the first type that exists on the blockchain. Each member on the network has the same power to read and write data on the blockchain network with agreed rules. Each member can freely enter and leave the network, validating transactions with the required hardware and certain software. Thus, a public blockchain is a type of blockchain that is fully distributed and decentralized because there is no entity that manages and controls the rules of the blockchain network.

However, due to the large number of devices, public blockchain generally requires a large amount of time and resources to reach an agreement. Examples of popular consensus of this type are: Proof-of-Works (PoW) used by bitcoin and Proof-of-Stake (PoS) used by Ethereum.

Proof-of-Work (PoW) [21] PoW works with the concept of "mining" competition. Each node that wants to get a reward must compete simultaneously to solve a mathematical puzzle of a certain hash target. The node that solves the puzzle first will be rewarded with the cryptocurrency or token used in the system, for example, Bitcoin or Ether on Ethereum. PoW is a well-known consensus with excellent integrity and can tolerate several attacks [11]. However, PoW has some drawbacks, such as consuming many resources, such as computing and electrical power. Such waste causes many problems to be integrated into other fields with limited resources.

Proof-of-Stake (PoS) [7] Proof-of-Stake (PoS) is a development of PoW that consumes a lot of resources. The mining concept on PoW is still carried out on PoS, but there is no competition in PoS. PoS will select nodes that can propose blocks based on the number of stakes or cryptocurrencies on the network to replace the competition. The node with the highest stake will be chosen as the miner. Working concepts like this can drastically solve the problem of resource usage in PoW. However, with the work concept based on "stake", an additional problem arises: it will enrich nodes that already have a lot of stakes. Meanwhile, nodes with few stakes can not become block proposers, so the distribution of energy use is uneven. In addition, multiple nodes with the highest stake can dominate the network and increase the risk of a 51 percent attack.

2.1.2 Private Blockchain. Private blockchains have a different structure from public blockchains, while public blockchains are fully decentralized, private blockchains have a fully centralized structure. To be able to enter the blockchain network, new members need permission from the centralized entity to be able to access, write and validate blocks on the blockchain. The advantage of a private blockchain is that it provides privacy to all members of the blockchain network compared to public blockchains. However, it has drawbacks because there are several parties who have full control over the

rules of the blockchain network.

Private blockchains are suitable for cases where readability or public audit is not required. In addition, a high level of trust must be built between participants. Compared to public blockchains, private blockchains have faster transaction speeds and lower transaction costs because in general the mathematical competition process will be replaced by a verification process by each member. "Raft" [22] is a consensus example of implementing a private blockchain.

Raft [22] Raft is an implementation of ordering service consensus, which is a development of Crash Fault Tolerant (CFT). CFT allows a consensus process to continue to run even though the process has N failures, while there are N/2+1 nodes running. In addition, Raft implements a "Leaders and Followers" process that uses consenters on the ordering service nodes. Raft's most popular application is the Hyperledger Fabric. In Hyperledger Fabric, Raft is implemented as a bridge link to build PBFT consensus, because PBFT and Raft have similar procedures in Hyperledger Fabric integration.

2.1.3 Permission Blockchain. Consortium blockchain (permissioned blockchain) is a combination of public and private blockchain. Permissioned blockchains have the characteristics of being partly decentralized, only some members of the network have rights to access and validate transactions. Rights on the network are determined by the identity and role of the members in the system's design. Usually, a permissioned blockchain comprises several companies with the same business interests, so it requires a smart contract to perform and validate identities and business logic before committing to transactions.

Popular permissioned blockchain implementations are Hyperledger with consensus Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Elapsed-Time (PoET), OpenEthereum with consensus Authority Round (AuRa), Go-Ethereum with consensus Clique.

Proof-of-Elapsed-Time (PoET) [11] PoET is a type of permissioned blockchain developed by Intel in early 2016. Consensus PoET uses the lottery concept for each network member, which requires members to wait for some time according to the lottery they receive. If one of the members has finished proposing a block, the time to be waited for will be reset and get a random time again. Thus each member has the same opportunity to be able to propose a block. The most famous application of PoET is on the Hyperledger Sawtooth platform.

Practical Byzantine Fault Tolerance (PBFT) [8] Consensus that use rotation to select proposers (Leader) of blocks on the blockchain network. In PBFT, one Leader will be chosen while the others will be the backup. Each node must be connected to the other. The validation process in PBFT requires all nodes to check each other's contents of blocks that the Leader has proposed, so that the more network members, the longer the validation time.

Proof-of-Authority (PoA) [12] Like PBFT, PoA adopts a round-robin rotation of proposers (Leader) so that all nodes will get a turn to become block proposers. Proof of Authority (PoA) is a family of consensus algorithms for permissioned blockchains known for their improved performance compared to Byzantine Fault Tolerance algorithms. PoA was initially proposed as part of the Ethereum ecosystem for private networks.

2.2 Blockchain Integration on IoT and WSN

Implementing blockchain technology was first introduced by Satoshi Nakamoto [21] in 2008 for cryptocurrencies, and advanced to implementing finance, healthcare, decentralized applications, voting systems and the Internet of Things (IoT) [4, 13, 15, 18, 26]. Blockchain has the characteristics of decentralization, immutable, integrity and reliable. With these characteristics, blockchain can solve some of the existing IoT issues. Several studies on blockchain implementation in IoT have solved issues such as centralized authority, heterogeneity and authentication [3, 5, 14, 16, 19, 20, 27].

According to Biswas et al. [5], the use of permissioned blockchain is more appropriate than public blockchain because permissioned blockchain has a less consumption of computing power, energy and storage resources than public blockchain. In their study, Biswas et al. [3] built a secure framework for IoT using Hyperledger Fabric. They designed each IoT device to implement a client peer and become part of the blockchain network. Besides that, they also grouped some IoT devices and used one of them to become a single peer global. As a result, they can significantly increase the speed of transactions in the blockchain network.

Ayoade et al. [3] have built a decentralized data management system on top of Ethereum that uses smart contracts to manage access permissions and audit trails. It can record all data on the blockchain. As a result, Ethereum's transaction throughput per second will increase as the write workload increases, limiting the blockchain's scalability. Thus, they suggest using a permissioned blockchain to save time, as all nodes are assumed to know each other. Singh et al. [25] has also tested the use of a permissioned blockchain. They have tested the performance of the consensus PoA algorithm and compared it to consensus PoW for smart home device management with the raspberry pi 3. As a result, PoA uses much lower CPU utilization compared to PoW. Thus, PoA has the potential to be a lightweight consensus solution for IoT.

Aside from resource consumption, blockchain and WSN have problems with the way they communicate. WSN communicates on a multi-hop, while blockchain uses peer-to-peer communication. To resolve the differences in how to communicate on IoT and blockchain, several researchers apply clustering to the WSN network on blockchain. Clustering is a method in the form of groups on WSN nodes. Each cluster has a common node, a cluster head and a base station. The cluster head collects data from ordinary nodes and then collects it at the base station. Clustering on WSN has been shown to consume less energy and has better adaptation than flat routing algorithms [6, 29].

Cui et al. [10] use blockchain as identity authentication on WSN, usually relying on trusted third parties with a single point of failure risk. They divide the entire network into several types based on the capabilities of the nodes, namely ordinary nodes, base stations and cluster heads that form a hierarchical network. They divided the blockchain network into public and local network. Each base station and end-user are interconnected, forming a public blockchain. Public blockchains are useful for registering and authenticating cluster node heads and providing authenticated communication between nodes across WSNs. The local blockchain registers ordinary nodes for authentication. Ordinary nodes create smart contracts deployed to the cluster head to verify registration and authentication requests. The security and performance analysis shows that the scheme has comprehensive security and better performance.

2.3 Proof-of-Authority

In its implementation, Aura and Clique have different validation methods. Both algorithms have the same first stage where the block proposer (Leader) is currently proposing a new block (block proposal). However, the Aura algorithm requires a second stage, namely block acceptance, while the Clique algorithm does not, as we can see in Figure 2.

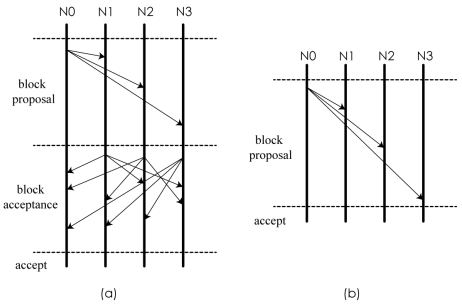


Figure 2: Step-by-step message exchange at the proof-of-authority algorithm. (a) Aura, (b) Clique

2.3.1 Authority Round (AuRa). The AuRa algorithm was first used by an Ethereum client named OpenEthereum [23] which uses the Rust programming language. All members on Aura are assumed to be synchronized in UNIX time t in a synchronous network.

$$\frac{UNIX\,time}{t} \tag{1}$$

Time is divided into discrete steps of duration t, determined by the equation 1. Each authority calculates deterministically the index i of each step as

$$i = t/StepDuration \tag{2}$$

Where $StepDuration$ is a constant that determines time UNIX for each step. The Leader in step i is the authority identified by equation 3, where N = number of nodes.

$$l = i \bmod N \tag{3}$$

Each authority has a local transaction queue (Qtx) and blocks queue (Qb). Every transaction that has been made will be collected at $(Qtxn)$ for each authority. At each step, the Leader enters the transactions in $(Qtxn)$ into block b and then broadcasts the block to another authority (block proposal step in Figure 2(a)). Then each authority will send the received blocks to other authorities for validation (acceptance block step in Figure 2(b)). If all authorities validate that block b received is the same, then block b will enter the queue (Qb). All blocks that are validated even if they are empty will enter the queue, but if the block to be included in the queue is proposed by an authority that is not expected to become a Leader then the block will be rejected.

Block b in queue Qb will be committed to the blockchain network when most authorities have proposed their block. In these networks, the majority of authorities can be trusted, which can prevent suspicious leaders from committing illegal blocks. Any suspicious behavior (such as different block contents in the validation process) will trigger a vote in which a majority can reliably blacklist the current Leader. The blocks they propose can be discarded before being executed and committed on the blockchain network.

Block finality in the Aura algorithm is a condition where the block in the Qb queue will enter the network when the queue has reached a certain condition. In step s1 on the blockchain, the block is committed up to two times, while the block $bi+1 \cdots bi+n$ is pending. Block bi can be committed because $n = \frac{k}{2}+1$ where k is the number of proposed blocks. The next block has been proposed after bi, and thus block bi can be finalized. Likewise, in step $s2$, block $bi+1$ can be finalized because the queue contains further blocks, as shown at Figure 3.

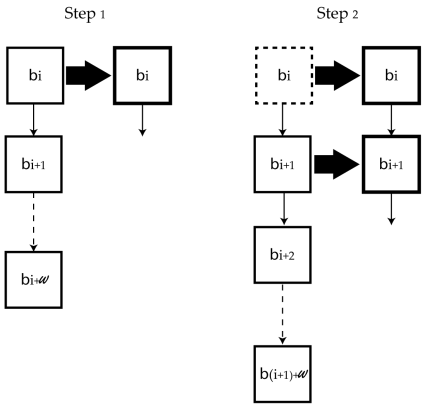
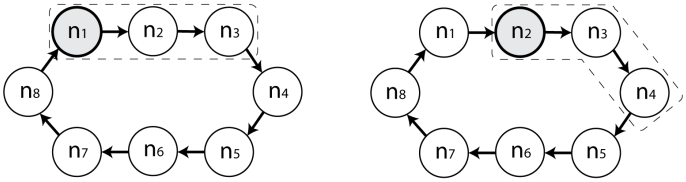


Figure 3: Aura finality mechanism

2.3.2 Clique. The Clique algorithm [9] is the original consensus used on the Go-Ethereum (Geth) platform [17]. In Clique's algorithm a member of the network is named "authority" which has a unique ID. Each authority is responsible for validating and mining blocks (block proposer) on the blockchain network. The task of becoming a block proposer is then determined using round robin fashion on the registered

unique ID.

The Clique algorithm determines the steps and the Leader by combining the amount of authority and the block number. In the Clique algorithm, n authorities may propose blocks at each step, as shown in Figure 4 (a), $n1$ being the Leader, $n2$ and $n3$ can propose blocks. To avoid an authority that can screw up the network, each authority is only allowed to propose one block every $N/2+1$ block. So, there are at least $N(N/2+1)$ authorities allowed to propose blocks for each step. Just like Aura, if the Leader acts suspiciously, we can expel them. Voting against other authorities can be carried out at every step, and if conditions are met, the authority is removed from the list of valid authorities.



(a) (b)

Figure 4: Clique leader selection

Figure 4 shows two successive Leader selection steps. For example, if there are $N=8$ authorities on the network, then there are $N(N/2+1)=3$ authorities who have the right to propose blocks at every step. So, as we can see in Figure 3(a), $n1$ is the current Leader, while $n2$ and $n3$ may propose blocks. In Figure 3(b), $n1$ cannot submit a block because it is no longer a Leader which requires it to wait for a number of $N/2+1$ steps to propose another block. Meanwhile, $n4$ is the sub-leader who can propose blocks, and $n2$ is the current Leader.

Because multiple Leaders can propose blocks during each step, forks can occur. However, the possibility of a fork is limited because every non-leading authority that proposes a block delays its block randomly, so the Leader's block will probably be the first to be accepted by all authorities. If a fork occurs, the GHOST protocol [12] is used. GHOST (Greedy Heaviest Observed Subtree) protocol is a protocol on the blockchain. This protocol is tasked with selecting a valid chain and proceeding as the main chain.

In the Clique algorithm, the GHOST protocol used is based on a block score approach, i.e., the leader block with the higher score will be the block that enters the blockchain, thus ensuring that the fork will eventually be resolved.

Fork in Clique algorithm is a condition where the last block at each node is different, so the network must determine which block will be used as a reference and the main chain. Figure 5 (left). illustrates the step in which authority leader $n2$ and authority non-leader $n3$ propose a new block simultaneously. In this step, $n3$ and $n4$ have the second block (b2) proposed by $n3$. Whereas $n1$, $n2$ and $n5$ have blocks proposed by $n2$. In the end, the block proposed by $n3$ on $n4$ will be replaced by $n2$. As shown in Figure 4 (right), each authority easily detected the resulting fork during the next block because the proposed next block will reference the previous block that is not available for the authority. The GHOST protocol used in the Clique algorithm is a scoring mechanism where if there are two authorities who propose a block simultaneously, only the block from the Current Leader $(n2)$ will enter the blockchain. Therefore, the GHOST protocol can overcome the fork.

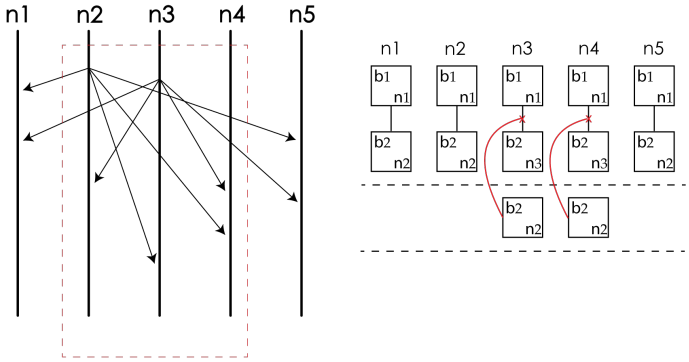


Figure 5: GHOST protocol mechanism when fork occurred

3 Comparison Method

In this study, two aspects will be compared and analyzed. First, we describe the experimental setup on Aura and Clique to compare transaction time and block drop performance. Second, we explain the method of comparing the message exchange of the Aura and the Clique algorithms on WSN with the cluster topology.

3.1 Experiment Setup

We carried this performance comparison experiment with Virtual Machine software with six processor cores and 8 Gb of memory on a personal laptop with Intel I7-9750H, 32 GB DDR4 memory, Nvidia GTX 1660 Ti, and 1 Tb M.2 NVME SSD. We are testing Aura on Ethereum Client OpenEthereum version 3.3.2 and Clique on Ethereum Client GoEthereum (GETH) version 1.10.14.

Table 1 contains the configurations listed in the test. The number of nodes and authority used is 8, the block interval is 15 seconds and the total transactions made are 100 per node. The default difficulty used is 1. To simulate IoT conditions, each node will send one transaction every 5 seconds.

3.1.1 Message exchange Mechanism. Based on the message exchange mechanism in Aura and Clique, the exchange of proposal block messages will be distributed to each network node and accepted by each node. The key challenge of implementing Proof-of-Authority on WSN is the different ways of communication. Blockchain communicates peer-to-peer, while WSN communicates in a multi-hop manner with a mesh topology. Figure 6 shows an example of implementing

Table 1 : Simulation configuration settings

Parameter	Authority Round	Clique
Number of Node	8	8
Number of Authorities	8	8
Block interval	15s	15s
Total transaction	100 per node	100 per node
Difficulty	1	1

the Proof-of-Authority (PoA) message exchange in a mesh topology commonly used in WSN networks.

When Proof-of-Authority is applied directly to the mesh topology, as shown in Figure 6, each transaction will consume a large amount of energy on the network. For example, when node 1 wants to submit a message for a block proposal, node 1 must deliver the message to node 2 through node 8. However, node 1 cannot communicate to node 8 directly, so the message must be delivered in a multi-hop through node 2 – node 4 – node 7 or another path to node 8. Naturally, the intermediary device (node 2, node 4 and node 7) will have more burden to convey messages from other nodes, so it is necessary to choose the right topology to implement Proof-of-Authority on WSN.

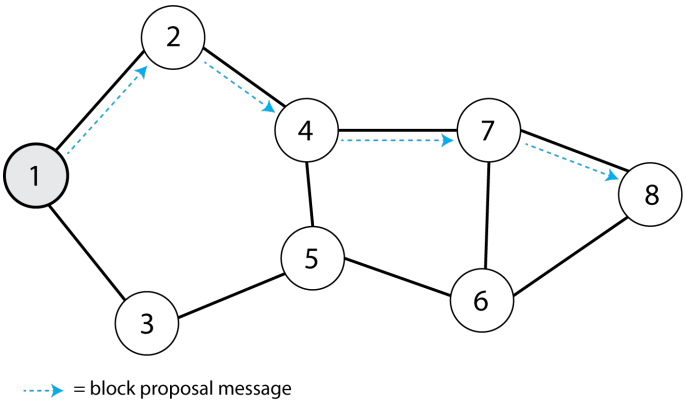


Figure 6: PoA message exchange on mesh topology

The study of Cui et al. [6] and Alghamdi et al. [7] has implemented a blockchain on a WSN as a cluster with a star topology. They suggest that dividing WSN devices into clusters will make blockchain integration easier. Their schemes have better performance results. However, blockchain implementation cannot be applied directly to the star topology. So, the message exchange mechanism needs to be modified to run on a star topology.

Figure 7 shows the ideal modification of the message exchange mechanism proposed by the researcher so that Proof-of-Authority can be optimal in a star topology. Nodes will be divided into two types: ordinary nodes that will serve as authorities and base stations as intermediaries for each node to communicate and validate. The ordinary node will be connected directly to the base station, which is assumed to have no problem with limited resources. Thus, ordinary nodes are not burdened by communication between nodes.

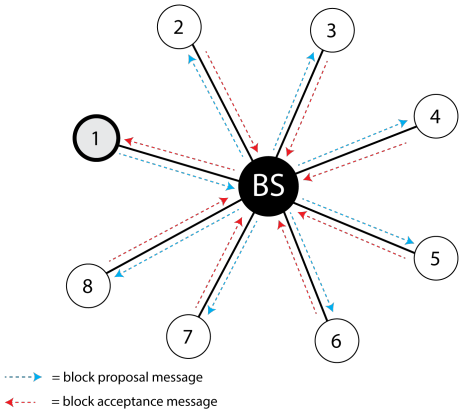


Figure 7: Ideal message exchange for WSN

4 Result and Discussion

4.1 Message Exchange Compatibility

Aura has a proposal block message exchange process - block acceptance - accept, as shown in Figure 8 When the message exchange process starts, Leader of the ordinary node will distribute the proposal block message to all nodes through the base station.

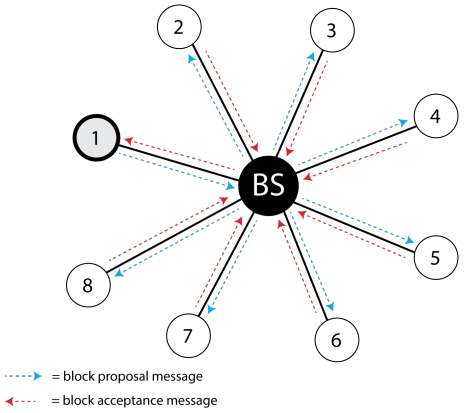


Figure 8: Aura algorithm message exchange scheme on WSN

Subsequently, the base station will distribute the message to all nodes and give a reply (block acceptance) to the Leader node, and the block status will change to “accept”. Each node will validate and enter the block into the blockchain. Assuming the base station has no limit on computing and energy resources than WSN nodes, this scheme can apply to clustered WSN. However, a message exchange scheme like this will cause scalability problems. Scalability occurs because the more node members, the more time it will take to distribute and validate from the node to the base station.

Figure 9 shows a schematic of the clique algorithm for exchanging messages in a star topology. The advantage of implementing Clique in this topology is that it has a number of $N(N/2+1)$ Leaders who can propose blocks simultaneously. In addition, the message exchange process on Clique is also shorter than Aura based on Figure 1, where Clique does not require the block acceptance stage. Thus, at one time there are several Leaders who enter blocks into the network and a short message exchange process and increase the transaction throughput. However, Clique has a very fatal drawback for WSN which makes the block unable to enter the network due to the formation of a fork. According to the GHOST protocol, only blocks from the main Leader can enter the network, and blocks from other Leaders will be discarded.

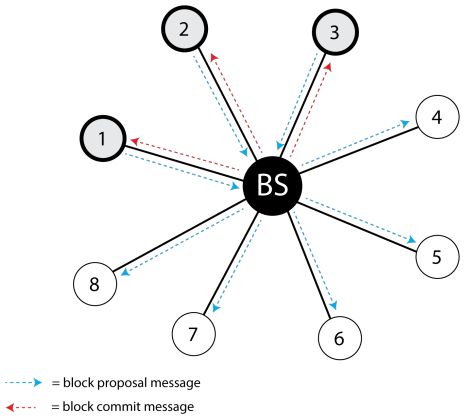


Figure 9: Clique algorithm message exchange scheme on WSN

Unfortunately, the execution of the GHOST protocol is not suitable for its application to WSN because WSN will always continue to provide valuable data. If some data from its members is discarded during the block proposal process, it will reduce the essence of implementing WSN itself. Thus, the mechanism of the Clique is not optimal compared to AuRa because it wastes valuable information. The best solution for this implementation is to modify or replace the GHOST protocol to have a function to have a block queue, so that proposed blocks from sub-Leaders are not discarded.

4.2 Performance Evaluation

4.2.1 Transaction time. Transaction time on a blockchain network is the time it takes for a blockchain system to validate transactions. In the permissioned blockchain, we can set the block interval as needed so that the block speed will be static, but the message exchange mechanism affects the transaction speed in the Aura and Clique algorithms. We can see the comparison of transaction speed in Figure 10.

Aura's transaction time is longer than Clique's on each node, as shown in Figure 10, in 100 transactions, Aura has an average transaction time of 31.62 ms, while Clique has an average transaction time of 6.03 ms. This is because the Aura scheme requires block acceptance, as shown in Figure 1, during block verification, while Clique does not. So, the more nodes, the higher the time to exchange messages on Aura. Meanwhile, Clique has a faster transaction time because it only requires a proposal block during the message exchange process.

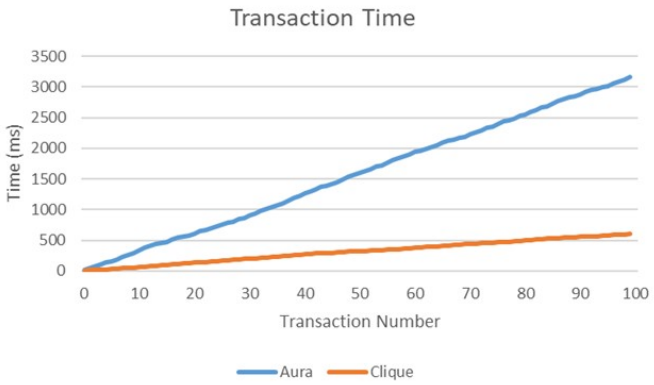


Figure 10: Transaction speed comparison

4.2.2 Transaction Drop. Transaction Drop is transaction data in the queue that is deleted and does not enter the blockchain network. On the WSN network, data will be represented by transactions continuously entered into the blockchain, which can trigger a transaction drop on the blockchain network. The comparison of transaction drops can be seen in Figure 11. Aura had no dropped transactions. All transactions submitted by each authority have been successfully verified (mined).

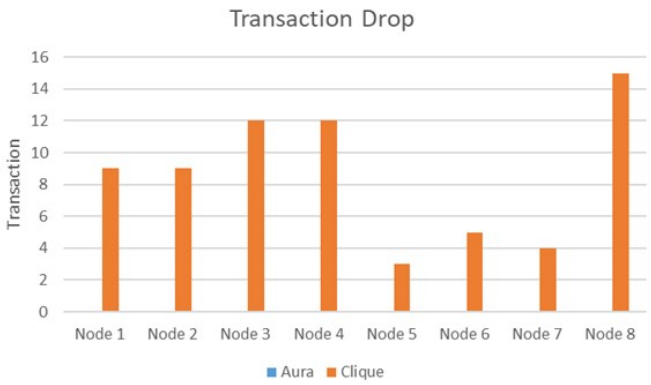


Figure 11: Transaction drop comparison

This is because Aura only rotates one Leader who can propose for a block at every step, so there are very few forks. Meanwhile, Clique had 69 transactions drop out of 800 transactions that had been entered or about 8 percent of transaction drops, as shown in Figure 6. Clique allows blockchain networks to have $N(N/2+1)$ Leader. At each step, several authorities can submit blocks simultaneously.

In Clique, if a fork occurs, the GHOST protocol will be executed, which only includes the proposed block from the

Leader, while the proposed block from the sub-leader will be discarded. Each block on Clique contains three transactions. So, the number of transaction drops that occur is the number of blocks multiplied by three.

Based on the evaluation results, both consensuses have advantages and disadvantages to WSN. However, Aura will be easier to develop for its integration to clustered WSN than Clique. Aura's message exchange mechanism can be implemented on WSN. Other than that, Aura had no problems with Fork formations. However, modifying the message exchange mechanism is necessary to improve the transaction time.

On the other hand, Clique has more challenges in its application to clustered WSN. Although the transaction speed is high, if the incoming data is not intact by all nodes, it will be a problem with WSN technology. This happens because the GHOST protocol on Clique will remove blocks that contain valuable data, which is the main essence of WSN technology.

5 Conclusion and Future Works

This research has carried out the integration of blockchain technology using Proof-of-Authority on WSN. Block generation is proven to be faster and uses less power when PoA is used. In addition, monitoring and management of network members can be carried out using PoA consensus. The comparison results show that Aura has a Transaction time of 31.62 ms / 100 transactions, while Clique has 6.03 ms / 100 transactions. Even though Aura's transaction speed is slower, Aura doesn't have any wasted blocks, as with Clique, which has about 8 percent of the total transactions. The term "transaction" in the WSN system is input data such as sensor data, monitoring data, and image data categorized as valuable and resulting from environmental observations from WSN devices. Losing a transaction on the blockchain system integrated with the WSN is a shortcoming that removes the essence of the WSN technology itself. Thus, Aura is more suitable to apply to WSN compared to Clique.

For future work, researchers will continue to implement and adapt the peer-to-peer blockchain into a star topology (WSN cluster) to produce a Proof-of-Authority design that can be optimally applied to WSN.

Acknowledgments

This work is supported by the Indonesian Government Scholarship PMDSU Grant number NKB-3046/UN2.RST/HKP.05.00/2020 from the Ministry of Research, Technology, and Higher Education (Kemristekdikti).

References

[1] N. S. Alghamdi and M. A. Khan, "Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities," *CMC-Computers Materials Continua*, 66(3):2509-2524, 2021.

[2] "Aura." [Online]. Available: https://openethereum.github.io/Aura, 2022.

[3] G. Ayoade, K. Hamlen, V. Karande, and L. Khan, "Decentralized IoT Data Management Using Blockchain and Trusted Execution Environment," in 2018 IEEE International Conference on Information Reuse and Integration (IRI), IEEE, pp. 15-22, 2018.

[4] M. Banerjee, J. Lee, and K.-K. R. Choo, "A Blockchain Future for Internet of Things Security: A Position Paper," *Digital Communications and Networks*, 4(3):149-160, 2018.

[5] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," *IEEE Internet of Things Journal*, 6(3):4650-4659, 2018.

[6] S. M. Bozorgi and A. M. Bidgoli, "HEEC: A Hybrid Unequal Energy Efficient Clustering for Wireless Sensor Networks," *Wireless Networks*, 25(8):4751-4772, 2019.

[7] V. Buterin, "Ethereum: Platform Review," Opportunities and Challenges for Private and Consortium Blockchains, 2016.

[8] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Transactions on Computer Systems (TOCS)*, 20(4):398-461, 2002.

[9] "Clique." [Online]. Available: https://github.com/ethereum/EIPs/issues/225, 2022.

[10] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang and J. Chen, "A Hybrid Blockchain-based Identity Authentication Scheme for Multi-WSN," *IEEE Transactions on Services Computing*, 13(2):241-251, 2020.

[11] B. Curran, "What is Proof of Elapsed Time Consensus?(PoET) Complete Beginner's Guide," ed: Blockonomi. url: https://blockonomi. com/proof-ofelapsed-time-consensus, 2018.

[12] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," Italian Conference on Cyber Security, 2018.

[13] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A Trust Architecture for Blockchain in IoT," in Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 190-199, 2019.

[14] G. Dittmann and J. Jelitto, "A Blockchain Proxy for Lightweight IoT Devices," in 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 82-85, 2019.

[15] F. M. Enescu, N. Bizon, A. Cirstea, and C. Stirbu, ”Blockchain Technology Applied in Health the Study of Blockchain Application in the Health System (I),” in 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), IEEE, pp. 1-4, 2018.

[16] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, ”Healthcare and Fitness Data Management Using the IoT-based Blockchain Platform,” *Journal of Healthcare Engineering*, 2021:12 pp, 2021.

[17] ”Go Ethereum.” [Online]. Available: https://github.com/ethereum/go-ethereum, 2021.

[18] F. . Hjálmarsson, G. K. Hreiarsson, M. Hamdaqa, and G. Hjálmtýsson, ”Blockchain-Based E-Voting System,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986, 2-7 July 2018.

[19] M. A. Islam and S. Madria, ”A Permissioned Blockchain Based Access Control System for IoT,” in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 469-476, July 2019.

[20] T. Kim, J. Noh, and S. Cho, ”SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network,” in 2019 IEEE International Conference on Consumer Electronics (ICCE), IEEE, pp. 1-4, 2019.

[21] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System.” Decentralized Business Review: 21260, (2008).

[22] D. Ongaro and J. Ousterhout, ”In Search of an Understandable Consensus Algorithm,” in 2014 USENIX Annual Technical Conference (Usenix ATC 14), pp. 305-319, 2014.

[23] ”OpenEthereum.” [Online]. Available: https://github.com/openethereum/openethereum, 2021.

[24] V. B. Pavel Khahulin Igor Barinov, ”PoA Network White Paper,”. [Online]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper, 2018.

[25] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, ”Managing Smart Home Appliances with Proof of Authority and Blockchain,” *International Conference on Innovations for Community Services*, Springer, pp. 221-232, 2019.

[26] P. Treleaven, R. G. Brown, and D. Yang, ”Blockchain Technology in Finance,” *Computer*, 50(9):14-17, 2017.

[27] L. Wu, W. Lu, F. Xue, X. Li, R. Zhao, and M. Tang, ”Linking Permissioned Blockchain to Internet of Things (IoT)-BIM Platform for Off-Site Production Management in Modular Construction,” Computers in Industry, 135:103573, 2022.

[28] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, ”A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks,” Sensors, 19(4):970, 2019.

[29] R. Zhang, J. Pan, D. Xie, and F. Wang, ”NDCMC: A Hybrid Data Collection Approach for Large-Scale WSNs Using Mobile Element and Hierarchical Clustering,”*IEEE Internet of Things Journal*, 3(4):533-543, 2015.

Delphi Hanggoro is an PhD student at Universitas Indonesia. He graduated from Computer Engineering at Diponegoro University in 2017, then continued Post Graduate at the University of Indonesia in 2018 and graduated in 2020. He is currently in the process of completing his PhD on the topic of performance improvement on consensus in the permissioned blockchain.

Jauzak Hussaini Windiatmaja has completed a bachelor’s program in Computer Science at Diponegoro University in 2018, he continued Post Graduate at the University of Indonesia in 2019 and graduated in 2021. He is currently running a PhD program at the Department of Electrical Engineering, University of Indonesia with topic integrating machine learning with blockchain.

Riri Fitri Sari She earned a Bachelor of Electrical Engineering from UI in 1994 and a Masters in Human Resources from Atmajaya University Jakarta in 1996. In 1997, she received an MSc in Software Systems and Parallel Processing from the Department of Computer Science, University of Sheffield, England with the Chevening Award from the British Council. She successfully finished her doctoral dissertation with research in the field of Active Network Congestion-Based Congestion Management and obtained her PhD from the School of Computing, University of Leeds, England. She was confirmed as a Professor in Computer Engineering in May 1, 2009, in the Department of Electrical Engineering, Faculty of Engineering, University of Indonesia. Currently, she is actively

teaching and researching in the fields of Computer Networking, Grid Computing, Information and Communication Technology implementation. From various scientific publications in the form of international journals and presentations at various electrical and computer engineering conferences in various countries and achievements in the application of information technology, Riri Fitri Sari was chosen to be a Senior Member of the Institute of Electronics and Electrical Engineers (IEEE).