BOHR

BOHR BLOCKCHAIN TECHNOLOGY SOLUTIONS

『BUILD HIGH PERFORMANCE EXPAND PUBLIC BLOCKCHAIN NETWORK』

Bohr conforms to the development trend of "blockchain +" era, and constructs a complete solution of practical public blockchain ecosystem, which has high scalability, effective security, reliability, decentralization and flexibility to develop a variety of application types. It will allow up to a million transactions per second. Bohr is based on the special basic protocol framework design, intelligent contract execution in the middle layer and the implementation of the upper functional architecture, which makes blockchain technology successful in real large-scale commercial applications.

BOHR TECHMOLOGY WHITE PAPER V.1.0

Introduction

Aiming at the common problems of transaction congestion, high transaction cost and long transaction confirmation time in the existing blockchain, Bohr aims to build the world's first high-performance development public blockchain network with the goal of "extremely light, extremely fast, extremely interesting and extremely wide", and supports massive concurrent transactions and faster transaction confirmation. Bohr has an innovative double-layer consensus mechanism and cosh consensus algorithm. By using the algorithm, a number of super nodes are selected periodically to give them the notarization right of data units, and they will send out effective notarization units to obtain block rewards. Bohr focuses on building a simple and easy-to-use decentralized digital token underlying blockchain, using declarative expressions to enhance expression ability.Smart contract, users can create and issue digital pass freely without writing complex smart contract code.

Bohr has an extensible wallet, which provides security and rich application interfaces for digital token, blockchain games and social networks. It enables new and unique ideas to run smoothly on the blockchain, making the use of blockchain a way of life, and making it possible for blockchain to be widely used in various fields.

Contents

Background

1.1 "Blockchain+"wave

1.1.1 Blockchain 1.0:

There is no application function, with digital currency return as the king.

1.0 era, represented by bitcoin, its status is irreplaceable. His characteristics are decentralization, world circulation, exclusive rights, no hidden cost, fixed quantity, uncontrolled issuance, convenient transaction and low transaction cost.

This generation of blockchain technology has no application function, that is, issuing currency. Its IT system architecture is very simple and secure. Bitcoin is considered to be the gold on the Internet. Its reserves are limited and will be used as the value of digital currency in the future.

In the era of blockchain 1.0, the buying and selling of digital currency is the most important form for people to participate in the blockchain. At this stage, few people pay attention to the application value of digital currency, and pay more attention to the return rate of digital currency.

In 2017, the return on investment in bitcoin reached 181%, and the total return on the whole category of digital currency was as high as 448%, far higher than that of real estate, gold and stock investment.

1.1.2 Blockchain 2.0:

Smart contract provides infrastructure support for upper application development.

Blockchain 2.0 is a programmable blockchain. Taking Ethereum as a representative, building an operating system on the Internet, it only puts forward a concept, and does not realize the real application, or does not meet the application requirements. Because its architecture is changed on the basis of bitcoin architecture, but the biggest contribution of blockchain 2.0 is to completely subvert the concept of traditional currency and payment through smart contracts. It can be roughly understood in the financial field. Such as bank settlement payment, cross-border payment, etc;

In the era of blockchain 2.0, blockchain forms a trust foundation based on the characteristics of traceability and unforgeability, which provides a trusted execution environment for smart contracts and makes it possible to realize automation and intelligence of contracts. Ethereum is a technical means to realize smart contract on the blockchain. It supports Turing's complete script language, and

provides the necessary infrastructure for developers to develop arbitrary applications on the basis of its "operating system".

The biggest difference between smart contract and traditional contract is that it is not restricted by the real social law. The contract subject will execute the agreement automatically after triggering the contract terms, while the arbitration platform will not judge the execution result in the smart contract, but undertake the responsibility of execution.

1.1.3 Blockchain 3.0:

The subversion of commerce lies in the change of production relations.

Blockchain 3.0 is beyond the financial industry, covering all aspects of social life. The most obvious feature of blockchain 3.0 is that it no longer relies on a third person or institution to gain trust or establish credit. It also saves labor and time costs and improves efficiency,

In the era of 3.0, blockchain 3.0 can meet complex business applications. Blockchain 3.0 goes beyond the economic field, and can be used to realize the increasingly automated distribution of physical resources and human assets around the world, and promote large-scale collaboration in science, health, education and other fields.

Blockchain 2.0 builds infrastructure such as digital identity and smart contract. On this basis, it hides the complexity of underlying technologies, and application developers can focus more on application logic and business logic. That is to say, entering the era of blockchain 3.0, the sign is the emergence of token. Token is the value transmission carrier on the blockchain network, which can also be understood as token or token.

The biggest effect of token on human society lies in its transformation of production relations. Joint stock companies will be replaced, and every actual participant becomes the owner of production capital. This new type of production relationship inspires each participant to continuously contribute their own productivity, which is a great liberation of productivity. If this kind of business activity is mapped to inflation in real society, as long as the former outperforms the latter, the holder of each token will gain profits over time.

In short, at present, the most important thing for token is to do a good job in ecological construction, and the first thing is to have a landing scene. Although the enthusiasm of "blockchain +" is high at present, the scenarios that are really suitable for "blockchain +" are still very limited. We believe that at least three points should be met:

there is a need for an account book in the scenario (not limited to the record value); there is a demand for authenticity; and a large-scale consensus needs to be formed.

1.2 Public chain Dilemma

It can be said that the biggest application of chain circle before 2019 is to fry currency. With the advent of the bear market, the way of money speculation has been verified to be unworkable. How can the public chain break the situation? To solve this problem, we must jump out of the thinking of "coinage" and return to the blockchain technology itself to find the answer.

From the perspective of block chain technology, the essence of each transaction is to check whether it can generate a vote in the block chain Nodes will vote through the transaction package out of the block, "block" broadcast in the node, each node received the "block" after the completion of its own account book modification.

From the working process of the blockchain, we may find five key points for the public chain to break down:

1) Security is the foundation and can't be easily controlled. At present, most companies adopt elliptic algorithm to ensure security, but in front of quantum computing, it will be cracked in a few seconds, which will lead to the disclosure of all our bank deposits and Internet

login passwords. Bitcoin and Ethereum also use elliptic algorithm, so there is no privacy in front of quantum computing. After cracking, it can make fraud and transfer money. Therefore, our calculation method must be able to resist quantum computing and protect against the risk of privacy leakage.

There are three ways to ensure extreme safety:

The first is zero knowledge proof, which is a verifiable encryption algorithm, and there is no decryption process in the whole process, which does not reveal privacy, and even quantum computing can not be cracked; the second is threshold encryption, which can be used as a token The third is lattice computing, which is a mathematical transformation process based on multi-dimensional space. With the increase of dimension, the difficulty of calculation is not only the increase of exponential level, but also the increase of complexity level. However, lattice computing consumes more CPU.

2) The core of decentralization lies in the node mechanism. A real distributed accounting node must have enough nodes to participate.

For example, only those with more than 1000 nodes can be called public chain, which is one of the reasons why bitcoin and Ethereum can be recognized by the industry. Secondly, the entry and exit of nodes are free according to the rules. Finally, the threshold of nodes should be low enough for the general public to participate. After all,

the core spirit of the blockchain is the active participation of community members. In order to allow the public to participate, it is necessary to avoid all kinds of competitions. Once there is a competition, it will eventually become a game for a few rich people. Moreover, the competition mechanism will certainly increase the cost and cause a waste of social resources, such as the computing power competition of bitcoin.

3) The performance should be good enough to avoid blocking applications as soon as they are running. Under the current network bandwidth and computing power, the 100 megabyte home broadband can actually run 12.5mb, and a transaction of 125b can make up to 100000 transactions. However, due to the constant broadcasting and voting needs of the public chain, as well as the loss of the actual environment, the single chip performance limit is estimated to be more than 8000-10000. The measured results of ec71967 ECS on the ec71967 mobile phone show that the ec71967 is up to the ec71967.

Considering the above two bottlenecks, the performance limit of single chip is estimated to be around 8000. Therefore, in terms of performance breakthrough, it has become a consensus in the industry to achieve a performance breakthrough by implementing distributed computing by fragmentation.

However, the difficulty of distributed computing is very great, and the security requirements of blockchain make it even more difficult. However, it is very strange why there are so many projects that are clearly applied to be public chains. Based on the understanding of the technical difficulty, I think that only two types of teams are likely to achieve real breakthroughs: one is the genius with more money and intelligence than Vitalik Buterin; the other is the distributed system team that has operated hundreds of millions of user products, and those who do not meet these two requirements can be ignored, because even if a certain team is strong in a certain direction, such as cryptography, it can not be big on the public chain Breach.

4) The cost should be cheap enough. The software and hardware cost of distributed accounting must be higher than that of centralized accounting, but it must be far lower than the total cost of centralized accounting. The reduction of gas fee lies in the reduction of public chain operation cost, which is a cost problem in essence.

The essence of mining income is a subsidy for gas fees. To see whether a business model is established, the simplest reason is to remove subsidies. From the perspective of high costs of BTC and eth, they will eventually fail to operate normally. This is also the reason why V Shenli gave up POW to POS. POW will definitely be eliminated in the computing power competition. Even if bitcoin will succeed in the

future, it will not run in the current chain (either upgrade completely or run on other chains).

In addition to abandoning the computing power competition, there is also a very important way to reduce the cost is to use idle bandwidth and idle hardware, which will make the actual cost of each node very low, even close to 0.In terms of bandwidth and computing power, 10000 100 megabyte home bandwidth is 1TB, and the computing power is 10000 sets * 8 cores * 2.8g/2 = 112t. In contrast, the bandwidth of EOS super node is 21 * 25gb = 525gb, and the computing power is 21 * 128 * 2.2g = 5.9t. It can be seen that even the super node of EOS cannot defeat the power from 10000 families.

5) Experience is better, the core is that the transaction confirmation (subject to the block) should be fast. It is hard to imagine the future. When you buy coffee with token, you will have to wait a few minutes to confirm. The experience is closely related to the transaction confirmation time. In the ideal state of eth, a block is generated in 15 seconds, and it takes 3 minutes to confirm the transaction after 12 blocks.

The mechanism of EOS is more opportunistic. The transaction confirmation has nothing to do with the block out. The block out time is 3 seconds, but it needs more than two-thirds of the nodes to confirm before the irreversible transaction. The whole process (1 + 14)

* 3 = 45 seconds, that is to say, it takes 45 seconds for EOS to complete the real transaction confirmation, rather than 1 second as advertised by itself.

Therefore, only if the above problems are solved gradually, can the public chain usher in the development and growth, and the application can be gradually implemented. The blockchain industry itself is a high-tech industry, hoping to realize machine trust with technical means and make the world a better place. As the technical bottleneck has not been overcome, there is only one application of speculation currency. But I believe that in the near future, the new generation of public blockchain chain and mature technology will open the era of large-scale commercial application landing, and that is the real blockchain.

1.3 Blockchain future

Blockchain uses P2P technology, cryptography and consensus algorithm technology, with the characteristics of data tamper proof, system collective maintenance, information transparency and so on. Blockchain provides a mechanism for information and value transfer and exchange in an untrusted environment, which is the cornerstone of building the future value Internet.

Trend 1: the application of blockchain industry has been accelerated, and the penetration and diffusion from digital currency to non-financial field has been promoted

As a general technology, blockchain technology has accelerated its penetration from digital currency to other fields and integrated with innovation in all walks of life. We believe that the application of blockchain in the future will be promoted by two camps. On the one hand, the IT camp, starting from information sharing, takes low-cost credit establishment as the core, and gradually covers digital assets and other fields. On the other hand, the cryptocurrency camp starts from currency, and gradually advances to the fields of asset side management and deposit certificate, and spreads to the application of credit investigation and general information sharing.

Trend 2: enterprise application is the main battlefield of blockchain, and alliance chain / private chain will become the mainstream direction

At present, the practical application of enterprises focuses on the field of digital currency, which belongs to virtual economy. We believe that blockchain applications in the future will shift from virtual to real, and more traditional enterprises will use blockchain technology to reduce costs, improve cooperation efficiency, and stimulate the growth of the real economy, which is the main battlefield of blockchain

applications in the future.

Different from the public chain, in enterprise level applications, people pay more attention to the management and control, regulatory compliance, performance, security and other factors of blockchain. Therefore, we believe that the strong management blockchain deployment mode of alliance chain and private chain is more suitable for enterprises to use in application landing, which is the mainstream technology direction of enterprise application.

Trend 3: the application promotes diversified technical solutions, and the performance of blockchain will be continuously optimized

In the future, blockchain applications will develop from single to multiple directions. Different applications such as bill, payment, insurance and supply chain are highly differentiated in real-time, high concurrency, delay and throughput. This will lead to a variety of technical solutions. We believe that blockchain technology is far from being finalized, and will continue to evolve in the future. There is room for efficiency improvement in the technical aspects of consensus algorithm, service fragmentation, processing methods, and organizational forms.

Trend 4: the combination of blockchain and cloud computing is getting closer, and baas is expected to become a public trust infrastructure

Cloud computing is the general trend. We believe that the combination of blockchain and cloud is also an inevitable trend. There are two modes for the combination of blockchain and cloud, one is blockchain in the cloud, the other is blockchain in cloud. The latter, namely baas, means that the cloud service provider directly provides the blockchain as a service to users. In the future, cloud service enterprises will more and more integrate blockchain technology into the ecological environment of cloud computing. By providing baas function, the deployment cost of enterprise application blockchain can be effectively reduced, and the initial threshold of innovation and entrepreneurship can be reduced.

Trend 5: the security problem of blockchain is becoming increasingly prominent, and security protection needs the overall consideration of technology and management

From the mathematical principle, blockchain system is almost perfect, with the advantages of openness and transparency, difficult to tamper with, reliable encryption, anti DDoS attacks and so on. However, from the engineering point of view, its security is still restricted by infrastructure, system design, operation management, privacy protection and technology update iteration. In the future, we need to consider the overall situation of technology and management, strengthen basic research and overall protection, so as to ensure the

application security.

Trend 6: the cross chain demand of blockchain is increasing, and the importance of interconnection is highlighted

With the deepening of the application of blockchain, enterprises or industries in the fields of payment and settlement, logistics traceability, medical records and identity verification will establish their own blockchain systems. We believe that cross chain cooperation and interoperability among these numerous blockchain systems in the future is an inevitable trend. It can be said that cross chain technology is the key to realize value Internet of blockchain, and the interconnection of blockchain will become an increasingly important topic.

Trend 7: blockchain competition is becoming increasingly fierce, and patent competition has become an important area of competition

With the increase of participants, the competition of blockchain will be more and more fierce. The competition is all-round, including technology, mode, patent and other dimensions. We believe that in the future, enterprises will strengthen the layout of blockchain patents. Since 2014, the number of blockchain patent applications has witnessed an explosive growth. Blockchain patents are mainly distributed in the United States in North America, the United Kingdom in Europe, China and South Korea in Asia, and this pattern will be

maintained in the future. The patent gap between China and the United States is narrowing, and China's application volume in 2016 has surpassed that of the United States. It can be predicted that the future blockchain patent competition will become increasingly fierce.

Trend 8: blockchain investment continues to boom, and the cumulative risk of token crowdfunding mode deserves attention

Blockchain has become a hot spot in the capital market. The future investment will continue the rising trend in 2014-2016. Different from the financing modes in other science and technology fields, there is a mode called "token crowdfunding" in blockchain field, namely initial coin offering (ICO), which is a crowdfunding method for startups to issue tokens and raise funds. With the increase of token crowdfunding transaction volume, many projects lack of audit, value fluctuation is huge, and the risk of being on the edge of supervision will increase, which is worthy of attention.

Trend 9: there are conflicts between blockchain technology and regulation, but the contradiction is expected to be further reconciled

The characteristics of blockchain, such as decentralization, disintermediation and anonymity, are incompatible with the traditional enterprise management and government supervision system. But we should also see the opportunities that blockchain brings to regulation. We believe that in the future, enterprises will

actively meet the regulatory needs and actively build in regulatory requirements in the design of technical solutions and modes, so as to not only achieve compliance operation, but also greatly save the cost of regulatory compliance. We also believe that in the future, the global regulatory authorities will embrace the new regulatory technology of blockchain, and use the new technology to enhance the efficiency of government regulation.

Trend 10: credibility is the core requirement of blockchain, and the importance of standards and specifications is becoming increasingly prominent

In the future value delivery network based on blockchain, we will build the trust foundation completely with algorithms and software. However, we believe that this is far from enough, and standards are needed to increase the trust of the blockchain. In the future, the standard of blockchain will standardize the technology and governance of blockchain from the perspective of users and business oriented, from the dimensions of smart contract, consensus mechanism, private key security, permission management, etc., so as to enhance the credibility of blockchain and increase the weight of trust in blockchain.

Introduction

Bohr is a global open source blockchain community project, which is a customizable blockchain infrastructure composed of microkernel and functional modules. Bohr has developed a set of industrial blockchain technical standards, which follows the principles of hot plug, modularization and parallel expansion, and provides replaceable functional modules such as smart contract, multi chain parallel, consensus mechanism, P2P network, storage, encryption, multi-level account, etc.

We hope that through the blockchain technology, we can help

the original life and work in the lack of centralized trust system scenarios, freely build decentralized business model, so as to solve the trust contradiction between individuals and commercial entities in society.

Based on Bohr, this simple basic main chain, we will provide rich modular components, just as the CPU, hard disk, memory, motherboard are assembled into a computer. Users can freely choose modules such as consensus, storage, contract, arbitration, account system, anonymous policy, permissions, etc., and assemble them into sub chains suitable for their own needs. The sub chain is not limited to public chain, but also can be private chain or alliance chain.

After market research and analysis, we find that there are some problems in the development of blockchain. The scarcity of technical talents and high R & D cost of blockchain can not be alleviated in a short time; more and more application scenarios need the support of blockchain technology; the performance of existing blockchain is limited, and different chains cannot communicate; institutions tend to use alliance chain and private chain, But the two are not completely trusted. Bohr offers a reliable solution for this.

2.1 Flexible and easy to use blockchain infrastructure

Bohr provides complete Turing based modular development for developers and users. Developers and users do not need to study cryptography, consensus mechanism, storage methods and other underlying technical details, and use a simple and fast programmable environment to directly connect commercial applications, so as to reduce the commercial cost of blockchain.

2.2 Adapt to massive blockchain application scenarios

At the application level, it can be expected that the blockchain will serve as the underlying basic support for institutions and even individuals in many aspects of work and life. Bohr provides support for various future application scenarios and different needs of the bottom layer of the blockchain through operation mechanisms such as modularization, multi chain parallel and smart contract.

2.3 Commercial implementation of high performance driven blockchain

Commercial applications have very high performance requirements. Bohr is committed to solving the problem of limited performance of existing blockchain. It adopts parallel extension

technology and separates the business of main chain and sub chain through the multi chain parallel operation mechanism of "main chain + sub chain", so as to meet the demand of million level TPS.

2.4 Balance between data transparency and commercial confidentiality

For institutions, data confidentiality and security are extremely important, but the openness and transparency of blockchain makes them worry. Through data isolation and cross chain audit, Bohr ensures the business data confidentiality and security of the sub chain, and solves the balance between data transparency and commercial confidentiality.

Framework

3.1 Design concept

Bohr is a new blockchain architecture, positioned as an easy-to-use high-performance blockchain platform, aiming to realize the performance expansion of distributed applications to meet the real business needs of the real world. This is achieved by creating an operating system like architecture that can build applications. The architecture provides account, identity and authorization

management, policy management, database, asynchronous communication and program scheduling on thousands of CPUs, FPGAs or clusters. The blockchain is a new architecture, which can support millions of transactions per second and achieve second level confirmation through low latency and high concurrency hardware acceleration technology.

The architecture definition includes two parts: hardware architecture and software architecture, which is a fusion of HPC (high performance)

It is composed of high-performance cloud computing nodes and cloud computing hardware.

In addition to the network management, consensus algorithm and blockchain task processing functions supported on the core nodes under the standard blockchain software architecture, the core node introduces a software acceleration engine matching with the acceleration hardware, and supports million users' access per second through toe technology, consensus algorithm acceleration, data compression, data encryption and other technologies. The cloud terminal under this architecture can be a traditional PC, intelligent terminal, etc., and it can also be a terminal device with hardware acceleration characteristics.

3.2 Technical solutions

3.2.1 technical advantages

Bohr builds a demand-oriented, rewarding data contribution, subcontracting to achieve data structured community network, to build a safe, efficient, traceable, no data precipitation, further in-depth development of data trading platform, through data competition and data decentralized transactions to systematically solve the above pain points. Combined with the needs of blockchain network and data value discovery and exchange, Bohr's architecture design follows the following basic principles:

- ✓ **The transaction is credible**

Transaction history records enter the blockchain and are stored in certificates permanently. Both sides of the transaction trust the transaction network at low cost, which requires the network to have both reliability and privacy, and avoid intermediary problems such as data precipitation.

- ✓ **Incentive compatibility**

Economic system design promotes the network node to release data, develops derivative value discovery function based on data, and participates in the whole ecological development, so as to promote the data value discovery and exchange cost decreasing.

- ✓ **Refine transaction mode**

Through the design of network mechanism, the transaction of

data assets will be more refined.

✓ **Support highly concurrent transactions**

It supports high concurrency data exchange, and the laboratory network environment can reach million level. It will become the infrastructure of massive artificial intelligence, Internet of things, robots for large-scale data acquisition, exchange, edge computing result exchange and other capabilities in the future.

✓ **Supporting data quality verification**

It supports data sampling, cross comparison, format comparison, type identification, range identification and other automatic verification means. It provides multiple data quality verification capability settings by default while ensuring transaction security.

✓ **Supporting derivative data services**

It supports the function of programmable model calculation for data, supports developers to develop more complex data analysis tools with common language and access to Bohr, supports access to Oracle network, and improves the function scope of smart contract.

✓ **Support cross chain blockchain services**

It supports the access to Bohr of blockchain services with mature solutions in terms of data storage and computing power.

3.2.2 Framework

Bohr follows a mature six-tier technology architecture, which

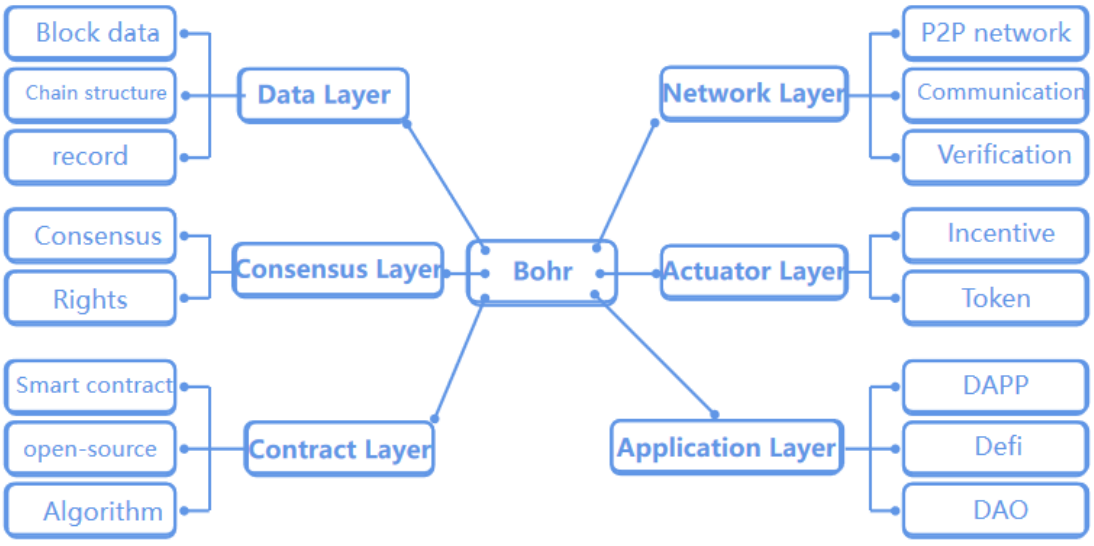
includes data layer, network layer, consensus layer, actuator layer, contract layer and application layer.

1) Data layer

The data layer is the lowest level data structure in the whole Bohr blockchain technology. It mainly describes the most basic physical form of Bohr blockchain. It is a block + linked list data structure, including Bohr's block data, hash function, Merkel number, asymmetric public and private key data encryption technology, timestamp technology, etc.

2) Network layer

The essence of Bohr blockchain network is a P2P (peer-to-peer)



network. The resources and services in the network are distributed on all nodes. The transmission of information and the realization of service are carried out directly between nodes without the

intervention of intermediate links or centralized servers. Each node not only receives information, but also generates information. Nodes synchronize information by maintaining a common blockchain. When a node creates a new block, it notifies other nodes in the form of broadcast. After receiving the information, other nodes verify the block and create a new block on the basis of the block, so as to maintain a bottom account for the whole network The role of Ben. Therefore, the network layer will involve the design of P2P networking mechanism, data dissemination mechanism, data verification mechanism, and these designs can affect the speed of block information confirmation. Therefore, network layer is an important research direction on how to break through the bottleneck of blockchain technology scalability.

3) Consensus layer

Bohr consensus layer encapsulates consensus algorithm and consensus mechanism, which enables highly dispersed nodes to reach consensus on the validity of block data efficiently in decentralized blockchain network. It is one of the core technologies of blockchain and also the governance mechanism of blockchain community. Its main role is to determine who will carry out the accounting, and the way of accounting affects the security and reliability of the whole system.

4) Actuator layer

The incentive layer is commonly known as the mining mechanism. It integrates economic factors into the blockchain technology system and designs a set of economic incentive model to encourage nodes to participate in the security verification of blockchain, including the issuance mechanism and distribution mechanism of economic incentive.

The incentive layer mainly appears in the public chain, because the public chain must encourage several points to participate in bookkeeping, and punish the nodes that do not comply with the rules, so that the whole system can develop towards a virtuous circle. In the private chain, there is no need for incentives, because the nodes participating in bookkeeping often complete the game outside the chain and require them to participate in bookkeeping through compulsion or voluntariness.

5) Contract layer

The contract layer mainly includes various scripts, codes, algorithm mechanisms and smart contracts, which is the basis of blockchain programming. Embedding the code into the blockchain or token, realizing the self-defined smart contract, and automatically executing it without a third party when certain constraints are met. This is the basis for the decentralized and trusted machine of blockchain.

In terms of contract, the first generation blockchain is not perfect.

For example, bitcoin itself only has the function of writing simple scripts, which can only be used for transactions, and can not be used in other fields or other logical processing (of course, when the definition of bitcoin in junior high school is just a point-to-point payment system, it does not want bitcoin to become an operating system). The second generation blockchain represented by Ethereum greatly strengthens the programming language protocol, realizes Turing completion, and can realize any function application in theory. Bohr is optimized and upgraded based on Ethereum. Anyone can upload and execute any application, and the effective execution of the program can be guaranteed.

6) Application layer

The application layer is the display layer of the blockchain, which encapsulates various application scenarios and cases of the blockchain, similar to the application on the computer operating system, the portal website on the Internet browser, the search engine, the e-mall or the app on the mobile terminal, etc. All kinds of DAPP applications built on the Bohr chain will also be built on the application layer in the future programmable finance and programmable society.

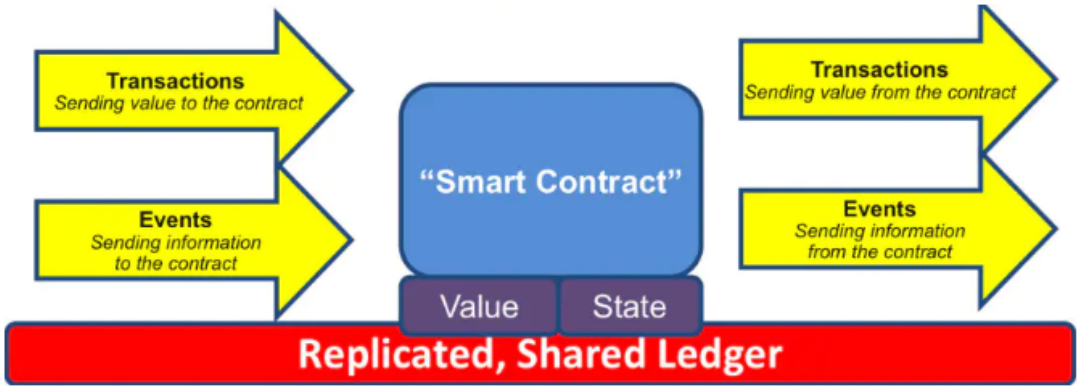
3.2.3 Smart Contract

The concept of smart contract can be traced back to 1995, almost at the same time as the Internet. The term "smart contract" was first proposed by Nick Szabo, a Cryptologist widely praised for laying the

foundation for bitcoin. In essence, these automatic contracts work like if then statements in other computer programs. Smart contracts only interact with real-world assets in this way. When a pre programmed condition is triggered, the smart contract executes the corresponding contract terms.

Blockchain technology is a distributed storage scheme of transaction oriented data. However, specific in the "should", the transaction basis can be derived from the "general" should. In the realization of these applications, we can realize them through a series of programs. Such a program is called a smart contract. Since the implementation of smart contract is related to cryptocurrency, it is usually regarded as the "part" of blockchain technology, but it is more suitable as the application layer of blockchain. In fact, smart contract should be called "stupid contract", because its enforcement is realized by code definition and then by program code execution. So it's not that the contract book has intelligence, means that the contract can be written in advance in the form of code. Code operation, implementation, and implementation. In order to realize the function of smart contract, cryptocurrency usually needs to be added to the consensus mechanism. The commonly implemented form can be script language or Turing complete program language. The latter usually requires a separate virtual machine to isolate the correlation with other modules.

Bohr's intelligent contract execution engine bohrvm adopts a modular and pluggable design method. Firstly, we develop an execution engine Bohr JVM that supports Java language, and then we will provide an execution engine Bohr EVM that supports solid language. In order to make the best use of the open source community's accumulation of smart contract technology and experience and improve the reusability of smart contract, Bohr JVM draws lessons from the EVM virtual machine of Ethereum. The implementation of Bohr VM's smart contract is fully compatible with Ethereum's smart contract specification. Java is used as the development language of smart contract. Through the architecture design of microservices and multiple security check mechanisms, it provides a high-performance and secure execution sandbox for native



Java smart contract execution.

Bohr It has a non Turing complete declarative smart contract. This smart contract is designed to explain the expected goal of the contract. While supporting Boolean operation, it increases the support for

variable operation and contract data access, and does not support stack and jump class instructions. This not only retains the advantages of declarative contract language, but also enhances the expression ability of contract language Bohr enhances the storage capacity of internal data of smart contract, and greatly improves the support ability of declarative smart contract for complex application scenarios. Compared with Turing's complete smart contract, declarative smart contract has the advantages of low complexity, lightweight and high performance, and reduces the writing difficulty and error probability.

```
["and", [
   ["sig", {pubkey: "one pubkey"}],
   ["sig", {pubkey: "another pubkey"}]
]]
```

Bohr does not have the concept of an account. Bohr is stored in a data unit of an unalterable distributed ledger in the form of utxo. In Bohr's smart contract language, address definition is a Boolean expression that can be calculated as true or false. If the signature provided by the transaction is valid and generated by the private key corresponding to the specified public key, the expression evaluates to true. All expressions of smart contract will eventually calculate a Boolean value, and multiple sub expressions can be combined through Boolean operation. For example, the following definition requires two signatures.

In order to spend money with the address defined above, two signatures must be provided at the same time. We use JSON to write expressions, and we can use well supported, optimized JSON parsers.

The "or" operation can be used to describe the signature of the private key corresponding to any public key.

```
["or", [
   ["sig", {pubkey: "laptop pubkey"}],
   ["sig", {pubkey: "smartphone pubkey"}],
   ["sig", {pubkey: "tablet pubkey"}]
]]
```

You can use the above definition to control the same address on three different devices, which may be your computer, mobile phone and tablet.

Address defined instructions can be nested, such as:

```
["and", [
   ["or", [
      ["sig", {pubkey: "laptop pubkey"}],
      ["sig", {pubkey: "tablet pubkey"}]
   ]],
   ["sig", {pubkey: "smartphone pubkey"}]
]]
```

Address definition can require participants in a collection to reach

a threshold, such as a 2-3 signature.

```
["r of set", {
    required: 2,
    set: [
        ["sig", {pubkey: "laptop pubkey"}],
        ["sig", {pubkey: "smartphone pubkey"}],
        ["sig", {pubkey: "tablet pubkey"}]
    ]
}]
```

The above expression means that any two signatures can make the expression true. If a key is lost, the address is still available, and the definition can be modified to set a new value for the lost key. In addition, different items can be given different weights, and a minimum weight requirement can be set.

```
["weighted and", {
    required: 50,
    set: [
        {weight: 40, value: ["sig", {pubkey: "CEO pubkey"}] },
        {weight: 20, value: ["sig", {pubkey: "COO pubkey"}] },
        {weight: 20, value: ["sig", {pubkey: "CFO pubkey"}] },
        {weight: 20, value: ["sig", {pubkey: "CTO pubkey"}] }
    ]
```

```
}]
```

Address definitions can refer to other addresses.

```
["and", [
   ["address", "ADDRESS 1 "],
   ["address", "ADDRESS 2"]
]]
```

This definition means that the signature is delegated to other addresses, which is useful for constructing co controlled addresses. This syntax gives users a lot of convenience. They can change the definition of the part of the address they have the right to manage according to their own wishes, without affecting other users. Address definitions can be used to configure data added to the Bohr VM.

```
["in data feed", [
   ["ADDRESS1", "ADDRESS2", …],
   "data feed name",
   "=",
   "expected value"
   ]]
```

If the data feedback result added to the Bohr VM by an address is equal to the expected value, the result of the expression is true. By specifying the source of data feedback, the Oracle function on the chain can be realized. Using the oracle on the chain can expand very

powerful functions.

```
["or", [
  ["and", [
    ["address", "ADDRESS 1"],
    ["in data feed", [["EXCHANGE ADDRESS"], ["EURUSD", "+", "0.200"], ">","1.1500"]]
  ]],
  ["and", [
    ["address", "ADDRESS 2"],
    ["in data feed", [["TIMESTAMPER ADDRESS"], "datetime", ">", "2016-10-0100:00:00"]]
  ]]
]]
```

The above expression relies on two predictors, one that publishes the euro / dollar exchange rate and the other the timing. First, both parties prepare funds for the address defined by the expression and pay their respective shares to the address. Then, if the euro / dollar exchange rate announced by the exchange address plus 0.200 has exceeded 1.150, then address 1 will receive all funds. If this does not happen before October 1, 2020, address 2 will be fully funded. In another interesting example, a consumer buys goods from a merchant, but he doesn't trust the merchant very much. If the goods are not sent

to him, he hopes the money can be returned to him. At this point, the consumer can pay the money to a shared address defined in the following way.

This definition is valid only if FedEx stores the package number on the chain. If the goods are released, the merchant can unlock the funds under the first clause. If the goods are not delivered before the agreed date, consumers can get their money back. Address definition can realize transaction query. Suppose the user wants to buy at least 1200 units of digital assets, but is only willing to pay 1000 Bohr, and he is not willing to wait for the seller online all the time. He can only post an order on the trading platform and automatically complete the transaction when the matching Seller appears. He can create the address as follows and send 1000 Bohr to it.

```
["or", [
   ["address", "USER ADDRESS"],
   ["and", [
      ["address", "EXCHANGE ADDRESS"],
   ["has", {
      what: "output",
      asset: "ID of alternative asset",
      amount_at_least: 1200,
      address: "USER ADDRESS"
   }]
```

]]

]]

The first or condition means that the user can cancel the order at any time and take back his Bohr. The second or condition, when a transaction that meets the conditions appears, Bohr is paid to the Commission trading platform to authorize it to spend money. The trading platform will publish the order information publicly. The seller can view the order list, generate an exchange asset transaction, and sign with the trading platform.

3.2.4 Flexible cross chain mechanism

Bohr Through a series of targeted collaborative smart contracts, asynchronous communication, state machine and hash locking technology, a set of general flexible cross chain mechanism is realized, the communication bottleneck of each blockchain system is broken, and all kinds of digital assets are interconnected. Appropriate cross chain collaboration mechanism can effectively ensure the effectiveness of consensus and value between internal parallel chains and other public chains And reliable delivery.

The cross chain technology includes two parts: one is the interconnection and interworking between Bohr and the external chain. Bohr and other chains are realized through a common intelligent contract, which adapts to the characteristics of other chains,

and completes the interaction with other chains based on asynchronous operation of state machine. The other is the interworking between other chains based on Bohr platform.

Bohr also provides a more complex smart contract to support the interconnection and interworking between other chains. To support two different types of other chains, the smart contract combines with the relay chain to complete the interconnection of different types of chains. Cross chain transaction is a de trust message between blockchain networks, which is a key infrastructure component for inter link communication. Cross chain transactions are initially created on the source block, and then processed and forwarded through bridges and connecting networks before finally reaching the target blockchain. As mentioned earlier, the creator of a cross chain transaction must use Bohr as a communication to pay for the transaction cost, thus motivating the participants at each intersection.

Bohr cross chain communication is implemented through an adapter, which creates a compatible block header. Bohr designs a hierarchical side chain mechanism to solve the problem of cross chain transactions matching different chain block generation speed. According to the block generation speed of the chain, the chain is divided into different layers, and then each layer is provided with a dedicated adaptation chain or adaptation module to drive cross chain transactions at the same layer.

3.2.5 Multi Chain parallel mechanism

Classic blockchain networks, such as bitcoin network and Ethereum, adopt single chain structure, and all transactions and transactions are carried out in one chain. The advantage of single chain structure is that the process of transaction and consensus is relatively simple, which can well meet the needs of users in the early stage of blockchain development. However, with the development of blockchain technology and the increasing market demand for blockchain, single chain architecture has gradually exposed many unsolvable pain points

1) There are bottlenecks in overall throughput and performance: bitcoin only has 7 TPS and requires 6 block confirmation mechanism, and Ethereum block out interval also takes 10-20 seconds, which seriously hinders the growing demand for blockchain business development.

2) Inter chain business interference: single chain architecture is easy to cause congestion of the whole system due to the busy of individual business, and many normal transactions can not be processed and confirmed in time; closed network structure: cross chain interaction between different chains cannot be realized, and business interaction needs between multiple platforms cannot be met. In order to overcome the limitation of single chain structure, Bohr

adopts multi chain parallel structure.

Parallel multi master chain mechanism: Bohr can lead to multiple main chains, each of which is responsible for special business areas, independent and interrelated, with less coupling between the main chains. Taking advantage of the advantages of parallel processing, the storage strategy is introduced for the process blocks, and the overdue data are archived historically to improve the system processing efficiency. Multi chain can solve the function support of different business and different forms of chain, and improve the performance at the same time; cross chain consensus realizes data audit and value circulation.

Because of the particularity of different services in the real world, as mentioned above, single chain structure is difficult to support a variety of heterogeneous services perfectly. In Bohr, each chain only serves the business with the smallest function set, and each cohesive business runs in a separate chain, which can not only achieve effective security isolation, but also achieve the maximum value of computing and resource utilization. Different chains interact with each other through cross chain protocol to realize value exchange.

Bohr multi chain structure can meet the needs of various types of complex services in the real world. Different types of services with different characteristics run in different sub chains, such as computing intensive, IO Intensive and hybrid types operate well on different

chains; businesses with different security levels can also run at different levels. For example, according to the business needs of banks, there will be higher requirements for data confidentiality and security and strong consistency of transactions, so they can be separated in the most secure layer.

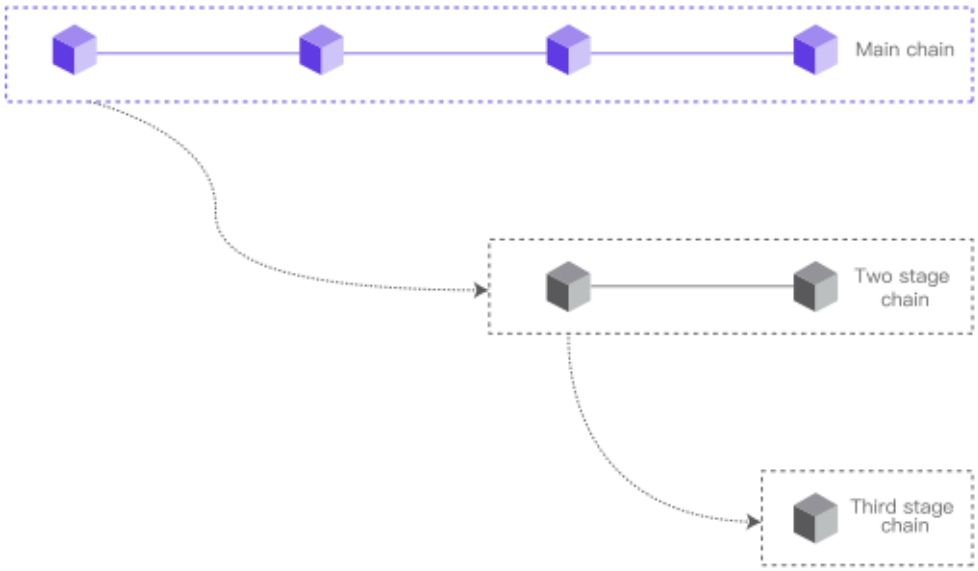
Parallel side chain scheme: in Bohr's ecosystem, the chains indexed by the main chain are side chains, and each side chain is designed to handle only one special type of transaction. When one side chain needs to verify the information from another side chain, it must include the block header information of Bohr main chain. In the face of some main business chains, the transaction records in the block can lead to the side chain as required. Bohr introduces the side chain scheme, and each side chain can operate in parallel. That is, each application can set up a side chain independently. Bohr blockchain provides built-in, perfect and easy-to-use side chain support. The side chain has a variety of consensus algorithm modules for users to choose from. The side chain can issue tokens, and the main chain and side chain can conduct two-way asset transfer. All side chains share computing power with the main chain, so all side chains have the same security as the main chain. At the same time, the energy consumption of the whole system can be minimized to avoid huge energy consumption and carbon emission caused by separate mining. The main chain grows according to the rules of the blockchain, and the

changed part of the record in the main chain block is recorded by the side chain, which realizes the organic combination of the fixed part of the block information and the changed part. The side chain records the subsidiary data of the main block transaction, which does not affect other transaction information. Each side chain can operate in parallel, and the transaction record of the side chain can be signed and confirmed by the smart contract or relevant stakeholders.

However, it is necessary to inherit all messages and services from the upper chain to the lower chain through the consensus of the upper chain and the lower chain. On this basis, the secondary chain develops its own independent application scenarios based on the application model of the superior chain, and is isolated from the superior chain.

Bohr side chain is not limited to one layer in system design principle, but can establish multi-level chain. As shown in the figure below: the so-called multi-layer auxiliary chain structure is to derive the next level side chain from the side chain. The upper layer of chain is called the parent chain, and the derived chain is called the child chain.

In addition to supporting the third party to build the side chain on the Bohr public chain, Bohr will also construct some side chains providing basic services, such as ID service, token issuing service, fast payment service and digital asset trading service, which are important components of Bohr infrastructure.



3.3 Security system

3.3.1 Elliptic curve Diffie Hellman key exchange

Elliptic curve cryptography (ECC), an algorithm to establish public key encryption, is based on elliptic curve mathematics. The use of elliptic curves in cryptography was proposed by Neal Koblitz and Victor Miller in 1985. The main advantage of ECC is that, in some cases, it provides equivalent or higher levels of security than other methods using smaller keys, such as RSA encryption algorithm.

Another advantage of ECC is that it can define bilinear mapping between groups, which is based on Weil pair or Tate pair; bilinear mapping has found a lot of applications in cryptography, such as identity based encryption.

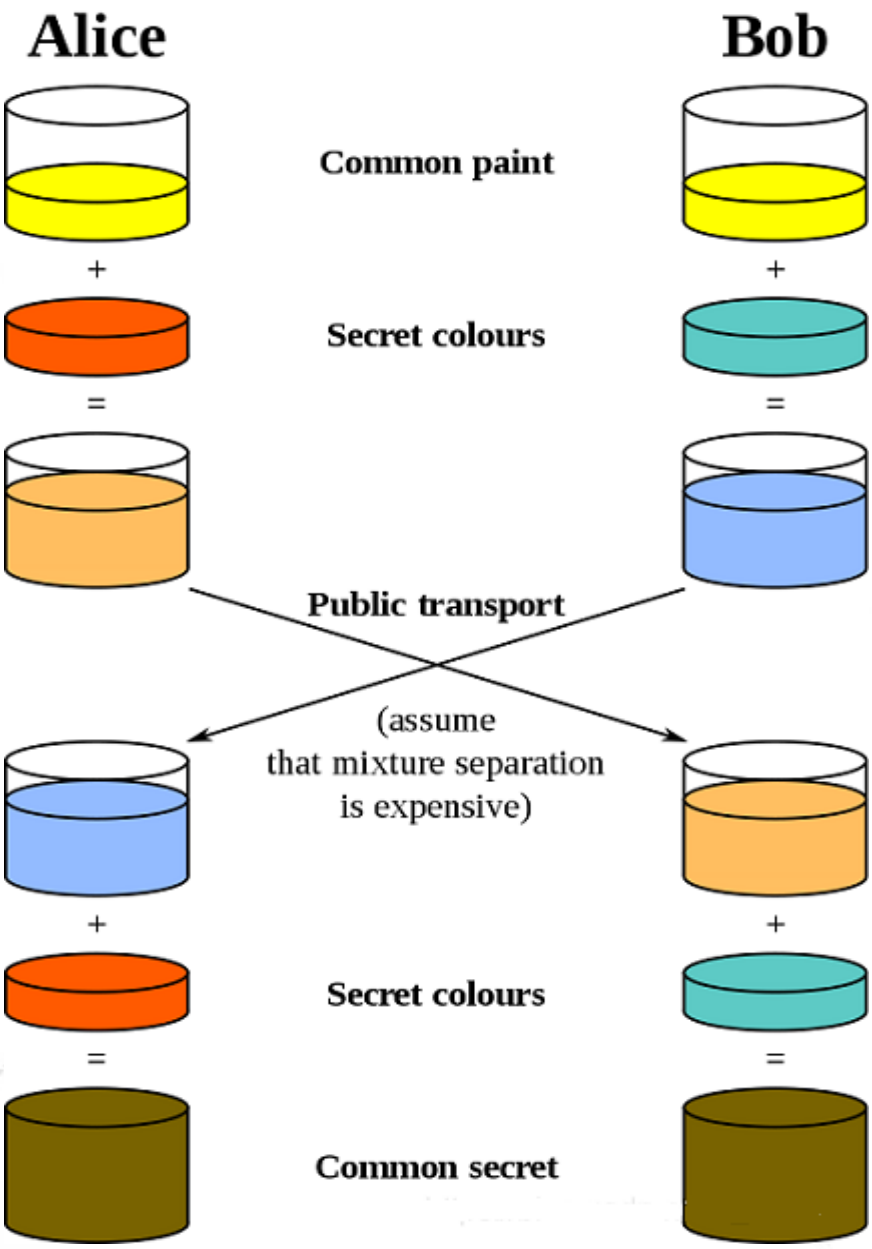
Elliptic curve Diffie – Hellman key exchange (ecdh) is an

anonymous key agreement protocol. Under this protocol, the two sides establish a secure common encrypted data in an insecure channel by using the pair of public key and private key established by elliptic curve encryption through Diffie Hellman key exchange algorithm. This is a variant of Diffie Hellman key exchange, which uses elliptic curve encryption to enhance security.

Bohr uses elliptic curve encryption algorithm to generate a key pair, which includes a private key and the public key derived from it. The private key is used for digital signature when sending data, and the public key is used to verify the source of the data. Digital signature ensures the consistency of the data on the chain and prevents the data from being tampered maliciously.

DH key exchange is a secure protocol, which allows both parties to create a key on an insecure channel. Even if the data sent to each other is known by a third party, the key of the encrypted information cannot be known.

The main idea of solving the problem can be explained by the following figure:



Alice and Bob want to negotiate a color that only the two of them know. What can we do if we can't let a third party know? The solutions are as follows:

Let's start with the color they share (yellow in the picture). This yellow is known to all, and it doesn't matter to a third party.

Alice chooses a color that only she knows (red in the picture) and

mixes it with the known yellow to form a new color (brown in the picture).

Bob also chose a color that he knew only (light green in the picture) and mixed it into the known yellow to form a new color (light blue in the picture).

Alice and Bob exchange the mixed colors. (it is assumed that it is difficult for people to find out which two colors are mixed from the mixed colors, and the security guarantee depends on this. Therefore, even if the third party knows the mixed colors, it is useless, because it can not infer that only Alice and Bob own red and light green.)

After receiving the mixed color sent by Bob, Alice adds the red that only she knows, and gets the secret color = Yellow + Red + light green (earth color in the picture, at the bottom of the picture).

After receiving the mixed color sent by Alice, Bob adds the light green that only he knows, and gets the secret color = Yellow + light green + red.

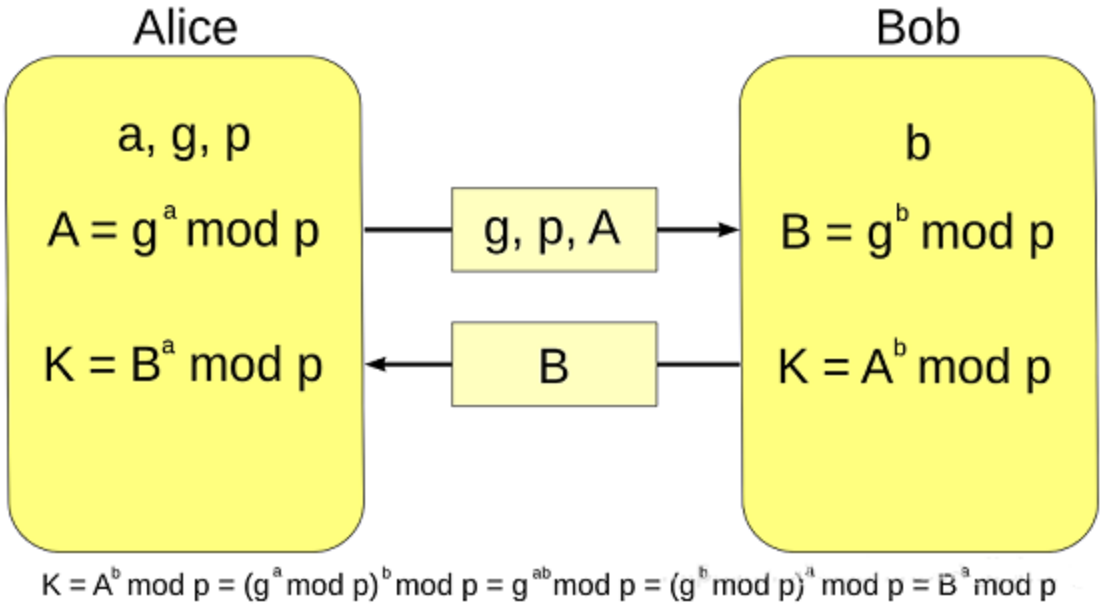
So far, Alice and Bob have the same secret color that only they know.

The key here is that after mixing the colors, people can't know which two colors are mixed. Therefore, it is easy to think of mathematical problems, discrete logarithm problems. The mathematical description is as follows:

Here, only Alice knows a, only Bob knows b, g and p are public, K

and K are the final calculated shared secret key.

The general description is as follows:



1. Alice and Bob negotiate a finite cyclic group G and its generator g, a large prime number p;

2.Alice generate a random numbe a，calculation A = gamodp，send A to Bob；

3.Bob generate a random numbe b，calculation B = gbmodp，send B to Alice；

4.Alice calculation K = Bamodp = (gb)amodp，get shared key K；

5.Bob calculation K = Abmodp = (ga)bmodp，get shared key K；

(gb)a=(ga)b because the group is multiplicative commutative, it involves the content of number theory and algebra. Alice and Bob negotiate K at the same time as the shared key.

Finally, security issues, DH key exchange can prevent eavesdropping (that is, it doesn't matter if you know the data we exchange), but DH itself does not provide authentication services for both sides of the communication (the premise of correct exchange is that Alice must ensure that the other party is Bob), so it can not resist man in the middle attack.

3.3.2 Symmetric encryption algorithm

Symmetric encryption algorithm, as the name implies, the key of encryption and decryption process is the same. Both the speed and intensity of encryption and decryption are very fast. The disadvantage is that all participants need to hold the key in advance. Once someone leaks it, the security will be destroyed. In addition, how to distribute the key in advance in the insecure channel is also a problem, which needs to be realized by Diffie Hellman protocol or asymmetric encryption.

Symmetric cipher can be divided into two types: block cipher and sequence cipher. The former divides the plaintext into fixed length data blocks as the basic encryption unit, which is widely used. The latter only encrypts one byte or character at a time, and the password changes constantly, so it is only used in some specific fields, such as the encryption of digital media.

The representative algorithms of block symmetric encryption

include DES, 3DES, AES, idea, etc

Des (data encryption standard): a classical block encryption algorithm. In 1977, fips-46-3 was adopted by FIPS to encrypt 64 bit plaintext into 64 bit ciphertext. The key length is 64 bit (including 8-bit parity check bits).

3DES: Triple DES operation: encryption → decryption → encryption. The processing process and encryption strength are better than des.

AES (Advanced Encryption Standard): adopted by the National Institute of standards (NIST) to replace des as the implementation standard of symmetric encryption. From 1997 to 2000, NIST selected Rijndael algorithm (developed by Belgian cryptologists Joan daemon and Vincent Rijmen) as AES, and the standard was fips-197. AES is also a grouping algorithm. The packet length is 128, 192 and 256 bits. The advantage of AES lies in its fast processing speed. The whole process can be described mathematically. At present, there is no effective cracking method.

Idea (international data encryption algorithm): proposed by James Massey and Lai Xuejia in 1991. The design is similar to 3DES, and the key length is increased to 128 bits, which has better encryption strength.

Stream cipher is also called stream cipher. In 1949, Claude Elwood Shannon (founder of information theory) first proved that to achieve

perfect security, we can use symmetric encryption of "one-time password book". That is to say, both sides of the communication use random key string of the same length as the plaintext to encrypt the plaintext. Sequence cipher adopts the similar idea, and generates pseudo-random key string through pseudo-random number generator every time. Representative algorithms include RC4, etc. Symmetric encryption algorithm is suitable for a large number of data encryption and decryption process; can not be used in signature scenarios; and often need to distribute the key in advance.

3.3.3 Asymmetric encryption algorithm

Asymmetric encryption is a great invention in the history of modern cryptography, which can solve the problem of key distribution in advance. As the name implies, in asymmetric encryption algorithm, the encryption key and decryption key are different, which are called public key and private key respectively. Generally, the private key needs to be generated by random number algorithm, and the public key can be generated according to the private key. The public key is generally public and can be obtained by others; the private key is generally held by individuals and cannot be obtained by others.

The advantage of asymmetric encryption algorithm is that public and private keys are separated, and insecure channels can also be used. The disadvantage is that the processing speed (especially the

process of key generation and decryption) is often slow, generally 2-3 orders of magnitude slower than symmetric encryption and decryption algorithm; at the same time, the encryption strength is often not as strong as symmetric encryption algorithm. The security of asymmetric encryption algorithm is often based on mathematical problems. At present, it is mainly based on the classical mathematical problems such as large number prime factor decomposition, discrete logarithm, elliptic curve and so on. Representative algorithms include RSA, ElGamal, elliptic curve cryptosystems (ECC), SM2, etc.

RSA: the classic public key algorithm, proposed by Ron Rivest, ADI Shamir and Leonard Adleman in 1978, won the Turing Award in 2002. The algorithm takes advantage of the difficulty of prime factorization of large numbers, but there is no mathematical proof that the two are equivalent. Maybe there is an unknown algorithm decrypting without factoring large numbers.

Diffie Hellman key exchange: Based on the discrete logarithm, the two sides can negotiate a public key on the insecure channel;

ElGamal: designed by Taher ElGamal, it takes advantage of the difficulty of finding discrete logarithm under modular operation. It is used in PGP and other security tools;

Elliptic curve cryptography (ECC): a series of modern algorithms which are concerned about. It is difficult to calculate the special inverse multiplication of a specific point on an elliptic curve. It was first

proposed by Neal Koblitz and Victor Miller in 1985. ECC series algorithms are generally considered to have high security, but the process of encryption and decryption is often time-consuming;

Asymmetric encryption algorithms are generally suitable for signature scenarios or key agreement, but not suitable for encryption and decryption of large amounts of data. At present, it is generally believed that RSA algorithm may be cracked in the near future, and elliptic curve series algorithm with higher security strength is generally recommended.

Ecosystem

The issuance and transaction of blockchain token is one of the core application scenarios of blockchain technology. However, from the perspective of practical operation, any token transaction needs an underlying wallet software as support. Once a new currency needs to be issued or a new transaction type is added, the wallet software must be upgraded, because the old software may not be able to trade new currency or Support these new features. Ethereum is a good platform, which can provide functions such as issuing tokens and defining transaction types. However, the preparation of Ethereum smart contract requires higher professional skills. Turing's complete smart contract can be used for some simple asset applications (such as issuing and trading)It seems too cumbersome and prone to errors. The "Dao" incident is not accidental. The security of smart contracts and the ease of writing applications need to be paid more attention. The recent "EtherCAT" congestion also proves that the transaction performance of Ethereum needs to be improved.

Bohr team will firmly move forward along the technology roadmap formulated at the initial stage of the project, take

technological innovation as the driving force, take application ecology as the goal, and rely on the open source ecosystem to promote Bohr's continuous technological innovation, and create an extremely light, fast and simple public chain.

4.1 Token system

Token is the proof of human being in production, savings, exchange, distribution and other activities. It is a kind of identity, a right, a carrier of value and a link of relationship. With it, we can carry out various activities such as production, savings, exchange and distribution, and use, process and distribute all materials. The limitation of centralized flow hinders the creation, transformation and Realization of value. If it is combined with the abuse of power, it will lead to corruption and unfairness. In order to reduce the cost of circulation, it is beneficial to reduce the cost of circulation. In theory, the purpose of pass is to break the barriers set up by anyone, give the same identity and power to any assets and rights, and endow them with ideal liquidity, especially those assets and rights which are relatively scarce and have long-term potential for appreciation, so the pass card has more advantages in terms of liquidity.

Token economy is a new concept put forward by the blockchain industry recently. Many people don't know what is token economy.

Economy has a standard concept: economy is the creation, transformation and Realization of value; human economic activity is the activity of creating, transforming and realizing value to meet the needs of human material and cultural life. The general certificate is considered to be a kind of economy that will dominate the society in the future.

4.1.1 Bohr token is not crypto coin

In network communication, the original meaning of token is "token and signaling". Before Ethernet became the general protocol of LAN, IBM once pushed a LAN protocol called token ring network, token ring network. Each node in the network transfers a token in turn. Only the node that gets the token can communicate. This token is actually a kind of right, or proof of rights and interests. With the popularity of blockchain concept and the emergence of Ethereum and its erc20 standard, anyone can issue a custom token based on Ethereum. Therefore, "token" began to be widely translated as "token" and was accepted by people.

In terms of function, token is the last tool for payment and transfer in smart contract transactions. But in fact, token can represent any proof of rights and interests, which is more than money, so it is wrong to translate token into token. On the contrary, token can be used as a proof of any rights and interests, but to represent money

alone is very harmful. Money is right, money is politics, and monetary right must belong to the state. Bohr token system aims to use token in other more reasonable ways. Token is defined as negotiable encrypted digital proof of rights and interests in Bohr system. According to the Swiss classification method, the general securities are divided into payment type, application type and asset type; according to the classification method of the United States, the general securities are divided into application type and security type; while in New Zealand, all the passes are regarded as securities. However, from the perspective of Bohr token model design, Switzerland's trisection is more appropriate.

4.1.2 Three elements of Bohr token system

The first is the digital proof of rights and interests, that is to say, the general certificate must be a certificate of rights in the form of numbers. It must represent a kind of right, an intrinsic and intrinsic value.

The second is encryption, that is to say, the authenticity, tamper proof, privacy protection and other capabilities of the pass are guaranteed by cryptography. Every pass is a right protected by cryptography. This protection is stronger and more reliable than that provided by any law, authority or gun.

Third, it is negotiable, which means that the token must be able

to flow in the Bohr network so that it can be verified anytime, anywhere.

4.1.3 Introduction to Bohr token system

Before we analyze the general model in detail, let's explain "mining". In the context of blockchain, mining is the act of obtaining a token by making contributions to the blockchain system. According to the different types of certificates, the meaning of mining is different, that is, the specific content of contribution is different.

Bohr token system can be divided into three types: payment type, application type and asset type.

For the payment type token, it is mainly obtained by contributing computing power (such as bitcoin) or providing token mortgage such as POS and dpos mechanism (such as nextcoin) to maintain the stability of the system's accounting system.

For the application-oriented token, it is mainly obtained by providing data or providing other tradable services, such as taking the subway to obtain the pass and providing articles to obtain the pass. In this scenario, the contribution made by the people who obtain the pass is not to maintain the accounting system, but to form the basic transaction ecology. Bookkeeping is more of the function of the underlying public chain.

For asset-based securities, it is basically similar to traditional

securities. The acquisition of the pass is based on the equity of the assets it represents. For this kind of token, such as STO, which is very popular now, it can be compared with the traditional securities regulatory laws and regulations.

4.1.4 Typical ideas of Bohr token application

1. Create an open and credible "industrial public account book"

The blockchain is a public account book, and the bottom public chain is the public account book of the whole society. In the last equity era, it was based on equity to do merger and integration. In the era of blockchain, industrial cooperation is based on currency right and token.

2. Design the industry win-win organization system of disintermediation

Designing a win-win industrial organization system to intermediary is also called token economic design. The core is how to cooperate efficiently.

3. Create a user driven value creation mechanism

User driven is C2B, trusted network users can advance the funds to producers, and then when the producers complete the delivery, consumers and producers will achieve value win-win.

4. Build an intelligent industrial cooperation network

Upstream and downstream or distributed collaborative

organizations should have at least one it based and intelligent collaboration network among its members.

4.1.5 10 classic models of Bohr token system

The combination and transformation of blockchain and traditional enterprises is a multi-party collaborative project, which requires the joint efforts of all parties. In the future, it will have a huge impact on various industries and generate great momentum. Starting from the asset model of traditional industries and combining with the actual business scenarios, the paper divides the application of token economy into 10 modes.

1. Monetary model

The currency mode of token economy is essentially cryptocoin, the most typical of which is bitcoin, which is a necessary module for most blockchain projects. Under the currency mode, the token issued based on Bohr network can be used for point-to-point payment and settlement, as well as the pricing of asset token. It can also be used for various digital encryption purposes, such as fund circulation, consumption incentive, investment and financial share management.

2. Traceability model

The token of this mode mainly comes from the online traceability of food safety. The distributed ledger and digital encryption technology of blockchain are used to encrypt and store the food /

agricultural product data collected by the Internet of things. The nodes in each food chain are encrypted and confirmed on the chain through DAPP. Finally, the traceability closed loop is realized by consumers.

3. Integral model

This mode is relatively special, because the integral itself is similar to virtual currency, so many blockchains are actually doing points. But the integral mode under the general certificate economy is based on the consumption and behavior of consumers to attract, encourage and stimulate, and then achieve differentiated service and care. This mode is suitable for retail, FMCG and 3C durable goods, that is, membership industry.

4. Miner model

Based on the "mining machine + currency" mode, users and investors can use mining machines to mine, obtain the platform's exclusive digital encryption token, and exchange or trade zone income. This mode is suitable for hardware manufacturers.

5. Asset model

In fact, it is a kind of digital assets on the chain, including physical assets and encrypted assets. It may also be the ownership, use right, management right, income right or digital rights and interests of digital encryption.

6. Data model

Through the data token, the personal data is monetized, and the

data control right and income right are returned to the individual. The token economy of data mode is suitable for enterprises that contact and manage massive user data, or the traffic platform of massive user entrance.

7. Content model

The token of this model can realize distributed ledger and monetization around content creation, intellectual copyright and art copyright, and realize the industry consensus value of content authenticity, copyright traceability, and creator, reviewer and collector.

8. Service model

The value-added service is realized through the contract and the sharing service. Suitable for on-demand, call by call services, such as takeout, housekeeping, real estate agents, after-sales door-to-door, etc.

9. Fans model

Make the idols or Internet Celebrities and big V in the entertainment circle into the token of the entertainment chain, and further hate winning the scenes of goods, rewards, services, ticketing, etc., to form a distributed entertainment value agreement. This model is suitable for entertainment industry companies.

10. Storage model

The idle broadband and storage space are used to realize broadband sharing and distributed storage for the needs of people or

institutions, so as to obtain the token given by the other party, and realize the sharing economy application scenario mode combined with storage and broadband.

4.2 Application system

Bohr public chain, established by a completely point-to-point "decentralized" network, its design model enables the link between the chain and the chain. By setting up a series of trusted data sources, the application can start the intelligent contract and intelligent application on the chain after the occurrence of specific events in reality. By setting the threshold value, the application can specify that the smart contract is only executed on a small number of nodes, which greatly saves the computing power of the whole network, and can also specify a small number of nodes for the transmission and storage of main data, which makes it possible for the application scenarios of blockchain such as decentralized finance, supply chain, Internet of things, distributed commerce, commodity traceability, etc.

Bohr's new blockchain architecture provides account, identity and license management, policy management, database, asynchronous communication and program scheduling on thousands of CPUs, FPGAs or clusters. The blockchain is a brand-new architecture. Through low latency and high concurrency hardware acceleration

technology, it can realize millions of transactions per second and reach second level confirmation. It is a character that is much higher than the underlying operating system of Ethereum.

Bohr's DAPP ecology can provide a broader stage for developers to combine with richer industries. Based on its own characteristics of decentralization, unforgeability and anonymity, blockchain is naturally suitable for combining with some fields, such as content, games, etc. In short, people may not need many public chains, but they will need a lot of applications. DAPP is likely to trigger the next wave of blockchain user traffic. The application scenario of blockchain should not only be "speculation", but a good industry state should be that users hold coins for the purpose of using blockchain services and products, so that the traffic is enduring and passing through cattle and bears. Therefore, the future Bohr DAPP ecological imagination space is huge.

Bohr has made a lot of technical investment in DAPP to solve the industry problems and open up a new way for the introduction of DAPP in blockchain system in the future. While compatible with the current mainstream public chain contract (erc20 contract, etc.), Bohr has great friendliness on the mainstream development language Java.

Excellent bottom technology blessing. The mature underlying public chain in the future should have relatively perfect technical characteristics, such as "innovative smart contract", "layered", "sliced",

"side chain", "cross chain", "Multi Chain parallel", "agent re encryption" and "mass storage" technologies. Bohr has turned these technologies into reality one by one and created a precedent in the public chain industry.

4.2.1 Decentralized reward + commercial media

In the era of the Internet, we are used to sharing, mobile payment and online social networking. In our generation, we are still imagining how the Internet will change our lives. The blockchain is coming. Just like the Internet in those years, it has swept all walks of life like a beast, bringing impact changes.

Red envelope is an online scene with high activity. Therefore, no matter Tencent or Alibaba, many brands will use this medium to achieve the dissemination of brand voice and the acquisition of accurate users. The significance of the blockchain red envelope lies in this. It is a carnival in the circle. Blockchain enthusiasts and digital currency enthusiasts can release or obtain red packets through the way they follow. This red envelope can also be the same as other digital assets, with appreciation space and community rights. It is also a good opportunity for "people from outside to come in", with the continuous transmission of blockchain users Broadcast, more ordinary users can enter the "city" of blockchain, get their first digital assets, and experience the convenience brought by blockchain technology.

Bohr blockchain red packet has both the technical characteristics of blockchain, such as tamper proof, secure encryption and permanent retention; it also has the characteristics of digital currency, which is a token and can also appreciate. Bohr blockchain red packets integrate the needs of commercial media from all walks of life, and capture the traffic and fans you want in the simplest, most stupid, most effective and accurate way! Create a quick and accurate drainage box!

4.2.2 Decentralized social networking

Bohr is a social network based on blockchain technology, which defines attention value and provides a free and decentralized social network for the new generation of young users.

Bohr advocates attention value. He thinks that the undifferentiated human labor condensed in the value of Internet goods includes not only the labor value on the supply side (attention value), but also the attention value on the demand side. Simple understanding is that in the Internet era, not only content service providers provide valuable content services. At the same time, user groups also provide valuable and huge information for the platform.

Bohr advocates equality. He believes that personality is equal to everyone, and the way to obtain and use benefits on social networks should be equal. This is the fundamental starting point for the

establishment of Bohr social platform. Realize the paid knowledge payment platform, so that we media people and platform content exporters reflect the value that should belong to them. Equality for all has become a fundamental value throughout Bohr.

Bohr is committed to building a global social platform that integrates free content publishing, chat without platform constraints, and freely displays itself. In view of the fact that the social platform is now controlling our speech and privacy, our independent thinking and personalized needs are intolerable, Bohr makes social interaction more free, more relaxed and more arbitrary, which is in line with the taste of young people. What's more, all the data generated by Bohr's end-to-end data encryption chat, blockchain based group chat and the hidden room burning after reading are stored in use Users have their own "free database", so that users have all the rights and interests to process data. Upload, store and disseminate all forms of content including text, pictures, audio, video and expandable content without being kidnapped. Make it a safe and efficient social platform with high quality content. Return the control of the Internet to every user, so that the bottom users can see the information they really need.

4.2.3 Decentralized Finance

Since 2019, the concept of DEI (decentralized Finance) has become a hot topic, and has experienced the sublimation from

"serving the financial industry" to "completely changing the financial industry". It has become a milestone in the ten-year development history of blockchain and occupies an important position in the blockchain industry.

Financial industry is the key development direction of blockchain technology application, and more than one third of blockchain projects can be classified as defi. According to the academic definition of Finance and according to the BICS (blockchain industry classification standard), at least 38% of the blockchain projects in the top 1000 of the current market value directly serve the financial industry, including non bank finance, wallet & trading, securities asset management, stable circular, banking services and payment settlement.

Many in the industry are excited about the future of defi. But at the same time, the current situation in the early stage of development is that most users have low awareness of it, and the number of users is also very small.

Up to now, except for star projects such as markerdao and Rex, the current flow and deposited funds of other projects are still very small, which is actually a typical feature of a new field in its infancy.

On the one hand, the development of defi is subject to the performance of the underlying public chain.

The current defi project is mainly built on the Ethereum network.

At present, the performance bottleneck of Ethereum is relatively prominent, and there is still a long way to go to break through the performance bottleneck. Under such a situation, those projects with higher performance requirements will be in an awkward situation.

On the other hand, compared with traditional financial products, decentralized financial projects are much more difficult to use and have higher requirements for users' cognition, which will greatly affect the development speed of defi.

In addition, the security of decentralized financial projects needs to be verified by practice, and users' trust will be accumulated continuously. In our contact with some developers of the defi project, we found that these temporary problems will not affect their confidence in defi. They generally believe that defi will be the inevitable trend of historical development, and has incomparable advantages in improving privacy, fairness, asset security, reducing financial costs, and de trusting.

In view of the current dilemma of defi, Bohr supports the future development of defi industry with superior performance of the underlying public chain technology, and actively develops richer defi ecological mode to release the potential of blockchain finance.

4.2.4 Decentralized games

Blockchain games are based on the development of blockchain

technology, generally including strategy, cultivation, sandbox, gambling, cards and so on. Blockchain has become a hot spot in the development of modern Internet games because it can solve the problems of traditional game mechanism opaque, user information security is not guaranteed, and game asset liquidity is poor.

In recent years, blockchain technology has been reused in the Internet, and even promoted to the national strategic level. Therefore, the blockchain industry has developed rapidly. It is estimated that the market size will reach 14 billion US dollars in the world by 2022, among which blockchain games show great growth potential. The global blockchain game industry is showing a rapid growth trend, with a market size of $17 million in 2019 and expected to reach $145 million by 2022.

Blockchain games can be divided into Ethereum games, public chain games, linker games, private chain games, etc., which are developed based on Ethereum, public chain, private chain and other platforms. At present, blockchain games are mostly developed based on Ethereum, but Ethereum has some disadvantages such as imperfect function, high cost and insufficient performance. Therefore, Bohr solves the performance problems of Ethereum with superior performance of the underlying public chain technology.

In the context of the rapid development of the Internet industry, the application demand of blockchain technology continues to rise,

and the market scale is constantly expanding. As an important subdivision market in the field of blockchain, blockchain games have great potential for future development. At present, in the blockchain game industry chain, blockchain game development profits account for a relatively high proportion, and the future development potential of this field is greater.

4.3 Business system

The core architecture of "commercial flow control" is "block chain control", which is different from traditional business flow control architecture.

In terms of the logistics, they can no longer interact with the logistics industry through the multi-level logistics service system, but can not be directly connected with the logistics industry based on the traditional logistics system The impact of control.

In this way, in the Bohr blockchain business model, manufacturers focus on creating more valuable products for consumers, and agents at all levels realize the transmission of product value to consumers through value coupling and transmission. The prosperity and positive development of the business ecology of the blockchain can be realized through the common prosperity economy rather than the oligopoly economy. The following is the business model planning of

Bohr blockchain:

4.3.1 Blockchain Cooperatives to create a real sharing economy

Blockchain can be applied in various industries, such as the well-known sharing economy such as Uber. But they are not really sharing economies. Because Uber's success is not due to sharing, their success is because they don't share. They are just integration. They collect information and sell it. Uber just builds a platform. They have to sign contracts and abide by treaties. And all the above mentioned, blockchain can be solved through the mode of smart contract.

4.3.2 The rights creators, turning content into assets

Now there are a lot of artists who sign contracts with the platform to earn 10% and 5% of the money. But in fact, artists can earn more through blockchain, and they can better cooperate with Taiwan through blockchain. The Internet is very important for content creators. As for music, it is very convenient for us to listen to music through the Internet, but at this time, music becomes information and can be copied continuously through the Internet, so music becomes a commodity without cost. We download more and more music, but these artists are making less and less money. Nowadays, if intellectual property creators want to make money, they can upload their works

to the blockchain. Every time someone downloads his works, he can directly earn a commission.

4.3.3 The Re-intermediators and reduce Commission

The next direction is the new middleman. In China, the United States and the world, the volume of cross-border transactions is very large every year. All transactions need to pay the corresponding commission to the middleman of cross-border transactions, but the person who needs to get the money most should be the payee, so this is not fair in fact, because they have to take out a part of the money to pay the Commission, rather than use it where it is really needed. Through blockchain technology, we can create new value in asset intermediation.

4.3.4 The Blockchain Supply Chain and synchronizes data in real time

The next aspect is the supply chain. Now more than 500 billion goods are sold through the supply chain. They exist in every corner of the world, but sometimes we don't know if the arrival time is accurate. If one belt, one road or another, is the only one in Africa or the "one belt and one way" country, we need to send the goods to all users in the block chain. The supply chain can also understand the situation of people's demand for goods through the demand chain.

4.3.5 Animating the Physical world and connect different devices

There are a lot of devices that we can monitor in our lives today. Whether it is a smart light bulb or a solar panel, people need to control it, and corresponding control can be achieved on the blockchain.

4.3.6 The platform builders get rid of the dependence on the platforms of large companies

Because the platform is the mainstream form, people develop new applications on the platform. Embracing a new platform can get rid of old platforms, such as banking systems or Amazon services. We can develop applications through some new platforms.

4.3.7 Big, better data to recapture users' digital assets

Big data is a hot word now. It is also an increasingly important asset in the new era, even more valuable than oil. In the digital economy, we have to think about what is the basic assets. Many large companies seem to be doing capitalization operation, but in fact, their most important assets are data. Whether Google or Baidu, the amount of data they manage is unimaginable. They provide corresponding services through these data. But these data are not in our possession,

but in the hands of third parties. This is questionable, because even though we have our own information, we leave our privacy to the companies that manage the data. What if we get the data back? We can have our own digital world. When we need to provide data, we can only provide the necessary information according to the legal requirements. You don't have to pay for coffee. You need to show me your ID. But now you need to give more information that you don't need to provide, so from a privacy perspective, blockchain can also help. In addition to big data, we will also have more and higher quality personal data. Users or consumers, who provide their own information on the basis of consensus, will also be better utilized.

4.3.8 The new public sector, changing the way of doing things from politics to social services

The last point is the new public sector. Blockchain technology can be used for inter government activities. For example, with online voting, the Internet has become an important way to participate in voting. We participate in the voting and need to make sure that we vote for the party we support, that our vote is anonymous and that the results are verifiable. But the Internet is actually not very conducive to voting media, because it is often hacked, resulting in inaccurate voting results. So the voting system hasn't changed much in the past 20 years. There are other areas, such as land rights and pension plans.

All projects that need to be registered as assets can use blockchain to better serve citizens.

Distribution

5.1 Distribution plan

5.1.1 Technical parameters

Project Name: Bohr

Project code: BR

Mining mechanism: cosh (consensus of hash stake, Kosh algorithm)

Total issue: 835 million

Block time: 5 seconds

T P S：1000000/s

Gas rate: 0.0001BR

Project vision: Bohr directly hits the pain point of the block chain industry's large-scale implementation, breaks down technical barriers with rapid smart contracts, unblocks market interaction with multi-dimensional ecological structure, and takes the whole field defi ecology as the breakthrough point, so as to relieve the public chain market in the bottleneck stage and empower the decentralized business ecology.

5.1.2 Mining output

Block height	Daily production	Stage production	Total production	Second	Day	Year
0	0	0	0	0	0	0.00
5635000	1280000	417407407	417407407	28175000	326	0.89
11270000	640000	208703704	626111111	56350000	652	1.79

16905000	320000	104351852	730462963	84525000	978	2.68
22540000	160000	52175926	782638889	112700000	1304	3.57
28175000	80000	26087963	808726852	140875000	1630	4.47
33810000	40000	13043981	821770833	169050000	1957	5.36
39445000	20000	6521991	828292824	197225000	2283	6.25
45080000	10000	3260995	831553819	225400000	2609	7.15
55016500	5000	2875145	834428964	275082500	3184	8.72
58963500	2500	571036	835000000	294817500	3412	9.35
58963501+	2288	58963501+, the output is 2288 per day, the annual output is 835000BR, the annual inflation rate is about 0.1%				

5.1.3 Mining rules

Bohr first created cosh (Consensus-of-Hash-stake) hash equity consensus. The main idea of hash equity consensus is that the accounting right of node is proportional to the node's computational power equity, and the node's computational power equity is obtained by pledge Bohr and converted into hash equity. Compared with pow, POS and dpos, it eliminates the waste of resources caused by mathematical operations, and its performance is greatly improved. All participants can compete for bookkeeping rights, realize complete decentralization and better supervision.

The calculation formula of mining efficiency of hash calculation force is as follows:

1hash calculation capacity mining quantity = (1 / hash number of total calculation power pool) x block reward x 0.85

5.1.4 Force distribution

(1) Proxy node

Destroy 1000 BR and add the server to generate agent. In the first 9.35 years (block height below 58963500), 10% of each block reward is used for agent node incentive; after 9.35 years (after block height 58963501), all block awards are used for proxy node incentive. According to the voting ranking, the top 51 agents enjoy the block award, while the 52 agents do not enjoy the block award.

(2) Distribution of computational power

Bohr initial mining amount is zero, and all block rewards are allocated according to the following proportion through calling contract:

85% allocated to voting Awards (calculated according to cosh algorithm)

10% allocated to the agent node (used to maintain the normal operation of the block)

5% allocated to new users (incentive and promotion incentives for new users)

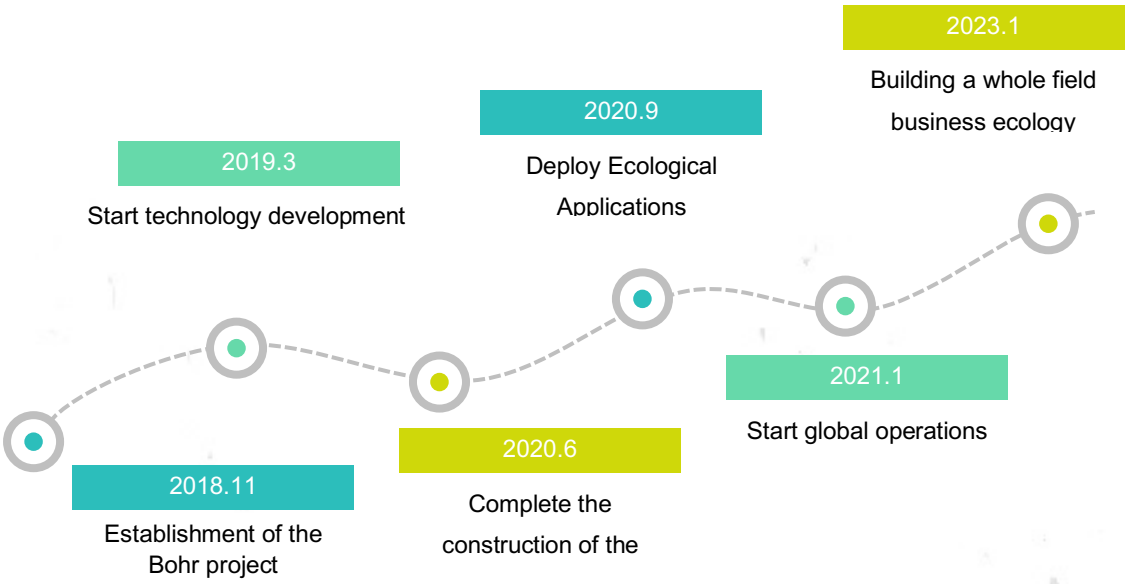
5.2 Incentives

(1) Reward for voting mining promotion: for each user directly promoted, 10% of the computing power of the promoted user will be

added, with no ceiling.

(2) New user promotion reward: for each direct promotion of a new user, 10% of the computational power of the promoted user will be added, with no ceiling.

Planning


2018.11
Establishment of the Bohr project
2019.3
Start technology development
2020.6
Complete the construction of the
2020.9
Deploy Ecological Applications
2021.1
Start global operations
2023.1
Building a whole field business ecology

Risk Tip

This document is for information purposes only and is for reference only and does not constitute any offer, solicitation or offer to sell shares or securities in Bohr and its related companies. Such offers must be in the form of a confidential memorandum and must comply with relevant securities and other laws. The contents of this document shall not be interpreted as forcing participation in the transaction. No action in connection with this white paper shall be deemed to be a transaction, including a request to obtain a copy of this white paper or to share it with others. Participation in the transaction means that the participant has reached the age standard, has complete civil capacity, and the contract signed with Bohr is true and effective. All participants signed the contract voluntarily and had a clear and necessary understanding of Bohr before signing the contract.

The Bohr operations team will continue to make reasonable attempts to ensure that the information in this white paper is true and accurate. During the development process, the platform may be updated, including but not limited to platform mechanism, token and its mechanism, token allocation. Some contents of the document may be adjusted in the new version of the white paper as the project progresses. The team will publish the updated content to the public through the announcement on the website or the new white paper.

Participants are requested to obtain the latest version of the white paper in time and adjust their decisions according to the updated contents. Bohr expressly disclaims any liability to participants for (I) reliance on the contents of this document, (II) inaccuracies in the information contained herein, and (III) any actions resulting from this document. The team will spare no effort to achieve the goals mentioned in the document. However, due to the existence of force majeure, the team can not fully make the commitment.

Bohr is an important tool for platform effectiveness, not an investment. Ownership of Bohr does not mean that the ownership, control and decision-making power of Bohr are granted to its owners. Bohr, as a digital cryptocurrency, does not fall into the following categories: (a) currencies of any kind; (b) securities; (c) equity interests in legal entities; (d) stocks, bonds, notes, warrants, certificates or other instruments conferring any rights.

Bohr's value-added or not depends on the market rules and the demand after the application is implemented. It may not have any value. The team does not promise its value-added and is not responsible for the consequences caused by the increase or decrease of its value. To the maximum extent permitted by applicable law, the team shall not be liable for any damages and risks arising from participation in the swap, including but not limited to direct or indirect personal damage, loss of commercial profits, loss of business

information or any other economic loss. Bohr abides by any regulatory regulations and industry self regulatory statements that are conducive to the healthy development of the swap industry. The participation of participants means that they will fully accept and comply with such inspection. At the same time, all information disclosed by participants to complete such checks must be complete and accurate. Bohr clearly communicated the possible risks to the participants. Once the participants participate in the swap, they have confirmed that they have understood and approved the terms and conditions in the rules, and accept the potential risks of the platform, and bear the consequences.

Reference

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

2. Vitalik Buterin. Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform. 2013.

3. Melanie Swan. Blockchain: Blueprint for a new economy. " O' Reilly Media,Inc.",2015.

4. Frederick P. Brooks. The Design of Design: Essays from a Computer Scientist. "Addison-Wesley", 2010.

5. Andrew S. Tanenbaum. Modern Operating Systems "Pearson", 2007.

6. Joseph Poon and Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016.

7. Gavin Wood. Ethereum: A secure decentralized generalized transaction ledger.2014.

8. Hyperledger Whitepaper. 2016.

9. Muhammad Saqib Niaz and Gunter Saake. Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data. 2015.

10. Robert McMillan. The inside story of mt. gox, Bitcoin' s 460 dollar million disaster.2014.

11. Sunny King, Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012.

12. David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol

consensus algorithm. Ripple Labs Inc White Paper, 5, 2014.34

13. Leslie Lamport. The Part-Time Parliament. ACM Transactions on Computer Systems, 21(2):133–169, May 1998.

14. Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. ACM Transactions on Programming Languages and Systems(TOPLAS), 4(3):382–401, 1982.

15. Leslie Lamport. Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM, 21(7):558–565, Jul 1978.

16. Paul Tak Shing Liu. Medical record system using Blockchain, big data and tokenization. Information and Communications Security, pages 254–261.Springer, 2016.

17. Robert Love. Linux Kernel Development. “Addison-Wesley”, 2010.

18. Shawn Wilkinson and Tome Boshevski, Storj: A Peer-to-Peer Cloud Storage Network. 2016.

19. Contract. URL https://en.Bitcoin.it/wiki/Contract, 2014.

20. Mandatory activation of segwit deployment, UASF, BIP 0148. URL https://github.com/Bitcoin/bips/blob/master/bip-0148.mediawiki, 2017.

21. Smart Property. URL https://en.Bitcoin.it/wiki/Smart_Property, 2016.