

JD Rockefeller Token

Create a whole new field of finance

Edward Adam Davis

August 25, 2020

Draft Version 0.8

The phrase "double coincidence of wants" was coined by Jevons (1875). "The first difficulty in barter is to find two persons whose disposable possessions mutually suit each other's wants. There may be many people wanting, and many possessing those things wanted; but to allow of an actual act of barter there must be a double coincidence, which will rarely happen."

Marx said in the last of the 11 outlines of the outline on Feuerbach that "philosophers only interpret the world in different ways, and the problem is to change the world". Science and technology have always been harmonious but different. Science explains the world, but what is more important to mankind is that technology can transform the world as a methodology. Newton's theory can only be applied to ivory tower at first, and Watt's steam engine is a key turning point of human society.

Throughout the history of global development, there is no special significance between human beings and other organisms in the field of biology. Human biological disposition has not played a decisive role in the later human civilization. The main difference between humans and animals is the application of technology. Technological progress is the first driving force to promote the development of human society and undertakes the important task of human civilization progress. Based on technology, production, commerce, military affairs, politics, science, morality, culture and civilization will have their focus.

So far, human society has experienced three industrial revolutions, namely, the steam age, the electrical age and the information age. Steam engine, power, Internet and other major technological breakthroughs are part of the main driving force of global economic development, which are called "general purpose technologies" (GPT).

Today, the fourth industrial revolution represented by digital technology has swept. New technologies such as blockchain, 5g, artificial intelligence, Internet of things, cloud computing and other emerging technologies constantly burst out new business vitality. While enabling economic development continuously, they also affect human life in a multi-dimensional and deep level.

Table of Contents

1 *Industry background*

1.1 Public chain dispute

1.2 DAPP market pain points

2 *Introduction to JD Rockefeller Token Project*

2.1 Project introduction

2.2 Origin of JD Rockefeller Token

2.3 Core advantages

2.4 Whole field ecology

3 *Technical architecture and security system*

3.1 Design concept

3.2 Technical scheme

3.3 Security system

4 *Core team*

5 *Issuance of token*

6 *Strategic planning*

7 *Risk tips*

8 *References*

Public chain dispute

Public chain, as the underlying infrastructure for various DAPP applications. Only by building a high-speed and stable basic public chain, can the side chain and smart contract of various landing applications have the underlying operating system available, which is the soil and cornerstone for breeding killer applications. Scalability is the basic premise of public blockchain, especially when high throughput, high concurrency, stability and security are the key factors affecting user experience.

In 2019, scalability remains a big challenge for the public chain, as the TPS of mainstream blockchain platforms (including bitcoin, Ethereum, ripple, EOS, litecoin, Cardano, Tron and iota) are generally less than 1000 TPS. Most of these blockchain platforms cannot meet the speed and concurrency requirements of real-world applications.

In order to solve this problem, the blockchain industry is making the following attempts: first, large blocks, that is, to enhance the storage space of each block. This method has been tried in bitcoin. A block size of bitcoin is only 1MB. At the end of 2017, segwit2x increased the block size from 1MB to 2MB, but for security reasons, segwit2x finally cancelled the segwit2x hard fork; the second is that Off chain transaction, that is to add lightning network or side chain outside the main chain. Ethereum is trying to pay some Ethereum or bitcoin as deposit in advance, and then trade with other people through other methods off the chain; the third is the agent consensus agreement, that is, many people become super nodes and form small groups. EOS is trying to use this "parliamentary" consensus to generate blocks, and then broadcast the blocks to the whole network, so as to reach the consensus of the whole network.

However, these three attempts can not solve the contradiction between transaction speed, decentralization and security of blockchain.

Since the concept of defi came into being, there have been thousands of eligible blockchain projects, most of which are focused on the issuance of warrants, financing, trading and related financial instruments, and are mainly deployed in Ethereum public chain. In the second quarter of 2020, the total transaction volume of Ethereum DFI increased by 403% compared with the same period last year. The market value of several Ethereum defi projects has more than doubled in the second quarter.

Take makerdao, an automated mortgage lending platform in the lending platform, as an example. Established in 2014, makerdao is the most valuable project listed on the ETH network. The digital assets of users are pledged through smart contracts, and then the stable currency Dai of the same amount is lent to users.

Dai is a debt contract at the level of mortgage positions. All mortgage positions are subject to uniform excess mortgage rate requirements. If the market value of collateral falls, the issuer needs to replenish collateral or return some Dai to maintain the mortgage rate. If the mortgage rate is lower than the liquidation rate, it will trigger the liquidation of mortgage bond position, which is similar to the closing mechanism in equity pledge financing. If the collateral disposal is insufficient to cover the debt gap, MKR will issue additional shares and auction to obtain Dai, which is equivalent to the MKR holder as the ultimate loss bearer.

Similar to lending in traditional finance, there is also a problem of maturity mismatch in the field of cryptocurrency, that is, the contradiction between "the lender wants to repay the fund for a short time" and "the borrower wants to borrow for a long time". In traditional finance, the term mismatch is adjusted by banks, but it is difficult to solve the problem by algorithm in the field of cryptocurrency.

Compound is a decentralized lending platform. Depositors can transfer their own token into compound smart contract (coin deposit) and transfer the stored token from compound smart contract back to their address in the future. The borrower can borrow money from compound with the token deposited as collateral. The number and type of the token borrowed by the borrower and the token deposited by himself are inconsistent, but the excess mortgage rate should be met. If the borrower does not have enough collateral, the compound agreement will force the liquidation of the collateral.

However, the risk of compound platform is also obvious, because based on excess mortgage, the price of collateral fluctuates greatly. If it drops sharply, there may be insufficient collateral. According to the agreement, there are two ways to deal with it. One is to supplement the collateral, and the second is that the smart contract will clear the mortgage. Therefore, once the price drops sharply, whether it is the additional collateral or the disposal of collateral, the transaction will be conducted on the blockchain of Ethereum, which will lead to transaction congestion and make it difficult to clear the market asset risk.

JD Rockefeller Token proposed two important solutions for the application of defi loan. The first is to move towards the point-to-point lending mode, which matches the term of deposit and borrowing, and makes more upgrades on the basis of early ethland; the second is to dynamically manage the term of deposit and borrowing through algorithm.

At present, the total lock up volume of defi has exceeded US \$2 billion, but the whole market is still in the early stage of development, and it still faces problems such as public chain performance, social demand and security risks.

Throughout the DAPP market, there is still a huge pain point, that is, there is an embarrassing situation of "same but not at all", which is the so-called pain of lacking "chain" with currency but without chain.

At present, the consensus mechanism of DAPP must be consistent with the main chain (e.g. the current POW + POS of Ethereum). Therefore, it is inevitable that DAPP will adapt itself to the business logic and implementation scenarios. Therefore, most of dapps are mainly focused on decentralized transactions, as well as nurturing and gambling games based on transfer transaction scenarios. The application scenarios are very single.

What's more, due to the lack of basic service providers in Ethereum to reduce the threshold for app farmers to participate in DAPP development, the small stock of blockchain application development talents can not meet the development needs of geometric level growth, and the ecological diversity of the whole industry is seriously insufficient.

Introduction to JD Rockefeller Token Project

Project introduction

JD Rockefeller Token is a public chain based on dpos consensus mechanism. In the future, it will build a blockchain ecosystem covering "prism decentralized exchange + public Chain Wallet + profi products + blockchain cross-border e-commerce platform + diversified DAPP applications".

Similar to Ethereum, JD Rockefeller Token can be used by developers to develop applications and serve users by writing smart contracts. JD Rockefeller Token is also a blockchain development and application system jointly built and shared by all the people. It is committed to solving the problems of poor expansibility and difficulty in secondary development of the existing three blockchain basic networks of bitcoin, Ethereum and EOS due to their development languages.

JD Rockefeller Token uses Java language, which is more widely used and less difficult for secondary development, to develop the operating system, and encapsulates a large number of API interfaces for non professional blockchain developers to use, which greatly reduces the development of decentralized blockchain applications by ordinary developers, and greatly promotes the development of blockchain technology.

Aiming at the challenges of the current blockchain industry, JD Rockefeller Token has made a series of innovations in blockchain technology and concept, including the consensus mechanism based on the combination of pbft and dpos consensus mechanism, the concept and implementation of blockchain master contract, the application of decentralized wallet, the separation of transaction book and smart contract account book, etc Chain has become a bridge between the blockchain world and the real business world.

JD Rockefeller Token source

Prism means balance in Latin, which means balance of all things

Core advantages

JD Rockefeller Token supports millions of users

Applications like eBay, Uber, airbnb and Facebook need blockchain technology that

can handle tens of millions of active users every day. In some cases, applications may not work properly unless a large number of users are reached, so a platform that can handle a large number of users is critical.

JD Rockefeller Token is free of charge

Sometimes application developers need to be flexible to provide free services for users, users do not have to pay for the use of the platform. The platform that can be used for free will naturally get more attention. With enough user scale, developers and enterprises can create corresponding profit model.

Easy upgrade and troubleshooting

Applications based on JD Rockefeller Token naturally need to be able to support software upgrade during function iteration. All software may be affected by bugs. When a blockchain underlying platform encounters a bug, it needs to be able to fix the bug.

Low delay

Timely feedback is the foundation of good user experience. If the delay time exceeds a few seconds, it will greatly affect the user experience and seriously reduce the competitiveness of the program.

Serial performance

Some applications cannot be implemented by parallel algorithms because command execution must be sequential. Applications such as exchanges often need to handle a large number of serial operations, so a successful blockchain architecture needs to have strong serial performance.

Parallel performance

Large scale applications need to divide the workload between multiple CPUs and computers. JD Rockefeller Token can realize multi terminal parallel function.

Whole field ecology

JD Rockefeller Token public chain is a completely point-to-point "decentralized" network. Its design model makes it possible to get through the chain on and off the chain. By setting up a series of trusted data sources, the application can start the smart contract and intelligent application on the chain after a specific event occurs 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. The new blockchain architecture built by JD Rockefeller Token provides account, identity and license management.

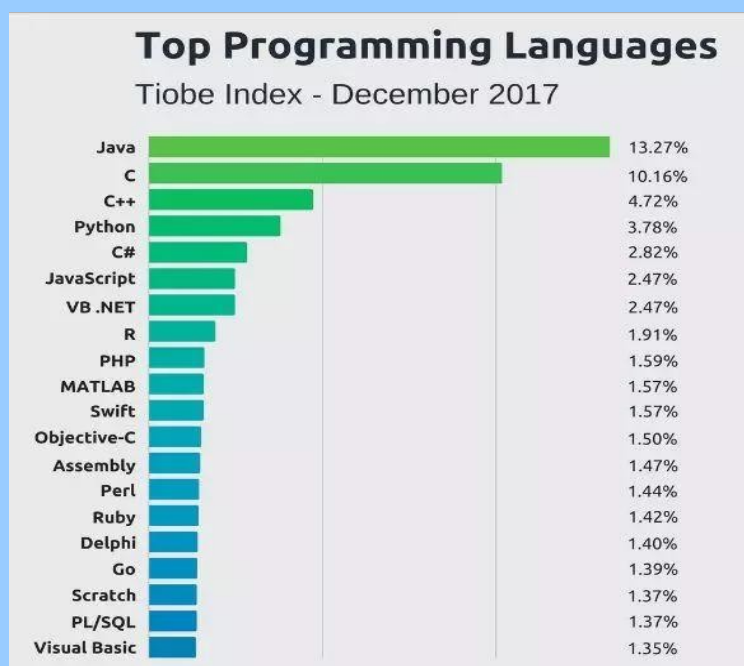
Technical architecture and security system

Design concept

Programming language is a formal language used to define computer programs. It is a standardized communication technique used to give instructions to computers. A computer language that allows programmers to accurately define the data that a computer needs to use and precisely define the actions that should be taken in different situations.

Programming language, commonly known as "computer language", has many kinds. Generally speaking, it can be divided into machine language, assembly language and high-level language. Every action and step that the computer does is executed according to the program that has been programmed in the computer language. The program is the set of instructions to be executed by the computer, and all the programs are written in the language we have mastered. Therefore, if people want to control the computer, they must send commands to the computer through the computer language. At present, there are two forms of general programming language: assembly language and high-level language.

Popular blockchain development language, development language popularity ranking:



Java language

Java is a portable "small C++" originally designed by sun for embedded programs. The idea of running small programs on the web really attracted a lot of people's attention, so the language rose rapidly. As it turns out, Java isn't just good for embedding animations on Web Pages - it's an excellent little language for complete software programming. "Virtual machine" mechanism, garbage collection and no pointer make it easy to implement reliable programs that are not easy to crash and do not leak resources. Although computer language is not the formal sequel of C++, Java borrows a lot of syntax from C++. It discards a lot of the complex functions of C

++ to form a compact and easy to learn language. Unlike C++, Java forces object-oriented programming. It is as difficult to write non object-oriented programs in Java as it is to write "hollow powder code" in Pascal.

The advantages of Java language: binary code can be transplanted to other platforms, programs can run in web pages, the class library contained is very standard and extremely robust, automatic allocation and garbage collection can avoid resource leakage in the program, and a large number of code routines on the Internet.

Among the three basic network development languages of blockchain, C++ is the mainstream, but it is recognized that the language with great difficulty needs a high level of technology to control. Go language has not been widely used, and there are still some shortcomings. As for the development languages of solid, LLL, serpent and web assembly, few people have heard of them. The complexity and high learning cost of these main network development languages and smart contract development languages have seriously restricted the development of blockchain applications.

As the most widely used development language, Java has been integrated into various systems of various industries. At the same time, Ethereum token and smart contract are the most widely used and mature. Using java language for development, completing the Ethereum standard smart contract mechanism, and building a simple and easy to understand blockchain technology development community can promote the rapid integration of blockchain technology into the existing industry. Based on the above reasons, JD Rockefeller Token chooses Java language to develop the main network. JD Rockefeller Token is a high-performance consensus algorithm ABFT based on the improvement of pbft algorithm in pure java language. JD Rockefeller Token main network implements the erc20 token standard of Ethereum [which will be extended to erc-827 standard in the future), and uses Java language as the development language of smart contract. Moreover, it encapsulates a large number of API interfaces for non professional blockchain developers to use, which greatly reduces the development of decentralized blockchain applications by ordinary developers, and promotes the development of blockchain technology faster.

Technical scheme

JD Rockefeller Token builds a community network with demand orientation, rewards data contribution and subcontracting to realize data structure, and creates a secure, efficient, traceable, data free and further developed data trading platform. It solves the above pain points systematically through data competition and data decentralization. In combination with the requirements of blockchain network and data value discovery and exchange, the architecture design of JD Rockefeller Token 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.

refined trading mode

Through the design of network mechanism, the transaction of data assets will be more refined.

Market oriented data pricing

Through the design of network mechanism, we can ensure that the market-oriented data pricing is more detailed.

Support high concurrency transactions

It supports high concurrent data exchange, and the laboratory network environment can reach million level, which will become the future massive artificial intelligence.

Support 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.

support derived 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 JD Rockefeller Token, supports access to Oracle network, and improves the function scope of smart contract.

Support cross chain blockchain services

It supports the access of blockchain services with mature solutions in data storage and computing power to JD Rockefeller Token.

Overall architecture

JD Rockefeller Token follows a mature six-layer technical architecture, which is divided into data layer, network layer, consensus layer, incentive layer, contract layer and application layer from top to bottom.

<div> <div>Bancor-Enabled Token Symbol: BANCOR</div> <div>Reserve Token: ETH (Ξ)</div> <div>Constant Reserve Ratio (CRR): 20%</div> <div>Initial Token Price: Ξ1</div> <div>Crowdsale Proceeds: Ξ300,000</div> <div>Tokens issued in the Crowdsale: 300,000</div> </div>								
Activity	ETH Received (Paid-out)	BANCOR Issued (Destroyed)	Effective Transaction Price	ETH Reserve	BANCOR Supply	BANCOR Market-cap	Current BANCOR Price	Price change
Post-crowdsale initial state				Ξ60,000	300,000	Ξ300,000	Ξ1.0000	
300 ETH converted to BANCOR	Ξ300	299	Ξ1.0020	Ξ60,300	300,299	Ξ301,500	Ξ1.0040	0.40%
700 ETH converted to BANCOR	Ξ700	694	Ξ1.0066	Ξ61,000	300,993	Ξ305,000	Ξ1.0133	0.93%
1302 BANCOR converted to ETH	Ξ(1,306)	(1,302)	Ξ1.0046	Ξ59,692	299,691	Ξ298,460	Ξ0.9959	-1.72%
100 ETH converted to the BANCOR	Ξ100	100	Ξ0.9966	Ξ59,792	299,792	Ξ298,960	Ξ0.9972	0.13%

Data layer

The data layer is the bottom data structure in the whole blockchain technology. It mainly describes the most basic physical form of the blockchain. It is a block + linked list data structure, including: blockchain data, hash function, Merkle number, asymmetric public private key data encryption technology, timestamp technology, etc.

Network layer

The essence of 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 services 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.

Consensus layer

Consensus layer encapsulates consensus algorithm and consensus mechanism, which enables highly dispersed nodes to reach consensus on the validity of block data 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.

At present, there are at least dozens of consensus mechanism algorithms, including proof of work (POW), proof of interest (POS), proof of entitlement (dpos), etc.

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.

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. If bitcoin is regarded as a global ledger, Ethereum can be regarded as a global computer. Anyone can upload and execute any application program, and the effective implementation of the program can be guaranteed.

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-mail or the app on the mobile terminal, etc. For example, DAPP applications of various blockchains currently built on public chains such as eth, EOS, Neo, etc., the future programmable finance and programmable society will also be built on the application layer.

Innovative consensus mechanism

The core concept of blockchain is consensus mechanism. Consensus among participants is the core of the whole JD Rockefeller Token blocknetwork. If there is no central organization, the participants of the blockchain also need to agree on the established terms. Edward Shils's "consensus concept" requires the following conditions: 1) the members of the group jointly accept the laws, rules and norms. 2) Members of the group unanimously approve the agencies that implement these regulations. 3) A sense of identity or solidarity so that members of the group recognize that they are equal in terms of consensus.

At present, the representative public chains in the blockchain industry are BTC and eth, whose transaction confirmation time is long, the throughput performance is low, and the bookkeeping confirmation mechanism which relies heavily on the competition of computing power has security risks.

JD Rockefeller Token consensus module algorithm is improved based on pbft algorithm and dpos node representative election rules, and realizes high performance robust

consensus algorithm JD Rockefeller Token BFT. Under the premise of ensuring the strong consistency of BFT system, the overall transaction throughput capacity and system stability of the system are improved, which can stably reach million TPS, and the transaction confirmation time is controlled within 3S.

Performance comparison between Ethereum and JD Rockefeller Token consensus mechanisms:

	Consensus mechanism of Ethereum (POW + POS)	JD Rockefeller Token (dpos) consensus mechanism
Performance (transaction processing TPS)	10-20/s	100000/s
Block generation time	15s	3 s

Dpos consensus mechanism

The dpos consensus mechanism adopted by JD Rockefeller Token is a reform of traditional mainstream public chain BTC (POW mechanism) and eth (POS mechanism). It provides a method of transaction processing and decentralized consensus protocol in trusted cryptocurrency network. The purpose is to reduce the waste of computing power and resource cost in POW based consensus mechanism.

The dpos consensus mechanism is somewhat similar to the board voting. In a decentralized system, the decision-making power is distributed to all the holders of coins. When the holders vote more than 51%, the decision is considered to be passed and the decision is irreversible. In this mechanism, there is an important role called representative. The representative is the node that generates blocks. If you want to be a representative, you must pay a certain amount of security money to ensure the credibility of the representative. Users have the right to elect representatives. Each user can vote for a trusted representative, and the top n representatives who get the most votes in the whole network have the right to produce blocks. The number of votes held by these n representatives is equal to the number of shares held by the node. These n representatives will produce blocks in turn according to the schedule.

If more than 51% of the stocks pass through the blocks, the blocks will be considered successful. For each block generated, they will get benefits from the transaction fees in the blocks, and these benefits will also be a kind of incentive mechanism to maintain online participation.

The actual price of a smart token is calculated as a function of the transaction size.

R - Reserve Token Balance

S - Smart Token Supply

F - Constant Reserve Ratio (CRR)

- T = Smart tokens received in exchange for E (reserve tokens), given R , S and F

$$T = S((1 + \frac{E}{R})^F - 1)$$

- E = Reserve tokens received in exchange for T (Smart tokens), given R , S and F

$$E = R(\sqrt[F]{1 + \frac{T}{S}} - 1)$$

In the dpos consensus mechanism, the reliability of the representative is particularly important. When the holder selects the representative, he can see the error rate of the representative block, so that he can correctly select the representative. On the other hand, representative blocks are generated in turn according to time. Therefore, when a representation error generates a block, as long as it is not recognized by 51%, then the block will be generated by other representatives in the next time period. It can be said that dpos consensus mechanism is more effective than POS consensus mechanism.

Dpos consensus mechanism is a consensus mechanism to get rid of mining in a real sense. However, the mechanism relies on the votes of all participants. When the participation is not enough, the representatives tend to be concentrated in the hands of the holders who hold a large number of votes in the whole network, thus losing the characteristics of decentralization. However, on the other hand, the use scale, frequency and area of the third-party application platform are also discussed. The hot degree of block chain establishes a strong user group, thus reducing this risk to the minimum.

PBFT algorithm

BFT (Byzantine fault tolerance), namely Byzantine fault tolerance, is a fault-tolerant technology in the field of distributed computing. Byzantine fault tolerance comes from Byzantine general problem. In 1999, the paper "fault tolerance" was proposed by practical Byzantine, i.e. probabilistic byfault.

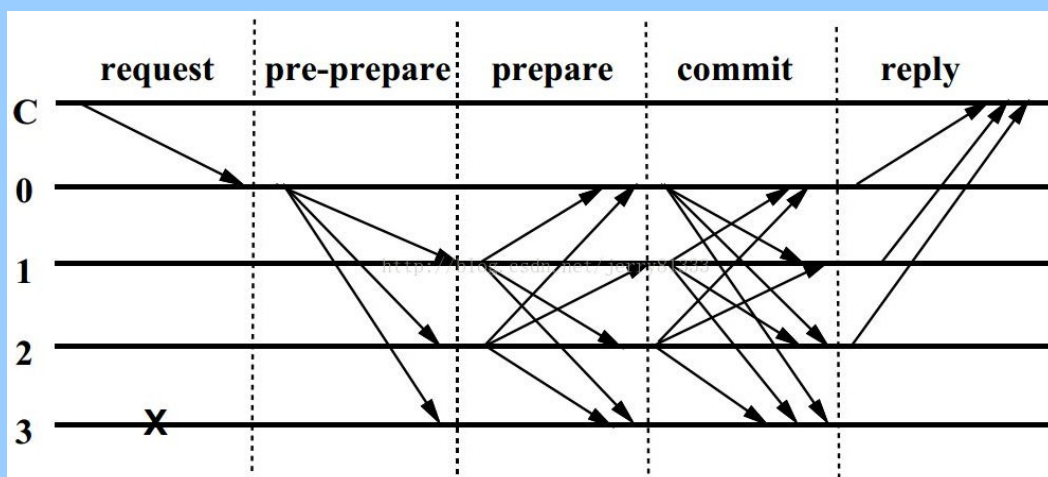
PBFT algorithm can work in asynchronous environment, and solve the problem of

low efficiency of the original Byzantine fault-tolerant algorithm through optimization. The complexity of the algorithm is reduced from exponential level to polynomial level, which makes Byzantine fault-tolerant algorithm feasible in practical system application, and has been widely used. PBFT algorithm can guarantee safety and liveness at the same time when the number of failed nodes is less than $1/3$. PBFT algorithm uses cryptography related technologies (RSA signature algorithm, message verification coding and digest) to ensure that the message passing process can not be tampered with and destroyed.

PBFT is a replication algorithm of state machine, that is, service is modeled as state machine, and state machine replicates in different nodes of distributed system. Each copy of the state machine keeps the state of the service and implements the operation of the service. The set of all copies is represented by the capital letter R , and each copy is represented by integers from 0 to $|R| - 1$. For the convenience of description, it is usually assumed that the number of failed nodes is f , the number of whole service nodes is $|r| = 3F + 1$, and F is the maximum number of copies that may fail. Although there can be more than $3F + 1$ copies, the additional copies do not improve reliability except for reducing performance.

All copies operate in a rotation called a view. In a view, one replica acts as the primary node and the other replica nodes act as the backup nodes. Views are integers that are numbered consecutively. The master node is calculated by the formula $P = V \bmod |R|$ where V is the view number, P is the copy number, and $|R|$ is the number of replica sets. When the master node fails, the view rotation process needs to be started.

The implementation process of PBFT algorithm is as follows:



C is the sending request end, 0123 is the server, and 3 is the server of downtime. The specific steps are as follows:

Request: the requester C sends a request to any node. Here is 0

Pre prepare: after receiving the request from C, server 0 will broadcast and spread to 123

Prepare: 123, record and broadcast again after receiving, 1 -> 023, 2 -> 013, 3, unable to broadcast due to downtime

Commit: 0123 node in the Prepare phase, if it receives more than a certain number of the same requests, it enters the commit phase and broadcasts the commit request

Reply: 0123 node will give feedback to C if it receives more than a certain number of the same requests in the commit phase

Byzantine fault tolerance can accommodate nearly 1 / 3 of the error node errors. IBM created hyperledger uses this algorithm as a consensus algorithm.

PBFT algorithm has high transaction throughput and throughput, high availability and easy to understand. At the same time, it also has the following disadvantages:

The computational efficiency depends on the number of nodes participating in the protocol. Because each replica node needs to synchronize with other nodes, the performance will decline rapidly with the increase of nodes. However, it can have good performance in the case of fewer nodes, and the probability of bifurcation is very low. It is not suitable for blockchain with too many nodes and poor scalability.

The system node is fixed and can't deal with the open environment of public chain. It only applies to alliance chain or private chain environment.

PBFT algorithm requires the total number of nodes $n \geq 3F + 1$ (where f represents the number of bad nodes). The number of failure nodes in the system should not exceed 1 / 3 of the whole network nodes, and the fault tolerance rate is relatively low.

The number of nodes in PBFT algorithm is fixed, and the node identity is determined in advance, so it can not be added or deleted dynamically. It can only be used in the scenario of alliance chain or private chain with fixed number of nodes. PBFT has been applied in many scenarios. In blockchain scenarios, it is generally suitable for private chain and alliance chain scenarios with strong consistency requirements. However, if dpos node representative election rules can be combined, it can also be applied to

public chain, and the Byzantine fault tolerance problem can be solved in an untrusted network.

JD Rockefeller Token BFT algorithm

According to the principle and advantages and disadvantages of PBFT algorithm, we have developed our own dpos node representative election rules, formed JD Rockefeller Token BFT algorithm and applied it to JD Rockefeller Token public network. The election rules of our node representatives are as follows:

Proxy: a proxy is an account that can be used to vote and can be a verification node. Any JD Rockefeller Token user can apply to become an agent (it needs to consume PRI, and the hardware requirements of the computer can meet the minimum requirements of the node).

Validation node: a validation node is a proxy that allows mining blocks and validating BFT protocol transactions. To be a proxy, you need to get enough votes to get into the top 51. Every 200 blocks, swipe the verification node again. The verification nodes that do not participate in mining blocks and verifying BFT protocol transactions will become ordinary agents, and other qualified new agents will be transformed into new verification nodes. The PRI obtained by the verification node mining blocks is used as the reward of the verification node. At the same time, it can also dock with the mine pool and share the PRI with his voters.

Dpos has been running on bit stocks and steel for many years, with a transaction speed of over 1000 transactions per second and a short block out time; on the EOS test network, the block out time is shorter. However, EOS runs on the basis of 21 super nodes. The hardware and software configuration of the node server required by EOS is extremely high, and ordinary users can not participate in it. In order to truly decentralize and let more people participate, we suggest that the node server should reach 8GB memory, dual core CPU and 100 Mbps bandwidth. At the same time, the deployment test of the test environment uses 3s of block out time and transaction confirmation time of 3S to generate a block, so the system can run stably.

The fastest transaction confirmation time of bitcoin is 10 minutes, and the outgoing block time of Ethereum is 15s. By default, Ethereum needs 15 to 30 confirmations, that is, the confirmation time from 3:45 to 7:30 after the transaction is online. The block out time of EOS is 0.5s. After the transaction is broadcast to the blockchain, it needs two rounds of node confirmation (the longest time is about 3 minutes, 336 blocks, and then a transaction will become irreversible.)

The ABFT consensus has six stages. On each block, the verifier will go through these stages to forge the next block. The following time is set with the minimum standard node server.

Smart contract

Smart contract is a new technology that can only be realized through blockchain. Ordinary, standard contracts cover the terms of the agreement between the parties, and are often enforced by law; smart contracts are digital, stored in the blockchain, and use encrypted code to enforce the agreement. In other words, smart contracts are just software programs that, like all programs, execute exactly as the programmer intended. Smart contracts are like programming applications: "as soon as they appear, execute them." Basically, through mathematical calculation, smart contracts can negotiate the terms of the agreement, automatically verify the performance, and even implement the agreed terms, all of which do not need to be approved by the central organization. Smart contracts make intermediaries such as notaries, agents and lawyers almost meaningless.



The concept of smart contract was originally conceived by Nick Szabo, a computer scientist and cryptographer, in 1993. In a 1994 article, Nick wrote: "the overall goal of a smart contract is to meet common contractual conditions (such as payments, liens, confidentiality, and even enforcement), minimizing anomalies and the need for trusted intermediaries. Related economic objectives include reducing fraud losses,

arbitration and enforcement costs, and other transaction costs. Some of today's existing technologies can be regarded as rough smart contracts, such as POS terminals and (credit cards), electronic data interchange (EDI), and agoric allocation of public network bandwidth.

Although the smart contract only came to life when bitcoin was born in 2009, Ethereum fully accepted it, making it possible to execute and store smart contracts in its distributed ledger. Ethereum's platform is designed to execute smart contracts, making transactions possible and impeccable. In many ways, smart contracts are the cornerstone of all blockchain technologies. In addition, many emerging blockchain startups rely on the revolution that smart contracts are expected to create.

Just as there is a network of nodes to verify bitcoin transactions, smart contracts also use node networks to verify that all aspects of the protocol have been completed. They don't need middlemen like lawyers to verify the existence of these aspects. The nodes and the code in the smart contract can verify it. This also makes smart contracts transparent and traceable to all parties involved. As a result, trust between the parties is no longer controversial. Sometimes lawyers will still be needed, but most of the work has been done.

Finally, because smart contracts are embedded in a blockchain where all data is stored in a decentralized and distributed manner, no one can control the funds until the contract is fulfilled. This money is usually the local cryptocurrency of the

Blockchain, just like Ethereum's Ethereum.

JD Rockefeller Tokenvm (JD Rockefeller Token virtual machine)) is the execution environment of smart contract, which provides intelligent control logic for application layer, combines with high-level language parsing and transformation, and flexibly supports basic application of virtual machine; external interface of virtual machine is realized through customized API operation, which can flexibly interact with ledger data and external data.

JD Rockefeller Token's intelligent contract execution engine JD Rockefeller Tokenvm (JD Rockefeller Token virtual machine) adopts the modular and pluggable design method. Firstly, we develop JD Rockefeller Token JVM which supports Java language, and then we will provide JD Rockefeller Token EVM which supports solid language. JD Rockefeller Token JVM is to maximize the accumulation of smart contract technology and experience of open source community, and improve the reusability of smart contract, and learn from EVM virtual machine of Ethereum. The implementation of JD Rockefeller Tokenvm'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 mechanism, it provides a high-performance and safe execution sandbox for the implementation of native Java

smart contract.

JD Rockefeller Token achieves more thorough decentralization while greatly improving TPS. Compared with the existing generation 1, 2 and 3 generation public chain TPS, BTC's TPS is only 7 times / s, ETH's TPS is 30 times / s, EOS's is only 3900 times / s, and JD Rockefeller Token's TPS has reached an amazing million times / second, fully reaching the commercial level of application. Its consensus mechanism is also the fairest and safest. The code is all original written, not some public chain's Ctrl + V.

JD Rockefeller Token will really introduce DAPP in the future. At present, the mainstream public chain is difficult to expand and lack of interoperability, so self built modules are needed to develop DAPP on the blockchain. The underlying public chain is the basis for the application of blockchain technology. If DAPP finds that a certain underlying public chain has a better technical system, the probability of its settlement will be greatly improved. According to the technical director of JD Rockefeller Token team, JD Rockefeller Token has made a lot of technical investment in DAPP to solve the above problems and open up a new way for DAPP introduction of blockchain system in the future. While compatible with the current mainstream public chain contracts (erc20 contracts, etc.), JD Rockefeller Token has a great degree of 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", "de duplication encryption" and "mass storage" technologies. JD Rockefeller Token turns these technologies into reality one by one in itself, creating a precedent in the public chain industry.

JD Rockefeller Token ecology greatly improves the enthusiasm and currency holding ability of community users, which provides community initiative for JD Rockefeller Token to promote commercial applications in the future. At the same time, it has a very simple one button token function. Compared with gas consumed by Ethereum, such as expensive price and complicated contract issuing, JD Rockefeller Token has extremely low fuel cost.

JD Rockefeller Token implements commercial application. The introduction of commercial applications such as e-commerce, payment, logistics, games, industrial robots, information traceability, etc. will promote the extension of blockchain technology to traditional industries and drive the transformation and upgrading of traditional industries, so as to enjoy the technological dividend brought by JD Rockefeller Token.

Decentralized trading environment. The decentralized trading environment established by JD Rockefeller Token enables users' assets to be decentralized and trusteeship, so that all transactions are on the chain, which can not be tampered with, open and

transparent. This decentralized transaction is not an exchange, but a token established by commercial applications. Through on-chain exchange, transactions are completed, and the effective rights of commercial circulars are completed through contracts, and a series of commercial activities are launched.

In short, JD Rockefeller Token is equivalent to providing a better system platform than the existing public chain network for the application of blockchain technology to all walks of life. Imagine, with a more perfect and advanced public chain system like JD Rockefeller Token, the application prospect of its blockchain technology to commercialization will be broader, and the holding value of JD Rockefeller Token is immeasurable.

It can be said that in the whole blockchain industry, the layout of the underlying public chain is just in its infancy. For potential public chains like JD Rockefeller Token, which focus on ecological construction, everything is possible in the future.

Flexible cross chain mechanism

Prism Through a series of targeted collaborative smart contracts, asynchronous communication, state machine and hash locking technology, chain realizes a set of general flexible cross chain mechanism, breaks through the communication bottleneck of each blockchain system, and makes all kinds of digital assets interconnected. Appropriate cross chain collaboration mechanism can effectively ensure the consensus and value between internal parallel chains and other public chains Effective and reliable delivery.

Cross chain technology includes two parts: one is the interconnection between JD Rockefeller Token and external chain. JD Rockefeller Token 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 JD Rockefeller Token platform. JD Rockefeller Token also provides a more complex smart contract to support the interconnection and interworking between other chains. Due to supporting two different types of other chains, the smart contract combines with the relay chain to complete the interconnection and interworking 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 JD Rockefeller Token as a communication to pay for the transaction cost, thus motivating the participants at each intersection.

JD Rockefeller Token cross chain communication is implemented through an adapter, which creates a compatible block header.

JD Rockefeller Token designs a hierarchical side chain mechanism to solve the problem of cross chain transactions matching the generation speed of different chain blocks. 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 the cross chain transactions of the same layer.

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

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.

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, JD Rockefeller Token adopts multi chain parallel structure.

Parallel multi main chain mechanism: JD Rockefeller Token can lead to multiple main chains. Each main chain is responsible for special business fields, which are independent and interrelated. The coupling between main chains is relatively small. It can give full play to the advantages of parallel processing, introduce the storage strategy for process blocks, and archive the overdue data in history, so as to improve the system processing efficiency. Multi Chain parallel solution to different problems.

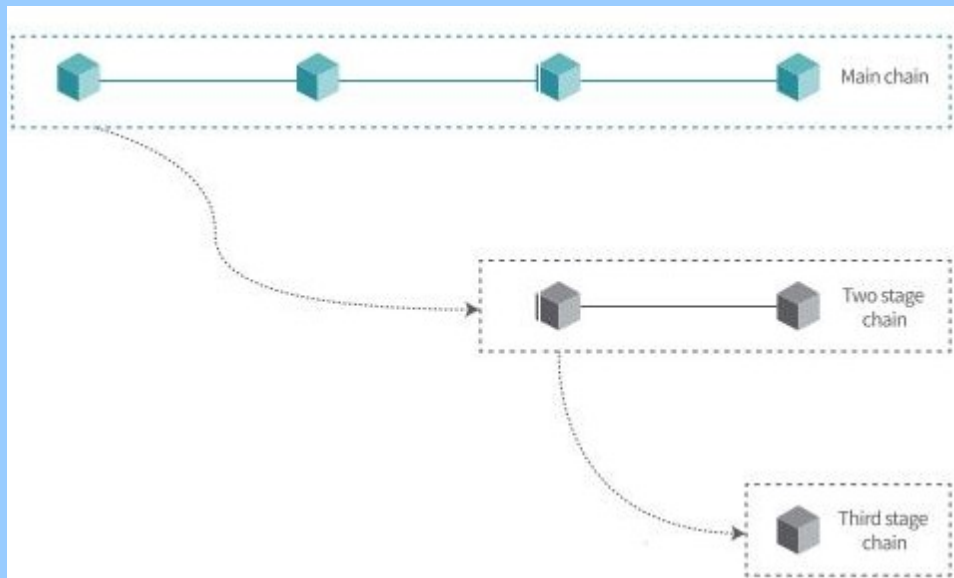
Parallel side chain scheme

In JD Rockefeller Token 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 contain the block header information of JD Rockefeller Token main chain.

In the face of some main business chains, the transaction records in the block can lead to the side chain as required. JD Rockefeller Token introduces side chain scheme, and each side chain can operate in parallel. That is, each application can set up a side chain independently. JD Rockefeller Token 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.

In the side chain system, the side chain can also have its own side chain, but it must follow the consensus inheritance relationship from top to bottom. The sub chain needs to inherit the consensus of all the superior chains and synchronize the messages of all the superior chains. However, the performance, security and message data service of the shared services can also be guaranteed by the common recognition and system of the main chain or other parent chains. 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.

JD Rockefeller Token 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 JD Rockefeller Token public chain, JD Rockefeller Token itself 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 JD Rockefeller Token infrastructure.

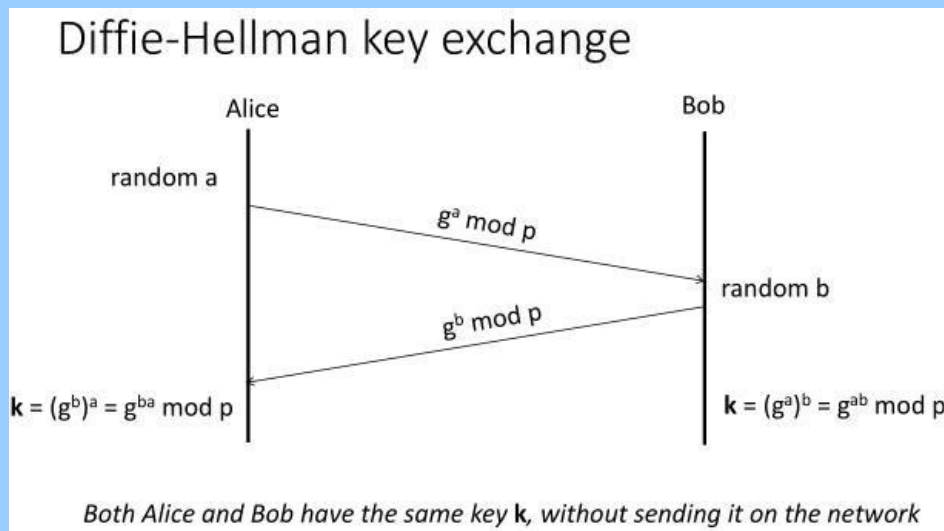
Safety system

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.

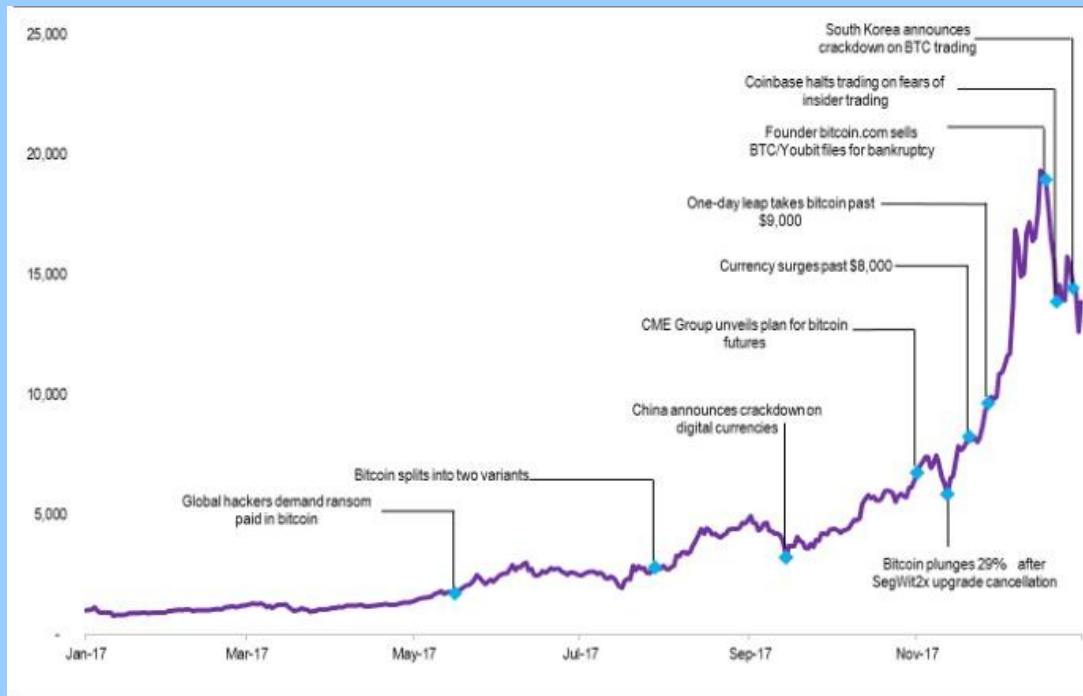
Elliptic curve Diffie – Hellman key exchange (ecdh) is an anonymous key agreement protocol. Under this protocol, the two sides establish a secure common encrypted data in an insecure channel by using the pair of public key and private key established by elliptic curve encryption through Diffie Hellman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

JD Rockefeller Token uses elliptic curve encryption algorithm to generate a key pair. The key pair 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.



*The private key K is a 256 bit binary number randomly selected from 0 to (slightly less than). For convenience, it is generally represented by 64 bit hexadecimal digits. Public key can be calculated from private key by elliptic curve algorithm: $k = K * G$, which is an irreversible process. G is the generating point in elliptic curve algorithm.*

The data signature algorithm based on the public-private key pair generated by elliptic curve encryption algorithm is called elliptic curve digital signature algorithm. The signature key is the user's private key, and the signed "information" is the data uploaded or updated by the device. The formula is as follows:



When users send or update data to the chain, they sign the data with their own private key, and publish the corresponding public key at the same time. Other nodes verify the signature according to the data sent or updated and the public key published by the device. Only the owner of the private key that can generate this public key can generate a specific signature for the message to be sent. Thus, it can be verified that the data is sent by a device, and the device cannot tamper with the information sent.

Proxy re encryption

Proxy re encryption (English: proxy re encryption) is a key conversion mechanism between ciphertexts. The whole process of ciphertext transmission involves three subjects: the authorized person, the agent and the authorized person. The authorized person can use his private key to decrypt the ciphertext encrypted with his public key, but he cannot share the encrypted content with the authorized person, because the authorized person does not have the authorized person's private key. Proxy re encryption solves the problem of private key owner (authorized person) sharing ciphertext with others.

Proxy re encryption is to entrust a trusted third party or a semi honest agent to convert the encrypted ciphertext encrypted by his public key into one that can be decrypted by the private key of the other party, so as to realize password sharing. In the real world, most of the companies that provide computing services have low credibility. The scientific solution is to encrypt and put them on the cloud to obtain the ciphertext form. However, we want the other party who is willing to share the secret to obtain the plaintext content of the ciphertext. That is, the encrypted

ciphertext with our public key can only be decrypted by our private key, and can be decrypted by converting it into the private key of the other party . This process is proxy re encryption.

The authorized person uses his private key and the authorized person's public key to generate the re encryption key through the re encryption key generation algorithm, and gives the key to the agent. After receiving the ciphertext message from the authorized person, the agent re encrypts the ciphertext through the re encryption key. In this process, the agent cannot decrypt the ciphertext. Then the agent sends the re encrypted ciphertext to the authorized person. The authorized person decrypts the ciphertext with his private key. The whole proxy re encryption scheme involves the following algorithms:

Key generation algorithm: the algorithm generates public key / private key pairs for users.

Re encryption key generation algorithm: given the private key of the authorized person and the public key of the authorized person, the algorithm can generate the re encryption key.

First layer encryption algorithm: given the public key and plaintext of the authorized person, the algorithm generates the first layer ciphertext. This layer ciphertext cannot be further converted.

Second layer encryption algorithm: given the public key and plaintext of the authorized person, the algorithm can generate the second layer ciphertext. This layer ciphertext can be further transformed into the first layer ciphertext by re encryption algorithm.

Re encryption algorithm: given the authorized public key and the second layer ciphertext, the algorithm can generate the first layer ciphertext by using the re encryption key.

First layer decryption algorithm: given the first layer ciphertext sent to the authorized person and the authorized person's private key, the algorithm can decrypt the plaintext.

Second layer decryption algorithm: given the second layer ciphertext and the authorized person's private key, the algorithm can get the plaintext.

The correctness of the proxy re encryption scheme requires that for any condition, any plaintext and any valid key pair, the following equation can be obtained:

Non interactive zero knowledge proof

Zero knowledge proof was proposed by S. Goldwasser, S. Micali and C. Rackoff in the early 1980s. It means that the prover can make the verifier believe that a certain conclusion is correct without providing any useful information to the verifier. Zero knowledge proof is essentially an agreement involving two or more parties, that is, a series of steps that two or more parties need to take to complete a task. The prover proves to the verifier and makes him believe that he knows or owns a certain message, but the proving process cannot disclose any information about the proved message to the verifier.

Open source fog computing framework

Fog computing was named after Steve Bellovin of Columbia University in New York. His purpose at that time was to use "fog" to block hackers. Later, Cisco officially proposed for the first time, giving new meaning to fog calculation. Fog computing is a distributed computing infrastructure oriented to the Internet of things, which can extend the computing power and data analysis applications to the "edge" of the network. It enables customers to analyze and manage data locally, so as to obtain real-time insights through connecting the network.

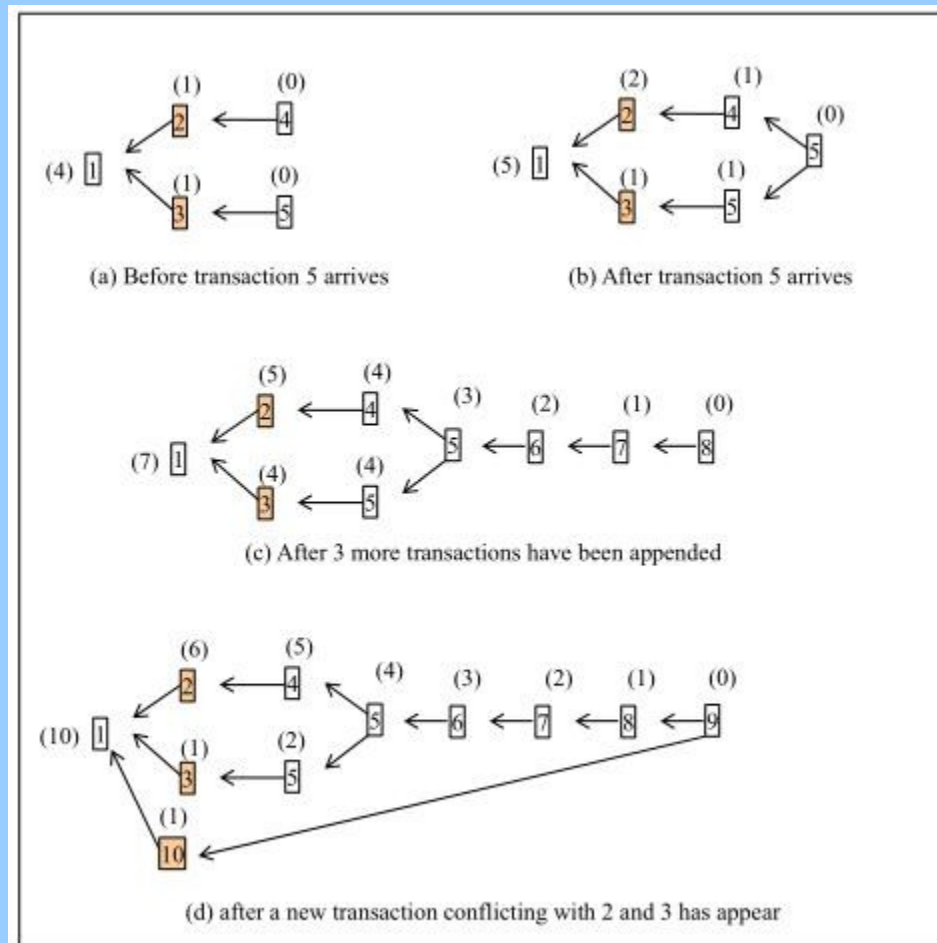
In 2012, Salvadoran et al. Proposed in an article on cloud data security, by using false information as bait, "catch" the secret "mole", and then achieve the purpose of protecting users' real information. Unlike cloud computing, which saves all data, data processing and applications in the cloud, fog computing distributes them in the devices on the edge of the network.

In the cloud server Between IOT and Internet of things (IOT) devices, network devices (routers, mobile phones, switches, set-top boxes, proxy servers, etc.) or special devices are used to provide computing, storage and network communication services, which makes data and computing closer to terminal devices, thus reducing the computing and storage overhead of cloud servers, and improving the response speed and network bandwidth of application systems. The name "fog computing" is because fog is closer to the ground than clouds. Fog computing does not have strong computing power, because the computing power is provided by peripheral and scattered computing equipment.

Fog Computing mainly uses the devices in the edge network, and the data transmission has very low delay. Fog computing has a vast geographical distribution, which is a large-scale sensor network with a large number of network nodes. Fog computing has good mobility. Mobile phones and other mobile devices can

communicate with each other directly. The signal does not have to go around the cloud or even the base station to support high mobility.

In JD Rockefeller Token, the fog computing part adopts openfog open source part. Openfog can meet three basic requirements: low latency, maintaining user privacy, and multi-channel link.



Core team

The team behind substratum is an American software developer, which has been one of the fortune 100 companies in the past 10 years. Companies such as Apple, Facebook, Disney, HP and other companies, architecture, development and deployment of software. Case. We have the necessary experience to create solutions on this scale.

Our team has 22 members, including developers, designers, architects and project managers. Most of them Team members have been working together for more than 13 years. We are a stable and active development team for Fortune 100 Strong company set up project.

Justin Tabb

He graduated from the Federal University of technology in Zurich, majoring in management economics. He was a Chartered Financial Analyst of diasoft, a Russian financial technology giant. Since 2014, he has deeply participated in the operation of several internationally famous blockchain projects such as Eth and EOS, and has mature operation and management experience in traditional finance and blockchain finance. He has been the global eco CEO of JD Rockefeller Token since 2019.

Abram Cookson

Graduated from the Federal University of technology in Zurich He majored in computer and information science. He once served as an information security engineer of diasoft, a Russian financial technology giant. In 2014, he joined the blockchain industry together with Mr.

Issuance of token

Release plan

Project Name: JD Rockefeller Token Project abbreviation: pri

number of warrants to be issued: the total number of warrants to be issued is constant at 8000000, and will never be issued again.

receiving currency: JDST, which is a decentralized digital asset issued based on JD Rockefeller Token technology.

Token distribution

JDST is a fuel consumption token issued by prism foundation and applied to the public chain. Its distribution ratio is as follows:

4000000 JDST: for mining and ecological construction

800000 JDST: for foundation holding

500000 JDST: for airdrop award and public chain fund maintenance

2700000 JDST: for private equity

Strategic planning

The project was established in November 2018

Formulation of decentralized public chain ecological scheme in January 2019

Preliminary construction of product concept and logic in February 2019

Start infrastructure development in March 2019

Technical Framework infrastructure completed in March 2020

In April 2020, mobile wallet and blockchain browser will be developed

Main network test in May 2020

Technical white paper released in June 2020

Open source code in July 2020

The project will be launched in August 2020

Q4 will log into the global mainstream digital asset trading platform in 2020

In 2021, the first batch of games and encrypted social DAPP launched in Q1

Q2 prism goes online in 2021

In the second half of 2021, we will build a whole field of ecology, landing in many fields, such as defi, cross-border e-commerce, payment, games, short video, logistics and information traceability

Risk tips

This document is only for the purpose of conveying information and does not constitute an opinion on buying or selling JD Rockefeller Token shares or securities. No more than 120 securities may be offered under the relevant laws or regulations. This document does not constitute any investment advice, investment intention or solicitation of investment in the form of securities. This document does not constitute, nor is it understood to be, any offer to buy or sell, or any invitation to buy or sell any form of securities, nor is it any form of contract or promise. JD Rockefeller Token clearly states that relevant interested users clearly understand the risks of JD Rockefeller Token. Once investors participate in the investment, they mean that they understand and accept the risks of the project, and are willing to personally bear the corresponding results or consequences for this. JD Rockefeller Token team clearly states that it will not bear any direct or indirect losses caused by participating in JD Rockefeller Token project, including:

Because of the economic loss caused by user transaction operation;

Any error, omission or inaccurate information of the company shall be understood by the individual;

The loss caused by individual transaction of various blockchain assets and any action caused by it.

PRI is a cryptocurrency based on JD Rockefeller Token. We can't guarantee that pri — will increase in value. In some cases, the value of pri — may decline. People who do not

use their JD Rockefeller Token correctly may lose the right to use JD Rockefeller Token, or even their pri. JD Rockefeller Token is not a kind of ownership or control right. Controlling JD Rockefeller Token does not mean ownership of JD Rockefeller Token or JD Rockefeller Token application. JD Rockefeller Token does not grant any individual any right to participate in, control, or make decisions about JD Rockefeller Token and JD Rockefeller Token application.

Risk tip: many digital asset exchanges are closed due to security issues. We attach great importance to safety, but there is no absolute sense of 100% safety in the world, such as various losses caused by force majeure. We are committed to doing everything possible to ensure the safety of your assets.

Reference

Nick Szabo. Formalizing and securing relationships on public networks. First Monday, 2(9), 1997

Back, "Hashcash-a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>. 2002

Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013

Gavin Wood. Ethereum: A Secure Decentralized Generalised Transaction Ledger. 2018

W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>. 1998

Andreas Antonopoulos: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2014

Sheldon M. Ross. A First Course in Probability. 2009

Nash John. "Non-Cooperative Games" The Annals of Mathematics. 1951

Schlegel, H.: Reputation Currencies. Institute of Customer Experience.

Marko Vukolić: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. 2016

Adam Back, Matt Corallo: Enabling blockchain innovations with pegged sidechains

Vitalik Buterin: Zk-SNARKs: Under the Hood

Eli Ben-Sasson: Zerocash: Decentralized Anonymous Payments from Bitcoin

Petar Maymounkov: Kademlia: A Peer-to-Peer Information System Based on the XOR Metric

Everett Hildenbrandt: VM: A Complete Semantics of the Ethereum Virtual Machine

L. LamPoRt, Constructing digital signatures from a one-way

function, Technical RePoRt SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.

"Winternitz one-time signature scheme" <https://gist.github.com/karlgluck/8412807#comment-1258433>