# Pointnity Network



highcompatibleSex,canshared,Interactive collaboration of distributed systems

Draftv1.0

**A simple introduction**

The concept of blockchain

Blockchain development process

The value of the blockchain

Blockchain challenges

       1. Distributed consensus

       2.performance

       3. scalability

       4.system security

       5.data and storage

Future development of blockchain

**Second, Pointnity**

What is pointnity Network?

Pointnity Network Interpretation

HUB distributed information processing system

    1.HUB design goals and effects

2. Customized blockchain organization

Multi-chain interaction, controllable business information and ecological cooperation display

          1. The essence of blockchain cross-chain

2. Blockchain cross-chain architecture model

3.generate and package cross-chain transactions

4. Providing sub-chains with cross-chain transactions to prove the launch of main-chain cross-chain services

5.the implementation of the main chain cross-chain transaction code

6.Initiating Outer Chain Contract Service Call

7.the implementation of the external contract code

8.generate a transaction log, update the status of the account

Supports extended aptamer chain internal channel cross-chain

**Third.the consensus mechanism and system module**

Improved Byzantine Consensus Algorithm Usage and Research

       1. POINTNITY's Byzantine consensus algorithm design meets the validity attribute

       2. Basic Byzantine calculation model and reliable broadcast

             2.1 Base calculation model

             2.2 Reliable Broadcast

       3. Blockchain Byzantine Consensus

3.1 Multivalued Byzantine Consensus

3.2 Binary Byzantine Consensus

4. From multivalued to binary consensus Byzantine system

4.1 The reduction

4.2 Correctness certification

5.Binary consensus on the final synchronous Byzantine system

5.1 The BV Broadcast to All Communication Abstractions

5.2 Secure Binary Byzantine Consistency Algorithm BAMPn

5.3 Safety certification

5.4 Eventual synchronization hypothesis

5.5 Binary Byzantine Consensus Algorithm BAMPn

Piontnity token function

Naming system

System security

**FOUR. PONT Token Details and Law**

**FIVE. the conclusion**

# Official content

**The concept of block chain**

Block chain is originally in the seminal paper currency bits invention, it is a promising technology. For tracking the distribution of ownership of digital assets. The technology is designed to allow a process to agree on a series of consecutive trading block, these transactions can exchange those assets cited features of the contract. If these distributed ledgers are not accessible by users with certain privileges, the company has been successfully deployed in other instances a federated environment. Thus limiting the appropriate license carefully selected set of institutions of decision-making tasks

In 2016, the growing interest in this technology community overview distributed a number to block chain-related scientific activities provide. For the distributed computing community, which seems to be a typical state machine replication application. In the classic state machine replication, each command (or action) can be called at any time by any process and applied to the state machine, no matter what order the previous application Yes. The processing target block chain expression is added to the next target agreed transaction processing block chain, and copying the state machine is the next sequential consent is applied to the state machineofEquivalent to the case where continuousofconsensus.

However, one of the main differences between the chain and the block state machine replication relationship between the consecutive negotiation embodiment consistent. Is deleted in the case of each block chain requires consistent. A related front and subtle. More precisely, plus 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 a content, a hash of the block output. Identifying consensus instance number of the proposed decision block X must be embedded in the instance number. In view of this hash block chain is a set of new computer technology, new technological innovations, subvert the traditional Internet.

**AreaDevelopment of block chains**

AreaBlock chain technology came into being in the earliest prototype of Bitcoin project. Behind Bitcoin distributed as accounting platform, there is no centralized management, Bitcoin network has been running steadily nearly eight years, to support a huge transaction. No serious flaws.AreaIdentifying descriptive literature first block chain is a bit credits, one peer network electronic cash system, the presentCleverWritten, but it is focused on the bits token system. In factAreaBlock chain, wherein the block chain is described as a history recording bit currency trading account, and no clear definition of the concept.

More broadly,AreaChain is a decentralized recording technology. Nodes participating in the system may not belong to the same organization, you do not need to trust each other;AreaData block chains held 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, allocated to achieve as much as possible;

Encryption mechanisms to ensure that the transaction can notIsDenial and destruction,Protection of user information and record as much privacy. more importantly,contractcanAnd DistrictBlock chain combine to provide a more flexible functionality of the contract, it already supports simple script calculation. To perform more complex operations. The block chain extended beyond mere data recording and actually has "ubiquitous computing" means point.

**AreaBlock chainspricevalue**

A typical modern enterprise, the merchant by completing negotiations and execution of transactions in the course of the contract.AreaBlock Chaining good at how to manage contracts and ensure the smooth implementation of the contract. And block chain characteristic value varies according to the type and application scenarios.

In terms of technical characteristics,AreaBlock chains are typically considered:

· Distributed Fault Tolerance: The network is very robust, fault tolerant about one-third of the abnormal state of the node.

Non-tampering: consistent data submitted is always there, it can not be destroyed or modified.

· Privacy: Password guarantee that unauthorized data access, but can not be resolved.

**AreaChallenges brought about by the block chain**

The key technologies and challenges, from a technical point of view,AreaBlock 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,Application of block chain may stimulate further development of the art of cryptography, including random number generation, security strength,Encryption and decryption performance,And 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.

Distributed Consensus

This is an old topic, the core is how to solve this change is consistent on the network,It is generally accepted,LetThis information is confirmed. Big difference between public anonymous scenes of this problemand those with rights management. In BitcoinAreaConsidering the block chains in the worst case scenario in a anonymity disclosed. "Workload prove" introduced by a few people to avoid malicious data corruption. Probabilistic model to ensure that the last one is legitimate longest chain. In addition, the mortgage interests. 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. Prisoners of war and other algorithms allow more than half of uncooperative nodes PBFT, less than a third of the theory of non-cooperative node ratio.

deal withperformance

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,AreaBlock chain system processing performance, can not simply be 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. At present, the open-source block chain itself has been implemented properly configured on 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.

Expansibility

Common distributed system can expand the processing capacity of the entire system by adding nodes, forBlocksChain 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. Therefore, the totalCalculation processing and storage capacity dependsComputing capacity of the network on each node. 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 the franchising modeinHigh performance core node may be used as a proxy node and the access node weak node.

system security

AreaBlock chainRelying on well-designedExisting encryption algorithms. However, this is to ensure that theyabsoluteSafetyIt? 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 block chain or performed without legal protection.

Secondly, potential vulnerabilities in software implementation is inevitable. Taking into account the OpenSSL has been used 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, the publicAreaAll transaction records block chains are publicly visible. Is Big DataeraWhen people began to get excited,They determined that such disclosure is harmless to you? Indeed, there are a lot of things can be analyzed here, they are large enough, enoughHaveInfluence. In fact, in bitcoin block chain from end-user transaction.

In addition, as a fully distributed system, the lack of effective public block chain adjustment mechanism, which is difficult to solve the problem, to make it fairer and more perfect. As long as certain vested interest groups to unite against it,becauseThey can not participate,thereforeThis cast a Bitcoin worth of its own shadow.

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.

Databases and storage systems

Block in a block chain network needs to be written to the database for storage. ObservedAreaBlock chain applications,HaveHash calculation and verification of a large number of operations, 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. So, we canAreaBlock chainofApplication design features some targeted special database-The horizontal key database DBN RocksDB, has a high random write and sequential read performance, it has been widely used inAreaInformation storage block chain. inpointnity It appears that there may in the futureThere will beMore targeted "database block block the DBB", dedicated to the new types of data traffic, as depicted at block chain, wherein each record comprises a natural full block information and history information are associated. Once the writing is recognized, it 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 spread their business transactions? These are urgent problems. If this problem is not solved, it will be a big obstacle blockchain technical landing.

**What is pointnity**

POINTNITY NETWORK was founded in November 2017 is a focus on eco-compatible, interactive collaboration, solving technical 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.

Because in the development of technology, information technology will inevitably become part of the islands of information, valuable concepts are not a powerful implement 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 have a strong conceptual resource assistance, and lowering the barriers to technology development team of more startups, as well as providing one-stop solution best supporting stack.

BackboneThe improved PBFT consensus algorithm provides an external system interaction across chain collaboration. Low friction transactions are secured channel within the system,To provide effective protection for the good ecological development, in order to overcome many of the existingBlock chain technologyBottlenecks, speed up the block chain has spread to the quality of individual scenes pointnity committed to creating a highly flexible and compatible, collaboration, data storage and more authorityShowDistributed ecosystem decentralized to go.

**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, third-generation 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.

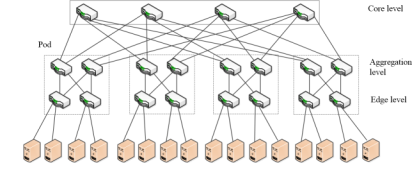
**HUB distributed information processing, storage system**

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

Named dispersed and found: the end user should be able to (a) the registration and use of human-readable name and (b) find that mapped to human-readable name of network resources, without trusting any remote party.

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.

Comparable 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, which do not provide the performance / bandwidth is comparable to a centralized service pointnity proposed to solve these problems.

1: survival failure of the underlying Blockchains

Our structure and did notBlock chain to make any use restrictions. Any blockchain may be used as long as it is provided an operation (where all blockchains) the whole rowSequential logic, 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.

2: logic to maintain than complex and many Blockchains blockchains, like Revenge, while achieving the control logic and data stored in the plane blockchain level (although they leave,Open the possibility of future use of external data stored in). 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, they get deployed and after the introduction of new features 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 remain outside the complex blockchains.

3: Global scalable data index

Any decentralized network would need an index to the data it stores. Go back to the beginning of the 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 - at all (a) the particular case of the data set in the case of dispersion and stored in a small volume (b) 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.

**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. Now, we can replicate what we want, or need 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.

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

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 one wanted to exchange foreign currency, such as Bob, Alice will sell $ 10 Bob, Bob received Alice gave him $ 100, according to the exchange rate at the time, he gave Alice 657 yuan. From the point of view books, foreign currency exchange of the entire process is like this.

First, Alice has $ 100 on a $ books, Bob has $ 0 in the dollar on the books;

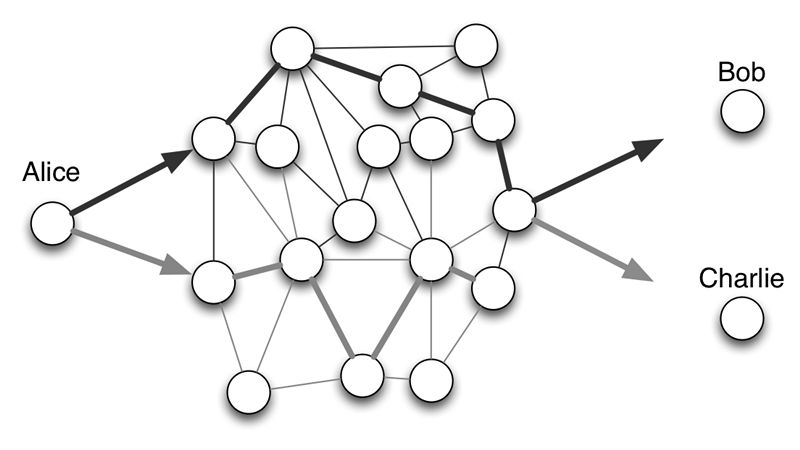
Alice 0 yuan RMB books, Bob 657 yuan RMB books.

Alice then transfer on the books of $ 100 dollars to Bob,

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 only.

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 the block chain cross chain

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.

Block chain cross chain architecture model

Architectural model independent block chain has been described in the foregoing, all independent block chain if you need support across the value chain transfer or exchange, you need to be present outside the chain of service contracts, service contracts outside the chain with the general service contract is not essentially different is 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 cross the 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 swap body on another block to own chain the public 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 can be achieved A↔B a cross chain contract service 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:

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-chain transactions provide proof sub chain initiates 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.

Execution 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.

Generate transaction log, update status books

Code exchange contracts across the value chain to achieve, does all the A↔B trade matching, form the sale of market depth with B chain value chain value A body of a body, once the match on the main body X and Y transaction request, to form a matching transaction for 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.

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.

Code execution 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.

**Insider trading channel**

Inside the trading channel

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.

¹-2 / ¹-² / 2 / ¹-²-³ / 2

Cross-channel mode with chains inside, is offchain, our POINTNITY supports dual use functionality as intermediaries relay contracts and bottom strand as the underlying operating system, our internal channel cross-link technology can be turned on chain and the results of executing the external passage interoperate across the chain.

**Consensus layer**

inPOINTNITYByzantine consensus algorithm proposed design meets the definition of consensus validity extended attributes. Structurally, it is composed of two parts.

The first component is a multivalued binary ConsensusThe time to achieve consistencyReduced.itIs fully synchronized, neither randomization(E.g., Casper then bet)Nor is the ultimateCenter ofleaderMust cutThere is no signature. This reduction is always determined first asynchronous non-predetermined value O (1) consensus sequence of binary. 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 <after N / 3 (as previous reduction), and additional synchronization hypothesis, i.e., there is a time, which is transmitting a message transmitted by the non-defective by the process delay constants the upper bound (this happens, but neither the time, nor is it a constant process known. in practice, this means that the BBC algorithm always terminate unless the transmission delay is always increased (in this case, different synchronization Suppose as described may be used).

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

The algorithm does not use leaders elected (in favor of the proposed value through a specific process), orEffort to prove, Equal to the value of the role of consensus which means that each participant plays presented. 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 already noted, the consortium revenge R3 50 machines in a machine owned by a consortium of revenge total mining capacity blockchain in June 2016 of R3, which gives a significant advantage, this machine to attack blockchain 12%.

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 applications[[1]](#footnote-0)Financial 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.

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. Π = {P1, ..., PN} is a set of pi; it referred to as PI I "Index." "Asynchronous" means that each processing proceeds at its own speed, which may vary over time and is still unknown to other processes. "Sequence" refers to a time during the execution of a step. This does not prevent it with the appropriate multiple executing threads.

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 I ∈Y PI∈Y 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" means that there is no restraint on the message transmission delays, but these delays are limited. "Reliable" means the network is not lost, copy, modify or create messages. "Point" refers to any connection processed by the 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 the pj", wherein m and TAG is a type of the contents of the message sends a message to a process PJ. To simplify the description, assume that a process can send a message to itself. Method, PI by executing the original "Receive ()" message. Macro operation of the broadcast TAG (M) is used as "used for each PI∈Π pies 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 calculated collusion "pollution" (e.g., while they should send messages with different content from the message transmitted with the same content, if they are non-fault). Byzantine exhibits behavior of a process known as fault. 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 [∅] for indicating an asynchronous MessagePassing Byzantine previous basic computational model; ∅ indicates 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 operation processing expressed RB\_broadcast () and RB\_deliver (). When the PI call operation RB\_broadcast () (respectively, RB\_deliver ()), we say that it "RBbroadcasts" message (respectively, "RB- provide" message). A broadcast RB- example, if the sender px process, 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 PX broadcast message and RB-m, all non-faulty process ultimately provides meters from the RB-PX

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

Output RB- validity attribute refers to the input terminal, and RB- unity indicates that no duplicate message. endOnly statements that the process must RB- situation to deliver a 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 transmissionMessage 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].

Algorithm in the algorithm described in implemented 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] shown in .

3Blockchain 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.

Byzantine consensus based on a predicate validity 3.1Multivalued

In this paper, we consider a generalization of the classic Byzantine consistency, the introduction informally. Because of its effectiveness requirements excited by blockchain, it depends on effective application of specific predicate to indicate whether the value is valid, we call this predicate validity of the Byzantine consensus problem-based (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]](#footnote-1)

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 predefined represented as predicates ().

The classic definition of this definition Byzantine general consensus, does not include a valid predicate (). 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 the v is valid. 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.

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, and BBC- BBC- agreement termination.

4From 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 reduction in the non-predetermined value of O (1) Examples of the consensus sequence of binary decisions. Other reducing or returns a predefined value if the consensus ⊥ suspension, or intolerance Byzantine fault and perform binary consensus sequence of claim dlogne instance. 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" reduced working model BAMPn, T [t <N / 3, BBC]

4.1The reduction

Binary consensus object as mentioned earlier, in addition to broadcasting RB- abstract, the method can mark BIN\_CONS [1..N] two yuan Byzantine array of cooperation consensus object. Examples BIN\_CONS [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\_CONS [K] by calling BIN\_CONS [K] .bin\_propose (V), wherein, v∈ {0,1}. Then, it executes a particular thread, and finally returns the value corresponding to the code determined by BIN\_CONS [K].

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

Array proposalsi [1..N] is initialized to [⊥, ..., ⊥]. proposalsi [J] of the object contains a value PJ recommendations.

bin\_decisionsi initialized to [1..N] [⊥, ..., ⊥] array. bin\_decisionsi [k] of the object contains a value (0 or 1) is determined by the binary objects consensus BIN\_CONS [k] is.

|  |
| --- |
| Operation mv\_propose (VI) is (01) RB\_broadcast VAL (ⅵ);  If repeated ∃K: (proposalsi [k] of 6 = ⊥) ∧ (BIN\_CONS [K] .bin\_propose () does not call)  Then call BIN\_CONS [K] .bin\_propose (1) END IF;  Until (∃`: bin\_decisionsi [ `] = 1) terminal repeat sequence;  For each k that BIN\_CONS [K] .bin\_propose () call Not  It does not call for BIN\_CONS [K] .bin\_propose (0) end;  Until (V1≤x≤n box \_decisionsi [X] 6 = ⊥);  Ĵ ← min {x satisfies bin\_decisionsi [X] = 1}; (09) wait\_until (Proposalsi [j] of 6 = ⊥);  Return (proposalsi [J]).  When VAL (v) is delivered from PJ RB- do, if valid (V) and then proposalsi [j] if the ← V cutoff.  When BIN\_CONS [K] .bin\_propose () Returns a value b do bin\_decisionsi [K] ← Bay |

Figure 1: from the multi-value to binary Byzantine consensus BAMPn, T [t <N / 3, BBC]

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 by RB-RB-broadcast technology PJ value v, which is stored in proposalsi [j] is valid if v (line 11).

Stage 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, PK RB- from each process having an associated delivery recommended values ​​(lines 02-03). Examples of common pi binary found BIN\_CONS , wherein 1 is determined (line 04) to stop the cycle. (Binary consensus of our proposed after allowing only O (1) message arrived after a delay stage (2) of the ends.)

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 BIN\_CONS [k], there is no process has provided a value from the associated process PK RB-. The purpose of these common shares is to ensure that all binary consensus, the final termination.

Phase 4: the value of pi is determined (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]](#footnote-2)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 PJ value from the process (lines 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).

4.2Correctness prove

Lemma 1. The decision is worth at least a binary consensus, all non-fault process exit repeat the cycle.

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

Evidence is contradictory. Let us assume that, in any non-fault process P1, no bin\_decisionsi [ `], 1≤`≤N, is constantly set to 1. Thus, there is no non-fault process exit "repeat" loop (line 0204). Valid values ​​as non-defective RB-PJ broadcast process, it follows from the RB-terminated -1 characteristic, each non-fault proposed to provide an effective process PI RB- PJ, so we end up with proposalsi [j] of 6 = ⊥ PI processing in each non-defective.

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]. Thus, the BBC termination, BBC- protocol, BBC- effectiveness and tolerance of intrusion, which returns all instances BBC process to a value of the non-defective, wherein the outlet

"Repeat" cycle. 2Lemma 1

Lemma 2 determination 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, when this process is the non-faulty pI of such proposalsi [j] of 6 = ⊥ it calls BIN\_CONS [j] of .bin\_propose (1). Since the line 11, it follows proposalsi [j] contains a valid value. 2Lemma 2

Lemma 3 is not a non-fault handling two different values ​​determined.

Let us consider two prove any non troubleshooting Pi and PJ, PI so decided proposalsi [K] and PJ decided proposalsj [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, itfollowsfromline07that (V1≤x≤nbin\_decisionsi [X] 6 = ⊥) with

(V1≤x≤nbin\_decisionsj [X] 6 = ⊥), from which we conclude that both pi and PJ known examples (line 12) is determined by the binary value of each binary consensus. Due to the properties of each binary consensus agreement BBC- instance, we have ∀x: bin\_decisionsi [X] = bin\_decisionsj [X]. Let decanoate [X] = bin\_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 BIN\_CONS [k] is a non-invasive properties of fault tolerant process p` call BIN\_CONS [K] .bin\_propose (1). In line 03 may be issued as the call only, we conclude (verb from line 02), the proposals` [K] = V 6 = ⊥. P` as fault-free, 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] = proposalsj [K], wherein draw conclusions prove the lemma. 2Lemma 3

Lemma 4. The 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 non-return results in each example of troubleshooting. 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 . 2Lemma 4

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.

2Theorem 1

In the final synchronization Byzantine system 5Binary 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.

5.1The BV broadcast to all communication to abstract all

Broadcast binary value (BV-broadcast) communication abstraction has been introduced (which is implemented in the Appendix A review) in [49].

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\_broadcast TAG (m), we say that it "BVbroadcasts message TAG (meters)." Content of the message m is 0 or 1 (hence the "binary value" word Communications Abstract names herein).

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, initialized to ∅, adding new value is 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 v∈bin\_valuesi, V has a non-fault process BV- broadcast.

BV- uniform. If the value of v is added to the fault set bin\_valuesi no process P1, the final v∈bin\_valuesj no defect each process PJ.

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 process Pi (i) become non-empty set bin\_valuesi, (ii) becomes equal, (iii) contains the values ​​of all the non-faulty processing broadcast, and (iv) does not contain a value only by the broadcast Byzantine type of process. However, (ii) and (iii) does not occur when the process known non-defective.

Byzantine consensus algorithm in binary security 5.2A BAMPn, T [T <N / 3]

2 depicts 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 previous broadcast BV- abstract, 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 ∅) storing a set of stainless steel by a monovalent BV- broadcast associated filling local output. (This can be a single infinite array of local variables bin\_valuesi replacement, re-start of each round ∅. Here, we consider one array to simplify the presentation.)

Double: 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] () for propagating its current bin\_valuesi [R] is a value obtained by PI (broadcast under the macro (help) operation).

Let us consider the algorithm of FIG. 2 after it has been deposited proposal The ESTI binary (line 01), each non-fault sequence into the asynchronous process PI wheel. Each round r, using a broadcast BV- instance, its local variables associated with the process pi is bin\_valuesi [R].

|  |
| --- |
| Operation bin\_propose (VI) is  ESTI ← six; RI ← 0;  While (true) do  RI ← RI + 1;  BV\_broadcast EDT [RI] (ESTI);  wait\_until bin\_ value ;  Broadcast AUX [RI] (bin\_valuesi [RI]);  wait\_until message AUX [RI] (b\_valp (1)), ..., different AUX process P (X), 1≤X≤N - [RI] (b\_valp (N- t)) has the (TN) - receiving tons, and their content is such, that ∃ a non-empty valuesi (ⅰ) valuesi⊆bin\_valuesi [RI] and (ii) the value of ;  2 ← RI double mold;  If (valuesi = {V}) // valuesi is a single, whose elements v  Then ESTI ← V; if (V = BI) before deciding (V), if not ended, if;  Otherwise ESTI ← double  just in case;  The end of a period of time. |

Figure 2: a binary security algorithm for Byzantine agreement BAMPn, T [t <N / 3] conduct during the non-faulty process oxygen circular pi can be broken down in three stages.

Stage 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: The second estimate of 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 waits 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.

Valuesi from at least the value of the message AUX [R] () - different processes (N t) is.

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 valuesi contains a single element 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 this value has been proposed by two non-fault process, cause such convergence protocol, selecting one of them the PI (b, i.e., all non-faulty at the same process) 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 algorithm can be used [49] given by randomization techniques terminated. Instead, we keep it simple and to postpone this algorithm in Section 5.5 of uncertainty terminal solutions.

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, it is possible to broadcast only the AUX [R] 06. consider any non-fault line processing PI ({v}), then it follows from line 07 predicate (valuesi containing only V), predicate line 09 (valuesi a single), and the dispensing line 10, i.e., the value held ESTI v. 2Lemma 5

Lemma 3 Let T <N / 3. (PI, PJ∈C) ∧ (valuesri = {V}) ∧ (value.

Proof: PI is provided a process trouble 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 ≥t + 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}). Is (n - T) + (T + 1)> N, it follows that Qi ∩QJ = 6∅. Let PK∈ Qi ∩QJ. As PK∈ Qi, this is not a defect of the process. Thus, in line 06, PK send the same message AUX [R] ({}) to pi and PJ, 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 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 = v. Thus, all non-fault decision process in a stainless steel monovalent, and in the decision v each non-fault decision process has been previously distributed 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) = R MOD 2. 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 line 07 wait\_until () statement terminates at 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, V 6 = (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) mod 2), we have the value ofIn each non-fault process P1. Thus, each non-fault line 10 in the decision process.

Theorem 2 satisfy the safety performance of the consensus algorithm described in Figure 2.

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 v 6 = (R-mode 2), is determined to prevent them.[[4]](#footnote-3)

5.4Eventual synchronization hypothesis

Consensus impossibilityIt it is known, there is no consensus algorithm to ensure the safety and fully asynchronous messaging system activity, which, even in a single process may crash [24]. 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 the synchronization is assumed that the fault detector is provided with a , the constraint (see for further development). As the announcement date, we here consider the method of synchronization based on additional assumptions.

Additional synchronization is assumed in the following, it is assumed after a certain limited time [tau], the packet transmission delay upper limit δ. 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].

5.5A binary Byzantine consensus algorithm BAMPn, T [T <N / 3,3Synch]

In this section, we describe this is to ensure that our binary O to terminate the Byzantine consensus algorithm (t) of the wheel, 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. FIG 3 is a new line number "at the end next", where 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 purpose, the circular sequentially plays the role of the coordinator in each process . More precisely, the process is set to P1, ..., the PN, the circle r PI coordinator process is such that i = ((R - 1) MOD N) + 1.[[5]](#footnote-4)

Additional local variables and message types in addition to ESTI, RI, bin\_valuesi [R], and valuesi, each process manages the following local variable PI.

timeri a local timer and a timeout value timeouti, both to use 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] () to attempt to facilitate broadcast its value is a value determined.

|  |
| --- |
| Operation bin\_propose (VI) is  ESTI ← six; RI ← 0; timeouti ← 0;  While (true) do  RI ← RI + 1;  (NEW1) coordi ← ((RI - 1) MOD N) + 1; timeouti ← timeouti + 1; timeri provided to timeouti;  BV\_broadcast EDT [RI] (ESTI);  (NEW2) If (I = coordi) and wait\_until (bin\_valuesi [RI] = {w}); // w is a value of the first entering bin\_valuesi of [the RI] RADIO COORD\_ value [RI] (w) of  just in case;  wait\_until (bin\_valuesi [RI] 6 = ∅) ∧ (timeri expired);  (NEW3) arranged to timeri timeouti;  (NEW4) if (COORD\_ value [RI] (W) received from pcoord I) ∧ - (Watts ∈bin\_values ​​then AUXI ← {w}  Otherwise AUXI ← bin\_valuesi [RI]  just in case;  Broadcast AUX [RI] (AUXI);  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 content is such that, ∃ valuesi such that a non-empty (i) valuesi⊆bin\_valuesi [RI] and (ii) valuesi = ∪1≤x≤n-tb\_valx) ∧ (timeri expired);  (New5) if (when considering the entire message of the set of AUX [RI] () received, sets values1i, values2i, ... satisfy the previously waiting predicate) ∧ - (AUXI which is one) then valuesi ← AUXI END IF;  2 ← RI double mold;  If (valuesi = {V}) // valuesi is a single, whose elements v  Then ESTI ← V; if (V = BI) before deciding (V), if not ended, if;  Otherwise ESTI ← double  just in case;  The end of a period of time. |

Figure 3: a safe and BAMPn binary Byzantine algorithm consensus site, T [t <N / 3,3Synch]

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

In 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, whose expiration for a simple reset to the modified line M-07 predicate.

Line NEW2, NEW4, M-06, and New5 implement a mechanism that allows the current round of coordination, trying to impose its bin\_values ​​set to enter a judgment of the value of[[6]](#footnote-5). 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 M-05 and M-07: In addition to the predicate 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, the set {w} AUXI (line NEW4) all non-fault handling, and broadcasts it (line M-06). W predicate ∈bin\_valuesi [RI] for preventing Byzantine coordinator sends the non-faulty process false foil.

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 will round (R 1) or (R + 2) means that during their decision.

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 δ. 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. tfirst0) will be used to represent the sign of t is elapsed since the beginning of the algorithm have been, observed as measured by the amount of time given the full knowledge of the global viewer G.ģ measurement time unit the same time at least 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 (tfirst0 time, when the first non-consensus start troubleshooting).

tlastr is the last non-faulty process PLAST arrival circle R (tlast0 is the time when the last non-consensus start troubleshooting) as the time measured by the G.

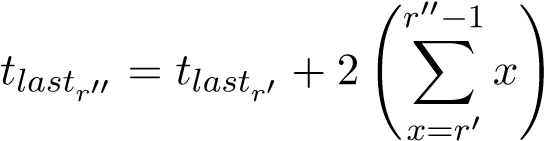
For a circle is synchronous, all non-fault process must have enough time to get all the news that a timeout before any due process trouble-free broadcast of trouble-free process that round. In this case, the last non-fault is processed in turn reaches the coordinator, which may take up to COORD\_VALUE [R] 3 prior to the delay message () message received by all non-fault handling (message comprises up to 2 delayed until a value into its bin\_values [r] and the further delayed broadcast message COORD\_VALUE [R]. Therefore, we must have a round in which r

tlastr + δ≤tfirstr + timeoutr. (1)

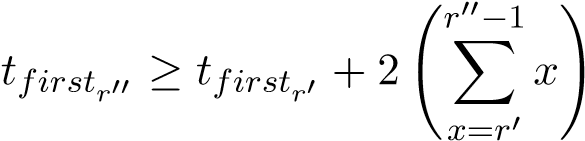
It should be noted that taking into account the time-out from 0 0 round, each by one round of growth, we can replace any one of R timeoutr River

Consider first round timeoutr0≥δ wherein R0 satisfied. R00 R00 wherein for any circle ≥R0 maximum amount of time to complete plastr00 wheel will be 2 × timeoutr00. This is due to the fact, finally trouble-free process in an information circular arrival will not have to wait more than δ longer to accept, to meet on-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-faulty process requires 2 × timeoutr00 R00 least complete circle.

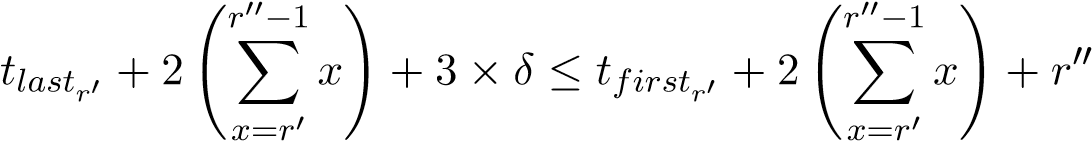
From a certain round in which R00 process last no defect in time can be written as:

 .

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

 .

1 block to the results of this inequality points:

.

Remove the equal components, we have:

tlastr0 + 3 × δ≤ tons first [R0 + R00.]

Therefore, through a circular R00 = tlastr0 + 3 × δ - tfirstr0 synchronization is guaranteed.

Now we will show that once inequality (1) satisfies an R00 (which timeoutr00≥δ), 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 + 3 × δ≤tfirstr00 + timeoutr00. (2)

And it needs to prove the following inequality is true:

tlastr00 + 1 + 3 × δ≤ tons first [R00 + 1 + Timeout [R00 + 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 + 2 × timeoutr00 and tfirstr00 + 1≥tfirstr00 + 2 × timeoutr00. This clogging of the inequality (3) results in:

tlastr00 + 2 × timeoutr00 + 3 × δ≤tfirstr00 + 2 × timeoutr00 + timeoutr00 + 1.

Aliquots result in:

tlastr00 + 3 × δ≤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. 2Lemma 12

The 5.6Proof 3Synch 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 bin\_valuesi [R]. It follows from this local variables and ESTI observed, any non-fault handling (line M-07, New5,10 or 11 defined or updated) from valuesi may contain only during non-fault value. More specifically, we have the following.

Lemma 5. Let R be considered circular, and v is no fault current estimate of the process. Then, we have bin\_valuesi [R] = {V} M-05 line of each non-fault process pi.

If a 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 PK is Byzantine and coordinate round transmittable different values ​​in a non-fault occurred, let us consider the received message COORD\_VALUE [R] non-fault handling ({1 - V}). The (1 - v) of ∈ / bin\_valuesi [R], online NEW4, PI performed "else" portion, where it is provided to AUXI {V} (unique value of [R] in bin\_valuesi), 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. The following facts prove collection bin\_valuesi any non-fault process of troubleshooting can only contain non-recommended value.

Lemma 8. Since 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) the message transmitted by the wheel COORD\_VALUE Coordinator , there is a circle R, as valuesri = {w} in each process the non-defective.

Let us consider a time τ from (due to the lemma 12) system behavior synchronous (time-out value of all non-fault process, so that all information provided by non-faulty process of exchange of timely arrival). Let r PK is coordinated by the failure of the process is not after τ minimum 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. By Lemma 10, all non-fault decision process for a W R + 1, wherein the proof of Lemma conclusions drawn. 2Lemma 14

Theorem 3 Algorithm described in FIG. 3 solves the binary system model BAMPn Byzantine agreement, T [t <N / 3,3Synch].

Demonstrate proof directly from Lemma 13 (BBC- validity and BBC- Protocol) and lemma 14 (BBC- followstermination).

**Pointnity Token**

\* Cross-chain as a reward for the verifier

\*The data is stored in HUB can get as a reward token pont work.

**Name**

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 passwords and ID search engines combine to provide an 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

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

Human-readable (a name that looks like Paul should not 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa)

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 , 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.

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 architecture of the complex technology, greatly reducing development time and cost value, so pointnity is a developer-friendly gathering place.

**Block Chain Development**

The rapid development of the Internet in recent years, coupled with the strength and depth feedback physical world, has radically altered the production, living and management decision-making model of modern society, the formation of the real physical world - tight coupling virtual network space, interaction and actual situation parallel co-evolution of social space, gave birth to the "Internet +" and 4.0 and a series of national industrial strategy for the future development trend of social network certainly from CPS + actual physical world (Cyber-physical systems, CPS) to spiritual artificial world, forming a physical network + + artificial man - machine - ternary composition integration coupling system, information systems called social physical (Cyber-physical-social systems, CPSS) present, based on parallel societies have gradually taken shape CPSS its core is the actual situation and the essential characteristics of the interaction with the parallel evolution

CPSS block chain is parallel to achieve one of the infrastructure of society, its main contribution is to provide a data structure of a well-established center to a distributed social systems and distributed artificial intelligence research, interaction mechanics and computing models, to achieve parallel and lay a solid social foundation and credit data on the basis of the data base, the management Edward Deming once said: in addition to God, everyone must speak to the data center of the social system, however, the data usually controlled by the government and large enterprises and other "minority" in the hands, a few people "speak", its impartiality, the authority may even security can not be guaranteed. block chain data through highly redundant distributed storage nodes, held by "everyone" in the hands, can do real "data democracy." on the basis of credit terms, its highly centralized system of social engineering complexity and social complexity inevitably there will be "Merton system" characteristics, namely uncertainty, diversity and complexity of social systems in the central institutions and rule-makers may arise due to acts of dishonesty individual interests; the block chain technology Contribute to social systems software-defined, the basic idea is to reject centralized institution, to the unpredictable behavior of the program code in the form of a smart contract early deployment and curing block chain data, and afterwards can not be forged and tampered with automation execution, which to some extent can the "Merton" social systems into a comprehensive observation can be actively controlled, can accurately predict the "Newton" social system .

ACP (artificial social Artificial societies, computational experiments Computational experiments and parallel execution Parallel execution) method is so far the only parallel system into the field of social management, integrated research framework, is a logical extension of the lower complexity of science in parallel with the new era of social environment and innovation. ACP method can naturally be combined with the block chain technology, block chain-driven parallel social management. first, P2P networking block chain, distributed collaboration and consensus based on the contribution of economic incentives and other mechanisms themselves distributed modeling natural social system in which each node in a distributed system as an autonomous agent and self-government (Agent). with the improvement of the ecological system of the block chain, chain blocks each node and the growing consensus complex and intelligent autonomous contract through participation in various forms Dapp, form a particular form of organization and the DAO DAC, ultimately the DAS, i.e. ACP artificial society. Secondly, the programmable characteristics of contracts intelligent block chain such that each may be species "WHAT-IF" type of virtual experimental design and evaluation of results deduced scenario, this calculation experimented Obtain and automatically or semi-automatically execute optimal decision. Finally, the block chain with a combination of things such as intelligence assets, which makes China Unicom real physical world and the virtual network space as possible, and through real and actual situation interaction and artificial social systems parallel tuned achieve synergies and optimize social management decision-making is not hard to foresee the future of the real physical world of physical assets are registered as chain intelligence assets when the time is approaching block chain-driven parallel society.

**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, and Canada and the United StatesAs well as China'sResidents are expressly excluded any PONT exchange 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" without any express or implied representations and warranties, including, but not limited to:

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

Contents of this website without any errors or for any purpose;

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: POINITY this website does not constitute a recommendation to any 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 certified by KYC DonateDETAILED format by KYC

Name:

Sex:

Nationality (does not support the United States, Australia area、china):

date of birth:

ID card / passport / driver's license:

ID Photo:

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

Number of intended contributions(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 POI tokens.

**Token Rule:**

A total of 5 billion tokens

**pre-sale: 5%**

Official ratio: 1: 35000(note: Pre-sale contributors lock-in rules, 50 immediately after the exchange is available, and the remaining 50% is released for 6 months on the online exchange.)

**Sale: 15%**

Official ratio: 1: 23000(note: the sales contributor releases 50% of PONTs immediately after the exchange, and the remainder is released after 3 months of trading.)

**Team 35:** technical development and operation awards for team members(note: team lock-in is released in linear equilibrium within 24 months after 12 months on the exchange, once every two months, for a total of 12 releases.)

**Cooperation Organization 25**: use it for ecological incubation, expand the radiation scope of the project, and establish beneficial and good cooperation(note: depending on the circumstances, the minimum time limit for the release and locking of the cooperative organization's tokens is 6 months.)

**Community 20:** to provide advice on community operations, maintain and build a good community environment, you can receive token awards.(note: community escrow release and lock-in, depending on the circumstances, lower limit of unlocked time)

This token is a ERC-20 token and will be replaced by 1:1 tokens on the main network

**In conclusion**

With the strong rise of digital encryption to Bitcoin currency as the representative of an emerging block chain technology has become the hot research topic in academia and industry. Credit to the center of the block chain technology can not be tampered with and programmable features so that it has a wide range of applications in digital encryption monetary, financial and social systems. However, compared with the block chain booming business applications, theory and technology research foundation block chain is still in its infancy, and many more the essential, vital to the development of the industry chain block scientific issues that must be follow-up study. This paper systematically reviews the basic principles of the block chain technology, techniques, methods and applications in order to provide useful inspiration and reference for future research .

PointnityIs a compatible open network, ITheyI believe that his appearance will truly enhance the further development of blockchain world. Here, we sincerely hope that more people will participate in the construction blockchain world has made blockchain contribute to the construction of the world.

1. [↑](#footnote-ref-0)
2. [↑](#footnote-ref-1)
3. [↑](#footnote-ref-2)
4. [↑](#footnote-ref-3)
5. [↑](#footnote-ref-4)
6. [↑](#footnote-ref-5)