Pointnity Network

High SpeedCompatible Extensions, interactive collaboration across the chain to the center of the operating system

Draftvl.0

1. Text

Block chain is in the original Bitcoin as a carrier to create a new kind of technology under, it is a promising technology. For tracking the distribution of ownership of digital assets. The technology is designed to allow a continuous process in a series of block trading agree that these transactions can be invoked in exchange for assets the function of the contract. These ledgers are distributed by the miners do not have specific permissions composition.

For distributed computing, which seems to be a typical application of state machine replication. When copying the classical state machine, each command (or operations) can be invoked at any time and by any process applied to the state machine, the processing target block chain expression is added to the data agree in the next block, and going to state copy the target machine.

However, one of the main differences between the chain and the block state machine replication relationship between the consecutive negotiation embodiment consistent. Block chain needs of each case of inconsistency is deleted (about a subtle and before). More specifically, block, it must be explicitly included in the final piece of information pointing to the original connection to the block chain. This is a typical use of a hash function having an elastic collision, when applied to the contents of one block, the block hash output. Identifying consensus instance number of the proposed decision block X must be embedded in the instance number. In view of this chain block is a block of new technological innovations set of computer technology, subvert the traditional Internet.

Block chain development process:

Block chain technology came into being in the earliest prototype of Bitcoin project. As a distributed computing network behind Bitcoin, there is no centralized management, Bitcoin network has been running steadily nearly eight years, to support a huge transaction. No serious flaws. Identifying descriptive literature first block chain is a bit coins, electronic cash system is a point to point network by name (Nakamoto) written, but it is focused on the bits token system. In fact, there are chain block, which the chain block is described as a historical record for bitcoin trading account, there is no clear definitions and concepts.

More broadly, the block chain is a decentralized recording technology. Nodes participating in the system may not belong to the same organization, does not need to trust each other; data block chain is maintained by all nodes. Each node can be involved in maintaining the copy, and get a copy of the complete record. Compared with traditional accounting methods, its features include:

Support the growth of the chain can add records, and records can not be tampered occurs;

Decentralization, more focused, there is no centralized control, and can reach a consensus, as far as possible to achieve a fair distribution;

Encryption mechanisms to ensure that the transaction can not deny and undermine the protection of user information and record as much privacy. More importantly, the contract can be smart with combined transaction block chain, to provide a more flexible functionality of the contract, it already supports simple script calculation. To perform more complex operations. This may be extended beyond the block chain has the meaning of pure data recording points and actually has "pervasive computing".

1.1 blocks and even the value of:

A typical modern enterprise, the merchant by completing negotiations and execution of transactions in the course of the contract. Block chain adept at how to manage contracts and ensure the smooth implementation of the contract. Characteristic block chain varies according to the type and application scenarios.

In terms of technical characteristics, the block chains are typically considered:

- distributed fault-tolerant: the network is very strong, one-third of the abnormal state of the fault-tolerant nodes.
- Non-tampering: consistent data submitted is always there, can not be destroyed or modified.
- Privacy: Password guarantee that unauthorized data access, but can not be resolved.

1.2 block chain challenges:

The key technologies and challenges, from a technical point of view, the block chain involves a variety of fields, including distribution, warehousing, cryptography, psychology, economics, game theory, network protocols and so on.

- How to prevent transactions from being tampered?
- How to prove the identity of the transferee?
- How to protect the privacy of both parties?

Password exactly is an effective means to solve these problems provides. Traditional solutions include hashing algorithm, encryption and decryption algorithms, digital certificates and signatures (blind signature, the application of the block chain technology could stimulate further development of cryptography, including random number generation, the strength of the security, encryption and decryption performance, as well as new technologies such as quantum computing, and so on, the RSA algorithm can not provide adequate security, which will depend on breakthrough mathematical sciences and the further development of a new generation of computing technology appears.

1.2.1 Distributed Consensus

This is an old topic, the core is how to solve this change is consistent on the network, is a well-recognized, and this information is confirmed. Big difference between public anonymous scenes of this problem and those with rights management. In Bitcoin block chain, taking into account the worst case scenario in a public guarantee of anonymity. "Workload proven to work side 〃 to avoid malicious data corruption. Probabilistic model and to ensure that the last one is legitimate longest chain.

In addition, there Possum disabled organization and Casper, secured by the equity. These algorithms are based on the economic interests of the game. Let malicious participants lost their economic interests, so as to ensure the cooperation of most people. At the same time, it must be confirmed by generating a plurality of blocks and probability assurance. Blockchain broader support more consensus mechanism, including the classic Byzantine algorithm, which can solve the problem of uncertainty. Issue of consensus will be of great academic value of research focus for a long time. The main indicators include fault-tolerant nodes and the convergence speed ratio. prisoner of war (POW) and other algorithms allow more than half of the non-cooperation of the nodes and PBFT less than a third than the theory of non-cooperative node to ensure the stability of the network.

1.2.2 Performance

How to improve transaction throughput and reduce transaction confirmation delay. Currently, the open bit chain block credits can only support about 7 bits per block credits average throughput. Secure transaction confirmation time is one hour. Just make sure charges are broadcast to the network and transaction services, there is a high probability that the transaction will eventually be packaged into blocks. Unlike conventional distributed system, the processing performance of the chain block can not be simply extended by increasing the number of nodes. In fact, depending on the processing power of a single node to a large extent. Hardware-assisted encryption and decryption functions will be the core element of node performance. Currently,Open Source block chain itself has achieved a normal configuration at the platform level, a single client with hundreds of transactions per second throughput, optimistic forecasts will soon break through thousands of times per second baseline. But there are still tens of thousands per second peak there is a big gap in the existing securities trading system. In addition, from design and engineering platform deployment, there are some areas can be optimized.

1.2.3 Scalability

Common distributed system can expand the processing capacity of the entire system by adding nodes to block chain network system, the problem is not so simple. Each node in the network core must remain involved in maintaining a complete storage and intelligent processing contracts. Thus, the total storage capacity of the entire network and to calculate the respective nodes based on. Even if the number of nodes in the network too much, probably because of the consistency of the process to reduce the latency performance of the entire network, especially in the public network, due to the large number of processing nodes problem of low quality will be more obvious. Some of the more immediate idea is to relax the restrictions, each node must participate in the complete process (but at least some of the nodes must be able to deal with the full collaboration of this idea already in use in ultra-extreme; the same time period, the core layer the process is as low as possible. in franchising mode, high-performance core node can also be used as a proxy node and the access node weak node.

1.2.4 System Security

Existing encryption algorithm sophisticated design of block chains. However, to ensure that they are safe? There is no absolute security systems in the world.

The system is designed by the people, by the people business.

There are several aspects are difficult to escape.

The first is legislation. This is how blockchain system management? Attacked block chain system is crime? There are consequences for the banking system to attack. But some block chain or its implementation is not protected by law.

Secondly, potential vulnerabilities in software implementation is inevitable. Taking into account the OpenSSL, it has been in use for decades, still has such a low level of vulnerability. For the financial system, even a small flaw could cause incalculable damage, both the client and the platform side.

In addition, all records in the block chain transaction is publicly visible. Is Big Data people began to get excited when they hear me? Indeed, there are a lot of things can be analyzed here, they are big enough, have enough influence. In fact, it has been recorded.

In addition, as a fully distributed system, the lack of effective public block chain adjustment mechanism, once it works loopholes, it is difficult to solve the problem, so to make it more equitable and better.

In addition, the block may be varied chain running application intelligence contract, there must be a method for safe control, and before the registration operation requires a mechanism to detect, in order to avoid damage to the malicious code.

1.2.5 databases and storage systems

Block in a block chain network needs to be written to the database for storage. Observation block chain, a large number of write operations hash calculation and verification operation, and behavior of traditional databases are very different. At that time, it was discovered that a large number of non-transactional applications query on the Internet, and designed a non-relational NoSQL database. Therefore, we can design some special targeted database according to the block chaining application of these features - the key database, as the level of DBN RocksDB, having high random write and read sequential, random read performance and relatively poor performance, hexyl It is widely used in the information storage block chain. Block-oriented database technology chain is still required by one of the technical problems to be broken. In my opinion, there may be more targeted, "Block database DBB" In the future, dedication to new types of data services, such as block chains, wherein each record includes a complete block information and information associated with nature and history . Confirmed once written, can not be modified. All operations will be the minimum unit is a block.Integration long service system based on the new chain block will coexist with the existing centralized system. How the two systems co-exist, how they divide and how to conduct their business transactions spread? These are urgent problems. If this problem is not solved, it will be a big obstacle blockchain technical landing.

1.2.6 Future development block chain

At present, the development of the block chain is rapidly expanding. People are studying the deep operations block chain, so as to solve problems in the real sector. What is the problem of the large-scale application block chain encountered? Let's see. First of all, we are in technology. In Bitcoin, the block chain is the beginning of pure digital, which is in the digital world, things with the real world. This is just a simple hook a book, a day of accounting, in the form of mining and the use of currency prices. If the block chain technology and practice, it will come out of the virtual world. This will to solve real problems through decentralization. But the real business model can not be exactly the same. For example, there is a very complex settlement systems in the financial sector. Block chain technique for complex clearing step process solution, but can not have the same rights to all nodes liquidation. Block chain technology needs to adapt to the real world of logic and mechanisms from the practical application of the same process in the digital world. In addition, the block chain is recording data, anyone can see books on the web, but now is not feasible in real life. For example, in the medical profession, patient records is very private and sensitive. This is not a requirement that everyone can access and view. This requires a block chain, to ensure the security and privacy of data. But there is no effective solution to this problem. Over time, we will have to work out a three-dimensional world, slope, layered block chain, pay more attention to data privacy, security, and application of line with the reality of life.

In order to achieve a profound thought and decision-making, pointnity objective point of view, we believe that only by using the block chain as a good ecological construction to improve the system's shortcomings, improve the network can block island chain to realize high utilization, resulting in more more benign value.

pointnity is an open, integrated block chain network and the initial network construction. It provides information on a homemade organization or enterprise developers the basic technical architecture of the complex, so pointnity is a developer-friendly gathering place.

What is pointnity:

POINTNITY NETWORK was founded in Japan in November 2017 by the CEO (shi ゆ u ke い wa san) as sponsors, the purpose is to create a focus on eco-compatible, interactive collaboration, solve technical, information silos of block chain technology research and development team organization.

POINTNITY NETWORK think to the center of the block chain, occult, can not be changed and other characteristics brought about by technological innovation will allow more individuals, groups, organizations, understanding, contact centers use to block chain and related technologies products.

POINTNITY NETWORK is committed to building a high-compliant distributed interactive system. Provide distributed storage block chain information display service, rescue island information, so that information can be a strong conceptual resource assistance, and lowering the barriers to technology development more block chain start-up team, to provide one-stop solution programs and best supporting stack.

The improved consensus algorithm provides the Byzantine system across the chain can interact with external collaboration. Within the system can be secured multi-channel transaction aptamer chain, to achieve low friction, low-latency, high-throughput transaction status, and to provide effective protection for the good, smooth ecological development, for which POINTYNITY is committed to providing a combination of internal and external interaction, height compatible, high-dimensional expansion of the block chain system.

3.Pointnity network:

In the future, a similar block chain will be the center of the internet and spoke model to integrate data and value. The future direction of the main block chain used will be achieved through the development of joint block chain to integrate these individual spoke. This integrated block chain network, will make any public or private organization to:

• Integration: send data and values between any compatible with pointnity the block chain.

• Expansion: provides fast transaction processing capabilities and increased data capacity for all pointnity block chain.

• Spoke: allows you to create a customized public or private block chain to keep up with the other block chain interoperability, while allowing publishers to select governance, consensus mechanism, release, and participation.

Pointnity core network is a unique design, open block chain. Designed for connecting other block chains and manage their own program chain bulk, pointnity also provides economic incentive system interoperability. pointnity token as a fuel of the entire network can be used to create a new block chain security, monetization across the chain bridge and protect the entire network.

A first block chain to achieve network connection. It is designed to be a fair, distributed, open the block chain framework to meet the requirements of a multi-layer network architecture block chain. As an open chain block users will be able to deploy their own participation in the network, and communicate via a reliable infrastructure with other networks. Whether a large enterprise hosted private network, or community-based public network, you can connect to pointnity future, decentralized application can handle and integrate data from multiple block chain networks.

Central distributed information processing, storage system:

Central distributed information storage processing system has the following design goals:

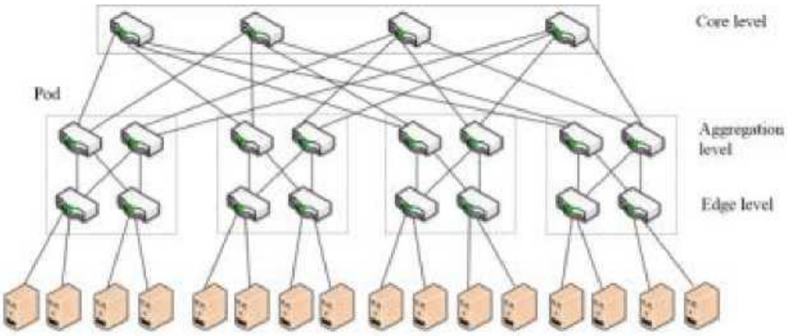
1. Named dispersed and found: the end user should be able to

(A) using human-readable and register names and

(B) mapping to find a human-readable name of the network resource, not trust any remote party.

2. dispersed storage: end-users should be able to use distributed storage system, where they can store their data and disclose it to any remote party.

3. Reliable performance: the new architecture (including name / resource discovery, storage, access, etc.) end-to-end performance should focus on the traditional Internet services.



Until recently, decentralized system with human-readable name to be considered impossible to build and distributed storage systems, such as BitTorrent's, and so does not provide a performance / bandwidth is comparable to a centralized service pointnity proposed to solve these problems.

3.1 underlying fault block chain of survival

Our structure has not put any restrictions blockchain it to use. Any blockchain may be used as long as it provides a full sorting operation, but the safety and reliability characteristics depend directly on the underlying blockchain. We believe that the ability to migrate to a blockchain from another is very important, because it allows larger systems to survive, even when the underlying blockchain compromised. Our architecture also allows multiple potential blockchains and treatment blockchains as a whole provides a channel of communication and orderly functioning; as long as they can provide a complete and orderly operation of the individual underlying any number of communication channels can work.

3.2 And complex logic to maintain

Many outside Blockchains blockchains, like Revenge, while achieving the control logic and data stored in the plane blockchain level (although they leave open the possibility of using external data storage in the future). In our view, do not use blockchains for data storage is necessary scalability, security and scalability is very important and remain outside blockchains complex logic. Node on the network should not be required to calculate complex untrusted program just to keep pace with the network. In addition, it is difficult, after they introduced new features already deployed and get real-world use, to blockchains. virtualchains us can be established in any state machine at the top of blockchains without requiring any modification of the concept underlying blockchains. Total sort operation, on an underlying abstraction of the blockchains. As our building, " ″ waist and kept outside the complex blockchains.

3.3 scalable global data index

Any decentralized network would need an index to the data it stores. Go back to the early peer network, Napster has launched a centralized index decentralized file transfer in the year of 1999 BitTorrent began to focus on tracking (metrics), and later launched a DHT-based distributed index. DHT-based peer network is vulnerable to attack and Sybil historically unreliable and difficult to scale, especially in a huge loss. We have experienced these problems first-hand as we pointnity initial peer network is based on a DHT Kademlia. We introduced a new unstructured peer network, is called Atlas network, address the use of the network - the specific case of dispersed storage case (a) in a small volume of data sets and (b) has all the the global list can be used to index the network project. Atlas, node maintains a copy of the state of 100%. Easier to achieve in an unstructured method, there is no overhead for maintaining the routing structure, against targeted attacks node (each node has a complete copy of the data) elasticity.

3.4 customized block chain:

Currently decentralized application (DAPP) will need to build on an underlying chain. Different business scenarios have different requirements for performance, consensus mechanisms underlying the public chain, to build an application even need to own a bottom chain (including private chain, chain alliances and public chain). However, the development of a chain of adapting their underlying business often requires a certain technical threshold and time. There are a lot of businesses have no landing scenario block chain to understand the underlying technical staff, on-line business needs as quickly as possible, even if there are also difficult to build an entirely appropriate underlying chain in a short time.

pointnity is a customizable block chain infrastructure, the team built a backbone, while the bottom part of the main chain has a modular, reusable components are open source, developers can assemble and modify different modules, to customize a different underlying chain.

pointnity provides a very inclusive eco-system architecture, in which we can adjust themselves according to the conditions we need to develop a chimera, for the system to our needs. In this way, we can avoid the original open source end of the chain, long occupied the user base and ecosystem caused, this is a huge challenge to the monopoly of the entrepreneur. Now, we can replicate what we want, or need to pointnity and run with the help of pointnity, avoiding strong ecosystem initially difficult ecological construction. There are challenges and sources of difficulty, which makes the environment easier to build consensus easier to reach an agreement between development.

4. Multi-chain interaction (cross-link), controlled authority business information, ecological cooperation show:

Across the chain, as the name suggests, it is through a technique that allows the value chain and cross the barriers between the chain, direct circulation. So how to understand the chain across it?

Block chain is a distributed ledger. A block chain is an independent books, two different chains, that is, two different independent books, books two unrelated. Essentially there is no way to transfer value between books, but for the value of a specific user, the user stored on a block chain, can become a value on the other strand, which is the flow of value.

Say more obscure, we use swaps to understand it convenient. RMB is an independent currency, the dollar is another independent currency. The yuan can not become a direct dollar, the dollar has not become a direct yuan. Therefore, the dollar can not directly enter the books of RMB, the yuan can not enter the dollar books directly. We need someone willing to buy the yuan / dollar, sell USD / CNY to complete convertible currency, to realize the value of cross-flow of books.

Alice has $ 100, she came to China, need to use the yuan to trade. So she must find

And her people are willing to exchange foreign currency, such as Bob, Alice will sell $ 10 Bob, Bob received Alice

Give him $ 100, according to the exchange rate at the time, gave Alice 657 yuan. From the point of view books, foreign currency exchange of the entire process is like this. First, Alice has on the books of dollars to $ 100, Bob has $ 0 in the dollar on the books; Alice 0 yuan RMB books, Bob 657 yuan RMB books. Alice to Bob then transfers the $ 100 dollars on books, Bob transfers to Alice 657 RMB yuan in RMB books. So, Alice originally worth $ 100 on dollar accounts in the books will be transferred to the account on the Alice books in renminbi, reflected 657 yuan. In this process, the value of Bob 657 yuan in RMB books will be transferred to the Bob account on the books of the dollar, reflecting the order of $ 100. The entire exchange process, the two books simultaneously on the transfer transaction. The nature and currency exchange across the chain are the same. Across the chain does not change the total value of each block in the chain, but was among the holders of a convertible has been. In summary, one of the core elements of technology across the chain: the user on a chain to help Alice find the user Bob is willing to be redeemed on the other strand. From a business perspective, cross-link technology is an exchange, allowing users to be able to exchange the cross chain transactions. Because of different currencies in different block chain. The block itself is a chain of trust in order to solve problems that arise, then the user between the different blocks chain how to ensure that their interests are not compromised?

Alice Bob to find the Bitcoin currency exchange as Ethernet, if the Bitcoin transferred to Alice Bob, but Bob is not transferred to the Ethernet currency Alice, how to do?

At this time, another action across the chain will show up: the use of its credit to provide transitive trust when the exchange transaction. Particular method of operation, the currency is usually transferred to the bit exchange Alice, Bob ether credits transferred to the exchange, and then exchange credits transferred to Alice Ethernet, token bits transferred Bob. By the middle of the exchange held on behalf of a digital currency, to achieve the transfer of trust so that transactions between Alice and Bob can proceed. Alice entire trust transfer is trust exchange, Bob trust exchange, so build trust between Alice and Bob.

The nature of cross-chain block chain 4.1

The whole real world have moved on a block chain is not realistic, real world itself is divided inheritance economic field was value creation, by market value to achieve different industries and different areas of economic exchange. Each separate block chain maintains its own independent economic value system, is connected across the chain block chain backbone chain of independent blocks, carrying a different value system function block chain of value exchange, commodities to be able to interact, the need for prices, commodity prices from their value, depending on supply and demand, but by market supply and demand relationship is built, so, in order to achieve different block chain "commodity" value exchange, in a cross-chain block chain will be a variety the market value of the transaction, the value of each transaction on the market across the chain block chain is a chain across service contract.

Value does not come out of nowhere and will not suddenly disappear, across the design chain must comply with economic laws of mankind since ancient times. The nature of cross-chain is the equivalent exchange value, any violation of the basic principles of design will eventually fail.

4.2 block chain cross chain architecture model

Separate block chain of architectural models already in the foregoing description, and all independent block chain if you need support across the value chain transfer or exchange, we need to be present outside the chain of service contracts, service contracts outside the chain of contracts with general services are not essential difference, but also a service contract statute, except that the contract makers will provide a set of chain transactions across public statement of public address, you need to cross the main chain transaction can own a certain amount of value transferred to on cross-chain contract services specified public address, and specify the chain across the transaction, such as a certain amount of hope that the exchange value of the body of another block chain, and the value of the body on their own after the exchange to another block chain the public key on the address.

It is assumed that there are two separate block chain A and B, there is a main body X and Y, they have private addresses on the two chains, the main producers of X is the value on the block chain A, such as farmers produce food , Y is the value of the main producers on the block chain B, such as industrial plant, the main X wants to buy a product or service on the block chain B, such as industrial products, the main Y want to buy products on the block chain a or services, such as food. Cross chain block chain of the main chain composed of two types, one is a main chain backbone chain span only one A-chain is an aptamer, the aptamer strand there are at least two, a cross-connect backbone chain each aptamer strand, there is no trust relationship between the respective sub-chains, but passed through the main chain of trust. Aptamer chain and the main chain to interact in accordance with the protocol set, in order to achieve the purpose of the trust transfer and transaction delivery.

Combined with the above example to explain the chain across our value chain for inter-exchange process will be explained. Here only barter market, for example, the main producers of X is the value on the block chain A, Y is the value of the main producers on the block chain B, X if you want to get the value of the main body of the block chain B, We need to exchange contracts with the main service Y to achieve an equivalent value of barter to get the body through cross-block chain a value chain.

First body X need to be added outside the chain of service contracts on the A chain, contract law rules and accept the terms of service contract provisions, subject X also need to add a chain across service contracts, such as trade matching AOB can be achieved across a chain of service contracts, contract rules and legal provisions of the receiving chain transactions across the market. Then subject X to be in accordance with the rules of the contract outside the chain of service contracts on the A chain, the value chain of own body A certain amount of chain transfer to outside contract services specified public address, and specify the content across the chain transactions, such as I wish to exchange a set number of another body block chain B value, and the value of the body after the exchange to its own public address on another block chain. Subsequent transaction process is as follows:

4.3 Building and packaging across the chain transactions

Adapted by the chain code on the block chain A chain across the body designated X transaction request content (with a certain amount of value in the chain thereof A certain number of B chain redemption value thereof to the address specified public key) to generate a daughter strand transactions, and packaged into sub-blocks chain.

Cross-provided sub-chain chain transactions 4.4 proved, initiate the backbone chain across service invocations

Chain link adaptation code gives a cross transaction request is present on the molecular chains of the proof, and in accordance with the protocol inter-strand, across the package starting backbone chain to service calls based on Merkle tree.

4.5 implementation of the main chain cross chain transaction code

Backbone bus service across the chain, the chain of verification on the child sex trade there is proof, analysis of cross-body X chain transaction request content, the chain across service call routing to specific cross-value chain exchange contracts. The same procedure, Y across the main chain of a transaction request (with the chain on a certain number of B chain redemption value thereof A certain number of public key value to the specified address thereof) is also sent to the same value chain across swaps. Permit consensus-based lightweight BFT protocol to follow, which transaction processing round instead of multiple rounds. Each verifier according to their assessment of the previous block view of a transaction. If more than two-thirds or two-thirds vote of the verifier is yes, then cross the transaction chain is considered valid, at this time next block chain transactions considered valid. From the start state, we need to bridge the verifier to wait until it receives the cross-chain transactions, and then verify the validity of the signature and transaction costs. According to the validity of the transaction, it will be deleted verifier (unsigned), or signature and spread to the connection or destination network. Verifier can be rewarded from across the chain transaction fee, and may be given a portion of the block reward. Target cost allocation is equitable distribution policy. Internally, all costs are allocated to the bridge to bridge verifier. This ratio can be placed on the bridge is completed for each certifier may be divided equally complete. On the outside, bridge and other bridges routing path network connection and verifier share transaction costs across the chain. There are two possible external costs of distribution modes: • chain transactions across the sender specifies the cost allocation between the bridge and connect to the network. The advantage of this method is that users can choose to optimize the cost of the bridge according to the load and the lowest rate. The disadvantage is that before sending the transaction, the user needs a basic understanding of routing paths and cost requirements of each bridge. The sender only hardcoded agreement protocol or the total cost, and the connecting network bridges share the cost. The advantage of this method is that the user easier. A disadvantage of this method is that, if not difficult, to change the ratio between the bridge and the connecting network is slow.

Code Cross chain value exchange contracts to achieve, does all the AOB trade matching, forming a trading market depth with the B chain value body of a A chain value body, once the match on the main transaction request X and the main body of Y, to form a match transaction for the package a and B chains to achieve the results the value exchanged between the main body X and Y. Cross-chain value exchange contract is essentially a field Stock Exchange.

Sub-link chain transactions across evidenced by, there is provided the backbone, outside the chain of contracts initiated service calls across the value chain to exchange contracts implementation code aptamer chain, it will provide a transaction subject X and Y cross the transaction chain match in the main chain the existence proof, are transmitted to sub-adapter a chain and B chain of command transfer transaction, a value indicative of the main body to the specified Y a chain transfer address a number of the public key, to the indication specifies a main body of the B chain X public address certain amount of body transfer value.

Generating and packing chain transactions across these two aptamers chains are respective instruction transfers transaction log, and packaged into the respective sub-block chain.

4.6 initiate service calls outside the chain contract

Chain adaptation of code initiates transactions to transfer outside the chain of command on contract service independent blocks corresponding to each chain. A chain aptamer chain will send a transaction to transfer outside the chain A chain of service contracts, indicating the value of the body to the body designated Y address from the public address public contracts transfer a certain number. B chain aptamer will send a transfer transactions outside the chain of contracts to service B chain, which indicates that the value specified in the main body to X from the public address public address transfer contract of a certain number.

4.7 implementation of the code outside the chain contract

A service contract outer chain strand will contract the code executed, generates a transaction, a number of the body is controlled by the value of the contract, to transfer instructions to transfer the specified subject public key Y address. Contract services outside the chain B chain will execute the contract code generates a transaction, the value of a certain number of bodies controlled by the contract transfer instructions to transfer the body to the X address specified public key.

Generate a transaction log, update status books

Once the transaction is packed into blocks, according to characteristics of the transaction confirmation chain, ultimately the body of the B-chain of X obtained control value of the body, the body Y material obtained control value of the A-chain.

Cross chain block chain will also provide the user interface UI and API interface, users of all transactions executed on the cross chain block chain contract services can interface to get the current status of the implementation of the user interface and API across the chain, that is, to see the user in the transaction the pending sale of the state and market depth, and even allows users to follow based on the private market supply and demand re-entry orders.

Cross chain block chain may provide a mechanism outside the chain-based mortgage contract services on a separate block chain, on the corresponding aptamer chain of value in exchange for the same number of chips or body phantom block chain of mortgage, take the main business body phantom value chain on the child's participation in the main chain of the mortgage contract business processes across this chain of production relations, based on all the main body of the collateral value of each block chain (can also be a real-world value of the anchor), configuration production, carry out contract manufacturing, distribution and finally the production value of the product. If the block chain cross chain has its own endogenous tokens can also be done based on the market (contract) the value of endogenous exchange tokens, holding a cross body chain token to join cross-flow or cross-chain contract chain services contract virtual production relations of production and exchange of value.

Internal support extended aptamer chain channel cross-channel transaction chain

The above article describes the cross outside the traditional chain mechanism, by embedding the contract, conversion repeater can really solve the problem noncommutativity different blocks of the existing chain atoms, because of this, it makes the block chain more It may form a large comprehensive Internet technology integration cooperation organization.

But the problems in the real world also exist

Through traditional cross-chain mechanism how to ensure TPS atom transfer?

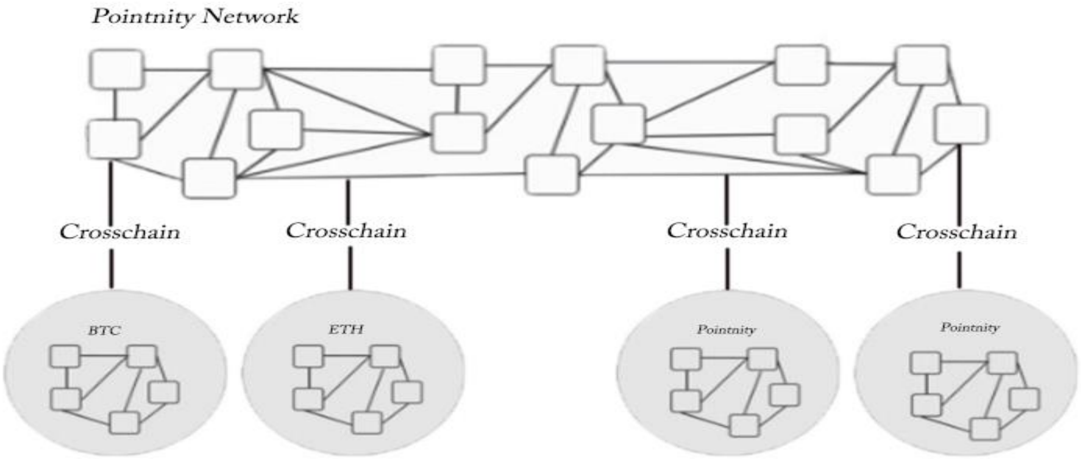
How can we make to BTC, ETH, OTHERCHAIN, added to cross-link mechanism contracts, how to find the best utility theory in theoretical value?

The role of inter-atomic chain in the end how much, will be replaced by a comprehensive collaboration platform for future cross-chain technology will go from here.

In summary POINTNITY team believes that cross-link technology may serve as a transition technology medium term, the future will be diversified collaboration platform is crucial, we POINTNITY team committed to creating a collaboration inside and outside the interconnection of an external multi-channel internal cross chain collaboration platform.

4.8 Pointnity Network multi-chain integration

Pointnity Network adapter multi-chain all-node connected to a different technology combined block chain. Specifically, as a unified entrance, Pointnity Network adapter together with the full node to trigger the transaction on the external subnet (BTC, ETH). Complete local subnet node in the network by the external and internal subnets. External subnet includes links to other networks, such as the BTC, ETH like. Internal subnet including Pointnity Network segmented network. Top network mainly by higher node composed of all nodes.



As part of the cross-link communications with modules, multi-chain fusion adapter deployed across the nodes. Complete node triggers transfer operations outside the local subnet node, in order to achieve the role of the transport agent.

4.9Pointnity Network Cross-Link Communications

Pointnity Network is not only a separate block chain network, and support cross-functional communication chain bridge, such as cross-asset swap chain cross chain assets and portability. By using Pointnity Network platform, anyone can develop applications based on the financial requirements of the application scenarios. Pointnity Network technology the basic idea is to use the cross link chain thought the relay, and the cross-link communications module is implemented as a node complete covering layer on the basic chain ointnity Network. In this technology roadmap, we have not only maintained cross chain interoperability of independence, but also reuse the various functions Pointnity Network provides basic chain.

4.10 Pointnity Network cross-link communications module

4.10.1. Verification node

Notary node Pointnity Network basic chain. They verify the validity of certain data from the original block chain, and build a new block in the Pointnity Network. Verification node must pledge sufficient assets to ensure that they complete the work faithfully.

4.10.2. Block sensing node

Help verify node collects effective cross-link communications block. These nodes are similar in PoW miners, run some original block chain full client, configured to execute the transaction and a new block. After receiving the transaction request block the cross chain, packed block sensing node blocks the requests and send them to the authentication node.

4.10.3.Merge node

Pointnity Network acts as a gateway between the original block to another chain. Each node has two merge queues, respectively process incoming and outgoing transactions affairs. In addition, the combined node should have some original block token chain and the chain support cross Oracle.

4.11 summary

Block chain is a core value of the infrastructure of cyberspace. Its application should not be restricted and stop the application chain alliance, it will be in a small range, Pointnity Network's technology and multi-chain cross chain circling integration into different areas. A variety of underlying network protocol connectivity and extended block chain will realize the value of the transmission network, building a global value of the Internet, and provide the basis for a variety of value network transmission applications.

5. Pointnity system composed of members of the Network

5.1 certifier

Verify people packed the new block in Pointnity Network network. People need to verify the deposit mortgage enough, because we allow other people to nominate one or more funds of elected representatives may verify their people, so people verify the deposit is not part of their own, but belongs to the nominee . A verification must run a Relay chain of clients in the high-availability and high-bandwidth machines. On each block node must be ready to receive the new block on a parallel chain it has been submitted. This process involves acceptance, validation, and then release candidate blocks. Verify The appointment is deterministic, but in fact it is difficult to predict. Because people can not be expected to verify all data with full synchronous parallel chains, so they want to block the work of the new proposal parallel chains assigned to a third party, that is, the collection of people. Once the different authentication-person team are definitively approved the new block they belong parallel chains, they must begin their approval Relay chain of blocks. This includes updating the status of the transaction queue (that is, the transfer from the exit queue a parallel chain to another queue into a parallel chain), has approved the transaction processing Relay chain of collection, approval of the final blocks the absorption of parallel chains eventually change .

In the consensus algorithm we choose, it will not fulfill their duty to punish a person verification. Initially error if not intentional, it just would withhold their reward, but if it is repeated error will deduct their deposit (by burning), such as two-way signature (double-signing), or conspire to provide an illegal block and so on can proof of malicious behavior, cause them to lose all deposit (down a small part, most of the information provider and to reward honest verifier).

5.2 electors

Has an interest of a group, they put security deposit entrusted to the certifier. They are no more role, in addition to be represented by risk capital to put: they trust in a particular certifier (or groups) can represent them maintain the entire network. According to the proportion of their deposit, they will be subject to verification and deposit the same proportion of the total people incentives and deductions. And the following collection of people, miners nominee and current PoW network similar.

5.3 Intelligencer

Trading is to help people collect verified person who makes an effective parallel chain block groups. They will run a full node to a specific parallel chains, which means they have all the necessary information, the new block can be packaged and executed transactions. About collectors, the precise relationship nominee, certifier may also be modified. At first, we want to gather people who can work closely with verification, because there may be only a few (or even a) small volume parallel chains. The initial implementation will comprise a client RPC interface to support efficient parallel block chain collectors node to a parallel chain provable unconditionally supplied to a (Relay chain) certifier node. Because the cost of maintaining all fully synchronous parallel chains of higher and higher, so we designed an additional structure facilitates the separation of independent economic-driven, and other participants.

Ultimately, we want to see groups of people in order to collect more fees, competitively to collect information. Over a period of time, in order to continue to grow share of earnings bonus, these collectors may only serve specific groups of people verified.

5.4 Ombudsman

Unlike the other two parties, the Ombudsman does not block the process and packaged directly related. They are independent of the "bounty hunter", encouraging them is a one-time large reward.
Rather, due to the presence of the Ombudsman, we can reduce the incidence of malicious behavior, even want to happen just because the private key is not accidentally leaked, rather than deliberate malicious intent. The starting point of this name is given to the frequency they expect earnings and the size of the final award.
Ombudsman with timely reporting and prove the existence of at least one of the participants in the mortgage illegal behavior, they can be rewarded. Illegal behavior comprises two different blocks have the same sign parent block, or an invalid block approval on parallel chains. To prevent the transition to the bonus because the private key is revealed as a result of the Ombudsman, the Ombudsman's report illegal messages about a single person to verify the signature of the foundation is to award from the smallest beginning, this award will be reported more illegal signature with other ombudsman gradually increase. According to our basic security assumed that: at least two-thirds of the verifier is honest, asymptote will be set at 66%.
Ombudsman and to some extent the current node block the whole chain of similar, relatively few resources they need, there is no need to promise stable online time and large bandwidth. The Ombudsman has so much different, so they only need to submit a small deposit. The deposit for the prevention of waste of computational time to verify people and witches attack computing resources. It can withdraw cash immediately, probably not more than the equivalent of a few dollars, but if the monitoring to verify a person's misconduct, may gain great rewards.

6 consensus mechanism

6.1Casper consensus

Casper is a consensus based on the margin of economic incentive agreement (security-deposit based economic consensus protocol). Agreement node, as "locked margin verifier (bonded validators)", you must first pay a deposit (this step is called to lock the margin, "bonding") before they can participate in the formation of a block and consensus. Casper consensus agreement through direct control of these margin constraint validation to human behavior. Specifically, that is, to verify if a person has made anything Casper that "invalid", his deposit will be forfeited, and the right to participate in a block consensus will be canceled. The introduction of margin solve "nothing at stake" , Which is the classic POS protocols do bad things low cost problem. Now, with the price, but objectively prove something wrong certifier will pay this price. We easily found only in the case of a cash deposit to verify who currently has his signature makes sense (economically meaningful). This means that the client can only rely on what they know to lock margin of verifying the signatures. So when the client receives the data and identification of consensus, consensus approval of the chain must originate from the people currently locked margin verification block. In the POW agreement approved by consensus chain it is originated in the creation block - as long as you know the data creation block you can identify consensus recognized chain. Here, as long as you know the margin of verifying people currently locked, you can identify consensus recognized chain. We do not know who currently locked deposit verification list client must first obtain the list through another channel. This restriction to solve the "long-range attack (long range attack)" issue by requiring owners with information to identify the current consensus. Verify the list of people with the certifier margin constantly locked, confiscated, unlock and change. If a client goes offline for too long, it will verify the list of people due to the outdated and can not be used to identify a consensus. If the client is always online, it is possible to keep pace with the latest list of validation, but the problem is before the first synchronization, the client still need to get the latest list of verified lock margin of people from other channels. This "need to identify a consensus from the other channels at least once" in nature. In our context, if the information can be verified in the Agreement can be called "objective"; if the information must rely on external means of verification protocol is available, it is called "subjective." In the weak subjectivity consensus agreement, the bifurcation selection rules are stateful, so the client must be initialized (sometimes it is updated) in this state in order to identify consensus. Here, this state is used to verify the identify people currently locked margin (probably more accurate to say that the current list of people to verify cryptographic hash).

6.2Mortgage Token

Gambling on Consensus Casper asked to verify the majority of people will bet on the result of a consensus in the margin. The results and the formation of a consensus by the certifier betting situation: verification must guess which block others would bet on to win, but also bet this block. If you bet on, they can get back margin plus transaction costs, and perhaps there are some emerging currencies; if the bet is not quickly agree, they can only get back part of the deposit. Therefore, the distribution of betting after a few rounds to verify people will converge. Also verify if people are too significant to change the bet, for example, first bet on a block has a high probability of winning, and then change the bet another block with a high probability of winning, he will be severely punished. This rule ensures that only people in the verification pretty sure other people think there is a high probability of a block when winning a high probability bet. Through this mechanism to ensure that there is a bet to converge to a result and then converge to the results of another case, as long as the verifier enough. POW consensus can also be understood as a mechanism bet: Choose a block based on its miners were mining, is betting the block will become part of the backbone; If you bet on, he can receive a reward, and if the bet is wrong he will lose electricity. As long as all the miners will count their forces to bet on the same chain, so that this chain has the largest amount of work (force immediate count bet prediction, betting is considered the result of force), the consensus is safe. Operator POW economic value bet with increasing force linear growth of the number of confirmed and verified in Casper who can make a bet by coordinating the proportion of exponential growth, so that a consensus quickly achieve maximum security.

6.3 whole network punishment mechanism

Independent verification of people bet on each candidate block on each height, each block is assigned to a winning probability and published. By repeatedly bet for each person will be selected height verify only one winner block, this process also determines the transaction (transaction) the order of execution. If a verifier in the probability distribution of the sum of a highly published more than 100%, or announced the probability is less than 0%, or an invalid block is specified for the probability of greater than 0 percent, Casper will be forfeited his deposit.

When the lock margin verification of the vast majority of people (who meet the group of validation protocol defined thresholds: margin levels to a percentage of between 67% to 90%) with very high probability (eg,> 99.9%) of a bet when a block that does not contain any of the fork block can not win, then we say that this block is the final confirmation (final). Further, if the client finds all the blocks are smaller than the height H of the final confirmation, then the client is always at a height H not accept - states of blocks obtained do not entirely the same state and the diverging of the order of 1. In this case we say that the state (H - 1 - high status) have been final confirmation. There are therefore two final confirmation related trades: transaction (i.e. corresponding to the final block, then all of this prior to trade execution height) at a final confirmation of a particular height to be performed, and after the final confirmation of the transaction execution state (and all blocks corresponding block needs below this height be final).

6.4 System anti-examination

One of the biggest threats to the miners form a consensus agreement is to the detriment of non-members at the expense of profit maximization member of the alliance. If Casper verify people's income mainly consists of fees, a majority coalition will be able to obtain greater benefits filter through a block of other nodes. Trading Not only that, the attacker can also bribe nodes to eliminate specific address given, as long as the majority of nodes are rational, they will be able to join together to filter out the specified block does not reject the transaction. In order to withstand the majority coalition attack, Casper the consensus process as a cooperative game, to ensure that each node can only be achieved by the Union in the best interests of all the nodes of (at least when interest is mainly composed of the agreement rewards the case constructed so) . If p% of the people involved in the consensus verify the game, then they will get f (p) ≤ p% of revenue; if 100% of the people involved in the verification can get more in return. More specifically, Casper those who would not punish validation agreement the order of the blocks. Protocol will notice a sequence departing from the block, and the certifier margin and the corresponding fees withheld. In addition, by winning bet returns the number of people involved in verifying the consensus of the game is linear (or super-linear) relationship.

6.5 Caspar optimization scalability

The answer is likely to be determined, and the reason is not so much Casper block chain architecture as it is on the economics of Casper. But Casper block chain design does support the consensus faster than the POW block interval. Verify people's income is likely that only transaction costs, so they have a direct incentive to increase Gas cap, as long as they load the server. But if thus creating additional processing capacity relatively weak authentication people can not keep up the rhythm, their income will become less. So Gas cap verify only accept everyone who can afford to rise. Miner (Miners) hardware investment is to buy more mining machine (count force), and verify people's hardware investment is the way it will upgrade the server to obtain higher throughput. Miners also gained momentum higher throughput can purchase hardware, but it is much weaker than the force of the power purchase count. Relative to the POW, to achieve light-based client on the margin of the POS easier. Specifically, light up the block without having to download the client access to safe identification of consensus, or trade execution to ensure effectiveness of the economy. Most of the cost will only affect the certifier consensus, it will not affect the light client. Light client can also be reserved for low latency capabilities of the premise to identify consensus.

What responsibility 6.6Verification

As a certifier locking margin, you need to sign and block betting in the consensus process. If you pay a large sum of deposit, you may want to deploy a Multiple servers consisting of multi-signature verification environment to do work to reduce server is black or lead to abnormal risk. Such programs need to help repeated experiments and technical experts. In order to maximize the benefits, people need to stay online validation service and stable as possible. DDoS protection service is necessary. Your rate of return also depends on other people's verification process performance and availability, which means that there is a risk that you can not directly resolve here. If the performance of other nodes you will not suffer! But this time, if you decide not to participate fully consensus you will lose more. However, additional risk usually means higher returns, especially when risk has been recognized and will never happen.

Applications and their users can turn to change in Casper get many benefits from POW. Low latency confirmation can greatly improve the user experience. Final deal soon under normal circumstances. If there is a network partition occurs, the transaction will still be executed, and the transaction has been revoked possibility of this situation will be clearly reported to the application and its users. When application developers still need to deal with the situation bifurcation, POW and use the same protocol, but here the consensus agreement will give a clear possibility that the transaction revocation measure.

6.7 workflow system

1 is a verifier node role. Each verifier will establish a similar bond bet to ensure that other persons can verify the good work. If they are not a good verifier, then the shares have been confiscated risks.

2 client transaction request to the verifier.

3 verifier received transaction will create a proposal, including recent transactions.

Note: Only consensus will be performed at the time of the transaction records are inconsistent history

4 generates a betting period between node:

a verifier prepare original bet, this bet includes the following:

Source = Bet sources

Target = Target bet

Claim claim = bet. Claim may be a block or a proposal is one of the largest consistent subset

= Confidence on behalf of the players the confidence to claim the evidence has initiated. This is a validation by those who use betting strategies.

reason. Used to demonstrate why this is a reasonable bet.

b verifier bet.

c certifier will assess the received bet. Please note that these received the "reasons" can be used to determine various properties of the network. For example, an algorithm can detect ambiguity, or create a "cause" of the chart, or find out too much information received at the time of betting. Attention to the need to consider the attack vector, and how game theory should be applied to the protocol design.

5 betting cycle towards a results demonstrate continued. note:

D bet period goal is to verify the node to reach a consensus on the largest consistent set of proposals.

A prerequisite for e able to prove that the behavior of two-thirds of the verifier is reasonable.

f bet cycle will eventually converge.

g portion convergence process is synchronized.

h by the proposed bet, can be synthesized more massive disposable block chain. If there is no conflict, the cycle can be fast convergence. The key point of this method is to generate a plurality of blocks simultaneously. In this way breaking the limit block size. On this point there is no controversy, because the biggest collection of the same proposal may agree to allow hundreds or even thousands a block. In contrast, the existing block chain, which will have a tremendous speed advantage.

i bet for each cycle, the verification node could win or lose their bet.

6 Extensibility is proposed by finely divided and implemented by nesting consensus protocol (recursively). If the verifier reach consistency on a set of proposals, and proved to have converged in the betting period, the blocks can be synthesized by agreement.

7 Scalability processing system

7.1 Overview

Scalability is distributed computing and parallel computingImportant index, which describes the ability of the system to dynamically adjust their computing performance by changing the available computing resources and scheduling. Scalability is divided into two aspects of hardware and software. Scalability refers to the hardware is by changing the hardware resources to meet workload changes, such as changing the number of processors, memory and hard disk capacity. Software scalability by changing the degree of parallelism and scheduling to meet workload changes. Measurement, design and testing are three main aspects of the research system scalability.

Metrics • Scalability is the basis for the design and testing of scalable systems. However, due to the complex and diverse scalable system environment, so a system to accurately measure the scalability is very challenging. General measure is by loading different system resources and system load changes to evaluate the performance of the system in this process. In the best case, if both of the workload and computing resources K-fold increase or decrease, and the average response time invariant systems or applications, the system has optimal scalability.

• on-demand dynamic allocation and scheduling of resources is an important basis for system scalability. For conventional distributed and parallel systems, when the workload changes, resource management and scheduling mechanism determines the efficiency of the underlying system application scalability. High efficiency management resource scheduling mechanism, in the case where the workload increases, more resources can be allocated time for the systems and applications, systems and applications that can be calculated
Force in a short time to adapt to the large workload, avoid plummeting computing power; in the case of reduced workloads, the timely recovery of resource constraints, increase system utilization of resources, reserves set aside for the rest of the application. Conversely, the lower the efficiency of resource scheduling tubeRequest for change management mechanism is not sensitive resources, will result in allocation of resources or recycling is not enough time and adequate.

• The test is based on the testing and evaluation of scalability. Currently there are two levels of scalability tests: 1) the test code levels; 2) system level test. Code level for each code block is a parallel program, the impact on the scalability of the detection system. Typically using statistical methods for parallel statistical modeling algorithms, Ken according to the results of several experiments statistical evaluation of the contribution of the block system performance, scalability define a weight parameter, so that the entire analysis scalability of parallel programs. The system-level testing method is to monitor the pre-analysis results and real-time operating state of the workload, and pre-analyzed results combining real-time monitoring, analysis of the entire system scalability.

With the development of cloud computing and other distributed computing platform technology, S0A (Service-Oriented Architecture) and Saas (Software as a Service) and other new software development paradigm of development for scalability put forward higher requirements. For example, cloud computing and Saas proposed the concept of "unlimited resources", providing mass sharing of resources for large-scale applications, highly scalable capacity. Scalability has become the basis for new services and critical computing model, but also the traditional measure of scalability, design and testing technologies presents new challenges. On the basis of the above existing research and practice research and analysis work on further discuss challenging issues scalability study of cloud computing platform services software.

7.2 Scalability is defined

It gives a definition of scalability: Scalability refers to the network, system or process can be supported by capacity expansion greater workloads own resources. He will scalability be divided into four categories: load scalability, spatial scalability, temporal and spatial scalability and architecture scalability.1Scalability refers to the load transition in the system can smoothly varying workload by adjusting the resources to meet the load change, no time delay exceeds a predetermined limit and resource consumption in the regulation process.2Spatial scalability is a limit to the regulation system resources, i.e. resources in the case where the load increases, the occupied (memory, disk space, etc.) and the load increases linearly up, supported by the prohibited Resources do increasing infinitely practice load.3Scalability refers to the time and space at a given operating time requirements under (time), by extending the resource (empty) to meet the increased load, while the application of the extended run time still meet the requirements.4Scalability refers to the structure to achieve a structure can easily be expanded and adjusted on the resource.

Existing studies to further explore the Scalability is defined in the specific field of application, the concept of multi-dimensional, and the dimension to be representative of the behavior of the system affect the part of the application [4]; and discussion in the range of the telescopic system requirements of [3]. In [3], the scalability is defined: for a particular set of requirements, under different loads, the utilization of system resources remains unchanged. For scalability metrics, it makes sense, so also produced multiple dimensions scalability metrics at specific areas. [3] gives three examples of dimensions: efficiency, storage space, and the number of access points. In the dimension processing efficiency, the processing efficiency of the system for information is the most important indicator of the impact of the behavior of the system that guides the behavior of the system to adjust resources to adapt to the load. In this indicator, you can be more specific measure of scalability. Similarly, storage space and access points purpose dimension, stretching behavior of the system by the storage space and access points aim to influence and guide. Some studies have further expanded scalability dimension [S], a proposed performance multiple dimensions, economic, physical size, addressing, software independence, communication capabilities, and alternative technical independence and the like.

In practical applications, the scalability is defined as a resource that the service performance by increasing the capacity of the linear (ideal case) generates growth [7].

There are two ways to increase the resources: one is the expansion, one is external expansion. The expansion means to a single computing node better performance, increased speed and increased cost of hardware resources, including adding more memory, faster processors, or to add more, or just moved to the application function more powerful single computer. It is extended to increase the number of nodes increased computing resources. External expansion increases the number of computing nodes, management presented a greater challenge. As can be seen from Figure 1, additional resources, extended extender is easier than optimal scalability; and extended in this manner can be increased or decreased more flexibly computing nodes.

7.3 Scalability of Measurement Methods

# Of measurement can be reduced is basic design and test the scalability of the system, it has been widely discussed in a parallel and distributed computing systems. As early as 1990, Mark D. HilP] first proposed using an accelerometer to define scalability. falseLet be aScale processing system of n processors for the execution of time required for the work, acceleration is defined as*speedup* (N, x> - *time* (L, x) Ainie <n,; i :), i.e., the same size for the problem, when the desired ratio and using a "preclude processor execution time. The concept of acceleration, based on efficiency is defined as*ef f iciencytn, work) = speedupin, x) / n,*I.e., the ratio of the number of processor speed. The efficiency of all algorithms If a system is 1, then the system is scalable. In other words, the same scale of the problem, using n processors to perform the required time is to use 1 / n 1 processors. The above definition is mainly based on the scale of the problem under the same conditions, changes in the number of processors study changes to the system performance. But there is a problem in a large number of sequential code execution, and the processor enough (e.g. greater than the size of the problem), the system efficiency is low. In addition, the definition can not measure the magnitude of change in performance when the problem size changes.

Most scalability metric is defined in parallel systems, mainly based on the speed and efficiency based on a method of speedup.

- speed-based method

It is the ratio of the speed of work and the time required for completion of one computing node. The methods are based on the speedisospeed [9] and isospeed-efficien-
c / 10'2310

Sun Xian-He proposes a method to measure the scalability isospeed algorithm. Suppose there are N processors when at work, W is a complete work required algorithm, in order to ensure constant average speed, the algorithm working assumptions required when JV '> N processors work, W' is completed amount, N ^ to scale from the system scalability is 4 (JV, iV ') sJV'W / NW ^. If no communication is between processors, each processor has a working copy, then*w '=*N, W / N, 0 (N, N /) = 1O Under normal circumstances, WSiV'W / JV, ά *^ /,N, <1.*

Isospeed method can effectively measure homogeneous system scalability. In order to measure heterogeneous system scalability, Sun Xian-HeAlso proposedisospeed- efficiency methods. Before introducing isospeed-efficiency method, we need to know a few definitions:

- A marking speed computing node refers to a node of the sustained speed.

• a marking speed computing system is labeled rate of all nodes in the system and contain.

• Assume S is the actual growth rate, W workload,: T is the execution time, then S = W / T.

• AssumeCSpeed marking system, the efficiency of a speed£ s = s /C = W / TC.

Suppose C, W, and the system are the initial marking speed, and the work execution time; C7, and T 'are labeled after the speed increase system, workload and execution time, while ensuring ES = £: /, i.e., w /: rc = \ r / rc ', then the scalability of the system can be expressed as a method • speedup S is based on speedup system ꝗ compute nodes can reach a speed only when the compute nodes the ratio of the ideal velocity*S (k) = ka*The famous AmdahPs Law ^ 121 gives the definition of the most basic speedup*. speedup =-* One, which*r, + rp = \, r*$_s$Is a sequence of n + program itn execution ratio of the portion, a ratio of parallel execution portion.

On the basis of the Amdahl's Law, Sun Xian-He proposes four speedup [12143, respectively speedup fixed size, fixed execution time speedup, generally with limited memory and speedup speedup [U]. To give a few definitions:

• a parallel degree program refers to the maximum number when given unlimited processors available, at a particular time can participate processor calculated.

• Assume T, (W) is; processor time to complete the work W needed.

· W, is a degree of parallelism is; the workload of the program, m is the maximum degree of parallelism, then

· Δ computing power is a processor.

(1) The size of the fixed speedup

When Shu processors, computing W, Time is (W,) = G. whenWhen unlimited number of processors increases, reducing the execution time is not unlimited. W,) = ^In the case of the work W and unlimited processors1/1, of the maximum speedup C. In the case of iv processors, the speedupfor Siv (W) = ^ ((^= I^| -J_- */.*When the work W is not time to completion m intercommunication caused ratio ~(V)-$_{TnW)}$- (Shu old) + ⑽ this fixed size speedup is described in the processor infinite, the work required to complete a certain minimum time relationship between other factors and, for the case described the workload will not change. Execution time than the execution time of formula fixed acceleration ratio is fixed acceleration 7 "*(W ^* 2W ", 'wherein ꝗ indicator system is the result of a change that is fixed execution time:. N (*w) = tn* (w '),That £ w, - = £ ¥ [☆] + Qn (w ').

(2) Memory bounded speedup memory is bounded formula acceleration ratio is 2W * SN (W ') =+Qn(W *) in the formula, ꝗ indicators through the system is changed, and M is the upper bound on the memory of each processor, and W = Then *= G (NM) = g (Ng ~ x*(W)).

(3) General speedup

General speedup suitable for shared virtual memory environment, the formula is*'^ -Cp* (:?, W) Generalized Speedup = 1 CXs.Wo/In the formula, 4 (〗, W) is the degree of parallelism in system Z p processors are available in the ash produced upon completion of the work cost.

• based on the efficiency of the method

Efficiency £: refers to the acceleration of each individual generated by the processor, i.e.,*Eik) - S (k) / k0*

Ananth Y. Grama put forward isoefficiency [] 5'⑹ method to measure the scalability of the system. The system consists of a parallel and a parallel architecture running parallel algorithm in the above composition. K is the order of execution time of the execution time of an algorithm on a processor. 7 parallel execution time; A parallel algorithm is the corresponding execution time on the processors. All processors in the time it takes to do the work of those not sequential algorithm called overhead 7. Then / 2; = is the +7 ;. Then the speedup is*S = -y =* effectiveness^{E}= ^ = *Ti + T* =. The assumption is to perform an operation cost,WIs the question # 1 +J i ± QiTw + Is based on a constant efficiency, then W = KT. This is the famous soefficiency function. This method is suitable for parallel combination algorithm / architecture.

Parallel system execution time is an important indicator of efficiency. Each node is a parallel system symmetry, the number of nodes is a suitable scaling properties. However, these properties are not suitable for scale distributed systems, the above measurement method can not be used in a distributed system. Prasad Jogalekar and Murray Wood- side as a distributed system is proposed based on P-scalability ^ 17 "based on cost - efficiency scalability metrics M, where efficiency is a function of system throughput and quality of service. The system to be scaled system under the control factor 々 telescopic retractable-based strategy. A («response represented per second throughput; / (« is an average for each response, the service quality obtained by the calculation; CA) is the second operating cost, productivity F (fc) = A («* / («/ [:(" scalability*In ih, k2)* =FCfeVFCfc).

7.4 Distributed Resource Scheduling and Management

Distributed resource management is the foundation of distributed systems and applications, the efficiency of resource allocation and scheduling directly determines the upper system and application scalability. This section analyzes two modes distributed resource scheduling and management systems typically they correspond.

Distributed Resource Scheduler resource scheduling around, build a resource management system, monitoring the status of each resource, the state feedback to the resource scheduler basis for decision-making. The allocation scheduler made, the underlying operation of the resource assigning resources on different nodes. Resource allocation and resource operations can affect the scalability of the system, the program determines the resources needed tasks can be scheduled time, and the operating efficiency is determined resource scheduling resources for time-consuming, both the joint decision the system for mission needs and resources change change of reaction time, thus affecting scalability.

According to the core control program whether the resource allocation, distributed resource management system can be divided into central and distributed modes. Center scheduling of distributed resource management system for all resource requests to the dispatcher core processing, each node to allocate resources from the core program. And distributed scheduling request received by the one computing node that interacts with other nodes and negotiation to complete resource allocation.

7.4.1 center scheduling mode

Distributed scheduling central resource management system typically consists of four components, which are the scheduler, information storage center, and local resource allocator resource manager. Scheduling system generally center of the frame shown in FIG.

1 Early devices tune ~ h'~ Disappeared consultation resources' task
information storage centerI
I 1-? - New stays source, task information
Resource allocation life resource allocation command
I local resource is to 1 I managed locally owned I Cl I management
I Local resources ~ i I Local resource ~~ i I Local resources1 ~

FIG center scheduling resource management framework 2

In this framework, four components function as follows. .

Scheduler: a recipient who is performing resource scheduling algorithms and the scheduling request, it according to the specific content of the request, to store the state information stored in the center resources and tasks based on the information, a resource allocation calculated by scheduling algorithm program, and to pass this program to the resource allocator.

Information Storage Center: stores real-time status information resource and task information is based scheduler to make resource allocation scheme, the scheduler can obtain this information by means of active queries.

Resource allocator: executor actual resource allocation scheme, resource allocation scheduler administered will be split into smaller units, i.e., resource allocation command. Each resource allocation command is a tuple, includes a resource identifier and a node corresponding to the number of resources in the resource node to be assigned. At the same time, resource allocator also responsible for updating the information stored in the center.

Local resource managers: a monitoring and resource allocator on each resource node, it receives resource assignment command, task running state and resources on the node is requesting allocation amount of resources, and monitors the local node, to these states feedback to the resource allocator, update the information stored in the data center by the resource allocator.

Having a central dispatch resource management system are representative of resource management framework to Karl Czajkowski element calculation proposed by [19], LegioJ® and Nimrod / G [21]. Here will be described a workflow system dispatch center by Legion.

In Legion, the resource node using the resource reservation mechanism to allocate local resources. That is, for a particular resource allocation command, the command is transmitted to the monitor after parsing a resource nodes corresponding to the node according to a command to reserve resources for the task, the task is completed before, the resources are not occupied. Meanwhile, the resource node is also responsible for updating the status of tasks and resources, it can add its own initiative or update information collection center, collection center can also ask information resource node to get the information they need.

Legion, a typical resource allocation process is as follows.

1)Decision steps of: receiving a resource request dispatcher, and content information via a state inquiry information collection center resolution request tasks and resources, to generate a resource allocation scheme in accordance with pre-defined scheduling policy.

2)Negotiation procedure: resource allocator received from the scheduler at resource allocation plan, test the legality of the plan. If legitimate, you step into the assignment; if illegal (for example, on a resource allocation exceeds the number of nodes required resources are available), the resource allocator will consult with the scheduler, draw a new legal program. Consultation is based on information gathered in the center of information and resource allocation.

3)Allocation step: resource allocator according to legal resource allocation, set aside resources to send commands to the monitor, the monitor command after receiving the required number of reserved resources to the task at hand locally. After reaching the mission, monitors start the task, and the task of monitoring the local operating conditions and status of the local resources.

4)Information Update: after the task starts running, the resource node update or add tasks and resource center to collect information according to predetermined time intervals status information, information collection center can also take the initiative to query information on the resource node.

More than four steps cycle, after the end of the updating, in a new round of decision-making steps and start again, request assign the task to the next, until after resource scheduling all tasks are completed, the cycle stopped.

Center scheduling of resource management can better maintain the scalability of the system when the system load is small, because the scheduler can obtain status information for all of the tasks and resources of the system from the information storage center, according to the information to make quick one-step decision-making and resource allocation command to the resource allocator to complete. However, when the system load is large, the scheduler needs many requests handled frequently, resulting in slower response scheduler, the system takes a long time to reschedule, poor scalability of the system.

7.4.2 distributed scheduling mode

Legion resource distribution frame is based on the aforementioned center scheduling. The disadvantage is also obvious dispatch center, it is only one component to make resource allocation decisions, this component can easily become the bottleneck of the system. When it appears the problemWhen the resource allocation system will not be continued. Distributed scheduling a plurality of frame members are able to fulfill the functions of components of the resource allocation, thus avoiding a significant system bottleneck. Distributed scheduling mode resource management system, the nodes are connected to each other through a communication configuration of FIG, any node can be connected and their synergistic partners to meet the resource request received.

For a distributed scheduling mode of each node, it has three components.

1) Communication components: for partners and other nodes to communicate, collaborate and is the basis for decision-making among resource nodes.

2)Decision component: the core node control unit determines the collaborative way between the node and the final resource allocation algorithm specified.

3)Local resource management components: monitor the status of local resources, the decision to provide the basis for decision-making components.

ARMS (Agent-based Resource Management System) [20] is a typical distributed resource management system scheduling mode. Agent is autonomous intelligent software entity that has autonomy, through communication between each other in the case of goal-driven between social, reactivity and adaptability characteristics, Agent, to changes in the external environment and events make in response, the completion of certain tasks. In ARMS, each Agent embodies a resource in the system. Agent organized in a hierarchy, the structure shown in FIG. 5, FIG Each node is an Agent.

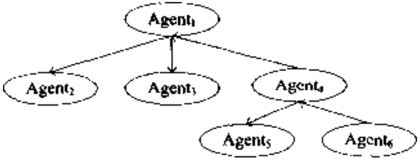
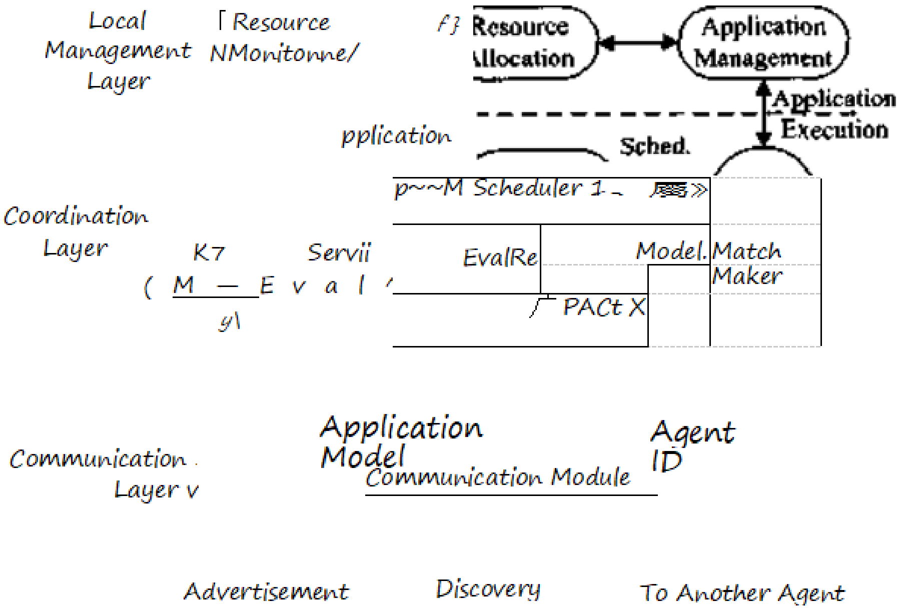


FIG 5 Arms hierarchy of Aqent

ARMS is divided into three layers in the Agent, namely the local resource management, collaboration, and communications layer layer. Agent of the structure shown in Fig. ARMS Agent in functional layer 3 as follows.

. • communication layer is responsible for communication with other Agent Agent, the information is divided into three types: 1> Advertising (Advertisement), a new Agent



Aqent structure of FIG 6Arms

When the hierarchy, its use of advertising information She Agent announce their presence; 2) exploration (Discovery), information is requested to explore the resources of distributed applications; 3) forwards (To another agent), and it has itself when Agent know when the parent node, child node can not satisfy a request, it will forward the request to their adjacent nodes, by the neighboring nodes continue to look for the right resources. A- gent or when a neighboring node was found to meet his request, the request will be forwarded to the node from the neighboring node to complete the work allocated resources.

Collaborative layers: a core structure of Agent, Agent using the ACT (Agent Capability Table) to maintain itself, the performance of the information resources of parent and child nodes Agent Agent represented. ACT can be divided into four categories: 1) T_ ACT, to maintain their own information; 2) L_ACT, the child node is used to maintain information on Agent; 3) G_ACT, the parent node is used to maintain information on Agent; 4) C "ACT, used to maintain cache Agent information.

Scheduler to schedule tasks by estimating the end time of the request, the purpose of scheduling is to find a minimum of the end time. The end time of T- = exet-Yts, exet request is an estimated execution time, ^ is the time of the request started. PACE (Performance Analysis and Characterize Environment) engine can be estimated ep "ARMS application contains a request application model (ap at the request of the situation and application of local resourcesplication model, am), an end time estimated by PACE to the eval function is defined inside the associated previous request. Agent estimated order to fight the use of ACT is: C_ ACT, T_ ACT, L_ACT, G_ACT. The estimation result, find the minimum corresponding to ACT. If T_ACT, Match Maker transmits the scheduling result to the local management, local resource allocation. Otherwise, it forwards the request to the ACT corresponding Agent. If you do not meet the conditions of ACT, forwarded to their parent and child nodes will be requested to continue the process of finding the above by the parent and child nodes, until the ACT meet the conditions found.

Local Management: Responsible for monitoring of local resources, allocate and manage applications, is the interface layer and a local Agent underlying system.

Distributed scheduling resource management system applied to the load is larger, making the specified dispersed into the respective different nodes in parallel, so that the system can still quickly re-scheduling of resources under heavy load. In a small system load, a node to make scheduling needs to communicate with multiple nodes, but this reduces the efficiency of decision-making and reduce the scalability of the system.

8 Status Scalability Testing

Testing and verification is the basis of evaluation of scalability. Scalability can be tested in two main ways: 1) the test code level. By performing the test a plurality of sets of different conditions, and the evaluation code blocks in each test program in response to the correlation coefficient of the total time. Comparative tests in all groups the code block correlation coefficients, to measure the degree of parallelism of the code block. By the degree of parallelism of each code block scalability assessment procedures. 2) system level test. System-level testing by estimating the work load, real-time monitoring of test runs and test run results to comprehensively evaluate the program scalability.

In most studies, scalability, just as a test of performance indicators, for scalability current testing methods and systems more limited study itself. The following describes a code level, respectively, and a system-level test method scalability.

8.1 Test parallel code Scalability

Parallel scalability of the code can be obtained by analyzing the performance of each code block: block parallelism as possible, a small increase in processor instructions can protectParallel efficiency program; otherwise, need to add more processors to maintain the efficiency of the program. Testers often modeling approach to analyze the performance of the system or program, system and application depending on the composition and structure of internal model modules constructed interrelationships system performance analysis.

Because of the logical relationship between the structures and components internal parallel computing systems are complex, difficult and expensive modeling, and difficult to guarantee the correctness of the model. To this end, Gordon Lyon [24] Chu mention the DEX (statistically designed experiment) method, the test of DEX parallel programs and the system as a complete whole experiment, the various parameters of the system considered snippet and each factorial experiments . Based on the operation result of the program, by monitoring performance metrics for each parallel program code modules, using statistical methods to analyze the impact of each block of code in the program run time, each code block obtained degree of importance of the efficiency of the algorithm. DEX introduced the SP (synthetic perturbation), for applying respective test disturbance factors, for the manufacture of these perturbations delay system is running, the experiment used to build the mapping factor experimental results. When a factor / is applied perturbation can cause a delay of the disturbance analysis to measure / degree of influence on the system or running.

DEX parallel program for the purpose of a test of P, P identify code blocks may be run bottleneck. DEX, the experiment in group units. In the same set of experiments, the various factors of the system remains unchanged, and for each code block in the disturbance continues to change, by perturbation analysis of this group of experiments and proceduresThe relationship between the running time, come running time of the sensitivity of each code A large block, when the time delay is applied to the same length of the disturbance, resulting in the greater run time delay. Followed by another group of experiments, the system change factor (typically the number of processors), in case of increase or decrease the number of processors, the value of £ reanalyzed each code block. The final possibility, the same block comparison value £ both experiments, was observed in the case of increased processor £ growth rate, the greater the increase £ module, indicating that the block parallelism worse, become the bottleneck of the Big. If £ processor increases with decreases, then the degree of parallelism is preferably block, the smaller becomes the bottleneck possibilities.

8.2 Scalability Test System Design

Scalability reflects the ability of the system may vary depending on system needs and resources change, continue to meet performance requirements. Scalability test systems need to focus on changing the relationship between system requirements and resources and system performance, so the scalability test system can be divided into the following four modules. -

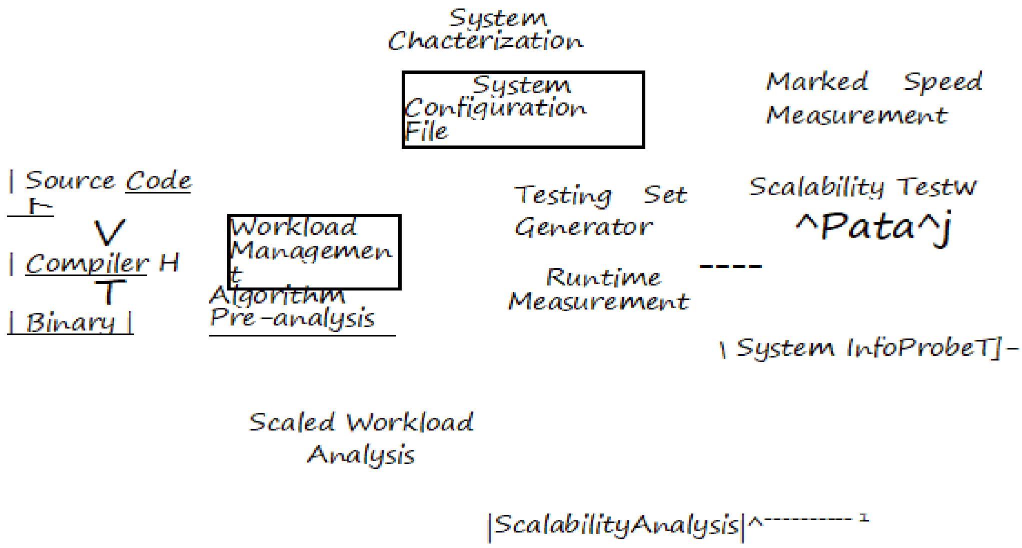
1)Workload Analysis Module: for real-time capture and analysis of dynamic workloads.

2)Resource performance analysis module: for real-time analysis of the changing performance of the underlying resources.

3)System performance monitoring module: used to capture performance data at run time, for further analysis.

4)Scalability Analysis Module: The first three modules data captured in real time to analyze the scalability of the system.

STASCScalability Testing and System Analysis) [23] a - a typical system-level testing system scalability, which consists of four parts: the system wherein component analysis algorithm pre-assembly, assembly and test scalability analysis scalability components. STAS is characterized by its combination of workload algorithms and final test response time, combined with the load and the resources to make an assessment of scalability. Meanwhile STAS also supports testers definition of scalability testing methods since. STAS structure shown in Fig.



A configuration diagram of FIG. 7 STAS

Wherein the system components: Its mission is to obtain information on the underlying system, and measure the performance of each node is calculated. It is divided into two modules: a system information detection module and node performance measurement module. The system information detection module detection system of each node, or nodes from deduplication unavailable, leaving only active nodes. For activitiesNode, Node performance measurement module to measure the performance of the node by a user-defined bench- mark. The final output of this module is a set of tuples: <node name, property>.

Pre-analysis algorithm module: it analyzes the source code of the distributed algorithm as input, workload output files, and executable algorithm. The work load analysis algorithm can be done at the same time compiler, you can also employ user-defined analysis mode. User to measure the load artificially algorithm specified by the equation between the input data and the workload.

Scalability test components: it is responsible for runtime scalability test systems and algorithms in the manner defined by testers. It consists of three modules: the test module set is generated, real-time measurement module and a database module. The test set generation module from the first two nodes, each node will be expanded to twice the size of the last. And the test set the algorithm to obtain the pre-analysis module executable files and algorithms incorporated by load input time measurement module ultimately be stored and test execution time with these parameters to the database module for analysis component analysis.

Scalability Component Analysis: database module in its data by using the algorithm and to calculate the scalability of the system is defined iS0Speed-ew.

9 Cloud explore the system scalability problem computing background

SaasCSoftware as a Service) model is based on the new software application software to provide Internet services, Saas provide users with a complete software, users can access the service via the Internet, only in accordance with their needs to the rental service provider, eliminating the need for purchase hardware, software development and ongoing maintenance costs. Cloud computing is parallel computing and distributed computing concept development, which provides a reliable infrastructure for Saas. The cloud is able to self-manage and maintain a collection of virtual computing resources. Cloud computing has the following characteristics: 1) scalability, the size of the cloud can dynamically expand and contract to meet the changing needs of users; 2) pay-as, users can own actual consumption of cloud resources to buy paid; 3) very large scale, the scale of cloud computing in general has reached more than hundreds of thousands of servers; 4) persistent, cloud computing system can provide long-lasting computing resources and capabilities for the user. These Unlike traditional distributed and parallel computing features, metrics on scalability for cloud computing, design and testing to bring new and challenging issues.

9.1 Cloud computing scalability of the problem

Cloud scalability is not only the traditional focus on scalability, but also emphasize the contraction of the cloud. One of its important features namely pay-on-demand, allowing multiple cloud tenants in a shared cloud computing resources can save costs as much as possible. This requires the user's application workloads in a small time, be able to reduce the consumption of resources applications, while reducing resource consumption can maintain the performance of applications, to meet the needs of users. Scalability more traditional focus on behalf of the "extended" scalability, in the case of computing resources increase, the growth rate of a certain measure of performance indicators. In contrast, cloud computing is also concerned about the "shrinking" in this regard, namely to reduce the workload, application performance can still get the case to meet the cloud can be recovered resources, improve resource utilization, reduce the ability of the user fee. Measure shrinkage of cloud computing include not only a measure of resource growth brings increased performance, but also include measures to enhance the degree of reduction of resource utilization metrics and user fees when the load decreases.

9.2 Cloud computing scalability design issues

Cloud computing large scale features make the same number of resources in a cloud computing platform becomes very large, the performance requirements of the Resource Management System is also higher. In the center scheduling and distributed scheduling modes, when the scale of the cloud, the central dispatcher scheduler will become the bottleneck of the system. Accordingly, the cloud is more suitable for distributed scheduling paradigm. The distributed scheduling the decision-making distributed to each node, reducing the probability of occurrence of a bottleneck. At the same time created a new problem: resource allocation is carried out through communication and collaboration between the different nodes of the multi-party collaborative decision-making model is more complex than the type of decision-making center.

In a distributed scheduling, multi-party collaborative decision-making model design requires attention to the following questions.

Heterogeneity between nodes: the ultra-large-scale cloud computing system, there will be different structure of resource nodes. When scheduling the nodes of these isomers, these isomers can not directly operate nodes need to design an abstract resource node to mask the differences between the different nodes, the upper operation only acts in the abstract resource node.

Between node communication protocol design issues: agreement between the node defines the format and exchange of information, and the information exchanged between the nodes constitute the basis for scheduling algorithms to make decisions. In the design of the protocol, the protocol needs to take into account the accuracy and completeness of the problem. To ensure the accuracy of the information exchange between nodes is error-free, and to ensure the completeness of the agreement can cover all possible scenarios of the exchange of information between the nodes to avoid because of lack ofLess of aTreatments scene and error.

9.3 Cloud computing scalability testing issues

Test as a measure of system scalability based on the test system should be designed for the characteristics of the test system. Cloud computing scalability test system should have the ability to solve the following problems: 1) the ability to monitor real-time, cloud computing has the characteristics of durability, but also can not be accurately estimated workload, resource performance at the moment, so it is necessary to test the system can capture real-time data, comprehensive application performance metrics to analyze the cloud computing platform scalability; ability 2) two-way test, as opposed to the traditional distributed computing only focus on capacity expansion, the test should be concerned about the same time, "stretch" and "shrink" both to analyze scalability or contractible under different scenarios. When increasing the applied load, as measured by the number of new scalability of resource allocation and use of lift; when the load decreases, is calculated by the number of resource consumption reduction measure shrinkage properties.

ConclusionScalability as an important attribute of the cloud, with the development of cloud computing and Saas, which has become a hot issue ®f of study. Scalability definitions and metrics will also vary with the different scenarios. In the context of cloud computing, scalability research focus will be to define and measure the scalability when resources are shrinking, heterogeneous cloud resource allocation and resource nodes in real-time two-way scalability measurements.

10. Improved Byzantine consensus research

10.1POINTNITY proposed extended definition of validity attributes

Structurally, it is composed of two parts.

• The first component is reduced to a binary multi-value consensus consensus. Reduced, which is fully synchronized, neither randomized nor is the ultimate leader, there is no signature. To our knowledge, this is the first asynchronous reducing unscheduled always determine the value 0 (1) binary consensus sequence. The earliest examples of reducing wait before terminating only reliable broadcast concurrent instances of spawning binary consensus. Because it is assumed that t <N / 3, where n is the number of processes and t is the number of errors during the upper bound, this reduction is best toughness.

• The second component is a binary Byzantine consensus (BBC) algorithm, neither randomized nor the last leader, there is no signature. It is broadcast on the appropriate binary value (BV-broadcast) abstraction, for introducing randomization consensus. Calculated from a point of view, the BBC algorithm requires t <N / 3 (as previous reduction) and additional synchronization hypothesis, i.e., a time after which transmitting a message transmitted by the non-defective by the process delay constants sector (this happens, but neither the time, nor is it a constant process known own. in practice, this means that the BBC algorithm always terminate unless the transmission delay is always increased (in this case, different assumptions synchronization as described may be used).

The resulting multivalued Byzantine algorithm is optimal consistency and toughness (T <N / 3), and the best time, since it terminates at 0 (t) is. In addition to its optimal characteristics and the concept is simple, multi-value obtained by the Byzantine consensus algorithm is well suited for the consortium blockchains three following reasons:

The algorithm does not use leaders elected (in favor of the value proposed by a particular process), or proven to work - which means that the consensus of each participant plays a role equal to the value proposed. In particular, because it does not depend on the verification of work choice, because more than any other time in Bitcoin ticket or revenge, node consortium could not reach a consensus. We have noticed that in June 2016 Revenge of R3 R3 50 machines consortium in a machine owned by a consortium of revenge blockchain total mining capacity, which gives a significant advantage of this machine to attack 12% blockchain of.

The algorithm is to indulge in, it is always safe despite any delays. We believe this is an important characteristic of every day, one million $ US trade volume blockchain applications1Financial institutions may prefer their blockchain service is not available, rather than undermine, after the Internet communication delay congestion impact. This is usually used as test bed consortium R3, wherein attacker can decide to use the network delay Revenge algorithm block contrast double spending two conflicting.

Finally, because we focus on the consortium blockchain model in which the consensus of participants is limited to members of the consortium, we can assume the identity of n consortium members are known by all participants. Usually only a subset of all the participants involved in the consensus blockchain, for example, only the consensus N = 15 out of 50 treated R3 is participating. These provide us with the identification of Sybil attack algorithm a natural protection without the need for any expensive verification mechanism.

Roadmap sheet 7 constituting part. Computational model described in Section 2. Section 3 describes the Blockchain Byzantine consensus. Section 4, in binary Byzantine agreement, reducing the multivalued Byzantine agreement, Section 5 presents the final synchronization relies on a binary hypothesis Byzantine agreement. The composition of these two algorithms provide free leader, no signature, no randomized and multi-valued

Byzantine consensus. Section 6 describes related work. Finally, Section 7 concludes the paper.

10.2 Byzantine basic computation model and reliable broadcast

2.1Base calculation model

The processing system is processed by the asynchronous asynchronous order n, i.e. gang door = 1, ..., PN} is a set of n;. " ″ index" i is called PI ″ means that each asynchronous process proceeds thereof at their own pace, which may change over time and is still unknown to other processes. "Refers to a sequence ″ a process step is performed once. This does not interfere with its proper multiplexing multiple threads of execution.

Local processing time is negligible with respect to the message transmission delay, which is considered to be zero. (We show you how to relax this assumption in Annex B and C) and two representations GY PIGY I used to say, PI belonging to the set Y.

Processing of the communication by the communication network via the asynchronous message reliably to-point switching network. "Asynchronous ″ mean there is no restraint on the message transmission delays, but these delays are limited." Reliable ″ refers to the network is not lost, copy, modify or create messages. "It refers to any connection point ″ processing a bidirectional channel. Thus, when the process receives a message, it can recognize its sender.

Method, the PI by calling the primitive "to TAG (m) to pj is ″ wherein TAG is a type and m the message the contents of which sends a message to a process PJ. To simplify the description, assume that a process can send a message to itself . method, PI message received by the execution of the original "received ″ . Macro operation of the broadcast TAG (M) is used as "PI en pies for each TAG (m) to the end of pj ″ shortcut.

Fault model can process up to T exhibit Byzantine behavior. A Byzantine process exhibit any of the methods: it may crash, can not send or receive messages, send any message, to start in any state, performing any state transition, and the like. In addition, the process can be Byzantine collusion "pollution ″ calculations (e.g., but they should send a message with different content having the same content transmitted message, and, if they are non-fault). Behaviors exhibited Byzantine fault process is known. otherwise, the non-fault.

Let us note that since each connection is handled by the channel, the Byzantine process may not impersonate another process. Byzantine process which can control the network message is received by sequentially modified, but they are not always defer message received.

Symbol Abbreviation BAMPn, T [0] is used to represent the previous calculation substantially Byzantine asynchronous MessagePassing

Model; 0 means no additional assumptions.

In the Byzantine system

2.2Reliable broadcast

This abstract definition of broadcasting (in short, RB- broadcast) proposed by G. of Bracha. It is a single-trigger pair abstract all communications, which provides two processing operations and represents RB_broadcast RB_deliver. When the PI call operation RB_broadcast (respectively, RB_deliver), we say that it "RBbroadcasts ″ message (respectively," RB- provide ″ news). A broadcast RB- e.g., when the process

px is the sender, defined by the following properties.

RB- effectiveness. If a non-faulty process from the non-fault-pixel processing, and provide RB-meters PX RB- broadcast message m.

RB- Unicity. A non-faulty process RB- provide a message from a pixel at most.

RB- termination 1. If there is no defect and RB- PX broadcast message m, all non-faulty process from the final

PX RB- provide meters

RB- termination -2. If a non-faulty process RB- PX message delivered from the m (may be faulty), all non-faulty process ultimately provides the same message m from PXRB-.

Output RB- validity attribute refers to the input terminal, and RB- unity indicates that no duplicate message. Event of termination statements that the process must RB- deliver the message. Their second is what makes broadcast and reliable. It was shown in a t <N / 3 is the upper limit for T, when performing such an abstraction has.

Let's remark, it is possible that the value can be delivered by non-fault RB- process, but it is actually a Byzantine and the sender has not invoked RB_broadcast. This is possible, for example when the sender Byzantine network level, in which several messages sent to different subsets of the playback process occurs, and executes a predicate RB- RB- transport algorithm is abstract broadcast messages in a final satisfaction. When this happens, by abuse of language, we say that the sender of the call RB- broadcast. This is achieved by the fact that, in this case, the non-faulty if the sender is not the process can not distinguish between a fault or motivation.

Additional constraint t symbols substantially enhanced computational model <N / 3 are expressed BAMPn, T [t <N / 3].

The algorithm implemented in the algorithm described RB- broadcast BAMPn, T [t <N / 3]. Accordingly, it is the best toughness t. The algorithm requires three communication step, application in a broadcast message. Only two model systems BAMPn communication step algorithm, T [T <N / 5] are shown.

10.3, Blockchain Byzantine consensus

As propagation algorithm consensus on all the news value is assumed (multi-value and binary consensus algorithm presented below), all non-fault process raised.

Based on the effectiveness of the predicate

10.3.1Multivalued Byzantine consensus

In this paper, we consider a generalization of the classic Byzantine consistency, the introduction informally. Because of its effectiveness requirements excited by blockchain, depends on effective application-specific O predicate to indicate whether the value is valid, we call this question the effectiveness of the Byzantine predicate based consensus (expressed VPBC) and define it as follows. Assume that each process is not flawed, it proposed an effective value, each of them has in such a way, also has a satisfactory value determines the following properties. 2

VPBC termination. The value of a final decision on each non-faulty process.

VPBC- agreement. Two non-fault decision process is not different values.

VPBC- effectiveness. Value determination is effective, it is effective to meet the expressed predefined predicates.

The classic definition of this definition Byzantine general consensus, excluding the predicate effective. As an example, in a collision fault model, any proposed value is valid. In the Byzantine basic consensus, any suggestions values are valid unless all non Troubleshooting made the same value V, in this case, only V is effective. This predicate into account the introduction of the consortium blockchains, as well as other possible specific distinctive features Byzantine consensus problem. In the context of the consortium blockchains, proposal is not valid, the hash value is added to the appropriate Blockchain last block if it does not contain.

10.3.2Binary Byzantine consensus

Multi-valued VPBC implementation relies on a potential binary Byzantine consensus (expressed as BBC). It's a free leader, as well as free signature free randomization implementation described in Section 5.

This duality Byzantine consensus validity attributes are as follows: If all non Troubleshooting made the same value, no other values can be determined. To prevent confusion, the nature of the validity of the termination agreement and the BBC is denoted

BBC- effectiveness, BBC- agreement and BBC- termination.

10.4 from multi-value to binary consensus Byzantine system

This section describes the consensus of the former Byzantine binary, reducing the value of multi-Byzantine consensus. We reduced guarantee an end after two binary sequence consensus instance. This is, to our knowledge, the first predetermined deceleration value of the non-consensus sequence in the example of a binary 0 (1) determined. Other reducing or returns a predefined value if the consensus Shang suspension, or intolerance and Byzantine fault required to perform a binary sequence consensus instance dlogne. Our reduction is based on the abstract RB- broadcast communications, and examples of the underlying binary Byzantine consensus. Let BBC said that to solve the computing power required for two yuan Byzantine consensus. Thus, "multi-value to binary 〃 reduce work model BAMPn, T [t <N / 3, BBC]

10.4.1The reduction

Binary consensus object as mentioned earlier, in addition to broadcasting RB- abstract, the method can mark BIN_C0NS [1..N] two yuan Byzantine array of cooperation consensus object. Examples BIN_C0NS [k] allows the process to find the value of non-fault by PK proposed agreement. This object is achieved by binary Byzantine consensus algorithm presented in Section 5.

To simplify the description, we think that this is a process which is involved in PI Release BIN_C0NS [K] by calling BIN_C0NS [K] .bin_propose (V), wherein, vG {0,1}. Then, it executes a particular thread, and finally returns the value corresponding to the code determined by BIN_C0NS [K].

Each process PI-managed local variables following local variables; Shang default values can be represented by one (failure or no failure) processes proposed.

Array proposalsi [1..N] is initialized to [Shang, ..., Shang]. proposalsi [J] of the object comprising

PJ recommended value.

bin_decisionsi initialized to [1..N] [Shang, ..., Shang] array. bin_decisionsi [k] of the object

It contains the value (0 or 1) is determined by the binary objects consensus BIN_CONS [k] is.

Operation mv_propose (VI) is

(1) RB_broadcast VAL (vi);

⑵ If Repeat 3 K: (Proposalsi [k] = Shang 6) eight (BIN_CONS [K] .bin_propose not call)

⑶ then call BIN_CONS [K] .bin_propose (1) END IF;

Until ⑷ (3 ': bin_decisionsi ['] = 1) terminal repeat sequence;

Such that for each k ⑸ BIN_C0NS [K] .bin_propose () call Not

```
⑹ not call for BIN_C0NS [K] .bin_propose (0) end;
⑺ wait      Mill _decisionsi [X] 6 = Shang);
J <- min {x satisfies bin_decisionsi [X] = 1};
wait_until
(Proposalsi [j] = 6 Shang);
Return (proposalsi [J]).
When VAL (v) is delivered from PJRB- do, if valid (V) and then proposalsi [j] of "V off if.
When the BIN-CONS [K] _bin_propose () Returns a value b do bin_decisionsi [K] f Bay
```

The algorithm of the reduced multivalued binary Byzantine Byzantine consensus consensus is described in this algorithm, a procedure call operation mv_propose (V), wherein, v is its value pseudomultichannel consensus value 1 in FIG. A process pi behavior can be broken down into four stages.

•Stage 1: PI propagation value (lines 01 and 11). A method by calling the first PI RB-broadcast operation (wire 01) which processes the transmission of all values. When a transfer process RB- a value of PJ vRB- broadcast technology, it is stored in proposalsi [j] if v is valid.

•Phase 2: PI has been involved a first set of binary consensus instances (lines 02-04) is.

Then, the PI enters a loop where it began to participate binary consensus Examples BIN_CONS [K], it is proposed 1, each process from PKRB- having associated delivery suggested value (lines 02-03). Examples of pi found consensus binary BIN-CONS ['], wherein 1 is determined (line 04) to stop the cycle. Stage (2) arriving after the (binary consensus of our proposed after allowing only O (1) delay the end of the message.

•Stage 3: PI began to participate in all other binary consensus instances (lines 05-06).

It knows a binary instance of consensus decision after 1, PI call in all instances it has not been involved in binary consensus BIN-CONS [K] bin_propose (0). We note that this is possible, some examples of BIN-CONS [k], and no process has the process associated with a value PKRB-. The purpose of these common shares is to ensure that all binary consensus, the final termination.

•Stage 4: Determined value for pi (lines 07-10 and 12).

Finally PI consensus that successful binary objects, i.e., the first (according to the process sequence index), i.e., those that returns 1 (line 08) is. 3 Let BIN_CONS [J] is such a consensus binary objects. Since the decision value of 1 is associated, at least one non-fault proposed procedure shown in FIG. 1, which means that the process values from the PK line 02-03) RBdelivered of. We observed that, due to the termination of -2 RB- property, the value of each process is final RB- delivered without defects. Thus, PI decided that (lines 09-10).

10.4.2Correctness prove

Lemma 1Yes determine the value of at least 1 case of a binary consensus of all non-fault process exit repeat the cycle.

From the operational point of view, this lemma can be restated as follows: At least one 'e [i..N] so that each non-faulty process P1, we end up with bin_decisionsi ['] = 1.

Evidence is contradictory. Let us assume that, in the process of any non-fault P1, no bin_decisionsi ['], 1 <' <N, 1 is set to continue. Thus, there is no non-faulty process exits "〃 repeated loop (line 0204). As a non-valid value when the fault occurred PJRB-broadcast, it follows from the RB-terminated -1 characteristic, each non-fault process PI RB- PJ's proposal to provide effective, so we end up with proposals! [j] = 6 in each non-PI Shang treatment failure.

It follows the first sub-predicate from line 02 of all non-fault handling Pi call bin_propose (1). In the object BIN_CONS BBC [J]. Therefore, from the BBC termination, BBC- agreement, BBC- effectiveness, and intrusionTolerance, which returns values for all BBC process instance to a non-fault, wherein the outlet "〃 cycle is

2Lemma 1

repeated.

Lemma 2Determination value is a valid value (i.e., it is effective to satisfy the predicate).

We first prove that observed for a value proposalsi [J] is determined by the circumference of a process, we need bin_decisionsi [J] = 1 (lines 08-10).

If the value is 1 when BIN_CONS [j], bin_decisionsi [j] = 1 is a processing decision PI (line 12) in each non-fault final true. If only one example proposed a BBC, and (ii) BIN_CONS in line 03 from (i) the value [J] intrusion resistance, i.e. at least one non-fault PI procedure call BIN_CONS following facts [j] of .bin_propose (1). Because the predicate line 02, this is such that the non-faulty process pi proposalsi [j] it calls BIN_CONS [j] of .bin_propose (1) 6 = Shang. Since the line 11, it follows proposalsi [j] contains a valid value.

Lemma 3Two non-fault decision process is not different values.

Let us consider two prove any non troubleshooting Pi and PJ, so Pi decided proposalsi [K] and PJ decided to proposals〗 [K2]. It follows from line 08 is K1 = min {x satisfies bin_decisionsi [X] = 1} and k2 = MIN {x satisfies bin_decisionsj [X] = 1}.

Ontheonehand, itfollows even omline07that (V1 <x <nbin_decisionsj [X] 6 = Shang), from which we conclude that both pi and PJ known binary values determined by each instance of binary Consensus (line 12). Due to the properties of each binary consensus agreement BBC- instance, we have Vx: bin_decisionsi [X] = bin_decisionsj [X].

Let decanoate [X] = in_decisionsi [X] = bin_decisionsj [X]. From line 08 it is K1 = K2 = min {x dec satisfy [X] = 1} = K then follows. Thus, decyl [K] = 1.

On the other hand, it is derived from a non-faulty process p BIN_CONS [k] intrusion resistant properties' call BIN_CONS [K] .bin_propose (1). Line 03 may be sent as the only call, we conclude that (predicate from line 02), the proposals' [K] = V 6 = Shang. As p 'is no failure, and it follows from the RB-RB-terminated -2 unity for all non-fault handling characteristics supplied from PK RB- v. Thus, we end up with proposalsi [K] = proposals〗 [K], which concludes the proof of Lemma.

Lemma 4The value of each non-fault handling decision.

It follows from the proof of Lemma 1, there are some PJ allows us to finally have bin_decisionsi [J] = 1 in the process of all non-fault and non-fault does not always online processing block 04. Therefore, all non-fault process calls each binary consensus instance (line 03 or line 06). Further, due to their characteristics BBC- termination, each of n binary consensus instance returned in the results of each non-faulty process (line 12). Thus, in the always-on 07. Finally, no trouble-free process PI block, as seen in the proof of Lemma 3, line 09 predicate is free from defects in every process, summed up the proof of the lemma, ultimate satisfaction .

Byzantine Consensus Model (VPBC) of a multi-value system algorithm in the tool of FIG. 1 described theorem BAMPn, T [t <N / 3, BBC].

Evidenced by Lemma 2 (VPBC- potency), Lemma 3 (VPBC- protocol), and Lemma 4 (VPBC termination) as follows.

10.5 In the final synchronization Byzantine system Binary consensus

This section describes the underlying binary consistency Byzantine algorithm BBC, which provides a process operation bin_propose. The advantage of this algorithm is that it is guaranteed to terminate, if all non-faulty process made the same value, if not synchronized and always in a constant number of message delays. The algorithm may terminate within a fixed time, this is the case, e.g., if all non-fault handling proposed by the same value. The algorithm relies on all communication to all binary abstract (BVbroadcast) and final synchronization hypothesis, which is described in the following section. The algorithm gradually established. We first present a simple algorithm, only to meet consensus safety performance (BBC- effectiveness and BBC- protocol). The algorithm is then synchronized with the final extension to meet the consensus assumptions active property (BBC- termination). The purpose of this gradual approach is for ease of understanding and proof.

10.5.1The BV broadcast to all communication to abstract all

Broadcast binary value (BV-broadcast) communication abstraction in already incorporated (which is implemented in the Appendix A review).

Broadcast to all is defined BV- abstract all communications, it provides a method BV_broadcast represented by a single operation. When a process calls BV_broadcastTAG (m), we say that it "BVbroadcasts message TAG (meters)." Content of the message m is 0 or 1 (hence the "abstract name of the binary value of the communication 〃 herein the term).

In a broadcast BV- e.g., each binary value of the non-faulty process PI BV- broadcast, and obtains a set of binary values, local variables are stored in read-only setting is represented as bin_valuesi. This set, is initialized to 0, add new values received. BV-broadcast defined by the following four properties.

BV- obligations. If at least (T + 1) during non-fault BV- same broadcast value v, v is added to the final set of non-defective bin_valuesi each process pi.

BV- reasons. If no fault is pi and vG bin_valuesi, V hexyl BV- broadcast via a non-fault process.

BV- uniform. If the value of v is added to the process P1 is set no fault bin_valuesi, final vG bin_valuesj PJ in each process without defects.

BV- terminated. Finally, each non-fault process pi bin_valuesi collection is not empty.

Play a BV- Properties The following properties are a direct consequence of the previous character. Finally, the non-faulty processing set bin_valuesi PKO becomes non-empty, (ii) becomes equal, (iii) contains all values processed by the non-fault broadcast, and (iv) does not contain a Byzantine process only by the broadcast value . However, (ii) and (iii) does not occur when the process known non-defective.

Byzantine safe binary 10.5.2A consensus algorithm BAMPn, T [T <N / 3]

We describe a simple binary consistency Byzantine algorithm, satisfy the model system BBC- BAMPn effectiveness and properties BBCAgreement, T [T <N / 3]. The algorithm, which is based on a circle, depending on

Abstract BV- previous broadcasting, have the same structure, the introduction of random consensus algorithm.

Local variables Local variables for each of the following management process PI.

ESTI: Current estimates place the value of the decision. It is initialized value of PI raised.

RI: Local round number, initialized to zero.

• box -valuesi [1 ..]: an array of binary values; bin_valuesi [R] (initialized to 0) is stored on

Stainless steel and had a monovalent BV- broadcast associated refill the local output set. (This is an infinite array can be replaced by a single bin_valuesi local variables, arrays a re-start of each round of 0. Here, we consider, in order to simplify the presentation.) • Dual: Auxiliary binary value. valuesi: an auxiliary set of values.

Message Type The algorithm uses two types of messages, indicated as EST and AUX. Both use in each round, a round number so they always appear.

EST [R] in a stainless steel by the PI value to estimate BV- broadcast its current decision ESTI be used.

AUX [R] values for propagation thereof (the broadcast (the help of the current bin_valuesi [R] by PI)

Macro actions).

Let us consider the algorithm of FIG. 2 after it has deposited the proposal The ESTI binary (line 01), each non-fault sequence into the asynchronous process PI wheel. Each round, "using a broadcast BV- example, its associated local

In the process variable pi is bin_valuesi [R].

```
Operation bin_propose (VI) is
(1) ESTI ^ six; R.0;
(2) and (really) do
(3) RI traffic RI + 1;
(4) BV_b road cast seven] _0) EDT [RI] (ESTI);
(5) wait-until  bin- value;
(6) a broadcast AUX [RI] (bin-valuesi [RI]);
(7) wait-until message AUX [RI] (b_valp (1)), ..., over different AUX
Cheng P (X), iaa - [RI]; = Ul <i; < "_ t, valx) (b_valP (N- t)) has the (TN) - receiving tons, and it  Their content is such that 3 -
Such that a non-empty valuesi (i) valuesi £ bin-valuesi [RI] and (ii) the value of
(8) bis HI mode 2;
(9) If (valuesi = {V}) // valuesi is a single, whose elements v
(10)    Then ESTI ^ V; if (V = BI) before deciding (V), if not ended, if;
(11)    Otherwise ESTI
(12)    just in case;
(13)    The end of a period of time.
```

- a security algorithm for binary BAMPn Byzantine agreement, T [t <N / 3] conduct during the non-faulty process oxygen circular pi can be broken down in three stages.

•Phase 1: The current estimate (lines 03-05) coordinated the exchange.

PI process first proceeds to the next round, and BV- broadcast its current estimate (line 04). After, PI wait until it sets bin_valuesi [R] is not empty (let us recall that when bin_valuesi [R] is not empty, it is not necessarily its final value).

•Phase 2: Estimated second exchange in favor of convergence (lines 06-07).

In this second stage, the PI broadcast (Thus, this is neither a nor RB- BV- broadcast broadcast) message AUX [R] (the content of which is bin_valuesi [R] (line 06). Then, the PI wait until it receives a set of values that satisfy the following two properties valuesi.

-valuesi £ bin_valuesi [R]. Thanks BV- reason attributes, which ensures (even Byzantine AUX false message transmission process [R & lt] () contains only the values proposed by the Byzantine process) valuesi comprising a non-fault handling only by the broadcast values.

Different processes - (t N) - the value of at least valuesi messages from AUX [R] ().

Thus, in any round R, line 07, valuesi £ {0,1} and broadcast only the value of a non-fault comprises BV- process line 04.

•Stage 3: Try to decide (lines 08-12).

This stage is a purely local computing stage, during which (if not yet complete) trying to determine the PI value b = R 2 mode (line 08 and 10), which depends on the content of valuesi.

- If the element contains a single valuesi v (line 09), then v becomes the new estimate of the PI. In addition, v is a candidate decision. In order to ensure BBC- agreement, V can be determined only if V = B. This decision is determined by the statement implemented (V) (line 10).

- If valuesi = {0,1}, and PI can not be determined. Since these two values already proposed by the non-fault process, cause such convergence protocol, selecting one of them the PI (b, i.e., the same procedure in all non-fault) as a new estimated value (line 11).

Let us observe the decision (five) PI does not terminate the call to participate in the algorithm of pi, namely PI continue the endless cycle continues. The randomization algorithm may use the techniques presented to termination. Instead, we keep it simple and to postpone this algorithm in Section 5.5 of uncertainty terminal solutions.

10.5.3Safety prove

PI process is a non-fault process, so valuesri predicate satisfied by line 07. In addition, the set of values valuesi, let us recall that in a given operation, C represents a non-fault handling in this run.

Lemma 5 provided T <N / 3. If at the beginning of a round r, all non-fault process has the same estimate V, after which they never change their valuation.

We assume that all non-faulty proof treatment (which at least N - T> T + 1) have the same when they begin estimating v Accordingly a river, they broadcast the same message BV- EST [R] (v) in a line 04 it is the duty BV- BV- reasons and properties, each non-faulty process pi is derived bin_valuesi [R] = {V} in line 05,

Thus it may broadcast only AUX [R] 06. consider any non-fault handling PI ({v}) in the line, then it follows (valuesi only comprises v) from line 07 predicate, line 09 (valuesi a single), and a distribution line 10, i.e., the value held ESTI v. 2Lemma 5

Lemma 6 ■ provided T <N / 3. (PI, PJGC) A (valuesri = {V}) A (Value: BU (-)) demonstrate this: PI is provided a fault-free process, such valuesri = {V}. It follows the same PI message received AUX [R] ({V}) from the line 07-- different processes (N t), i.e., from at least (N - 2T) different non-fault handling. The n - 2 t in d + 1, which means that the PI message received AUX [R] ({V}) from at least (T + 1) of different non-homogeneous set of process failure.

PJ is so fault-free process, such valuesrj = {w}. (- TN) different treatment. Thus, PJ received at least one group from QJ AUX [R] ({W}). It is (n - T) + (T + 1)> N, it follows that Qi nQ '= 60. Let nQ PKG together. " As PKG Qi, this is not a defect of the process. Thus, in line 06, PK send the same message AUX [R] to pi and P ", so we have V = Watts.

2Lemma 6

Lemma 7. disposed T <N / 3. Value processed by the non-fault decision, made by the process of the non-defective.

Let us prove considering the round R = 1, due to the characteristics of the reasons BV-BV- broadcast line 04, it follows that the set bin_valuesi [1] contains only non Troubleshooting recommended value. Thus, non-fault line 06 during the broadcast message AUX [1] () containing the values set by the proposed process only the non-faulty. Then, the predicate it from line 07 (i) as follows (values1i £ bin_valuesi), and abstract BVJustification BV- broadcast attributes, such that each set of non-defective values1i process contains only non-defective by the recommendation process values. Thus, ESTI distribution (either in line 10 or 11) provided by the value presented by the non-faulty process. The same principle applies to two R = 2, R = 3, etc., these results prove the lemma.

2Lemma 7

Lemma 8. provided T <N / 3. Two non-fault decision process is not different values.

Let R be a first round proved, during which no fault decision process, so that PI is a trouble-free process, (line 10) determined in a circle R, and v is a value to make its decision. Thus, we have valuesri = {V} where, v = (R modulo 2).

If another non-fault decision process during oxygen PJ wheel, we have valuesrj = {W}, and since Lemma 6, we have W = # Thus, all decisions in a non-fault handling stainless monovalent, and determines v each non-fault decision process has previously allocated v = (R modulo 2) to its local estimation in a stainless steel monovalent ESTI.

Let PJ is not a flaw, it is not decided in a stainless steel prices. As valuesri = {V}, and PJ is not a value determined stainless steel, it is not always the next Lemma 6 there valuesrj = {1 - V}, so valuesrj = {0,1}. Thus, the circular R, PJ execution pipeline 11, where it is assigned a value (R mode 2) = v to its local estimation ESTJ.

Thus, all non-faulty estimation process begins with the same local v wheel (R + 1) = RMOD2. Since Lemma 5, they will always maintain this estimate. Accordingly, no process of a different value by the non-defective, the circular R, wherein the proof that the lemma is not yet determined in the determined future rounds.

2Lemma 8

Lemma 9. Let the system model is BAMPn, T [T <N / 3]. No trouble-free process remains blocked in a circle forever.

We have proof by contradiction assume a first round, some non-fault process PI remain forever blocked. Since all non-fault termination process circle (R - 1), they have begun a comprehensive r instance stainless steel price and all calls BV broadcast. Since BV-termination characteristic line 05 wait_until () statement terminates at each process the non-defective. Then, if all non-faulty processing a broadcast message AUX [R] (line 06), it follows wait_until statement terminates in line 07 each process the non-defective. Thus, there will always be blocked in the first round during which the non-fault process is still round oxygen.

2Lemma 9

Lemma the system 10. The model is BAMPn, T [T <N / 3]. If all non-faulty process Pi terminate valuesri circle R = {V}, which are determined by the wheel (R + 1).

If all non-faulty demonstrate this process, valuesri = {V}, and r is the circle such that V = (R 2 mode), it follows that (if not already done so) from lines 08-10, one each non-fault handling decide when stainless steel prices. If r is such that, V6 = (R modulo 2), which each non-fault current estimation process V (line 10).

As the next round, we have: V = ((R + 1) mod 2), and valuesri + 1 = bin_valuesi [R + 1] = {V} in each non-fault process P1, each wheel during non-fault during the decision (R + 1). 2Lemma 10 Lemma 1. Let the system model is BAMPn, T [T <N / 3]. If each non-fault process PI terminates with a circular R valuesri = {0,1}, and it is determined by their circle (R + 2).

If each non-fault proof procedure is such that pi valuesri = {0,1}, line 11 during its execution oxygen circle, we have ESTI = (R-mode 2) = V start wheel (R + 1). Due to Lemma 5, it is always to maintain this estimate. Since all non-faulty procedures to perform round (R + 1) and (R + 2) (Lemma 9) and v = ((R + 2) we have the value of ^ 2 = W P1 in each non-fault occurred. Thus visible, each non-fault line 10 in the decision process.

Theorem 2 satisfy the safety performance of the algorithms described consensus.

Evidenced by Lemma 7 (BBC- potency) and Lemma 8 (BBC- Protocol) is proven as follows.

It described the decision does not guarantee the decision-making algorithm in Figure 2. While some non-fault process which can occur, for example made 0, other trouble-free process proposed 1, and Byzantine double play during the game, each proposal to 0 or 1 for each process trouble-free, so it will never happen, in a circle all non-faulty process ends either valuesi = {0,1}, or they all have valuesi = {v}, where v is 0 or 1. In other words, if not all of the non-faulty process made the same initial value, the process may be made after the Byzantine round, circular, having a non-fault process valuesi = {0,1}, rather than the rest of the process has a fault valuesi = {v }, where v6 = (R-mode

10.5.4Eventual synchronization hypothesis

Consensus impossibility ^ It is well known, there is no consensus algorithm to ensure the safety and fully asynchronous messaging system activity, which, even in a single process may crash. Since the collapse of the fault model is less serious than the Byzantine model fails, the process can not reach a consensus, if possible, make Byzantine fault is still the case.

In order to avoid such a possibility, and to ensure consistent termination properties, the model must be rich with additional computing power. Examples of such power may be set in the input vectors, randomized, or synchronization failure detector is provided with assumed constraints. As the announcement date, we here consider the method of synchronization based on additional assumptions.

After additional synchronization is assumed in the following, assume that a finite time T, the transmission delay of packets 5 of an upper limit. This assumption is a 3Synch (eventual synchrony hypothesis). To take advantage of it by using a timer, we also assume that the process can be accurately measured intervals, although they do not need to have synchronized clocks.

Symbolic model BAMPn, T [T <N / 3] and is represented 3Synch enriched BAMPn, T [t <N / 3,3Synch].

10.5.5A binary consensus Byzantine algorithm BAMPn, T [T <N / 3,3Synch]

In this section, we describe this is to ensure consistency as 0 in binary Byzantine algorithm (t) terminate our wheels, which is known to be the best. The algorithm described in FIG. 3 in FIG. 2 is extended security algorithms The goal is to add the consensus termination property. The same line with the same number of two algorithms. New line in FIG. 3 is numbered "Next 〃 end, wherein x is an integer, and the modified line by the" M-〃 prefix. In addition to using local timer based on the wheel, and ultimately benefit from 3Synch assumptions, which extends round the concept of coordination algorithms used: plays a special role in each round scheduled process of coordinating efforts to impose the value of the other wheel of the decision process . For this reason, in turn play a more accurate circular coordinator role in each process.

, The set of process P1, ..., the PN, the circle r PI coordinator process is such that i = ((R - D MOD N) + 1.5 additional local variables and message types in addition to ESTI, RI, bin_valuesi [R], and valuesi, each inlet

PI management process following local variables.

timeri a local timer, and timeouti - a timeout value, both to the use of assumptions 3Synch.

coordi round is coordinated indicators.

AUXI is a secondary set of values for stored value (if any) is currently coordinating efforts to exert their judgment value.

Circle R coordinator, using message type COORD_VALUE [R]

(1) to broadcast its attempts to become a value in favor of the decision.

Operation bin_propose (VI) is

(2) ESTI f six; RI ^ 0; timeouti ^ O;

(3) and (really) do

(4) RI traffic RI + 1;

(NEW1) coordi ^ ((RI - 1) MOD N) + 1; timeouti ^ timeouti + 1; timeri provided to timeouti;

(4) BV_broadcast EDT [RI] (ESTI);

(NEW2) If (I = coordi) and wait_until (bin_valuesi [RI] = {w}); // w is a value of [the RI] RADIO COORD- value [the RI] of entering bin_valuesi;

(M.5) wait-until (bin-valuesi [RI] 6 = 0) eight (TIMERi expired);

(NEW3) arranged to timeri timeouti;

(NEW4) if (COORDjt [RI] (W) received from a # pcoord)

(W G bin-values and AUXIf {w}

Otherwise AUXI Service bin-valuesi [RI]

just in case;

(M.6) broadcast AUX [RI] (AUXI);

(M.7) wait-until (message AUX [RI] (b-valp (1)), ..., AUX [RI] (b-valp (N- t)) has been received

From the (N - t) different process P (X), 1 <X <N - t and their contents

Is such a non-empty set 3- valuesi such ⑴valuesi £ bin_valuesi [RI] and (ii) valuesi = U1 <x <n-tb_valx) eight (TIMERi expired); (New5) if (considering the entire message of the set of when AUX [RI] () received, sets values1i, values2i, ... satisfy the previously waiting predicate) eight (one of them is AUXI) then valuesi traffic AUXI END IF;

Double fRI mold 2;

If (valuesi = {V}) // valuesi is a single, whose elements v Then ESTI ^ V; if (V = BI) before deciding (V), if not ended, if; Otherwise double ESTI Service In BAMPn a secure site and binary Byzantine consensus algorithm, T [t <N / 3,3Synch]

Description Extended algorithm describes the following items appear in Figure 3 of the new and revised statements.

- the line NEW1, PI calculating the current wheel coordinator, and set its local timer, which is used in the predicate of the expiration line M-05. The timeout value is initialized before entering the loop, then rose in every round.
- NEW3 line is a timer that expires for resetting a simple line in the modified M-07 predicate.

Line NEW2, NEW4, M-06, and New5 implement a mechanism that allows the current round of coordination, trying to impose a value of 6 into the first judgment of its value bin_values set. The fact that, after the presence of a time, by a non-fault message exchange process is timely, it will have to ensure that the wheel during this period, the non-faulty process will have a single value in their valuesi sleeve (which binds - 10 required by the lemma their decision).

- modified lines of the M-05 and M-07: In addition to the predicate in the corresponding line considered in timer expires.

As just seen, the idea to start the operation of these new or revised statement is: caused such a decision from the overall coordination of the interests of a defect-free, by requiring the process, so that all non-fault process uses it to play a recommended value. to this end:

Circular coordinate PK broadcast message COORD_VALUE [RI] (W), wherein w is set into its bin_values (line NEW2) the first value. If PK is no fault, the fault-free process timeout value is large enough, and the message transmission delay binding, all non-faulty process will receive the line M-06 before the timer expires.

- Then, assuming that the previous item, is set to Wa Laid AUXI (line NEW4)} all non-fault handling, and broadcasts it (line M-06). W predicate Gbin_valuesi [RI] for preventing Byzantine coordinator sends the tank during the non-faulty false.
- Finally, all non-faulty process will receive the message AUX [RI] ({W}) from a - different processes (N t), and set by line New5 valuesi = {w}. This circle (R1) or mean that their decision (R + 2) period.

From asynchronous to synchronous decision-making in order to ensure the final synchronization hypothesis, and after each trouble-free processing time-out value is large enough (that is, than the upper bound messaging big delay), we need to eventually perform all non-synchronized troubleshooting Round . It observed that, since the initial asynchronous, non-fault on the consensus algorithm can process at different times. In addition, due to the potential participants Byzantine process, a number of non-faulty process can be ahead of two, without decisions, and other trouble-free process is still executing the previous rounds. By using a long process times out all round, and ultimately achieve synchronous behavior from their circle.

Lemma 12. We consider the algorithm of Figure 3 will ultimately no faults in the process of synchronization round from their behavior.

3Synch final proofing has an unknown message transmission delay constraint 5. As noted in Section 2, assuming local processing time is equal to zero. (Or, in Appendix B and C do not depend on this assumption is provided with two additional evidence). Hereinafter, description will be given in time units of integers. Subscripts (e.g. tfirstO) will be used to indicate the sign of t is elapsed since the beginning of the algorithm has, as a whole so that the global number of viewer G. known from the measured time unit measuring a given time period at least as observed the rate of non-fault processes and events can occur at integer time unit.

We will use the following definitions:

tfirstr as measured by a G in the first time of non-failure process pfirst arrival circle R (tfirstO time, when the first non-consensus start troubleshooting).

tlastr is the last non-faulty process PLAST arrival circle R (tlastO is the time when the last non-consensus start troubleshooting) as the time measured by the G.

For a circle is synchronous, all non-fault process must have enough time to get all the news that a timeout before any due process trouble-free broadcast of trouble-free process that round. In this case, the last non-fault is processed in turn reaches the coordinator, which may take up to COORD_VALUE [R] 3 before the message is received by all the non-faulty delay to process messages (including messages delayed until up to 2 a value into its bin_values [r] and the further delayed broadcast message COORD_VALUE [R]). Therefore, we must have a round where r tlastr +5 <tfirstr + timeoutr.

It should be noted that taking into account the time-out from 0 0 round, each by one round of growth, we can replace the R timeoutr consider any round of the first round of the river which timeoutrO ^ R0 meet. For any round in which R00 R00 plastrOO 2R0 maximum amount of time to complete the round will be 2xtimeoutr00. This is due to the fact, finally trouble-free process circle arrival will not have to wait to receive more than 5 longer in order to meet the information on the line M-05 and M-07 to the required conditions, in order to take time to perform the wheel will no more than two timeout length polymorphism. All other non-fault process takes at least 2xtimeoutr00 complete circle R00.

From a certain round in which R00 process last no defect in time can be written as:

$$t_{last_{r'}} + 2\left(\sum_{x=r'}^{r''-1} x\right)$$

When the first time the process reaches a circle without defects R00 is:

$$t_{first_{r''}} \geq t_{first_{r'}} + 2\left(\sum_{x=r'}^{r''-1} x\right)$$

1 block to the results of this inequality points:

$$t_{last_{r'}} + 2\left(\sum_{x=r'}^{r''-1} x\right) + 3 \times \delta \leq t_{first_{r'}} + 2\left(\sum_{x=r'}^{r''-1} x\right) + r''$$

Remove the equal components, we have:

tlastrO + 3x52 tons a desk / ^ 0 + R00.

Therefore, through a circular R00 = tlastrO + 3x5 - tfirstrO synchronization is guaranteed.

Now will show that once inequality (1) satisfies an R00 (which timeoutr00> 5), it will remain satisfactory in all of the following rounds. Consider wheel R00 + 1, in view of inequality (1) Established in round R00, we have:

tlastr00 + 3x5 <tfirstr00 + timeoutr00. (2)

And it needs to prove the following inequality is true:

Father tlastr00 + 1 + 3 5 <t | a / A00 + 1 + overtime / ^ 00 + 1 (3)

Using the same parameters as the above process of the first and last times wherein R00 + 1 reaches the wheel has:

tlastr00 + 1 = tlastr00 + 2xtimeoutr00 and tfirstr00 + 1> tfirstr00 + 2xtimeoutr00. This clogging of the inequality (3) results in:

tlastr00 + 2xtimeoutr00 + 3x5 <tfirstr00 + 2xtimeoutr00 + timeoutr00 + 1.

Aliquots result in:

tlastr00 + 3x5 <tfirstr00 + timeoutr00 + 1.

This inequality, which is equivalent to Inequality (3) having the same components, the inequality (2), except that instead of having timeoutr00 + 1 timeoutr00. Thus, Inequality (3) must be satisfied, because the inequality (2) is satisfied. This is summed up by any one of R00 after real. 5.6Proof 3Synch 2Lemma 12 based algorithm

The certificate consists of two parts :(a) show, add statements consistent security proof idle time algorithm in FIG. 2, and (ii) show that all non-faulty final decision process.

Lemma 13. Validity and satisfaction algorithm BBC- BBC- protocol properties as described in FIG.

Proof to prove the lemma proof comprising 5,6, 7 and 8, maintain the correct, these proofs 3 substantially remains the algorithm takes into account FIG correct because, as the new and modified assignment statement does not set bin_valuesi [R] in the non-fault handling, and with a characteristic not bin_valuesi timing hypothesis, non-faulty process can not contain only by the PI process Byzantine recommended value setting spoon bin_valuesi [R]. It follows from this observation, the non-faulty at any

Li (line M-07, New5, 10 or 11, defined or updated) and local variables from valuesi ESTI can contain only non-faulty process values. More specifically, we have the following.

• Lemma 5. Let R be a circle under consideration, and v is no process failure of current estimates. Then, we have bin_valuesi [R] = {V} M-05 line of each non-fault process pi. - If the fault-free round coordination PK, we each non-fault occurred AUXI = bin_valuesi [R] = {V}. It follows then valuesri = {V} and lemma since the line 09 and 10 hold true.

- If the coordinate PK Byzantine circle and different values may be sent to non-fault process, let us consider the received message COORD_VALUE [R] non-fault handling ({1- V}). (1 - v) of G / bin_valuesi [R], online NEW4, PI performed "else" portion, where it is provided to AUXI {V} (bin_valuesi unique value in [R & lt]), and the following lemma.

• Lemma 6, since it does not rely on a timer, and relates only to the fact that valuesri each group and the two non-fault process valuesrj single, still prove effective.

• Lemma 7. proof of the fact that following collection bin_valuesi any non-fault process of troubleshooting can only contain non-recommended value.

• Lemma 8. Because it depends only on sets valuesri trouble-free processes, this proof is still correct. Lemma 14. The algorithm described in Figure 3 ensures that each non-fault decision process.

Prove that we first observed, due to the expiration of the timer always, "wait" statements (revised line M-05 and M07) always terminates, so Lemma 9 is still correct. Readers can also check the proof of Lemma 10 is still valid.

It still indicates that there has rounded R at the final end, which all non-fault handling Pi w have the same value in their set of variables (valuesri = {W}) (from which decides Since Lemma 10) demonstrated shown that, due to the assumed final synchronization (a) in, (b) the wheel coordination mechanism, and (c) of the message by the wheel

Coordinator transmission COORD_VALUE, there is a circle R, as valuesri = {w} of each process in the non-defective.

Let us consider a time t (arrive in time-out value of all non-fault process, so that all information exchanged by the non-faulty process) from (due to the lemma 12) synchronization system behavior. Let r PK is coordinated by the process does not fail after t min of the number of turns. The circular R, PK broadcast COORD_VALUE [R] line NEW2 (W), a first value is set into its watt bin_valuesk [R] is. Message COORD_VALUE [R] (w) is received by all non-faulty process in a timely manner, to the set {w} AUXI line NEW4. Thus, all non-fault handling broadcast AUX in the M-06 line of [R] ({W}) and the line receiving M-07 in the (N - t) of the AUX [R] ({W}) from a different process message, the line is set to {w} New5 valuesi. All non-fault decision process for a W R + 1, wherein the proof of Lemma conclusions drawn. Theorem 3 Algorithm 2Lemma 14 described in FIG. 3 solves the binary system model BAMPn Byzantine agreement, T [t <N / 3,3Synch].

Proof evidence from Lemma 13 (BBC- validity and BBC- Protocol) and lemma 14 (termination) directly.

Naming system:

The traditional use of the Internet Domain Name System (DNS) maps humanreadable names to IP addresses (which gives the location of the nodes and content). When Internet users type in their browser, DNS server returns a human-readable names to IP addresses in cnn.com. ICANN, a non-profit organization, management and DNS root servers. The server is the central point of trust and failure; they can be taken offline by DDoS attacks and change the DNS server domain mapping through coercion, deception or change from their responses.

In pointnity, we need to replace the dispersion DNS i.e., binds human-readable name to discover data, but without any central point of failure or control system. There is thought that human-readable name is not important, long ID and password of search engine combining alternative DNS - school. Our view is that human-readable names is to provide a good user experience, and essential in practice, it would be hard to convince Internet users to change their habits, and stop using the online human-readable name.

No basic computer science challenges and build a naming system. There are three attributes, we may need to have a name: The name is

(1) The only (meaning that the absence of two independent people can create and use unique names like cnn.com)

(2) a human-readable

(3) Dispersion (name should be selected by the user in the center at the edge of the network by the central authorities, rather than on behalf of the user). Computer science challenge is before blockchains, naming system only allows three characteristics [15], any two of the three never at the same time. This limit is called the triangle Zooko. For example, the public key is unique, decentralized because users can generate their own computers without any central service, but not human readable. Twitter handle is human readable, unique, rather than scattered (Twitter, the company controls namespace). A nickname is human readable and dispersed (the user can select anyone nickname), but not the only. Blockchains party Zooko triangle, and for the first time there may be no use of a unique human-readable name of any centralized services.

Namecoin is the first system to use blockchain establish decentralized naming system. Our experience running Namecoin production network on the show, highlighting the maximum mostsecure blockchain network requires a certain degree of security and reliability issues terms of reference are as follows: a space corresponding to the key organization and can not exceed a franchise

System Security

Security pointnity defensive programming language derived from the design of the AVM and strict restrictions on the time, space and resource use. In addition, the security focus will also be provided by scripting language authoring tool. For example, the logical correctness pointnity chain code may, model checking verification and analysis tools provided by conventional bytecode.

PONT token rules and Legal Notices

Please note that this is not any type of investment Description

This document does not constitute any form of prospectus; it is not a solicitation to invest, not in any way involve the provision of securities in Canada or the United States, Canada and the United States and China as well as residents of explicitly exclude any exchange of PONT token donation in public products .

DISCLAIMER:

This site is for reference only. POINITY and all related companies and affiliates do not guarantee the accuracy of the conclusions reached by this site "as is provided 〃, without any express or implied representations and warranties, including, but not limited to:

1 warranties of merchantability, for a particular purpose, or non-infringement of ownership;

The contents of this website without any errors or for any purpose;

3 such content will not infringe rights of third parties. All ensure clear sound. POINITY and its subsidiaries expressly disclaims any form of liability and damages resulting from the use, reference or reliance on information contained on this website caused, which we are not responsible.

Recipients specific notice as follows:

• does not provide any securities: PONT token (such as the POINITY white paper) is not intended to constitute securities in any jurisdiction. This site does not constitute a prospectus, nor does it provide any form of document, nor does it constitute an offer or solicitation of securities or any other investment product or any other jurisdiction.

• No suggestion: This POINITY website does not constitute any recommendation PONT exchange token, should not rely on any contract or contribution decision.

• No, said: Recipient or its advisers did not cause on this website, or contain information, statements, opinions or issues derived (expressed or implied) or the accuracy or completeness of any omission in this document or to make representations or warranties now or any other future available to any written or oral information or advice about the party or its advisers. For any plan or predict the future prospects of achievement or reasonableness makes no representations or warranties Nothing in this document should not be considered for future commitments or statements. To the maximum extent.

• Donation: We only accept donors through specific KYC KYC certified the following format Name:

gender:

Nationality (does not support the United States, Australia, China, China):

date of birth:

ID card / passport / driver's license:

ID Photo:

Proof of bank card statement, utility bill payment, property receipts identity information:

Contribution amount (ETH):

Risk Warning: Potential contributors should independently evaluate their preferences for these risks, and decided to consult with their advisor before making any contribution to the PONT tokens.

Token Rule

The total number of tokens to 5 billion

Pre-sale: 5%

Official ratio: 1: 35,000 (Note: pre-sale Blocking rule: 50 percent before exchange release on-line, the remaining 50% is paid on-line exchange after 6 months)

Sale: 15%

Official ratio: 1: 23,000 (Note: Lock Sale rule: before the release of 50% of the exchange line, the remaining portion is released in the exchange line after 3 months).

35% of the team: Panelists technical development and operation Award (Note: Team token lock on the token is released within 24 months after 12 months in a linear fashion after the line balance, released once every two months). A total of 12 times.

Cooperation 25%: use it for eco-hatch, expand radiation scope of the project and to establish useful and good cooperation (Note: Lock the rules, as the case may be, the organization released a token of cooperation and locking time limit minimum of six month.)

Community 20%: To advise the community operate, maintain and build a good community environment, community involvement operators can obtain a token reward. (Note: Community token release and lock, unlock, as the case may be no time limit.)

This token is a token Erc-20, PONT token after the main network line 1: 1 is replaced by a token-based network.

in conclusion

With the rise of digital encryption technology to bitcoin block chain represented by the emerging technology has become a hot academic and research industry. Block chain technology can not bring tampering and programmable features, it has been widely used in digital encryption, monetary, financial and social systems. However, compared with the booming business applications block chain, basic block chain theory and research technology is still in its infancy ,, critical to the development of enterprises. Scientific issues of the industry chain must be follow-up study. This paper systematically reviews the basic principles of the block chain technology, techniques, methods and its application, combined with the existing problems and prospects to build Pointnity it is a compatible open network, I believe he will enhance the block chain of the world Further development.

Here, we sincerely hope that more people participate in the construction of the block chain block chain in the world has contributed to the construction of the world. Welcome to Pointnity Network.

references

[1] Hill M D. What is scalability [J], ACM S1GARCH Computer Architecture News, 1990,18 (4):? 18-21

[2] Bondi A B. Characteristics of scalability and their impact on per- formance [C] // .. Proc Second Int51 Workshop on Software and Performance ACM Press, 2000: 195-203

[3] Brataas G, Hughes P. Exploring architectural scalability *[C ~ \ //* Proc. Fourth Int^{9} . 1 Workshop on Software and Performance ACM Press, 2004: 125-129

[4] Duboc L, Rosenblum DS, Wicks T. A Framework for Modelling and Analysis of Software Systems Scalability [C] // ICSET 06. Shanghai, China, 2006

[5] Gustavson D B. The many dimensions of scalability [C] // COMPCON 1994:. 60-63

[6] van Steen M, van der Zijden S, Sips H J. Software engineering for scalable distributed applications [C] //Proc. 22nd Int'l Computer Software and Applications Conference 1998:. 285-293

[7] http:.. // msdn microsoft com / zh-cn / library / aa292172 (v = VS. 71)

[8] Jogalekar P, Woodside M. Evaluating the scalability of distributed systems [j]. IEEE Trans. Parallel and Distributed Systems, 2000, 11 (6): 589-603

[9] Sun XH, Rover D T. Scalability of Parallel Algorithm-Machine Combinations [Rj, IS- 5057, Ames Lab. »Iowa State Univ, 1991

[10] Sun XH, Chen Y, Wu M. Scalability of Heterogeneous Compu- ting [C "# Proceedings of 34th International Conference on Parallel Processing 2005:. 557-564

[11] Amdahl G. Validity of the single-processor approach to achieving large scale computing capabilities [C] // Proc. AFIPS Conf. 1967: 483-485

[12] Sun XH, Ni L M. Scalable Problems and Memory-Bounded Speedup [J] J. Parallel and Distributed Computing, 1993,19:. 27-

[13] Sun XH, Ni L M. Another View of Parallel Speedup [C]//Proc. Super computing *'90.* Los Alamitos, Calif: IEEE Computer Soc.
Press, 1990: 324-333

[14] Sun XH, Zhu J. Performance Considerations of Shared Virtual Memory Machines [JIEEE . Trans Parallel and Distributed Systems, 1995,6 (11); 1185-1194

[15] Grama AY, Gupta A, Kumar V. Isoefficiency: Measuring the Scalability of Parallel Algorithms and Architectures [J] IEEE Parallel and Distributed Technology, 1993,1 (3):. 12-21

[16] Grama A, Gupta A, Kumar V. Isoefficiency function: a scalabili.. Ty metric for parallel algorithms and architectures [R] IEEE Parallel Distributed Technol Systems Appl, 1993: 12-21

[17] Jogalekar PP, Woodside C M. A Scalability Metric for Distributed Computing Applicationsin Telecommunications [R], SCE-96- 07. Ottawa, Canada: Department of Systems and Computer Enginering, 1997

[18] Kumar V, Gupta A. Analyzing the scalability of parallel algorithms and architectures: A survey [C] // Proceedings of the 1991 International Conference on Supercomputing 1991.

[19] Czajkowski K, Foster I, Karonis N, et al. A Resource Management Architecture for Metacomputing Systems [J]. Information Sciences. 1-19

[20] Cao J, Jarvis S A. ARMS:. An agent-based resource management system for grid computing [J] Scientific Programming, 2002, 10: 135-148

[21] Buyya R, Abramson D »Giddy J. Nimrod / G: An Architecture for a Resource Management and Scheduling System in a Global Computational Grid [J] Computer, 2000:. 1-7

[22] Chapin SJ, Katramatos D, Karpovich J, et al. Resource Management in Legion [JJ Future Generation Computer Systems, 1999, 15 (5):. 583-594

[23] Chen Y, Sun X, STAS; A Scalability Testing and Analysis Sys- tem [Q / ^ 2006 IEEE International Conference on Cluster Computing 2006:. 1-10

[24] Lyon G »Kacker R, Linz A. A scalability test for parallel code [J] Software:. Practice and Experience, 1995,25 (12): 1299-1314

[25] Liu CL, Layland J W. Scheduling Algorithms for Multiprogramming in a Hard Real-time Environment [J] J. ACM, 1973, 20 (1):. 46-61

[26] Schmid U »Blieberger J. Some investigations on FCFS scheduling in hard real-time applications!] J]. Journal of Computer and Sys
tem Sciences, 1992,45 (3): 493-512

[40] . Jin H, Wang HA, Wang Qiang, et al A comprehensive design method of task priority [J] Journal of soft parts / 2003/14 (3):. 376-382

[41] . Wang Yongyan, Wang Qiang, Wang Hongan, et al A Real-Time scheduling algorithm based on priority Table and its reality [J] Journal of Software 2004 15 (3):. 360-370

[42] Huang Decai, money can. Complexity and New algorithm of Multi-machine related Task equilibrium scheduling problem [J]. Computer Engineering and Science 22 (2) p. 16) Schmid S, Sifalakis M, Hutchison D. Towards Autonomic Net- works [. J] Lecture Notes in Computer Science, 2006,4195: 1-11

[43] Baumgarten M, Bicocchi N, Kusber R »et al Self-organizing Knowledge Networks for Pervasive Situation-aware Services [C] // IEEE International Conference on Systems, Man and Cybemeti- cs Quebec» Canada »October 2007:.. 1-6

[44] Wang Hui-qiang, Feng Guang-sheng, Zhao Qi-an, et al. Progress of Research on Cognitive Networks [M]. Sciencepaper Online, 2009

[45] Hillston J. Fluid flow approximation of PEPA models [C] //Proceedings of tVie 2nd International Conference on Quantitative E. Valuation of Systems Torino; IEEE Computer Society Press, Sep. 2005: 33-42

[46] Katsuno Y, Aihara T. Autonomic Network Configuration for Networkable Digital

Appliances [J], IEEE Transactions on Consumer Electronics, 2005,51 (2): 494-500

[47] Devroye N, Mitran P, Tarokh V. Achievable Rates in Cognitive Radio Channels [J] IEEE Transactions on Information Theory, 2006,52 (5):. 1813-1827

[48] Sahai A, Hoven N, Tandra R. Some Fundamental Limits on Cognitive Radio [C] // Forty-second Alierton Conference on Communication, Control, and Computing. Monticello »Israel, October 2004: 1-11

[49] Jovicic A, Viswanath P. Cc ^ nitive Radio: An Information-Theoretic Perspective [OL] http:..... // www ifp uiuc edu / ~jovicic / JV06 pdf, June 2006

[50] Koulouriotis DE, I ^ akoulakis IE »Emiris DM, et al. Development of Dynamic Cognitive Networks as Complex Systems Ap. Proximators; Validation in Financial Time Series [J] Applied Soft Computing, 2005,5 (2): 157'179

[51] Thomas RW, Friend DH, Dasilva LA, et al. Cognitive Networks: Adaptation and Learning *to Achieve Eend-to-End* Performance Objectives [J], Communications Magazine, 2006, 44

(12): 51-57

[52] Kephart J O. Research Challenges of Autonomic ComputingfC*] / J* . Proceedings of the 27th International Conference on Software Engineering Missouri, USA, May 2005: 15-22

[53] Strassner J. Autonomic Networking: Theory and Practice [C*] //* Proceedings of *2008* . IEEE / IFIP Network Operations and Manar gement Symp Salvador, Brazil, April 2008: 786- 786

[54] Hinchey M, SterrittR. Autonomicity-an Antidote for Complexity?[C]// Proceedings ofComputational Systems Bioinformatics Conference, Workshopsand Poster Abstracts.Stanford University»Aug. 2005: 283-291

[55] . Gelenbe E, Lent R. Power-aware Ad-hoc Cognitive Packet Networks [J] Ad-hoc Networks »2004,2 (3): 205-216

[56] Gelenbe E, Lent R, Xu Z. Measurement and Performance of a Cognitive Packet Network [J] Computer Networks, 2001,37 (6):. 691-701

[57] Gelenbe E, Lent R, Xu Z. Design and Performance of G gnitive Packet Networks [J] Performance Evaluation, 2001,46 (2/3):?. 155-176

[58] Hey L A. Reduced Complexity Algorithms for Cognitive Packet Network Routers [J] Computer Communications, 2008,31 (16).:
3822-3830

[59] Koulouriotis DE, Diakoulakis IE, Emiris DM, et aL Development of Dynamic Cognitive Networks as Complex Systems Approximators: Validation in Financial Time Series [J] Applied Soft Computing, 2005,5 (2):. 157- 179

[60] Rondeau TW, Bostian CW »Bruce A F. Cognitive Techniques Physical and Link Layers [M], Cognitive Radio Technology Ne- wnes:!. Burlington, 2006: 219-268

[61] Smith JM, Bruce A F. Cognitive Techniques: Network Aware- ness [M] Cognitive Radio Technology Newnes:.. Burlington *
2006t299-311