CHAOS

More Commercial Ecological Platform for Smart Contract

EXECUTED BY the CHAOS FOUNDATION @2017

Contents

1

CHAOS 1

1. BACKGROUND 3

1.1 Blockchain Technology 3

1.2 Origin of CHAOS 3

2. POSITIONING OF CHAOS 3

3. TECHNICAL ARCHITECTURE 4

3.1 Blockchain Services 5

3.1.1 Network Protocol 5

3.1.2 Consensus Mechanism 6

3.1.3 Data Storage 6

3.1.4 Security Mechanism 6

3.2 Component service. 7

3.2.1 Account center 7

3.2.2 Smart contract 7

3.2.3 Operation and maintenance center 8

3.2.4 Programmable script 8

4. APPLICATION SCENARIOS 8

4.1 Digital asset issuance and management 8

4.2 Internet credit investigation 8

4.3 Supply chain traceability 9

4.4 Information publicity 9

4.5 Mutual insurance 9

5. COS 10

5.1 Value 10

5.2 Distribution 10

6. TEAM 11

1. Background

1.1 Blockchain Technology

Blockchain is a distributed technical solution for data flow and sharing, which adopts a decentralized way to maintain a credible data ledger. Therefore, it is also known as distributed ledger technology (DLT, Distributed Ledger Technology). Blockchain solves the problem of multi-trust in the technical level, and builds a credible infrastructure enabling free flow of values.

Bitcoin is the first generation product and a practical prototype of blockchain. From the perspective of social influence, it is successful and manages to broadcast its decentralized, de-trusted value concept into the society. Since 2016, more and more institutions and enterprises have noticed the core value of the blockchain technology. Start-up companies have begun to study its application.

1.2 Origin of CHAOS

As the exploration and research of the blockchain technology in the commercial field, it is considered to be the core technology for the commercial application of smart contracts. With the initial success of the Ethereum experiment, the prospect and implication of blockchain and smart contract stand out.

Since 2015, our team has been focusing on smart contract. Not until 2016 did the team launch the development of CHAOS which is a blockchain and smart contract platform. Combined with the team's accumulation in the business scene and the understanding of the technology commercialization, CHAOS's initial idea is to build an easy-to-use smart contract eco-platform for business, rather than a simple application for digital asset circulation.

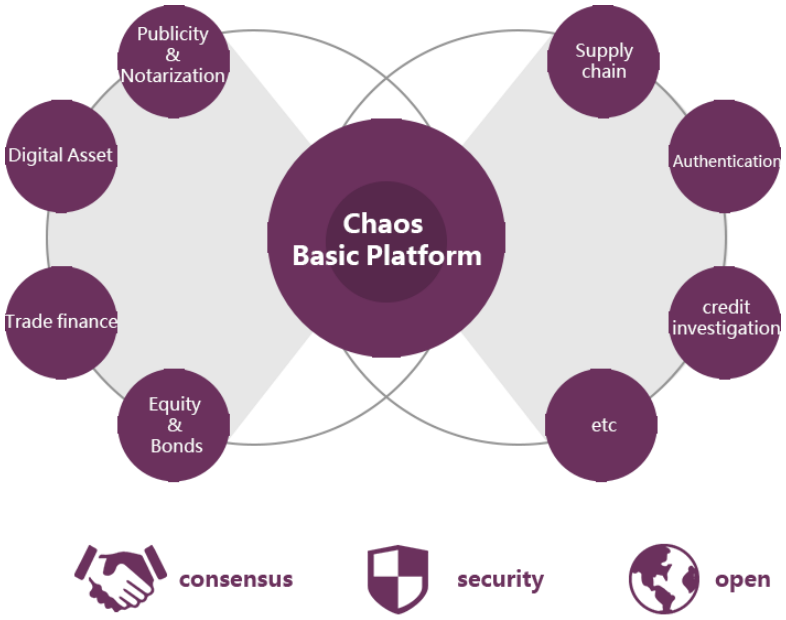
The word CHAOS derives from Khaos (English: Chaos), who is the legendary god of chaos, the beginning of the world and every concept. According to Hesiod and early ancient Greek mythology (8th century BC), in the beginning of the universe, there is nothing but only Khaos, a boundless and empty space. So its name Chaos becomes the synonymous with the beginning of the universe. We chose CHAOS as the name of the project, for the purpose that CHAOS will be the foundation and base for all commercial applications of smart contract.

2. Positioning of CHAOS

CHAOS aims to provide solutions in scenarios without trust and build a blockchain infrastructure, that is, an ecological intelligent blockchain platform for smart contract. CHAOS is committed to helping businesses rapidly implement products in the blockchain, achieving the real servitization of blockchain. CHAOS mainly completes two levels of technology: the underlying blockchain infrastructure with service

supported, and the highly scalable development environment and tool library for application-layer businesses.

At present, the research and development of blockchain mainly concentrate on two areas: one is the underlying infrastructure; the other is the upper application. Currently, the underlying infrastructure of blockchain is mainly to solve the problem of transaction speed. The Lightning network technology is a solution to the problem of transaction speed targeting at the Bitcoin network. The upper application of blockchain is mainly to build a Turing-complete programmable environment and the supporting tool library, so that developers can use it to implement de-centered applications rapidly. The founder of this area is Ethereum.



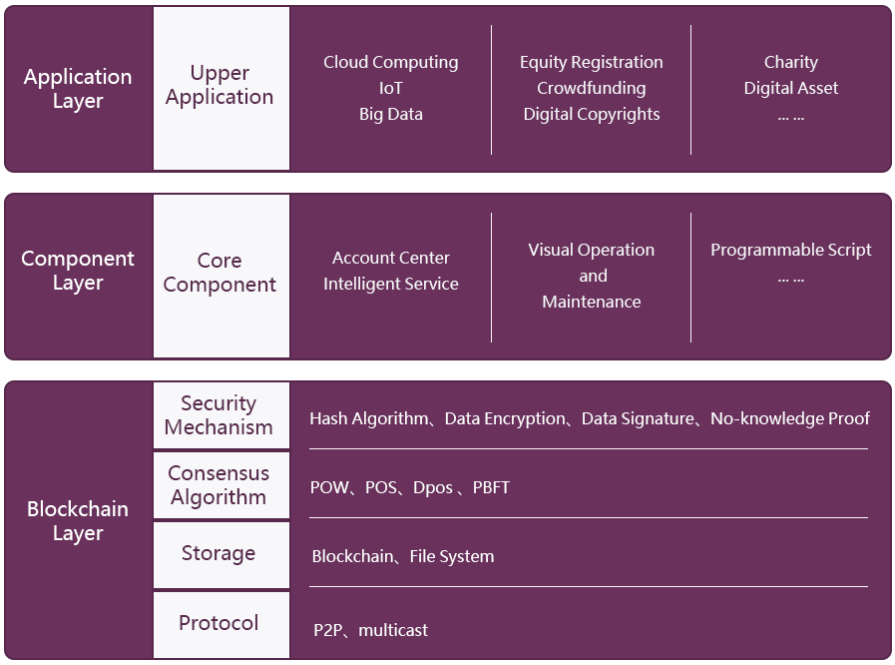
Framework of the CHAOS network

Compared with Bitcoin, CHAOS is clearly advantageous in the implementation of blockchain application development. Based on CHAOS, developers can easily develop third-party applications. While, compared to Ethereum, CHAOS has no risks and concerns about hard forking. CHAOS attempts to build a blockchain ecosystem that is different from Bitcoin and Ethereum, and extends itself to various business areas, such as law, exchange, credit, financial lending, VC financing, and asset ownership.

3. Technical Architecture

The CHAOS system is divided into three parts: the underlying blockchain services, the component layer in the middle and the upper application layer. The underlying layer provides complete blockchain services, including network protocol, data storage, consensus mechanism and security mechanism; the middle layer provides a blockchain development kit for packing the blockchain, facilitating the upper application to invoke and monitor blockchain services as well as to build smart contracts; the upper layer

constructs reliable applications based on business scenarios.

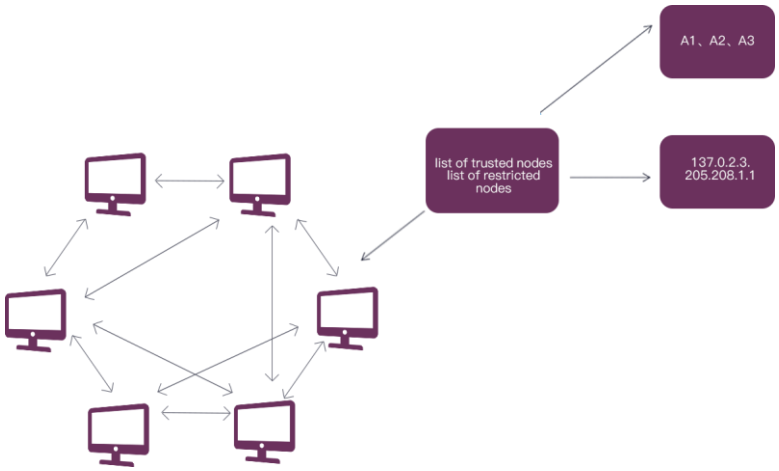


Design Scheme of the CHAOS System

3.1 Blockchain Services

3.1.1 Network Protocol

The network protocol is based on the mature P2P networking protocol, where each node maintains the neighbor node list and dynamically organizes the network in a self-organization way. In addition, security measures, such as a list of credible nodes and IP restrictions, are introduced to enhance its security and robustness in CHAOS.



IP security Mechanism Description

3.1.2 Consensus Mechanism

The problem of consistency trusts existing in the node is solved, and the ability to withstand malicious attacks is guaranteed in CHAOS. CHAOS currently supports PoW and PoS algorithms, and a variety of consensus algorithms will be supported, including DPoS, PBFT, DBFT, and so on.

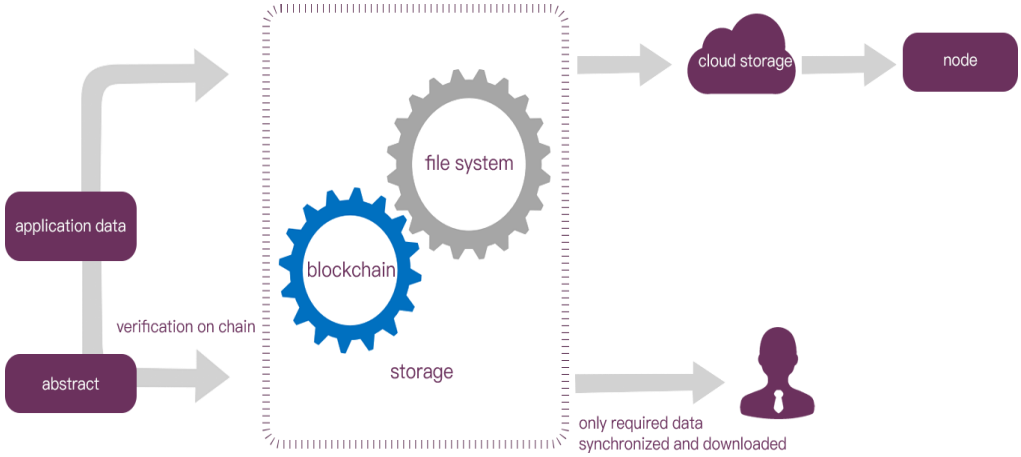
3.1.3 Data Storage

In CHAOS, data storage consists of two parts: the blockchain and the file system. Data storage is the underlying core technology of blockchain, including data format definition and data access mode. Blockchain data is still stored on a chained data structure, while application data is stored in the file system. However the application data digest is saved in blockchain for credible verification.

As blocks will continue to grow, resulting in increased occupied space by application data, it is impossible for a common computer to accommodate such a large amount of data. In fact, most users do not need to store all the data, but simply download the block data for basic validation, which means that most application data do not have to be saved locally. We propose a solution based on data partition and cloud storage. Details are as follows:

Data partition: data are categorized into hot data, cold data, necessary data and unnecessary data. Ordinary users can rapidly access to blockchain validation just by downloading necessary data.

Cloud storage: historical data are saved in the cloud and distributed to various nodes around the world to achieve the decentralization. This method is adopted to store historical data and improve the efficiency of data synchronization through the CDN acceleration.



Data Partition and Cloud Storage Solution

3.1.4 Security Mechanism

By adapting the network layer, we design a set of safe joining mechanism, which limits the connection of unauthorized users, thereby improving the security of CHAOS blockchain system. It means

that a new entrant will be authorized for access this network only by gaining permits from over half (configurable) of maintainers of the blockchain network. It is somewhat similar to a vote, except that the voters are the existing maintainer of the blockchain network.

It is very useful for private chain and alliance chain. Only in the condition that more than a half of members in the alliance agree the entrance of new node, the new node can access to the blockchain network and participate in digging.

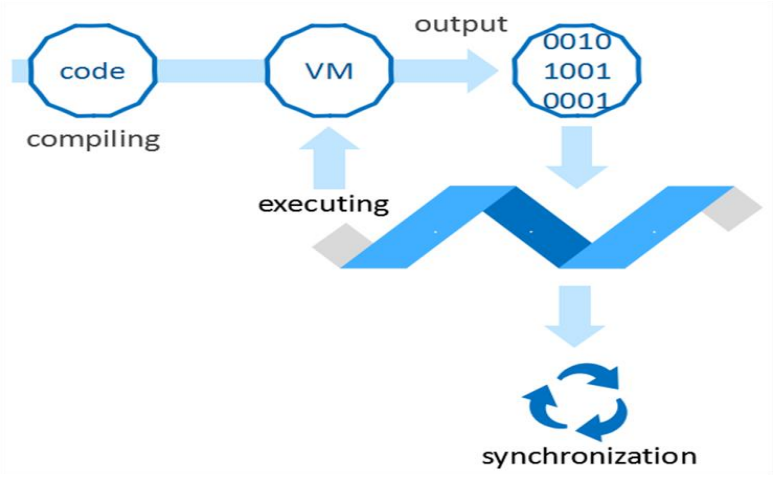
3.2 Component service.

3.2.1 Account center

The account center is able to generate and manager public and private keys. Private key can be used for transaction signature, transaction verification and multiple signatures. It supports address real-name authentication with one user supporting several addresses. Advanced function authorization is opened for specific users so as to achieve audit supervision. Also it provides mapping between application layer address and blockchain address. For applications, they don't need the actual blockchain address of users, but only need the application address.

3.2.2 Smart contract

CHAOS provides underlying components for upper applications and supports the issuance of application assets. Developers can issue internal tokens based on existing blockchain and accomplish the transfer between application tokens and blockchain currency. CHAOS provides smart contract service. Smart contract is a section of script which has been set in advance and can't be modified after issuance. It supports custom data structure in smart contract to realize complex business logistics and develops various decentralized applications by combining custom assets or blockchain currency. Smart contract provides data encryption by which only personnel related data can see the data, and it supports the plugging application consensus mechanism to reach special consensus demand in pluggable fields; users can use the contract as long as developers deploy the developed smart contract to blockchain.



Smart Contract Execution Model

In order to adapt to the future blockchain environment better, the design of our system takes the

interconnection of different blockchain into account. It provides a set of basic service to developers, so as to achieve asset transformation and cross verification among blockchain platforms.

3.2.3 Operation and maintenance center

The center provides diversified visualized blockchain management tools to monitor blockchain. It supports parameter configuration, online forking vote and block browser which can be used to check real-time block data, node distribution and the whole network operation situation. Besides, it provides multi-dimension data analysis through which abnormal situation in blockchain can be found and followed by raising alarm.

3.2.4 Programmable script

In order to facilitate developers to program smart contract based on blockchain, we transform and abstract the underlying layer of blockchain and provide an easier way for programming that is using script language.

Smart contract code will run in script virtual machine so as to achieve segregation during operation aiming to control script authority. Also script can access blockchain data which can achieve smart contract logic by inputting blockchain data into script virtual machine.

Script language is greatly favored by developers due to simple grammar and easy-using. Taking the generality and learnability of the language as think standard, we use lua and javascript as the script languages to develop smart contract at the early stage. In the future, CHAOS will support more languages for developers.

4. Application scenarios

As a technical agency to solve the trust problem, CHAOS plays its role in many application fields, including digital asset, credit investigation, supply chain, information announcement and insurance, etc. Here we select some application scenarios to explain how CHAOS works.

4.1 Digital asset issuance and management

Financial digital asset issuance enjoys following advantages by using blockchain: the total remains constant; asset flows freely; flow direction can be traced; participants maintain the credibility of asset together. Traditional stock, equity and profit voucher can be integrated on blockchain and issued as related digital asset.

Publishers register the asset voucher in blockchain and issue their digital asset. Once the issuance is finished, digital asset maintenance will not be restricted to publishers but be jointly conducted by digital asset holders and participants, so as to really achieve socialized operation. Blockchain is a network with value circulation through which digital assets can flow and exchange freely among nodes. If new institutes or users want to participate in the process, they only need to joint the system with the blockchain system of digital asset or become one node in the blockchain network. That also enhances the diversity of circulation channels of digital asset. The value of asset is decided jointly by institutions or users who operate the digital asset, which achieves value orientation through socialized circulation.

4.2 Internet credit investigation

In Internet credit investigation field, normal small enterprises are unable to accurately draw users'

credit investigation image due to lack of data source, thus they have to depend on large institutions. The monocentric credit investigation mode usually relies on the scale effect of enterprises. Enterprises who provide credit investigation service suffer huge costs of information collection and maintenance. On that account, credit investigation service features monopoly.

Internet credit investigation based on CHAOS is a kind of open and shared service mode which can be treated as an alliance chain inside the industry. Data in blockchain can't be forged or falsified, which enhances trust among enterprises. Enterprises participating in the alliance chain need to share data in blockchain which will be jointly maintained and verified by all enterprises.

The data sharing mode based on blockchain also enriches data sources of credit investigation and strengthens the reliability of service. Many enterprises jointly maintain the credit investigation system, which can reduce costs.

4.3 Supply chain traceability

Supply chain data flows among upstream and downstream enterprises and government supervision departments. Thus it is necessary to ensure the facticity and irreversibility of data. Under traditional supply chain mode, data can't flow freely among enterprises or between enterprise and supervision departments, thus data can be easily faked.

Supply chain based on CHAOS ensures that data will not be falsified. In addition, upstream and downstream enterprises and government supervision departments share one network and maintain the authenticity of network data together. Data from all process including confirming feedstock, producing, stocking in warehouse and finally distributing to agencies and distributors is recorded in blockchain, thus the facticity of data can be traced from source. Various enterprises in supply chain can better clear the upstream and downstream relation and enterprises which have indirect upstream-downstream relation are also connected.

4.4 Information publicity

Under current information publicity mode, authority of information is totally decided by the main object of announcement. The credibility-based proof mode is easy to breed many insider trading.

It greatly meets the requirement for information publicity field as data in blockchain can't be falsified or denied. As long as information publicity is achieved in blockchain, the credibility is not limited to single institution but from public nodes. Information only accepted by the public can be recorded in blockchain and then be publicized. Once the information is announced to the public, it will not be falsified by any institution or person. The blockchain ensures the reliability of public information through the technical level.

4.5 Mutual insurance

More and more platforms go into the mutual insurance business as it is open on Internet. Internet insurance business suffers two problems, non-transparent fund flow and indemnity standard. Under current Internet insurance mode, the public, especially insured users fail in monitoring fund flow, which can easily cause platform embezzlement.

Once the mutual insurance business based on CHAOS is developed, the insured fund amount and flow of users will be recorded in blockchain. Users can check their fund flow and can apply to check all

insured fund flows if permitted by authority, which enhances the credibility of the platform implicitly

Once an indemnity event occurs, users can decide if it is needed to compensate and the compensation amount by voting. That can avoid large compensation dispute and lower the operation risk.

5. COS

5.1 Value

In traditional Internet commercial world, trust comes from centralized center. By decentralization, CHAOS leaves trust determination to all system participants who will receive corresponding asset reward. In the blockchain ecological system of CHAOS, the trust in virtual world is endowed with value.

In CHAOS system, the medium used to conduct asset reward and embody value is called COS token. COS is the only system token in CHAOS ecological system which is equal to the currency in virtual world to measure value. In CHAOS ecological system, different applications can issue different asset tokens relying on COS. These tokens circulate in the ecological system according to the specific needs of applications and serve as value medium or equity voucher of application.

In a summary, COS mainly serves as system fuel and value transferring medium of blockchain application. Specifically speaking, it is as follows.

System fuel: CHAOS is a public chain. Issuing smart contract based on CHAOS needs to consume a certain amount of COS.

Value transferring medium: As the only token in CHAOS ecological system, COS acts as a value medium. Smart contract in blockchain can conduct trading, clearing and settlement via COS. All transactions can be traced and can't be falsified.

We hope that CHAOS community fans and business applicants can issue their own smart contract applications through CHAOS system, so as to keep perfecting the CHAOS ecological system and improve the value of COS.

5.2 Distribution

In CHAOS system, COS will be issued with constant amount and there will be no additional issuance. 10 million tokens are available in total, which are pre-excavated and generated based on POW (proof of work). The distribution proportion is shown below:

Angel investment: 1 million (10%);

ICO: 6 million (60%) ;

Team reserved: 1 million (10%);

Foundation: 2 million (20%)

Explanation: CHAOS project is a community-based public chain project. CHAOS foundation will totally take charge of the promotion and business cooperation. Shares held by the foundation will be used for media, third-party cooperation, follow-up member recruitment, strategic investment, etc. Reserved fund will be locked for two years and be released gradually in the third year with the releasing proportion no more than 20% each year.

6. Team

Thomas	Technical director
Breton	Architect engineer
Prescott	Back-end engineer
Grover	System security expert
Micheal	Business counselor

Thomas is a computer specialist with 20 years of computer software R&D experience. He once served as technical expert in many Internet tycoons. With 3-year blockchain technical research experience, Thomas is the founder of CHAOS project, responsible for the entire technical work of this project.

Breton is a software architect engineer focusing on designing open source software, who once participated in the design and development of many block chain projects and has deep understanding of Bitcoin and Ethereum architecture. Breton is mainly responsible for the system architecture design and development of CHAOS project.

Prescott graduated from the major of computer engineering; CIT. Prescott learned computer programming at the age of 14 and is good at many computer programming languages. He has won prizes in many international computer programming contests and started to engage in the block chain development since 2013. Prescott takes charge of the technical development of this project.

Grover is a software security expert, 25-year experience in computer security field, who has once provided role support for many large institutions as security counselor. Grover is responsible for the system security of CHAOS project.

Michael is a business counselor, who once took charge of Internet enterprise market brand. In the CHAOS project, he is responsible for business contact and market promotion.