electronics

MDPI

Article

Medical Data Storage Model Based on an Alliance Chain

Kejia Chang [1], Wenlong Feng [1,*], Yu Zhang [2], Wang Zhong [1] and Xiandong Zheng [1]

[1] School of Information and Communication Engineering, Hainan University, Haikou 570228, China
[2] School of Computer Science and Technology, Hainan University, Haikou 570228, China
* Correspondence: fwlfwl@163.com

Abstract: Aiming at the problems of centralized storage, low sharing efficiency, and the security and privacy of traditional medical data, a medical data storage model based on a consortium chain is proposed. First, the Distance algorithm is designed based on the geographical relationship of nodes, which reduces the amount of communication between nodes, improves the communication efficiency between A nodes, and ensures the efficiency and reliability of grouping. Second, the dynamic election is combined with the Distance algorithm to design the election strategy of the primary node, which realizes the scientific and reasonable ranking of the medical nodes, improves the reliability of the selection of the primary node, and ensures the efficiency of the medical nodes in the alliance chain to quickly reach consensus when the medical data are uploaded to the chain. Finally, the model designs a method of information separation, which combines the distributed database IPFS (InterPlanetary File System) with the blockchain, which greatly reduces the pressure of medical data storage in the blockchain and improves the operation efficiency. The experimental results show that the medical data storage model can effectively improve the problem of the sharp increase in the amount of communication between medical nodes in the network and reduce the impact of malicious consensus nodes.

Keywords: medical federated chain; storage model; PBFT algorithm; consensus algorithm

Citation: Chang, K.; Feng, W.; Zhang, Y.; Zhong, W.; Zheng, X. Medical Data Storage Model Based on an Alliance Chain. *Electronics* **2022**, *11*, 2495. https://doi.org/10.3390/electronics11162495

Academic Editor: Jun-Ho Huh

Received: 21 July 2022
Accepted: 9 August 2022
Published: 10 August 2022

1. Introduction

In recent years, with the development of technologies such as big data and cloud computing [1–3], more and more medical institutions choose to store patient medical data in the cloud, which improves the efficiency of storage and retrieval but also faces the problem of the centralized storage of data, which will not guarantee the integrity and security of medical data [4] once the third-party server is down or in the event of a malicious attack. As a distributed ledger, blockchain [5] provides a new decentralized model for solving the problem of data storage in medical institutions.

The literature [6] proposes a medical data blockchain system based on cloud storage to protect the privacy of data, but the use of the POW consensus algorithm needs to consume a lot of computing power. The literature [7] performs medical data storage using the original PBFT algorithm, which requires the participation of all medical nodes and greatly reduces the communication efficiency. The literature [8] classifies medical institutions into ranks based on medical resources and uses a hybrid consensus mechanism of DPOS and PBFT to improve consistency and efficiency, but there is a subjective concept of ranking. The literature [9] uses the POW consensus algorithm for identity management and authentication to ensure the confidentiality of shared medical data, but the algorithm wastes medical resources greatly. The literature [10,11] proposed the POV consensus algorithm and POB consensus algorithm to solve the POW energy consumption problem, but they are mainly used in public chains. Although these partially adopted methods improve the shortcomings of medical data storage to some extent, there are also problems. In essence, they do not use resources rationally, they do not take into account the actual situation where there are great differences between individual medical nodes, and the algorithms

used rarely address the efficiency of consensus, the network overhead, and the scalability of the blockchain, which affects the overall efficiency when the number of nodes increases.

Based on the existing research, this paper designs a medical data storage scheme using blockchain technology. The novelty is that this paper uses the geographic location resources of medical nodes to design the Distance algorithm before storing medical data on the chain, which makes full use of medical resources to enable the better allocation of medical nodes into groups. In this paper, multiple medical nodes are divided into several node groups. Each node group includes a primary node and multiple secondary nodes, they use a hierarchical strategy to reach consensus, and the primary node is dynamically selected within each group by the proposed distance ranking hybrid mechanism, which is difficult to solve in PBFT, which improves the reliability of primary node selection. By combining the first consensus layer and the second consensus layer sequentially according to the traditional PBFT model, the traffic in the consensus process can be greatly reduced, and the medical alliance chain system can reach consensus quickly, making the blockchain system data storage more efficient. In this paper, when acquiring medical data for chaining, compared with [12], which used IPFS for information separation technology, by uploading the PHR of patients to IPFS, its generated index is on the chain, which makes the medical alliance chain have a lower system overhead. This solves the problem of centralized medical data storage, which is difficult to share, and improves the efficiency of medical data storage.

The medical data storage model has many important components; the model mainly consists of six entities: the supervision center, hospital, patient, data user, IPFS, and medical alliance chain. Figure 1 shows the components of the system storage model.

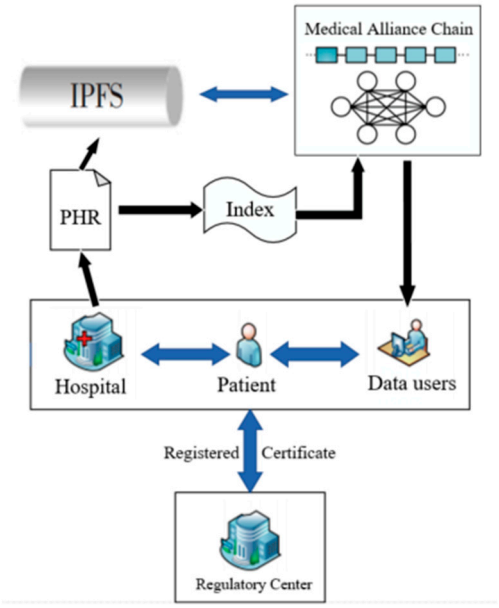

Figure 1. Medical data storage model components.

Among them, the supervision center issues registration certificates to users who enter the medical alliance chain for the first time and at the same time manages and supervises hospitals, patients, and data users. Hospitals, as medical nodes, encrypt medical data after being authorized by patients, store PHR (Personal Health Record) information on the medical institution's own distributed database IPFS, and generate an index link index of PHR. While the index is signed using the patient's private key, this index is hidden from unauthorized users, and this index is entered into the blockchain ledger after encryption. The patient, as the owner of the personal health record PHR, mainly sets the access policy for his medical data. If the data user wants to obtain the patient's medical data, he needs to obtain the authorization of the patient. IPFS is an interplanetary file system which is used to store patients' encrypted PHR and generate the index. The medical alliance chain

is composed of multiple medical institutions which jointly maintain the blockchain, store the index of medical data, and reach a consensus agreement.

The main contributions of this paper are as follows:

(1) The complete medical data of patients are encrypted and stored on IPFS [13], and the index generated by it is stored in the alliance chain, which can safely store the medical data of patients and improve the data sharing among medical institutions.

(2) A Distance algorithm is proposed to group medical institutions according to their geographic locations to maximize the communication efficiency between medical nodes.

In each group, the distance algorithm and the comprehensive rating of medical institutions are combined to generate a consensus node set ranking, and the primary node is dynamically selected from it, which reduces the possibility of the primary node doing evil and improves the stability of medical data on the chain.

(3) The improved consensus algorithm is adopted based on PBFT for consensus chaining, which effectively reduces the communication complexity of the system.

The rest of this paper is arranged as follows: in Section 2, the Distance algorithm and consensus mechanism of the medical data storage model are introduced in detail, along with the selection strategy of primary nodes in the medical alliance chain and the specific process of the improved consensus algorithm. Section 3 shows that the model in this paper can achieve secure storage and improve communication efficiency through security analysis and communication complexity analysis. Section 4 concludes the paper and provides an outlook for the next research work.

2. Medical Data Storage Model

When users enter the medical alliance chain for the first time, they need to submit relevant registration information to the supervision center, which verifies the user's qualification identity, generates a public-private key pair for the passed user using an asymmetric encryption algorithm [14], and uses the private key to sign the user's public key to generate a digital certificate.

When the patient visits the hospital, the doctor will provide the patient with personal health record (PHR) information. The patient's PHR includes the patient's identity, age, clinical diagnosis, medication status, and other information. At the same time, we classify the patient's PHR information for sensitivity. Information of different sensitivities is stored in the form of key-value pairs [15], giving different access rights for different secret keys, and the PHR information is stored on the medical institution's own distributed database IPFS. An index link of PHR is generated, which is a pointer to the file stored in the medical institution's own distributed database. The index is signed using the patient's private key, and this index is hidden from unauthorized users. This index is encrypted and recorded into the blockchain through the improved consensus algorithm in this paper ledger, which reduces the pressure of data storage and high frequency access in the blockchain. The patient obtains the index from the blockchain through the private key and gets his PHR from the medical institution.

The medical data storage model uses the Distance algorithm combined with the characteristics of medical resources for grouping to ensure the reliability of the grouping. The distance ranking hybrid mechanism selects the primary node, which improves the attack resistance of the system. The double consensus layer mechanism is for any node group. The primary node of the node group gets the medical data index and verifies the medical data index to generate the reserve message. The primary node sends the reserve message to each secondary node of the node group for the first PBFT consensus. When the first consensus is passed, the primary node sends the reserve message to the primary node of the other group for the second PBFT consensus. After the second consensus is passed, the primary nodes of other groups send the preparation messages to each sub-node of the other node groups for verification, and the medical data index will be stored for each medical node after the verification is passed. The node change mechanism is to evaluate the nodes after the consensus is completed. Byzantine nodes are marked and restricted to become

master nodes, and the medical nodes are dynamically adjusted within a T according to their behavior members to improve the scalability of the model. The whole model flow is shown in Figure 2.

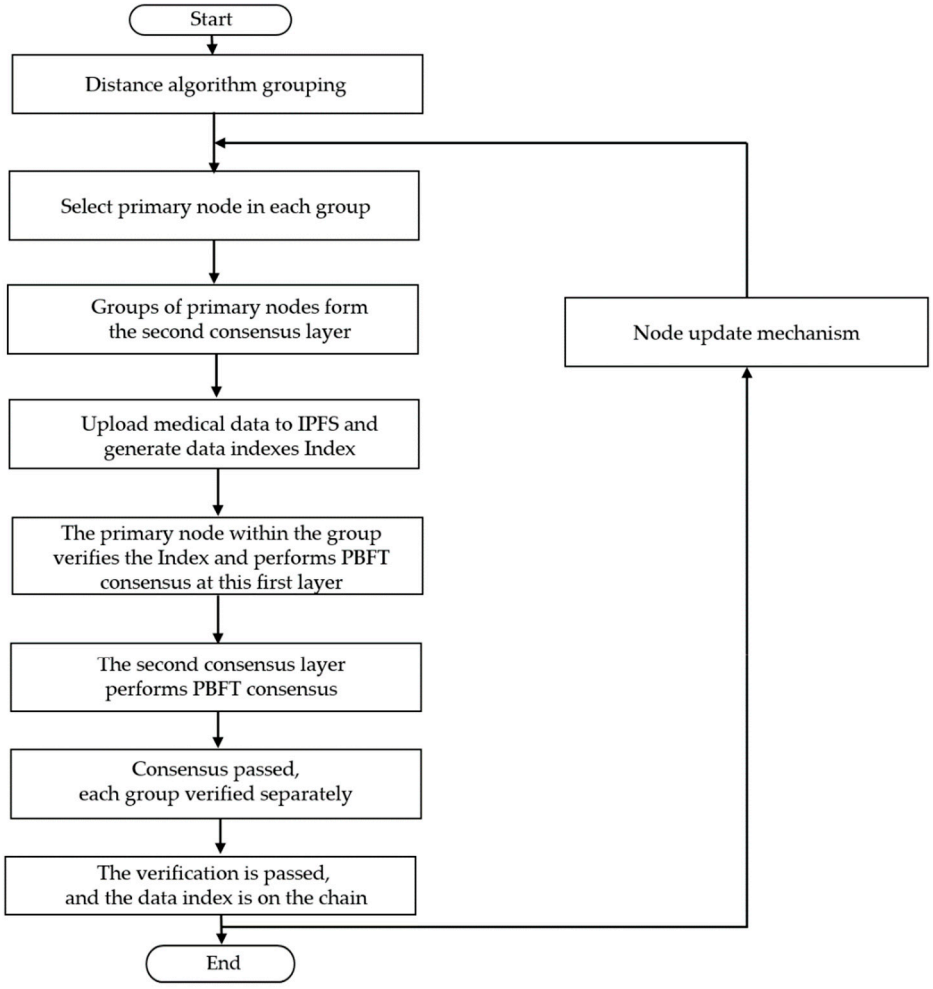

Figure 2. General flow chart of the model.

2.1. Distance Algorithm

According to the distribution of different medical nodes, the positions of medical nodes are relatively fixed. First, initialize the system: in a fixed period T, set several authorized hospital nodes into the initial set $U = \{n_1, n_2 \ldots n_i \ldots n_j \ldots\}$, group the U nodes in the group, and then re-determine which group joins according to the distance of the unjoined or ungrouped medical nodes, which is the basic idea of the Distance algorithm. By randomly selecting a node in the initial set as the current center node, set a threshold radius R, take the current center node and all medical nodes within the G_1 threshold radius as a group R, and then remove the already assigned nodes in the two-dimensional plane from U. Repeat the above until m a group is allocated, that is, $G = \{G_1, G_2 \ldots\ldots G_m\}$. The threshold radius R is the average value of the distance from the current hospital node n_i to the other hospital nodes in the initial node set U, which is expressed by the following formula:

$$R = \sum_{j \in U} \frac{d_{ij}}{|U|}, \tag{1}$$

where is d_{ij} the shortest distance from the current node n_i of the hospital to another node in a certain period. After assigning m groups, if there are still medical nodes that are not included, calculate the average of the distances from this medical node to the already

assigned m groups, respectively, md and calculate the average of the distances from node j to G_1 as follows.

$$md(j, G_1) = \sum \frac{d_{jG_1}}{|G_1|}, \tag{2}$$

According to Formula (2), the average distance between node j and the other groups in G can be calculated md, and the node can be added to md the group with the smallest average distance. If the calculated distance averages md are the same, the further selection of the appropriate group to join can be made based on the minimum standard deviation, which is given by the following formula:

$$sd(i, u) = \sqrt{\sum_{j \in u} \frac{\left(d_{ij} - md(i, u)\right)^2}{|U|}}, \tag{3}$$

Ensure that the probability of Byzantine errors is reduced when the number of medical nodes in each group satisfies $n > 3f$.

The following is the pseudo-code for the Algorithm 1.

Algorithm 1 Distance algorithm

Input:
Initial node collection U
Threshold radius R
Number of groups m
Output:
Initial groups G
1: *Initialize.* $G \leftarrow \{G_1, G_2 \ldots\ldots G_m\}$
2: for i *in range* $(1, m)$
3: c $\leftarrow$ *random* (U)
4: $G_i.add(c)$
5: $R \leftarrow (\sum_{j \in U, j \neq c} d_{cj})/(|U| - 1)$
6: for $j \in U$ && $j \neq c$
7: if $d_{cj} < R$ && !$enough(i)$
8: $G_i.add(j)$
9: $U \leftarrow U$-$\{j\}$
10: $U \leftarrow U$-$\{c\}$
11: *while* $U \neq \emptyset$ && $n \in U$
12: *for i in range* $(1, m)$ && ! $enough(i)$
13: $k, n \leftarrow \min(md(n, G_i)), sd(n, G_i))$
14: G_k. $add(n)$
15: *return* G

Algorithm 1 is equivalent to using m disjoint circles to cover these medical nodes, respectively, where the $enough(i)$ function returns true when the number of nodes in the i-th circle has been sufficient; otherwise, it returns false. It is ensured that the number of nodes in the m groups after using this grouping algorithm meets the predefined condition of $n > 3f$, which satisfies the possibility under the Byzantine [16] condition.

2.2. Consensus Algorithm of the Medical Data Storage Model

In order to ensure the reliability of data storage in the medical data blockchain platform, according to the characteristics and needs of specific medical data [17], a blockchain-based medical data storage consensus algorithm is designed. The consensus algorithm is an inheritance for the traditional PBFT algorithm, based on which the complexity of generality is reduced, and the improved PBFT algorithm does not require all nodes to participate, which greatly improves the communication efficiency. The algorithm includes four stages: grouping, election, consensus, and update. Aiming at the shortcomings of the PBFT consensus algorithm [18], this paper will fuse the Distance algorithm to create

a new consensus mechanism suitable for medical data storage. The medical nodes are grouped according to the Distance algorithm, and the medical nodes in different groups are combined according to the national hospital comprehensive rating and the Distance algorithm. The election of the primary node adopts the distance ranking hybrid algorithm. The scalability of the model is increased by the set node change mechanism. The consensus node set in this model sets a threshold value, and when the overall rating of a medical node is lower than the threshold value in a fixed period, it will be removed from the federated chain, while other medical nodes are re-ranked. The setting of the threshold method has fully mobilized the enthusiasm of medical institutions to provide better services for patients and will also become an important criterion for evaluating medical institutions in the future.

2.2.1. PBFT Consensus Algorithm

The PBFT (Practical Byzantine Fault Tolerance) algorithm aims to solve the problem of how to finally guarantee consistency and correctness in the presence of evil nodes in the whole system. The algorithm consensus protocol is divided into three stages, and the specific process is shown in Figure 3.

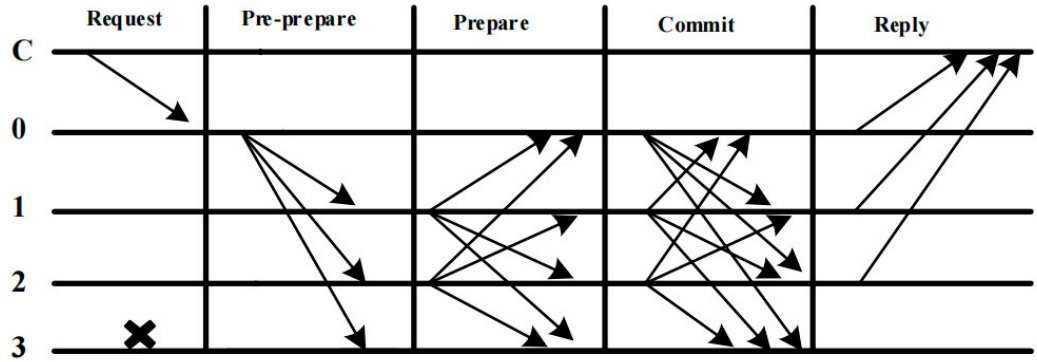

Figure 3. Flow chart of the PBFT consensus mechanism.

2.2.2. Consensus Mechanism for Medical Data Storage

1. Grouping: First, all medical nodes of the system are divided into M groups according to their distances within a fixed period T by the Distance algorithm. The specific cycle duration can be set appropriately according to the reality. The reason for regrouping medical nodes at intervals is to consider that the medical nodes of this model may change, which may affect the consensus efficiency. The generated master node ranking is fixed within a certain period and will only change due to master node replacement and the dynamic applications of medical nodes to join and exit.
2. Election: In m groups, in order to further improve communication efficiency and reduce the probability of malicious nodes becoming primary nodes, the selection of primary nodes adopts a distance ranking hybrid algorithm. The primary node election method adopted for the medical imaging blockchain platform is:

$$T = md * \alpha + vi * \beta \quad (\alpha + \beta = 1), \tag{4}$$

$$T = sd * \alpha + vi * \beta \quad (\alpha + \beta = 1), \tag{5}$$

Among them, T is the final ranking result of the primary node, md is the average distance, sd is the standard deviation of the distance, and vi is the comprehensive ranking of the hospital. α and β are different correction parameters set according to the change in the ranking value of medical institutions. $0 \leq \alpha, \beta \leq 1$. According to Formula (2), we calculate md for each node in the group to other nodes, and when the same md occurs, we calculate sd for each node in the group to other nodes according to Formula (3). The purpose of the distance ranking hybrid mechanism is to select a

number of primary nodes that are closer to each other in each group, thus reducing the transmission delay of preparatory information in the consensus phase.

3. Consensus: Assuming that there are Byzantine nodes in the node, when conducting sub-consensus groups, poll within the m group. If there is a request from a medical node to upload medical data, upload this request to the current primary node of the group first; the primary node will sort and verify the request, generate a pre-prepared message, and then send the sorted pre-prepared message to other medical nodes in the group for the first PBFT consensus. When the primary consensus group consensus is performed, the block will be confirmed by the second PBFT consensus in the primary consensus group after passing the consensus verification process of the sub-consensus group. When the first PBFT consensus is successful, the master node T1 of the group will broadcast the generated pre-prepared message to the master nodes of other groups for the second PBFT consensus. During the consensus process, each master node broadcasts its own digital signature and collects the digital signatures of other master nodes, and when the consensus is passed, each master node will package all the collected signatures and requests and send them to the other hospital nodes in the group, respectively. After receiving the packaged message, the hospital node verifies the digital signature collection, executes the request content after the verification is passed, and updates the medical data to the local blockchain ledger so that the consensus is completed. Below is the pseudo-code of this Algorithm 2.

Algorithm 2 Consensus

Input:
Initial node collection U
Initial groups G
Request node client
Collection of primary nodes T
Output:
Consensus results res

$send\ req(client, client.\ primary, req)$
$res \leftarrow false$
$res \leftarrow start(G_i + T)$
$if\ res\ is\ false$
$res \leftarrow start1(G.one)$ && $start2(T)$
$if\ res\ is\ true$
$two \leftarrow Package(req)$
$for\ t\ in\ T$
$broadcast\ (t\ node, G_t.one, two)$
$for\ node\ in\ G_t.one$ && $verif(two)$
$execute(req)$
$Return\ res$

The flow of the consensus algorithm for the specific medical data blockchain is shown in Figure 4 below:

4. Update: Most of the data of the medical imaging platform are stored in the server. If the master node hospital fails or goes down, the master node will be replaced to ensure the normal and efficient operation of the medical imaging platform. The node replacement mechanism is as follows: according to the result of the above election, the master node will be polled down in the master node ranking set according to the ranking result T. If the rotating master node is also down, the rotation will continue down. The rotated master node will be removed from the consensus. In order to ensure fairness, if the master node is replaced within a fixed period T, the set T of the election will be recalculated so that all other nodes have the opportunity to become the master node to prevent a monopoly caused by a single node. When a new medical node wants to join, by calculating the average distance md from the medical node to each node group, the smallest distance average node group is selected, and the new

medical node is added to the small node group when there is no medical node data index up-link request in the node group. When a medical node wants to quit, the medical node that wants to quit sends a quit command to the primary node of the node group that the medical node wants to quit, and after verification, the medical node is deleted from the node group when the node group is free. At the same time, we can regroup after a fixed period T. The specific period T can be set according to the new hospitals and the actual demand to ensure the most efficient transmission efficiency and reduce the consensus delay and communication times.

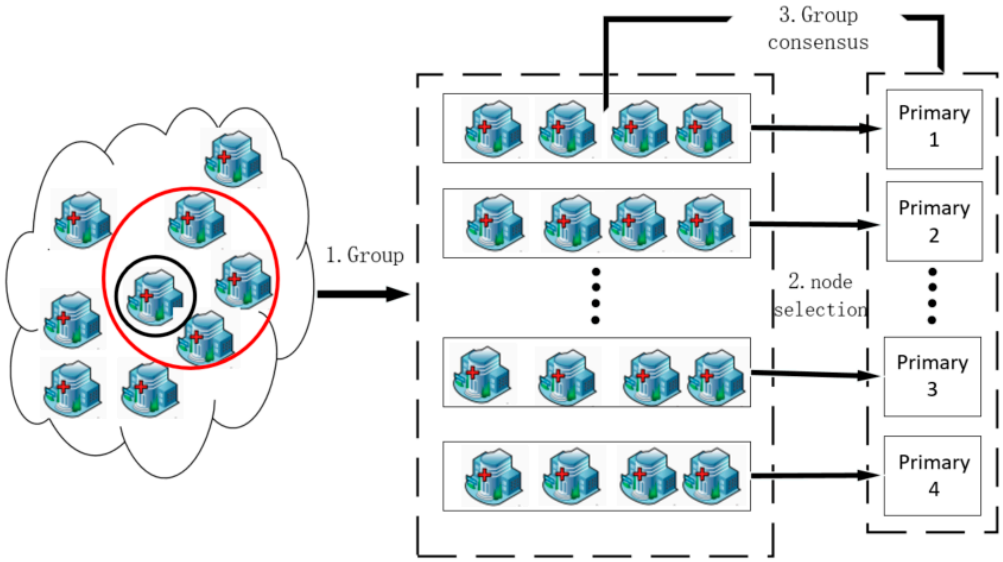

Figure 4. Consensus model diagram of the medical data storage blockchain.

3. Analysis and Evaluation

3.1. Security Analysis

3.1.1. Comparative Analysis

The traditional health care data models all have monopoly and privacy problems [19]. In this paper, we use the alliance chain combined with IPFS to ensure the secure storage of data without relying on third-party entities, and each medical node communicates with each other in a peer-to-peer manner. IPFS stores the original data and places the encrypted data hash index on the chain, thus avoiding the traditional storage that leads to the central medical node being maliciously attacked. For the medical alliance chain in this paper, there are usually new medical nodes that want to join and medical nodes in the alliance chain that want to exit. By setting a dynamic access mechanism that allows medical nodes to dynamically join and exit this medical alliance chain, when a new medical node wants to join, the smallest distance average node group is selected by calculating the average distance *md* from this medical node to each node group. When there is no medical node data indexing request in this node group, the new medical node is added to this small node group. When a medical node wants to quit, the medical node that wants to quit sends a quit command to the master node of the node group that the medical node wants to quit, and after verification, the medical node is deleted from the node group when the node group is free. At the same time, we can regroup after a fixed period T. The specific period T can be set according to the new hospitals and the actual demand to ensure the most efficient transmission efficiency and reduce the consensus delay and communication times, so the storage model in this paper has good scalability and reliability. The following comparison (Table 1) is used to analyze and compare the differences with existing solutions.

Table 1. Scheme comparison.

Programs	Blockchain-Based	Consensus Mechanism	Focus on Medical Issues	Affiliate Chain
Factom [20]	No	None	No	No
MedRec [9]	Yes	POW	Yes	No
AMDSM [8]	Yes	DPOS + PBFT	Yes	No
This article	Yes	Improvement of PBFT	Yes	Yes

3.1.2. Security Analysis of Attack Blocks

This experiment uses the fabric underlying platform to test [21] that, when an attacker launches a block masquerading attack, it needs to make a parallel chain to replace this medical data chain faster than the normal consensus node. Assume that r is the probability that an honest medical node creates the next node, w is the probability that the attacker makes the next node, and n is the number of blocks the attacker needs to fill; then, the probability that the attacker succeeds w_n is:

$$w_n = 1 - \sum_{k=0}^{n} \frac{\lambda^k . e^{-\lambda}}{k!} \left(1 - \left(\frac{w}{r}\right)^{(n-k)}\right), \lambda = n\frac{w}{r}, \quad (6)$$

The w-values taken are 0.1 and 0.2, and the size of w_n according to Equation (6) is calculated as shown in Figure 4. From Figure 5, it can be seen that the probability of a successful attack w_n by the attacker tends to decrease exponentially as the block increases. In addition, since the real medical alliance chain network has a large number of nodes and a large amount of computing power and the number of blocks in the main chain is much larger than 10, the probability of a successful attack by the attacker is almost 0.

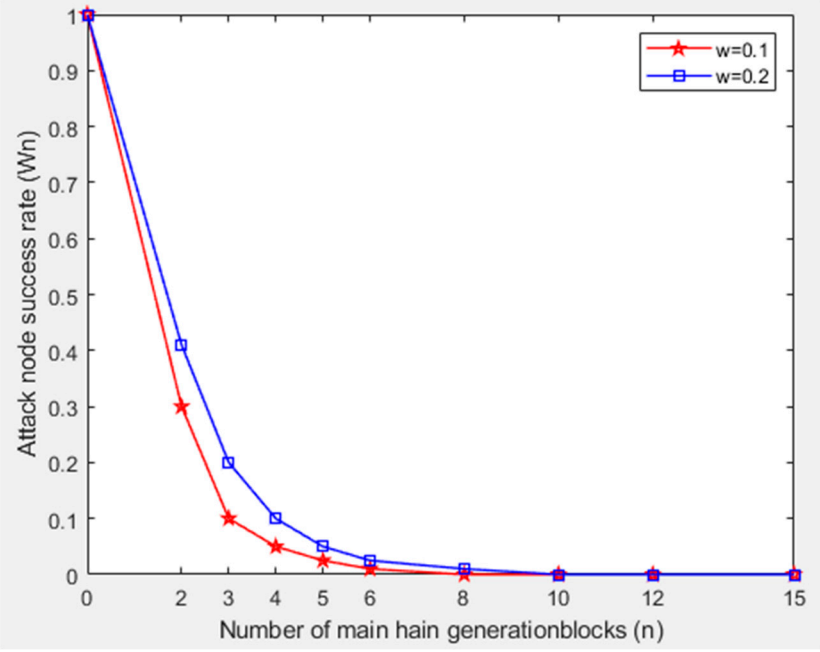

Figure 5. Probability of a successful attack.

3.2. Analysis of Communication Complexity

This paper adopts the method of grouping medical nodes into consensus slices and simplifying the second consensus process to solve the problem of the high communication complexity and poor scalability of PBFT. Specifically, a node must broadcast a message to all other nodes, and at least 2/3 of the nodes receive a valid message. From Figure 2, it can

be seen that the number of communications between the nodes in the network of PBFT in the pre-preparation phase is $n-1$, the number of communications between the nodes in the network in the preparation phase is $n*(n-1)$, and the number of communications between the nodes in this network in the commit phase is $n*(n-1)$, so the number of communications in the network of the traditional PBFT consensus algorithm is $2n^2-n-1$. The number of SG-PBFT three-stage inter-node communications in the references [22] is $(n/2-1)*(n/2+1)$. Assuming that there are n consensus nodes in the medical alliance chain for group slicing, which are divided into k groups by Distance, the improved secondary communication complexity of this paper is compared with the communication complexity of the above algorithm, as shown in Table 2.

Table 2. Comparison of Communication Complexity.

	Pre-Prepare	**Prepare**	**Commit**	**Total**
PBFT	$n-1$	$N*(n-1)$	$N*(n-1)$	$2n^2-n-1$
SG-PBFT	$n/2-1$	$(n/2-1)*(n/2-1)$	$n/2-1$	$(n/2-1)*(n/2+1)$
	The First Time		**The Second Time**	**Total**
This article	$(1+2n/k)*(n/k-1)$		$(k-1)*(2k+1)$	$(k-1)*(2k+1)+(1+2n/k)*(n/k-1)$

In order to show the difference between them more clearly, this paper compares the communication complexity under different numbers of network nodes. When the number of nodes in the network does not reach 32, the communication complexity of the three consensus algorithms is not much different. In this medical data storage alliance chain, when the number of medical nodes increases, the difference between the two increases significantly. The communication complexity of the traditional PBFT algorithm increases rapidly at a quadratic level, and the communication complexity of the medical data consensus in this paper increases almost linearly and slowly. The difference between SG-PBFT and the method in this paper also increases significantly with the number of nodes. Assume that n/k in the grouping in this article is an integer, as shown in Figure 6 below.

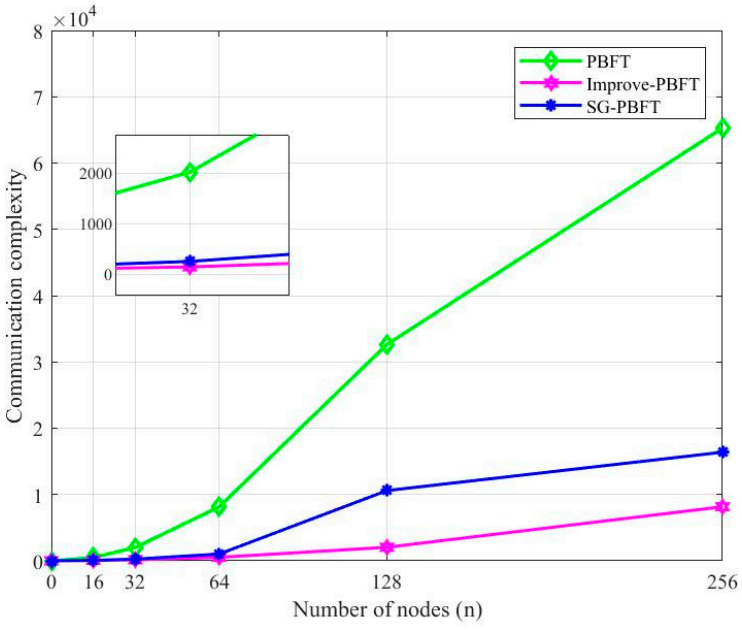

Figure 6. Comparison of communication complexity with different numbers of nodes.

4. Conclusions and Outlook

With the rapid growth of medical data, the centralized storage of medical data may be eliminated, and the rise of blockchain technology is one of the ways to solve this problem. The medical data storage model proposed in this paper can help existing centralized medical institutions transform to meet the increasing demand for the safe storage of medical data. At the same time, the main node is selected by dynamic ranking and the replacement algorithm, reduces the risk of system downtime, and ensures the load balance of each medical node. By using the distributed storage algorithm, uploading the user's encrypted index protects the system to a certain extent. Blockchain technology is under experimental research in various countries. This paper lacks the combination of related technologies such as smart contracts. The next step will be to improve smart contracts to further improve the model.

Author Contributions: Conceptualization, K.C. and W.F.; methodology, W.Z.; software, K.C.; validation, X.Z. and W.F.; formal analysis, W.Z.; investigation, K.C.; resources, Y.Z.; data curation, K.C.; writing—original draft preparation, K.C.; writing—review and editing, W.F.; visualization, W.Z.; supervision, Y.Z.; project administration, Y.Z.; funding acquisition, W.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key Research and Development Project under Grant 2018YFB1404400, the National Natural Science Foundation of China under Grant 62062030, and the Major Science and Technology Project of Haikou under Grant 2020-009, and Key R&D Project of Hainan province (Grant #: ZDYF2021SHFZ243).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Acknowledgments: The authors would like to thank the editors and the reviewers for their valuable time and constructive comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Souiki, S.; Hadjila, M.; Moussaoui, D.; Ferdi, S.; Rais, S. M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation. In Proceedings of the 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH), Boumerdes, Algeria, 9–10 February 2021.
2. Naumov, V.; Szarata, A.; Vasiutina, H. Simulating a Macrosystem of Cargo Deliveries by Road Transport Based on Big Data Volumes: A Case Study of Poland. *Energies* **2022**, *15*, 5111. [CrossRef]
3. Thakur, N.; Han, C.Y. Indoor Localization for Personalized Ambient Assisted Living of Multiple Users in Multi-Floor Smart Environments. *Big Data Cogn. Comput.* **2021**, *5*, 42. [CrossRef]
4. Hao, W.; Yujiao, S. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *J. Med. Syst.* **2018**, *42*, 152.
5. Chen, W.; Zheng, Z. Blockchain Data Analysis: A Review of Status, Trends and Challenges. *J. Comput. Res. Dev.* **2018**, *55*, 1853–1870.
6. Esposito, C.; Santis, A.D.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
7. Wang, H.; Liu, Y.; Cao, S.; Zhou, M. A medical data storage mechanism incorporating blockchain technology. *Comput. Sci.* **2020**, *47*, 285–291.
8. Feng, T.; Jiao, Y.; Fang, J.; Tian, Y. Medical and Health Data Security Model Based on Consortium Blockchain. *Comput. Sci.* **2020**, *47*, 7.
9. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open & Big Data, Vienna, Austria, 22–24 August 2016.
10. Proof of Burn [EB/OL.]. Available online: https://en.bitcoin.it/wiki/Proofofburn (accessed on 10 April 2018).
11. Zhang, L.; Li, Q. Research on Consensus Efficiency Based on Practical Byzantine Fault Tolerance. In Proceedings of the 2018 10th International Conference on Modelling, Identification and Control (ICMIC), Guiyang, China, 2–4 July 2018.
12. Perez, A.O.; Domingo-Palaoag, T. Blockchain-based Model for Health Information Exchange: A Case for Simulated Patient Referrals Using an Electronic Medical Record. In *IOP Conference Series: Materials Science and Engineering, Proceedings of the 5th International Conference on Information Technology and Digital Applications (ICITDA 2020), Yogyakarta, Indonesia, 13–14 November 2020*; IOP Publishing: Yogyakarta, Indonesia, 2021; Volume 1077, p. 012059.

13. Cheng, L.; Qi, Z.; Shi, J. EHR data security storage and sharing scheme based on blockchain. *J. Nanjing Univ. Posts Telecommun. Nat. Sci. Ed.* **2020**, *40*, 7.
14. Feng, X.; Shi, Q.; Xie, Q.; Liu, L. An Efficient Privacy-preserving Authentication Model based on blockchain for VANETs. *J. Syst. Archit.* **2021**, *117*, 102158. [CrossRef]
15. Xue, T.F.; Fu, Q.C.; Wang, C.; Wang, X.Y. A Medical Data Sharing Model via Blockchain. *Zidonghua Xuebao/Acta Autom. Sin.* **2017**, *43*, 1555–1562.
16. MJalalzai, M.; Busch, C.; Richard, G.G. Consistent BFT Performance for Blockchains. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S), Portland, OR, USA, 24–27 June 2019; pp. 17–18. [CrossRef]
17. Li, M.; Wang, C.; Yan, L.; Wei, S. Research on the Application of Medical Big Data. In Proceedings of the 2019 14th International Conference on Computer Science & Education (ICCSE), Toronto, ON, Canada, 19–21 August 2019; pp. 478–482. [CrossRef]
18. Gan, B.; Wu, Q.; Li, X.; Zhou, Y. Classification of Blockchain Consensus Mechanisms Based on PBFT Algorithm. In Proceedings of the 2021 International Conference on Computer Engineering and Application (ICCEA), Kunming, China, 25–27 June 2021; pp. 26–29. [CrossRef]
19. Chen, H.; Yu, J.; Liu, F.; Cai, Z.; Xia, J. Archipelago: A Medical Distributed Storage System for Interconnected Health. In *IEEE Internet Computing*; IEEE: New York, NY, USA, 2020; Volume 24, pp. 28–38. [CrossRef]
20. Snow, P.; Deery, B.; Lu, J.; Johnston, D.; Kirby, P.; Sprague, A.Y.; Byington, D. Business Processes Secured by Immutable Audit Trails on the Blockchain. Available online: https://bravenewcoin.com/insights/business-processes-secured-by-immutable-audit-trails-on-the-blockchain (accessed on 17 November 2014).
21. Atreyapurapu, S.B.; Amarendra, K.; Alishah, M.M. Hyperledger Fabric based Medical Record Security. In Proceedings of the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January 2022; pp. 223–228. [CrossRef]
22. Xu, G.; Bai, H.; Xing, J.; Luo, T.; Xiong, N.N.; Cheng, X.; Liu, S.; Zheng, X. SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles. *J. Parallel Distrib. Comput.* **2022**, *164*, 1–11. [CrossRef]