Hindawi
Scientific Programming
Volume 2021, Article ID 5343337, 9 pages
https://doi.org/10.1155/2021/5343337

Research Article

A Novel Trade Transaction Agreement Algorithm Using Blockchain Consensus Mechanism

Pan Yi

Department of Commercial, Chongqing City Vocational College, Yongchuan 402160, China

Correspondence should be addressed to Pan Yi; yipan1220@126.com

Received 9 September 2021; Revised 25 September 2021; Accepted 27 September 2021; Published 18 October 2021

Academic Editor: Tongguang Ni

Blockchain, the underlying technology of Bitcoin, has been deeply studied in various fields after its development in recent years. As a typical decentralized distributed data storage system, consensus reached among all participants in a blockchain system requires a consensus mechanism to be realized. In order to make blockchain applicable to different application scenarios, different consensus mechanisms have been proposed. With the further development of blockchain applications, more and more studies have been conducted on the consensus mechanism. However, some existing consensus mechanisms still have some problems in various aspects. Therefore, this paper proposes a trade deal algorithm based on the blockchain mechanism of consensus. First of all, according to PBFT, the lack of a dynamic problem in the VPBFT voting mechanism was introduced. The node system is divided into four types with different responsibilities and gives the number of relations between nodes. When the number of nodes is changed, it can be calculated according to the quantity relation, ensuring dynamic. Second, a data anonymous transaction and authentication protocol is designed. In the protocol, when the seller sells data, the mapping relationship between the real identity and the false identity of the data owner is blinded and sent to the buyer. When the buyer wants to verify their identity, the seller's identity can only be verified with the authentication of the blockchain. The proposed algorithm is superior to the current consensus in terms of time and energy consumption, throughput, and fault tolerance methods, which is proven through experimental tests and simulation analysis.

1. Introduction

Blockchain [1] is a decentralized distributed database characterized by decentralization [2], immutability [3], anonymity [4], autonomy [5], consensus, and other characteristics. It is a new technology that has the potential to change social interaction and trading methods. This technology's main benefit is its ability to exchange transactions without relying on trusted third-party entities in any way. Data integrity, built-in authenticity, and user transparency are all features it can provide. Blockchain is a decentralized distributed computing paradigm, not a technological innovation. The data structure it adopts is a series of data blocks formed in a chain in time sequence. It involves various technologies of cryptography and integrates technologies such as smart contracts [6], P2P networks [7], and consensus mechanisms. Cryptography is used to ensure that data blocks in the chain of ownership and right of privacy, due to the data block in the chain is electronic data. It is not easy to prove to belong to source and transparent data. As a result, we will need to include some information in the data signature to indicate the data and sources as well as some cryptography technology to ensure privacy and prevent data leaking. Smart contracts, which are programs or scripts that can be automatically triggered and executed, ensure that bookkeeping participants conduct transactions and bookkeeping in accordance with certain rules [8]. They use algorithmic scripts to implement some commercial logic rules and regulations, ensuring that blockchain can be used in more systems. To ensure the consistency of the generated data across the entire distributed system, a consensus mechanism is used. Because blockchain is a distributed and open network, there is no or little trust between the transaction's two parties. In order to reach a consensus on a specific topic, the consensus mechanism is critical.

Consensus [9] has always been a hot topic in the field of distributed systems research. As people's cognition has deepened and blockchain research has advanced, relevant research on the consensus mechanism to solve the consensus problem has become a hot research topic in recent years. In a distributed system, the so-called consensus problem occurs when all participants have the same status. The distributed system is maintained, checked, and maintained by each participant in the same way. As a result, a consensus mechanism ensures that all participants in a distributed system can trust one another and reach an accurate consensus on a proposal that needs to be confirmed. This paper further studies the PBFT consensus mechanism and its existing improved consensus mechanism and then proposes a new, improved PBFT mechanism: "Byzantine fault-tolerant consensus mechanism based on machine learning." A logical regression algorithm is used to predict whether the request is passed or not [10]. Data blocks are produced in advance and cached when the prediction is passed to wait for validation and reduce the delay. Then, the nodes in the system are dynamically classified by K-means clustering algorithm to ensure the regular operation of the anonymous trade transaction system.

The main contributions of this paper are as follows:

(1) In this paper, a data transaction and authentication protocol for anonymous data are being developed. The mapping relationship between the real identity and the false identity of the data owner is blinded and sent to the buyer when the seller sells the data. When a buyer wants to verify the seller's identity, the only way to do so is through blockchain authentication.

(2) In this paper, a machine learning-based Byzantine fault-tolerant consensus mechanism is proposed. All nodes in the system are initially classified into different types using K-means clustering and then reclassified as the number of nodes changes to ensure dynamic performance. A logistics regression algorithm is also used to predict validation results ahead of time, make full use of node idle waiting time, and reduce delay and resource waste.

The remainder of the paper is organized in the following manner. The background work is examined first in Section 2, followed by methodology in Section 3. The results and discussion are then presented in detail in Section 4. Finally, Section 5 concludes the paper.

2. Background

This section discusses the related work in the context of blockchain technology and anonymous storage transaction technology.

2.1. Blockchain Technology. Blockchain technology is proposed to solve the long-standing Byzantine general problem and the problem of double cost. In recent years, it has developed rapidly, and various kinds of digital currencies have emerged in an endless stream. For example, inspired by Bitcoin, a programmer at Google launched an improved version of the digital currency, Litecoin. The technical principle is the same as Bitcoin, but Litecoin is produced and traded on a different principle. In addition, Miers et al. [11] proposed the concept of Zerocoin based on the zero-knowledge proof cryptography principle. So far, there have been dozens of digital cryptocurrencies. In the future, not only in the field of digital cryptography but also in other fields blockchain will be fully developed.

So far, blockchain has proven to be successful not only in theory but also in practice. Vitalik proposed Ethereum, a single blockchain that allows for reprogramming to achieve arbitrarily complex computing functions, in 2013. Simply put, Ethereum is a smart contract-enabled public blockchain platform. More than 30 companies announced the Hyperledger Consortium Project in 2015, led by the world's largest open-source organization, the Linux Foundation. The goal of the project is to advance the development of blockchain and distributed ledger protocols. SuperLedger is a collaborative project that consists of subprojects for various purposes and scenarios, with a modular design, code readability, and long-term evolution path in mind. The SuperLedger community now includes over 140 businesses and organizations.

2.2. Anonymous Storage Transaction Technology. With the continued growth of the Internet, the number of terminal devices, servers, and users on the network is increasing. The amount of data produced is also on the rise. The question of how to protect these data and the data owner has become a focus of data security research. Furthermore, blockchain technology has cryptographic properties that allow one's identity to be protected without being revealed. As a result, current research is focusing on the combination of blockchain with anonymous storage and anonymous transactions. In terms of anonymous storage, Do and Ng [12] proposed a secure distributed data storage system with a keyword search service based on blockchain technology [13–15]. RSA [16] and the discrete logarithm hypothesis allow clients to upload data to cloud nodes in ciphertext form [17, 18]. While ensuring the availability of data, it also provides the data owner with the ability to grant others the right to search their data. Lu et al. [19] proposed a blockchain-based anonymous reputation system (BARS) to break the linkability between real identity and public key to protect privacy. Finally, Shafagh et al. [20] proposed a blockchain-based distributed access control and data management system for the Internet of Things, customized for IoT data traffic, and can achieve secure data sharing. Using blockchain as the storage layer, secure and flexible access control management is realized.

In terms of anonymous transactions, Heilman et al. proposed a solution to anonymity for transactions on and off the blockchain of Bitcoin. They have used an untrusted third party to issue anonymous credentials, which users can exchange into Bitcoin. The simultaneous use of blind signatures [21] and smart contracts ensures anonymity and

fairness during the exchange of Bitcoin certificates [22]. Aitzhan and Svetinovic [23] do not rely on certificates but trusted third parties in distributed smart grid energy trading transaction security problems. They use blockchain technology, multiple signatures, and anonymous to encrypt the message flow to realize the concept of decentralized energy trading system validation. It allows peers to negotiate anonymous energy prices and trade safely. Wang et al. [24] introduced a blockchain-based mutual authentication and key agreement protocol for edge computing-based smart grid systems. Using blockchain, the protocol can support effective conditional anonymity and key management without the need for other complex cryptographic primitives.

3. Methodology

In this section, the following subsections attention-based graph convolution, third-order hourglass networks, and residual dense module are discussed in detail.

3.1. Data Anonymous Transaction and Authentication Protocol. After the edge device encrypts the data and stores the address on the blockchain, it makes a transaction request when a user demands the stored data. At this time, the edge device serves as the seller, and the user serves as the buyer. The protocol uses the elliptic curve public-key encryption system to ensure the anonymity of the transaction. The corresponding relationship between the real identity and the false identity mapping is blinded by the improved blind signature and sent to the buyer. Under normal circumstances, the buyer cannot know the corresponding real identity and can only obtain its real identity by blind-decoding it during arbitration, as shown in Figure 1.

There are four actors in this agreement: buyer, seller, blockchain, and bank. Each has different responsibilities and functions.

(1) Buyer: a buyer is a user who is interested in specific data and has the need to purchase data. When the buyer wants to purchase a certain type of data, the buyer will issue a transaction on the blockchain network. The labeled type of data that the buyer wants to purchase is declared. The amount used to purchase data is valid. In addition, the buyer's public key, PK_Buyer, and the parameter, eq_b, are used to prove his identity.

(2) Seller: in this agreement, the edge device as the seller transacts data with the buyer. Before the transaction, the seller will check the transaction request issued by the buyer in the blockchain network. Suppose the seller is willing to transact with one of the buyers. In that case, it will publish a transaction in the blockchain, claiming that it is willing to transact with the buyer. The seller can show the data type LABEL of the data he owns.

(3) Blockchain: as a trading platform for buyers and sellers, blockchain releases transactions on the blockchain to realize direct transactions between the two parties without the intervention of a third party. Meanwhile, all transaction records are searchable on the blockchain and cannot be tampered.

(4) Bank: when the seller and the buyer make a formal transaction, the buyer will issue a cheque. After receiving the cheque, the seller will send it to the bank. The bank will complete the transfer through the corresponding accounts of the seller and the buyer on the cheque.

The agreement is divided into the following stages:

(1) Peripheral device registration stage: peripheral device, as the seller, needs to register with the blockchain before selling data to obtain the right to trade with the buyer.

(2) Check generation stage: this stage mainly includes the buyer sending a transaction request to the blockchain. The seller agrees to trade with the buyer and obtains the check.

(3) Data transaction stage: after the seller gets the cheque signed by the buyer, he/she initiates a transfer request to the bank. The bank verifies his/her identity and transfers the corresponding amount of the buyer's account to the seller's account. After successful transfer, the bank informs the seller, and the seller sends the corresponding data to the buyer.

(4) Certification stage: the buyer thinks that the seller's selling data is wrong and requests the arbitrator for arbitration. Under the supervision of the arbitrator, authentication is carried out.

3.2. Consensus Mechanism Based on Machine Learning. This paper proposes a practical Byzantine fault tolerance based on machine learning [25–29] (MLPBFT). To begin, the mechanism divides the nodes in the system into three nodes with different responsibilities: customer node, master node, and supervision node, using the K-means clustering algorithm [30]. The client node is also the data block producer and request initiator in MLPBFT. The transit node, or master node, preprocesses and forwards the request initiated by the client node to the supervising node. The monitor node primarily verifies and confirms the messages it receives and then replies to confirm the message once the verification is complete. Finally, after the client node sends the request, the waiting time will be used to predict the probability of the request passing through the logistic regression algorithm [31]. Then, based on the prediction result, decide whether to produce the block ahead of time. In addition, the consensus process will be suspended when the number of nodes in the system changes, to ensure the system's dynamism. The data pairs of multiple groups of different classification types caused by a change in the total number of nodes will be calculated using the K-means clustering algorithm, and the appropriate classification will be chosen.

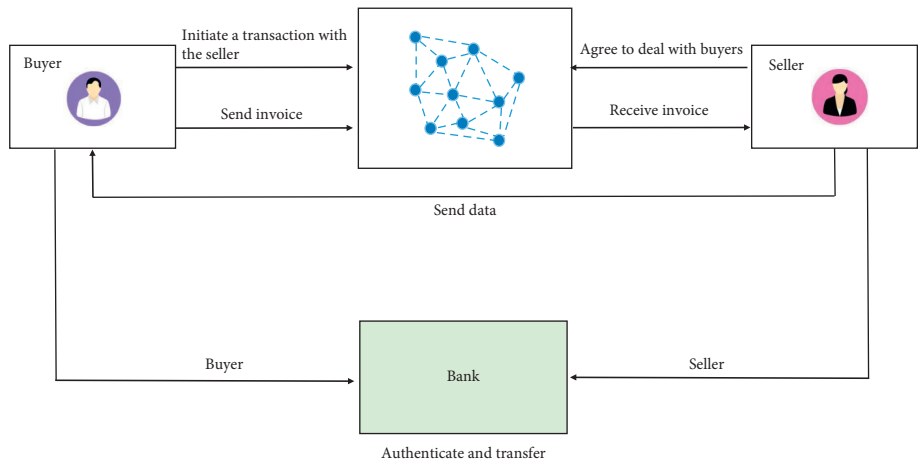

Figure 1: Model of the proposed protocol.

3.2.1. K-Means Algorithm. K-means is usually used to solve clustering problems and is a form of unsupervised learning [32, 33]. It is a clustering algorithm based on the distance between data. The distance between two data points is used as a criterion to judge whether the data is similar. The closer the distance is, the more similar the two data points are. The implementation steps are as follows:

(1) Suppose $D = \{d_1, d_2, ..., d_n\}$ is the training sample data, where $d_i = \{X_i, Y_i\}$, $1 \le i \le n$. Select K data from D as the initial K cluster centers, $K < n$. Set the selected K initial cluster centers as $\{(X_1, Y_1), (X_2, Y_2), ..., (X_K, Y_K)\}$. Then, the remaining data is recorded as $\{(X_{K+1}, Y_{K+1}), (X_{K+2}, Y_{K+2}), ..., (X_n, Y_n)\}$.

(2) Use the Euclidean distance method to calculate the distance $\{r_1, r_2, \cdots, r_K\}$ from each data in the dataset to each cluster center and record it. The calculation equation is as follows:

$$r_i = \sqrt{(X - X_i)^2 + (Y - Y_i)^2}, \quad 1 \le i \le K. \tag{1}$$

(3) According to the recorded and calculated distance, select the smallest distance, namely, $\min\{r_1, r_2, \cdots, r_K\}$, and classify the data and the corresponding initial cluster center into the same category.

(4) When all the data are divided, there are K clusters of the data set. All the data in each category are recalculated to calculate the new clustering center. The calculation method is generally to select the arithmetic mean of each dimension of all the data in this cluster.

(5) Go to step 2 and continue to calculate and iterate until the iteration ends when the relationship between the initial cluster center and the new cluster center meets the preset threshold.

3.2.2. Consensus Mechanism. A PBFT improvement scheme using a logistic regression algorithm is proposed in this paper. The K-means clustering algorithm can easily manage with a faster convergence speed before the data changes are easier to update the model characteristics. The differences between clusters produce a better result, and all that is required is to adjust the number of clusters in the K MLPBFT scheme. The MLPBFT consensus mechanism divides the network's nodes into three categories: client node, master node, and supervision node, using a K-means clustering algorithm. Nodes fall into various categories, each with its own set of responsibilities. The consensus process is completed through two stages: the preparation stage and the verification stage. On this basis, MLPBFT will use the logistic regression algorithm to predict the verification result of the request made by the customer node, while the customer node is waiting for the reply message, and complete the production of the data block in advance, when the predicted result is passed. Moreover, the K-means clustering algorithm will be started again when the nodes change. The nodes in the system will be reclassified to ensure the system's dynamic. In addition to the characteristics of dynamic and security, MLPBFT also has certain advantages compared with the consensus in terms of time and energy consumption, throughput, fault tolerance, and communication times.

3.2.3. Consensus Process. The MLPBFT is similar to the VPBFT consensus process. Instead of the PBFT's "three-phase" model, the MLPBFT adopts a "two-phase" model, consisting of a preparation phase and a validation phase, as shown in Figure 2.

The customer node initiates the request for the production data block. The *request* message is Request: <Bcontent, Tc, Sc>, where Bcontent is the data block to be produced, Tc is the timestamp of the *request* message sent by the customer node, and Sc is the signature of the customer node. The data block is divided into two parts, the block and the data. The block contains the relevant information of the previous data block. If the block is a creative block, the information of the block only identifies the block as a creative block.

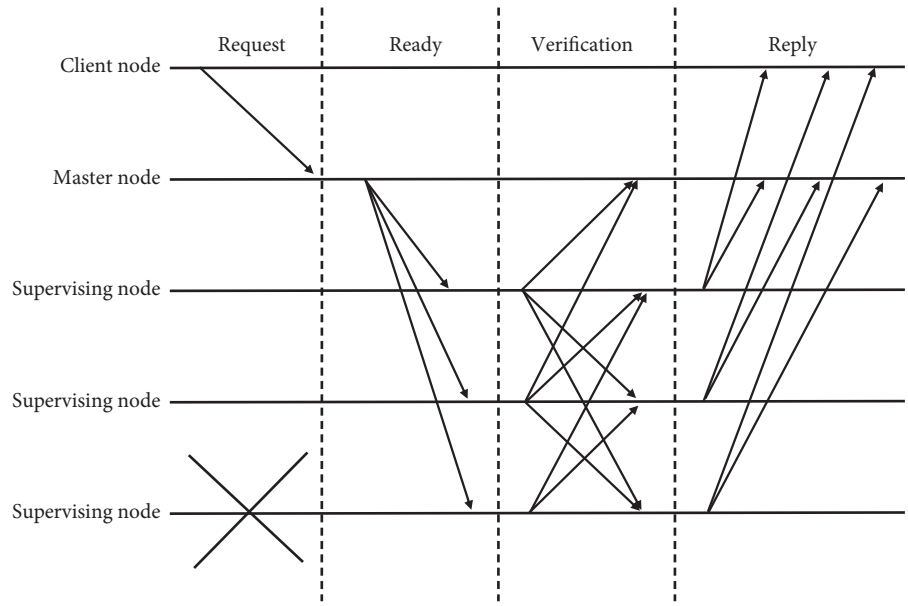

Figure 2: The consensus process of MLPBFT.

After the master node receives the *request* message, it first numbers the message and then extracts the message's important information. A summarized message is appended to the *request* message, then adds the timestamp and signature to form a *query* message, and then broadcasts the *query* message to all the supervising nodes. The *query* message is Query: <D, Tm, Sm>, where Num is the number, D is the abstract, Tm is the primary node's timestamp, and Sm is the primary node's signature. This stage is the preparation stage.

Monitoring nodes after receiving the master node to send over the query message, first verification, validation message contained within the request's specific content, and information are consistent. The master node is correct. Add validation results to Y; otherwise, add validation results to N. The valid form contains information of verification results. Supervisor nodes will broadcast *valid* messages to other monitoring nodes for mutual confirmation and verification. Valid:< ID, Num, Bcontent, Tc, Sc, D, Tm, Sm, Y/N>, where ID is the number of the monitor node itself. This phase is the validation phase.

When the supervisory node receives at least $1 + Ns/2$ (Ns is the number of supervisory nodes). A valid message with Y will reply to a confirmation message to the client node. The confirmation message is Commit: <ID, Num, Bcontent, Tc, Sc, D, Tm, Sm, Y/N, Ts, Ss>, where Ts is the timestamp added by the supervisory node and Ss is the signature of the supervisory node.

If the client node receives at least $1 + Ns/2$ Commit messages containing Y, it will be considered that the request was passed. The client node will directly chain the data block produced in advance according to the predicted result or produce the corresponding data block and chain it. Otherwise, the request was not approved. Discard the request and restart the request.

3.2.4. Dynamic Classification Based on K-Means. To conduct the initial type division of nodes in the system, the K-means clustering algorithm was started before the consensus process. The K-means clustering algorithm is triggered again when the total number of nodes in the system changes, automatically classifying all nodes in the system. They ensure that the system can continue to function without restarting after the number of nodes changes. The K-means clustering algorithm was chosen for two reasons. To begin, nodes in the MLPBFT consensus mechanism must be divided into three types, each with different responsibilities. The number of nodes of different types must be redivided when nodes join or leave. Second, the K-means clustering method is a more widely used clustering method, mainly used to complete data aggregation and classification. The algorithm is easy to understand and implement.

4. Experiments and Results

This section discusses experimental setup, data sets, evaluation methods, and experimental results discussed in detail.

4.1. Consensus Time-Consuming Analysis. Among the consensus mechanisms such as PBFT, VPBFT, K-PBFT, and MLPBFT, the consensus process is the most important. This experiment will simulate the consensus process of each consensus mechanism using a Python program in a network environment with fixed network bandwidth in order to compare the time consumed in the consensus process of these several consensus mechanisms. The consensus process, which is used in the experimentation process, starts with a consensus process and progresses over time. This time, all messages sent are serial transmissions, with the same data transmission resources and message size. At the same time, all consensus mechanisms are the same, with the same node number, data processing speed, and processing time. Figure 3 depicts the results of 10 experiments that were

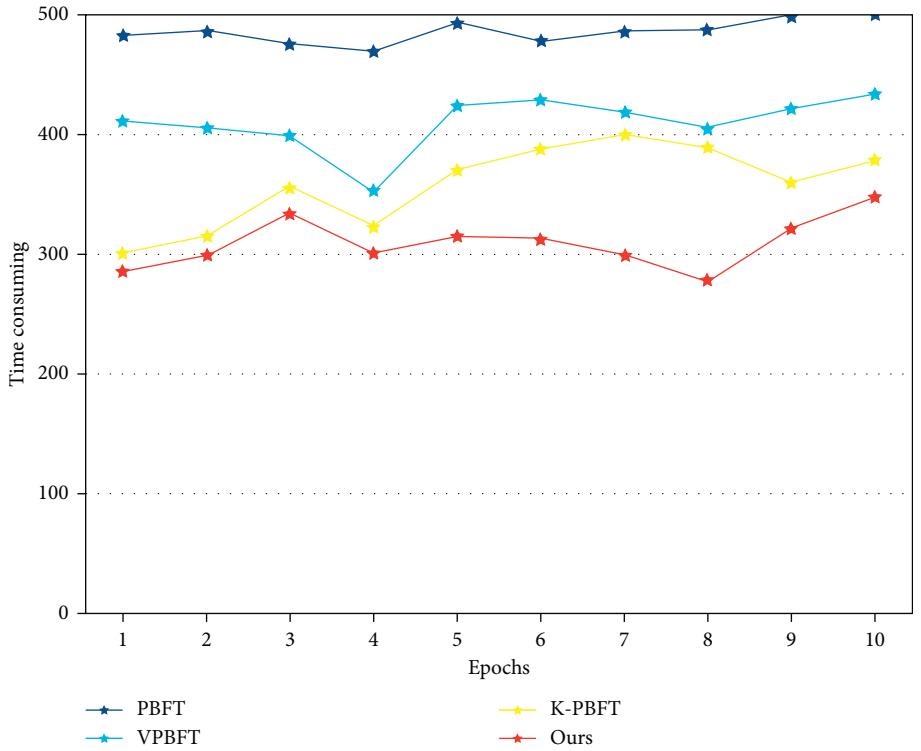

Figure 3: Time-consuming comparison results of the consensus process.

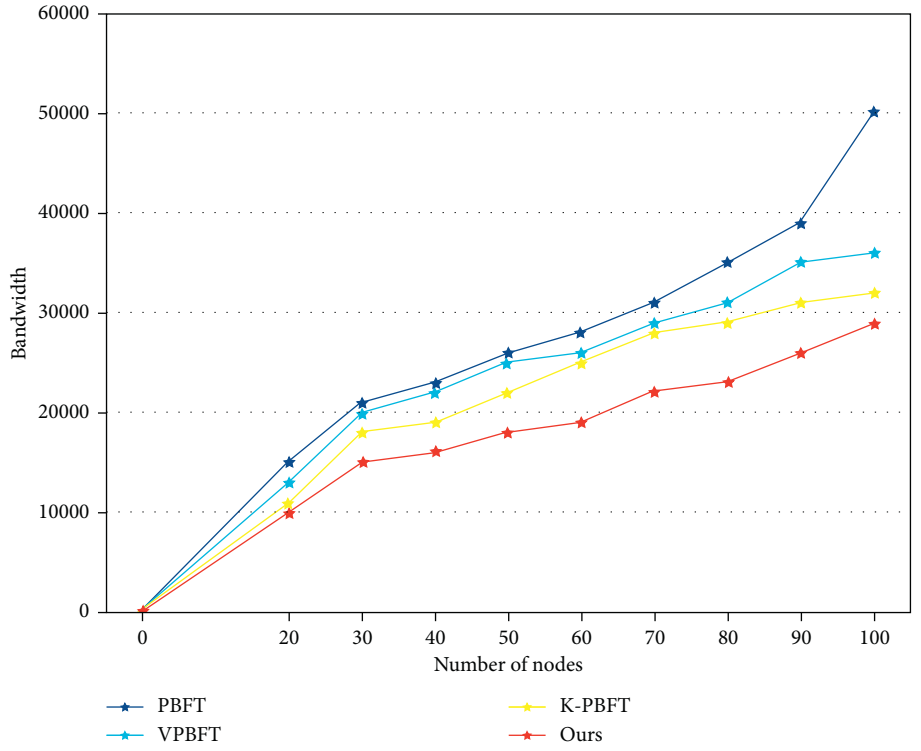

Figure 4: Comparison results of the bandwidth consumed by the consensus process.

conducted after simulating a consensus process of a consensus mechanism using Python and the program of the node itself.

As can be seen from Figure 3, under the same network environment and the same nodes, the time consumed by a consensus process of 1VB and PBFT is less than that of

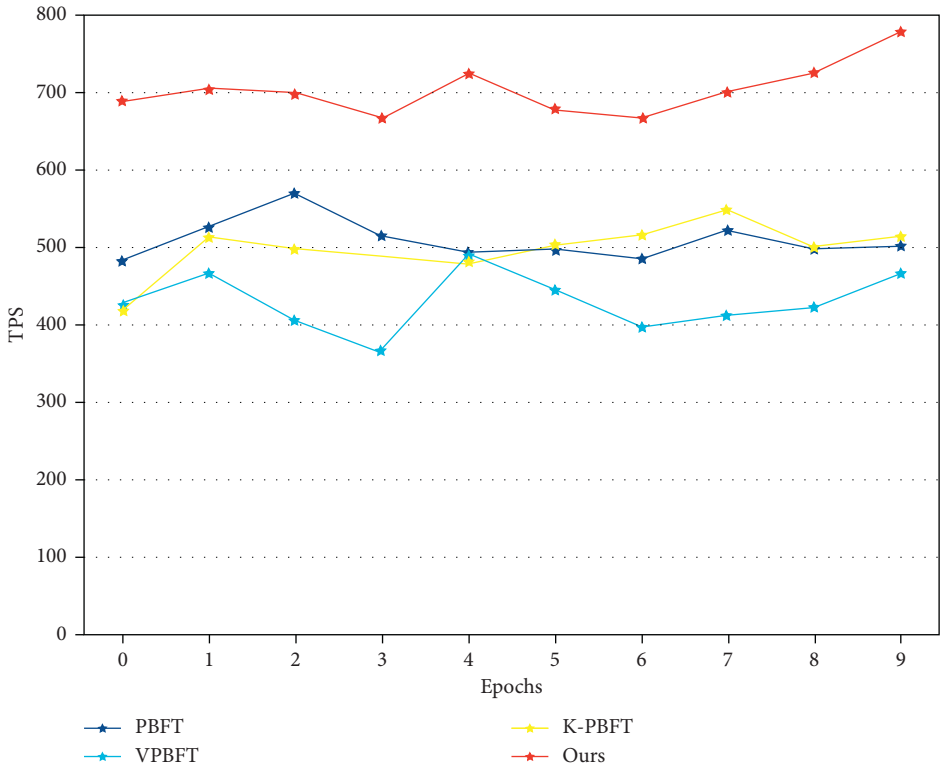

Figure 5: Comparative experiment results of throughput.

PBFT, VPBFT, and K-PBFT. For example, after calculating the average time of 10 experiments of each consensus mechanism, the average time of one consensus for MLPBFT was about 308.5 ms. In contrast, the average time of one consensus for PBFT, VPBFT, and K-PBFT was 484.8 ms, 409.4 ms, and 357.2 ms, respectively.

4.2. Bandwidth Usage Analysis. In the improvement scheme MLPBFT proposed in this paper, the consensus process is divided into a preparation phase and a verification phase. In the preparation phase, the master node needs to broadcast the entire network to send the query message to the supervisory node. The supervisory node needs to broadcast the valid message to other supervisory nodes for mutual confirmation and verification in the verification phase. Thus, it can be seen that the total network bandwidth required for the entire consensus process is twice the bandwidth.

It can be seen from Figure 4 that the network bandwidth consumed by the MLPBFT in the consensus process is lower than that of PBFT, K-PBFT, and VPBFT, which proves the superiority of this algorithm.

4.3. Throughput Analysis. One of the most important indicators for evaluating the benefits and drawbacks of the consensus mechanism is throughput. It is measured in transactions per second (TPS) and has the following calculation equation:

$$\text{TPS} = \frac{\text{SUM}(\text{transactions})}{T}, \tag{2}$$

where T is the time interval from when a transaction is issued to when a consensus is reached to generate a block, and SUM (transactions) is the total number of transactions included in the block generated in this time interval.

Figure 5 shows that the average throughput of MLPBFT is around 702.1 per second for the same number of nodes. It has a throughput of 194.12 per second, 175.64 per second, and 253.11 per second, respectively, which is higher than PBFT, VPBFT, and K-PBFT.

5. Conclusion

For some existing consensus mechanisms, there are still some problems in various aspects. This paper proposes a trade transaction protocol algorithm based on the blockchain consensus mechanism. First, in response to the lack of dynamics of PBFT, we proposed to introduce a voting mechanism in VPBFT. This mechanism divides the nodes into four types with different responsibilities and gives the number relationship between the nodes. When the number of nodes changes, it can be calculated according to the number relationship to ensure dynamicity. Second, a data anonymous transaction and authentication protocol is designed. In the agreement, when the seller sells the data, the mapping relationship between the real identity and the pseudoidentity of the data owner is blinded and sent to the buyer. When the buyer wants to verify the identity, the seller's identity can only be verified under the authentication of the blockchain. After experimental testing and simulation analysis, the algorithm in this paper is superior to existing

methods in terms of consensus time-consuming, energy consumption, throughput, and fault tolerance.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, Article ID 102397, 2021.

[2] A. E. Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. G. Sirer, "Decentralization in bitcoin and Ethereum networks," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 439–457, Springer, Berlin, Heidelberg, January 2018.

[3] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, pp. 1–8, IEEE, Nanjing, China, November. 2017.

[4] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.

[5] J. P. Queralta, L. Qingqing, Z. Zou, and T. Westerlund, "Enhancing autonomy with blockchain and multi-access edge computing in distributed robotic systems," in *Proceedings of the 5th International Conference on Fog and Mobile Edge Computing*, pp. 180–187, IEEE, Paris, France, April 2020.

[6] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: a systematic mapping study," *Telematics and Informatics*, vol. 35, no. 8, pp. 2337–2354, 2018.

[7] G. Fanti and P. Viswanath, "Deanonymization in the bitcoin P2P network," in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 1364–1373, Long Beach California USA, December 2017.

[8] M. A. Jan, J. Cai, X. C. Gao et al., "Security and blockchain convergence with Internet of Multimedia Things: current trends, research challenges and future directions," *Elsevier Journal of Network and Computer Applications*, vol. 175, Article ID 102918, 2021.

[9] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Generation Computer Systems*, vol. 107, pp. 760–769, 2020.

[10] N. Usman, S. Usman, F. Khan et al., "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics," *Future Generation Computer Systems*, vol. 118, pp. 124–141, 2021.

[11] E. B. Sasson, A. Chiesa, C. Garman et al., "Zerocash: decentralized anonymous payments from bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 459–474, IEEE, Berkeley, CA, USA, May 2014.

[12] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *Proceedings of the 2017 IEEE World Congress on Services (SERVICES)*, pp. 90–93, IEEE, Honolulu, HI, USA, June 2017.

[13] H. Juma, K. Shaalan, and I. Kamel, "A survey on using blockchain in trade supply chain solutions," *IEEE Access*, vol. 7, Article ID 184115, 2019.

[14] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: an analysis through the review of academic and trade literature," *Telematics and Informatics*, vol. 58, Article ID 101532, 2020.

[15] A. Batta, M. Gandhi, A. K. Kar, N. Loganayagam, and V. Ilavarasan, "Diffusion of blockchain in logistics and transportation industry: an analysis through the synthesis of academic and trade literature," *Journal of Science and Technology Policy Management*, vol. 12, pp. 378–398, 2020.

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[17] M. S. Hasan, F. Alvares, T. Ledoux, and J.-L. Pazat, "Investigating energy consumption and performance trade-off for interactive cloud application," *IEEE Transactions on Sustainable computing*, vol. 2, no. 2, pp. 113–126, 2017.

[18] M. Ashouri, F. Lorig, P. Davidsson, R. Spalazzese, and S. Svorobej, "Analyzing distributed deep neural network deployment on edge and cloud nodes in IoT systems," in *Proceedings of the 2020 IEEE International Conference on Edge Computing (EDGE)*, pp. 59–66, IEEE, Beijing, China, October 2020.

[19] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Bars: a blockchain-based anonymous reputation system for trust management in VANETs," in *Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 98–103, IEEE, New York, NY, USA, August 2018.

[20] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, pp. 45–50, Dallas Texas USA, November 2017.

[21] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[22] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions," in *Proceedings of the International conference on financial cryptography and data security*, pp. 43–60, Springer, Berlin, Heidelberg, February 2016.

[23] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.

[24] J. Wang, L. Wu, K. K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984–1992, 2019.

[25] M. Zhao, Q. Liu, A. Jha et al., "VoxelEmbed: 3D instance segmentation and tracking with voxel embedding based deep learning," 2021, https://arxiv.org/abs/2106.11480.

[26] H. You, L. Yu, S. Tian et al., "MC-Net: multiple max-pooling integration module and cross multi-scale deconvolution network," *Knowledge-Based Systems*, vol. 231, Article ID 107456, 2021.

[27] M. Zhao, A. Jha, Q. Liu et al., "Faster Mean-shift: GPU-accelerated clustering for cosine embedding-based cell segmentation and tracking," *Medical Image Analysis*, vol. 71, Article ID 102048, 2021.

[28] J. Zhang, X. Jin, J. Sun, J. Wang, and A. Kumar Sangaiah, "Spatial and semantic convolutional features for robust visual object tracking," *Multimedia Tools and Applications*, vol. 79, no. 21-22, pp. 15095–15115, 2020.

[29] W. Chu, P. S. Ho, and W. Li, "An adaptive machine learning method based on finite element analysis for ultra low-k chip package design," *IEEE Transactions on Components, Packaging, and Manufacturing Technology*, vol. 11, pp. 1435–1441, 2021.

[30] J. Chen, C. Du, Y. Zhang, P. Han, and W. Wei, "A clustering-based coverage path planning method for autonomous heterogeneous UAVs," in *Proceedings of the IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, Indianapolis, IN, US, September 2021.

[31] L. Huang, G. Xie, W. Zhao, Y. Gu, and Y. Huang, "Regional logistics demand forecasting: a BP neural network approach," *Complex & Intelligent Systems*, vol. 876, pp. 1–16, 2021.

[32] C. Wang, X. Bai, X. Wang et al., "Self-Supervised multiscale Adversarial regression network for stereo disparity estimation," *IEEE Transactions on Cybernetics*, 1–14, 2020, In press.

[33] C. Wang, X. Wang, X. Bai, Y. Liu, and J. Zhou, "Self-supervised deep homography estimation with invertibility constraints," *Pattern Recognition Letters*, vol. 128, pp. 355–360, 2019.