An overall architecture design of a hybrid blockchain technology that solves the separation of basic data and business data

Liu Feng*
Institute of Artificial Intelligence and Change Management /Shanghai University of International Business and Economics
Shanghai China
lsttoy@163.com

Li Ao Hua
Shanghai University of International Business and Economics
Shanghai China
leeduckgo@gmail.com

Wu Xuan Yong
Ernst & Young LLP
Shanghai China

Gao De Long
Shanghai University of International Business and Economics
Shanghai China
19921878685@163.com

Wang Ning Bo
WuXi Taihu University
Wuxi Jiangsu China
2536935847@qq.com

Xu Qing
Beijing University of Posts and Telecommunications
3467133430@qq.com

ABSTRACT

Starting from the characteristics of the blockchain, this paper creatively gives a underlying bi-chain design by taking advantage of the blockchain characteristics of Ethereum and BSN. In this paper, through the business design of the bi-chain interactive interface, through the implementation of the bi-chain coordination mechanism and consensus, to achieve functional coupling, module decoupling. And finally applied to personalized scenes. Provide the underlying service support for other subsequent Dapps.

CCS CONCEPTS

•Software and its engineering → Software creation and management →Designing software → Software design engineering •Computing methodologies → Distributed computing methodologies → Distributed programming languages

KEYWORDS

Bi-chain structure, Hybrid underlying blockchain, BSN, Architecture design, Digital identity system

1 Introduction

Nowadays, the upsurge of the blockchain has spread to all walks of life like a beast, gradually becoming one of the hottest and most concerned technologies in the Internet world. Compared with current popular information technologies such as big data, cloud computing, artificial intelligence, etc., the blockchain seems to be more in line with people's growing needs by virtue of decentralization, immutability, traceability, collective maintenance, openness and transparency [1] .Speaking of blockchain, everyone may think of Bitcoin in the beginning. Blockchain technology appears in the public eye with the birth of Bitcoin, which means that Bitcoin is a typical representative of blockchain 1.0 applications. The core underlying technology of Bitcoin is the blockchain, and many of its characteristics are derived from the blockchain. Because of this, Bitcoin has become the most successful blockchain application scenario to date.

In the era of blockchain 2.0, people have added the concept of "smart contracts" to the blockchain. With the icing on the cake of the blockchain, people have successfully used the support of smart contracts to push the blockchain technology to a wider range of applications, from a single currency business to four major financial services involving smart contract functions, banking, securities , Insurance and asset management [2].Not only that, the integration of blockchain technology with smart contract

technology can not only simplify complex processes and facilitate operation, make clearing more standardized and automated, but also minimize the possibility of errors. The development of blockchain to today has entered the era of blockchain 3.0. In addition to digital currencies, blockchain can play a great role in education, medical care, insurance, credit reporting and other fields. With the development of blockchain systems, different blockchain systems are adapted to different application scenarios. As shown in Sheet1 below, according to the consensus mechanism, blockchain can be divided into five types: private chain, closed alliance chain, read open alliance chain, write open alliance chain and public chain.

Sheet 1. Classification of blockchain types and related features

	Data base	Private Chain	Closed Alliance Chain	Open Alliance Chain		Public Chain
				Read Open Alliance Chain	Write Open Alliance Chain	
Read Permission	Interior	Interior	Alliance interior	Anybody	Anybody	Anybody
Write Permission	Interior	Interior	Alliance interior	Alliance interior	Anybody	Anybody
Proof of Data Not Tampered	No	Yes	Yes	Yes	Yes	Yes
Data Synchronization Permission (Building Slave Library)	Interior	Interior	Alliance interior	Anybody	Anybody	Anybody
Data Recording Permission	Interior	Interior	Alliance interior	Alliance interior	Alliance interior	Anybody (Competition)
Believablity	Trust a subject, difficult to verify	Trust a subject, users can verify their own data	Trust most in the alliance, users can verify their data	Trust most in the alliance, anybody can verify any data	Trust most in the alliance, anybody can verify any data	Based on trust algorithms and games

In the past, applications were based on a single blockchain system. As shown in Figure 1 below.

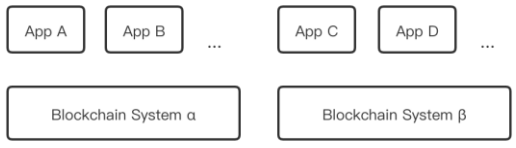

Figure 1. Traditional blockchain applications

As current blockchain applications become more complex, it is necessary to base an application on multiple blockchain systems and use different blockchain systems for different modules in the application in order to achieve high efficiency and decoupling. As shown in Figure 2 below.

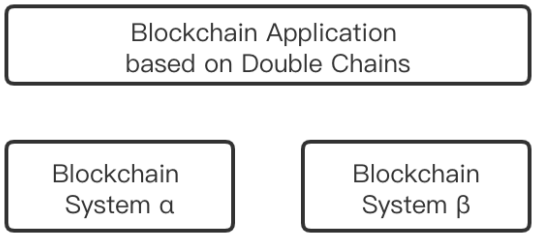

Figure 2. Double blockchain applications

2 Analysis of the development and current status of blockchain technology

2.1 Blockchain Technology

The concept of blockchain first appeared in " Bitcon: A Peer-to Peer Electronic Cash System" by Satoshi Nakamoto, which described: Blockchain is a data structure used to record the history of Bitcoin transaction accounts [3].From a technological perspective, blockchain involves many scientific and technological issues such as mathematics, cryptography, the Internet, and computer programming. From an application point of view, in simple terms, the blockchain is a distributed shared ledger and database, which is characterized by decentralization, immutability, leaving traces throughout, traceability, collective maintenance, openness ,transparency. These characteristics ensure the "honesty" and "transparency" of the blockchain and lay the foundation for the blockchain to create trust. The rich application scenarios of the blockchain are basically based on the ability of the blockchain to solve the problem of information asymmetry, and to achieve collaborative trust and concerted action among multiple subjects [1]. In simple terms, it means that blockchain technology is a master of cryptography, smart contract technology and other technologies. In a blockchain system, every time a certain period of time passes, the transaction data generated by each participant will be packaged into a block. Then, the blocks will be sorted in order according to time to form a chain of data blocks. Each node has the same data chain. After the data is written into the blockchain, it cannot be modified or deleted. Only one record can be added to indicate that the transaction is invalid. . This determines the openness and transparency of transactions [2], so as to achieve information sharing and consistent decision-making among multiple subjects, and to ensure that the identity of each subject and the transaction

information between subjects are immutable, open and transparent. The development of the blockchain to this day has produced a variety of blockchain applications, but whether it is Bitcoin, Ethereum or other applications, its basic blockchain system composition is shown in Figure 3.

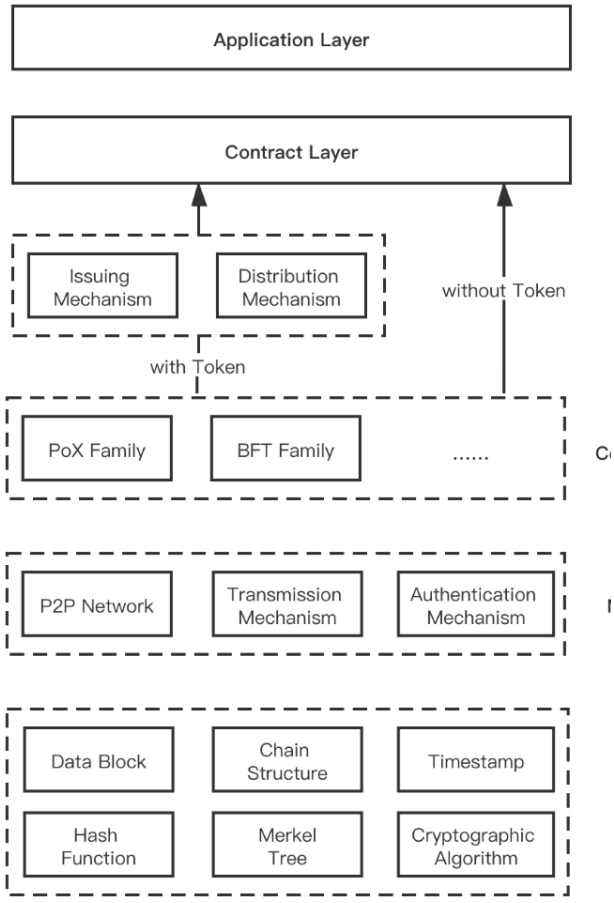

Figure 3. Six-tier architecture of blockchain system

.

2.2 Digital Identity

From the beginning of the birth of the Internet, only the IP address was found at the bottom of the Internet. There was no concept of accounts and identities. All accounts and identities were implemented based on the Internet application layer. The blockchain starts with Bitcoin, nodes and accounts are two different object models. We see that the earliest digital identity model on the Internet is the account model with password. This mode is simple and convenient, so it is still widely used today, and it is also adapted to the environment of the early development of the Internet. However, this traditional digital identity model not only requires everyone to remember and manage a large number of accounts, but digital identity is almost monopolized by several large-scale applications, such as Facebook, WeChat, etc., and then these applications began opening our own identity system, allowing other project parties to log in to their respective applications through traditional accounts, has formed what we now call the alliance identity model. Under this model, problems related to identity authorization and personal privacy are very easy to occur. Once there are problems with the company's security measures, the personal identity and privacy of countless people will be leaked out. Obviously, this model has shown huge limitations.

So we are seeing that the next generation of digital identities is moving in a more "free" direction. The management of digital identities has started to return to the main object, managed by itself, and no longer monopolized by the application side and the alliance side. On the other hand, the identities and identities of digital identities, which are what we call subject identifiers and subject attributes, begin to decouple [4]. The attributes of the subject form independent, verifiable credentials for a wider and controlled interaction of digital information. Then we see that the digital identity of the next generation must be distributed. From a local perspective, each of our identity certificates is issued by a centralized center; but from a global perspective, the identity of human society and the identity of the digital world are provided by countless centers. Therefore, centralization and decentralization are opposite and unified in the field of digital identity. In general, digital identities are distributed and have more flexibility and flatness. This is not only a true reflection of the real world, but also more in line with the needs of the development and governance of the digital world.

In this era of the Internet, only after the establishment of a distributed digital identity system can blockchain applications be connected to real-world applications, complete the relevant applications in the real world, and use the characteristics of blockchain technology to build a new and innovative application [5]. At present, WeChat and Alipay have become the actual entrance for Chinese people to enter the digital world. In the evolving new world of blockchain construction, we believe that distributed digital identities are the real entry point and that we adhere to open protocols. This entry point is no longer monopolized by a certain company or institution. Through this entrance, data can truly surround the owner and owner of the data, which is the controlled circulation and use of our personal subjects, and the value objects mapped on the blockchain can also be orderedly confirmed and transferred.

2.3 Blockchain-based Service Network(BSN)

Blockchain-based Service Network, a public infrastructure network based on alliance chain technology, provides public infrastructure network that has low-cost development, deployment, operation and maintenance, interoperability and supervision of alliance chain applications, and is committed to changing the high cost of LAN architecture of the current alliance chain. It provides developers with a public blockchain resource environment based on the Internet concept, which greatly reduces the development,

deployment, operation and maintenance, interoperability and supervision costs of blockchain applications, thereby enabling the rapid popularization and development of blockchain technology.
The blockchain service network consists of public city nodes and consensus sorting cluster services, which are developed, constructed, and operated by China UnionPay. Each city can establish one or more public city nodes, and all city nodes are connected through the Internet to form a blockchain service network with physical city nodes spreading across the country (future to global).

The publisher of a blockchain application only needs to deploy the application to multiple city nodes of the service network, and participants can access the city node gateway with almost no cost. Within each city node, all deployed applications share server resources.

On the service network, neither blockchain application publishers nor participants need to purchase physical servers or cloud services to build their own blockchain operating environment. Instead, they use the service network to provide unified public services and rent shared resources as needed , thereby greatly reducing costs for publishers and participants.

3 Reasons for the Application to Adopt a Bi-chain Architecture

From the perspective of engineering implementation, the bi-chain structure is equivalent to using a blockchain database, but now using two different types of blockchain databases. The reasons for adopting a double-stranded structure are as follows:

1）Different Consensus Mechanisms

Different blockchain systems are based on different consensus mechanisms, such as Raft, PBFT, PoW, PoS, and so on. Different consensus mechanisms determine the differences in the interaction between applications and blockchain systems. For example, when developing applications on a blockchain system based on the PoW mechanism, transactions require a certain number of confirmations to be finally confirmed, otherwise there is a risk of entering an orphan block. For PBFT-based blockchains, generally, no confirmation is required.

In our scenario, a blockchain system based on the A consensus mechanism may be used for various reasons, such as the need to support Bitcoin, or a blockchain system based on the B consensus mechanism may be required for other reasons, such as Digital identity. At this time, it is necessary to use the bi-chain mechanism.

2）Different Economic Models

In addition, different blockchain systems will use different economic models. For example, calling smart contracts on Ethereum consumes ETH as fuel (GAS); on some Fabric-based alliance chains, payment by calling services on the chain requires payment according to the requirements of the service provider. Different scenarios also fit different economic models.

3）Different TPS and Stability

TPS (Transactions Per Second) refers to the number of transactions per second that the server can process in the traditional computer field, and generally refers to the number of transactions per second in the blockchain field.

For different business scenarios, the required TPS is different. For example, it is generally believed that 7tx / s is sufficient for Bitcoin; 100tx / s is acceptable in some low-frequency scenarios; and higher tps is required for some higher-frequency scenarios.

Similarly, some blockchain networks can cause congestion at certain times for a variety of reasons. For some modules, these congestions are acceptable; for other modules, it is necessary to ensure the high stability of the blockchain network.

4）Different Blockchain Ecosystems

The application selects blockchain system , not only based on the blockchain system itself, but also taking into account the ecosystem built by the various applications on the blockchain system.

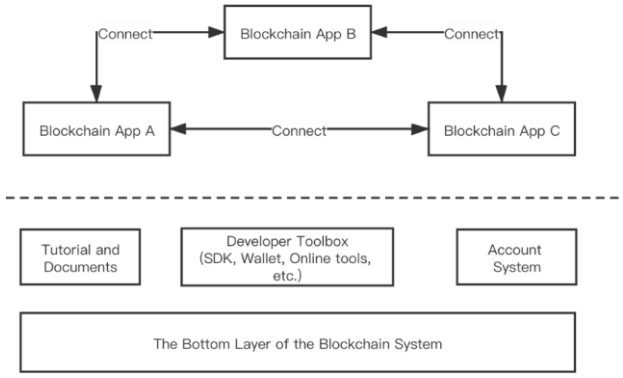

Figure 4. Ecological system diagram constructed by multiple applications on blockchain system

As shown in Figure 4, different applications on the same blockchain system use common tutorials, documents, and developer toolboxes, while sharing a set of account systems.

Therefore, various APPs in this blockchain system can communicate with each other, divert each other, and help each other in various ways to build a living ecosystem.

When building our blockchain application, we may need

to rely on different ecological forces, so we need a dual-chain or even multi-chain architecture.

4 Points to Note When Designing A Bi-chain Architecture Application

When designing a bi-chain structure application, there are several points to note:

1）The ability to recover applications from a "single point of failure" is required. The blockchain itself is a distributed architecture. If the application then uses a distributed design to prevent single points of failure, it will appear redundant and increase costs. Therefore, when designing the system, it is necessary to consider the need to restore application-critical data through on-chain synchronization.

2）hen different modules choose the blockchain system they are based on, they need to consider the aforementioned factors: consensus mechanism, economic model, TPS, stability and ecology. For example, because the most important thing in a digital identity system is stable reading and writing, the BSN chain is chosen.

3）The traditional database can freely upgrade the table structure. When designing a database for a blockchain application, it is necessary to consider the premise that future database upgrades will not conflict with data on the chain.

4.1 Bi-chain Overall Architecture Design

On the overall architecture, we generally divide the project into three layers from bottom to top, as shown in Figure 5 below:

First, Blockchain Layer

The blockchain layer includes two parts, the "BSN Network" and the "ETH-like Alliance Chain", which are responsible for "the necessary information on the chain in the digital identity system" and "out-of-organization capital flow".

Second，Application layer

The application layer consists of two modules, the Ethereum wallet and the digital identity system. The two modules share a local database and provide API interface to external systems.

Third, The External Layer

The external layer is each existing system and newly developed application, which is connected to the application layer through the API. It can be a "point system", such as the existing canteen system; or a "pointless system", which is only connected to a digital identity system, such as a small program developed by a community.

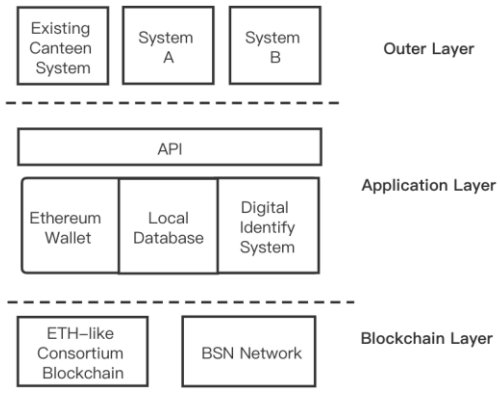

Figure 5. Bi-chain overall architecture design

4.2 Digital Identity System Architecture Design

The digital identity system interacts with the BSN network through the API interface provided by the BSN network As shown in Figure 4, and stores necessary information in a local database at the same time. In addition, the digital identity system also interacts with local modules and external applications through its own API system to implement the function of adding, deleting, viewing and modifying identity information.

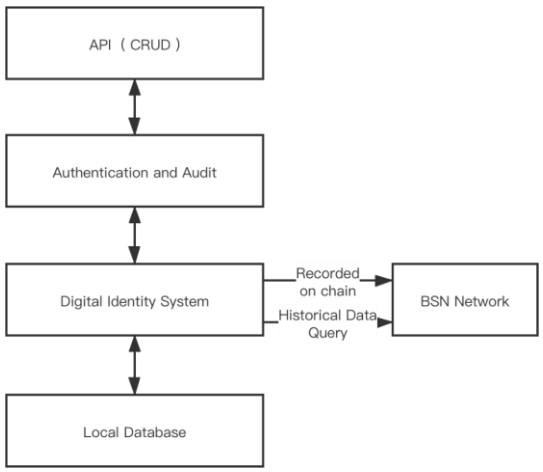

Figure 6. Architecture design of digital identity system

4.3 Account Module Architecture

The account module is transformed from a traditional blockchain wallet. The difference is that an Ethereum address corresponds to an organization in our local database. The entire design diagram

can refer to Figure 7, we call the Token in the account through a smart contract.

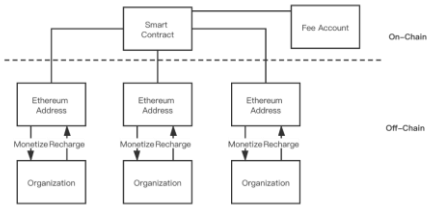

Figure 7. Blockchain account module design drawing

4.4 Database Structure Design

The simplest database structure includes four tables-user table, organization table, transaction table and account table. Among them, the user table and organization table belong to the "identity system", and the transaction table and account table belong to the "account module". Among them, the organization table is linked to the account table through the account_id foreign key. The design of related data can refer to Sheet 2.

Select the on-chain content of the local database as following:

• The key values that need to be disclosed in the user table and organization table should be stored on the chain via BSN, such as organization name and organization profile.

• In addition to the regular transaction information in the transaction, the user_id and account_id need to be stored in the transaction data, which can ensure synchronization and ensure that the transaction data on the chain is consistent with the balance data and the local database.

Sheet 2. Data structure design table(Bold keywords are foreign keys)

User	**Organazation**	**Transaction**	**Account**
id	id	id	id
Organizationp_id	name	tx_id	address
…	**account_id**	from	balance
	…	to	…
		amount	
		fee	
		user_id	
		account_id	
		…	

5 Bi-chain Application Design Case

5.1 Project Case Ideas Introduction

On traditional campuses, student meal cards can only be used on campus, which can cause the following problems:

• If there are few school cafeterias, meals may be more tedious.

• Students will go outside to buy food from dirty hawkers.

Therefore, this project addresses these two issues by rebuilding the original school cafeteria system so that meal cards can not only dine in the school, but also consume in dining restaurants joining the alliance. In this way, on the one hand, students can have more choices; on the other hand, the school can control the quality of the restaurant, and ensure the safety of students' meals.

The necessity of using blockchain technology in this project is as follows:

• With the participation of multiple schools, the adoption of a centralized system involves the issue of cost sharing. Administrative troubles arise when new institutions / schools join the system. But after using the blockchain technology, the schools to join only need to build their own nodes.

• Through the immutable identity system, the restaurants joining the alliance are more credible. In the later period, students can even chain reviews of restaurants to increase the cost of evil and trustworthiness.

• Collect students' consumption data through the ETH-like alliance chain.

6 Conclusions and Remaining Issues

Starting from the characteristics of the blockchain, this paper gives a low-level dual-chain design by comprehensively utilizing the two blockchain characteristics of Ethereum and BSN. Finally, it provides a business data separation for underlying platform with strong identity recognition and easy data tracking. This bi-chain interacts with the business through interface interaction, realizes functional coupling, decouples modules, and finally applies it to personalized scenarios.

Even so, there is still a lot of work to be done, such as the design between system sharding and blockchain sharding, how caches and queues are applied to actual systems, potentially improving the system's ability to handle high throughput and low latency .

FUND PROJECT

This project is funded by the Blockchain Technology and Application Research Center of the Institute of Artificial Intelligence Transformation and Management, Shanghai University of International Business and Economics.

ACKNOWLEDGMENTS

This paper from conception to implementation, and finally to the birth of an academic paper, is inseparable from the discussions and collisions of the Institute of Artificial Intelligence Transformation and Management of Shanghai University of International Business and Economics. Among them, it is inseparable from the massive support and assistance provided by colleagues of the Institute. Thanks together.

REFERENCES

[1]刘峰. 区块链热与企业机遇[J]. 企业管理, 2018, No.442(06):19-21.

[2]Vishnu Prasad Ranganthan, Ram Dantu, Aditya Paul,et al. A Decentralized Marketplace Application on the Ethereum Blockchain[C]// 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). IEEE, 2018.

[3]Jagdeep Sidhu. Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business[C]// 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017.

[4]Jong-Hyouk Lee. BIDaaS: Blockchain based ID as a Service[J]. IEEE Access, 2017, PP(99):1-1.

[5]Nesrine Kaaniche, Maryline Laurent. A Blockchain-based Data Usage Auditing Architecture with Enhanced Privacy and Availability[C]// 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). IEEE, 2017.