Research on Missile Data Security Based on Blockchain

Yidong Wang¹, Linhu Cong², Yi Fang²*, Jianqiu Deng² and Yuliang Chen²
¹Units 92228 of PLA, Beijing, 100010, China
²Naval Aeronautical University, Yantai, Shandong, 264001, China
*Corresponding author’s e-mail: 395510796@qq.com

Abstract. Existing aviation missile business data records and storage have the disadvantage of being tampered with easily, being traced difficultly, and other security risks. Aiming at these problems, this paper applies blockchain technology to the data recording and storage scene of aviation missile business, carries on the network structure design, uses the current mainstream encryption algorithm and the encryption technology, constructs the block chain based aviation missile service data recording storage system, and describes the system working principle and how the system protects the data. Security analysis shows that the system can effectively protect the security record and storage of data, and lays a certain foundation for further exploring the application of blockchain in military.

1. Introduction
Aviation missile business is an important regular work in the management of aviation missile equipment, covering many aspects such as the management, maintenance, use and transportation of aviation missiles, which involves more data items requiring registration records and a large amount of data [1].

The general use of the force is still paper recording, storage, this way has become more and more unsuitable for the requirements of the Force information construction, there are many drawbacks: personnel in the data recording is often because of scribbled can not be identified, paper materials are easy to pollute, usually concentrated in specialized archives and no backup, There are hidden dangers such as data loss, malicious tampering or destruction, many of the same data items fill up a lot of work, reduce the efficiency, the person in charge often has a signature when signing, the need for accountability leads to unclear division of responsibilities, the record format is not standardized, there will be a clerical error situation, reducing the credibility of the data When using a computer for data analysis, it is necessary to enter the data recorded by the paper into the computer first, which is inconvenient for the work.

Although some troops have been equipped with digital data recording software, to a certain extent to solve the above traditional records, storage methods, but this only completed the record, storage form changes, basically did not consider the credibility of the data and data traceability. Although the way data is stored has become digital storage, it still belongs to centralized storage, which is useless to fundamentally change the way it is stored.

In 2008, Nakamoto proposed bitcoin for the first time in his paper "Bitcoin:a peer-to-peer Electronic Cash System" [2], and blockchain, as the core technology of Bitcoin, played a vital role in the normal operation of bitcoin system. Blockchain is a kind of distributed data storage technology based on cryptography, which can guarantee the traceability of data and make the data difficult to be maliciously tampered with, while realizing the centrality, with the characteristics of anonymity and
high data reliability [3]. The research and application of blockchain in China is just beginning, mainly used in logistics [4], medical data [5], identity authentication [6], commodity traceability and other fields [7], however, there is very little research on a specific application scenario in the military field, and most of the research is at the system level of research [8].

In view of the above problems, this paper considers the problems of data access, recording and storage of aviation missile business. Using blockchain technology and using bitcoin data structure as prototype, this paper studies, improves and designs according to the actual situation of aviation missile business. The aim is to propose a special data model specifically for aviation missile business data in order to realize data distributed storage, improve the reliability of data and realize the traceability of data.

2. Block chain technology

2.1 Block Data structures
The simplest definition of a blockchain is to package the data into chunks (blocks) and use some cryptographic principles to connect the chunks to form a chain of multiple data chunks, the blockchain [9]. The chunks record not only the data that needs to be stored, but also many information for security validation and various digital signatures [10]. A typical bitcoin block data structure mainly includes: block number, the hash value of the previous chunk header, a random number and difficulty target to prove the difficulty of the workload, a timestamp, and a total hash merkle root used to validate the block trade. The block body mainly contains all the transaction information in the Block (ledger) as well as the Merkle root of all transaction information.

In a typical chunk data structure, the version number refers to the version of the current blockchain application; The hash value of the front chunk is the hash value that references the previous chunk in the blockchain; the Merkle root is the Merkle root hash value of the transaction data stored in the block body; the timestamp is the approximate time generated by the chunk The random number is a counter that is unique to the workload proof algorithm in the bitcoin system. Among them, Merkle root is an important guarantee for the block chain to realize tamper-proof and data traceability, the Merkle tree is a binary tree, Figure 1 is a merkle tree containing 4 transaction data, it can be seen that as long as a transaction data is tampered with, according to the hash algorithm characteristics of the hash algorithm, [11] The value of the last Merkle root changes very significantly, and it is also possible to prove the existence of a transaction in the trading list based on Merkle root. At the same time, the Merkle root structure can also determine the specific location of the tampered transaction data by validating the hash value.

![Fig.1 Simple Merkle tree](image)

2.2 Cryptography in Block chain
Blockchain is a kind of technology to protect data security based on cryptography principle and encryption algorithm, and the importance of cryptography principle and encryption algorithm to
blockchain is self-evident. For all blockchain applications, the most basic cryptographic principles and
cryptography algorithms are asymmetric encryption algorithms and hash algorithms.

The hash algorithm belongs to one of the three types of cryptography algorithms[12], or is called
"cryptographic hash Algorithm" or "hash Algorithm", which can map any length of binary plaintext
string to a fixed-length binary string, and it is almost impossible for different plaintext to be mapped to
the same binary string[13]. The role of the hash algorithm is equivalent to giving the data a unique
"digital fingerprint", often referred to as a summary. Hash algorithms are often used to validate data
integrity, such as an arbitrary length of data, which is generated by the hash algorithm, that is. When
you need to verify that it is complete, assume that the summary is to be tested. If the proof data is
complete and correct, the reverse indicates that there has been a change in the data. The commonly
used hash algorithm has MD5 algorithm, SHA-1 algorithm, SHA-256 algorithm, etc., China's national
cryptographic administration has also proposed the national commercial cryptographic hash Algorithm
SM3 algorithm. Wangxiaoyun and others analyzed the SM3 algorithm, proving that its performance is
superior to other hash algorithms under some conditions[14].

2.3 Data synchronization in Blockchain

The essence of blockchain is a distributed data storage system based on P2P network, each of which
holds a common maintenance ledger. The central issue in distributed storage is how to maintain the
synchronization of data between nodes in the network, while also tolerating some of the errors that
exist in the network. In blockchain, it is the consensus algorithm that ensures data synchronization.
The common consensus algorithms in blockchain are POW, PoS, DPoS, pbft and so on[15], and the
purpose of the consensus algorithm is to satisfy the consistency of distributed storage system in the
event of errors in some nodes.

3. Design of aerial missile data secure storage system based on blockchain

3.1 Workflow of aeronautical missile data secure storage System

Take a node in each node cluster in the network as an example, and the workflow is shown in Figure 2,
where the numbers represent the order in which the execution process is performed.

Before the system works, the CA node first issues a digital certificate for members of the system,
indicating membership. The consensus node needs to generate the private key based on the certificate
issued by the CA node, use the random number generation algorithm specified in the certificate, and
then generate the public key according to it, and finally pass it to the sort node to verify the digital
signature.

The following is a process and principle analysis:

Process ① means that after the operator completes the data record, the data and hash values that
need to be stored are submitted to the record node in the network, and the process is expressed as:

\[
\text{Client} \rightarrow \text{Any A} : Data = data_0 \parallel Hash(data_0) \]

Clients can make a separate computer, or it can be a client interface installed on a record node. The
role of the client is to provide the operator with a human-computer interface. This process simply
transmits the data to the record node and makes an operational request.

Process ② is the record node to stamp the data timestamp, use the hash algorithm to generate a
summary, and then use the private key encryption to record the digital signature of the node, submit to
the sort node, sort the node to verify the certificate of the record node, determine whether the data source is a legitimate member of the network, the process is expressed as:

\[ A \rightarrow B : \]
\[ Data = Data_s || Cert(A) || PRK_s(Hash(data_s || Ts)) , \]
which
\[ Data_s = data_s || Ts || Hash(data_s) \]

If the digital certificate validates through, executes the process \( \circ \) and \( \circ \), the sorting node broadcasts the data to all consensus nodes, and the consensus node audits the data according to the consensus algorithm and validates the signature. If both the audit results and the validation results are passed, the data digest uses the private key encryption to digitally sign the consensus node, and the process is expressed as:

\[ B \rightarrow All C : \]
\[ Data = Data_s || Cert(A) || PRK_s(Hash(data_s || Ts)) \]
if \( Hash(data_s) = PUK_s(PKR_s(Hash(data_s))) \)
\[ Every \ C \rightarrow B : \]
\[ Data = Data_s || Cert(B) || PRK_s(Hash(Data_s)) \]
Which
\[ Data_s = data_s || Ts || Hash(Data_s) \]

When the process \( \circ \) is executed, the sorting node receives the data sent by the consensus node, validates the validity of the digital signature of the consensus node, and determines whether the number of valid signatures satisfies the number of valid digital signatures required in the consensus algorithm. If satisfied, the data is packaged into chunks and broadcast to the entire network, and the entire network node receives the chunk and stores it in its own memory, the process is expressed as:

\[ if \ Hash(Data_s) = PUK_s(PKR_s(Hash(Data_s))) \]
\[ if \ n \geq N \]
\[ B \rightarrow All A and C : \]
\[ Data = data_s || Ts || Hash(data_s) \]

The data broadcast by the sort node contains the basic data items in the chunk data structure: The data that was originally entered, the timestamp that was stamped when the input data was submitted, and the summary generated based on the hash algorithm, used to generate the Merkle root structure and act as the hash value of the front chunk in the next chunk.

4. Security Analysis

4.1 Personnel identity Authentication
In the system design, the CA node is introduced, the digital certificate in X.509 format is introduced, and only the user has the digital certificate, which is judged as a trusted node by the system. You can set different kinds of digital certificates to identify identities, distinguish between record nodes, consensus nodes, and sort nodes. Users who do not have a digital certificate are not eligible to join the system, the record node cannot participate in the digital signature of the consensus node, and the distribution of the key for each node is achieved by issuing a digital certificate. At the same time, the user’s operation can be limited by digital certificate to realize the control of data visibility and maneuverability.

4.2 Data transmission security
In the data storage process, it needs to be transmitted multiple times across nodes through the P2P network, although the security of the P2P network is higher than that of the exposed network, but there
is also the risk that the external attack data will be tampered with. Two digital signatures, digital signature verification and multiple hash value calculations are used in the system, and the following five data transfer processes described above are analyzed separately: If the data is tampered with in the process ①, the recording node will find that the data does not match its hash value after the process ① is completed, and the decision data is invalid, if in the process ②, The data in ③ and ④ is tampered with, and when signing authentication, the signature authentication fails due to a change in the hash value of the signature, which invalidates the decision data, and when the data is tampered with in the process ⑤, it also causes the hash value to change, and when the hash value acts as the hash value of the front block in the next chunk, Can cause chunk data to be out of sync between nodes, the system will invalidate the front block where the error occurred and resynchronize the data.

4.3 Data storage Security
Malicious tampering with data after storage is complete, if the tampered block is in the middle of the blockchain, it causes the hash value to change, causing the front block hash value of the next chunk to match the chunk hash value, causing the blockchain to break, and the data will be resynchronized when the next new chunk joins; If the tampered block is at the end of the blockchain, the data is discovered and resynchronized when the next new chunk is added.

5. Conclusion
The air missile business data volume is large, the data item is many, the importance is high, realizes the digital distributed storage when the inevitable requirement. The distributed storage, data tamper-proof and traceability of blockchain technology enable it to solve many aviation missile business data records, storage security problems and hidden dangers. In this paper, the aviation missile business data security storage system, using typical block data structure, encryption algorithm and a variety of security measures to apply blockchain technology to aviation missile business data recording, storage scene. Security analysis shows that the system designed in this paper can meet the requirements of data security storage in terms of personnel role management, data security and authenticity, and has a certain application prospect in the military application of blockchain.

References
[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL].[2019-3-5]. https://bitcoin.org/bitcoin.pdf.
[2] Yuan Y, Wang F.Y. Blockchain:The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016(04):481-494.
[3] Zhou J, Li W J. Research on logistics blockchain consensus algorithm based on cloud computing[J]. Computer Engineering and Applications, 2018, 54(19):237-242.
[4] Ekblaw A, Azaria A, Halamka J.D., et al. A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data.[C]/Proceedings of the 2016 IEEE of International Conference on Open and Big Data, 2016. 25-30
[5] Dong G S, Chen Y X, Zhang Z L, et al. Research on Identity Management Authentication Based on Blockchain[J]. Computer Science, 2018(11):52-59.
[6] Qi X.C., Zhu Y.C., Shao Q.F., et al. A Warehouse Receipt Management System Based on Blockchain Technology[J]. Journal of East China Normal University(Natural Science), 2018(05):144-153.
[7] Sun Y, Lei Z, Zhan G.Y. Security of Military Data Based on Blockchain[J]. Journal of Command and Control, 2018(09):189-194.
[8] Zhao J.Z., Deng J.Q. Research on Management of Aviation Missile[J]. Plant Maintenance Engineering, 2016(10)40-42.
[9] Wang J.Y., Gao L.C., Dong A.Q., et al. Blockchain Based Data Security Sharing Network Architecture Research[J]. Journal of Computer Research and Development, 2017(04):742-749.
[10] Cai W.D., Yu L, Wang R, et al. Blockchain Application Development Techniques[J]. Journal of Software, 2017(06):1474-1487.
[11] Thomas C.G., Jose R.T. A Comparative Study on Different Hashing Algorithms[J]. International Journal of Innovative Research in Computer and Communication Engineering, 2015(07):4492-4495.
[12] Wang H.Q., Wu T. Cryptography on the Blockchain[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition), 2017(06):61-67.
[13] Wang X.Y., Yu H.B. SM3 Cryptographic Hash Algorithm[J]. Journal of Information Security Research, 2016(11):983-994.
[14] Boneh D, Boyen X. Efficient Selective Identity-based Encryption without Random Oracles[J]. Journal of Cryptology, 2011(04):659-693.
[15] Song T.Y., Zhao Z.L. Comparison of Blockchain Consensus Algorithm[J]. Computer Applications and Software, 2018(08):1-8.