Xiu C. (2024) BLOCKCHAIN-BASED ATHLETE HEALTH ARCHIVES DATA SHARING FROM THE PERSPECTIVE OF PUBLIC HEALTH. Revista Internacional de Medicina y Ciencias de la Actividad Física y el Deporte vol. 24 (95) pp. 336-352.
DOI: https://doi.org/10.15366/rimcafd2024.95.021

ORIGINAL

BLOCKCHAIN-BASED ATHLETE HEALTH ARCHIVES DATA SHARING FROM THE PERSPECTIVE OF PUBLIC HEALTH

Chen Xiu [1,2]

[1] Philosophy School, Zhejiang University, 310058, Hangzhou, China
[2] Zhejiang Urban Governance Research Center of Hangzhou International Urbanism Research Center, New key professional think tank in Zhejiang Province, Zhejiang, China
E-mail: 805585600@qq.com

Recibido 18 de Junio de 2023 **Received** June 18, 2023
Aceptado 18 de Febrero de 2024 **Accepted** February 18, 2024

ABSTRACT

Managing athlete health archives data from the perspective of public health is essential for disease surveillance, outbreak response, evidence-based interventions, policy development, and collaborative efforts. By leveraging this data effectively, public health organizations can enhance their ability to monitor and protect the health of athletes, as well as the broader population. It is particularly important to monitor and share exercise status and human health data to prevent sports injuries caused by improper exercise during exercise. Therefore, this article proposes a storage and sharing model for athletes' health Archive data based on blockchain distributed decision-making to achieve safe storage and sharing of athletes' health data. First, the design goals and requirements of the distributed decision-making authentication system are clarified. Build DID data structure and athlete health Archive data management based on blockchain and DID technical standards. Utilize the characteristics of blockchain data such as traceability, non-tamperability, openness and transparency to solve the problem of mutual trust in athlete identity authentication systems. The overall architecture of the blockchain-based distributed athlete health Archive authentication system and the design of each functional module of the identity authentication system were also designed, including identity registration, verification, authorization, etc. The unique identity identifier is used as the athlete's identity, the public and private keys are used for signature and verification, and the Merkel tree is used to record and verify the athlete's data records. Based on the blockchain platform, the smart contract security execution process is used to store athlete identity information on the

blockchain, ensuring that access records are traceable and tamper-proof.

KEYWORDS: Public Health; Data Sharing; Blockchain; Athlete Health Archives

1. INTRODUCTION

From the perspective of public health, blockchain-based research on athletes' health file data sharing is of great necessity. Athletes are subjected to tremendous physical and mental stress during competition, and their health is crucial to their personal and professional development (Bhattacharya, Singh, & Hossain, 2019; Gul, Subramanian, Paul, & Kim, 2021). By establishing a safe, transparent and trusted data sharing platform, public health agencies can better understand the health status of athletes, provide personalized health advice, and prevent and control potential health risks in a timely manner. First, blockchain-based data sharing of athletes' health profiles can improve data security and privacy protection. Blockchain technology, with its characteristics of decentralization, distribution and encryption (Velmovitsky, Bublitz, Fadrique, & Morita, 2021), ensures the security and integrity of data. Athletes' health data can be stored on a blockchain in encrypted form with access control through smart contracts, and only authorized public health authorities can access the relevant data. In this way, the privacy of athletes will be effectively protected, while public health agencies can obtain the necessary health information without violating privacy regulations. Second, by sharing data from athletes' health records, public health agencies can get a more complete picture of athletes' health (Attaran, 2022).

An athlete's health data includes information such as physical exam results, injury history, mental health evaluations, and more, which is critical to assessing an athlete's overall health status. Public health agencies can use this data to conduct comprehensive analysis to understand the potential health risks and specific needs of athletes, so as to provide personalized health advice and guidance (Mann, Clift, Boykoff, & Bekker, 2020; Randall, Goel, & Abujamra, 2017). For example, in response to a specific health problem of an athlete, the public health agency can recommend appropriate preventive measures or rehabilitation programs to help the athlete maintain physical and mental health. Finally, blockchain-based data sharing of athletes' health profiles helps prevent and control potential health risks in a timely manner. Public health agencies can detect abnormalities in time and take appropriate measures by monitoring athletes' health data. For example, if an athlete's physical indicators show abnormal changes, public health agencies can intervene in time to provide the necessary treatment or advice to prevent further development of the disease. In addition, public health agencies can use the shared health data for disease prediction and epidemiological surveillance, and take timely public health measures to protect the health and safety of athletes and the sports community at large (Patel, Fidrocki, & Parachuri, 2017).

Matching athlete health data and identity is one of the most basic and important conditions in medical testing and treatment. During the process of medical testing and treatment, if there is an error in matching athlete health data with athlete identity, it will have serious consequences for the athlete himself, and even It will pose a threat to the lives of athletes. At the same time, athletes' personal health data needs to be protected from malicious tampering during medical testing and treatment, otherwise it will cause doctors or nursing staff to make wrong judgments, leading to wrong treatment and diagnosis of athletes (Glick & Horsfall, 2005). Moreover, athletes' personal health data is closely related to their personal privacy, which will contain a lot of highly sensitive basic personal information, such as name, phone number, age, personal health status, etc. The laws of many countries clearly stipulate that the use of athletes' personal health data requires strict attention to patient privacy protection and information security.

Previously, athletes' personal health data mainly adopted the traditional centralised storage model, where each medical institution stores athletes' personal health data centrally in the local data storage repository, which not only increases the risk of the database being subject to a single point of attack, resulting in the possibility of the privacy of the health data being leaked, tampered with, or even damaged beyond recovery, but also makes the centralised storage of the data a difficult problem to be solved, and the convenience of data sharing no longer exists. The convenience of data sharing no longer exists. In recent years, with the rapid development of cloud storage technology, healthcare organisations have gradually shifted their data storage mode from local storage to cloud storage, which has the benefit of giving athletes complete control over their personal health data, and by setting up access rights to the cloud, only authorised users are able to access the specified stored data; however, the cloud storage method has its drawbacks as well. Cloud servers are subject to more cyber-attacks than local databases, and data users can lose control of their personal data due to certain malicious behaviours on the cloud servers, so how to ensure cloud security is one of the primary concerns in cloud storage scenarios for personal health data (Gupta, Verma, & Pawar, 2023; Thilakanathan, Chen, Nepal, Calvo, & Alem, 2014). This paper mainly studies the problems related to blockchain identity authentication and constructs a distributed identity authentication system based on blockchain. By analysing the deficiencies of the current blockchain identity authentication platform, the objectives of the system design are proposed. We analyse the requirements in terms of performance and functionality, and propose a decentralized identity structure and management model suitable for blockchain systems in combination with distributed identity technology standards. The main innovations and contributions of this paper are as follows:

(1) This paper proposes a novel identity data structure and management model. Identity data is divided into two types for discussion and analysis, and

different management schemes are designed. Optimisation and modifications are made to the traditional DID data structure. The data management scheme combines the characteristics of blockchain, and both on-chain and off-chain data records are traceable to ensure data consistency. The Json Web Signature design ensures trusted interaction between users and secure data sharing.

(2) According to the functional requirements of the system, the DID registration, update, authorisation, selective disclosure and verification processes are designed, and specific implementation methods are given.

2. Methodology

With the development of blockchain technology, the use of blockchain technology in solving the problem of matching athletes' health data with athletes' identity authentication is gradually emerging, which provides new ideas for solving the problem of matching athletes' data with athletes' identity authentication. When athletes go to hospitals for medical treatment, they face the situation that doctors make mistakes in matching athletes' health data with athletes' identities; at the same time, if the traditional biometric identification authentication scheme is used for identity authentication, it is necessary to transmit biometric templates, and due to the uniqueness and privacy of the biometric templates, transmitting the biometric templates directly over the network will make the biometric templates easy to be leaked; as well as the athletes' use of the As well as patients using smart cards to extract athletes' health data, there is also the risk of losing the smart card, which makes it impossible to extract athletes' health data in real time and may lead to the leakage of athletes' health privacy. Therefore, an athlete health data identity authentication matching scheme based on blockchain is proposed, and the core content of this scheme is the design of smart contracts. Based on blockchain technology, this scheme takes human biometric characteristics as one of the conditions for identity authentication matching, and conducts the authentication matching between athlete health data and athlete identity authentication by invoking the designed smart contracts, so as to ensure that the athlete health data is accurately matched with the athlete himself or herself, and to avoid the risk of the loss of health data due to the loss of smart cards.

2.1 Blockchain

2.1.1 Structure of the blockchain

The athlete sends a pending transaction to the blockchain network via the client, the transaction needs to be confirmed by multiple nodes before it is deemed legitimate, the blockchain network receives the pending transaction and broadcasts it to the other nodes in the network waiting for the nodes to process it. After the node releases a new block, the verified transaction will be added to the new block. A block consists of two parts: the block header and the

block body. The block header contains the metadata of the block. The block body contains the list of specific transactions. A node can verify the legitimacy of the transactions in the block at any time. If the block contains illegal or invalid transactions, the node will reject the block. Table 1 shows the specific data structure of the block header.

Table1: Data structure of the block.

NAME	DESCRIPTIONS
VERSION	Current version of the blockchain
HEIGHT	Number of blocks released on the blockchain
PREHASH	The hash of the previous block
BLOCKHASH	The hash value of the current block
TIMESTAMP	Time element of block generation
BLOCKSIZE	Size of the block
NONCE	Difficulty
ROOTHASH	Verify the integrity of the transaction

The overall architecture of the blockchain is divided into six layers, namely application layer, contract layer, incentive layer, consensus layer, network layer, and data layer. The application layer covers specific upper-layer business requirements, and blockchain-based scenarios and functions are expressed in specific applications. For example, digital currency, archive management and supply chain management, etc. The contract layer contains smart contracts deployed on the chain. Smart contracts are groups of codes that can be executed automatically. Smart contracts deployed on the blockchain have the characteristics of being tamper-proof and transparent. Users call smart contracts to read and verify data on the blockchain, and can even work together on and off the chain. Replacing manual execution with automated procedures not only saves labor costs but also enhances data credibility. The incentive layer provides a reward and punishment mechanism to encourage and stimulate nodes to participate in blockchain transaction processing to ensure the safe and stable operation of the entire network. Nodes obtain certain rewards through accounting.

There are two main ways of rewards: one is to publish new blocks, and the other is to commission from transaction fees. The consensus layer is responsible for the transaction sequence and transaction content consistency of all transactions in the blockchain network. The mainstream consensus algorithms in the blockchain include proof of work, proof of equity, and delegated proof of equity. The network layer is the basis for data interaction between nodes in the network. The blockchain network is built on a peer-to-peer network, and each node is connected in pairs and can communicate directly. Data is quickly broadcast in the network to every node in the network according to the propagation protocol. Even if some channels in the network

are damaged, data transmission will not be seriously affected. The data layer stores data in blocks, and each node saves all transaction data in the network. The data layer solves how to store and manage data in the network, including block headers, block bodies, transaction numbers, transaction integrity, etc.

2.1.2 Smart contract

Traditional two-party interaction models often rely on a trusted third party to enable mutual trust between the two data interacting parties. With the involvement of a trusted third party, the sender sends the correct transaction quantity and type of goods to the receiver. In most day-to-day scenarios, intermediaries can solve the trust problem between the two parties of a transaction, but centralised trust mechanisms are not irreplaceable. In blockchain systems, blockchain replaces the function of intermediaries to build new trust mechanisms. It is possible to solve the problem of mutual trust between the two parties to a transaction and reach a consensus on the transaction without relying on a trusted third party in the blockchain. Smart contract is a kind of computing programme. It's more implemented by means of code according to predefined rules that express the terms of agreement between participants.

Smart contracts deployed on the blockchain automatically enforce the terms of the agreement and do not require an intermediary to oversee and manage them. Deployment and execution of smart contracts is done by nodes in the network. According to Nick Szabo's theory, contract participants can evaluate the operational status of the protocol and check whether the contract is fulfilled or violated. Smart contracts also need to protect the privacy of the participants. At that time, there was no decentralised trust institution, so smart contracts were just an abstract concept. But with the development of blockchain, the theory of smart contracts was put into practice. Smart contracts are used in the field of computer encoding and replication of real-world contractual agreements. The basic principle of a contract is to create a legal agreement between two or more parties who must fulfil their contractual obligations. legal agreement between two or more parties who must fulfil their contractual obligations. Smart contracts can replace trusted third parties in traditional trust models.

Smart contracts can replace the trusted third party in traditional trust models by automating the execution of procedures in the blockchain network, featuring no intermediary fees, the trust of the participants and the fulfilment of their obligations. The characteristics of smart contracts are that they do not require intermediary fees, are trusted by the participants, and meet the needs of both parties. In addition to Bitcoin and Ether, there are evolving blockchain systems that are either derived from or independent of the original Bitcoin. In addition to Bitcoin and Ether, there are evolving blockchain systems that are

either derived from or independent of the original Bitcoin network and that offer innovative solutions to the different challenges it encounters.

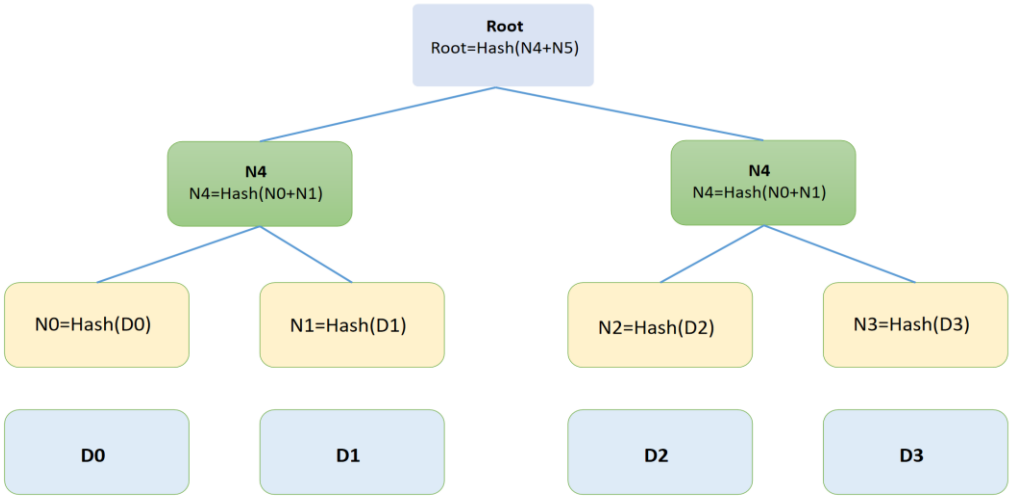

Figure 1: Structural diagram of Merkle tree.

2.1.3 Merkle Tree

In a peer-to-peer network, nodes in the network may synchronize data from the ledgers of multiple other nodes. If part of the synchronized files is damaged, the entire file needs to be resynchronized, which will cause a waste of computing resources. So a better way is to split the large file into smaller pieces. If the synchronized files are damaged, you only need to re-download the damaged parts to improve data synchronization efficiency. But how to confirm which specific data block has a problem? This problem can be solved by using Merkel tree. Before synchronizing the ledger, number all small data blocks so that a management list of data blocks to be synchronized can be obtained. The numbers in the list correspond to the contents in the data block. The hash algorithm will be used to achieve a verifiable one-to-one mapping relationship between the data block number and the data block content. The hash algorithm can convert data of any length into a fixed-length function, and the mapping is one-way, that is, the known data can be calculated to get the correct hash value, but the known hash value cannot be calculated and the correct hash value can be obtained by inversion. data. The content in the data block is hashed to obtain a fixed-length output, and hash collisions will not occur (different content is input but the same hash value is output). Each small data block is used as a leaf, and the Merkle tree is constructed from bottom to top through hash functions. Merkel tree contains a root node, several parent nodes and leaf nodes, as shown in Figure 1.

The leaf nodes in Figure 1 store specific data as the hash value of the transaction. n0, N1, N2 and N3 are the leaf nodes. n4 is the father node of N0 and N1, and N5 is the father node of N2 and N3. the data stored in N4 is the

hash function operation of the data of N0 and N1. n5 is the hash value after the hash function operation of the hash value of N2 and N3, and so on. And so on, the data stored in the root node is the hash value of the hash value stored in N4 and N5 after the hash function operation. As the hash value of the root node is calculated by the hash value stored in each leaf node layer by layer, so the leaf node storage value changes, then its hash path to the root node hash value of all nodes will be affected. Then the verifier can confirm whether the two Merkel trees are consistent by verifying whether the root hash value is consistent, as shown in Figure 2.

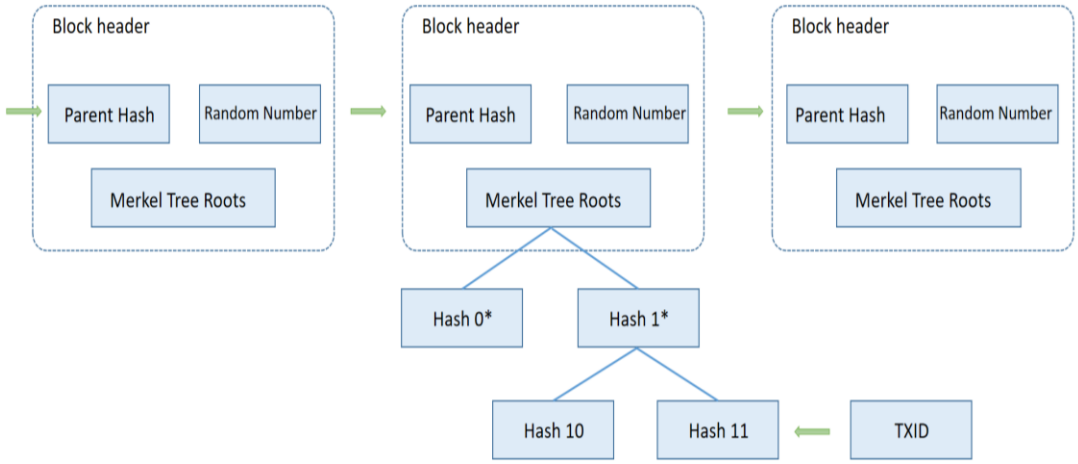

Figure 2: Schematic diagram of the process of blockchain verification of transactions.

2.2 Athlete Health Archives Data Management from Perspective of Public Health

Effective public health policies require a comprehensive understanding of population health. Athlete health archives data provides valuable information about the health status, prevalent injuries, and other health-related factors among athletes. This data can inform the development of policies and guidelines related to sports safety, injury prevention, and athlete welfare. By integrating athlete health data into public health policy-making processes, authorities can implement measures that protect athletes' health while promoting physical activity and sports participation.

2.2.1 ShoCard

ShoCard attaches a timestamp to the athlete's signed, encrypted identity information and integrates the information with hashed encryption. These hash-encrypted hashes are stored in a new block on the blockchain network. ShoCard sets up a central server that coordinates the interaction of encrypted identities between users and relying parties. The ShoCard decentralised authentication scheme has three phases: creation, authentication and verification. In the authentication phase, the relying party needs to verify the

user's credentials to determine whether the user is entitled to access. The user first provides the relying party with a reference to the encrypted certificate as well as the encryption key. As shown in Figure 3, Shocard uses a centralised server to manage the distribution of encrypted certificates between ShoCard users and. ShoCard has less risk of data leakage than schemes that store and distribute plaintext identity data. Users autonomously control the secure storage of identity data and the sharing of data with relying parties. However, ShoCard's role as an intermediary creates uncertainty about the stability of ShoCardID. If the centralised server does not exist and the intermediary role disappears, then ShoCard users will not be able to authenticate their identity in the system. This makes ShoCard more centralised in practice than other public schemes that rely on DLT.

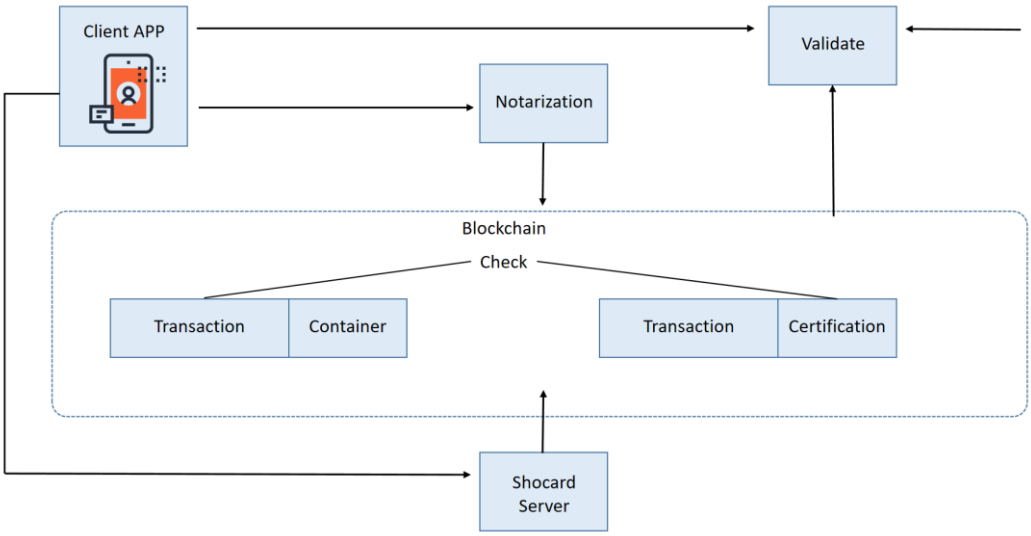

Figure 3: Schematic diagram of ShoCard architecture.

2.2.2 uPort

uPort identity credentials interact with information through smart contracts in Ethernet. Smart contracts can be uniquely addressed by 160-bit hexadecimal identifiers and can be invoked for execution in the virtual machine of each Ethernet node. uPort has designed two smart contract templates for identities, a controller and an agent. As shown in Figure 4, to create a new identity, the user creates a new asymmetric encrypted public-private key pair using the uPort application and then sends a new transaction to the Ethernet network. This transaction creates a controller, which contains a reference to the controller's public key. The user then creates a new proxy that contains a reference to the controller's contract address. uPort schemes do not have a centralised service provider and do not verify the identity holder of the uPortID. Therefore, uPort may allow some unauthorised risky devices to access the authentication methods on the user's mobile device. Because of the lack of intrinsic connectivity between uPorts, uPort does not require disclosure of

personal data to direct the uPortID for data interaction. uPortID for data interaction. However, the registry can collect information about identifiers and identity data. So while specific data in the attribute data structure can perform attribute-based searchable encryption, the overall Json data structure remains visible.

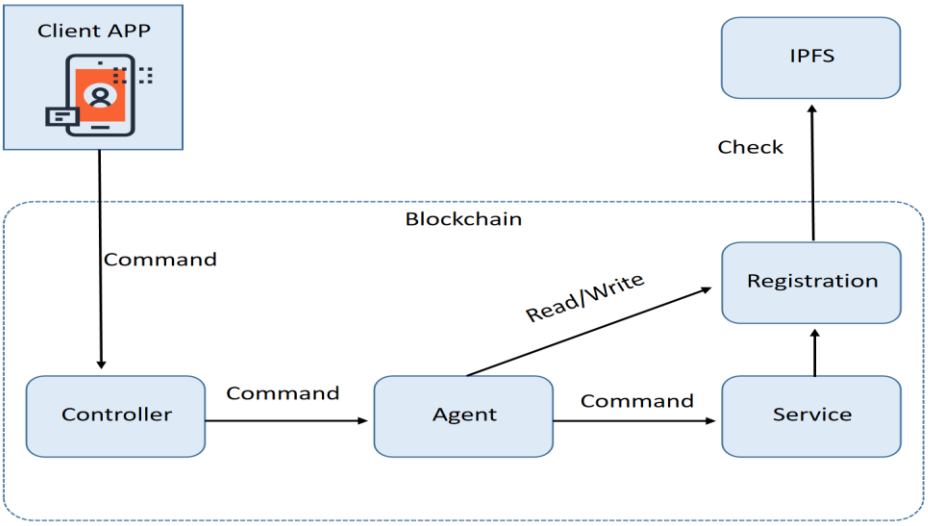

Figure 4: Schematic diagram of the uPort architecture.

2.2.3 Sorvin

Sorvin is a decentralised open source identity network based on licensed DLT. In the Sovrin identity network, users can generate the right amount of identifiers according to their needs, and these identifiers ensure that the user's identity privacy information is segmented to provide privacy and security protection. Each identifier is independent and managed by a different public-private key pair. The Sorvin architecture is detailed in Figure 5.It is divided into three main parts, the upper application layer, the data layer and the Sorvin ledger. It contains transactions associated with specific identifiers will be written, read, distributed and replicated between the management nodes. The data consistency of these nodes is guaranteed through a consensus protocol. The design of a permissioned ledger in Sorvin has two advantages.

First, the whole system does not need to calculate the proof of work to achieve consistency among ledgers, which reduces the computational cost of computing nodes and improves the transaction throughput of the whole system. Second, Sorvin's trust mechanism is code-dependent. A globally unified ledger will form a common root of trust, and the common root of trust is used to build the basic trust system. If other new organisations or individuals participate in the network, the new members in the network can become trust anchors (trust anchors are the anchors to which other new members can be added), and trust anchors rely on the common root of trust. By trust anchors relying on the common root of trust and new members relying on trust anchors, a network of

trust is developed layer by layer, ultimately achieving global trust.

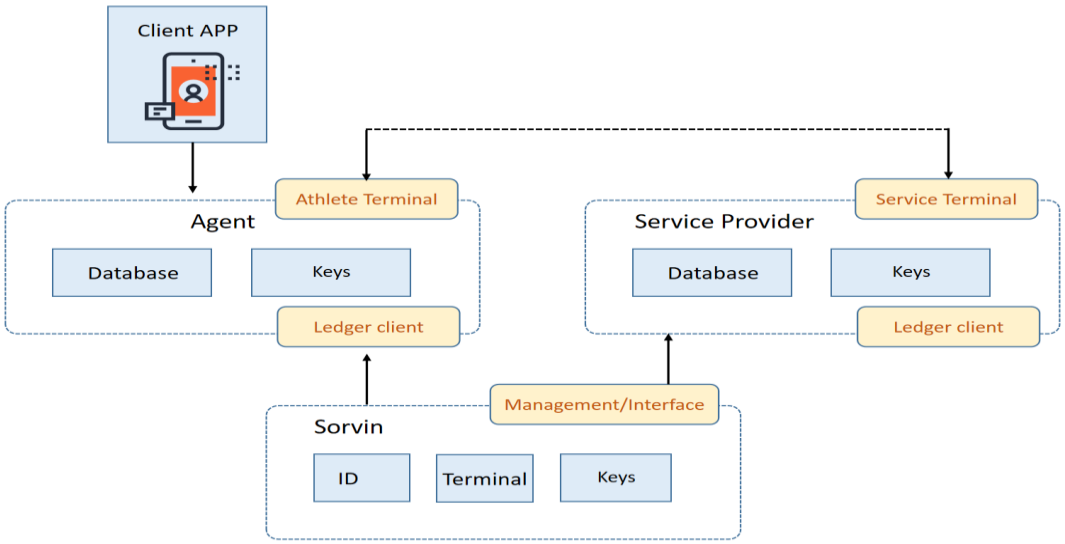

Figure 5: Schematic diagram of the Sorvin architecture.

2.3 Archive Verification

The process of registering personal data information for telemobilisation starts with the registration conducted by the hospital department. As shown in Algorithm 1, it is imperative for the hospital department to get essential personal identity details of persons who have been mobilized. These details include their identification number, name, age, gender, and other pertinent information. Once the fundamental identification information has been gathered, it becomes imperative to associate the health data of mobilized persons with their corresponding basic identity information.

This combined dataset should then be stored inside the IPFS distributed system, and the resulting data ID provided by the IPFS should be stored locally. The locally stored data ID supplied by IPFS is then used to gather the biometric features of the mobilisers in order to get random_R. Both the dataID and random_R are then saved appropriately. Once the smart contract template has been generated, the hospital department proceeds to fill the template with the necessary information and then transfers it to the Ethernet blockchain system.

Algorithm 1

REGISTRATION OF ATHLETE HEALTH DATA
function Register (Data, Info ID, Finger print, Contract Function, Department Account):
ID = Store Data(Data)
dataID = Transform Data (ID, Info ID)
random_R = Collect Data (Fingerprint)
contract Addr = Deploy (Contruct Function, data ID, random_R, Department Account)
end function

The process of deploying a smart contract is shown in Algorithm 2. The healthcare department utilizes an Ethereum account for the purpose of deploying smart contracts. Once the smart contract is deployed, the medical department will be prohibited from collecting or altering personal information of athletes. This includes fundamental identifying details, personal health data, and other information like the IPFS ID associated with the athletes.

Algorithm 2

CONTRACT DEPLOYMENT
function Deploy (Construct File, Department Account, data ID, random_R):
contract Data = open(Construct File)
contract = (contract Data['abi'], contract Data['bytecode'])
tx Spending = contract (Depart Account, data ID, random_R). transaction (Depart Account, gas)
address = Receipt (tx Spending)
return address
end function

The process of athlete identification verification and data matching is outlined in Algorithm 3. The verification of the signature is conducted by the medical department or athlete to certify the deployment of the smart contract. Commence the process of data conversion by inputting the data ID that has been previously gathered, after confirmation. In the event that the recently acquired hash value of dataID is found to be identical to the previous hash value hash_d, the random_R data conversion procedure will be executed.

If the newly acquired hash value, random_R, is equivalent to the previous hash value, hash_r, the data located at the provided data ID will be retrieved. Currently, the verification process of the athlete's identification has been completed, and the appropriate personal health data pertaining to the athlete's identity has been acquired. If any of the aforementioned processes proves unsuccessful, the process of identity matching verification and the subsequent acquisition of relevant data will not be accomplished.

Algorithm 3(a)

AUTHENTICATION AND DATA MATCHING
Iuput：New Hash_d，New Hash_r
Output：Data
function Match (address, data ID,New random_R, Match Account):
Data = IPFS.get File (data ID)
Department = Obtain Department (address, Department Account)
if Department == Department address
then
Old Hash_d = Access (address, 'retrieve', Match Account)

Algorithm 3(b)

New Hash_d = Transform Data (data ID)
If Old Hash_d == New Hash_d and Department == true
then
Old Hash_r = Access (address, ‘random_R’, Match Account)
New Hash_r = Transform Data (New random_R)
if Old Hash_r == New Hash_r
Then
return Data
end if
end if
end if
end function

The procedure of accessing the smart contract is outlined in Algorithm 4. Initially, it is important to authenticate the address of the smart contract and ascertain its validity. In the event that the smart contract address is deemed authentic, the acquisition of the smart contract is facilitated, hence enabling the extraction of the verification data contained inside such smart contract.

Algorithm 4

CONTRACT ACCESS
function Obtain Department (Address, Match Account):
Correct Address = Verify Address (address)
contract = get Contract (Correct Address)
data ID = Call (contract, ’Obtain Department’, Match Account)
random_R = Call (contract, ’Obtain Department’, Match Account)
end function

3. Experiment and Results

3.1 Hardware Configuration

Table 2 describes the hardware test environment of this experiment. One CA node and three consensus nodes in the underlying blockchain platform are deployed on the service configured as follows.

Table 2: Hardware configuration information.

TYPE	**DESCRIPTION**
CPU	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
RAM	16GB
HARDDISK	4T

3.2 Software configuration

Table 3 is the software tool configuration table that this experiment relies on. The underlying blockchain platform uses RayBaaS, MySQL is used to store off-chain DID related information, Httpd-tools is used for interface stress testing, and all services and applications are deployed and installed through Docker.

Table 3: Software configuration information.

TYPE	DESCRIPTION
DOCKER	17.03.0
DOCKER-COMPOSE	1.17.0
JDK	1.8
HTTPD-TOOLS	2.4.53
MYSQL	5.6
RAYBAAS	1.17.1

3.3 Experimental results and analysis

As can be seen by comparing the computational overheads in Table 4, in terms of keyword index generation, the present scheme reduces the bilinear operation time compared to the literature (Zhang, Deng, Shu, Yang, & Zheng, 2018), and uses one less exponential operation of the group G1 compared to the literature (Do & Ng, 2017), which can be seen to improve the efficiency of keyword index generation.

In terms of search matching, this scheme applies one more bilinear mapping compared to the literature (Zhang et al., 2018), which leads to an increase in computational overhead, however, compared to the literature (Zhang et al., 2018), this scheme and the literature (Do & Ng, 2017) are able to effectively defend against the keyword guessing attack, avoiding the problem of privacy leakage due to the keyword guessing attack.

Compared with the literature (Zhang et al., 2018), (Do & Ng, 2017), although this scheme applies one more hash operation on biometric random strings, the computational overhead required for a single hash operation is very low, and the hash operation can effectively ensure the patient's right to control personal health data autonomously and the right to share information.

In summary, although the search algorithm and biometric hash operation of this scheme increase the computational overhead, this scheme greatly improves the security of the data sharing process, and also improves the efficiency of the keyword index generation, and the excellent computing power of the node server can also make the increase in computational overhead within an acceptable range, so this scheme has certain advantages.

Table 4: Comparative results for computational overhead.

METHOD	KEYWORD INDEX	TRAPDOOR GENERATION	SEARCH MATCH
LITERATURE (Zhang et al., 2018)	$2F_2 + P + h_1 + h_2$	$F_1 + h_1$	$P + h_2$
LITERATURE (Do & Ng, 2017)	$2F_2 + h_1 + N_2$	$2F_1 + N_1 + 4N_2$	$2F_2 + 2P + N_1$
OURS	$F_1 + h_1 + N_2$	$2F_1 + N_1 + P + h_1 + h_2$	$N_2 + 2P + h_2$

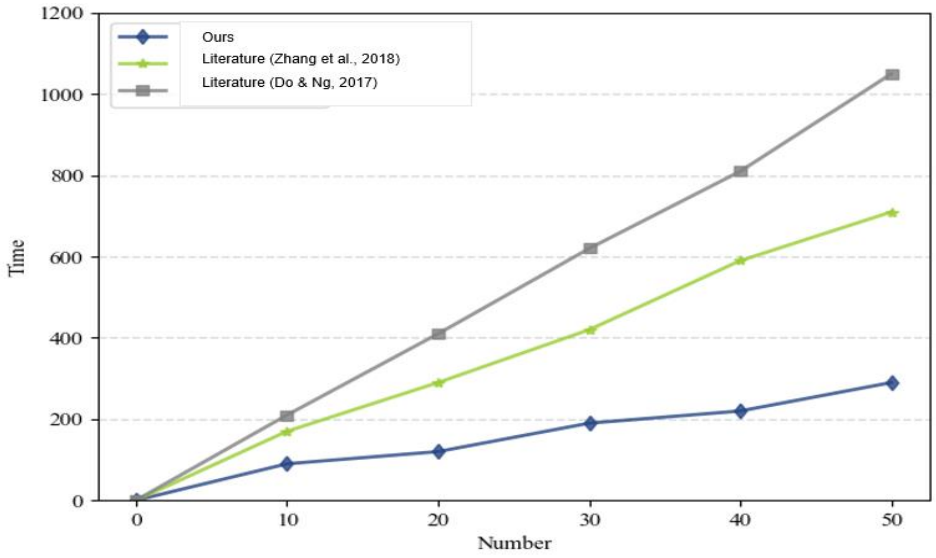

Figure 6: Schematic diagram of the Sorvin architecture.

Figure 6 shows the efficiency comparison between this scheme and the literature (Zhang et al., 2018), (Do & Ng, 2017) on search trap generation, the number of selected keywords is consistent with the number of generated keyword indexes, which is still 10, 20, 30, 40, 50. In Table 4, it can be clearly seen that, due to the fact that this scheme needs to carry out three different types of arithmetic operations when generating search traps, even though the complexity of generating search traps is higher, the gap in the generation of search traps is also shorter than the time in literature (Zhang et al., 2018), (Do & Ng, 2017); however, it can be calculated that the average time for generating a single search trap in this scheme is about 24ms, and when the data user initiates a share request for searching only one search trap is generated at a time, it can be assumed that the generation frequency of the search traps is low, and thus the execution efficiency of this scheme in generating search traps is superior, which is fully proved. the effectiveness of the proposed method.

4. Conclusion

Blockchain-based research on athletes' health file data sharing is very necessary for public health agencies. By establishing a safe, transparent and

trusted data sharing platform, public health agencies can better understand the health status of athletes, provide personalized health advice, and prevent and control potential health risks in a timely manner, thus safeguarding the health and professional development of athletes. In this paper, a model for the storage and sharing of athlete health Archive data based on blockchain distributed decision-making is proposed in order to accomplish the secure storage and exchange of athlete health data. Initially, the distributed decision-making authentication system's design objectives and requirements are defined.

The DID data structure and athlete health Archive data administration are based on DID and blockchain technology standards. The mutual trust problem of the athlete identity authentication system is resolved using the blockchain's data traceability, immutability, and openness and transparency. In addition, the overall architecture of the blockchain-based distributed athlete health Archive authentication system and the design of each functional module of the authentication system, such as identity registration, verification, authorization, etc., are designed. The unique identifier is used as the identity of the athlete, the public and private keys are used for signature and verification, and the Merkel tree is used to store and verify the athlete's data recordings. Based on the blockchain platform and utilizing the smart contract security execution process, the athlete identity information is stored on the blockchain, ensuring that the access records are transparent and tamper-resistant.

REFERENCES

Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management, 15*(1), 70-83.

Bhattacharya, S., Singh, A., & Hossain, M. M. (2019). Strengthening public health surveillance through blockchain technology. *AIMS public health, 6*(3), 326.

Do, H. G., & Ng, W. K. (2017). *Blockchain-based system for secure data storage with private keyword search.* Paper presented at the 2017 IEEE World Congress on Services (SERVICES).

Glick, I. D., & Horsfall, J. L. (2005). Diagnosis and psychiatric treatment of athletes. *Clinics in sports medicine, 24*(4), 771-781, vii.

Gul, M. J., Subramanian, B., Paul, A., & Kim, J. (2021). Blockchain for public health care in smart society. *Microprocessors and Microsystems, 80*, 103524.

Gupta, P., Verma, B., & Pawar, M. (2023). Internet of Everything-Based Advanced Big Data Journey for the Medical Industry. In *IoT in Healthcare Systems* (pp. 49-58): CRC Press.

Mann, R. H., Clift, B. C., Boykoff, J., & Bekker, S. (2020). Athletes as community; athletes in community: covid-19, sporting mega-events and athlete health protection. In (Vol. 54, pp. 1071-1072): BMJ Publishing Group Ltd

and British Association of Sport and Exercise Medicine.

Patel, D. R., Fidrocki, D., & Parachuri, V. (2017). Sport-related concussions in adolescent athletes: a critical public health problem for which prevention remains an elusive goal. *Translational Pediatrics, 6*(3), 114.

Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. *Journal of Health & Medical Informatics, 8*(3), 8-11.

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., & Alem, L. (2014). A platform for secure monitoring and sharing of generic health data in the Cloud. *Future Generation Computer Systems, 35*, 102-113.

Velmovitsky, P. E., Bublitz, F. M., Fadrique, L. X., & Morita, P. P. (2021). Blockchain applications in health care and public health: increased transparency. *JMIR medical informatics, 9*(6), e20713.

Zhang, Y., Deng, R. H., Shu, J., Yang, K., & Zheng, D. (2018). TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain. *IEEE Access, 6*, 31077-31087.