CSN Secure network

An underlying technology based on COSMOS

Cross-chain accounting network

Technology and Application White Paper

COSMOS technical description

1 Introduction

The joint success of the open source ecosystem, decentralized file sharing and public cryptocurrency has inspired an understanding of decentralization Internet protocols can be used to fundamentally improve the social and economic infrastructure and enhance network security. Between block and block The bookkeeping function is our technical goal. It is to realize distributed bookkeeping and let more people use it, thus establishing a unique For secure accounting networks, we have seen specialized blockchain applications, such as Bitcoin (a cryptocurrency), Zerocash (a cryptocurrency used for privacy) and general smart contract platforms such as Ethereum, and no A number of Ethereum Virtual Machine (EVM) distributed applications), such as Augur (prediction market) and TheDAO (investment companies) Club).

However, to date, these blockchains have suffered many drawbacks, including their low overall energy efficiency, poor performance or limited performance. The system and governance mechanism are immature. Recommendations to expand Bitcoin transaction throughput (for example, Segregated-Witness and BitcoinNG) is a vertical scaling solution, they are limited by the capacity of a single physical machine to ensure full auditability. Lightning Network can help expand Bitcoin transaction volume by completely eliminating ledger management, which is very suitable Micropayments and privacy-protected payment methods, but may not be suitable for more general expansion needs.

An ideal solution is to allow multiple parallel blockchains to interoperate while preserving their security. Use workload card Ming, this proved to be difficult, if not impossible. For example, merge mining allows to complete the work of ensuring the safety of the parent chain It can be reused on the sub-chain, but the transactions of each node must still be verified in order, and if most of the cases are merged and mined The blockchain is vulnerable to attacks. Part of the parent's hashing capabilities will not actively merge with the mining children. Provided for An academic review of the modern blockchain network architecture to provide more background information, and we provide a summary of other recommendations and their Disadvantages in "related work".

Here, we introduce the CSN security network, a novel blockchain network architecture based on the Cosmos architecture, which can

Solve all these problems. Cosmos is a network composed of many independent blockchains, called regions. These areas are composed of Tendermint BFT provides support, which provides a high-performance, consistent, and secure consensus engine similar to PBFT. Strict fork-accountability guarantees the behavior of malicious actors. The Tendermint BFT consensus algorithm is very It is suitable for expanding the public equity proof blockchain.

The first area of CbaBy vassal on Cosmos is called Cosmos Hub. Cosmos Hub is a simple tube The multi-asset equity proof of cryptocurrency based on the management mechanism enables the network to adapt and upgrade. In addition, you can connect to other areas To expand the Cosmos Hub.

CbaBy and the center and area of the Cosmos network pass through the inter-blockchain communication (IBC) protocol (a type of The virtual UDP or TCP of the chain) communicate with each other. The token can be safely and quickly transferred from one area to another, There is no need to exchange liquidity between regions. Instead, all inter-regional token transfers go through the Cosmos Hub, The center tracks the total number of tokens held in each region. The hub isolates each area from faults in other areas. because Anyone can connect the new zone to the Cosmos Hub, so the zone allows future compatibility with new blockchain innovations.

2 Design principles

2.1 Overview of Blockchain Bitcoin

The concept of decentralized digital currency and alternative applications such as asset registration have existed for decades. The anonymous electronic cash protocol of the 1980s and 1990s mainly relied on a kind of The blinding cryptographic primitives provide a highly private currency, but because they rely on a centralized intermediary, The agreement largely failed to gain traction. In 1998, Wei Dai’s B-money became the first to propose a solution It’s a proposal to create a currency idea based on confusion and decentralized consensus, but with regard to the details of how to achieve decentralized consensus, the proposal Very few. In 2005, Hal Finney introduced a "reusable proof of work" concept, which uses The idea of B-money and Adam Back’s computationally difficult Hashcash puzzle created cryptocurrency A concept, but once again did not reach the ideal relying on trusted computing as the back end.

Since currency is the first archived application, the order of transactions is usually very important, so decentralized currency needs to address decentralization The consensus is that this is the main obstacle faced by all Bitcoin currency agreements, despite years of creating a secure Byzantine content There has been a lot of research on the wrong multi-party consensus system, but all the protocols described only solve half of the problem. Agreement false Assume that all participants in the system are known, and "If N parties participate, then the system can tolerate up to A security boundary in the form of N/4 malicious actors. However, the problem is that in an anonymous environment, this security boundary is easy to Vulnerable to sybil attacks, that is, a single attacker creates thousands of simulated nodes on the server or botnet and uses Use these nodes to unilaterally obtain the majority share.

The innovation provided by Satoshi is the idea of combining a very simple decentralized consensus protocol based on each A node that combines transactions into a “block” in ten minutes creates a growing blockchain and uses proof of work as a machine Through this mechanism, nodes obtain the right to participate in the system. Although nodes with a large amount of computing power do have correspondingly more Great influence, but compared with the entire network, providing more computing power is much more difficult than simulating one million nodes.

Despite the roughness and simplicity of the Bitcoin blockchain model, it has proven to be good enough and will become The foundation of more than 200 currencies and agreements worldwide.

Ethereum

The purpose of Ethereum is to merge together and improve the concept of scripts, altcoins and on-chain protocols, and allow development People create arbitrary consensus applications that are scalable, standardized, functionally complete, and easy to develop. The interoperability provided by the same specification is all at the same time. Ethereum achieves this by building an essentially ultimate abstract base layer This point: a blockchain with a built-in Turing complete programming language, allowing anyone to write smart contracts and decentralized applications, In these applications they can provide ownership, transaction format and state transition functions. A simple namecoin The version can be written in two lines of code, and other protocols such as currency and reputation systems can be established within 20. Smart contracts, Password "boxes" that contain value and can only be unlocked when certain conditions are met can also be built on our platform, It is much more powerful than the functions provided by Bitcoin script, because it has the additional functions of Turing completeness, value recognition, and blockchain recognitio

Know and state.

In this section, we describe the Tendermint consensus protocol and the interface used to build applications using it.

In the classic Byzantine Fault Tolerance (BFT) algorithm, each node has the same weight. In Tenderm int, the section

Points have non-negative voting rights, and nodes with positive voting rights are called verification Device . Verifiers sign or vote via broadcast password

Come participate in the consensus agreement to reach an agreement on the next block.

The verifier’s voting rights can be determined from the beginning, or it can be deterministically determined by the blockchain. more Change, depending on the application.

For example, in a proof-of-stake application (such as the Cosmos Hub), voting rights can be offset by mortgages as collateral.

The number of tokens bet the amount to make sure.

note: ⅔ Scores such as and like represent the scores of total voting rights, and Do not Is the score of the total number of validators, unless all

The weights of witnesses are equal. > ⅔ Means "greater than ⅔ ", ≥ ⅓ Means "at least ⅓ ".

consensus

Tendermint is a partially synchronized BFT consensus protocol derived from the DLS consensus algorithm [20]. With its simplicity, Tendermint

Performance, and fork responsibility system. The protocol requires a fixed set of known verifications Device , Each of which verifies Device All are identified by their public key.

The verifier tries to reach a consensus on one block at a time, and one of the blocks is easy List. A full vote on whether to reach a total

knowledge. Each round has a round leader or proposer who proposes a block. Then, the validators will vote in stages

Decide whether to accept the proposed block or go to the next round. The proposer of the round is determined from the ordered list of validators, and he

Their voting rights are proportional.

The full details of the agreement are here in description.

The security of Tendermint stems from the fact that it passes the super majority (> ⅔) Voting and locking mechanisms use the best Byzantine content

The reason for the wrong function. Together they ensure:

≥ ⅓ Voting rights must be Byzantine, so as to violate security, in which more than two values must be submitted.

If any group of verifiers successfully violates security, or even attempts to violate security, they can proceed through the agreement. Row Recognition. This

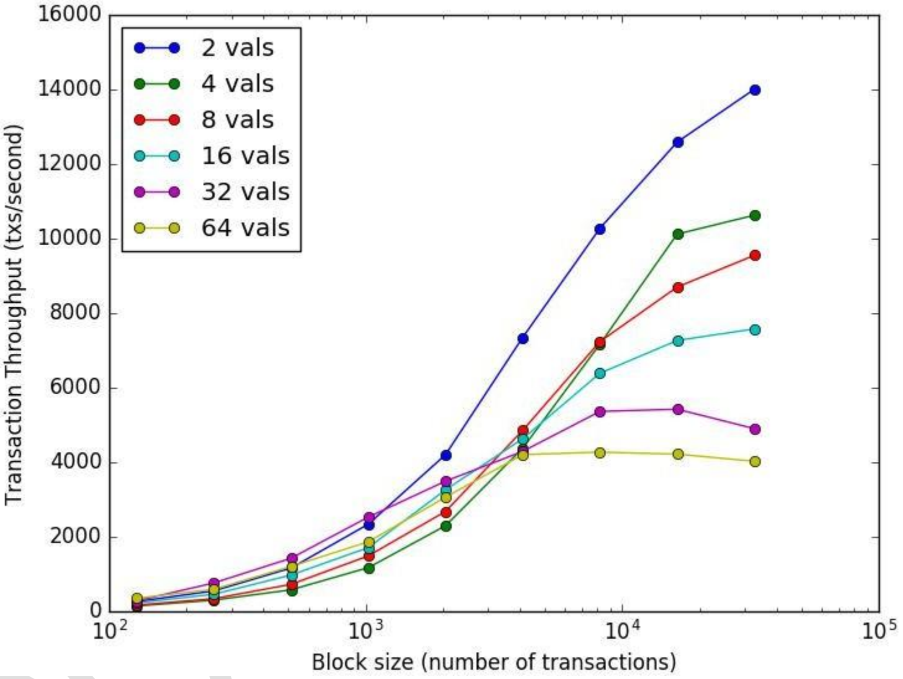
It includes both the disputed part Row Voting, including the right Do not Combine Reason Vote for Row broadcast.

Although strong force Guaranteed, Tendermint can still provide excellent performance. In 27 data centers distributed on five continents

In the benchmark of 164 nodes, in the commodity cloud instance, the Tendermint consensus can reach Reason Thousands of transactions, and

The submission delay is one to two seconds. It’s worth noting that even under severe confrontation conditions, the verification Device Crash or spread malicious

The ballot papers produced can also maintain more than one thousand times per second. easy Performance. See the figure below for details.



Cosmos Hub is the first public blockchain in the Cosmos network, calculated by the Tendermint BFT consensus

Law provides support. The Tendermint open source project was born in 2014 and aims to solve the Bitcoin workload proof consensus

Algorithm speed, scalability and environmental issues. Through the use and improvement of the

With the proven BFT algorithm, the Tendermint team was the first to prove the proof-of-stake cryptocurrency in concept.

Cryptocurrency solves the problem of equity abuse suffered by the first generation of proofs. -Conduct cryptocurrency transactions, such as NXT

And BitShares1.0.

Today, almost all Bitcoin mobile wallets use trusted servers to provide them with transaction verification. this is

Because proof of work needs to wait for many confirmations before the transaction can be regarded as an irreversible promise. in

Double-spending attacks have been proven on services such as CoinBase.

Unlike other blockchain consensus systems, Tendermint provides instant and provable secure mobile client payment

Payment verification. Since Tendermint is designed to never fork, mobile wallets can receive instant

Transaction confirmation, which makes it a reality to realize untrusted and practical payments on smartphones. This also applies to the Internet of Things

Use has had a major impact.

The verifier in Cosmos has a similar role to Bitcoin miners, but uses cryptographic signatures for voting. The validator is

The security dedicated machine responsible for submitting the block. Non-validators can delegate their mortgage tokens (called "atoms") to any

Verifiers to earn part of the block fee and atomic rewards, but if the delegated verifier is hacked or violated

Agreement, they will face the risk of being punished (cut). The effective security of Tendermint BFT consensus

Full guarantee, as well as mortgage deposits of stakeholders (validators and delegators), provide nodes and light clients with

Provable and quantifiable safety.

Governance

The distributed public ledger should have a constitution and governance system. Bitcoin relies on the Bitcoin Foundation and mining to coordinate

Level, but this is a slow process. After the fork to solve the TheDAO hack, Ethereum was divided into Ethereum and

ETC, mainly because there is no prior social contract or mechanism for making such decisions.

The validators and delegators on the Cosmos Hub can automatically change the system preset parameters (for example, gas limit).

System), coordinate the upgrade proposal to vote, and you can also vote to determine the human-readable constitution that can control the organization’s policies.

Amendment. The center of the universe. The constitution allows stakeholders to discuss issues such as theft and mistakes (such as TheDAO incident)

Unite on the same kind of problems, so that the problem can be solved faster and cleaner.

Each region can also have its own constitution and governance mechanism. For example, a Cosmos hub can have a hub

The construction of mandatory immutability (no rollback, except for errors implemented by the Cosmos Hub node), and each region

You can set your own rollback strategy.

By achieving interoperability between different strategic areas, the Cosmos network provides users with the greatest degree of freedom,

And has the potential to conduct unlicensed trials.

Hubs and zones

Here, we describe a new model of decentralization and scalability. Cosmos is supported by Tendermint

Many blockchain networks. Although the existing proposal aims to create a “single blockchain” with a global total transaction sequence,

But Cosmos allows many blockchains to run concurrently while maintaining interoperability.

On this basis, the Cosmos Hub manages many independent blockchains, called "zones" (sometimes called "shards",

Refers to the database expansion technology called "fragmentation"). Continuous updates from the area posted on the hub

The new block submission stream enables the hub to keep up with the state of each zone. Similarly, each zone is protected with the status of the hub

Support synchronization (but the regions are not indirectly synchronized through the hub). Then, by issuing the Merkle certificate

As evidence of the sending and receiving of information, the information packets are passed from one area to another. This mechanism is called

It is inter-blockchain communication, referred to as IBC.

Any area itself can be a hub that forms an acyclic graph, but for the sake of clarity, we only describe

Simple configuration of one hub and many non-hub areas.

Hub

Cosmos Hub is a blockchain hosting a multi-asset distributed ledger. Tokens can be managed by a single user or region

Hold by itself. These tokens can be moved from one zone to another in a special IBC pack called a "coin pack"

area. The hub is responsible for preserving the global immutability of the total amount of each token in the area. IBC coin data packet transactions must be

The sender, hub and receiver block chain.

Since the Cosmos hub acts as the central ledger for the entire system, the security of the hub is of utmost importance. Exhausted

Although each area may be a Tendermint blockchain, its security can be as low as 4 (if BFT is not required)

Consensus, or even less), but the hub must be protected by a set of globally distributed validators, these validators

It can withstand the most severe attack scenarios, such as attacks sponsored by a continental network or a nation-state.

area

The Cosmos zone is an independent blockchain that can exchange IBC messages with the hub. From the point of view of the hub,

The zone is a multi-asset dynamic member multi-signature account that can use IBC packets to send and receive tokens. Like encryption

Like currency accounts, the region cannot transmit more tokens than it, but can receive from others who own the tokens

Token. A zone can be designated as the "source" of one or more token types, thereby granting the zone to expand the token

Power of supply.

The atoms of the Cosmos Hub may be staked by validators in the region connected to the Hub. Although these areas are

A double-spending attack will cause Tendermint’s fork-accountability to cut atoms, but greater than ⅔ of

Areas where voting rights are Byzantine may be submitted to an invalid state. Cosmos Hub will not verify or execute in other regions

The transaction is committed on the domain, so users are responsible for sending tokens to their trusted zone. In the future, Cosmos Hub

The governance system may adopt Hub improvement suggestions that take into account regional failures. For example, when an attack is detected, you can

To restrict the transmission of outbound tokens from some (or all) areas to allow emergency circuit interruption (token

Transmission is temporarily stopped).

Inter-blockchain communication (IBC)

Now, let's take a look at how the hub and zone communicate. For example, if there are three blockchains, "Zone1",

"Zone2" and "Hub", we hope "Zone1" will generate a data packet sent to "Zone2" and pass

"Hub". In order to move data packets from one blockchain to another, a proof is issued on the receiving chain. certificate

It has been shown that the sending chain issued the so-called destination packet. In order for the receiving chain to be able to check this proof, it must

Able to keep up with the sender's block header. This mechanism is similar to that used by the side chain, which requires two interactions

The chain of two-way evidence to prove the datagram (transaction) flow to understand each other.

Naturally, two types of transactions can be used to define the IBC protocol: an IBCBlockCommitTx transaction that allows

Allows the blockchain to prove its latest hash value to any observer; another IBCPacketTx transaction allows the blockchain

Prove to any observer that a given packet was indeed hashed by the sender's application by hashing the most recent block

Merkle certificate issued.

By dividing the IBC mechanism into two independent transactions, we allow the local charging market mechanism of the receiving chain to determine the submission

(That is, confirmed) data packets, and at the same time, how many outbound data packets are allowed completely freely on the sending chain.

In the example above, in order to update the block hash of "Zone1" on "Hub" (or

The block hash of "Hub" on "Zone2" IBCBlockCommitTx), the block hash of "Zone1" must be used

Post the transaction on the "Hub" (or on "Zone2", the hash value is "Hub").

For more information on the two IBC transaction types, see IBCBlockCommitTx with IBCPacketTx .

Example

Distributed exchange

Just like increasing the security of Bitcoin by becoming a distributed, large-scale replicated ledger, we can use

Run the exchange on the blockchain to reduce the exchange's attack by external and internal hackers. We call it distributed

exchange.

Today, the so-called decentralized exchange in the cryptocurrency community is based on a transaction called "Atomic Cross-Chain" (AXC)

s things. Using AXC transactions, two users on two different chains can conduct two transactions on two ledgers together

The transfer transaction is committed, or not committed at all (that is, atomic). For example, even if Bitcoin and Ethereum are not mutually exclusive

Connected, two users can also use AXC transactions to exchange bitcoins for ether (or any of two different ledgers)

Italian two tokens). The advantage of running exchanges on AXC transactions is that users do not need to trust each other or transaction matching services.

Affair. The disadvantage is that both parties must be online to make a transaction.

Another type of decentralized exchange is a large-scale replicated distributed exchange running on its own blockchain. Advance Users who perform such transactions can submit limit orders and turn off their computers, and transactions can be made when the user is not online. Execute under conditions. Blockchain matches and completes transactions on behalf of traders.

Centralized trading can create a deep order book of limit orders, thereby attracting more traders. Liquidity on the exchange There is more liquidity in the world, so there is a strong network effect in the exchange business (or at least as a winner As the dominant effect). Today, the current leader of cryptocurrency exchanges is a 24-hour trading volume of 20 million U.S. dollars Poloniex, ranked second, is Bitfinex with a 24-hour trading volume of 5 million U.S. dollars. Given this strong With large network effects, AXC-based distributed switches are unlikely to win the transaction volume of centralized switches. in order to To make decentralized exchanges compete with centralized exchanges, it needs to support deep orders with limited price orders. Only blocks Only distributed exchanges on the chain can provide this.

Tendermint provides other benefits of faster transaction commit. By prioritizing without sacrificing consistency Considering fast certainty, the area in Cosmos can quickly complete transactions-for exchange order transactions and IBC orders The transfer of cards to and from other areas.

In view of the current state of cryptocurrency exchange, an important application of Cosmos is distributed exchange (also known as Cosmos DEX). Transaction throughput and submission delay are comparable to centralized exchanges. Traders can submit limit orders, It can be executed without both parties being online. With Tendermint, Cosmos Hub and IBC, traders can quickly Place funds in and out of the exchange to other areas.

Bridge to other cryptocurrencies

Privileged areas can serve as a source of bridging tokens for another cryptocurrency. The bridge is similar to the Cosmos hub and district The relationship between domains. Both must keep up with the latest block of the other to verify that the token has been moved from one to the other evidence. The "bridge zone" on the Cosmos network is in sync with hubs and other cryptocurrencies. By bridging The indirection of the region allows the logic of the hub to be kept simple, and is compatible with other blockchain consensus strategies (such as Bitcoin's Proof-of-work mining) irrelevant.

Send token to Cosmos Hub

Each bridge validator will run a blockchain with Tendermint, a special ABCI bridge application, And a full node of the "original" blockchain.

When mining a new block at the origin, the bridge area validator will sign and share its blockchain skills to the origin. The respective local views come to an agreement on the submitted blocks. When the bridge area receives payment at the origin (and agrees In the case of a PoW chain such as Ethereum or Bitcoin, sufficient confirmation has been confirmed), it will be in the bridge area Create a corresponding account with the balance on the domain.

In the case of Ethereum, the bridge zone can share the same validator set with the Cosmos Hub. On the Ethereum side Face (origin), the bridge contract will allow Ethereum holders to pass the bridge contract that sends Ether to Ethereum To transfer the ether to the bridging area. Once the bridge contract receives ether, unless the bridge contract is received from the bridge area Appropriate IBC packet, otherwise it cannot be withdrawn. The bridge contract tracks the set of verifiers in the bridge area, which verifies The set of validators may be the same as the validator set of the Cosmos Hub.

As far as Bitcoin is concerned, this concept is similar, the difference is that each UTXO will be multi-signed by a threshold P2SH Release to control, not a single bridge contract. Due to the limitations of the P2SH system, signers cannot communicate with The Cosmos Hub validator set is the same.

Withdraw tokens from Cosmos Hub

Ethereum in the bridge area ("Bridged Ethereum") can be transferred back and forth between hubs, and then through Transactions sent to a specific withdrawal address on Ethereum are destroyed. The IBC data packet can be used to prove that the transaction occurred on the bridge And then publish it to the Ethereum bridge contract to allow Ether to be withdrawn.

As far as Bitcoin is concerned, the restricted scripting system makes it difficult to mirror the IBC coin transfer mechanism. Every UTXO has Has its own independent release. Therefore, when the set of Bitcoin custody signers changes, each UTXO must Must migrate to the new UTXO. One solution is to compress and decompress UTXO sets as needed to reduce UTXO total.

The overall responsibility system of the bridge area

The risk of such a shrinking contract lies in the rogue verifier. ≥ ⅓ Byzantine voting rights may cause a fork, which will convert Ether Withdraw from the bridge contract on Ethereum, and keep Ether on the bridge zone. To make matters worse,> ⅔ Byzantine voting Rights may deviate from the original bridging logic of the bridging zone, thereby completely removing it from those who send it to the bridging contract. Steal ether.

These problems can be solved by designing fully responsible bridges. For example, all IBCs from hubs and origin Data packets may need to be confirmed by the bridge area, so that the hub or the originator’s bridge can effectively pick War and verify all state transitions and contracts in the bridge area. The hub and source should allow the bridge area verification procedure to pass

Account collateral, and the transfer of tokens from the bridge contract should be delayed (and the unsecured period of the collateral is sufficient

Long) to allow independent auditors to raise any challenges. We take the design of the specification and the realization of the system as

Suggestions for future improvements of Cosmos are open for approval by the Cosmos Hub governance system.

Ethereum scaling

For Ethereum, solving the scale problem is an unsolved problem. Currently, the Ethereum node processes each order

Transactions and store all states.

Since Tendermint can submit blocks faster than Ethereum's proof of work, Tendermint

The EVM area supported by consensus and running on the bridge ether can provide higher performance for the Ethereum blockchain. In addition,

Although the Cosmos Hub and IBC data packet mechanism does not allow arbitrary execution of contract logic, it can be used for coordination.

Adjust the movement of tokens between Ethereum contracts running in different regions, so as to use tokens as the center of sharding.

Heart's Ethereum extension provides the foundation.

Multi-application integration

The Cosmos region runs arbitrary application logic, which is defined at the beginning of the region's life cycle, and

And may be updated through governance over time. This flexibility allows the Cosmos region to act as

It is a bridge to other cryptocurrencies (such as Ethereum or Bitcoin), and also allows the use of the same code base but with different

The set of validators and those blockchain derivatives that were initially distributed. This makes many existing cryptocurrency frameworks (e.g.

Such as Ethereum, Zerocash, Bitcoin, CryptoNote, etc.) can be used with Tendermint BFT,

The latter is a high-performance consensus engine that can be used on the general network, opening up cross-platform interoperability

Great opportunity. In addition, as a multi-asset blockchain, a single transaction may contain multiple inputs and outputs, each of which

The input can be any token type, so that Cosmos can be directly used as a platform for decentralized transactions, despite the fake

Orders are matched through other platforms. Optionally, the zone can be used as a distributed fault-tolerant exchange (with subscription

Single book), which can strictly improve the existing centralized encryption currency exchange, while the existing centralized encryption

Currency exchange will be invaded over time.

Regions can also be used as a blockchain version supported by enterprise and government systems, where traditionally an organization or a group of groups

Some parts of specific services run by the organization are run as ABCI applications in a certain area, which allows it to continue

Inherit the security and interoperability of the Cosmos public network without sacrificing control of basic services. So yes

For organizations that want to use blockchain technology but completely give up control to a distributed third party, Cosmos

It may provide the best of both worlds.

Network partition mitigation

Some people claim that a major problem with consensus algorithms like Tendermint that is conducive to consensus is that any

Resulting in no voting power greater than ⅔ (For example, ≥eg offline), the network partition of a single partition will completely terminate the consensus.

The Cosmos architecture can alleviate this problem by using a global hub with regional autonomous regions.

In the district, the voting rights of each area are allocated based on the common geographic area. For example, a common paradigm might be

Allow cities or regions to operate their own while sharing a common hub (such as the Cosmos hub)

Area so that municipal activities can continue in the event that the hub ceases to be active due to temporary network partitions. please

Note that this allows real geological, political, and network topology characteristics to be considered when designing a robust joint fault-tolerant system.

Joint Name Resolution System

NameCoin is one of the first blockchains that attempted to solve the name resolution problem by adapting the Bitcoin blockchain. Do not

Fortunately, this method has some problems.

For example, using Namecoin, we can verify @ *satoshi* Is it on a particular public key in the past

Register, but unless we download the latest update since that name. This is due to Bitcoin's UTXO transaction

Limitations of the Merkleized model. In this model, only transactions (not variable application state) are

Merkle is transformed into a block hash. This allows us to prove the existence, but not the non-existence, to change the name later

New situation. Therefore, if you don't trust a complete node, or download the entire blockchain,

Incurring a lot of costs, we cannot determine the latest value of a name.

Even if a Merkleized search tree is implemented in NameCoin, its dependence on proof-of-work makes it lighter

Client verification becomes a problem. The light client must download a complete copy of the headers of all blocks in the entire blockchain (or to

Less update all headers since the last update of the name). This means that bandwidth requirements are linearly proportional to time

example. In addition, changing the name on the proof-of-work blockchain requires waiting for an additional proof-of-work confirmation block, which can be

It can take up to an hour of Bitcoin.

With Tendermint, what we need is the latest block signed by a quorum of validators (through voting rights)

The hash, and the Merkle proof of the current value associated with the name. In this way, the name value can be concise,

Fast and secure light client verification.

In Cosmos, we can take this concept and expand it further. Each name in Cosmos Note

Registered areas can have associated top-level domain (TLD) names, such as ".com" or ".org", and each name

It is said that the registration area can have its own management and registration rules.

Issuance and incentives

Atomic token

Although the Cosmos Hub is a multi-asset distributed ledger, there is a special native token called

CSN . Atom is the only collateral token of the Cosmos Hub. Atom is the holder can vote, verify or delegate it

His validator's license. Just like Ethereum’s Ether, atoms can also be used to pay transaction fees to reduce waste.

The amount of spam. Additional inflationary atoms and block transaction fees will be rewarded to validators authorized to validators

And representatives.

The BurnCSNTx transaction can be used to recover any proportion of tokens from the reserve pool.

Fundraiser

The initial distribution of Atomic Tokens and validators on Genesis will be distributed to Cosmos fundraisers (75%), the main donation

Supporters (5%), Cosmos Network Foundation (10%) and ALL IN BITS, Inc (10%)

Donors. From the start of generation, 1/3 of the total number of atoms will be rewarded to bound validators and delegators each year.

Limit on the number of validators

Unlike Bitcoin or other proof-of-work blockchains, the Tendermint blockchain has increased communication complexity

And it becomes slower and slower, more verifiers. Fortunately, we can support enough validators to

Very fast transaction confirmation time to build a powerful global distributed blockchain, and with bandwidth, storage and parallel calculations

With the increase of computing power, we will be able to support more validators in the future.

On the creation day, the maximum number of validators will be set to 100, and this number will increase by 13% by 10

Years, and finally determined to be 300 verifiers.

Year 0: 100

Year 1: 113

Year 2: 127

Year 3: 144

Year 4: 163

Year 5: 184

Year 6: 208

Year 7: 235

Year 8: 265

Year 9: 300

Year 10: 300

...

Become a validator after creation

CSN holders who have not yet signed can become verifiers by signing and submitting a BondTx transaction. Provided as offset

The number of atoms bet must be non-zero. Anyone can become a validator at any time, unless the size of the current validator set

More than the maximum number of validators allowed. In that case, only if the atomic weight is greater than that held by the smallest verifier

The transaction is only valid when the effective atomic weight (effective atom includes commissioned atom). When the new validator is replaced in this way

Existing validator, the existing validator will become inactive, and all atoms and delegated atoms will be

Enter the unlocked state.

Verifier's fine

If there is an intentional or unintentional deviation from an approved agreement, certain penalties must be imposed on the verifier. Some evidence can be immediately

Accepted, such as double signs at the same height and circle, or violation of "pre-lock" (Tendermint Consensus

Rules). These evidences will cause the verifier to lose its good reputation, its bonded atoms, and the amount in the reserve pool. Proportional token shares (collectively referred to as "equity") will be reduced.

Sometimes, the validator will be unavailable due to local network interruption, power failure, or other reasons. If in the past In the ValidatorTimeoutWindow during what time period, the validator’s submission vote is not If ValidatorTimeoutMaxAbsent is included in the blockchain multiple times, the validator will become inactive, And lose ValidatorTimeoutPenalty's equity (default is 1%).

Certain "malicious" behaviors will not produce obvious identifiable evidence on the blockchain. In these cases, if there are more Based on consensus, validators can perform out-of-band coordination to force these malicious validators to time out.

In the Cosmos hub due to ≥ ⅓ The voting rights alliance is offline and ceases to operate, or ≥ ⅓ Voting rights In the case where the inspectors of the censor review the evidence of malicious behavior entering the blockchain, the hub must be restored through a hard fork reorganization-proposal. (Link to "Fork and Censorship Attack").

Governance norms

Cosmos Hub is operated by a distributed organization, and the organization needs to define a clear governance mechanism to coordinate the blockchain Various changes of the system, such as the variable parameters of the system and software upgrades and structural revisions.

All validators are responsible for voting on all proposals. Failure to vote on the proposal in time will result in The verifier will automatically deactivate AbsenteeismPenaltyPeriod for a period of time (default is 1 week).

The delegator automatically inherits the votes of the delegated verifier. The vote may be manually rejected. Unbonded atoms are not shown Decision-making power.

Each proposal needs to deposit MinimumProposalDeposit tokens, which can be one or more tokens

(Including atoms) combination. For each proposal, voters can vote to decide whether they need to pay a deposit. If it exceeds

Half of the voters choose to accept the deposit (for example, because the proposal is spam), the deposit will enter

The reserve pool, except for the burned atoms.

For each proposal, voters can vote using the following options:

- Yes it is
- YeaWithForce
- That's right
- NayWithForce
- Abstain

Must be voted by Yea or YeaWithForce (or Nay or NayWithForce) by an absolute majority,

Only then can the proposal be passed (decided by failure), but 1/3+ of the votes can be rejected by "mandatory" voting

Count the votes. When the strict veto power is rejected, everyone will lose the value of VetoPenaltyFeeBlocks (default

Recognize the cost (except for unaffected taxes) for 1 day's blocking value) and be punished, but rejected the majority vote

The specified parties will also be punished for loss of VetoPenaltyCSNs (default 0.1%) of atoms.

Parameter change proposal

Any parameter defined here can be changed via ParameterChangeProposal.

Bounty proposal

The expansion of the atom can expand the atom and spend the reserve fund BountyProposal.

Text proposal

All other proposals, such as the proposal to upgrade the protocol, will be coordinated through General TextProposal.

route map

Related work

In the past few years, there have been many innovations in blockchain consensus and scalability. This section briefly outlines some important

factor.

Consensus system

Classic Byzantine fault tolerance

The consensus that there are malicious participants is a problem that dates back to the early 1980s, when Leslie Lampert

(Leslie Lamport) coined the term "Byzantine error" to refer to any process behavior that is different from the expected behavior

As, contrary to "crash error", one of the processes simply crashes. People found an early solution for the synchronization network

Solution, in the synchronous network, the message waiting time has an upper limit, although the actual use is limited to highly controlled

Environments, such as aircraft controllers and data centers synchronized by atomic clocks. Until the late 1990s, practical Byzantine

Ting-style fault tolerance (PBFT) was introduced as an effective partial synchronization consensus algorithm, which can tolerate arbitrary behavior

1/3 of it. PBFT has become a standard algorithm and has produced many variants, including one recently created by IBM,

As part of its contribution to Hyperledger.

The main advantage of Tendermint consensus over PBFT is that Tendermint has an improved and simplified underlying structure.

Some of them are the result of adopting the blockchain paradigm. Tendermint blocks must be submitted in order to avoid

The complexity and communication overhead associated with PBFT's view changes. In the universe and many cryptocurrencies, there is no

Necessary to allow blocks $N + I$,among them $I>= 1$ Commit, when block $\tilde{N}$ It has not been submitted yet. If the bandwidth is a block N not

The reason for submitting in the Cosmos zone, then the block $N + i$ Using bandwidth to share voting is of no avail. Such as

If the network partition or offline node is blocked N The reason has not been submitted, then $N + i$ Nor will it be submitted.

In addition, batching transactions into blocks allows regular Merkle hashing of the application state without

It is a regular summary like PBFT's checkpoint scheme. This can provide faster provable for light clients

Transaction submission, and faster communication between blockchains.

Tendermint BFT also includes many optimizations and functions beyond the scope specified by PBFT. For example, the verifier proposes

The block is divided into multiple parts and processed by Merkle, and then idled in a way to improve broadcast performance.

chat.

In addition, Tendermint BFT does not make any assumptions about peer-to-peer connections, and as long as the P2P network connection is thin

It can work normally if it is weak.

BitShares entrusted shares

Although it is not the first company to deploy Proof of Stake (PoS), BitShares1.0 is the research of PoS blockchain

And adoption has made a huge contribution, especially those PoS called "delegation". In BitShares, interests

Relevant parties choose "witnesses" who are responsible for witnessing and submitting transactions, and "representatives" who are responsible for coordinating software updates

The goal of BitShares2.0 is to achieve high performance under ideal conditions (100k tx/s, delay of 1s), each block

Both are signed by a single signer, and the transaction completion time is much longer than the block interval. The specification is still under development. Interests

Authorities can delete or replace improper witnesses every day, but there is no substantial collateral for witnesses or representatives, just like

Like Tendermint PoS, it will be reduced in the case of a successful double-spend attack.

star

On the basis of the method first proposed by Ripple, Stellar perfected the Joint Byzantine Agreement

The consensus model in which the process of participating in the consensus does not constitute a fixed and globally well-known collection. Rather, each process

Nodes will manage one or more "arbitration slices", and each "arbitration slice" constitutes a set of trusted processes. star

The "quorum" in is defined as a set of nodes, for each node in the set contains at least one quorum

Slice so that an agreement can be reached.

The safety of the stellar mechanism depends on the intersection of assumptions *any* Two arbitrations are non-empty, and the availability of one node requires

At least one arbitration slice is completely composed of the correct nodes, so that it can be used between large and small arbitration slices

It may be difficult to balance assumptions about trust without exerting obvious influence. Finally, the festival

The point must somehow select enough arbitration slices to have sufficient fault tolerance (or no “complete

Node”, which depends on most of the results of this article), and is the only provision strategy to ensure this configuration is hierarchical,

Similar to the Border Gateway Protocol (BGP), it is used by the top ISPs on the Internet to establish a global routing table, and

And it is used by the browser to manage the TLS certificate. Both are notorious for their insecurity.

The token strategy described here alleviates the criticism of the Tendermint-based proof-of-stake system in the Stellar paper.

Which released a kind called *atom* A new type of token that represents a claim on the future portion of fees and rewards.

Therefore, the advantage of proof of stake based on Tendermint is relatively simple, while still providing sufficient and provable

Security guarantee.

Bitcoin NG

BitcoinNG is a proposed improvement to Bitcoin that will allow vertical expansion, such as adding blocks

Size without the negative economic consequences usually associated with such changes, such as the huge impact on small miners. through

This improvement was achieved by separating the leader election from the transaction broadcast: the leader first passed the proof of work in the “microzone”.

Block" election, and then be able to broadcast the transaction to be submitted until a new micro block is found. This reduces the winning PoW

The bandwidth required for the competition allows small miners to compete more fairly and allows the last miner to conduct more regularly

Transaction to find microblocks.

Casper

Casper is a proof-of-stake consensus algorithm proposed for Ethereum. Its main mode of operation is "Accept by Bet".

By allowing validators to iteratively bet on what they think will enter the block based on other bets they have seen so far

The block of the chain can finally achieve finality. This is an active area of research by the Casper team. The challenge is to build

It can be proved to be an evolutionarily stable strategy betting mechanism. Compared with Tendermint, Casper’s main advantages

The trend may be to provide "availability rather than consistency"-consensus does not require more than a quorum of voting rights-possible

It comes at the cost of submission speed or implementation complexity.

Horizontal zoom

Ledger agreement

The Interledger protocol is not a strict scalability solution. It is through a loosely coupled bilateral network of relationships

Provide temporary interoperability between different ledger systems. Like the Lightning Network, the purpose of ILP is to facilitate payments,

But it specifically targets payments of different ledger types, and extends the atomic transaction mechanism to include not only hash locks, but also

Including the number of quorums (called atomic transfers). protocol). The latter enforces atomicity in transactions between ledgers

The mechanism of sex is similar to Tendermint's light client SPV mechanism, so it is necessary to use ILP and Cosmos/

Distinguish between IBC.

1. The notary of the connector in the ILP does not support membership changes, and does not allow the notaries to flexibly add

right. On the other hand, IBC is specifically designed for blockchain, validators can have different weights, and membership can be

In order to change in the process of blockchain.

2. Just like in the Lightning Network, the payment recipient in ILP must be online to send the confirmation back to the sender

square. When transferring tokens through IBC, the validator of the recipient's blockchain is responsible for providing confirmation, not receiving

user.

3. The most notable difference is that the ILP connector is not responsible for paying or maintaining the authoritative status of the payment, while the

In Cosmos, the validator of the hub is the authorizer of the IBC token transfer status, and each holder holds

The power of the number of tokens. Region (rather than the number of tokens held by each account in the region). This is a basic innovation

New, it can make tokens from one area to another area for safe asymmetric transmission; ILP connection in Cosmos

The analog of the connector is a durable and most secure blockchain ledger, the Cosmos Hub.

4. Payments between ledgers in ILP need to be backed by an exchange order book, because there are no coins from a category

An asymmetric transfer from an account to another ledger is simply a transfer of value or market equivalents.

Side chain

The side chain is a mechanism that expands the Bitcoin network by "bidirectionally pegging" the Bitcoin block chain instead of the block chain. (double

To hook is equivalent to bridging. In Cosmos, we say "bridging" to distinguish it from market pegs). Side chain allows

Xu Bitcoin effectively moved from the Bitcoin blockchain to the sidechain and back, and allowed experiments on the new features of the sidechain.

Just like in the Cosmos Hub, the sidechain and Bitcoin act as light clients with each other, using SPV proof to confirm

Determine when the coin should be transferred to the side chain and back. Of course, because Bitcoin uses proof of work, Bitcoin is

The central side chain suffers from many problems and the risk of proof-of-work as a consensus mechanism. Besides, this is a Bitcoin

The maximum solution, unlike Cosmos, which supports multiple tokens and inter-regional network topologies. that is,

The core mechanism of the two-way peg is in principle the same as the mechanism adopted by the Cosmos network.

Ethereum's scalability efforts

Ethereum is currently studying many different strategies to shard the state of the Ethereum blockchain to meet scalability requirements.

begging. The goal of these efforts is to maintain the current abstraction layer provided by the Ethereum virtual machine in the shared state space. Currently

A number of research work in progress

CSN vs Ethereum 2.0 Fuchsia

CSN has different design goals in Cosmos and Ethereum 2.0 Mauve.

- The universe is especially about tokens. Mauve is related to extended general computing.
- Cosmos is not restricted by EVM, so even different VMs can interoperate.
- Cosmos allows zone creators to determine who verifies the zone.

Anyone can Cosmos Initiate a new area (unless governance decides otherwise).

- The hub isolates area failures, so the global token invariant is retained.
- General zoom
- Lightning Network

- The Lightning Network is a proposed token transmission network that runs on the Bitcoin blockchain (and other public areas) Blockchain) by moving most transactions from the consensus ledger to the so-called "payment channel". Cryptocurrency on the chain This is made possible by the script, which enables parties to sign a bilateral stateful contract under which the Share the digital signature to update the status, and the contract can be closed by finally publishing the evidence on the blockchain. The system was first cross-promoted-chain atom exchange. By opening payment channels with multiple parties, Lightning Network participants can become It is the focus of routing other people’s payments to establish a fully connected network of payment channels,
- Although the Lightning Network can easily scale across multiple independent blockchains to allow The market transfers value, but it cannot be used to transfer tokens asymmetrically from one blockchain to another. The main benefit of the Cosmos network described here is that this direct token transfer can be realized. In other words, out of knot For cost-saving and privacy reasons, we expect that payment channels and the Lightning Network will be used together with our token transmission mechanism. broadly used.

Segregated witness

Segregated Witness is a Bitcoin improvement proposal , Aims to increase the throughput of transactions per block by 2 times or 3 times, and at the same time Make the block synchronization of the new node faster. The great thing about this solution is that it is within the limits of Bitcoin's current protocol How does it work and allow soft fork upgrades (that is, clients with older versions of software will continue to run after the upgrade).

Tendermint is a new protocol with no design restrictions, so it has different expansion priorities. initial, Tendermint uses a cryptographic signature-based BFT round-robin algorithm instead of a mining algorithm, which simply allows Horizontal scaling is performed through multiple parallel blockchains, while conventional, more frequent block submissions also allow vertical scaling.

---

appendix

Cross accountability

A well-designed consensus protocol should provide some guarantees in the event that tolerance is exceeded and consensus fails. This is byzantine

Court behavior can bring considerable economic returns, especially in economic systems. The most important guarantee is *Derived responsibility*

A form in which the process that causes the consensus to fail (ie, causes the client of the protocol to accept a different value-derived) can be

Identify and punish according to the rules of the agreement, or it may be a legal system. When the enforcement of the legal system is unreliable

Or when the cost is too high, the validator may be forced to pay a deposit to participate in it, and when malicious behavior is detected, the validator may be

To revoke or reduce these deposits.

Please note that this is different from Bitcoin, which is due to the asynchronous nature of the network and the probabilistic nature of discovering partial hash collisions.

Forking often occurs. Because in many cases, due to asynchrony, a malicious fork is indistinguishable from a fork

, So Bitcoin cannot reliably realize the accountability system for forks, except for the implicit miners paid for mining orphaned blocks

opportunity cost.

Gentle consensus

We will vote stage *Called PreVote* with *PreCommit* . Voting can be for a specific block or for

Correct *Nil* . We will compare the> of a single block in the same round ⅔ The PreVotes collection is called *Polka* , And put a single block in the same round

Of> ⅔ The PreCommits collection is called *Commit* . If in the same round >> PreCommit for Nil,

They will move to the next round.

Please note that the strict determinism in the protocol will lead to a weaker synchronization assumption, because defects must be detected and skipped.

Trapped leader. Therefore, the validator has to wait for a period of time before pre-selecting Nil, that is *TimeoutPropose* ,

And the value of TimeoutPropose will increase with each round. The next round of progress is completely asynchronous

Because only the verifier from the network> ⅔ The progress will not be completed until you hear it. In practice, to frustrate indefinitely

Weak synchronization hypothesis (resulting in consensus not being able to submit blocks), will require a very strong opponent, and pass in each test

Using the random value of TimeoutPropose on the certificate, it may become more difficult to do so.

Another set of constraints or locking rules ensures that the network ultimately submits only one block at each height. Can identify any A malicious attempt resulted in the submission of more than one block at a given height. First, the PreCommit of a block must With a reason, it appears in the form of Polka in the block. If the verifier is already in the round *R 1 on advance* Submitted a Blocks *, We say they have _lock* On that block and used to prove that the new round is on *R_2* The dots at the dots must be Must be in the round *R_polka* ,among them *R_1 <R_polka <= R_2* . Second, the verifier must propose and/or pre-First vote to lock their locked blocks. These conditions together ensure that the verifier does not have sufficient evidence as a reason PreCommit will not be performed in the case of, and the verifier who already has PreCommit cannot do other things provide evidence. This ensures the safety and effectiveness of the consensus algorithm.

Gentle light client

In Tendermint-PoS, the need to synchronize all block headers is eliminated, because the existence of alternate chains (forks) means Therefore, it is possible to reduce the mortgage shares ≥1/3. Of course, due to reduced requirements *Someone* Share the evidence of the fork, so light off The client should store any block hash commits it sees. In addition, the light client can periodically change with the validator set Keep in sync to avoid Long-range attack (But other solutions are also possible).

Like Ethereum, Tendermint allows applications to embed a global Merkle root hash in each block, So that you can easily query the status, such as account balance, value stored in the contract or whether there is unused The transaction output, etc., depends on the nature of the application.

Prevent remote attacks

Assuming that the broadcast network has a sufficiently flexible collection and a static verification assembly, it can detect the Any branch and cut the deposit for the problematic verification program. This innovation was created by Vitalik Buterin in 2014 It was first proposed at the beginning of the year to solve the unsecured problem of other proof-of-interest digital currencies.

However, because the set of validators must be able to change, for a long period of time, the original validators may all

Are not bound, so you can freely create new chains from the genesis block without paying any fees, because they

No longer need to lock up deposits. In contrast to short-range attacks, this type of attack is called a long-range attack (LRA).

In a short-range attack, the currently bound validator will cause a fork, so it should be punished (assuming the use of the fork responsible

BFT algorithm, such as Tendermint consensus). It is generally believed that long-range attacks are a key attack on proof of rights.

Fortunately, LRA can be mitigated as follows. First, the verifier must release the guarantee (thereby recovering its mortgage deposit,

And no longer earn the fees for participating in the consensus), the deposit must be transferred within a period of time called the "release guarantee period",

The period can be determined on the order. Weeks or months. Secondly, in order to ensure the safety of light clients, it is the first time

When connecting to the network, the most recent block hash must be verified against a trusted source (preferably multiple sources). This situation

Sometimes called "weak subjectivity." Finally, to stay safe, it must be synchronized with the latest verification assembly, at least

As frequent as the length of the unbundling period. This can ensure that the capital of the lightweight client in the validator is not mortgaged and due to

Know the changes to the validator set before this is no longer in danger,

Note that overcoming LRA in this way requires a thorough inspection of the original security model of the proof-of-work. in

In PoW, it is assumed that the light client can process the proof of work in each block header at any time from the trusted

The genesis block is synchronized to the current height. However, to overcome LRA, we require lightweight clients to go online regularly to track

They must be very careful when they log in for the first time to target trusted sources

The information heard in the network is authenticated. Of course, the latter’s requirements are similar to those of Bitcoin, and the latter’s protocol and soft

The files must also be obtained from trusted sources.

The above method of preventing LRA is very suitable for validators and full nodes of the blockchain driven by Tendermint, because

For these nodes will remain connected to the network. This method is also suitable for light clients who can expect frequent synchronization with the network

end. However, for light clients that are not expected to frequently access the Internet or blockchain network, you can use another

A solution to overcome LRA. Non-validator token holders can use their tokens as collateral for a long solution

Except for the binding period (for example, longer than the validator's unbinding period), release and provide proof for lightweight clients

And the auxiliary method of the past block hash validity. Although these tokens are not included in the security of the blockchain consensus, he

We can still provide a strong guarantee for light passengers. If Ethereum supports historical block hash query, then any

Everyone can bind their tokens to specially designed smart contracts and provide payment proof services, thereby effectively

Create a market for light client LRA security.

Overcome fork and censorship attacks

According to the definition of block submission, any ≥ ⅓ All voting coalitions can suspend the district by going offline or not broadcasting their votes.

Block chain. Such alliances can also review specific transactions by rejecting blocks that include these transactions, although this will lead to

As a result, a large part of block proposals are rejected, which will slow down the block submission speed of the blockchain, thereby reducing its utility and

value. Malicious coalitions may also broadcast votes in a trick stream, so that the promise of blockchain blocks is almost stopped.

Come, or participate in any combination of these attacks. Finally, it may be caused by double signing or violating the locking rules.

To the fork of the blockchain.

If there is also a rival in global activities, it may partition the network in some way so that the error

The subset of validators seems to be the cause of the slowdown. This is not only a limitation of Tendermint, but also

All consensus protocols whose network may be controlled by active opponents are restricted.

For these types of attacks, a subset of validators should be coordinated through external means to sign the choice fork (and its

Any evidence) recombination recommendations, and the initial subset of verifiers with verifier's signature. Sign such reorganization

The proposed validator will give up all other collateral for the fork. The client should verify the signature on the reorganization proposal and verify any

Any evidence, make judgments or prompt end users to make a decision. For example, a phone wallet application might tell users A security warning is issued, and the refrigerator can accept any reorganization proposal signed by the +1/2 original verifier by voting rights.

When ≥1/3 of the voting rights are dishonest, consensus cannot be reached without any asynchronous Byzantine fault-tolerant algorithm, but Fork assumes that ≥1/3 of the voting rights have been dishonestly double-signed or locked for changes. Therefore, sign the reorganization proposal It is a coordination problem. Any non-synchronization protocol cannot solve the coordination problem (that is, it is done automatically, and there is no need to The reliability of the underlying network is assumed). For now, our social consensus on the Internet media will emphasize The problem of group proposal coordination is left to human coordination. Before signing the reorganization proposal, the verifier must take care to ensure that there is no The remaining network is partitioned to avoid the situation of signing two conflicting reorganization proposals.

Assuming that the external coordination medium and protocol are robust, there is no need to worry about forks compared to inspection attacks.

Except for the need ≥ ⅓ Beyond the bifurcation and censorship of Byzantine voting rights,> ⅔ The voting coalition may commit arbitrary Invalid status. This is a characteristic of any (BFT) consensus system. Unlike dual signatures, dual signatures create Forks with easy-to-verify evidence, and submissions that detect invalid states require non-verifying peers to verify the entire Blocks, which means that they keep a local copy of the state and execute each transaction, and independently calculate the state root for themselves. Once discovered, the only way to deal with this failure is through social consensus. For example, in the case of Bitcoin failure In this case, whether it is due to a fork caused by a software error (as in March 2013), or due to Invalid state caused by court actions (such as July 2015), business, developers, and miners are closely connected, Established a social consensus with other organizations on what manual actions participants need to take to heal the network. In addition, due to It can be expected that the validator of the Tendermint blockchain is identifiable, so if necessary, the invalid state The promise of the company may even be punished by law or some external jurisprudence.

ABCI specification

ABCI contains 3 main message types, which are passed from the core to the application. The application responds accordingly Reply to the message.

The AppendTx message is the main force of the application. Every transaction in the blockchain carries this message. Application The sequence requires encrypted credentials for the current state, application protocol, and transaction to verify that it passes AppendTx messaging Every transaction received. Then, the verified transaction needs to bind the value to the key-value store or update UTXO database to update application status.

The CheckTx message is similar to AppendTx, but it is only used to verify the transaction. Tendermint BFT's memory pool First use CheckTx to check the validity of the transaction, and then only relay valid transactions to its peers. If random If the number is older, the application may check the random number incremented in the transaction and return an error on CheckTx.

The Commit message is used to calculate the cryptographic commitment to the current application state and put it in the next block header in. This has some convenient properties. The inconsistency of the update status will now appear in the form of a blockchain fork, This will catch a whole class of programming errors. This also simplifies the development of a secure lightweight client because it can pass inspections The block hash is used to verify the Merkle hash proof, and the block hash is signed by a quorum of verifiers (by voting Vote).

Other ABCI messages allow the application to track and change the validator set, and allow the application to receive block information, for example Such as height and number of votes submitted.

ABCI request/response are simple Protobuf messages. Check out Architecture file .

appendix

- **parameter** :
  - Data ([]byte): Request transaction byte
- **return value** :
  - Code (uint32): Response code
  - Data ([]byte): result byte (if any)
  - Log (string): debug or error message
- **usage** :

Append and run the transaction. If the transaction is valid, CodeType.OK is returned

CheckTx

- **parameter** :
  - Data ([]byte): Request transaction byte
- **return value** :
  - Code (uint32): Response code
  - Data ([]byte): result byte (if any)
  - Log (string): debug or error message
- **usage** :

Verify the transaction. This message should not change the state. The transaction is first run through CheckTx, and then broadcast to the memory pool

The peer node in the layer. You can make CheckTx semi-state and clear the state on Commit or

BeginBlock to allow related transaction processing in the same block.

crime

- **return value** :
- Data ([]byte): Merkle root hash
- Log (string): debug or error message
- **usage** :

Returns the Merkle root hash of the application state.

ask

- **parameter** :
- Data ([]byte): Query request byte
- **return value** :
- Code (uint32): Response code
- Data ([]byte): query response byte
- Log (string): debug or error message

rinse

- **usage** :

Refresh the response queue. The implemented application types.Application does not need to implement this message-it is determined by the project

Rationale.

information

- **return value** :

- Data ([]byte): Information byte
- **usage** :

Returns information about the state of the application. Specific to the application.

Setting Options

- **parameter** :
- Key (string): Set the key
- Value (string): The value to be set for the key
- **return value** :
- Log (string): debug or error message
- **usage** :

Set application options. For example, Key="mode", value="mempool" (used for memory pool connection),

Or Key="mode", value="consensus" (for consensus connection). Other options are application-specific

Ordered.

Initialization chain

- **parameter** :
- Validators ([]Validator): the original founding validator
- **usage** :

Called when self-generating

BeginBlock

- **parameter** :
    - Height (uint64): the height of the starting block
- **usage** :

Indicates the beginning of a new block. Called before any AppendTx.

End block

- **parameter** :
    - Height (uint64): the height of the ending block
- **return value** :
    - Validators ([]Validator): Changed validators with new voting rights (delete 0)
- **usage** :

Indicates the end of the block. After all transactions, call before each commit

For more details, see ABCI repository .

IBC packet transmission confirmation

There are many reasons why the sender may want the receiving chain to confirm the sending of the packet. For example, if it is expected that there is a problem with the sending ch

The sender may not know the status of the destination chain. Or, the sender may wish to

MaxHeight data packet field) imposes a timeout, and any target chain may suffer a denial of service attack, the number of incoming

The number of data packets has suddenly increased.

In these cases, the sender can request delivery confirmation by setting the initial packet state to

AckPending. Then, the receiving chain is responsible for including the contraction in the Merkle hash of the application through IBCPacket.

Write to confirm delivery.

First, post an IBCBlockCommit and IBCPacketTx on the "Hub" to prove the existence

IBCPacket "Zone1". Say IBCPacketTx has the following values:

- FromChainID: "Zone1"
- FromBlockHeight: 100 (say)
- Packet: An IBCPacket:
  - Header: an IBCPacketHeader:
    - SrcChainID: "Zone1"
    - DstChainID: "Zone2"
    - Number: 200 (say)
    - Status: AckPending
    - Type: "Coin"
    - MaxHeight: 350 (for example, the "hub" is currently at a height of 300)
  - Payload: <bytes of "coin" payload>

Next, post an IBCBlockCommit and IBCPacketTx on "Zone2" to prove the existence

IBCPacket "Hub". Say IBCPacketTx has the following values:

- FromChainID: "Center"
- FromBlockHeight: 300
- Packet: An IBCPacket:
    - Header: an IBCPacketHeader:
        - SrcChainID: "Zone1"
        - DstChainID: "Zone2"
        - Number: 200
        - Status: AckPending
        - Type: "Coin"
        - MaxHeight: 350
    - Payload: <same bytes of "coin" payload>

Next, "Zone2" must include the abbreviated packet AckSent of the displayed new state in its application hash. One

IBCBlockCommit and IBCPacketTx are posted back in the "hub" that proves the abbreviation exists

"Zone 2" of IBCPacket. Say IBCPacketTx has the following values:

- FromChainID: "Zone2"
- FromBlockHeight: 400 (say)
- Packet: An IBCPacket:
    - Header: an IBCPacketHeader:
        - SrcChainID: "Zone1"
        - DstChainID: "Zone2"

- Number: 200
- Status: AckSent
- Type: "Coin"
- MaxHeight: 350
- PayloadHash: <hash bytes of the same "coin" payload>

Finally, the "hub" must update the status of the packet from AckPending to AckReceived. This new most

The evidence of the final status should be returned to "Zone 2". Say IBCPacketTx has the following values:

- FromChainID: "Center"
- FromBlockHeight: 301
- Packet: An IBCPacket:

- Header: an IBCPacketHeader:
- SrcChainID: "Zone1"
- DstChainID: "Zone2"
- Number: 200
- Status: AckReceived
- Type: "Coin"
- MaxHeight: 350
- PayloadHash: <hash bytes of the same "coin" payload>

At the same time, unless there is evidence to the contrary on the "hub", "Zone1" may optimistically assume that the "coin" package has succeeded

deliver. In the example above, if AckSent has not received the "hub" from "Zone2" in box 350

Status, it will automatically set the status to Timeout. Evidence of timeout can be sent back to "Zone1", and

Any token can be returned.

Merkel tree and proof specification

The Tendermint / Cosmos ecosystem supports two types of Merkle trees: "simple trees" and IAVL+ trees.

Simple tree

Simple trees are Merkle trees for static lists of elements. If the number of terms is not a power of 2, some leaves will be in

Different levels. The "simple tree" tries to keep both sides of the tree the same height, but the left side may be one size larger. The

The Merkle tree is used to Merkle the transaction of the block, and the top element status of the application is root.

```
            *
           / \
         /     \
       /         \
     /             \
    *               *
   / \             / \
  /   \           /   \
 /     \         /     \
*       *       *       h6
```

```
  / \        / \        / \

h0 h1 h2 h3 h4 h5
```

A SimpleTree with 7 elements

IAVL + tree

The purpose of the IAVL+ data structure is to provide persistent storage for key-value pairs in the application state so that it can be efficiently

Calculate the deterministic Merkle root hash. use AVL algorithm Variant to balance the tree, and all operations are O

(Log(n)).

In an AVL tree, the height of the two subtrees of any node differs by at most one. Whenever this condition is violated during update,

It rebalances the tree by creating O(log(n)) new nodes (unmodified nodes that point to the old tree). In the original

In the original AVL algorithm, internal nodes can also store key-value pairs. AVL + algorithm (please note the plus sign) modified

AVL algorithm to keep all the values on the leaf nodes and only use the branch nodes to store the keys. This simplifies the algorithm,

At the same time keep the merkle hash trace short.

AVL+ tree is similar to Ethereum Patricia try . Need to weigh. The key does not need to be inserted into the IAVL+ tree

Is hashed before, so this can provide faster ordered iterations in the key space, which may make some applications

The program benefits. The logic is easier to implement, requiring only two types of nodes-internal nodes and leaf nodes. Merkle card

Ming is shorter on average, and it is a balanced binary tree. On the other hand, the Merkle root of the IAVL + tree depends on the update

order.

When binary variants are available, we will support other efficient Merkle trees, such as Ethereum's Patricia Trie.

Transaction Type

In the implementation of the specification, transactions are streamed to the Cosmos hub application through the ABCI interface.

The Universe Center will accept some major transaction types, including SendTx, BondTx, UnbondTx, ReportHackTx, SlashTx, BurnCSNTx, ProposalCreateTx, and ProposalVoteTx,

This is fairly self-explanatory and will be documented in a future version of this article. Here, we have recorded two types of IBC Main transaction types: IBCBlockCommitTx and IBCPacketTx.

IBCBlockCommitTx

The composition of an IBCBlockCommitTx transaction is as follows:

- ChainID (string): The ID of the blockchain
- BlockHash ([]byte): Block hash bytes, including the Merkle root of app hash
- BlockPartsHeader (PartSetHeader): The header byte set in the block part, which is only used to verify the Ticket signature
- BlockHeight (int): submitted height
- BlockRound (int): submission round
- Commit ([]Vote):> ⅔ Precommit constitutes a Tendermint vote for an overall commitment
- ValidatorsHash ([]byte): Merkle tree root hash of the new validator assembly
- ValidatorsHashProof (SimpleProof): A SimpleTree has Merkle-proof, To prove that ValidatorsHash vs. BlockHash
- AppHash ([]byte): IAVLTree Merkle-tree root hash of the application state
- AppHashProof (SimpleProof): A SimpleTree has a Merkle-proof to prove Ming AppHash vs. BlockHash

IBCPacketTx

AnIBCPacket consists of the following:

- Header (IBCPacketHeader): data packet header
- Payload ([]byte): The byte of the payload of the data packet. *Optional*
- PayloadHash ([]byte): The hash value of the packet bytes. *Optional*

Either Payload or PayloadHash must exist. The hash of IBCPacket is a simple meck of two items

Ergen, Header and Payload. An incomplete payload of an IBCPacket is called *Short shrink package* .

AnIBCPacketHeader consists of the following:

- SrcChainID (string): source blockchain ID
- DstChainID (string): target blockchain ID
- Number (int): the unique number of all packets
- Status (enum): Can be an AckPending, AckSent, AckReceived, NoAck,

Or Timeout

- Type (string): The type depends on the application. Cosmos reserves the "coin" packet type
- MaxHeight (int): If the status is not NoAckWanted or AckReceived reaches this height,

The status will change to Timeout. *Optional*

The composition of an IBCPacketTx transaction is as follows:

- FromChainID (string): The ID of the blockchain that provided this packet; not necessarily the source

- FromBlockHeight (int): A block containing the following packages (Merkelized) in the block hash of the source chain

Chain height

- Packet (IBCPacket): A packet of data, its state can be AckPending, AckSent,

AckReceived, NoAck, or Timeout

- PacketProof (IAVLProof): IAVLTree Merkle-proof, used for AppHash in a given

Highly the hash value of the proof packet of the source chain

{Figure X} describes the sequence of sending data packets from "Zone1" to "Zone2" through the "hub". first of all, IBCPacketTx proves to the "hub" that the packet is included in the application state of "Zone1". then, Another person, IBCPacketTx, proves to "Zone2" that the packet is included in the application state of "Hub". During this process, the IBCPacket field is the same: SrcChainID is always "Zone1", and DstChainID It is always "Zone2".

There must be a correct Merkel defense path in PacketProof, as shown below:

IBC/<SrcChainID>/<DstChainID>/<Number>

When "Zone1" wants to send IBCPacket packets to "Zone2" through the "Hub", no matter if the packet is In "Zone1", "Hub" or "Zone2" Merkelized, the data is the same. The only variable word Segment Status is used to track delivery.

CSN secure network application

1 Overview

CSN safety network is a brand new application based on COSMOS technology. It can be cleared from the above COSMOS technical documents

It is clear that COSMOS technology has good cross-chain transaction characteristics, which is a

Unity, consistency, and convenience point the way.

BABY EX Fund is Singapore's first and the world's first financial company to set foot in virtual currency asset management. BABY

EX Fund provides investors with a series of professional virtual currency asset allocation, management, asset appreciation, capital operation, etc.

Financial management services. In all financial activities undertaken by the BABY EX Fund, 80% of the profits come from various virtual

Fast and frequent exchange between currencies in a short period of time (a financial activity similar to foreign exchange business, through

Buy or sell at the unstable price of exchange between virtual currencies in order to make a profit at the difference between buying and selling).

At present, the CSN security network is completely independently developed by BABY EX Fund Company, as a non-public fund of BABY EX Fund.

Open, fully self-operated project, mainly to meet the synchronization record of different virtual currency transactions of BABY EX Fund, and guarantee

It is safe and cannot be tampered with.

2. The advanced nature of CSN security network

The "Impossible Triangle" in the Blockchain

Decentralization, security, and high performance constitute the "impossible triangle" of the blockchain. The three characteristics cannot be combined in the design.

When reached, only two of them can be met.

Decentralization means having a large number of nodes involved in block production and verification. Generally, the greater the number of nodes, the decentralization process

The higher the degree.

Security is the cost of gaining network control. It is usually anchored in the design of the consensus mechanism.

Assets, such as proof-of-work (PoW), are anchored in computing power.

Transaction performance is the number of transactions processed per second (TPS). The main reason for the low performance of the blockchain is that each transaction

The transaction must be agreed on all nodes.

The mainstream blockchains Bitcoin, Ethereum, and EOS all compromised on a certain feature of the "Impossible Triangle".

Bitcoin, as a decentralized digital currency, sacrifices performance characteristics and satisfies the requirements of decentralization and security.

Calculated demand. At present, the cost of attacking Bitcoin is the highest among all PoW public chains. With ASIC miners since

The updating of the body and the continuous addition of new mining machines can continuously improve the computing power of the entire network.

Ethereum 2.0 will adopt a Proof of Stake (PoS) consensus mechanism. On the Ethereum network, not only can you transfer money, but also

Smart contracts can be run, and the application scenarios are more complicated, but the current performance of Ethereum is low and congestion is more likely to occur.

EOS, as a blockchain application platform, is often accused of being centralized by the outside world. EOS uses agency rights

Proof of Benefit (DPoS) consensus mechanism, 21 super nodes are responsible for accounting and block generation. Now the EOS mainnet TPS is the most

It can reach more than four thousand. Because the number of nodes is small, the "decentralization" of the three major public chains is most likely to be

The world questioned.

Facing the Impossible Triangle, the CSN Security Network successfully solved the “trilemma” problem through a roundabout way.

1) When a virtual currency transaction is initiated on the CSN secure network, regardless of whether the transaction is a different account in the same currency,

In the case of different currencies on the same network, different currencies on different networks, etc., the CSN security network always first broadcasts to all nodes.

The 10 nodes with the highest accounting authority in the entire network record transaction information first.

2) In a cycle, the record node will automatically check whether the transaction has been recorded on other mainnets, that is, check

Whether the transaction is complete.

If the transaction has been successfully queried on other mainnets, it will be recorded once and all 10 priority recording nodes will be completed

After recording, broadcast on the whole network and record synchronously.

If the transaction fails to be successfully queried on other mainnets, the query cycle will be extended, and the transaction will still be less than

If half of the successful records are recorded, the transaction is declared unsuccessful, the transaction is rolled back, and the transaction is deleted.

3) Each accounting node can only queue up to process 3 records to be confirmed at the same time, when the node queue with high accounting authority node

When the queue is full, among the remaining nodes, the one with higher accounting authority will give priority to record and verify.

4) If a node initiates multiple transactions in a row, but fails to be recorded successfully, the node is judged to be a lying node and restricted Its authority to initiate transactions or record.

The asynchronous recording method of the CSN secure network can first determine that the transaction is successful at the moment the transaction is initiated, and To query on the CSN secure network. After the transaction is actually completed on other mainnets, it will be recorded on the entire network. Record to ensure data security. At the same time, it satisfies transaction efficiency and security, and the more nodes there are, the wait can be supported The more verification data, the transaction speed will not be affected at all.

3. CSN Security Network Development Plan

The BABY EX Fund currently manages a total of 100,000 BTC in various virtual currency assets, and the trading department balances every minute. Both will initiate 6 buy or sell orders. If you use the traditional way to trade, you need to spend several times Time is used to wait for transaction confirmation. This seriously affected the transaction efficiency of the trading department. Therefore, the BABY EX Fund launched the CSN secure network project. In internal testing, the CSN security network In addition to providing faster transaction speeds, it can also command automatic transactions with multiple accounts at the same time in the form of instructions. For virtual assets For property management users, the detailed description of each transaction can be clearly inquired from the account backend, so that investment customers can more Plus rest assured. Instead of concentrating all the virtual currency that needs to be traded in a few accounts, it is not similar to the traditional transaction method. In the account, once there is a problem with this account, it will be a devastating blow.

In order to achieve the ultimate decentralization of the CSN safety network, BABY EX opens up the safety network construction work for the public. With the current volume of BABY EX Fund’s own business, 100,000 basic nodes are needed to ensure the security of the CSN network Completely decentralized. With the increase in the number of basic nodes, the BABY EX fund will gradually shift from traditional trading methods to Move to the trading network based on the CSN security network until all businesses are successfully transferred to the network.

In the next step, BABY EX Fund will open the CSN secure network platform, allowing other financial companies or fund companies to use

Use the CSN secure network for virtual currency transactions. If everything goes well, the CSN security network will become a comprehensive

The world's first non-matching cross-chain trading platform.