Application of Blockchain Technology in Pet Medical Industry

Huajie Zhang¹, ², Shaofei Wu¹, ², *, Shenkuo Wang¹, ² and Ning Xia¹, ²

¹Laboratory of Intelligent Robot, Wuhan Institute of Technology, Wuhan, China
²School of Computer Science & Engineering, Wuhan Institute of Technology, 420205, Wuhan, China

*Corresponding author e-mail: wasbfc@yeah.net

Abstract. According to the development status of the pet diagnosis and treatment industry, it can be found that the industry is still on the rise at present, but the island phenomenon of information in the traditional medical industry information system also exists. The authenticity and timeliness of information interaction cannot be guaranteed, and Problems such as difficulties about industry chaos and data access also limit the development of the industry. This paper puts forward a model of pet medical data sharing based on block chain, and it has many characteristics, such as safety reliable, decentralized applies to resolve such problems as pet medical industry data sharing. The existing consensus mechanism has been improved, and then the solutions of the model and the possible impacts are discussed and analyzed by comparing the problems of the industry.

1. Introduction

With the progress of the times and the in-depth development of the market economy, the people's living standards have also increased rapidly under this general trend. The living standards improve with the increasing of urban life pressures [1], at the same time, an aging population problem has not been resolved. The only child and modern young people have to spend less and less with their parents and children to work, which causes the occurrence of empty nest phenomenon. Under this circumstance, more and more people choose to raise their favorite small animals as pets as a way for their emotional support and stress relief. With the increasing number of pets and the growing pet economy, the emergence and development of pet hospitals have escorted the development of this emerging market, providing health guarantees for the small owners of the pet family, but in the course of the development has exposed many problems, such as: traditional pet medical is not yet mature, and with the number of pets and pets rising, pet hospitals are also increasing, but the threshold of this industry is low, the relevant laws and regulations are still not perfect, resulting in the emergence of unlicensed operations or chaotic operations. In the pet medical service industry, the charges are generally more expensive, and consumers gradually lose confidence in the opaque information and unreasonable charges. In addition, due to the lack of supervision and leading enterprises in the industry market, the lack of motivation and lack of trust among the pet hospitals leads to a large amount of data in the database of individual pet hospitals, forming islands and other issues.
In recent years, although the blockchain has obtained a good development environment in China, there are still few technical documents that can be referenced at present [2], especially those concerning the application of blockchain technology in pet medical treatment [3]. This paper will combine the application of blockchain technology in data and medical applications, and propose a pet medical alliance chain data sharing scheme based on blockchain technology for solving the problems in the traditional pet medical industry information system. The program fully absorbs the advantages of the blockchain technology, and connects the pet hospital, the pet supply alliance and the government regulatory department to make it have the distinctive features of equality, efficiency and mutual trust. Based on the conceptual model and technical architecture of the PMAC (pet medical alliance chain), the paper explores the shortcomings and improvements of the blockchain technology and finally constructs the model.

2. Blockchain Technology

Blockchain technology originated from the seminal 2008 paper "bitcoin: a peer-to-peer electronic cash system" published in the cryptography email group by a scholar using the pseudonym "Satoshi nakamot" [4], which has not yet formed an industry-Recognized definition of blockchain. As explained in the book "blockchain revolution" that blockchain is an indestructible ledger of transactions in the distributed digital economy. It can programmatically record not only financial transactions, but also almost all valuable transactions.

2.1. The concept of blockchain technology

Blockchain technology [5] is to use the chain data structures to validate and store data, and use distributed node consensus algorithms to generate and update data, through the use of cryptography way to ensure the security of data transmission and access, using smart contracts to program and manipulate data in a completely new distributed infrastructure and computing paradigm. To put it simply, after each period of time, the transaction data generated by each participant will be packaged into a data block and the data blocks are arranged in chronological order to form the chain of the data block in the blockchain system. All participants have the same data chain and cannot unilaterally tamper with it. Any modification of the information can only take effect if the subject of the agreed proportion is approved, and only new information can be added but the old information cannot be modified or deleted, thereby realizing information sharing and consistent decision-making among multiple subjects, reaching the identity of each subject and the transaction information between subjects can not be tampered with, and can be open and transparent.

2.2. The technical principles of blockchain

Blockchain is a technology that collectively maintains a reliable database through decentralization and de-trusts. In fact, blockchain technology is not a single and completely new technologym but the result of the integration of various existing technologies. Blockchain technology is a technology in which everyone participates in recording information and storing information. In the past, data recording and storage were left to centralized institutions, while blockchain technology allowed everyone in the system to participate in the recording and storage of data. The blockchain technology constructs a P2P self-organizing network by using a distributed collective operation method under a distributed peer-to-peer network without central control points. Through the complex check mechanism, the blockchain database can maintain integrity, continuity and consistency. Even if some participants falsified, they can not change the integrity of the blockchain and tamper with the data in the blockchain. Key points involved in blockchain technology include: decentralization, collective maintenance, timestamps, reliable databases, de-trust, asymmetric encryption, and more.

Blockchain technology redefines the way that credit is generated in the network: in the system, participants do not need to know other people’s background information, and do not need the guarantee of third-party organization. Blockchain technology guarantees the system’s value transfer. The activities are recorded, transmitted, stored and final result must be credible.
The origin of blockchain technology principle can be summarized as a mathematical problem: Byzantine failures [6]. Byzantine failures extend to the life of the Internet and its connotation can be summarized as follows: in the context of the Internet, how can people be prevented from being deceived by vandal to make wrong decisions when they need value exchange activities with unfamiliar counterparties? Further extending Byzantine failures to the technical field, its connotation can be summarized as: how to achieve consensus among the various nodes distributed in the network in the absence of a trusted central node and a trusted channel. Blockchain technology solves the long-standing problem of Byzantine failures—a way to create a consensus network without having to trust a single node. Fig.1 depicts the blockchain data structure for Bitcoin [7].

3. Pet Medical Data Sharing Model
The types of blockchain can be divided into public chain and private chain [8]. On the basis of private chain, it can be further subdivided into fully-closed pure private chain and semi-open private chain—alliance chain. By analyzing and comparing the information subjects in the pet medical industry, it’s particularly important to select the appropriate blockchain type according to the structural characteristics of the industry.

3.1. Type selection of blockchain
The public chain has the highest degree of openness, the strongest decentralization attribute and the lowest admittance threshold, so everyone can participate in the mining and the maintenance of nodes and the safety is the highest. The public chain is completely decentralized blockchain in the true sense, which ensures that transactions can’t be tampered through cryptography. Meanwhile, it uses cryptographic verification and economic incentives to establish consensus in the unfamiliar network environment, so as to form a decentralized credit mechanism. The private chain is only used by private organizations, and the read or write permissions and the participation in bookkeeping permissions on the blockchain are also defined by the rules of private organization. Fewer verification of the nodes can improve the transaction speed but lose some security. Because it is a blockchain under the control of entities, it can conduct very cheap or even completely free transactions on the private chain, which is infinitely close to the centralized database. The consensus process of the alliance chain is controlled by pre-selected nodes, so it is not completely equal. It inherits the characteristics of fast transaction speed and low maintenance cost of the public chain. Although the alliance chain is a semi-open private chain, the privacy permissions will be very different and more complicated due to different application scenarios, and it is more reliable than the private chain.

Through the analysis, it is concluded that the public chain is too slow for the transaction and the entry threshold is too low for the specific organization environment; for the pure private chain, the
singleness of the service object results in the loss of important characteristics of the closed and centralized structure of the blockchain. In contrast, the alliance chain not only abandons part of the center to make it more widely applicable, but also realize partial decentralization of the network under the condition condition of ensuring the transaction speed, thus ensuring the non-tampering of data. Based on the structural characteristics of the industry, the form of alliance chain based on blockchain technology becomes the best choice. Table 1 shows the comparison of different types of blockchain from multiple perspectives.

| Table 1. Compare different types of blockchain. |
|-----------------------------------------------|
| Service object | Degree of centralization | Consensus speed | Transaction speed | Bookkeeper | Node storage mode | Transaction cost | Field of application |
|----------------|--------------------------|-----------------|-------------------|------------|-------------------|-----------------|---------------------|
| Public chain   | anyone                   | decentralized   | slow              | 3-20/s     | anyone            | PC              | high                | Finance, digital currency transaction, copyright authentication, etc |
| Alliance chain | Specific organization member | multi-center | fast              | 1K-10K+/s  | participant negotiation | specific server | medium              | Organizational transactions, audit settlement, etc |
| Private chain  | Individual or organization | centralization | fast              | 1K-100K+/s | customized         | specific server | low                 | Internal information system of large enterprises |

3.2. PMAC model
According to the industry characteristics, the components includes in the pet medical industry data sharing model are shown in Fig.2. Through the analysis of the current status of the industry, the model consists of data sharing between pet hospitals, data records of pet owners and pet hospitals, and supervision of the industry by the regulatory authorities. And by taking the pet owner to obtain pet health data as an example.

Operation steps are as follows: (1) the pet owner sends a request to the doctor to obtain the data to verify the identity of the pet owner; (2) after the verification, the pet owner authorizes the doctor to diagnose and treat the pet; (3) the doctor obtains the past medical history of the pet through the authorization of the pet owner by sending a request for the past medical record to the pet owner; (4) after both the pet owner and the doctor reach a consensus on the record content of the pet diagnosis and treatment, the recording operation is performed; (5) the pet owner performs a corresponding confirmation operation on the record; (6) update the content and status of the pet medical records after confirmation; (7) at the end, the status of the pet is updated, and the doctor acquires and stores the pet by locating the out line content of the pet.

3.3. Model architecture and consensus
The infrastructure of blockchain can be generally divided into data layer, consensus layer, network layer, construct layer and application layer. Since in the alliance chain, the normal operation of the maintenance alliance chain is the responsibility of each node, and the resulting benefit distribution can be completed through prior consultation, so the content of the incentive layer will not be discussed for the time being. Therefore it is sorted out from the other five levels, as shown in Fig.3.

In the existing blockchain projects, the main consensus mechanisms are PoW(Proof of Work) [8] and PoS(Proof of Stake) [9], and a small number of projects adopt the revised BFT(Byzantine fault tolerance) consensus mechanism and Bitcoin is the most successful cryptocurrency under the PoW mechanism. Although the PoW mechanism has successfullyproved its long-term stability and relative fairness, under the existing framework, PoW’s “mining” form will consume a lot of energy. Peercoin and Nextcoin use PoS model. Compared with PoW, PoS mechanism saves energy and introduces the concept of “coin day” to participate in random computing, but in the long run, generating blocks is much lower than the speed of network propagation and broadcasting. Therefore, under the PoS...
mechanism, it is necessary to limit speed the generated blocks to ensure stable operation of the main network.

Figure 2. PMAC Shared model structure.
Application layer

Contract layer

Consensus layer

Network layer

Data layer

Pet Medical Alliance Chain

Figure 3. PMAC technical framework.

Table 2. Comparison of consensus mechanism.

| Consensus mechanism | Mining cost | Token | Decentralization | Transaction throughput | Security threat | Application scenario example |
|---------------------|-------------|-------|------------------|------------------------|----------------|------------------------------|
| PoW (Proof of Work) | Power       | need  | yes              | 10min/block            | Concentration of power | Bitcoin                     |
| PoS (Proof of Stake) | currency time | need | incomplete       | 10min/block            | Node offline revenue | Peercoin                    |
| DPoS (Deposit-based Proof of Stake) | margin | need | incomplete       | 10s/block              | Candidate cheating | Bitshares                   |
| Casper              | margin      | need  | incomplete       | 3s/block               | Oligopoly         | Ethereum                    |
| PBFT (Practical Byzantine Fault Tolerance) | no         | no    | yes              | 1s/block               | DDoS             | Hyperledger                 |

According to the characteristics of PMAC multicentrism, this paper proposes a new suitable consensus mechanism—a dynamic random DPoS consensus mechanism based on VRF (verifiable random function). In VDPoS, the system will vote inside the proxy node at regular intervals, select three trustees to perform multi-directional verification of the transaction, and one of them will get the bookkeeping’s right. Through the VRF functions, the system can select a random subset of these nodes based on the weight of the proxy node. And the probability of agent node being selected is approximately equal to the ratio of own weight $w_i$, effective weight $\tau$ and total weight $W=\sum w_i$, $p=\tau/W$. The randomness of this consensus stems from the VRF function and a publicly verifiable random seed, on which each agent node can verify that a subset is selected as a trustee. Table 2 shows the comparison of existing consensus algorithms from multiple perspectives.

4. Evaluation and analysis

In this paper, the method of comparative analysis is adopted. On the one hand, since there is no corresponding model for the pet medical industry, the safety comparison between the VRF function and other random functions is carried out. On the other hand, through the discussion of the existing
problems in the current pet medical industry and analysis of the advantages and possible impact of the model.

Through the commonly used random number generation algorithms such as linear congruence, Mersenne twister and middle square method, are tested to generate scatter plots and compares the algorithms from the aspects of security, sparsity and time. The four subgraph of Fig.4 are drawn from 2000 points generated by different algorithms. By comparison, the middle square method has a significantly sparse distribution compared with other algorithms, that is, the algorithm may have hit the cycle length at 2000 points, while the other three functions have better randomness. And through the comparison of the random number generated time, the generated time of MT(Mersenne Twister) algorithm is about 800ms, the generated time of VRF algorithm and middle square method is about 100ms, and the generated time of LCG(Linear congruential generator) algorithm is about 60ms. In terms of security, the literature has proved the security of VRF, and other functions are not safe enough because of the short cycle.

Based on the analysis of various current problems, this paper proposes a blockchain-based information sharing solution for the pet medical alliance chain to solve the current problems, such as privacy and security issues: Trust and access issues through the promotion of electronic pet medical data, and the corresponding pet medical data with a trusted agent; The hacker attack and the medical data protection use the asymmetric cryptography to encrypt data to improve security; In order to prevent the occurrence of denial events, the information will be periodically anchored to the bitcoin public chain to prevent the occurrence of deadbeat events by virtue of the untamable features of the public chain. User engagement problem: In the past, users could not effectively manage their pet’s health data and related causes and treatment methods. Now, users can manage their pet’s electronic medical records by themselves, and entrust the rights through encryption technology. Medical data abuse and fraud: data abuse, accountability difficulties and improper charges in the pet medical industry, false statements and other chaos are currently facing larger problems. The model uses the responsibility system of rotation, using blockchain technology to facilitate accountability, and get credible and consistent results by logging online to avoid wasting money. Interoperability,
accessibility and data integrity issues: since the market is not yet stable, the data is stored in different data centers, data exchange between individual pet hospitals is difficult, and the problem of data islands is formed. In this paper, through the model to open up data islands between various pet medical institutions to achieve convenient data interoperability. And through the characteristics of distributed storage node of blockchain, multiple backups of data is guaranteed, and the problem of data loss or incomplete data is avoided. Through the alliance chain to achieve a unified data query interface, unified data standards, real-time data sharing.

5. Conclusion
You do not need to include page numbers or running headlines. These elements will be added by the publisher.

The management and data sharing of pet medical institutions, the information’s protection of black-hearted pet medical institutions and pet owners caused by data opacity have not yet formed a reasonable solution. From the point of view of the current, in addition to the privacy and safeguard legal rights of the consciousness that our pet health care industry chaos and lack of motivation to build platforms, the current privacy protection technology and the lack of right protective methods is also difficult, and the emergence of blockchain technology solves the problem and provides a corresponding effective solution mechanism. Firstly, data sharing of pet medical electronic medical records is achieved through the alliance chain, and data exchange between different pet hospitals is realized, which effectively provides the corresponding data support for subsequent medical research work. Then, users and transaction contents are treated openly and transparently through the use of blockchain technology, which effectively prevents unreasonable charges and eliminates the emergence of unlicensed or less-certified pet hospitals operating illegally through identity authentication. Finally, user can deepen their control of their data and pet data through electronic medical records, effectively preventing data leakage and abuse.

In this paper, as blockchain is an emerging technology, the current application is still exist in the experimental stage. Therefore, the research has some limitations and deficiencies in this paper. In the near future, it can be further demonstrated and realized by means of simulation and other methods, and it can be tried to be popularized to other application scenarios.

Acknowledgements
This work was supported by Natural Science Foundation of Hubei Province of China (Grant No.2018CFB681). We thank the editors and the anonymous reviewers for their insightful comments which have helped to improve the quality of the paper.

References
[1] Zhan H, Xizhe, Peng. China’s Population Aging from the Perspective of Public Policy [J]. 32(4) 2019, 106-124.
[2] Jesse Y H, Ko Deokyoong, Choi Sujin, et al. Where Is Current Research on Blockchain Technology?—A Systematic Review [J]. Plos One, 11(10) 2016, e0163477-
[3] Angraal S, Krumholz H M, Schulz W L. Blockchain Technology: Applications in Health Care [J]. Circ Cardiovasc Qual Outcomes, 10(9) 2017, e003800.
[4] Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[5] Risius M, Spohrer, Kai. A Blockchain Research Framework [J]. Business & Information Systems Engineering, 59(6) 2017, 385-409.
[6] drdobbs. The Byzantine General's problem [J]. Acm Transactions on Programming Languages & Systems, 4(3) 1982, 382-401.
[7] Fauzi M R R, Nasution, Surya Michrandi, Paryasto, Marisa W. Implementation and Analysis of the use of the Blockchain Transactions on the Workings of the Bitcoin [J]. IOP Conference Series: Materials Science and Engineering, 260(8) 2017, 012003.
[8] Tang C B, Yang Z, Zheng Z L, et al. Game Dilemma Analysis and Optimization of PoW
[9] Liu, Dongxiao, Alahmadi, Amal, Ni, Jianbing, et al. Anonymous Reputation System for IIoT-enabled Retail Marketing atop PoS Blockchain [J]. IEEE Transactions on Industrial Informatics, PP(99) 2019, 1-1.