Super diamond

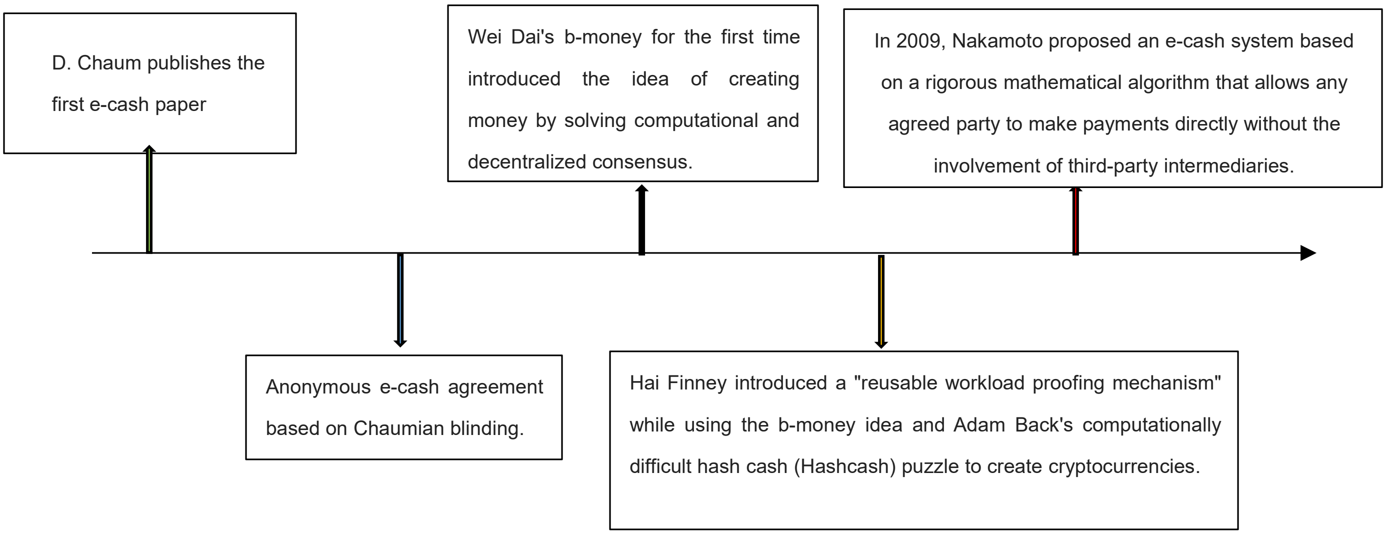
Value Transmission Protocol and Decentralization Platform.

Table of Contents.

Super diamond Design principles and concepts.

1.1 Background and significance of the block-chain technology

Since the publication of the first thesis on e-cash by D. Chaum in 1983, research on e-cash has not ceased until the publication of a white book entitled "A New E-Cash System" by Nakamoto in 2008, in an open source Of the block-chain on the run bitcoin block-chain into everyone's field of vision.



D. Chaum publishes the first e-cash paper

Anonymous e-cash agreement based on Chaumian blinding.

Wei Dai's b-money for the first time introduced the idea of creating money by solving computational and decentralized consensus.

Hai Finney introduced a "reusable workload proofing mechanism" while using the b-money idea and Adam Back's computationally difficult hash cash (Hashcash) puzzle to create cryptocurrencies.

In 2009, Nakamoto proposed an e-cash system based on a rigorous mathematical algorithm that allows any agreed party to make payments directly without the involvement of third-party intermediaries.

On January 3, 2009, the founding block of Bitcoin was excavated and the first Bitcoin transaction took place in Block 170 (from Satoshi to Hal Finney, January 12, 2009), Opened the bitcoin network as a booming era of peer-to-peer value exchange networks, and despite the various crises faced along the way, in terms of value, bitcoin started from scratch and made it’s way from the ground up to where it is today and has now reached around $ 10 billion Peer-to-peer payment network.

In the Internet protocol stack, we use more TCP / IP, HTTP, HTTPS, FTP, TELNET, SSH, SMTP, POP3 and other network layer, transport layer, application layer protocol, and with these protocols, we’ve basically perfected putting together a wide range of Internet services. However, if we take into consideration that before the emergence of bitcoin, we will find that we have not been able to access the Internet for the better transfer and transmission of peer-to-peer values without the aid of third parties. In fact, we are not short of a particular method, but we lack the Value Super Highway based on the Information Super Highway and the Value Transfer Protocol (VTP) on how to implement the Value Super Highway. Instead, the currency network is the first VTP protocol running on the information superhighway.With the development of interoperability technology (Internet, Internet of Things, VR / AR), people and objects, people and information interaction methods became more diverse, and more entities are digitized and symbolized. Once an entity after being digitized or symbolized, the physical assets are interconnected online mapping and segmentation, one of the problems is immediately facing: how to transfer these assets and value point to point?

1.2 Why design super diamond

Since the Bitcoin code was released in 2009, there have been many projects in the community that expand the technology boundaries of block-chain from different perspectives such as ColorCoin, NXTCoin, Ripple and Stellar, BitShare, Dash, Maidsafe, Factom and others. Later, there was also the Ethereum project dedicated to becoming a common smart contract platform and a decentralized application platform. However, the block-chain industry faces many challenges both from a technical point of view and from an industrial application point of view.

Super diamond hopes to build a brand-new block-chain ecosystem, integrate multi-sector block-chain applications and establish a block-chain ledger jointly maintained by all parties. This will not only enable information sharing, but also provide a Link identification and write the key information, thereby enhancing the tracking and traceability of the entire link, reducing the regulatory difficulty. Broadening the application boundaries and technology boundaries of block-chain technology enables ordinary Internet users to feel the value of block-chain technology and build a new ecosystem of developers and users based on block-chain technology.

1.3 Block-chain technology is facing the main problems

1.3.1 lack of new smart contract platform

Currently, the existing smart contract platform is mainly based on Proof of Work (POW) 2, while the consensus mechanism of Proof of Work (POW) is hard to be deployed on a large scale by industry.

- **1.3.2 Compatibility**

For example, based on the UTXO model of Bitcoin Ecology and Account model-based Ethereum Ecology is difficult to have compatibility.

- **1.3.3 Flexibility**

Because of the different actors, the requirements for the consensus mechanism are different in the public chain and in the coalition chain.

- **1.3.4 Compliance**

For example, the identity and KYC components required in the financial industry are hard to guarantee in the existing block-chain system.

- **1.3.5 Closed**

At present, most of the trigger conditions for smart contracts mostly come from the block-chain system itself, with few external triggering conditions and lack of interaction with the real world.

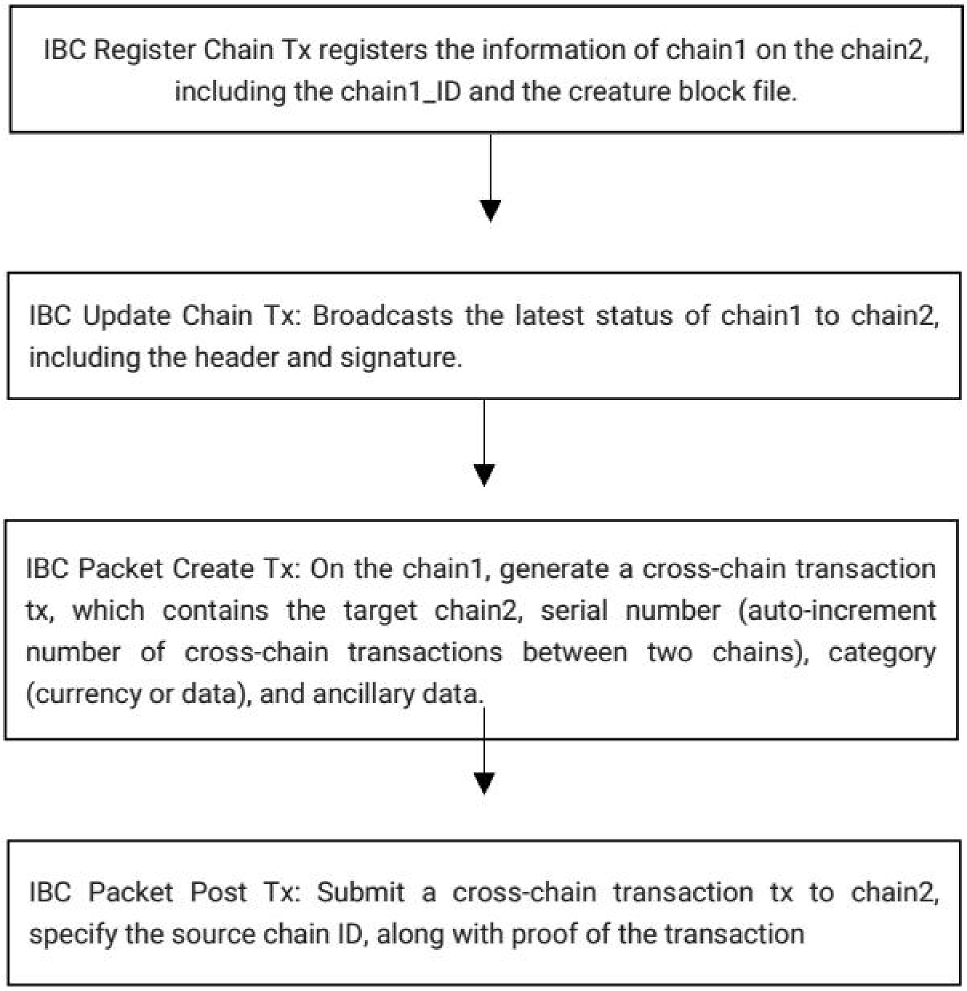
Super diamond to achieve the program

The Super Diamond is based on the Cosmos infrastructure. Cosmos is a new block-chain network infrastructure consisting of many modules, Cosmos Hub, Transit Bridge, Ethermint and others.

2.1 cross-link technology

The unique cross-link technology provides the basis for networked and multi-link interactions. Through the inter-link plug-in IBC (Inter-Block-chain Communication), to achieve two block chain mutual verification of cross-link data.

For example, chain1 and chain2, how to send data from chain1 to chain2.



IBC Register Chain Tx registers the information of chain1 on the chain2, including the chain1_ID and the creature block file.

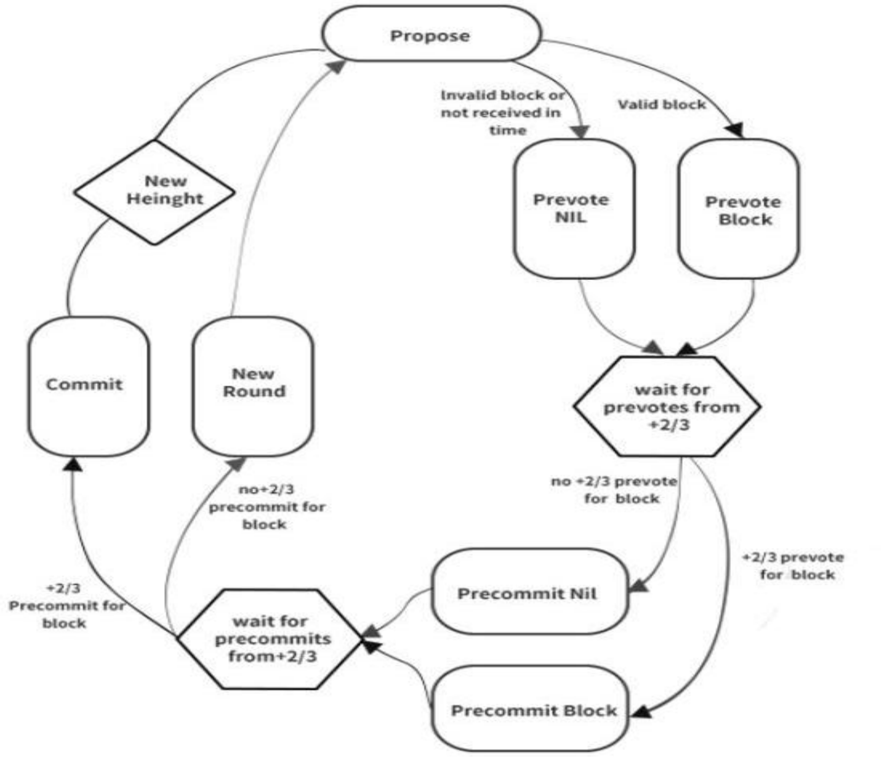
IBC Update Chain Tx: Broadcasts the latest status of chain1 to chain2, including the header and signature.

IBC Packet Create Tx: On the chain1, generate a cross-chain transaction tx, which contains the target chain2, serial number (auto-increment number of cross-chain transactions between two chains), category (currency or data), and ancillary data.

IBC Packet Post Tx: Submit a cross-chain transaction tx to chain2, specify the source chain ID, along with proof of the transaction

2.2 Consensus mechanism

Tendermint-dpos consensus for super diamonds, tendermint It is a consensus algorithm based on BFT, tendermint consensus algorithm is different from POW or POS mining, by a number of witnesses each have the right to vote, turns out the block, and then verify the people and each Vote for more than two-thirds of the vote, you can think of the block to reach a consensus and achieve final certainty, and will not be forked rollback.


Propose
Invalid block or not received in time
Valid block
New Heinght
Prevote NIL
Prevote Block
Commit
New Round
wait for prevotes from +2/3
no +2/3 prevote for block
+2/3 prevote for block
no+2/3 precommit for block
+2/3 Precommit for block
Precommit Nil
wait for precommits from+2/3
Precommit Block

Agreement to follow the rules:
The participants in the agreement called the "validator." They take turns to propose deals and vote on these blocks. Blocks will be submitted to the chain, each block occupying a "height". Submitting a block may fail, and if it fails, the protocol will begin the next round of submission, and a new verifier will continue to submit that high block. To successfully submit a block requires two stages of voting: "pre-vote" and "pre-commit". In the same round during the submission period, only more than two-thirds of the validators can pre-commit of the same block, the block can be submitted to the chain.

When more than two-thirds of the validators pre-vote on the same block, we call it a polka. Each pre-submission must be evidenced by a Pocar in the same round. For some reason, the verifier may fail to submit a block: the current proposer may be offline, or the network is slow. Tendermint allows them to confirm that a validator should be skipped. Before proceeding with the next ballot, the verifier will wait for a short period of time to receive a complete proposal block from the proposer. This dependency on timeouts makes Tendermint a weak synchronization protocol, not an asynchronous protocol. However, the rest of the protocol is asynchronous, and the verifier takes the next step only when it receives more than two-thirds of the set of validators. One reason Tendermint can be simplified is that it uses the same mechanism to submit a block and skip to the next round.

Based on the assumption that less than a third of the witnesses are byzantine nodes, Tendermint pledges that it will never violate its security - that is, the verifier will never submit conflicting blocks at the same height. To do this, it introduced some "locking" rules that modularized the path in the flowchart. Once a validator pre-submits a block, it is "locked in" on that block.

It must then vote for the block that is locked. Only in the following round, with a card in that block, can it be unlocked and pre-submit for a new block.

The Tendermint Consensus itself is a Consensus node with the same weight. In order to adapt to the Cosmos architecture of the public chain, Tendermint-dpos Consensus is derived from Tendermint-dpos Consensus, with user authorization, witness vote weight, witness penalty logic and inflation logic.

The Tendermint Byzantine consensus algorithm for fault tolerance is well suited to extending the common block-chain under the Proof of Entitlement.

The tendermint framework integrates the go version of the Contentious Convergence Algorithm in narrow sense with the basic functions of block data structure, p2p network, block and state data storage. It is a pure and functional block-chain system. Users can expand their applications through ABCI (Application Block-chain Interface) so that the block-chain itself is decoupled from the application.

2.3 trading model

Super diamond uses the total account balance model but contains multiple assets instead of the non-total balance model for bitcoin UTXO. The account address is the ripemd160 hash of the public key, and the status tree uses the IAVL tree. Of which:
The general transfer transaction for sendTx structure [Gas, Fee, Input list, Output list]

Input structure [user address, token list, serial number, signature, public key]

Output structure for the [address, token list]

The first time a user's address appears (serial number is 0), a public key needs to be declared because tendermint can not overwrite the public key from the signature, as Bitcoin or Ethereum did. Gas limits the available quota for the transaction (similar to Ethereum's gaslimit) and Fee is the fee to be paid. There is no direct statement of the gasprice concept (implied as Fee / Gas). The format of this transaction allows multiple assets of multiple accounts to be completed in the same transaction.

Instance counter installed as a sample plug-in, as a client, can be used to query the total number of transactions. Plugin can support any function, is to achieve the plugin interface go language package. The plug-in updates the status of basecoin and stores any data, and the plugin's data is stored in the Merkel tree via the KV structure.

2.4 address format

Super diamond design will introduce BIP32, BIP43, BIP441 concept Hierarchical Deterministic Wallets (or "HD Wallets") provides support for multi-currency, multi-account, multi-address, multi-key.

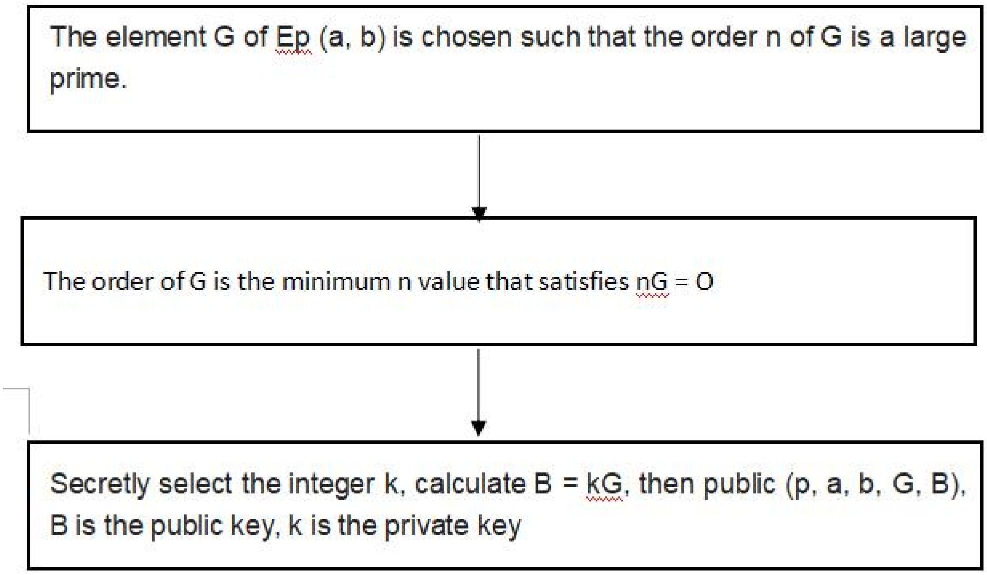
BIP44 provides a five-layer path proposal: (1) to determine the path rules; (2) currency; (3) accounts; (4) change; (5) address index. Users only need to save a master private key, you can control all currencies, all accounts of the wallet. BIP44 provides good support for the change mechanism. Users can avoid multiple exposures of the private key by avoiding multiple signings of the same private key as long as they do not collect multiple payments at the same address.

2.5 encryption algorithm

Super diamonds involve private keys, public keys, and address systems in the control and operation of assets. Traditional bitcoin code implementations encrypt ECDSA and SHA256 hashes based on elliptic curve functions.

Super diamond will further support the national compact SM2 and SM3. In achieving the same computational complexity, SM2 in the private key processing speed is much faster than RSA, DSA algorithm, the encryption efficiency is higher. The compression function of the SM3 algorithm has a similar structure to the compression function of SHA-2561 ·, but the design of the SM3 algorithm is more complicated. For example, each round of the compression function uses two message words.

SM2 algorithm released by the State Password Authority on December 17, 2010, the full name of the elliptic curve algorithm. Elliptic curves are not ellipses, they are called elliptic curves because they are represented by cubic equations and the equation is similar to the equation for calculating the circumference of the ellipse. In general, the cubic equation of an elliptic curve is:
$y2 + axy + by = x3 + cx2 + dx + e$ [where a, b, c, d and e are real numbers that satisfy certain conditions because the exponents in the equation are the highest Is 3, so we call it a cubic equation, or the number of equations is 3]
The equation used by the SM2 algorithm is: $y2 = x3 + ax + b$
The SM2 algorithm is implemented as follows:



The element G of Ep (a, b) is chosen such that the order n of G is a large prime.

The order of G is the minimum n value that satisfies nG = O

Secretly select the integer k, calculate B = kG, then public (p, a, b, G, B), B is the public key, k is the private key

Encryption M: The message M is first transformed into a point Pm in Ep (a, b), and then the random number r is selected to calculate the ciphertext Cm = {rG, Pm + rP). If r makes rG or rP O To reselect r Decryption Cm: (Pm + rP) -k (rG) = Pm + rkG-krG = Pm.

The security of the SM2 algorithm is based on the realization of a mathematical problem called "discrete logarithm problem ECDLP" that considers the equation Q = KP where Q and P belong to Ep (a, b) and K <p, then 1) p = "" Given q and p, calculating k is difficult.

SM3 password digest algorithm is China National Cryptographic Authority released in 2010 China commercial cryptographic hash algorithm standard. The SM3 algorithm is suitable for digital signature and verification in commercial cryptographic applications and is an improved algorithm based on SHA-256. SM3 algorithm adopts Merkle-Damgard structure, the message packet length is 512 bits, and the digest value length is 256 bits.

The compression function of the SM3 algorithm has a similar structure as the compression function of the SHA-256, but the design of the SM3 algorithm is more complicated. For example, each round of the compression function uses two message words.

Compared with the development path of Internet technology, we find that both the block-chain technology and the application of block-chain technology are in the early stage of industry development, and there are many worth exploring. Take the ease of use of the entire block-chain industry one step further, which is why we design super diamonds.

Super diamond project composition.

3.1 Information Super diamond – Block-chain browser

The block-chain browser is the main window for viewing block-chain information, and the content of each block can be viewed from the block-chain browser.

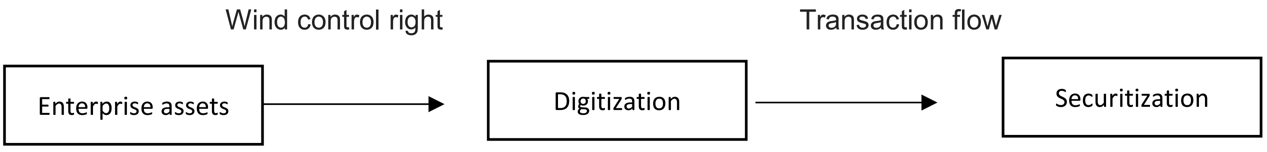
We use the Inter Planetary File System interstellar file system, or IPFS for short, to be a permanent, decentralized way to save and share files, a distributed protocol for content addressability, versioning, and point-to-point hypermedia. Set of distributed hash table, BitTorrent, Git, self-certified file system advantages in one.

A unique hash value is generated from the file contents to identify the file,not from the file save location. The same content of the file in the system will only exist one, saving storage space, and can trace the history of file modification. P2P holds all kinds of data and is a fine-grained, distributed and easy-to-combine content delivery network (CDN). Useful for all data types, including images, video streaming, distributed databases, operating systems, block-chains, and more.
IPFS can replace HTTP that always gets content from the data center. For example, getting a video can be downloaded entirely on the IPFS network without requiring the Internet to undergo heavy transmission over the backbone. Greatly reduce the cost of data transmission, user-friendly file access, saving network resources.

3.2 Channel Super Diamonds - Digital digitization of physical enterprise assets

3.2.1 entity corporate asset distribution

Real-world real assets owned by a business entity are converted into smart non-monetary assets in the form of electronic data that are held in the ordinary course of business to be sold or are in production through smart contracts. Issuance of coupons or points online, the company will be the distribution of equity assets in the form of digital, are the form of digital assets.
Super diamonds can digitize enterprise assets such as corporate assets ABS and ABS (securitization), digitize corporate assets through wind control (registration) and transaction (transfer), endorse the real assets and cooperate with the trustworthiness of the block-chain to ensure that The value of digital asset stability.



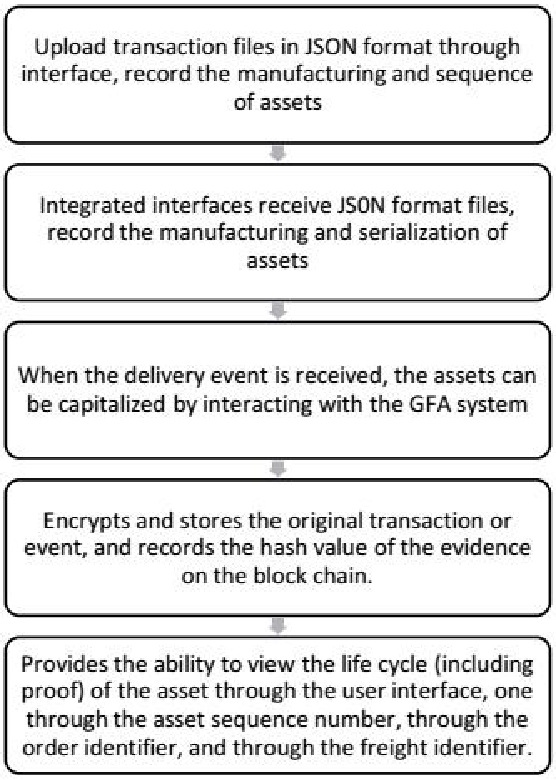
Both the value of the physical assets of the storage function, but also has all the digital assets have universal advantages, and huge liquidity advantage.

3.2.2 Solid enterprise block-chain system implantation

Physical enterprise inventory collection and logistics, hardware tracking, financial management, customer management, embedded block-chain system, to establish a network to coordinate the sharing of one or more books. Realize chain members, members of the chain entities, real businesses docking with each other, the block-chain and real traditional economic life get through, so as to improve the efficiency of economic life and reduce the cost of credit.

By deploying a cross-domain docking solution on the block-chain, the SDK for Node.js client interface accesses the block-chain. All application and user interactions flow through the user interface of the API or it.

The data flowing into and out of the block-chain is in JSON format, which makes the data easy to understand, use, and handle. In MVP, Node.js clients integrate with manufacturing systems using services provided on the block-chain.



Upload transaction files in JSON format through interface, record the manufacturing and sequence of assets

Integrated interfaces receive JSON format files, record the manufacturing and serialization of assets

When the delivery event is received, the assets can be capitalized by interacting with the GFA system

Encrypts and stores the original transaction or event, and records the hash value of the evidence on the block chain.

Provides the ability to view the life cycle (including proof) of the asset through the user interface, one through the asset sequence number, through the order identifier, and through the freight identifier.

Users can call GFA-Micro service and GFA systems for real-time asset capitalization checks. Smart contracts validate events against the current state of the asset and apply Action to verify Signature and support Document, provided that the client has specific Role Access privileges.

3.3 Project Super diamond (Super diamond) - multi-chain interoperability

Cosmos architecture, through the plug-in IBC (Inter Block-chain Communication), to achieve multi-chain verification of cross-chain data exchange between each other.

Cosmos combines high performance and consistency, and under its strict bifurcation responsibility system, prevents malicious parties from improperly operating. The Byzantine consensus algorithm for Tendermint Core is well suited to extending the public block-chain under the Proof of Entitlement.

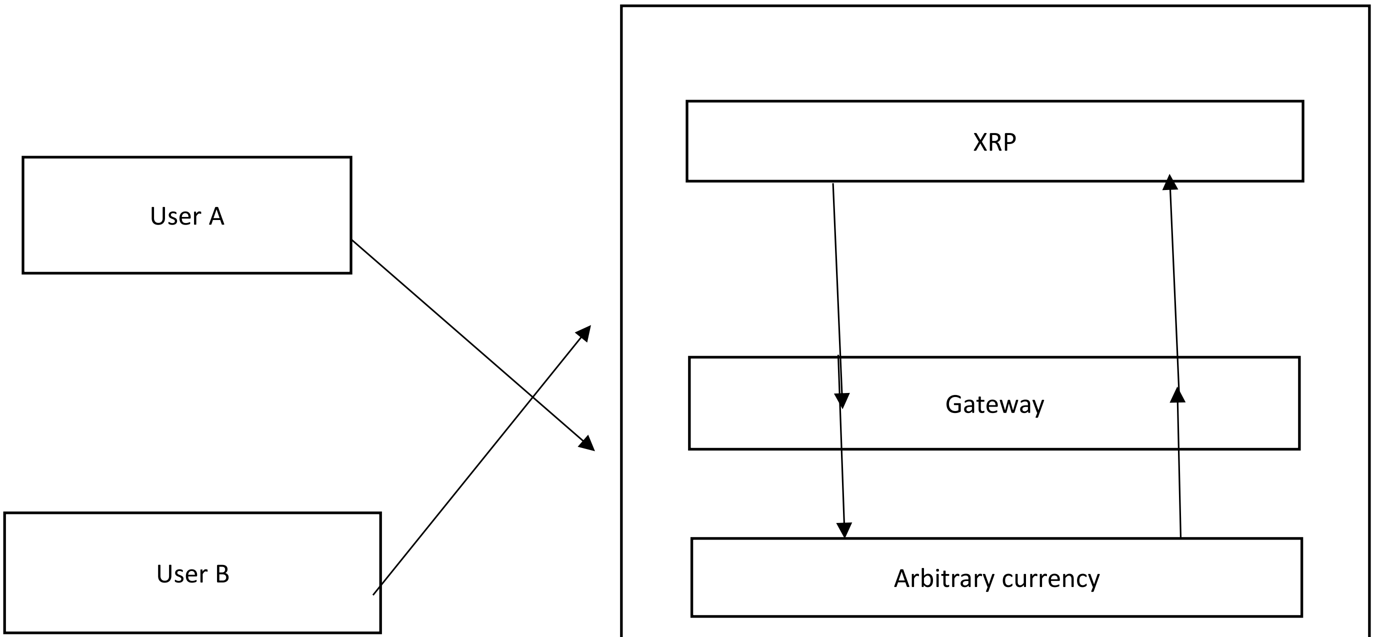
Based on the basic mechanisms of openness, sharing and connection, the basic protocol of cross-chain transaction solves the problem of interoperability between chain and chain, and has the three characteristics of cross-link + privacy protection + smart contract.

Embedded in different areas of the public chain. Linking different block-chains with each other's actual needs to each other and "linking" them into "nets" to enable data flow, business interaction and value interaction between chains and chains to form inter-regional, cross- Block-chain application capital chain community.

3.4 Multi-chain interoperability success stories

2017 Ripple's Inter-ledger agreement (ILP, cross-book protocol) opens the first Bitcoin add-on to help users seamlessly trade in multiple types of books. Ripple conducted live demonstrations with the open-source Bitcoin tool and another plug-in for the enterprise-level platform Chain, enabling the transfer of a single transaction in seven separate books. At the Block-chain Expo in Berlin, Germany, the deal was shifted in public block-chains, private block-chains, centralized ledgers, and traditional payment channels.

The Ripple system is based on the XRPG XRP, and user A converts any currency or virtual currency of any type into Swire XRP and sends it to user B in any other area. User B can convert the received funds into their own needs Of any currency; there is another model, user A will be deposited in the trust of the B gateway, gateway B transferred.



Super diamond advantages and applications

4.1 Decentralized

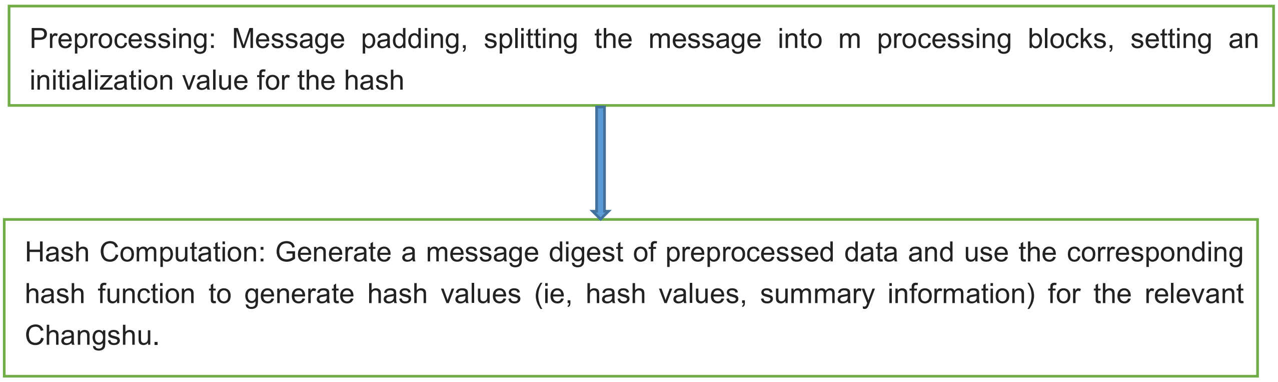
Peer-to-peer (P2P), also known as peer-to-peer networking technology, relies on the computing power and bandwidth of participants in the network. P2P networks are often used to connect nodes through AdHoc connections and are also used in data communications for real-time media services such as VoIP.

Distributed accounting and storage, there is no centralized hardware or management agencies, any node's rights and obligations are equal, the system data blocks by the entire system with maintenance functions of nodes to jointly maintain. Any node to stop working, will not lead to the entire system downtime.

4.2 Information can not be tampered with

Hash algorithm, the information can not be tampered with. Once the information has been validated and added to the block-chain, it is stored forever, with high data stability and reliability.

Hash algorithm is a one-way cryptosystem, only the encryption process, there is no decryption process. Through the hash function iteration, any length of the message input, compressed to generate "Message Digest" (Message Digest).



Preprocessing: Message padding, splitting the message into m processing blocks, setting an initialization value for the hash

Hash Computation: Generate a message digest of preprocessed data and use the corresponding hash function to generate hash values (ie, hash values, summary information) for the relevant Changshu.

Cannot be tampered with two meanings, first, "given a hash result R, there is no way to convert E to the original target text S", the second is "given the hash result R, even if you know a hash of the text S results R, cannot assert that the original target text is S ".

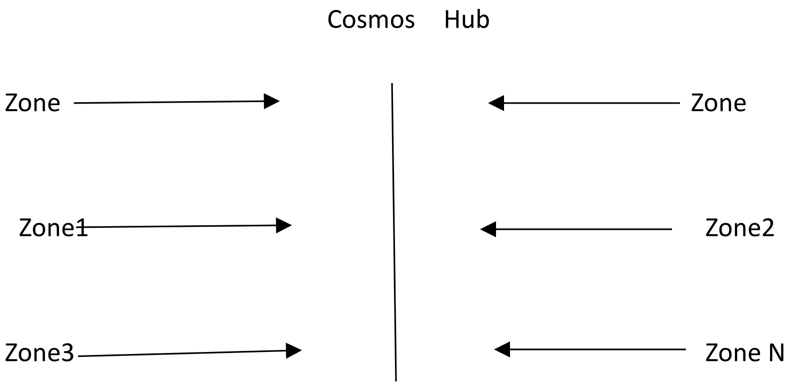
A hashing algorithm is a many-to-one mapping. Given a target text S, H can uniquely map it to R, and R has the same length for all S's. Since there is many-to-one mapping, there is no inverse mapping for H.

4.3 Openness

The system program is open, except for the proprietary information of the parties involved in the transaction is encrypted, the data of the block-chain is open to all and anyone can query the block-chain data through the block-chain browser. Therefore, the entire system information is highly transparent. Within the rules and time frame of the system, nodes cannot deceive each other, so that trust in "people" is changed into trust in the machine. Any human intervention does not work and the credit cost in the transaction is reduced. People new interface and sharing interface.

4.4 upgradeability

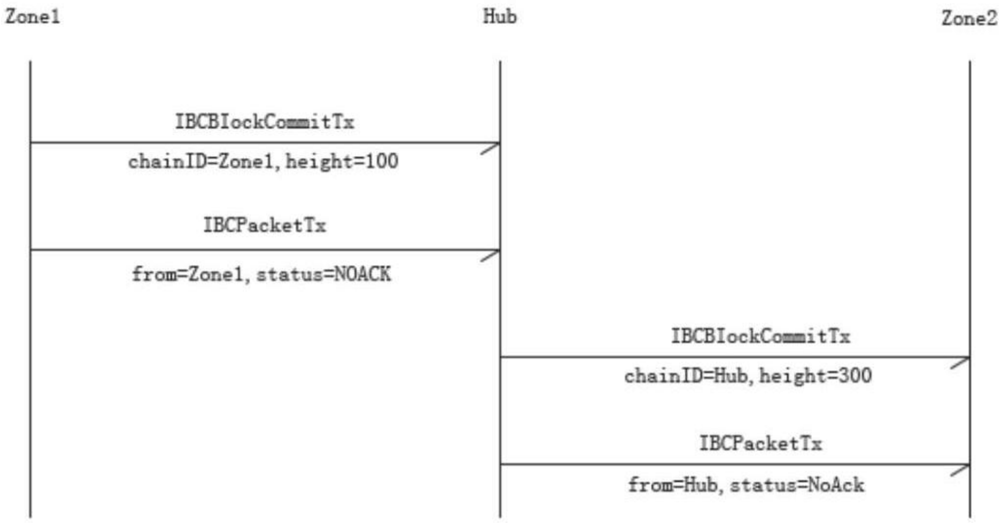
Block-chain how to upgrade. It is hard to get all the certifiers to upgrade to a new version at the same time, which can lead to hard-forking. Ethereum produces ETH and ETC due to hard-forking after DAO is hacked. With Cosmos, upgrading will no longer be a problem. You just have to add a new zone to Cosmos hub and invite users to transfer their information over.



4.5 Interoperability

Cosmo can connect many different forms of assets and applications, and this is a problem that other block-chain cannot solve well. By creating a new zone, you can embed a block-chain system on the Cosmos hub where information can travel freely without intermediaries.

If we now have three block-chains, "zone1", "zone2" and "cosmos Hub", w we want "zone1" to communicate via "cosmos Hub" and "zone2", the IBC mechanism splits into two separate transactions, That IBC Block Commit Tx transactions and IBC Packet Tx transactions.



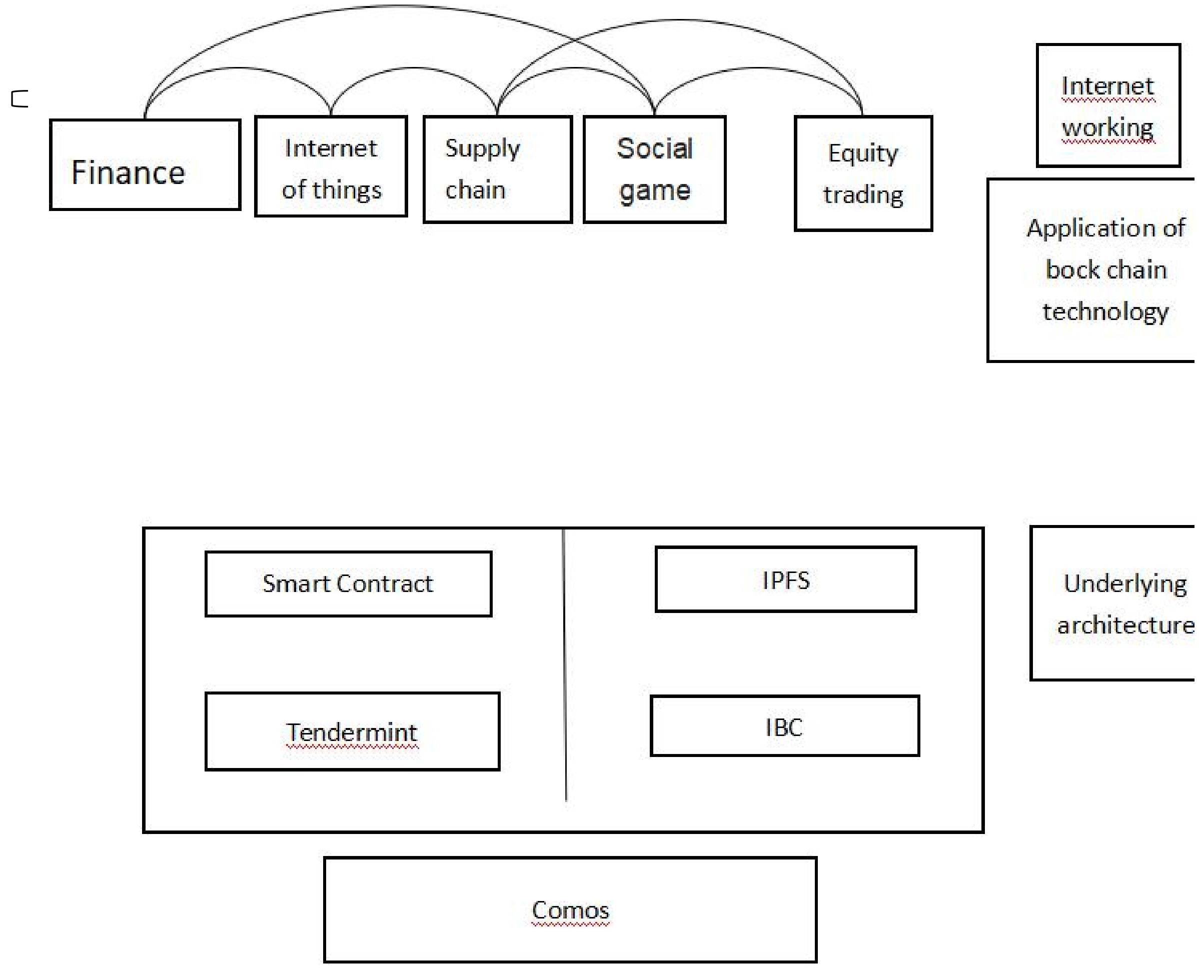
In order to update the block hashes for "zone1" on cosmos Hub (or the block hashes for "cosmos Hub" on "zone2"), the "zone1" block hashes for IBC Block Commit Tx transactions must be posted to the Hub (Or publish the "cosmos Hub" block hash of the transaction to "zone2").

4.6 expandability

Block-chain financial transfer rates are too low (eg, Bitcoin, Ethereum) compared to the everyday payment networks Visa and Mastercard. The Cosmos zone can be unlimited expansion, you only need to add a zone on the hub, so that half of the users can go to another zone above, so you can double the transfer rate. At the same time Cosmos hub to ensure that any one of the zone are synchronized connection.

4.7 multi-industry application support

The Super diamond system, which separates the Consensus Engine from the p2p layer, is implemented as a socket protocol, ABCI (Application Block-chain Interface), that meets the speed and capacity requirements of the block-chain common to multiple applications . Based on the current hyper diamond system, no matter what language, Rust, Go, Haskell, anyone can run an ABCI application using Tendermint consensus. With the introduction of simple contracts based on block-chain technology and Oracle and Data Feeds, it is also possible to introduce more offline factors. Identity and Privacy are designed to meet the regulatory needs of the financial industry.



Can support applications across multiple industries: for example, finance, IoT, supply chain, social and gaming, philanthropy, digital assets and equity. Also based on the ultra-diamond smart contracts and simple contracts, through a complete programming language, you can achieve more complex business logic support, and will support more industries.