****

iWorth White Paper

**微信图片_20210121151943**

**iWorth: Visual Smart Contract Social Application**

**Preface**

Since Satoshi Bento created Bitcoin, the decentralized cryptocurrency in early 2009, the concept of "block chain" has gradually been born in the world. In essence, block chain is a new type of database. Compared with traditional databases, it has the characteristics of security, anonymity and data traceability. If it is a decentralized public chain like bitcoin system, it also has the characteristics of expandability, uniqueness and non-tampering. Because the public chain project involves the problem of "data management role", consensus algorithm is naturally needed as the bottom support, such as common Proof-of-work and Proof-of-Stake. Bitcoin is the first successful application case of decentralized finance. However, with the gradual saturation of projects to solve financial problems through block chain, developers have turned their attention to how to apply block chain technology to other fields besides finance.

Undoubtedly, the most successful case is Ethereum created by Vitalik Buterin in early 2013. Ethereum combines "smart contract" with block chain to create a development environment for developers to publish smart contract. Contract is a database that can be added but cannot be modified or removed in Ethereum network. Ethereum wants to try to solve the problem of social trust through this and achieve the vision of forming a decentralized autonomous organization (DAO). But the public can't understand the architecture and principle of Ethereum, The threshold for issuing contracts is relatively high for the public, so the most extensive application value of Ethereum at present is to lower the threshold for project parties to initiate decentralized financial application projects and semi-financial application projects. For the public, Ethereum is only a relatively abstract and difficult concept to understand. The significance of iWorth lies in lowering and visualizing the threshold of contracts and block chains, inducing users to change their thinking, and relying on timely chat and communication, so that users can easily send a smart contract and view the information on the chain, and use block chains to change production relations, so as to shape users' personal values and rewrite the social credit system.

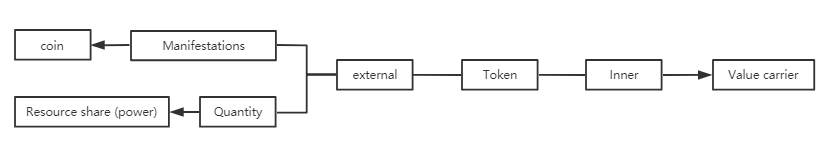
**Catalog**

* **Background**
* "Currency" and "Token"
* "Mining" and "Consensus"
* Smart contract
* Credit
* information internet and Value Internet
* **iWorth**
* Figurative
* Block ID
* Contract Court
* Block Browser
* Extensibility
* **System General Certificate and Economic Model**
* iWorth1.0--Grand Voyage
* iWorth Node--iWorth Node
* iWorth2.0--Stars Plan
* iWorth3.0--Watchman
* **Miscellaneous Concerns**
* **Summary**

**Background**

* "Currency" and "Token"

With the development and application of block chain technology, more and more people come into contact with this concept, and the vast majority of people come into contact with block chain because of "currency". All kinds of Initial Coin Offering (ICO) have been proved to be a feasible financing method for block chain projects. While this approach attempts to open up financing channels for investors outside the sphere of influence of venture capitalists, It also hinders the participation of other audience groups, Moreover, some illegal acts carried out in the name of ICO are gradually increasing, The vast majority of tokens are ERC20 encrypted tokens issued through anonymous Ethernet contracts. Due to their identifiability, circulation and anonymity, they often become speculative tools with a large number of economic bubbles. The sale of these tokens is almost equivalent to fraud, causing public anxiety about block chain related models, projects and technologies.

Block chain and token economy complement each other. Encrypted currency is only a manifestation of pass-through. It seems too one-sided to use the word "token" to represent the booster in the block chain application ecological model to maintain the ecological cycle and push it forward. In the bitcoin system, bitcoin forms a complete ecological closed loop and solves the social problem of no public bookkeeping, so it has use value. Nowadays, most coins do not have internal and applied value carriers to form an ecological closed loop, so they can only be called "coins" and cannot be called general certificates. However, in a real decentralized block chain project, there must be a general certificate to show a right or a value expression. However, the focus of media attention is mainly on the shallow threat of encrypted currency to the financial industry, which has relatively become a resistance to technological innovation in the block chain. The public also does not understand the deep meaning of block chain technology beyond simple transactions and currency investment, which makes the capital disk projects relying on anonymity of block chain flood. We have been looking for a universal value support and appropriate application scenarios to create a low-threshold block chain system that everyone can participate in.

* "Mining" and "Consensus"

"Mining" is a mechanism to compete for data recording rights in a decentralized public chain system. For example, bitcoin system competes for bookkeeping rights through Proof Of Work (POW). In public chain systems, there is also a consensus algorithm for Proof of Stake (POS). Mining is also a process of running consensus algorithms through computers.

Public chain consensus algorithms such as POW and POS all try to achieve a state of "randomly selecting nodes to block, the selection probability is proportional to some verifiable resources of the nodes, and overturning the blocks with the longest chain confirmed needs to master more than 50% of the resources". POW resources refer to workload, and nodes that can provide evidence of certain workload obtain block weight. POS resources refer to pass certificates, and those who provide proof that they own some pass certificates before a certain time obtain the right to block. The pain point of POS is that POS has not been tested in practice, while POW has been proved to be safe in practice. However, the real fact is that POS has not been proved to be unsafe in practice, but POW has exposed a great potential safety hazard in practice-51% attack: in an ideal decentralized block chain system, from the perspective of security, the interests of consensus participants should be consistent with those of the block chain system itself. Therefore, 51% attacks are not feasible, because participants who can dominate the consensus will not be willing to attack this block chain, otherwise they will lose their own interests. In fact, this is true for POS but not for POW. In fact, the interests of miners in the system are far less than the value of the whole system. When the interests of mining and tampering with the conflicts of interests, POW miners are entirely likely to commit malicious acts due to their own interests (such as double payment and data control). Bitcoin is safe, not POW. POW has exposed great potential safety hazards and problems, and POS can solve this problem. Although POS may not be superior to POW in other aspects, this is enough to be the reason why we need POS. However, POS works on the principle of interest binding, which will bring about centralized results in extreme cases. People who do not hold a pass cannot pose a threat to POS. The security of POS depends on the holder and has nothing to do with any other factors. In iWorth, we greatly optimized the POS consensus algorithm, greatly lowered the mining threshold, and gave every user the opportunity to participate in mining and get rewards.

* Credit

At present, there are many problems in the credit system of the whole society, such as the decentralization of trust sources: in the existing scenarios requiring multiple trust information, the process of obtaining and verifying proof materials is long, the cost is high, and the risk of data information leakage is high. However, the non-self-certification of identity also fundamentally limits the establishment of credit systems for various applications. Personal authentication based on a single information management system is difficult to form a comprehensive and comprehensive evaluation of individuals, and it is difficult to accurately know "what kind of me I am" and "what kind of you you are". The difficulty in coordinating community management is also a serious credit system problem. In community management, entrance control is a key point. However, in the Internet era, there is no effective mechanism to effectively review new entrants, which makes it difficult to ensure that the commonness of the community will not decrease with new entrants. Individuals do not have enough voice and transparency in the use and authorization of their own trust data, and lack convenient and low-cost means. With the addition of trust sources and the decentralization of trust sources, the cost of obtaining comprehensive authentication and multiple evaluation of trust sources is greatly increased, and more new trust sources will be generated. There are also the following typical problems affecting the social credit system:

1. Oligarchy of data: The management of data shows an oligarchy trend, forming multiple "data islands", which cannot completely cover the user's information, so the pricing of data is controlled by the data forwarder.

(2) Data exchange is difficult to be safe: Based on the existing centralized data exchange system, the data precipitation of centralized servers will often harm the interests of data sources and pose business threats to data customers.

(3) Reputation evaluation is difficult to synthesize: For "soft trust" such as reputation, a large amount of data and information are needed to support it. However, there is a lack of effective information circulation and coordination mechanism based on reputation management.

(4) False news is difficult to judge: the incentive mechanism based on the number of browses has resulted in the widespread dissemination of a large number of low-quality or even false and misleading information. How to judge these false news is always difficult.

(5) Equity management is difficult to be transparent: For the new equity management mode (such as crowdfunding, etc.), it is difficult to establish reliable trust in the operation of the project due to low transparency and asymmetric information.

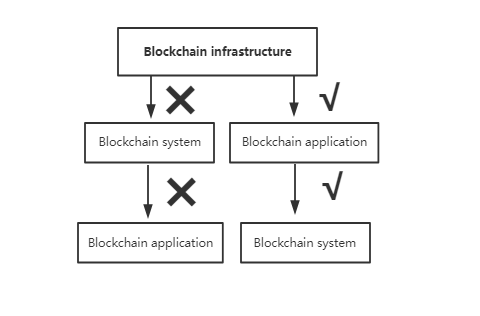
It is precisely because of the diversity of "trust" that the cost and pain points of "trust" in various scenarios are caused. How to construct an integrated trust mechanism combining diversity has become the pursuit of a new generation of "trust" basic system.

* Smart Contract

The concept of smart contract can be traced back to 1995 and appeared almost at the same time as the Internet. It was first proposed by cryptographer Nick Szabo, who was widely praised for laying the foundation for bitcoin. In essence, the smart contract logic prototype is a Finite State Machine (FSM). The working principle is similar to the if-then statement of a computer program. Smart contracts only interact with real-world assets in this way. When a pre-programmed condition is triggered, smart contracts execute the corresponding contract terms.

Ethereum combines smart contract with blockchain, By establishing an abstract foundation layer, it is POSsible to create contracts and decentralized applications and set up their freely defined ownership rules, transaction methods and state transition functions in them, Although it is stated in the White Paper on Ethereum that the Ethereum system allows anyone to create contracts, in fact there is still a high threshold for issuing contracts. Not everyone can program computers, so the Ethereum system is not universal. iWorth will classify and display parameters such as the type, state, condition and value of smart contracts, so as to visualize smart contracts and block chains so as to truly apply them to people's lives.

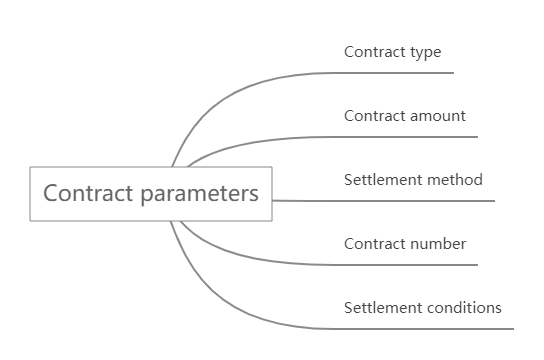
* Information Internet and Value Internet

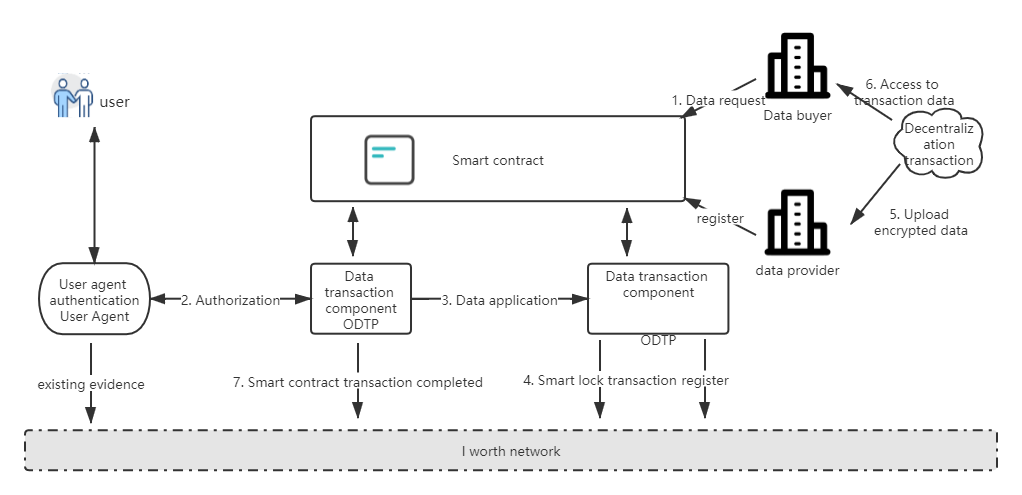
At present, the problem that the identity of information internet cannot be proved by itself fundamentally determines that the characteristics of information internet are "valuable but not useful", The key point to turn data into future social productivity lies in the authenticity of data. At present, if data transactions touch the laws of various countries, they cannot be proved, and privacy disclosure and other issues have gradually been paid attention to. Blockchain technology is undoubtedly the best choice to solve problems and let the information internet iterate to the new generation of value Internet, However, unlike the beginning of the rise of the Internet more than 20 years ago, the block chain is built on the basic information internet and is not a completely emerging technology application like the Internet in those days. Therefore, the development idea should be from the infrastructure layer to the application layer and then to the system layer, not from the system layer to the application layer. Because most of the existing block chain systems are closely related to encrypted currency, most of the system construction costs are not high and easy to implement. Even after spending energy on developing the system, if there is no suitable application scenario or it is not accepted by the market, the application secondary development cannot be carried out on the basis of the original system, and the result is often failure. Therefore, we need to find the appropriate application scenario of blockchain first, constantly adjust and create blockchain application products accepted and recognized by the market, so as to guide users to transform from traditional information internet platform thinking to Internet thinking of individual value shaping, expand to blockchain system of value interconnection, and open a new era of value internet.

**iWorth**

* Representational

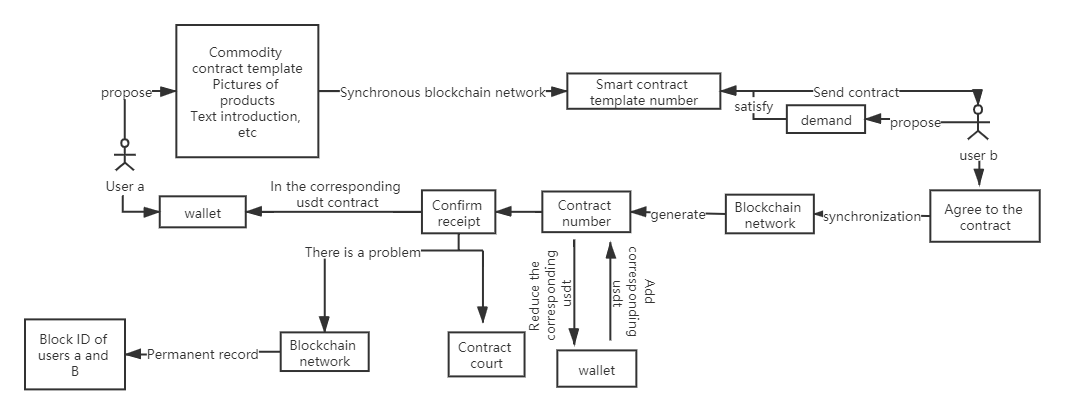
iWorth is an application product based on blockchain technology, which can create, receive and browse various types of visual smart contracts. You can use Worth Coin to run and create a smart contract. At present, we decompose a contract parameter through these dimensions, namely: contract type, number of contracts, contract amount, settlement conditions and settlement method. Custom contracts will enable users to set all contract parameters according to requirements, while skill contracts related to user pass certificates will simplify operations or limit unfriendly behaviors of users by fixing some parameters, such as confirmation by both parties to skill contracts that settlement cannot be based on time only, etc.

There are three contract types in iWorth, They are commodity contracts, skill contracts and custom contracts, The user can save the edited common contract parameters by lifting the contract template so that they can be called directly when using it. It can be understood that the contract template is the commodity of merchants on traditional Internet websites, but the guarantee intermediary has changed from a centralized monoPOLy platform to a block chain technology and users' own credit. So that the transactions completed by information matching do not have centralized high drawing and capital pledge.



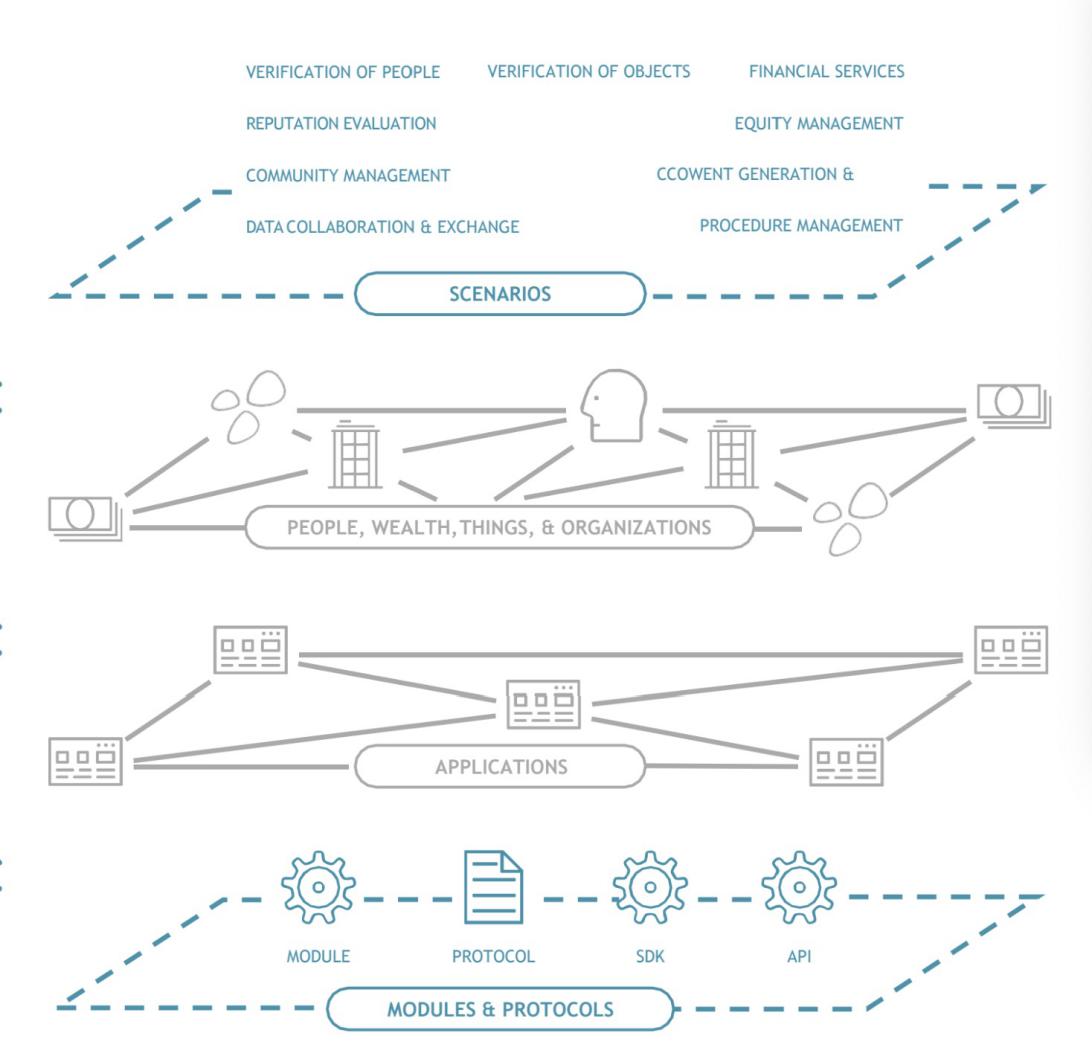
All smart contracts in force for users in the system will be synchronized to the blockchain network, Examples of application scenarios are as follows: User A needs to sell something of his own, A pro-posed a template for commodity contracts, information such as uploaded pictures, text introductions and the like of commodities are stored in the contract template. After the contract template synchronizes with the block chain network, an identifiable smart contract template number # 00001 is generated. At this time, when user B needs to purchase commodities of A, user A directly sends a commodity contract worth 10USD to user B using the previously edited template # 00001. After user B views the contract and clicks to confirm the contract, user B's wallet balance will be reduced by 10USD and 10USD will enter the commodity contract. At the same time, the contract will be synchronized to the block chain network and a unique contract number will be generated. B confirms the contract after receiving the goods and confirming them to be correct. At this time, the contract status changes and 10USD is transferred from the contract to User A's account. If there is a problem with the contract, the problem contract permanently recorded by the block chain network will be recorded on the Block ID of A and B, and the problem contract will be appealed to the "contract court" for processing.

A record of that problematic smart contract will appear on the user's personal business card, Other users can view the number of times the user's problem contract occurs. If both users are friends with each other, they can see the detailed information of the user's problem contract-when, at what price and what type of problem contract occurred, so that the user can define the user's own credit through personal behavior.

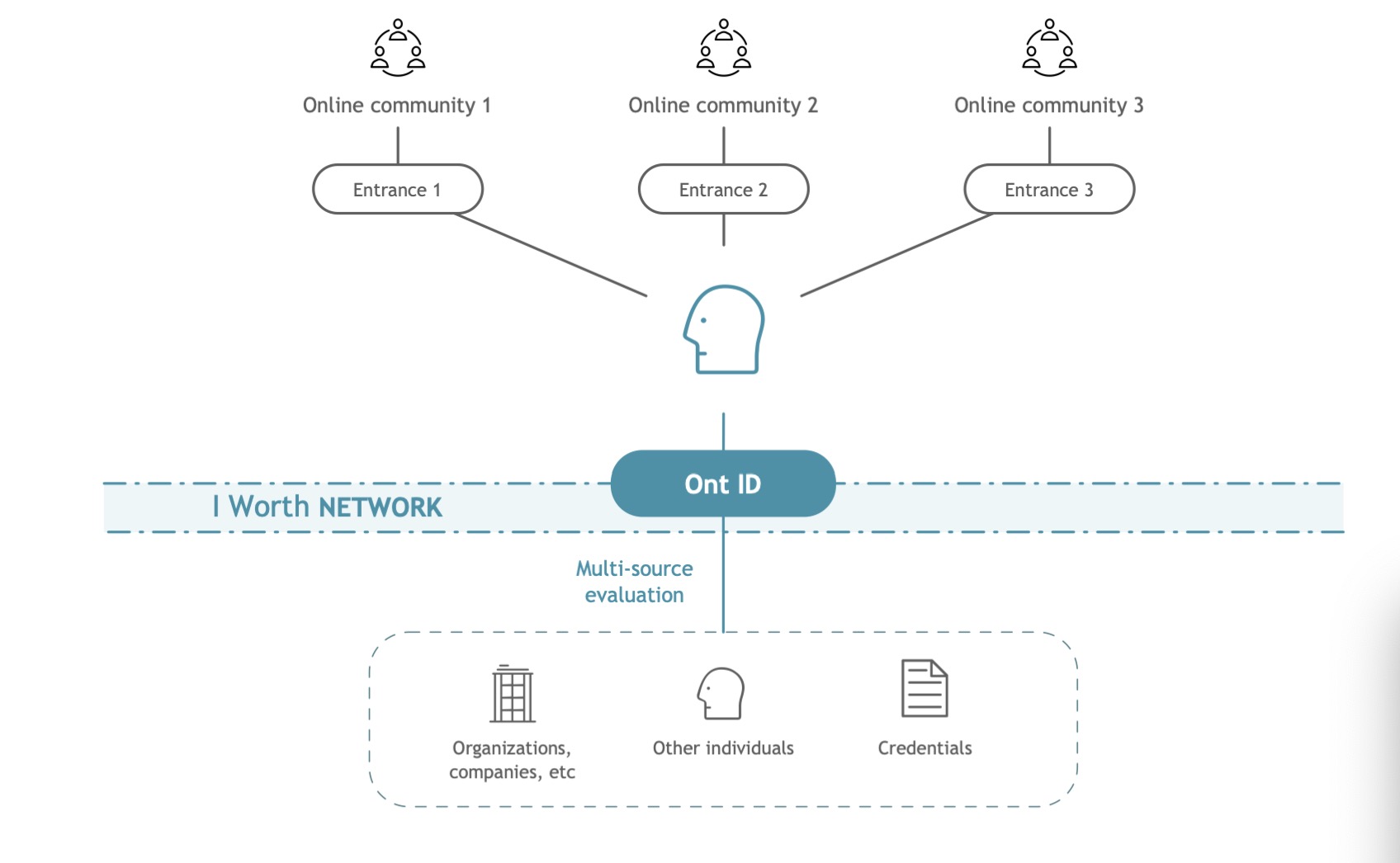


Contract court and contract browser are essential parts of the whole iWorth ecosystem, The contract court is responsible for dealing with the direction of funds in the contract after the problem contract occurs. The contract browser is used to inquire about the completion of past contracts to judge the credit status of the user when trading with the user, and gradually build a set of decentralized credit ecology unique to iWorth system, which is completely generated by the user's behavior. The contract, the court and the browser are interdependent. The court and the browser will be described in detail below.

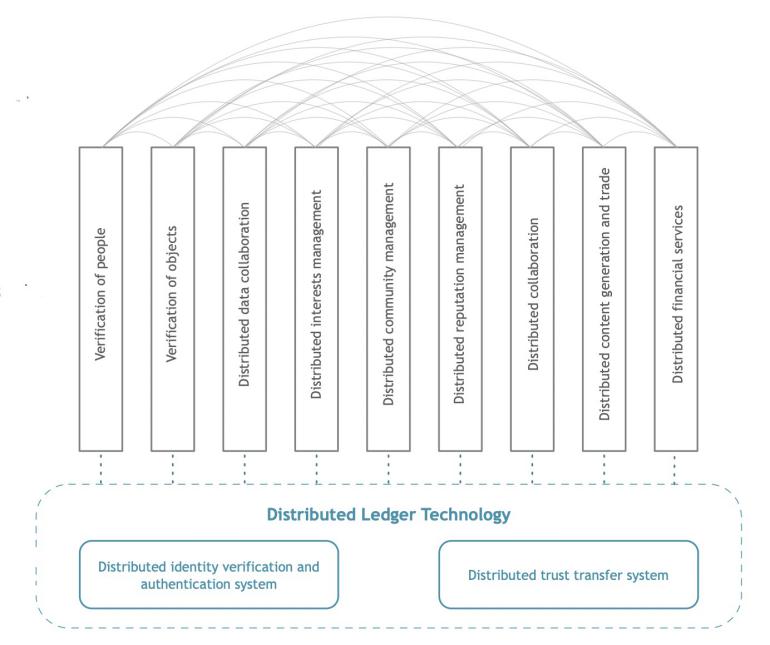
iWorth is committed to building an ecosystem of trust. It will be used as an application facility of the trust ecosystem. Based on this, various applications can be carried out and coordinated in various industries and scenarios in the future. The overall architecture diagram of the system is as follows:



iWorth is divided into three stages, which will be described in detail below. iWorth1.0 will introduce the concept of Block ID (see below for details) starting from human authentication. Complete distributed data collaboration through visual smart contract, Gradually complete the authentication of articles and the digital authentication of the ownership of articles, And bind it to the Block ID, the distributed reputation management system will be gradually established through visual smart contracts on the block chain network, so that distributed community management can be carried out through smart contracts. The healthy development of the community needs to reasonably control the entrance to ensure that the commonness of the community will not decrease with new entrants. Through chain drawing, community managers can confirm the credibility of information to ensure that new participants in the community are high-quality and qualified users. A healthy community must have a credit system, and users with different credits have different credibility and voice. Through iWorth' s experience or authoritative information proof, or grade proof in a community with common characteristics (such as technical community managers providing their own administrator identity authentication information in a certain interest exchange group), one can quickly and reasonably divide one's trust system in a community. From then on, Ethereum' s vision is to truly form a decentralized autonomous organization (DAO).

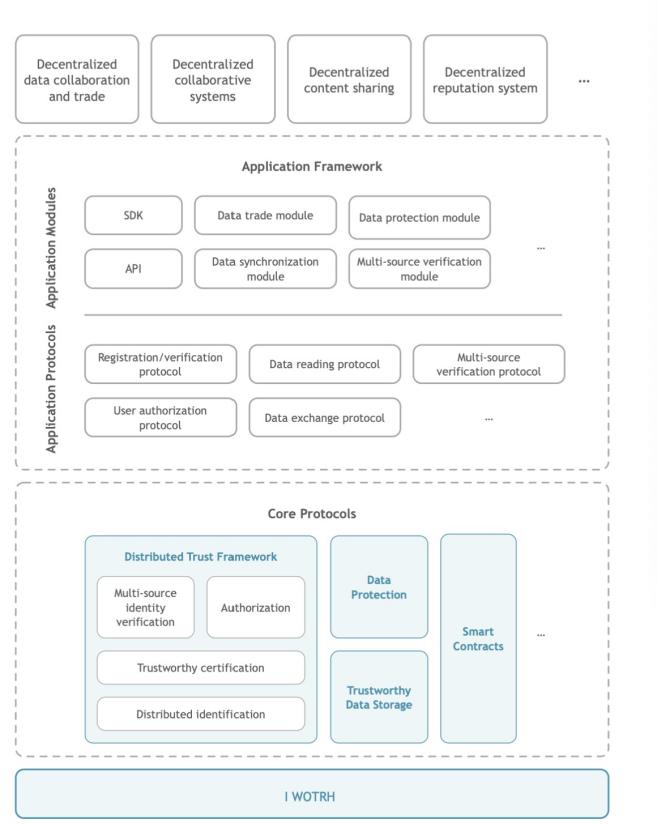


Distributed equity management is realized through node accretion modules restricted by smart contracts. In phases 2.0 and 3.0, iWorth will gradually explore more system-based expanded applications, such as content search engines, financial services, etc. All functional modules will rely on each other to create a decentralized and customized trust transfer system. The specific relationship is as follows:



The overview of iWorth technology architecture includes the following parts: distributed identity and multidimensional authentication, identity entity and distributed identity, distributed trust transfer system and human diversity identification and authentication system. The human diversity identification and authentication system will be described in detail in "Block ID".

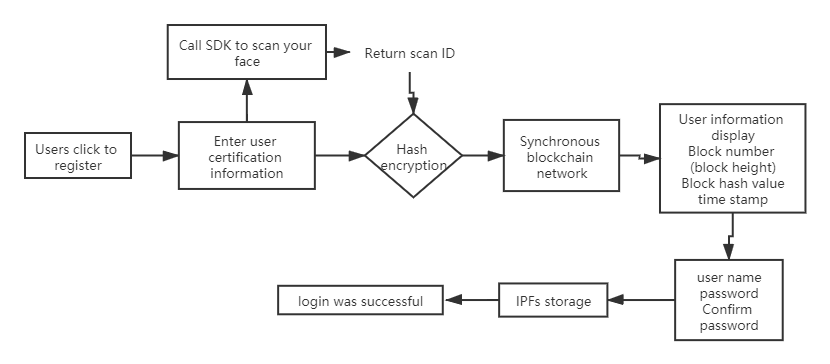
In iWorth, an entity (person, organization, thing) can also correspond to multiple distributed identities. Before the authorizer of the identity entity authorizes, any third party cannot infer the identity used by the entity in another system according to the identity used by the entity in one network system, which can greatly protect privacy and identity information rights.



Trust transfer mechanism is the implementation of trust use in iWorth. Specific identity subjects are acquired through various types and declarations of smart contracts. On the one hand, they can form multi-dimensional identities, and on the other hand, they can form a personal trust ecology starting from themselves. In specific requirements, trust can be transmitted through the presentation of statements and the provision of data records. On the one hand, trust authentication can be presented to others; On the other hand, trust data can be used many times to form multiple approvals, which will further expand the trust ecology.

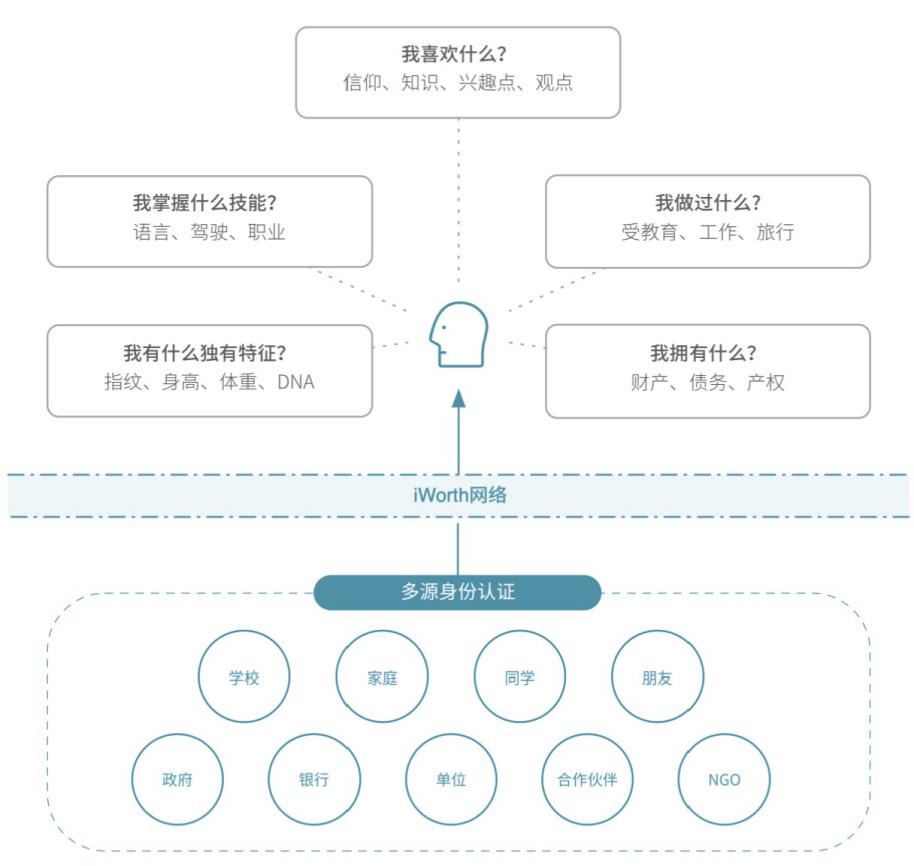
* Block ID

iWorth guarantees that the user's identity can be self-authenticated through Block ID, When the user registers, the system will collect the face of each user to generate a unique face recognition code, The face recognition code synchronizes the block chain network to obtain a unique block ID, The Block ID is equal to the current number of registrants, so the number of registrants is the height of the block. Users in different regions will improve the authentication process of the Block ID according to local POLicies, making the acquisition of the Block ID more rigorous, so as to ensure that users have only a unique ID that can confirm their identity.



We can't look at the impact of users' evil behavior on the system with traditional Internet thinking. Under the guarantee of the Block ID, users can only have one account number through their unique biological characteristics. Evil information will be permanently stored in the block chain network and displayed on personal business cards. I believe most users are unwilling to conduct contract transactions with evil users.

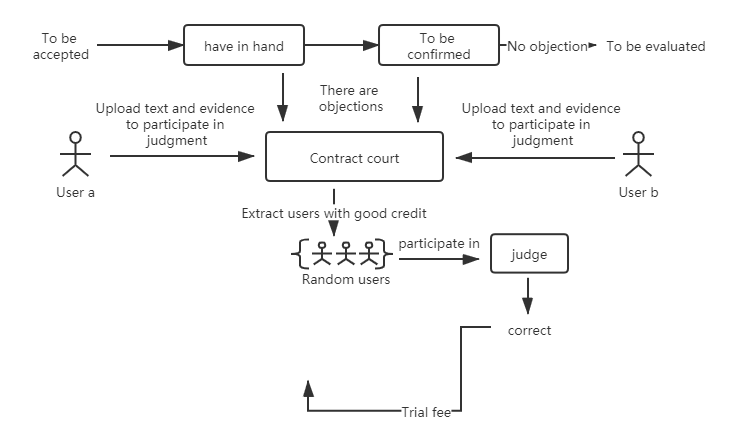
After iWorth carries out identity authentication, the system will carry out multi-dimensional evaluation on users, and users can submit or set various kinds of information to complete the diversity authentication of people by the system. In the real society, people have a variety of social relations, and any organization or individual associated with an individual has information related to this person. Through iWorth, users can link and authorize various data related to themselves. From government agencies to schools, banks and other enterprises and institutions, from family members, friends to colleagues, leaders, partners and other individuals can become authentication data sources, and realize integrated flexible application under the protection of privacy and authorization.



* Contract Court

In iWorth, a smart contract has four states: to be accepted → in progress → to be confirmed → to be evaluated. The smart contract in the "to be accepted" state is a contract that other users have not put USD into the contract to accept after sending the smart contract to the user; "In progress" is a smart contract that is in effect; The status of "to be confirmed" is that USD will not be credited to the initiator's account from the contract until the initiator confirms the completion of the contract and the recipient confirms the completion of the contract; "To be evaluated" refers to the evaluation of the contract after the contract is completed. Most of them are the evaluation of the contract template, which can be understood as the evaluation of a commodity or a skill.

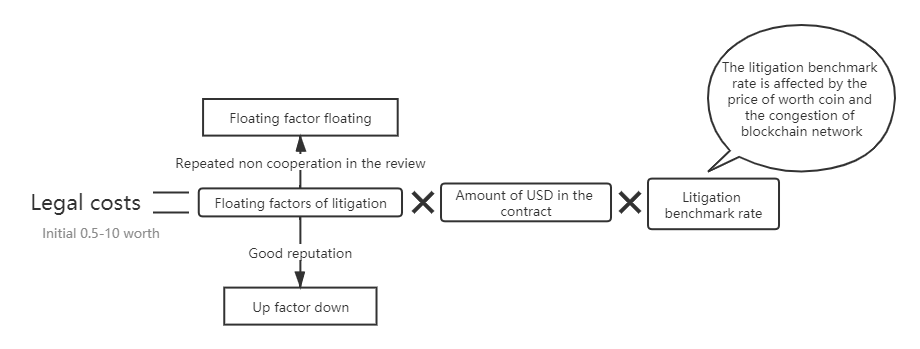
When a smart contract is "in progress" and "to be confirmed", the user can submit the disputed smart contract to the contract court for appeal, and both users need to upload text and evidence to participate in the judgment. iWorth will randomly select 20-30,000 users with good credit to participate in the trial of the contract according to the number of USD involved in the contract and charge a certain amount of Worth Coin as trial fees to share with the correct users participating in the trial.



The basic calculation formula of legal cost is:

**Legal cost = litigation floating factor \* USD quantity in contract \* litigation benchmark rate**

The litigation benchmark rate defaults to 0.1% at the beginning of the system, and the litigation floating factor defaults to 1 and is affected by user behavior. For example, if a user is drawn many times but does not accept the problem contract of judging others, when the user needs to appeal against the problem contract, his litigation floating factor rises to 1.2, while the reputable user may be lowered to 0.8. The litigation benchmark rate is affected by the price of Worth Coin and the congestion of blockchain network. Similar to the gas fee of Ethereum , the basic control fee for appealing to pay Worth Coin is about 1.5 USD, and the initial legal fee of the system is tentatively set at 0.5-10 Worth Coins.

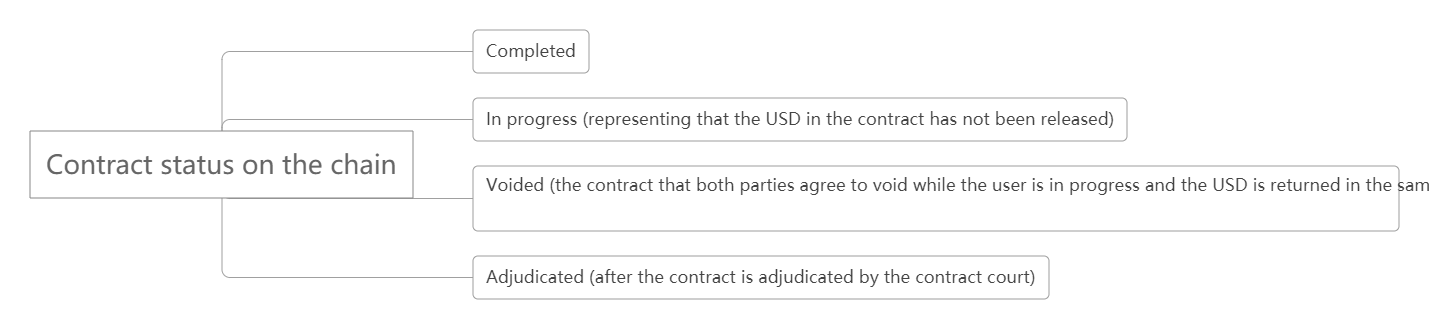


The contract court is a very important part of iWorth' s ecology, and its basic system needs to be gradually upgraded and improved. The contract court uses a decentralized voting mode instead of the traditional platform centralized mode to handle disputes.

* Block Browser

iWorth Block Browser and Contract Court are both in the "Block" module-Wallet. The block browser here does not browse the "identity authentication chain" of the registered application, It is a blockchain network with synchronous smart contracts, It is also iWorth' s main network, The smart contract blockchain becomes visualized in the block browser, Users can browse the entire block chain by sliding left and right, and can also search the block height to view the number of smart contracts on each block, the contract number, amount and status of each contract, etc. Of course, the information does not include the private information of the contract initiator and recipient.

There are four contract states in the smart contract chain: completed, in progress (representing that the USD in the contract has not been released yet), voided (the contract where both users agree to void and the USD returns to the original route when in progress), and tried (after the contract passes the contract court trial)



* Extensibility

iWorth needs a universal product definition. If only the application of iWorth' s visual contract based on block chain technology is abstract and not conducive to promotion, the final form of all universal application products is "social", so it is better to start with social. iWorth' s real identity, personal business card credit, contract transaction and other attributes are just in line with social applications. iWorth has introduced an intermediate key token--i Debris to increase the interest and universality of the system. i Debris will be described in detail below.

On the basis of blockchain, it can be found that almost all Internet centralized platforms can be replaced by smart contracts, such as smart contract taxi system using iWorth login operation, system for merchants to issue token and smart contracts to market shops, smart contract errands express system, smart contract music video property system, etc.

iWorth will open an era of de-platformized smart contracts

**System Token and Economic Model**

The iWorth system token is Worth Coin (Social Fuel), referred to as WTC for short, with a total amount of 210 million (210 million pieces), which will never be issued.

WTC can be obtained by i Debris (fuel fragment, abbreviated as i) synthesis. Worth Coin has three stages, namely Grand Voyage, Stars Plan and Watchman. All Worth Coins will be released in the first stage.

* iWorth1.0——Grand Voyage

The WTC is distributed as follows:

Of the 210 million Worth Coins, 100 million are block height awards. As mentioned in the "Block ID" section, block height is the number of registrants.

Rewards were released ten times, with a fixed release of 10,000,000 pieces. The trigger condition for releasing the reward is to reach the block height of the next reward Block ID, and users with the current reward Block ID will be rewarded.

For example, the first WTC release will be triggered when the block height reaches 39063, that is, 39063 users register, and the reward interval [1, 19531], and users with Block IDs in this interval get 512 WTC on average; Similarly, the second WTC release is triggered when the block height reaches 78125, and the reward Block ID interval is (19531,58594]......

The specific rules are as follows:

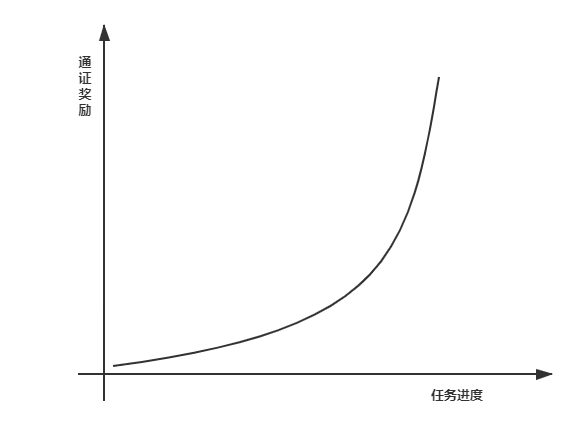
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of releases | Number of awards | Reach Block | Number of reward blocks | Average reward amount |
| 1 | 10000000 | 39063 | 19531 | 512.0065537 |
| 2 | 10000000 | 78125 | 39063 | 255.9967232 |
| 3 | 10000000 | 156250 | 78125 | 128 |
| 4 | 10000000 | 312500 | 156250 | 64 |
| 5 | 10000000 | 625000 | 312500 | 32 |
| 6 | 10000000 | 1250000 | 625000 | 16 |
| 7 | 10000000 | 2500000 | 1250000 | 8 |
| 8 | 10000000 | 5000000 | 2500000 | 4 |
| 9 | 10000000 | 10000000 | 5000000 | 2 |
| 10 | 10000000 | 19980469 | 10000000 | 1 |
| Total block height | | | 19980469 |  |

Each user can only get a block height reward once, and the block height reward can only be obtained if the user completes corresponding tasks, such as inviting new users or completing smart contracts. The more users who get Worth rewards, the more people they need to invite or complete smart contracts. When the total block height reaches 19980469, all rewards are released, and iWorth2.0--Stars Plan stage is entered.

The number of WTCs obtained by the start-up team is also highly Positively correlated with the blocks in the identity authentication chain. Ten million WTCs will be distributed in ten copies, with one million at a time. The release timing will be synchronized with the release timing of the block highly rewarded. Eventually, 10 million WTCs will be obtained, accounting for 5% of the total number of WTCs. According to the user's Block ID, the user will receive the block height reward task assigned by the system, as shown in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Number of releases | Reach Block | Reward block interval | Average Task Points |
| 1 | 39063 | (0,19531] | 64 |
| 2 | 78125 | (19531,58594] | 56 |
| 3 | 156250 | (58594,136719] | 48 |
| 4 | 312500 | (136719,292969] | 32 |
| 5 | 625000 | (292969,605469] | 20 |
| 6 | 1250000 | (605469,1230469] | 8 |
| 7 | 2500000 | (1230469,2480469] | 6 |
| 8 | 5000000 | (2480469,4980469] | 4 |
| 9 | 10000000 | (4980469,9980469] | 2 |
| 10 | 19980469 | (9980469,19980469] | 1 |

The size of the block height (Block ID) determines the upper limit for users to obtain Worth Coin awards. Users can complete tasks by inviting other users or completing smart contracts with different users. The size of task points determines the difficulty of tasks. The larger the task points, the more difficult the task, and the higher the upper limit for users to obtain Worth Coin. Every time a user invites a new user to use the system, he can get a little task point, and every time he or she completes the smart contract with two different users, he or she can get a little task point, and only by completing the smart contract, he or she can get a maximum of 50% of the task points.

The reward for each time a user invites a user or completes a contract increases with the progress of the task completion, The growth function refers to the "J" curve of natural growth of human biological ecological population, specifically N (t) = n (p ^ t), where N (t) is the number of Worth Coins obtained by obtaining task points for t times, t is the number of task points obtained by users, (p-1) is the growth rate (greater than 1) of the number of reward Worth Coins after obtaining points each time, and the image is similar to J-shape.

If the user fails to complete the block height reward task issued by the system according to the block height, The Worth Coin awarded by the system will be gradually reduced to 0. The 50% reduction token will be automatically entered into the node accretion address of each phase under the restriction of the smart contract chain Genesis block edited and open source smart contract (see iWorth node below for node accretion details), and will be distributed to the nodes and sub-nodes of the current period according to the ratio of 2: 1. The remaining 50% Worth Coin will be permanently destroyed into the black hole address.

Contract Socialing Is Mining:

WTC can be synthesized by idebris, and the total amount of WTC is 100000000 (100 million). idebris is the circulation gas of iWorth applications, which can be generated randomly by users' daily operation on the applications. Idebris has a maximum number.

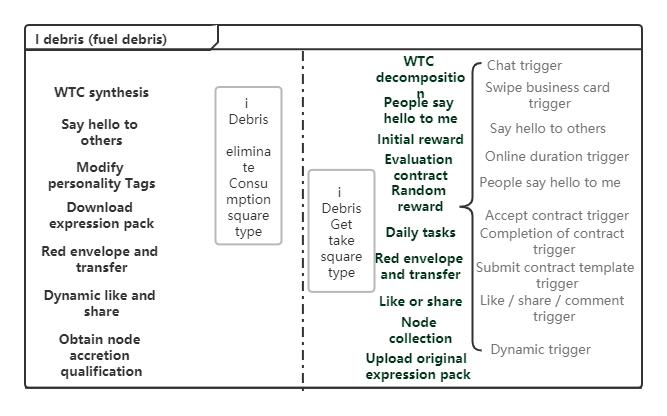
**Maximum limit of iDebris quantity = Worth release times \* 10000000 \* 100**

Worth Coin can be synthesized once per 100 iDebris, and each Worth synthesis needs to wait for 24 hours. The random interval of the number of synthesized Worths is [0.8, 5].

The synthesis probability is shown in the figure:

|  |  |  |
| --- | --- | --- |
| Quantity of iDebris consumed | Synthetic Worth Quantity | Trigger probability |
| 100 | 0.8 | 20% |
| 1 | 35% |
| 1.2 | 20% |
| 1.5 | 10% |
| 2 | 5% |
| 3 | 8.90% |
| 4 | 1% |
| 5 | 0.10% |

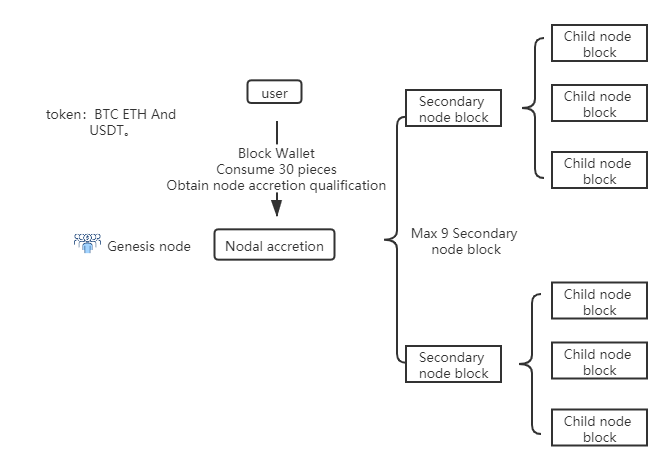
Users can get iDebris through various social activities. The specific triggering events are shown in the figure:



The Grand Voyage phase is dedicated to using token distribution to increase the number of users to build a group consensus, thus ensuring the wide application of contracts in the system. The user thinking is iterated from the traditional Internet's single search center platform problem-solving mode to the problem-solving mode of submitting and receiving contracts using block chain as the underlying technology. The first stage ends when the block height (number of users) of the authentication chain reaches about 20,000,000 (19,980,469), at which time all WTC issuance is completed.

* iWorth Node

In the iWorth1.0 phase, in order to better maintain and upgrade the system and ensure the security of the system, iWorth combined Ethereum (Ethereum) and Fabric's alliance block chain network to build a multi-node alliance chain limited by smart contracts. In iWorth network, there are two roles: node block and common block. Among them, node blocks are divided into four types: Genesis NODE Block, NODE Block, Secondary NODE Block and Child NODE Block.



Genesis nodes are start-up teams. Users of primary node blocks, secondary node blocks and sub-node blocks can obtain them through NODE Accretion of each phase. Users can enter the node accretion contract through "Block-Wallet-Node Accretion", The source code of the node accretion contract is also open source in the Genesis block of the smart contract chain. The node accretion has nine phases, each phase has one main node block, N sub-node blocks and multiple sub-node blocks, of which N= the number of phases, i.e. there are up to 9 sub-node blocks, and the duration of one node accretion is 7 days. The user needs to consume 30 fragments to obtain the qualification of node accretion. After the user opens the node accretion qualification, It is necessary to accrete tokens to accretion addresses to obtain node qualification.

Token is used to build physical node server to increase system stability, security and reduce centralization.

Users can exchange "Narf box" with fuel debris (i Debris) and open it with token to get a random number of Narf. Narf is only used as the intermediate conversion of node accretion, and does not have the transaction attribute of token. The Narf invested by users will be converted into node accretion ratio, and the sum of all participating users' node accretion ratio is 1 (100%).

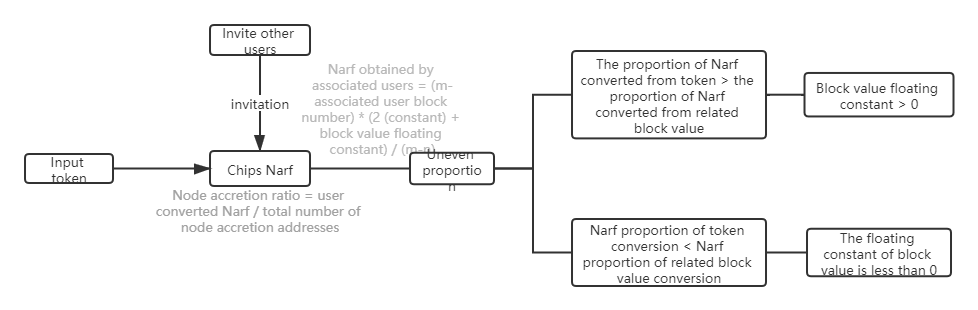
Conversion formula:

**Node accretion ratio = user converted Narf / total number of node accretion addresses**

The user can also invite other users to obtain the chip Narf accumulated by the node. The associated Block ID filled in by the user at the time of registration is associated with the topmost Block ID, which can obtain the Narf that all associated users invite users to contribute a random number. There is a negative correlation between the number of Narf and the user's Block ID. In the Block ID range of debris release in the same period, the larger the Block ID, the less the Narf. The specific algorithm is as follows:

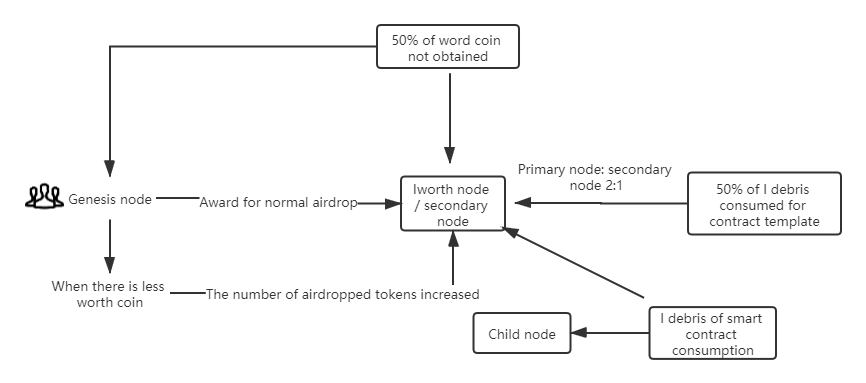
**Narf obtained by associated users = (M-associated user Block ID) \* (2 (constant) + block value floating constant) / (M-N)**

Block IDrs can also accrete through the Relate Blocks Value in the node accretion process of each period. Example: User A invites User B, The Block ID of B is 20000, which belongs to the Block ID of node accretion in the second stage. At this time, M-N=39063, the number of NARFs obtained by the associated user is (58594-20000) \* 2/39063=1. 9759, which is reserved to four decimal places by default. At this time, the user B invites the user C, and the Block ID of the user C is 55000. Then, the number of NARFs obtained by the associated user is (58594-55000) \* 2/39063=0. 1840, and the value of the associated block of user A is 1.9759 +0.1840=2. 1599, that is, the user's NARF is 2.1599. The block value floating constant defaults to 0, The constant defaults to 2; In the process of node accretion, if the proportion of NARF converted by token and NARF converted by associated block value is uneven, the floating constant of block value will change; When "token converted NARF proportion > associated block value converted NARF proportion", the floating constant of block value > 0, and the value of associated block obtained by inviting users will increase as a whole; On the contrary, if the NARF converted by the user through token accounts for a relatively small proportion, the block value rises by a constant of < 0, and the associated block value invited to the user becomes less as a whole.



The NARF obtained by the associated user may double each time, and the doubling probability is proportional to the size of the Block ID in each Block ID interval. The larger the Block ID, the higher the doubling probability, and the probability interval is (0%, 30%), so as to balance the difference that the user invites users with different Block IDs to obtain the value of the associated block.

iWorth secondary nodes are randomly generated through hash value collision. After users become iWorth nodes or secondary nodes, they can obtain 50% of all Worth Coins that have not been obtained in the current period. Nodes and N negative nodes can also obtain 50% of i Debris consumed by all users when submitting contract templates in the current period, with an acquisition ratio of 2: 1. The iWorth Genesis node will also give iWorth nodes airdrop rewards from time to time. If less Worth Coins are not obtained, the number of airdrop tokens will increase. Users of all nodes, sub-nodes and sub-nodes will obtain i Debris consumed by all users initiating smart contracts in the current period according to the node accretion ratio.



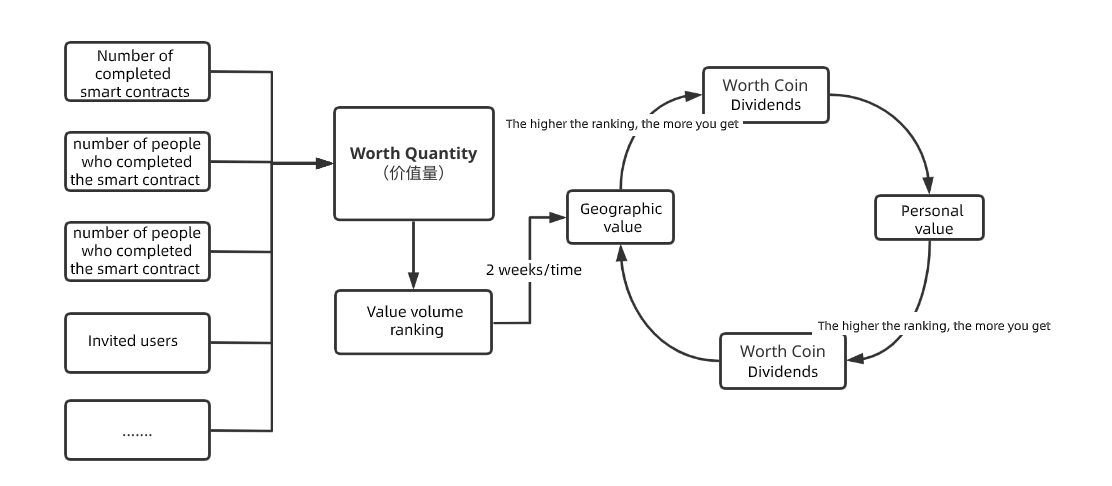
* iWorth2.0——Stars Plan

After the issuance of the system token Worth Coin, the iWorth system officially enters the 2.0 stars plan phase. The total amount of Worth Coin is constant. Since each user can not complete 100% of the block height task and the existence of black hole address, the total amount of Worth Coin must be less than 210 million. At this time, it will be up to I to initiate a contract or submit a contract template in iWorth Debris becomes Worth Coin.

In the stars plan phase, the system is still running in the form of multi node chain. At this time, iWorth will introduce a new variable - "worth quantity" (WQ for short). The worth quantity is related to the number of times users complete smart contracts, the number of people who complete smart contracts, the evaluation score of smart contracts, the invited users and other factors.

**WQ=A\* Number of contracts completed + B\* Number of people completing smart contracts + C\* Evaluation score of smart contracts + D\* Number of invited users**

Among them, ABCD is the value proportion constant (WQ proportion constant). Because the development of the system is unknown, it is not POSsible to directly publish the value proportion constant such as ABCD at present, and with the development of the system, more variables affecting the value will be generated. Based on the value WQ, the value WQ ranking is derived. At this time, the iWorth system will rank the value every two weeks according to the user's regional information. Users with the highest value ranking in the region can get Worth Coin dividends consumed by users in the region. Users with high value ranking can get more Worth Coin dividends, and then complete more contracts to create more value, so a virtuous circle......

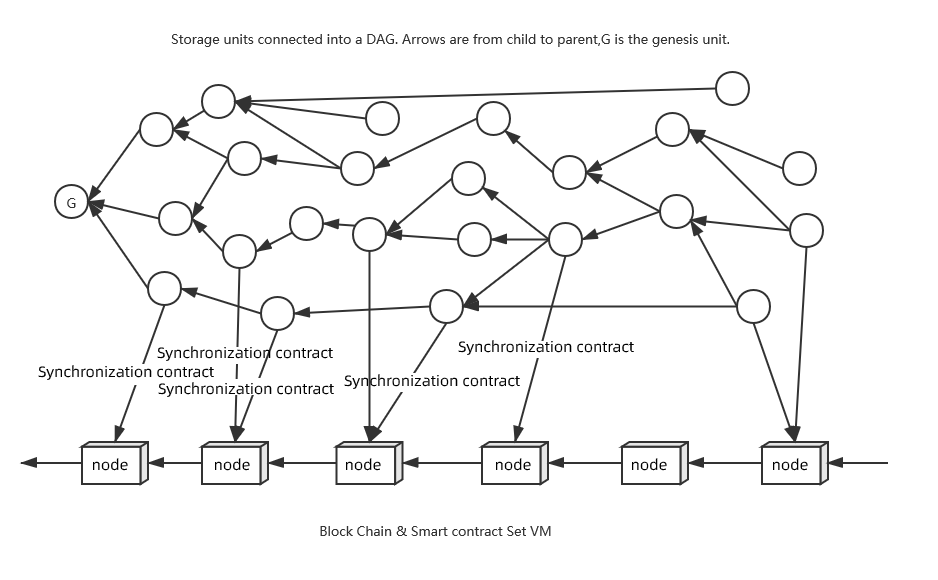


Because of the unknown and uncertain development of the system, Genesis Node will introduce more details of the 2.0 Stars Plan phase in the subsequent iWorth White Paper 2.0

* iWorth3.0——Watchman

After creating a large user base in Phase 2.0 and running stably for a period of time, iWorth will launch more smart contract applications DApp based on the identity authentication chain of one person and one number, such as smart contract shopping DApp, smart contract taxi DApp and smart contract store marketing DApp. At this time, iWorth' s main network (identity authentication and smart contract block chain network) transits from a multi-node alliance chain to a public chain of DPOS consensus algorithm. All node users (including secondary nodes and sub-nodes) will have priority in obtaining the right to vote. Delegated Proof of Stake (DPOS) is the fastest, most efficient, most decentralized and most scalable consensus model. DPOS uses rights holders' votes to solve consensus problems on the basis of equality and democracy. All network parameters, from fee list to block interval and transaction size, can be adjusted by elected representatives. The selected block producer can confirm the transaction within an average of one second. More importantly, this consensus agreement is designed to protect all participants from unnecessary regulatory disturbances, so it is most appropriate to use it during the transition period of the public chain.

After the end of the transition period, iWorth will use DAG technology to realize the main block chain, so that everyone can form their own block chain. We will build a parallel public chain dedicated to implementing smart contracts for contract and data solutions in the project. Each user's data is privatized and stored in IPFS.



In each DAG personal chain, transactions are carried out with its own Block IDand transaction ID (tid), As an attribute of each user action, This attribute is used to produce dynamic contract transactions when active transactions occur, At this time, the consensus algorithm of the lower chain is upgraded from DPOS to POW + POL using workload proof + random lucky number (number theory). The algorithm will randomly select each event of online users as a unit, select the current operation as the most node confirmation proof, and generate corresponding rewards, thus promoting the application activity through the lower consensus algorithm.

User data saves personal data in IPFS through the user's private key and the ID of each data link.

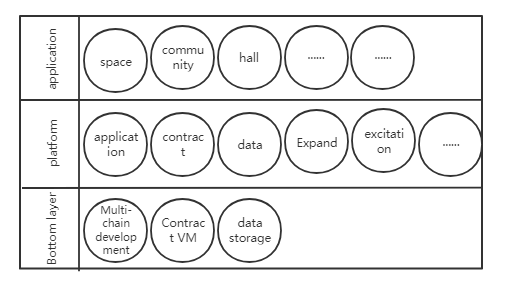
Implementation path:

Version 1.0 realizes system development + underlying mode blockchain

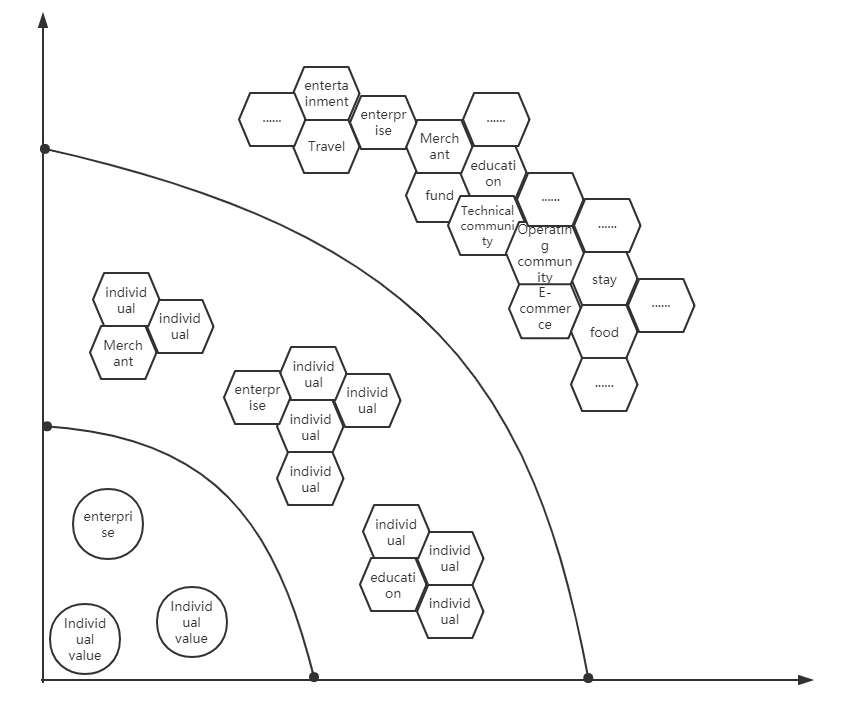
Version 2.0 iterative system function, realizing the hybrid blockchain mode based on DAG technology to upgrade the underlying blockchain system

Version 3.0 iteratively upgrades the DAG technology public chain system and integrates the smart contract layer POL mechanism blockchain VM

Version 4.0 upgrades system functions and has a dual operation mechanism based on value transfer. Running private chain + public chain



System function development path:



Compared with Ethereum, it is imPOSsible for each user to maintain his own link. All data exist in the main chain of Ethereum. If each user in Ethereum maintains one chain; First, the use of side chain method, second, the use of logical contract method, no matter which one, is costly. Moreover, for such bottom support, it is imPOSsible to realize the fast touch and real-time response of social networks.

The DAG technology adopted by iWorth system realizes that each user maintains his own data link, realizes multi-chain concurrency in the basic layer, and realizes the built-in contract virtual machine through chain structure to support the interaction of user contracts. The system is designed in layers, separating the service layer from the contract layer to improve the overall throughput. In the contract chain structure, Proof of Lucky Number, a random lucky number method, is introduced to mine, which is used as the mining proof of active users to improve the block output speed and randomness security.

With the increase of users and the expansion of the scope of consensus, iWorth will spontaneously form an autonomous organization within itself. In this regard, how to assist all users to form the POWer of the organization to create more value has become the mission of iWorth' s later development. Coincidentally, I met the "Three Worlds", A partner who specializes in implementing rules for distributed organizational governance, And reach strategic cooperation, It will assist iWorth to help users cooperate with each other through the "Intelligent Charter" tool, build the problems of code-level trust, equal decision-making, fair distribution and organizational governance in cooperation, establish the support of a wider range of ecological development in the later period, enlarge the value of each user, and each user participates in the construction of a huge interconnected ecological value chain. Let iWorth users establish better community collaboration, develop strong relationships, form cross-border trusted collaboration organizations, and upgrade individual intelligence contracts to organization intelligence charters.



iWorth adopts a data structure different from the previous block chain and DAG-based distributed book technology, which has the characteristics of high scalability, high concurrency and is suitable for multi-data link high concurrency application scenarios.

The data synchronization mechanism of traditional linear block chains (such as Ethereum) is synchronous, which may cause network congestion. DAG network adopts asynchronous communication mechanism, allowing concurrent writing. Multiple nodes can trade at the same time according to different rhythms without having a clear sequence. Therefore, the data of the network may be inconsistent at the same time, but it will eventually be synchronous.

In the traditional block chain network, there are many transactions in each block, which are packaged and sent by miners in a unified way, involving multiple users; However, there is no concept of "block" in DAG network. The smallest unit of the network is "transaction". The previous two transactions need to be verified before a new transaction can be carried out. In this way, DAG network does not need miners to transfer trust, transfer does not need handling fees, and at the same time, it establishes a data structure block chain of the underlying private chain to complete the point-to-point contract interaction function.

iWorth adopts POS + POL consensus method, POS is the proof of rights and interests, but it represents the bottom layer of the system as a compensation mechanism without POL proof. POS's object is a selection mechanism for calculating proof of rights and interests of the underlying private contract chain, is to redefine a compensatory workload proof method

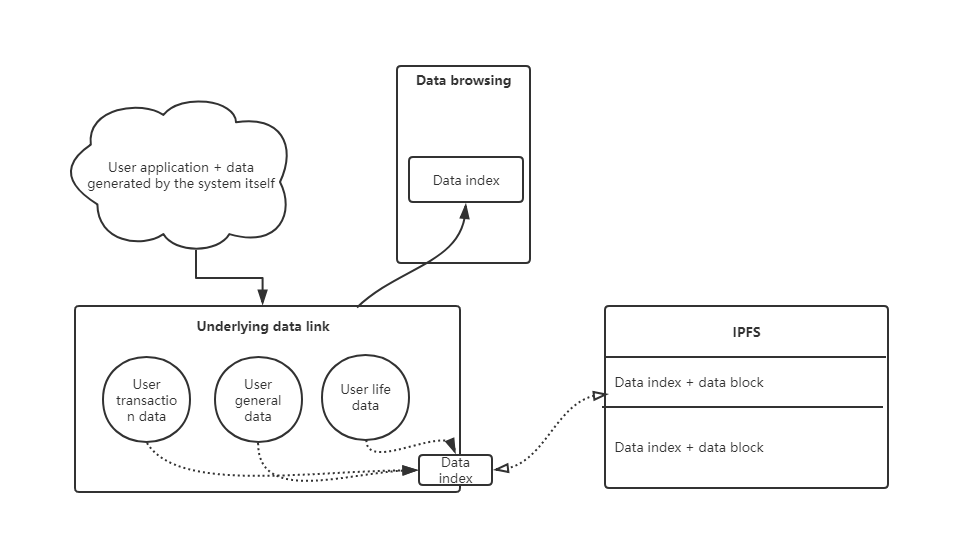
Where does POL come from? L is defined as Lucky Number here, and Taylor-Ulam configuration is proposed based on Ulam's participation in Manhattan Project; In 1955, the lucky number was put forward; The Ulam phenomenon was discovered in 1963; The conjecture of Bosuk-Ulam theorem is put forward. According to such an algorithm, the consensus at the first level comes from the fact that in online user applications, everyone is a mining node, and the bookkeepers are randomly selected through Lucky Number algorithm. In this method, we construct some columns of matrices similar to prime number spirals through current online users, as shown in the right figure.

According to the application properties of the system, the distribution algorithm of Lucky Number is reformed, and a large number of discrete data are stored and quickly indexed by dynamic Bloom Filter. According to the dynamic attributes of the system, it will affect the ranking of users in a certain period of time, and the independent event factors of each user change, and different sequences are constructed.



iWorth will construct a pseudo-random mining mechanism through dynamic Lucky Number + Bloom Filter.

iWorth uses DAG technology to solve the problem of multi-user and multi-data link concurrency. Of course, the structure of DAG will also cause problems, such as security and class centralization. Here, we focus on the implementation of the contract. Our implementation of point-to-point contract is to realize a private chain block chain mode of public data verification in the system to reach the contract transaction. The asynchronous operation of DAG makes the data stored between nodes deviate after running for a period of time when running smart contracts. From the reality, there is no project that can really develop smart contracts based on DAG network. The specific details of our implementation of this function will be continuously updated. The rights and interests way of POS is mainly the way to mine the bottom rights and interests when the first level consensus of POL does not find the data. The overall design and data structure are similar to POL. The modified design is mainly to make up for the unknown confirmation and accidental damage of POL, and the monitoring node in POL falls into the POS rights. POL for efficiency, POS for safety and justice.



The main technical principle is to realize verification and security node monitoring in DAG through Block ID, transaction ID, contract ID and hash generated in transaction users of each DAG chain, and the underlying private chain contract realizes the application of consistency and security of contracts. The system will form a hash chain of publicly verified data links, and through the proof and supervision of monitoring nodes, the results and algorithms will be disclosed to the application to provide personal verification. Aiming at a large amount of personal user data, it is encrypted and stored in IPFS by establishing data index.

* **Miscellaneous Concerns**
* About Our Team

iWorth team (Genesis node) is composed of many blockchain application geeks, aiming to build landing applications serving human beings in the blockchain world. “ Mr.Zero ”(code), "France" (code), "run" (code) and "avapxia" (code), etc. They all have a strong ideological consensus of anti platform and anti-monopoly. They think that the current era of platform information monopoly is a deformed form of social development, but it is also indispensable in the development of human Internet. They want to reconstruct and develop a new era of value Internet of information authenticity and information sharing through blockchain technology.

* About The Law

Due to the development needs of iWorth, the legal red line of each country should be avoided as much as possible in the first and middle stages of system development. Dapp of each country will be adjusted according to the legal situation and user usage habits of each country. iWorth of each country will be completed under the leadership of its country's nodes.

**Summary**

Thanks to the continuous efforts of iWorth Genesis Node, the visual Dapp has been implemented step by step after 3 years of polishing. As iWorth grows, we will continue to polish and update various user experiences, credit algorithm mechanisms and contract types of iWorth, and gradually expand iWorth ecology.

We believe that in the next 20 years, the development of smart contracts will become more mature, and smart contracts will gradually replace centralized platforms, thus forming a new P2P value Internet system.

**What is about to emerge is the "Grand Voyage Era" of the decentralized smart contract system.**