Designing a Blockchain-based SME transaction model using the Federated Byzantine Agreement to shorten transaction validation times

[1] Bernardinus Harnadi, [2] Erdhi Widiyarto
Information Systems Department, Computer Science Faculty
Soegijapranata Catholic University, Semarang, Indonesia
[1] bharnadi@unika.ac.id, [2] erdhi@unika.ac.id

Abstract— Since the world experienced the Covid-19 pandemic, the role of MSMEs in the e-commerce sector has grown rapidly and contributed 50% of Indonesia's GDP. However, investors and some consumers still underestimate MSMEs. They have a low level of trust in MSMEs. This is due to the lack of a transparent system so that cases of fraud against MSME products often occur. This issue of trust and transparency needs to be resolved with technological solutions. One technology that can solve this problem is Blockchain. However, currently there are still validation problems if it is to be implemented in MSMEs. This research aims to resolve validation time constraints in the implementation of MSMEs. This research builds a Blockchain-based MSME transaction model using Federated Byzantine Agreement (FBA) algorithm to solve validation time problems. The result shows that FBA is able to complete transactions with the fastest validation time compared to Proof of Work (POW), Proof of State (POS), and Proof of Authority (POA).

Keywords— Blockchain, FBA algorithm, transaction model, MSME, validation time.

I. INTRODUCTION

MSMEs play an important role in the progress of the business world in many countries. In recent years, MSMEs have experienced significant growth and have become one of the main sectors driving Indonesia's economic growth. In Indonesia, MSMEs are able to provide employment opportunities and play an important role in equalizing development results. The average growth of MSMEs reaching 4.2% per year shows a major contribution in increasing 50% of Indonesia's Gross Domestic Product (GDP) in the last 3 years [1]. On the other hand, MSMEs have characteristics such as operating on a small scale, low stability, lacking brand value, and inadequate data collection. These characteristics contribute to financing and transaction problems. An imperfect financial transaction system causes funding problems for MSMEs and information asymmetry creates problems in matching and tracking transactions.

Because MSMEs are considered to have a high risk of default, banks usually charge higher loan interest to MSMEs than large companies. MSMEs also have weak survival capabilities and an inefficient economic system. It also has experienced difficulty finding the right business partner due to limited information and the small market influence he had. Lastly, MSME transaction information is also vulnerable to change and difficult to track, which can be detrimental to partner companies.

The next condition, the large adoption of e-commerce platforms, has also driven the increase in popularity of MSMEs. MSME players realize the importance of an online-based supply chain supported by an adequate logistics service platform (LSP). Online platforms such as marketplaces play an important role in fulfilling orders in every transaction [2]. Current e-commerce trends require a good supply chain to support it. Therefore, e-commerce security becomes a valuable scheme for online-based supply chain systems. One source of funding for MSMEs currently comes from the supply chain financing (SCF) unit which acts as a credit guarantor [3]. However, these logistics services have inherent characteristics that can

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

hinder the development of secure supply chain financing systems.

There are several challenges faced by MSMEs on e-commerce platforms:

- Difficulty accessing capital: MSMEs need help to obtain funding from other parties with a safe transaction process.
- Potential for double spending: Transaction processes with external parties run the risk of causing double spending.
- High risk: MSMEs on e-commerce platforms face high risks in terms of product distribution and operations.
- Data manipulation: There is a possibility that certain parties manipulate data and disrupt MSME funding

One of the important breakthroughs of e-commerce platforms for digitalizing MSMEs is the integration of blockchain technology which uses a distributed data storage network.

Although interesting, Blockchain technology may not be the best for MSMEs on e-commerce platforms. The reason is, blockchain technology has weaknesses, including:

- High waiting time: The transaction verification process on the Public Blockchain takes a long time.
- Limited throughput: The number of transactions that can be processed per second on a Public Blockchain is limited.
- High energy consumption: Running a Public Blockchain requires large energy resources

Based on the background of the problem, this research aims to design a blockchain technology-based MSME transaction model using the Federated Byzantine Agreements (FBA) consensus algorithm to overcome blockchain problems such as validation waiting time, energy consumption and scalability.

This research was conducted on a laboratory scale and provides theoretical contributions. These results are useful for further development and application in the field of MSMEs and e-commerce.

II. BLOCKCHAIN SOLUTIONS

Digital platforms play an important role in collecting and analyzing information exchange in processes and supply chain management. In contrast to traditional supply chains that are geographically dispersed and require close supervision between sellers and distributors, today's business models demand better integration. Blockchain technology, which is essentially a secure and distributed digital record, offers a viable solution to the challenges faced by MSMEs.

Blockchain offers several advantages for MSMEs [4]:

- Save on Staff Costs: With a blockchain-secured platform, transaction assurance service providers for SMEs can save on staff costs.
- Efficient Authorization and Validation: Blockchain uses multiple blocks to store data, making the process of authorizing and validating transactions more efficient.
- Decentralization of Processes and System Integration: Blockchain enables decentralization of authorization processes, as well as better integration of e-commerce systems for MSMEs.

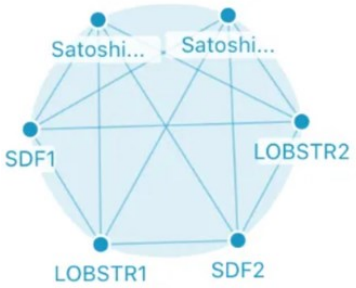
Blockchain uses encryption methods, key agreements, and smart contracts to guarantee data accuracy, security, and transparency [5]. Through the blockchain consensus mechanism, the security and transparency of user information is maintained. Therefore, financial institutions can utilize this data to assess the creditworthiness of MSMEs more easily and quickly, so that financing costs can be reduced [6].

Blockchain technology has great potential to increase user security by using a consensus mechanism. The financial sector has improved customer relationships in three ways: peer-to-peer transactions, integration of user records, and maintenance of distributed ledgers [7,8]. It combines user data, computing devices, and fund management, leveraging smart contracts that are more approachable and agile. An example of blockchain application in the financial sector is the Ethereum blockchain which provides a highly secure business network and enables digital securities.

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

Federated Byzantine Agreement (FBA

Mazieres introduced terminology of the FBA concept [9,10,11]. Mazieres stated that FBA is a group of nodes connected to each other to obtain agreement in validating every incoming transaction. Figure 1 shows a set of nodes that are members of the FBA network.



Gambar 1 contoh jaringan stellar (diambil dari stelarrbeat.io/blog

The concept of nodes is closed with FBAS model. Nodes on the FBAS model represents individuals. Each node represents a different entity or organization. For instance, {0, 1, 2} represents a set of three different nodes.

FBAS as proposed by Mazières, is a pair (V, Q) consisting of a set of nodes V and a quorum function Q: V → 2^{2^V} that determines the quorum intersection for each node, where a node is located all its quorum intersections itself - that is, ∀v ∈ V, ∀q ∈ Q(v), v ∈ q.

Every transaction that enters one of the nodes will have its validity verified. When a transaction has been verified, nodes will bring it to the slice quorum for approval. If a quorum has agreed to validate, the transaction is entered into the ledger and distributed to each validator node.

The FBA network model remains secure and sustainable. The network model determines the viability and security of FBAS. Security relates to the ability of outside parties to hack one or more nodes so they can validate illegal transactions. Meanwhile, continuity can cause nodes to become inactive, thereby making the network separate from the existing system, so that there is no agreement in the network as a whole.

Informally, each quorum slice of a node v represents a set of nodes that if all agree to externalize a value in a particular slot, then it is sufficient for node v to also externalize that value.

Quorum Slice in FBAS is a set of nodes selected by a particular node which is used as a reference in joint decision making with other nodes in the system. Informally, if all nodes in a slice quorum agree to decide on a value in a particular slot, then the nodes that have a slice quorum will also decide on the same value in that slot. In the formal definition of FBAS, the configuration of each node consists of the definition of its quorum slices. Meanwhile, quorum set is a function that determines the quorum set for each node in the network.

Quorum sets are more general and more related to the formal definition of FBAS, while quorum slices are more related to the configuration of each node in the network. Quorum chunks give each node the freedom to determine their preferences in choosing a quorum, while quorum pools provide a formal structure for consensus on an FBAS network.

III. METHOD

This research began by designing an MSME transaction model using an FBA-based blockchain system. Followed by creating, testing, and comparing the delay time of this model with other consensus models such as Proof of Work (POW), Proof of State (POS), and Proof of Authority (POA). Figure 2 shows the method in this research.

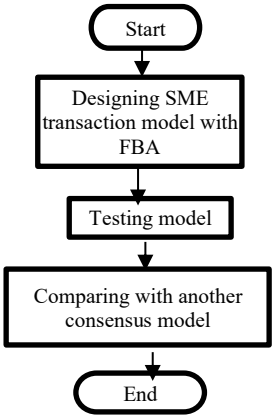


Fig 2. Method of research

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

IV. RESULTS AND DISCUSSION

Designing a blockchain-based MSME transaction model begins with transactions being accommodated in blocks. At the specified time, the block validates the FBA validator node network. When all transactions are validated, a new block will be formed which will be added to the blockchain network. The design of the blockchain-based transaction model can be seen in Figure 3.

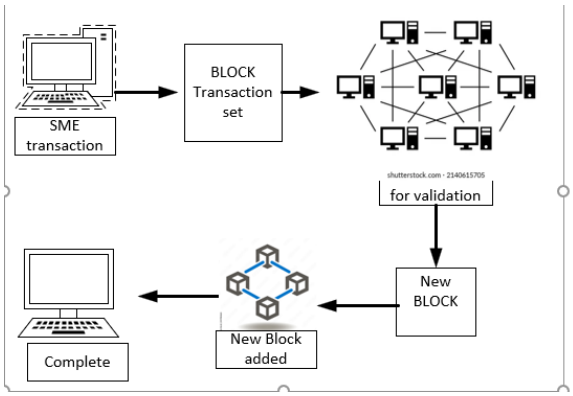


Fig 3. SME Transaction model base on blockchain

The model in Figure 3 can be applied to the supply chain model by changing transactions into goods movement transactions. However, the validator can be reduced to only certain parties validating the movement of goods. This is different from the transaction model which requires many parties to become validators in order to achieve transparency and a high level of trust.

At the FBA validator level, the validator process uses the Stellar Consensus Protocol (SCP). In this protocol, when a set of transaction blocks enters one validator, that validator will request approval from other validators. Before being handed over to a small group of validators. The block sending node has performed initial validation.

The slice quorum validation process uses the voting, accept, confirm method. This method is similar to the Byzantine Fault Tolerance consensus. Each validator node in the quorum slice votes, then collects whether the votes sent and received exceed the predetermined quorum. If the transaction block exceeds the quorum, then the transaction block will send a confirmation signal.

Block sets that have received confirmation will be sent to another quorum for approval. If all the quorum has reached agreement, a series of blocks will be added to the blockchain chain.

The process of approving a set of blocks into the FBA network is shown in Figure 4. Figure 4 shows the star consensus protocol designed by Junghun Yoo [12].

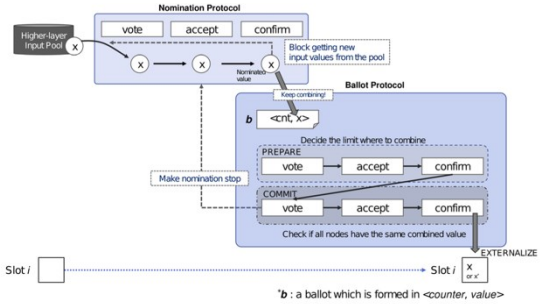


Fig 4. Stellar consensus protocol (SCP)

This blockchain-based SME transaction model was tested on a laboratory scale to record the time required for validation to occur or a new block to be formed. Testing is carried out in terms of validation time because one of the weaknesses of blockchain when applied to SMEs is the long validation time.

From this test we will find out the comparison of validation times between several currently popular consensuses such as POW, POS, and POA. The comparison is based on the number of nodes selected and the validation time achieved in ms (milliseconds).

The results of this test can be seen in Figure 5. FBA has a very short validation time compared to other consensus algorithms. For 10 to 100 validator nodes, the time required is still very short. Because, agreements in FBA start from the quorum portion and then increase to other quorum portion agreements. The protocol used only has 3 conditions, namely vote, accept and confirmation.

ISSN 2442-7888 (online) DOI 10.24167/Sisforma

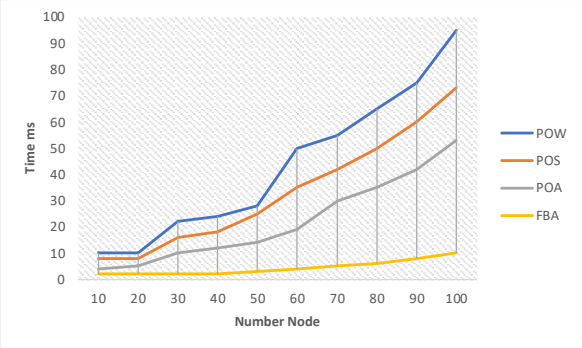


Fig 5 Result for time validation test

The results of this study also confirm the research from Tomic shown in Table 1. Table 1 shows a comparison of the FBA algorithm with other consensus algorithms with the result that FBA consensus is better than other consensus models such as PBFT, POA and Rakit [13].

Table 1. Comparison of consensus algorithms according to Tomic

Protocols Characteristics	dBFT	pBFT	FBA	PoA	Paxos	Raft
Security	Byzantine if f < 33.3%	Byzantine if f < 33.3%	Byzantine if f < 20%	Byzantine if f < 49%	Only from crash fault	Only from crash fault
Mutual trust	Nodes choose who to trust	Based on node selection	Flexible trust	Based on identity	Complete in terms of good intentions	Complete in terms of good intentions
Throughput	High	Moderate	High	Low	Moderate	Moderate
Scalability	High	Limited	High	Low	Limited	Limited

V. CONCLUSION

The blockchain-based MSME transaction model using the FBA consensus algorithm is able to reduce validation delay times significantly compared to POW and POS. FBA implementation also addresses scalability and energy consumption issues. However, validation using FBA is very dependent on the existence of a validator node. If a validator node goes down or is hit by a sybil attack, the FBA network will be paralyzed or insecure.

REFERENCES

[1] Fitriani Saragih, Rahmat Daim Harahap, Nurlaila; "View of Perkembangan UMKM Di Indonesia _ Peran Pemahaman Akuntansi, Teknologi Informasi dan Sistem Informasi Akuntansi." Riset dan jurnal akutansi, vol 7 no 3,2023

[2] Yan L, Yin-He S, Qian Y, Zhi-Yu S, Chun-Zi W, Zi-Yun L. "Method of reaching consensus on probability of food safety based on the integration of finite credible data on blockchain", IEEE Access, 2021;9:123764–76.

[3] Lu Q, Liu B, Song H. "How can SMEs acquire supply chain financing: the capabilities and information perspective. Industrial Management & Data Systems"; Technology (ICSITech), pp. 79 – 84, 2020

[4] Asaithambi, S., Ravi, L., Devarajan, M., Almazyad, A. S., Xiong, G., & Mohamed, A. W. (2024). Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs. *Egyptian Informatics Journal*, *25*. https://doi.org/10.1016/j.eij.2024.100444

[5] Cocco L, Mannaro K, Tonelli R, Mariani L, Lodi MB, Melis A, et al. A blockchain-based traceability system in agri-food SME: case study of a traditional bakery. IEEE Access 2021

[6] Chen Z, Zhu W, Feng H, Luo H. "Changes in corporate social responsibility efficiency in chinese food industry brought by COVID-19 pandemic—a study with the super-efficiency DEA-Malmquist-Tobit model". Front Public Health 2022;10. https://doi.org/10.3389/fpubh.2022.875030.

[7] Sasikumar A, Vairavasundaram S, Kotecha K, Indragandhi V, Ravi L,Selvachandran G, et al. "Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things". Futur Gener Comput Syst 2023;141:16–27.

[8] Oyinloye DP, Teh JS, Jamil N, Alawida M. "Blockchain consensus: an overview of alternative protocols. Symmetry" 2021;13(8):1363.https://doi.org/10.3390/sym13081363.

[9] Lachowski, Ł.: Complexity of the quorum intersection prop- erty of the

federated Byzantine agreement system (2019)

[10] Lokhava,M.,Losa,G.,Mazières,D.,Hoare, G.,Barry,N.,Gafni, E., Jove, J., Malinowsky, R., McCaleb, J.: Fast and secure global payments with Stellar. In: Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP '19), pp. 80–96. ACM, New York, NY, USA (2019)

[11] García-Pérez, Á., Gotsman, A.: Federated Byzantine quorum systems. In: 22nd International Conference on Principles of Distributed Systems (OPODIS 2018), pp. 17:1–17:16. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany (2018)

[12] Tonelli, R., IEEE Computer Society, Institute of Electrical and Electronics Engineers, & IEEE International Conference on Software Analysis, E. (n.d.). IWBOSE '19 : 2019 IEEE 2nd International Workshop on Blockchain Oriented Software Engineering (IWBOSE '19) : February 24, 2019, Hangzhou, China.

[13] N. Z. Tomić,(2021) "A review of consensus protocols in permissioned blockchains," Journal of Computer Science Research, vol. 3, no. 2

ISSN 2442-7888 (online) DOI 10.24167/Sisforma