THINKEY

The Ultimate BlockChain for the New World

Spark: New journey
June 21, 2019

Table of Contents

DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER THINKEY FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS (THE THINKEY TEAM) WHO HAVE WORKED ON THINKEY (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THINKEY IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF THINKEY TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE PROJECT WEBSITE (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

The Whitepaper and the Website are intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, the Distributor, and/or the Thinkey team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Foundation nor the Distributor is under any obligation to update or correct this document in connection therewith.

Nothing in the Whitepaper or the Website constitutes any offer by the Foundation, the Distributor or the Thinkey team to sell any Thinkey token (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of Thinkey. The agreement between the Distributor and you, in relation to any sale and purchase of Thinkey token, is to be governed by only the separate terms and conditions of such agreement.

By accessing the Whitepaper or the Website (or any part thereof), you represent and warrant to the Foundation, the Distributor, its affiliates, and the Thinkey team as follows:

(a) in any decision to purchase any Thinkey token, you have not relied on any statement set out in the Whitepaper or the Website;

(b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that Thinkey token may have no value, there is no guarantee or representation of value or liquidity for Thinkey token, and Thinkey token is not for speculative investment;

(d) none of the Foundation, the Distributor, its affiliates, and/or the Thinkey team members shall be responsible for or liable for the value of Thinkey token, the transferability and/or liquidity of Thinkey token and/or the availability of any market for Thinkey token through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to purchase any Thinkey token if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of Thinkey token would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, New Zealand, People's Republic of China (but not including the special administrative regions of Hong Kong and Macau, and the territory of Taiwan), the Republic of Korea, Thailand, and the Socialist Republic of Vietnam).

The Foundation, the Distributor and the Thinkey team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation or the Distributor). To the maximum extent permitted by law, the Foundation, the Distributor, their affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or

otherwise arising in connection with the same. Prospective purchasers of Thinkey token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the Thinkey token sale, the Foundation, the Distributor and the Thinkey team.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of Thinkey token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of Thinkey token and/or continued holding of Thinkey token shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of Thinkey token (the Terms and Conditions), which shall be separately provided to you or made available on the Website. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

No regulatory authority has examined or approved of any of the information set out in the Whitepaper or the Website. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

The information set out herein is only conceptual, and describes the future development goals for Thinkey to be developed. The Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or the Thinkey team, may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicted in the Whitepaper,

and the Foundation, the Distributor as well as the Thinkey team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

The use of any company and/or platform names or trademarks herein (save for those which relate to the Foundation, the Distributor or its affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Whitepaper or the Website to specific companies and platforms are for illustrative purposes only.

The Whitepaper and the Website may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.

No part of the Whitepaper or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Foundation or the Distributor.

1. New World

According to A Brief History of Humanity, the ability of human beings to fictionalize "consensus" on a large scale, and the collaboration based on deep cognition is the key to distinguish human beings from other species. Human beings surpass all species through regular collaboration to transform the world and create new things. How to effectively coordinate has always been the goal pursued by human beings, and the efficiency of collaboration has been greatly improved in every major era.

However, each major ear is ended with the generating of new wealth giant, which is just the change of people who controls the world for general public. Matridley said in The Origins of Virtue: The Evolution of Human Instinct and Collaboration that human thoughts are made up of selfish genes, and they are built to be gregarious, trustworthy, and willing to cooperate.

Basic principle of BT era

With the high speed development of information technology, human beings have developed from IT era to DT and AI era and built the new world of digital, which bring more confidence and freedom to human beings. However, human beings are more easy to be controlled for the lack of unified basic rules. The transition to BT (Blockchain Trusted) era is the inevitable development of human society and science and technology. The things that are required by BT era is not only the improvement of efficiency, more importantly, the basic rules of autonomy, fairness, and credibility in the new world are required.

We will understand the trend of the digital new world more clearly if we see the development of the digital new world in essence. Humans recognize the laws of the physical world and use them to change the world. The invention of computer enables humans to copy their own wisdom without cost and use it to transform the world. The computer network has deceased the space-time distance between humans, therefore, humans can work remotely through programs, which has improved the efficiency greatly. With the continuous dataization of the physical world, human beings are building a new digital world. Big data and artificial intelligence can turn data into information knowledge and form decisions, so that the allocation of social resources is optimized and the efficiency of all-factor production is greatly improved.

Although the new world of digital is a underlying technology without boundaries, which can be connected at will. The sovereignty, interests, and human nature of the physical world have been basically translated, forming numerous relatively independent unstable

spaces. During the translating of them, the rules are changed at will, which prevents further improvement of the efficiency of human collaboration seriously and inhibits the improvement of innovation efficiency of all human beings. The development of human

information technology is entering a singular stage,in which more innovations need to be stimulated. These are calling for the BT era and calling for the establishment of basic rules in new world.

Data subject

Internet giants who once advocated collaboration, freedom, sharing, and antitrust has became bigger monopolist for their own interest and monopolized data that should be owned by user. They tried their best to vie the time and attention of users to obtain continuous data and enclose these data in their own platforms to form several data islands. They even use this data to manipulate and harm the user, however, the public always regard the giant's tricks as a reward. This approach has greatly curbed innovation, turned the market into a naked "jungle" and turned innovation into "human exploitation, swindling" and war of resource attrition. Each service provider increases the difficulty and cost of user migration through a closed centralized account system to lock users in their own platforms.

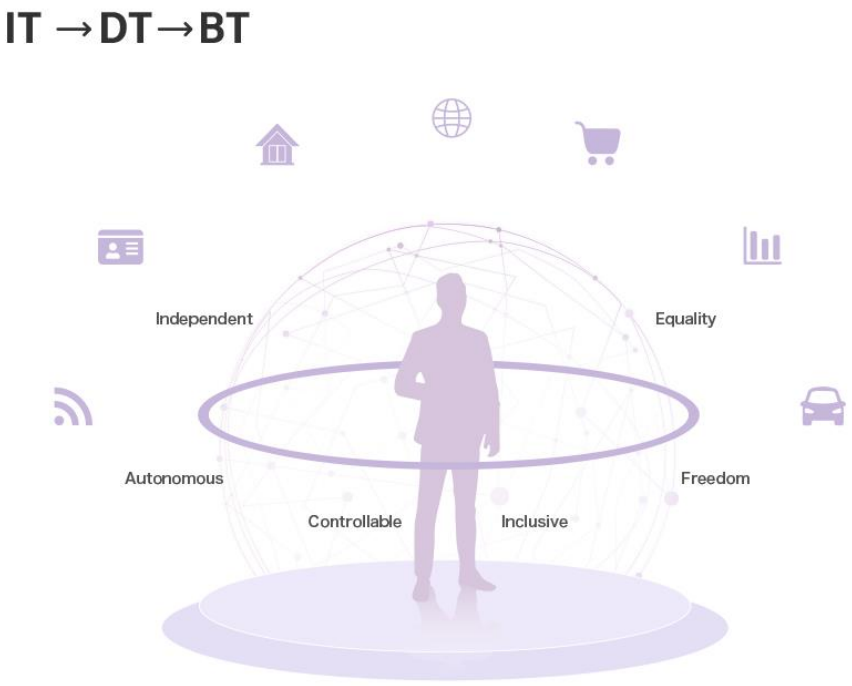
Decentralization

People strongly praised Facebook’s digital currency Libra shortly after the occurrence of the leakage of the privacy data of users. This is a global financial layout conducted by Facebook and some giants by using its user advantage in the digital world, which compliance with the rules that if you want to gain something, you want give something to others in advance. Everyone makes a rational reflection on the strongly centralized world after seeing the central bank of some countries (like Venezuela, Zimbabwe, Argentina, etc) makes the wealth of citizen turns into zero quickly through printing money arbitrary and hyperinflation. With the deepening of globalization, the whole world is experiencing the conflicts of politics, civilization and trade, the fierce confrontation between unilateralism and multilateralism, which makes us have stronger expectation for new world destiny community based on trust, cooperation and consensus. The balance that once fell to centralization was broken, and the balance quietly began to move to the other side.

Trusted new world.

Everyone is looking forward to a smarter, fairer and more promising future. However, we don't want to be the marionettes in the hands of Internet companies and don't want to be abandoned by organizations and countries that we trust and been harmed by them. The future we see is a credible world. We hope that the data segmented by the block can be opened, rather than spread the data in different places with a lot of redundancy and contradictions, which cannot form overall synergy after wasting a lot of resources. We hope that people can cooperate more with confidence, rather than communication friction (the cost of it is high),all kinds of intrigue and cheat between each other . We hope to have a decentralized trusted platform to provide safe and quality services to the world without spending a lot of time to choose and compare the platforms. We hope that the world will be more open and inclusive, so that every character can be treated equally, and there is a place in this world for it to lives with dignity. We hope that the value of the hard-earned money will preserved and increased, and the heart is full of security and happiness. We hope that the rules will be unified and transparent, the data information will be more credible, the value will be more fully circulated, and the credit can be transmitted on a larger scale in the future.

These beautiful longings are lighted as God opened a window of hope for us at the moment of encountering the block chain.



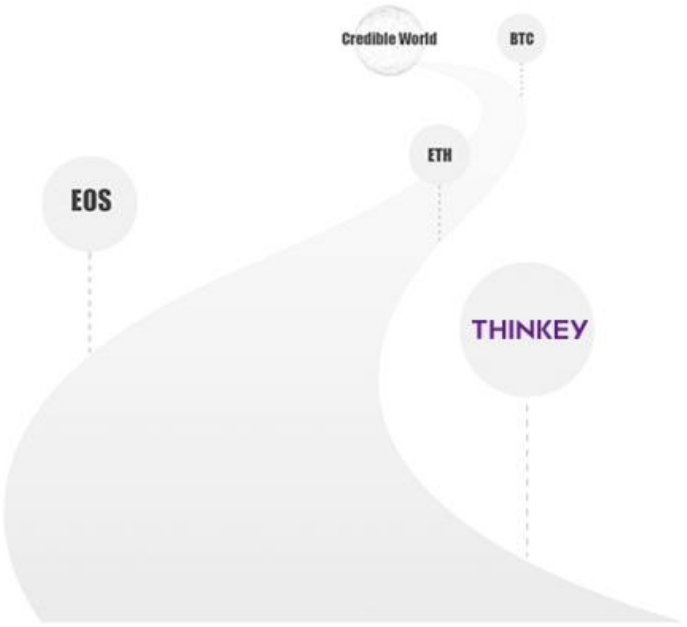
2. Olive Branch

New thought.

We have all been deeply shocked by the development model of Bitcoin, and are deeply attracted by the thoughts behind it. The block chain has brought a completely new thought to us: use technology to solve the trust problems among people. Block chain has brought a completely new operating model to us: start in a very light way, and exchange the current contributions and contributions with future value. And block chain has brought a completely new organizing method to us: open the boundary of organizations to attract more talents in creating value for ecosystem and guiding the development and evolution of ecosystem. Bitcoin is the starting point of the block chain. It is dedicated to building a credible distributed ledger system and a peer-to-peer electronic cash payment settlement system for everyone. Everyone gradually summarized and recognized the block chain's openness, transparency, unchangeable, openness and consensus features after being inspired by Bitcoin. With these advantages, people naturally want to do more things and solve more problems based on this. Ethereum proposed the concept of "smart contract" to solve more problems, with more flexibility and autonomy through writing contract code. Unfortunately, Ethereum has used Bitcoin's underlying framework logic and made some improvements, but it does not fundamentally solves the performance bottlenecks and storage bottlenecks of Bitcoin, therefore, the entire network may be blocked by large number of simple transactions, the high concurrent execution of complex tasks becomes even more impossible.

New aim

Neither Bitcoin nor Ethereum is not the final form of the block chain. If the future world is inevitable to be a trusted world, then, there will be a large number of entrepreneurs and developers who will develop various applications for the problems they find, the needs of users, and the services they want to provide. Therefore, they must need an infinitely scalable, secure, and easy-to-use platform to carry various rules, assets, data, and business logic, supporting a large number of Internet-level applications and massive users. To do this, we must jump out of the existing limitations of Bitcoin and Ethereum, and design them from a higher and longer perspective, and focusing on how to build a secure and trusted underlying technology to reconstruct whole ecosystem. This is Thinkey- core engine of trusted new world.



This engine need to support the development of a large number of decentralized ecosystem (public chain), decentralized applications (DAPPs), distributed business scenario and distributed autonomous organization.

Thinkey provides everyone with free, fair, open and just environment like the ground carries and nourishes everything that grows in the trusted world. It opens the boundaries and shoves the threshold to provides friendly participation port and interface to everyone. Respects each individual's autonomy and hobbies to enables them to participate in interested, valuable, meaningful, gaining work or creation autonomously, for small consensus is also valuable, small individuals are also branded, and small collaboration is also powerful.

New journey

In the final analysis, the blockchain solves the problem of trust. It is a “trust bond” and a “rule engine” that connects more and more parties that need collaboration or bursts emerging effect between parities that used to think that they would never cooperate with each other, however, they will establish a close relationship in the future. In the future, the “+ blockchain” will become the mainstream. The traditional business will be upgraded in a gradual or innovative way, and there will be new business models and product forms that will break out, but the starting point must be that the characteristics of the market demand are very compatible with the characteristics of the

block chain. Of course, there is still a long way to go before the large-scale penetration and application of blockchains, because the formation of consensus, the value of trusted data and the demonstration of ecosystem value will not realized immediately. Everyone who participates in the blockchain industry should have patience, perseverance, confidence, and determination, instead of eager for quick success, and dreaming of getting rich quickly. The healthy development of the blockchain must return to value and empower the long-term industry. This is a long slope with a lot of wet snow. Now it needs the wisdom and strength of everyone to roll the snowball, because we know that there is a state of mind called openness, a spirit called freedom, and a power called unity. We will eventually change the direction of the tide when we cross the boundaries of the family, the company, and the country, the vast majority of people united truly and a community of destiny grows a lot.

3. Thinkey Emerges at the Right Moment

Thinkey is the core engine of the trust new world

This engine will operate forever and support stintless business. Various rules programs that cannot be changed are running on the engine, and trust is efficiently transmitted between different subjects. The current and historical state of the engine can be verified. People and things in the physical world can have an eternal identity in the world, humans and machines (programs) collaborate efficiently in this world to change the world. Human beings constantly turn their own understandings and thoughts into algorithms or rules. People, organizations, machines (programs) efficiently collaborate to create material and ideas and perform tasks based on these rules and procedures. Blockchains continue to accumulate in the world and make the world evolve faster and faster.

3.1 Use trust to connect and drive the world

No matter how the world develops and evolves, the main theme of "trust is just needed, consensus is the cornerstone, cooperation is the driving force" will not change. Thinkey is emerging for the maximum range of trust, consensus, and collaboration. As the black chain infrastructure that can support massive application and user and face large scale commercial application, it provides convenient, friendly, efficient and secure development and deployment environment to enable all things to be on the line easily and create distributed commercial new ecosystem that connects all things and collaborate the world and uses trust to connect and drive the world.

3.2 Build the intelligent and evolved ecosystem

We can seen the underlining logic of a group of ordinary people can do extraordinary cause and the the possibility of evergreen and crossing discontinuities of organizational foundation in the development and evolution progress of Bitcoin. Thinkey will explore ways to open organizational boundaries, motivate and attract more and more members to participate in it , collaborate efficiently to form resultant. Build a benign development ecosystem that can continuously iterate forward and evolve. Become a real decentralized intelligent and evolved ecosystem through introducing "negative entropy" to solve the "entropy death" problem of the second law of thermodynamics continuously. It has strong anti-vulnerability, therefore, it can break into a butterfly

continuously until eternity in the process of continuous evolution.

3.3 Thinkey value

Core value of Thinkey: openness and tolerance, freedom and equality, and cooperation and mutual benefit.

Openness and tolerance: At the beginning of the design, Thinkey is an open, infinitely scalable, secure, and highly autonomous system. Thinkey uses the hierarchical multi-level model to be the public chain of the public chain. The ecosystem participants can not only deploy their own DAPP, deploy a customized public chain, but also deploy their own ecosystem. Its inherent inclusiveness will eventually eliminate discrimination and connect the global economy and business entities to make the world more prosperous.

Freedom and equality: The future new world will be a whole connected by blockchain, and the cornerstone of the new world of blockchain is the public chain. Blockchain is gradually transforming our information Internet to develop into value Internet. Everyone is equal in the blockchain network, and Thinkey opens an equal door to everyone. Thinkey is for everyone, it is a new world where everyone can participate, a blockchain that everyone can passes and a public chain. Freedom is the basic feature of the generalized economy. The freedom of the nwe world of blockchain new world is a higher level of freedom + self-discipline, government regulation + community autonomy, because the common scientific and technological beliefs join the new world of blockchain to achieve true freedom and equality.

Cooperation and mutual benefit: Cooperation, consensus, and win-win are the most important components of human civilization, and they are the root cause of human beings to surpass all things. Thinkey's hierarchical multi-level consensus system generates passive trust through blockchain technology, forming a non-tamperable consensus mechanism, thus achieving the highest level of trust to date—without trust and achieving ecosystem win-win.

4. Thinkey Technology

Technology is always rational and logical, and its essence is unchanged. However, in the blockchain industry, new technical terms, new concepts, and new interpretations emerges one after another. However, many of them are mystifying, confusing, and even distorting the truth to fishing in troubled waters.

The purpose and significance of establishing a trusted new world described above involves a large scope. But the current blockchain technology is still in the category of computer science. Maybe one day there is a non-computer technology that can meet the requirements mentioned above, but that is another dimension. From the digital world itself, this is currently a viable and effective mean.

Blockchain technology solves trusted problems in a distributed consensus manner, although it sacrifices real-time computational efficiency, it provides a new platform, space, and logic that centralized methods cannot bring. The trustworthiness of blockchain is bounded, and computing and storage are also obviously flawed, but it is the core of the trusted world. It needs to be integrated and enhanced by other technologies to make the trust to be transmitted on a larger scale and build a trusted new world together.

In the technology of blockchain, it is the basic requirement and foundation that decentralization is not needed to be licensed. The chain of alliances that need to be licensed has important significance and role in the whole trusted world. But we can’t attend to trifles and neglect the essentials, the public chain is still the fundamental. The alliance chain is also included in Thinkey's design, which is a simplified version based on unlicensed technology with a small scope of trust. The purpose of the cooperation between the public chain and the alliance chain is to better expand the scope of trust transmission, but this transmission is conditional.

Let's first explain the blockchain from a theoretical perspective, analyze it from the basic model, then talk about the construction of the system model, and then the design and implement the specific algorithm mechanism. We hope that the technical logic, development route, essence, advantages and disadvantages of the blockchain will be more clearly described through the system, from simple to complex, and in a simplistic way, reflecting the advanced nature, attractive charm and infinite potential of Thinkey technology.

4.1 Blockchain model

In order to understand the nature of blockchain, we define a blockchain model based on transaction firstly, quantify the parameter indexes such as security, consistency and decentralization, and propose related functions to construct a blockchain model that can be quantified.

The blockchain system $\Omega|$ is made up of five parts, including: f is consensus function, V is node set, T is transaction data set, S is message set and B is block set.

Blockchain system means the node set V writes the constantly produced transaction data set T into block set B through consensus function f and generate the system of message set S. Consensus function f, which is determined by system, includes message consensus function fs and block consensus function fb. The node set V is changed with the change of time. T represents the current time, Vt represents the node net of the system $\Omega|$ at the time of t, Vt-in represents the node net that is newly added into the system $\Omega|$ between t and t+1, Vt-out represents the node net that exit the system $\Omega|$ between t and t+1,

$$Vt+1=Vt+Vt\text{-}in-Vt\text{-}out$$

Transaction data set $T:=\{T^v \mid v \in V\}$ is changed as time changes. For any $v \in V_t \cap V_{t+1}$, T_t^v represents the transaction set that has not been processed at the time of V, T_{t-in}^v represents the message set the V receives from t to t+1. T_{t-out}^v represents the message set that has been processed from t to t+1.

$$T_{t+1}^v = T_t^v + T_{t-in}^v - T_{t-out}^v$$

Message set $S:=\{S^v \mid v \in V\}$ is changed as time changes. For any $v,u \in V_t \cap V_{t+1}$, $S_t^{v,u}$ represents transaction set at the time of V. $S_t^{v,u}$ represents the message set the V receives from u from t to t+1. S_{t-out} represents message set that will not affect consensus function after t+1. Then,

$$S_{t+1}^{v} = S_t^{v} + \sum_{u \in V_t, u \neq v} S_t^{v,u} - S_{t-out}^{v} + T_t^{v}$$

Meanwhile, the message consensus function will generate the message set send to u by V at the time of t+1: $M_{t+1}^{u,v} = f_s(S_t^v, B_t^v, u)$。

Block chain set $B: = \{B^v \mid v \in V\}$ is changed as time changes. For any $v \in V_t \cap V_{t+1}$, B_t^v represents the blockchain set confirmed at the time of V. And B_t^v meets the chain structure, block set for the time of t+1 generated by block consensus function is :

$$B_{t+1}^{v} = f_b(S_t^v, B_t^v)$$

4.1.1 Decentralization of consensus algorithm

The decentralization of the blockchain system is reflected at multiple levels, the key of which is the decentralization of consensus. The decentralization of consensus is an important difference between the blockchain system and the traditional Internet system, and an important factor in determining the democracy and security of the blockchain

Judging whether a consensus agreement is decentralized is a matter of opinion. There is no widely accepted standard at present. The decentralization has two main purpose: the structure of the system is dispersed, so that it will not be invalidated due to the dropping, rebellious or attacking of a few nodes. Consensus is done by system participants. This democracy increases the transparency and credibility of the system and prevents the system from being controlled by the oligarchy.

How much voice each participant should have in the system needs to consider two aspects: the possibility and fairness of centralization.

Blockchain is a decentralized system, and any node can be a phased center without mandatory central control functions. First, the system needs to give its weight Wvo a fair and reasonable weight evaluation system based on the computing power, system contribution or network transmission capability of the node, which can stimulate the operation of the system, improve cooperation efficiency, enhance system performance, and promote ecosystem development. For example, in Proof of Work (PoW), Wv is the ratio of the computing power owned by v, and in Proof of Stake (Pos), Wv is the ratio of the token owned by v. We use

$$W(U) := \sum_{v \in U} w_v$$

to represents the sum of the weight of the node set u in the system.

During the operation of the blockchain system, nodes in the system can profit from packaged transactions, generated blocks, or other processes. The power a_v of the node v in the system is defined as the expected profit ratio of v. In a completely decentralized system, the power of each node is consistent with his weight, then the degree of decentralization of the system Ω can be defined as:

$$\sigma := \sum_{v \in V} |a_v - w_v|$$

And the lower the $|\sigma|$ value of the system Ω is, the higher the degree of the decentralization of the system.

4.1.2 Security and consistency of the system

Blockchain is a decentralized system, there is no central node to maintain the block set B. The design of the consensus function f is that the set of maintenance blocks between different nodes is the same to achieving consistency. However, the system may have a node v, which does not follow the consensus function f to intentionally sending an error message $M_{t+1}^{v,u} \neq f_s(S_t^v, B_t^v, u)$ to u to affect the consistency of the operation of other nodes with the whole network, we call such nodes as bad nodes. Bad node set:

$$H_t = \{v \in V_t \mid \exists u \in V_t \, s.t. \, M_{t+1}^{v,u} \neq f_s(S_t^v, B_t^v, u)\}$$

If $W(H_t) \leq \eta \cdot W(V_t)$ is meet at any time of t, we call the system Ω satisfy the fault-tolerant parameter η, where W is the node weight function (see 4.1.1).Fault-tolerant parameter η, we define the efficient code set at the time of t as:

$$U_t^{\eta} = \arg \max_{U \subseteq V_t \mid W(U) \geq (1-\eta)W(V_t)} \{| \bigcap_{v \in U} B_t^v |\}$$

and the block set of the system as $B_t^{\eta} = \cap_{v \in U_t^{\eta}} B_t^{v}$. If any block $b \in B_t^{\eta}$ meet $\forall k \geq$ t+r at any time of t, $Pr[b \in B_k^{\eta}] \geq 1 - 2^{-c}$. We call that the system Ω meet the confirmation parameter τ where c is a given constant. Given parameter η, define τ as the smallest confirmation parameter that can be met by the system. The consistency in distributed systems includes: strong consistency $(\tau = 0)$, weak consistency $(\tau \leq \tau^*)$ and the final consistency $:(\tau < \infty)$. In the blockchain system, due to factors such as network delay and consensus, it is impossible to guarantee strong consistency of node data in the entire network at any time, and only weak consistency can be pursued. Given parameter τ^*, for a fault tolerance parameter η, if the system Ω meet the confirmation parameter τ^*, we call that the system Ω meet the η consistency. Thus, we define security ζ of the system Ω as the maximum fault-tolerant parameter that satisfies the acknowledgment parameters τ^*, ie

$$\zeta = \max_{0 \leq \eta \leq 1} \eta \text{ s.t. } \tau(\eta) \leq \tau^*$$

4.1.3 Performance of the system

The performance of the blockchain system mainly reflects the time required to confirm the transaction. Generally, two parameters are used to describe the confirmation time (only the time required for a transaction) and throughput (the maximum number of transactions confirmed per unit time). The confirmation time is the shortest period for the user to make a transaction. If the confirmation time of a system is very long (for example, Bitcoin takes about 1 hour), the user experience will be poor and the application scenario of the system will be limited. If the throughput is too small to handle all transaction requests, some transactions will be blocked or discarded, which will cause delays in the overall system. More generally, given a set of transactions T, define d(T) as the delay required for all transactions in T to be acknowledged, the expected value of that time:

$$D(T) := \mathbb{E}[d(T)]$$

reflects the ability of the system to deal with transactions in T, where the expected value is taken to reflect the randomness of the system and the environment. When T contains only one transaction, D(T) is the confirmation time of the system. When T contains many transactions, D(T) can reflect the throughput of the system. Unlike the single indicator of throughput, for a set T of the same size, D(T) may change (or even drastically change) according to the specific transaction contained in T. The discussion of performance makes sense only if the system is sufficiently consistent and decentralized. Therefore, the problem of improving performance is to optimize the function D under the premise of ensuring the degree of centralization $\sigma \leq \sigma^*$ and safety $\xi \geq \xi^*$ (among which σ^* and ξ^* are the constant of the system) of the system. The definition here allows us to consider the trading patterns in the actual application and to analyze and optimize them in a targeted manner.

To confirm a transaction in a blockchain system, it is necessary to ensure the consensus of all participants. In order to optimize performance, the computational complexity and communication complexity of the consensus algorithm should be improved. The classic PoW consensus mechanism requires nodes to perform a large number of additional operations to gain the right to package, which also greatly increases the computational complexity after ensuring the security and stability of the system. PoS, DPoS and some of their variants proposed later avoids the extra cost of PoW, but the nodes still need to be verified and signed, and the smart contract also increases the amount of computation required to process the transaction, and these operations are unavoidable. The communication complexity of the consensus algorithm is divided into two parts: the participants of the consensus need to reach a consensus first, and then broadcast to all the nodes of the whole network. In order to achieve security under the premise of decentralization, that is, to allow a certain number of malicious nodes in the network, each transaction needs to be verified by a certain number of nodes before being confirmed,

which requires all consensus nodes to be subject to the transaction. Broadcasting can be done after consensus is reached, for it will not affect the speed of the acknowledgment, but if there are many full nodes in the network, the bandwidth and time required for the broadcast may affect the performance of the network.

4.1.4 Efficient consensus mechanism

For a transaction set T, the delay time for the confirmation of all transactions is :

$$d(T) = h\left(d_{comp}(T), d_{comm}(T), d_{empo}(T) \mid \sigma \le \sigma^*, \zeta \ge \zeta^*\right)$$

where d_{comp} represents the delaying of consensus calculation, d_{comm} represents the delaying of consensus communication, d_{empo} represents the delaying of consensus authority assignment. σ, ζ represents the decentralization degree and security of the system, σ^*, ζ^* is the constant of the system. In order to improve the efficiency of the consensus mechanism, it is necessary to optimize the d_{comp},d_{comm} , and d_{empo} in the performance function.

1. D_{empo}, d_{empo} is mainly determined by the allocation of consensus authority.

In the current blockchain system.The methods for assigning consensus permissions mainly include: distribution based on the computing power, distribution based on equity, and distribution based on authentication, etc.

Blockchain system that distribute consensus authority on the basis of computing power. In order to ensure the degree of decentralization of the system, which enable each node to obtain the influence a_v matching its right W_v, the power proof function of $G_{work}(w_v) =$ a_v is needed. At this time, $\sigma = 0$, however, a lot of calculation is needed to obtain G_{work} and d_{empo} is a little high.

There is equity function that is easy to be calculated in the blockchain system that distribute consensus authority on the basis of equity, the G_{stake} meet $G_{stake}(w_v) = a_v$.

At this time, $\sigma = 0$, d_{empo} is a little low.

Blockchain system that distribute consensus authority on the basis of authentication need to introduce the authentication of the third party to guarantee the fair and just of the influence. This method is more suitable for the blockchain of the alliance chain type, and is not suitable for the basic public chain.

2. D_{comm} is determined by the scale of consensus node set.

In the case where the consensus algorithm is unchanged, the smaller the set of nodes participating in the consensus, the lower the amount of data that needs to be transmitted, and the lower the d_{comm}. The size of the consensus node set is limited by system security.

Assuming that the node set of the system Ω is V, the security factor is ζ, the consensus process is completed by one subsystem Ω_c, the node set of the subsystem is U, the security coefficient is ζ_U, and the proportion of bad nodes is z. At this time, the safety probability of the subsystem Ω_c is

$$Pr(z \le \zeta_U) = \sum_{i \le \zeta_U |U|} \frac{\binom{\zeta|V|}{i}\binom{(1-\zeta)|V|}{|U|-i}}{\binom{|V|}{|U|}}$$

When $|U|$ is small, although the d_{comm} is low, the probability of corresponding consensus system security has also become very low, and the reliability of the entire system has decreased.

In order to ensure the safety of the system meet $\zeta \ge \zeta^*$, the size of consensus node set meet $|U| \ge k^*$.

D_{comp}, d_{comp} is mainly determined by the computing performance of node. In the case where the consensus algorithm is unchanged. The higher the computational performance of the nodes participating in the consensus, the shorter and lower the time required to complete the consensus, and the lower the d_{comp}. In the consensus process, the computational performance of node v is e_v, and the influence of node v is a_v, then the upper limit $|e_\Omega|$ of the computing performance of the entire system $|\Omega|$ satisfies:

$$e_\Omega \le \sum_{v \in V} a_v \cdot e_v$$

It can be seen from this formula that the upper limit of the computing performance of the system can be improved by increasing the influence (a) of the node or increasing the computational performance (e) of the node.

Improve node performance: When the average computational performance of the node with influence (a) in the system is increased by m times, the upper limit of the computing power of the system is increased by ma times. Although the upper limit of

the calculation performance of the system can be improved by improving the computational performance of the influence node, due to the limitation of the Moore model, in a system with rapidly increasing performance requirements, the performance requirements of the entire system cannot be satisfied simply by improving the computational performance of the node.

Improve node influence: in traditional single-chain system $\sum_{v\in V} a_v = 1$, m branches are running at the same time through the multi-level layering method, which can greatly increase the influence of the nodes. Assume that the right of node v in the i chain is $a_{v,i}$, $\sum_{v\in V, i\in[k]} a_{v,i} = m$, then:

$$e_\Omega \le \sum_{v\in V, i\in[k]} a_{v,i} \cdot e_v$$

Even in a system with rapidly growing performance requirements, it is still possible to meet the performance requirements of the system by increasing the number of trees that are chained and reduce d_{comp}.

4.1.5 Consensus protocol stack

Based on the above theoretical analysis model, our system has designed an efficient, scalable, decentralized, secure and reliable consensus protocol stack. Specifically, the system $\{\Omega(f, V, T, S, B)|$ contains a blockchain Tree. In the Tree, the blockchain system corresponding to the non-leaf node x is a structural blockchain Ω^{st}, and is responsible for maintaining the node set and the block set of the blockchain system corresponding to all the child nodes of the x. The block system corresponding to the leaf node y is a trading blockchain Ω^{tx}, and all transaction data are consensuses on the trading blockchain.

Assuming that the number of structural blockchains in the tree is m_{st} and the number of trading blockchains is m_{tx}, then the size of the blockchain tree Tree is $m_{st}+m_{tx}$, which is dynamically adjusted as the size of the data transaction set changes.

The structure blockchain $\{\Omega_i^{st}(f^{st}, V_i, S_i, B_i), i \in [1: m_{st}]$ is responsible for consensus on the node set and block set of the blockchain corresponding to its child nodes on the Tree, where:

- F^{st} is a structural blockchain consensus function, including the message consensus functions f_s^{st} and f_b^{st}.

- Vi is the set of nodes of Ω_i^{st} that changes with time. If the system Ω_i^{st} has a parent node on the Tree and the blockchain system corresponding to the parent node is Ω_i^{st}, then, $V_i \subseteq V_j$.

- Ω_i^{st} does not contain the transaction data set, the message set Si and the block set Bi are determined by the message consensus function f_s^{st} and the block consensus function f_b^{st}.

- The block b of Ω_i^{st} contains the node set and the block set of the block chain corresponding to the child nodes of the Tree.The structure blockchain $\Omega_i^{tx}(f^{tx}, V_i, T_i, S_i, B_i), i \in [1: m_{tx}]$ is responsible for consensus the transaction data subset Ti. Where:

- F^{st} is a structural blockchain consensus function, including the message consensus functions f_s^{tx} and f_b^{tx}.

- Vi is the set of nodes of Ω_i^{tx} that changes with time. If the system Ω_i^{tx} has a parent node on the Tree and the blockchain system corresponding to the parent node is Ω_i^{st}, then, $V_i \subseteq V_j$.

- Ti is the transaction data set of Ω_i^{tx} and meet:

$$\bigcup_{i \in [m]} T_i = T \quad \text{and} \quad T_i \cap T_j = \emptyset, \forall i, j \in [1: m]$$

Therefore, in any transaction that $t \in T$, t can only be consensus for one time.

- The message set Si and the block set Bi of Ω_i^{tx} are determined by the message consensus function fsst and the block consensus function fbst.In the following, we prove that the Thinkey system Ω satisfies the decentralization parameters σ^*, and the performance of the system does not decrease with the increase of the number of system nodes |V| and transaction data|T|.

- The transaction data set T is split into several subsets T1, T2, ..., Tm, and then consensus is made by m transaction blockchains.

- All consensus calculations are delayed , when the number of trading blockchains grows and the size of the transaction data set grows substantially the same, dcomp is constant.

- The node set Vi of the transaction blockchain Ω_i^{tx} and the influence $a_{i,v}$ of the node are determined by the block set Bj of the blockchain system Ω_i^{tx} corresponding to the parent node on the Tree. The influence distribution function $G(v) = \{a_{i,v} | i \in [1:m]\}$。 can be calculated at constant time by using a verifiable random function. Therefore, the delay in the allocation of consensus permissions is $d_{empo} = O(1)$. When the size of the system node (|V|) increases, d_{empo} is a constant. Select the child node set in the transaction blockchain through the influence of the node to carry out consensus process. Then, broadcast it to the node set Vi of Ω_i. At this time, the

- delay of the consensus communication is $d_{comm} = O(|U|)$. When the size of the selected child set of the noe is a constant, d_{comm} is a constant.

  - The constant time influence distribution function G of the Thinkey system satisfies

$$\sum_{v \in V} \left| \frac{1}{m} \sum_{i \in [1:m]} a_{i,v} - w_v \right| \leq \sigma^*$$

- Therefore, the system Ω satisfies the decentralization parameter σ^*.

4.2 Trusted distributed computing platform

From a system perspective, a blockchain is a trusted distributed computing platform that can act as a shared computing resource. Customers can view this platform as a new-generation computing facility. They send any request to them. When the platform receives the request, it first checks its legitimacy, then processes the request on some nodes and returns the result to the client. Through this process, data and messages are transmitted on the platform, managing compute nodes and resources in a distributed manner. In particular, an effective blockchain design should have the following attributes. (a) Safety: all results shall be correct. (b) Liveness: each valid request is processed in a fixed (small) time. Here, we assume that the platform has a unified trusted interface that allows clients to send requests and receive results. In addition, a consensus protocol is required to ensure that the same content is run on different compute nodes.

The most relevant classic model is state machine replication. However, unlike the SMR model (requires licensing [9]), the blockchain platform allows any node to join without obtaining the permission. In the setting of permission-less, nodes are untrustworthy, which introduces a challenging problem called as “Sybil attack”. In “Sybil attack”, an attacker can generate a large number of compute nodes, and then easily control most compute nodes to reach a consensus. To prevent Sybil attack, a common method is to use Workload Proof (POW) [8] or Proof of Equity (POS) [6].

In our technology-related white paper, the system model is described. Qualitative analysis is carried out from the aspects of consistency, reliability and security, scalability, etc., and a framework for analyzing the scalability of the blockchain system is proposed.

4.2.1 Scalability

Where T and Q represent the throughput and quality of service of the system, respectively. S represents the overall cost of the system, including node costs, network broadband costs, and so on. For the blockchain, its Q is mainly determined by the average confirmation time d and the target confirmation time d. In order to normalize Q to (0,1) interval, we set $Q = \frac{\hat{d}}{d+\hat{d}}$. When $d \to \infty$, Q=0; when $d \to$, Q=1.

Given the initial configuration C, we can extend the configuration of the system to Ck

by scaling factor k. The policy σ specifies how to expand the configuration. For example, when the initial configuration C has n nodes and the policy increases the number of nodes to k, the number of nodes in the configuration Ck is equal to k*n. Then we can calculate the scalability quantitatively:

$$\psi_\sigma(k) = \frac{F_{C_k}}{F_C}$$

If $\psi_\sigma(k)$ is equal to 1 or monotonically increases as k increases, we say that the system has perfect scalability under strategy σ .

4.2.2 Scalable strategy and assessment

The scalability of the system is based on the expansion strategy a. There are two ways to improve system performance. One is by increasing the performance of each node, and the other is by increasing the number of nodes. Similar to Amdahl's law [1] [4], which is the formula for calculating the theoretical acceleration of distributed systems, we have defined the acceleration of the blockchain system. Suppose we use k times of budget to build the platform, some parts of it is used to improve the performance of each node, and the other to increase the number of nodes. Here we assume that all nodes are the same. We use r times of the budget to improve node performance and it can increase the performance by f(r) times. The function f(r) can be any function. Due to hardware limitations, we usually set $f(r) = \sqrt{r}$ or log r.

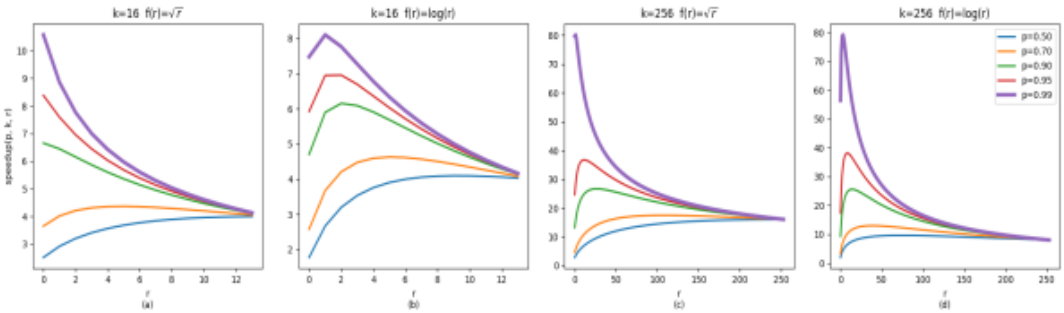
Then, the number of nodes can be expanded by $\frac{k}{r}$ times. For request set A, it is assumed that the proportion p part can be processed in parallel, while the remaining 1-p part functions are serialized (for example, p=0 in Bitcoin). Then the acceleration ratio of the entire system can be expressed as:

$$\text{Speedup}(p, k, r) = \frac{1}{\frac{1-p}{f(r)} + \frac{p \cdot r}{f(r) \cdot k}}$$

The metric $\psi_\sigma(k)$ can be approximated as：

$$\psi_\sigma(k) \approx \text{Speedup}(p, k, r)/k.$$

As shown in the following figure, a larger p-value results in higher acceleration, and the design of the block system should focus on supporting more parallelism through architecture and protocol design.



Acceleration corresponding

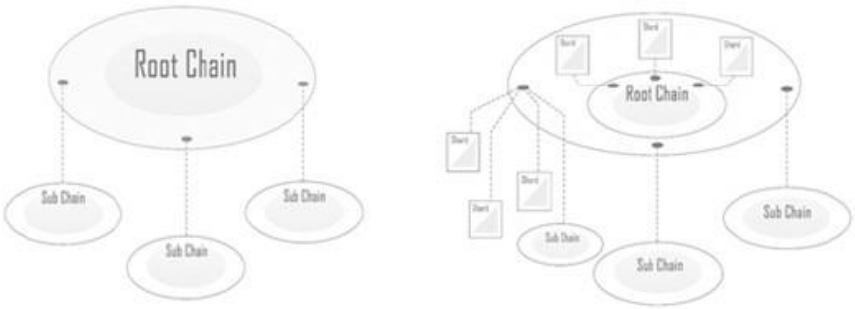
(a) $k = 16, f(r) = \sqrt{r}$, (b) $k = 16, f(r) = \log r$, (c) $k = 256, f(r) =$

$\sqrt{r}$ 和 (d) $k = 256, f(r) = \log r$。

4.3 Thinkey architecture

4.3.1 Hierarchical multi-level chain structure

From an implementation perspective, our chain structure is a hierarchical multi-level chain structure.



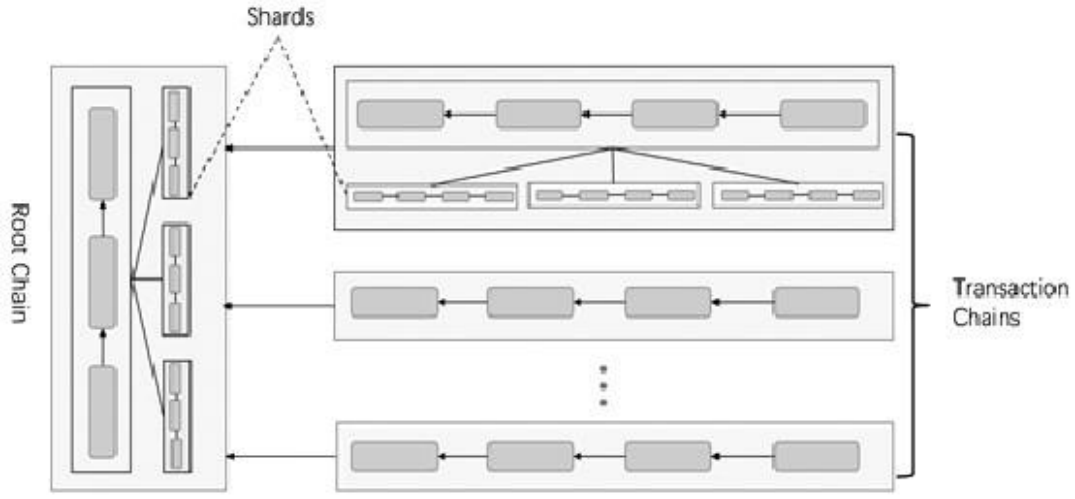
Thinkey's chain is divided into two main functions: the main chain and the business chain. Each chain is a complete system with its own state. The main chain acts as the leader and coordinator of the entire system. It serves as the entry point of business chain and source of trust, recording the metadata and summaries of the identified blocks for each business chain, and generating random seeds for use in committee elections for all chains, and record the election results. At the same time, the workload from the business is shared by all the business chains, and the contract-based parallel computing is performed by using the message-driven protocol based on the Actor model. All nodes in the system maintain the state of the main chain. The node can verify any block data of the service chain already included in the main chain by updating and verifying the blocks of the main chain. This structure has the following main advantages:

1. Nodes only need to obtain the current state of the main chain from the trusted source when joining the system, or rebuild from the Genesis block without synchronizing all the data of the entire system, which greatly reduces the load of the entire system.

2. The consensus of each chain is performed independently and in parallel, which greatly reducing the requirements for network bandwidth and computational processing.

3. The main chain acts as a coordinator for the system, providing cross-chain synchronization and allowing the entire system topology to be dynamically adjusted.

4. Nodes can use the digests in the main chain and Merkle certificates to verify transactions initiated from another business chain. Therefore, the block generator of the service chain does not need any information from other service chains to handle inter-chain transactions.



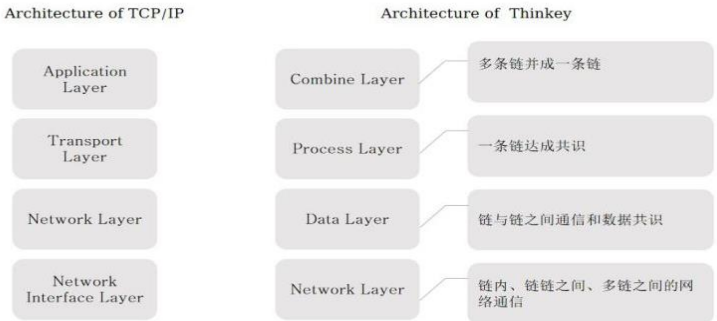
We can separate different business chains to run separately according to different transaction types or business entities. They can operate independently and conduct cross-chain communication by the evidence provided by the main chain. Or they can form a dependent parent-child relationship chain, where the sub-chain inherits the attributes of the parent chain. For example, the currency type of the account balance on this chain, the election method of the chain, and the like.

This relationship is logically related, it has a direct impact on the attributes of the chain and the network connection, which makes it easier to exchange data between the sibling chains. Thinkey's design principle is to allow each business chain to expand its own sub-chain downwards, but in actual use, the problem can be solved basically within three layers.

Whether it is the main chain or the business chain, there may be congestion when there are too many requests. When congestion occurs, the request can be spread over different fragments by sharding the chain to improve the throughput capacity of the chain. As the number of shards increases, the throughput linear of the chain increases. The shard itself is also a chain that runs independently, and there is an optimization between the shards for cross-slicing transaction requests, which greatly improve the execution speed of cross-chip transactions between the segmentation chains. This hierarchical multi-level structure is flexible and scalable, and can be dynamically adjusted. Therefore, each chain will not become a performance bottleneck for the entire network. In addition, as the number of chains increases, the throughput linear of the entire system increases without generating too many redundant messages.

4.3.2 Four-layer system structure

Based on the hierarchical multi-level chain structure above, we designed a four-layer implementation framework from a system perspective to facilitate the future scalability and upgrade of the system.



The first layer is the integration layer, which mainly solves the overall consensus of the whole system. It is mainly responsible for dividing requests and nodes, and assigning different requests to specific committees for processing. All requests are firstly sent to the integration layer where they will be split and assigned to different committees for parallel processing. They need to be partitioned according to their type since not all requests can be processed in parallel. In addition, all active nodes are registered at the integration layer. These nodes are divided into different committees in a random manner and are assigned with different requests. We need to make sure that each committee is credible, that is, the proportion of malicious nodes within each committee does not exceed a certain threshold set by the system.

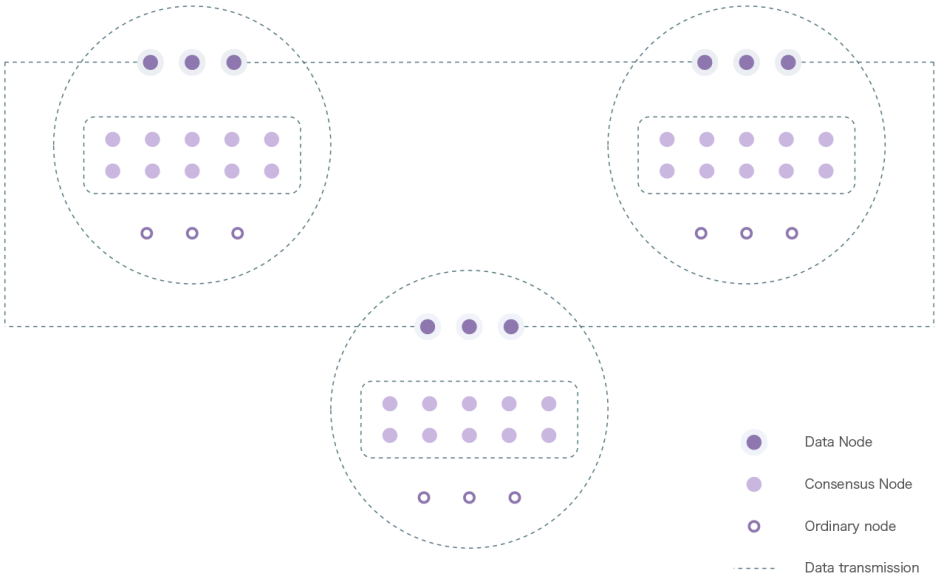
The second layer is the processing layer, which mainly solves the single-chain consensus problem. It needs to solve the assigned request and generate a log. Each committee contains a set of nodes, and when the committee receives a given request, it needs to process the request, reach a consensus, and generate a log. This layer only needs to consider how to reach consensus in the committee as soon as possible since the credibility of each committee is guaranteed by the upper layer.

The third layer is the data layer, which mainly solves the consensus among multiple chains. The logs and request data generated by each committee are aggregated according to specific coding methods to form a single log. The goal of the system is to generate consistent log for each code. Therefore, an aggregation algorithm is needed to be used to integrate all the logs generated by the nodes in the committee and reach the unified log. Coding methods are also needed to reduce the storage of each node. In addition, the corresponding data from the data layer must be synchronized since nodes will join and leave the committee from time to time.

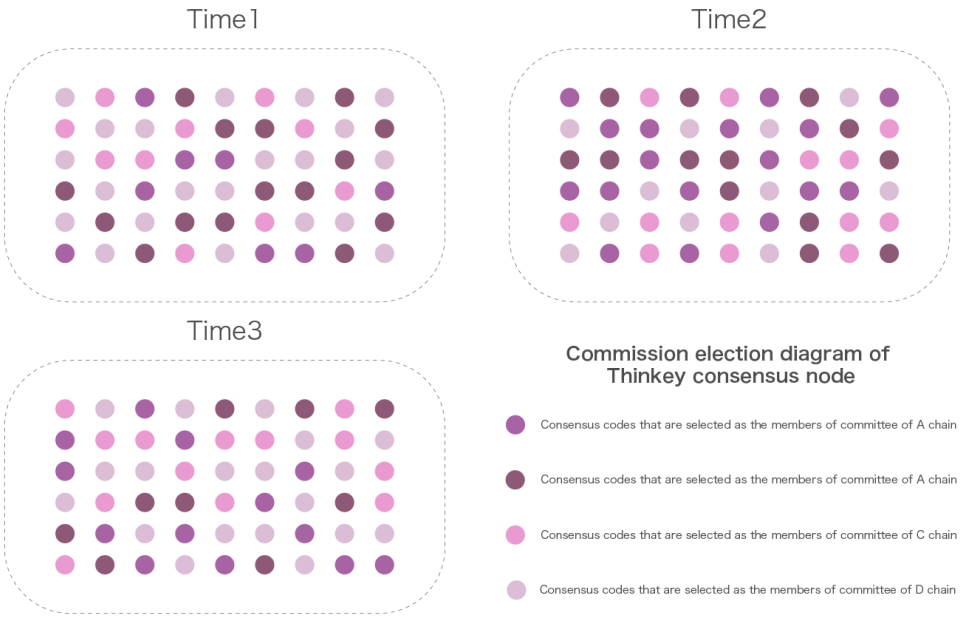
The fourth layer is the network layer, which mainly solves the communication between different attributes and task nodes. This layer is the basis of the entire system that establishing communication between compute nodes. Within the network layer, we can build a multi-layered network and build a consensus network layer for each committee.

4.4 Thinkey consensus protocol

In Thinkey system, there are three types of nodes in each chain: data nodes, consensus nodes and common nodes. The data node is responsible for the storage of all the data in its chain and the interaction between the chain and the chain. The main responsibility of the consensus node is the operation, packing and consensus of the chain, and the common node only carries the service. The figure below shows the relationship of different nodes between multiple chains.



Each participating consensus node is randomly assigned, and will be re-selected as time goes by, as shown below:



4.4.1 Committee selection

To counter the Sybil attack on unprivileged systems, we use a Proof of Equity (PoS)-based election algorithm. Early blockchain projects such as Bitcoin and Ethereum used Workload Proof Consensus (PoW). Consensus participants compete for the bookkeeping right through the "mining" (that is, to carry out some specific complex calculations). Mining requires a lot of power and takes up a lot of computing time, but these resources do not contribute to improving the efficiency of the system. In fact, because the confirmation of a transaction requires the reception and verification of most nodes across the network, the time spent in broadcasting information on the network also increases as the number of nodes increases, and the efficiency will decrease.

In addition, if the consensus algorithm requires each transaction to consume bandwidth, computation, and storage resources for each participant, the performance bottleneck of the system will depend on the weakest participant in each dimension. In this case, the nodes participating in the consensus should only be the "super nodes", which form centralization in fact.

Therefore, we have chosen a consensus mechanism based on proof of interest (PoS). In the PoS mechanism, the consensus participants' billing rights depend on the assets they own.. In our consensus algorithm, consensus participants prove their rights by submitting a deposit. The system regularly selects a certain number of participants through a random algorithm, according to the proportion of the deposit to form a committee responsible for a period of time. In the multi-chain system, the committees of each chain can exist at the same time and run independently of each other since only the selected committee members need to participate in each block. As the number of nodes in the network increases, it is possible to support running more sub-chains at the same time to utilizing the resources of the nodes efficiently.

Compared with PoW, PoS consensus does not need to be excavated, which greatly reduces the threshold for participation in consensus and energy consumption, and is more likely to achieve true decentralization. On the other hand, unlike DPoS's super node, the committee is randomly elected, which guarantees fairness and gives everyone the power to participate in the block and get rewards, and also prevents the various problems caused by the monopoly of super code. Similar to PoW, the security of the PoS algorithm only needs to assume that most of the rights are not malicious and the network satisfies weak synchronization.

The selection algorithm requires the following security attributes

- Assume that the proportion of equity in the honesty node among all participants is δ_0 .

  At least the proportion δ_1 of committee members elected in each election is honest. In addition, the algorithm should be fair because the probability that each participant is selected (roughly) is proportional to the number of shares invested by the participants.

- Committee members should be mobile and unpredictable so that opponents cannot attack the system through corrosion committee members (assuming that corruption takes longer than the committee's life).

In Thinkey, we implement the above properties through the following process. First, when the next committee needs to be selected, the sub-chain must send a singal on the main chain for all nodes are listening to the main chain.. The election of all chains is carried out in the main chain. Through the summary information on the main chain, the main chain can collect the election status of each chain and publish it in a unified manner. At the same time, random seeds are generated periodically on the main chain to ensure the randomness of each chain election.

Nodes that are willing to participate in the consensus need to register on the main chain by sending a special type of transaction. The transaction also stipulates the equity amount, which will be transferred to a specific share account and frozen, instructing the node to withdraw and withdraw the equity.

After the main chain issues the election information, the consensus participants can see the election information in the main chain, and use the corresponding random seed and their private key to calculate the value of a verifiable random function to determine whether they are selected. When a node finds itself having the right to join a chain committee, it will join the chain's network firstly and send its own ID and verifiable random function proof, which will be recorded by the current committee. At the same time, new members of the committee need to prepare for participation in the consensus and join the committee's network. They also began to synchronize the state of the sub-chain. The received block and status can be verified by the abstract on the main chain.

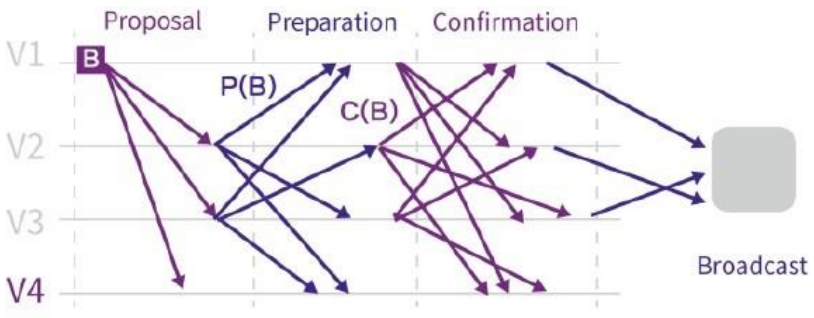
The elected nodes will establish a small consensus network for communication within the committee. The owning of dedicated network reduces latency and bandwidth consumption for peer-to-peer communication and broadcast between committee members. On the other hand, if the set is incorrect, the network may be less stable and more vulnerable to attack. You need to make sure your network topology is robust and securely exchange node information through using encryption. At the beginning of the next era, the new committee should generate a new key, synchronize and update the

current state of the chain, and establish a connection in the new consensus network.

The fairness of the election is crucial to the security of the system: if the attacker can occupy a majority of seats in a committee, there is no way for the committee to come out normally. On the one hand, in order to ensure that random seeds cannot be manipulated, each random seed is generated by a set of members of the committee through threshold signatures: This approach greatly increases the difficulty for an attacker to predict subsequent random seeds and prevent random seed generation, as compared to random seeds independently generated by blocker. On the other hand, we have designed incentives that make honest committee members willing to record new committee members, rather than seeking to retain their powers by destroying elections.

4.4.2 Committee's consensus

We assume that there is a part of the synchronous communication model within the committee, in which there is a valid Byzantine fault-tolerant algorithm, and a tailor-made PBFT variant is designed for this purpose. The committee only accounts for a small portion of the entire network, and they will build a smaller network to reduce the delay of the broadcast, so they can get out of the block stably and efficiently. Due to the nature of the PBFT algorithm, when the nodes in the committee satisfy the weak synchronization hypothesis, the block algorithm can run safely when the malicious nodes accounts for less than 50% of the nodes. Therefore, under the premise of the security of the election algorithm, the activity, correctness and uniqueness of each committee can be guaranteed. In addition, our deposit and penalty mechanisms make it costly for members of the committee to do evil, which encouraging honest users to refrain from doing evil by reporting other people's malicious behavior.



The execution of nodes can be divided by rounds. Each round consists of three phases: proposal, preparation and confirmation (as shown in the pictured above). State transitions are driven by event. In order to keep the system active in the event of a network failure or malicious attack, the local clock may trigger a timeout.

Proposal stage: The person in charge of the committee broadcasts the proposed motion to other committee members.

Preparation phase: After each committee member receives the suggested block, it broadcasts a message containing the signature of the block.If a timeout is triggered before the suggested block is received, the committee members sign and broadcast a special message to the other committee members (indicating that the leader is defective).

Confirmation phase: At the end of the preparation phase, each committee member signs and broadcasts a signature received during the preparation phase. Signature aggregation can be used to reduce the size of messages in the validation phase significantly.

Based on the messages received during the validation phase, each committee member can decide whether an agreement has been reached on the block and to broadcast the agreed block or empty block and the evidence of making such decision. Malicious node punishment. In the case of detecting a node with a definite misbehavior (for example, a node that sends a different message to a different node at the same stage), the round will be aborted by outputting an empty block. However, misbehaving nodes will be subject to a large number of economic penalties, which make this attack unsustainable. Optimization. If the number of signatures received during the preparation phase means that most honest committee members have received the same proposal block, committee members may reach an “early consensus”: members can use the signature to output the block as proof of the protocol before the validation phase (in different forms compared to conventional protocols). Please note that the node still needs to participate in the validation phase.

4.4.3 Safety analysis

Let N be the number of nodes, n be the number of nodes expected in the committee, and m is the number of committees. The number of malicious nodes is N. When the node in the committee that exceeds the proportion p is a malicious node, we will say that the committee election is failed. Without loss of generality, we set N=n*m. Suppose there is a completely random $\text{oracle } O: [N] \to [m]$. Fixed a committee that defined Ai as the event of the proportion i>p of malicious nodes in the committee. Then, for each $i \in [m]$, we have

$$Pr[A_i] = \sum_{x=\rho n+1}^{n} \frac{\binom{\lambda N}{x} \cdot \binom{(1-\lambda)N}{n-x}}{\binom{N}{n}}$$

We can get through the union bound

$$Pr\left[\cup_{i\in[m]} A_i\right] \leq m \cdot Pr[A_i]$$

We can ensure that the probability of an event occurring is negligible by setting the appropriate parameter settings.

4.4.4 Cross-chain message and verification

In a multi-chain system, cross-chain operation is unavoidable. Each chain needs to process some messages generated by other chains. There are two kinds of cross-chain messages in our system. The first one is the message mi from Ci to CR which contains the summary of the Ci block. There are two types of cross-chain messages in our system. The first is the message mi from Ci to CR which contains a summary of the Ci blocks. The message mi is used for the confirmation of the Ci block, and each block has only one such message. The second is the external relay message $m_{i,j}$ from Ci to Cr. $m_{i,j}$ will be recorded on Ci blocks before it is sending to Cj.

Before we can process these messages, we should verify them first. There are two types of verification for the messages of the chain: (1) verify the signature, and (2) verify the message hash. Both methods are useful and the use of them is depending on the type of message. The message mi from Ci to CR attaches the signature of the Ci committee member and can be used to verify authenticity. Since the members of the Ci committee are recorded in CR, each node of CR has the public key of the current committee member of Ci, and can verify the signature of mi.

Messages $m_{i,j}$ from Ci to Cj has verifiable proof . It is recorded on the block of Ci before $m_{i,j}$ is being sent to Cj. On the block of Ci, there is a Merkel tree Ti for recording all external relay messages. Proof refers to the hash value of all sibling nodes from the Merkel root to its entry path. The root hash of Ti is included in the summary of Ci. Since the summary of Ci is recorded in the main chain CR , and each node in Cj is also a node in CR , each node in Cj can obtain the root hash of Ti and pass the proof. The reason for not using signature verification is to prevent situations where members

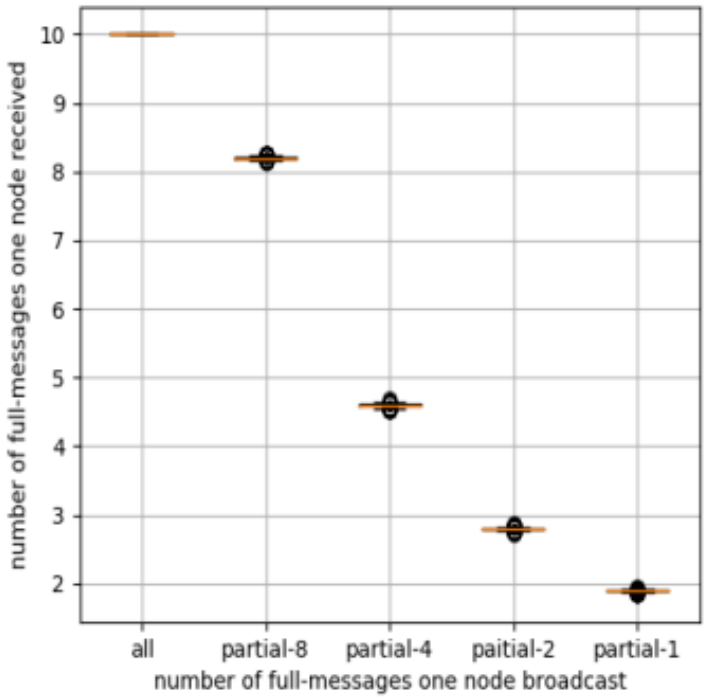
of the Ci committee are not completely reliable. Messages generated by this block will only take effect if their block is finally confirmed by CR. However, for cross-sliced messages of the same sub-chain Ci, the verification speed may be faster, and it is only necessary to wait until the digest is recorded on its sub-chain Ci rather thabn the main chain CR.

4.4.5 Network algorithm

As a bottleneck of high-throughput blockchain, P2P technology has attracted more and more attention as a potential technology for blockchain networks. In the blockchain, efficiency and redundancy are key issues that must be paid attention to in all blockchain P2P network designs due to a large amount of data broadcasting operations is required.

Traditional blockchain P2P networks (such as Bitcoin and Ethereum) are often based on non-structural design ideas. At the time of broadcasting, some broadcaster manufacturing is suitable for alleviating message redundancy problems. For example, when broadcasting a large message M, the node P randomly selects some of the nodes in the connection list for full transmission. For the remaining nodes (eg, Q), only M's configuration file (eg, a hash of M) is sent.

It only extracts messages from P when Q needs message M and cannot find it in its own database. In the experimental part, we proved that the design can significantly reduce the redundancy of message transmission by comparing several sets of parameters. However, this solution still has limitations. For example, under a structured P2P network, the requirements for high throughput and point-to-point transmission will become insufficient. In this case, a structured network (such as DHT) is a solution that can be used for further optimization. The node follows some rules during the network phase (for example, Chord [11], Kademlia [7]). This provides directional guidance for data transfer, which can greatly reduce the number of useless transfers. However, in blockchains, especially in public chain projects, there are assumptions that nodes can join and exit arbitrarily. Frequently replaced networks will result in significant cost of structural maintenance. Therefore, one of the challenges of adopting a structured P2P network is to deal with the instability and uncertainty of complex networks. In Thinkey, we use a combination of structured and unstructured methods. In some scenarios (such as point-to-point transmission), we use structured P2P network methods to reduce redundancy and increase efficiency while at the same time unstructured transmission as a guarantee of stability.



The figure above shows the impact of some broadcast mechanisms on reducing message redundancy. We assume that each node is randomly connected to 10 nodes. The horizontal axis represents the amount of complete information received by each node when the node sends complete information to all 8, 4, 2, and 1 neighbors. We calculate the redundancy of the network as it expands from 100 nodes to 1000 nodes for each case. And we can seen that:

- When the number of complete message broadcasts is reduced, system redundancy can be significantly reduced. When a node broadcasts a complete message to only one neighbor, each node receives only the same complete information less than twice.

- When the number of neighbors connected to each node is constant, the amount of redundancy is independent from the size of the network.

4.5 Thinkey multi-chain parallel model

For multi-chain systems, current single-chain system account models (eg, UTXO or Ethereum accounts) are no longer adapted to new requirements, especially when dealing with large numbers of cross-chain operations. We have designed a new account model that allows us to implement complex logic on a multi-chain system in an asynchronous and lock-free manner. In this model, we split the transactions involving a group of accounts into multiple steps in the form of messages. Each message is received by a unique subject

and executed by the corresponding chain.The transaction is finally implemented after all the messages are executed.

4.5.1 General parallel model

There are many mechanisms in parallel computing, including stand-alone local computing, distributed network computing(such as locking, etc.), but these are very poor or not applicable to the multi-chain parallelism of blockchain. We have analyzed the Actor model (proposed by Hewitt et al. [3] in 1973,which is a conceptual model for dealing with concurrent computations) in depth. It is combined with many scenarios to design new parallel applications, such as some email systems, Web services, and objects with locks in Java, etc.

An Actor refers to a basic unit of computation. It can receive a message and perform calculations based on it. Its important feature is that Actors are isolated from each other, they do not share memory with each other, each Actor maintains a private state that cannot be changed by another.

When receiving a message, the computing unit can simultaneously:

1. Sending a limited number of messages to other computing units.

2. Create a limited number of new computing unit.

3. Specify the behavior to use when receiving the next message.

The actions mentioned above have no assumed order and they can be executed in parallel. Each computing unit can receive messages from other computing units. Messages are sent asynchronously to the computing unit, and each computing unit processes the messages in order, ans there is no restrictions on the order in which the messages arrive. Multiple actors can be run simultaneously.

4.5.2 Thinkey parallel model

We design a parallel model based on Actor as our basic framework. In Thinkey, the structure mainly contains the following information:

Address: the unique identifier of the blockchain account.

Balance: current balance of the account.

Nonce: a scalar value equal to the number of external messages sent from this address.

Code: the program logic that process the information.

Storage: The internal status of the account, which can be empty.

Each account is controlled by a private key. In the code, the account defines its own processing for the messages it receives, which allows it to send messages to other accounts, create new accounts, and mody internal states. For some specification messages, each account has the same general handling method (such as "tran" and "add"). Each account can also customize the way other messages are made.

There are two types of messages: external messages and relay messages. External messages are created by an account that is signed with a private key. The relay message is generated by the account that executes the send command during execution, which is similar to the message in Ethereum. The biggest difference is that the execution of relay message is asynchronous in our model and is synchronous in Ethereum. Therefore, these messages in our model support cross-chain propagation.

The messages in Thinkey mainly contain the following information:

1. From: The sender's address.

2. Recipient: The recipient’s address.

3. Nonce: The scalar value is equal to the number of external messages sent by the sender, and is null for the relay message.

4. Input: Specify the input data set called by the message.

5. Verification data: A signature that identifies the sender's external message, or a certificate that relays the message.

You can verify the external message by signing and nonce and verify the relay messages by evidence.

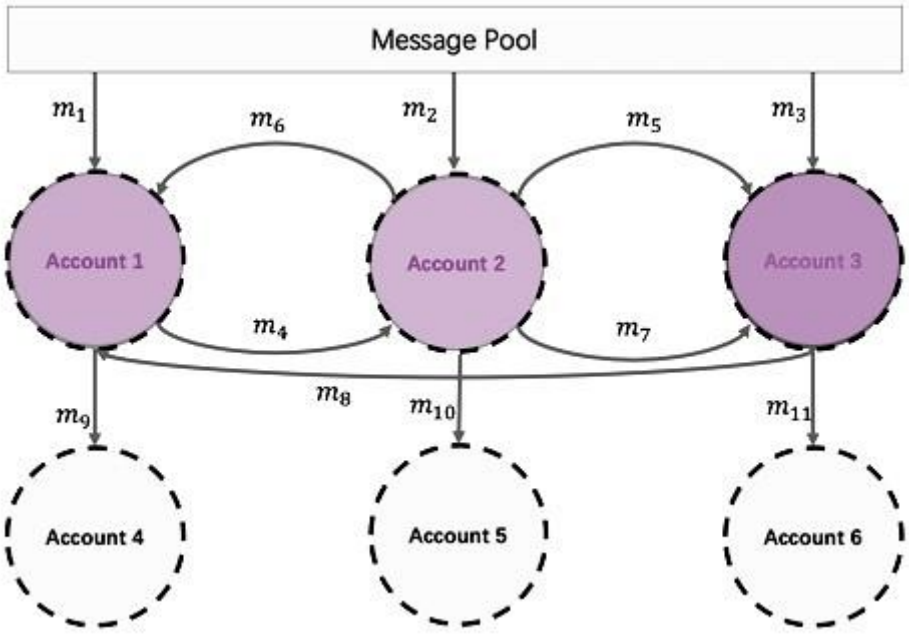
4.5.3 Blockchain calculation based on parallel model

In our parallel model, there are three types of message for each block on chain C:

- Imputing message. These messages are currently unconfirmed, and the recipient accounts are all on chain C, they can be external messages or relay messages generated by other chains.

- Internal relay message. These are the relay messages generated during the execution of the entire block, and the receivers are also located on the C chain, therefore, they can be confirmed on this block.

- External relay message. These are the relay messages generated during the execution of the entire block, and the receivers are located on other chains, therefore, these messages shall be confirmed by other chains.



The following shows an example shown above. There are three accounts 1, 2, 3 on the C chain, and three accounts on the other chain 4, 5, 6. In particular, there are three input messages (ie m1, m2, m3) received by accounts 1, 2 and 3 respectively.

For each account i, we use σ_i to represent the order in which the messages are processed and the message is generated. Therefore, we have

$$\sigma_1 = (m_1 : m_4 \mid m_8 \mid m_6 : m_9)$$

$$\sigma_2 = (m_2 : m_5, m_6 \mid m_4 : m_7, m_{10})$$

$$\sigma_3 = (m_5 : m_{11} \mid m_3 : m_8 \mid m_7)$$

Therefore, σ_i represents the account processes the messages m1, m8 and m6 in order. The internal relay message m4 is generated by processing m1, and the external relay

message m9 is generated by processing m6. Then, we have the internal relay message set $\{m_4, m_5, \ldots, m_8\}$ and the external relay message set $\{m_9, m_{10}, m_{11}\}$.

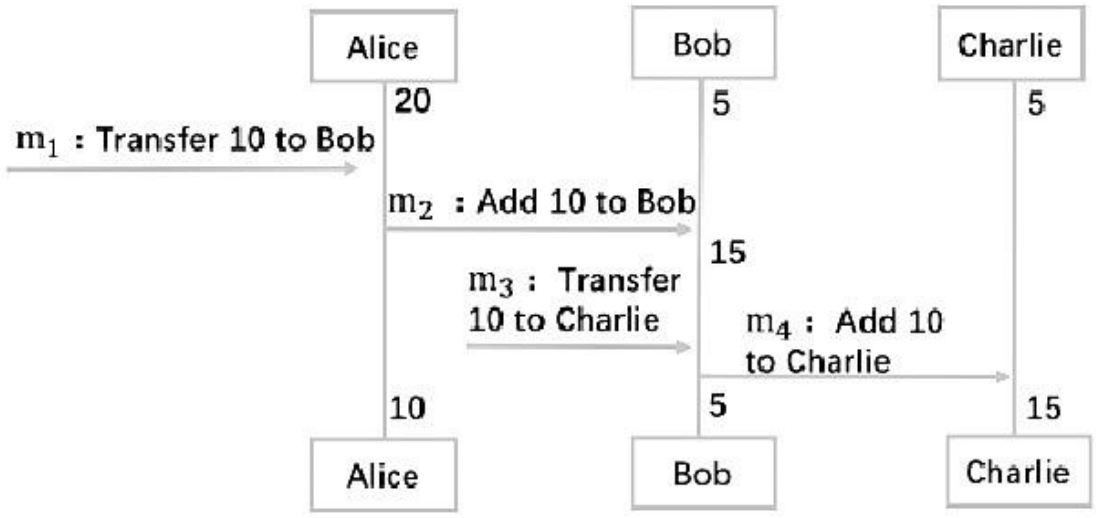
When receiving the block proposed by the responsible person, the members of the committee need to verify to prevent malicious persons. In our system, the node verifies three parts:

The validity of each input message, that is {m1, m2, m3}.

Validity period for the processing of each account, that is $\{\sigma_1, \sigma_2, \sigma_3\}$. And the verification can be conducted independently.

Validity of the order of processing message, that is the order $\sigma = (\sigma_1, \sigma_2, \sigma_3)$.

In order to verify the order of the processed messages σ, we create a directed graph Ga. For two events e1 and e2, e1-e2 indicates that e1 occurs before the e2. Assume that $\overrightarrow{m_i}$ represents that the account of the event (i) has received message mi, $\overleftarrow{m_i}$ represents that the account of the event (i) has sent the message mi. The, we have $\overleftarrow{m_i} \rightarrow \overrightarrow{m_i}$ for each σ_i. For example, when i=1, we have $\overrightarrow{m_1} \rightarrow \overrightarrow{m_8} \rightarrow \overrightarrow{m_6}$. We can create a directed graph Ga on the basis of these relationship of σ.



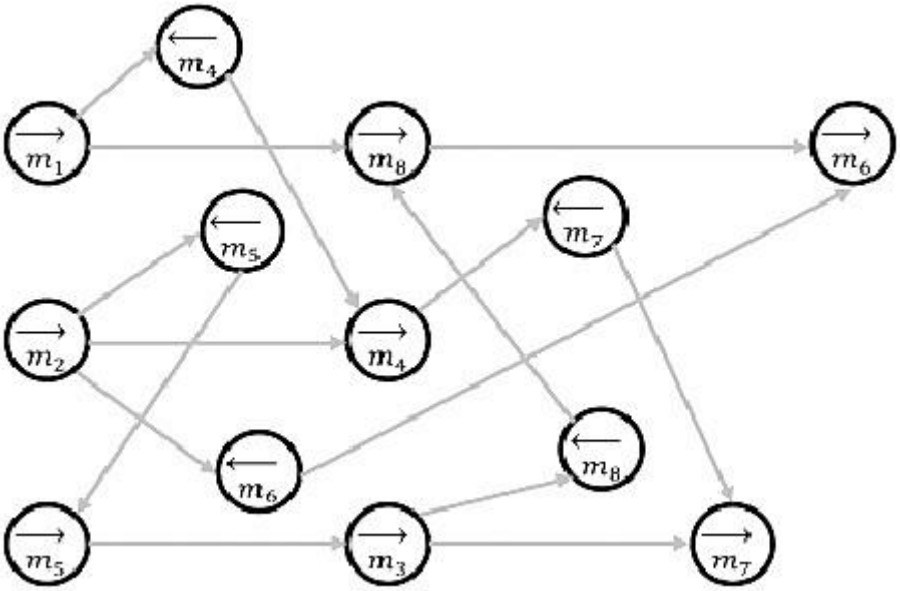
Theorem: The order of processing messages $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is valid only if the directed graph Ga does not exist bad.

4.5.4 Payment application

The following is an example of a payment process based on our model design. We define the local state of an account, called the balance (see the following text). There are two types of message, “tran” and “add”, which represents withdrawn and deposit respectively.

```
1: balance
2: while receive message m do
3:    if m = {: tran, address, bill} then
4:       if balance ≥ bill then
5:          balance = balance − bill
6:          send (address, {: add, bill})
7:       end if
8:    else if m = {: add, bill} then
9:       balance = balance + bill
10:   end if
11: end while
```

In the above algorithm, we wrote a simplified example code describing the payment process in Elixir [12].



As shown in the picture above, we demonstrate the process as an example. Suppose there are three accounts, Alice, Bob and Charlie, with a balance of 20, 5, 5 respectively. Two messages m1 and m3 are signed and issued by Alice and Bob. Message m1 is a transfer of10 from Alice to Bob and m3 is a transfer of 10 from Bob to Charlie. Then, according to the code message m1, it is processed on Alice's chain as follows:

1. If the signature of m1 is valid, then the committee member of the Alice chain will package this unconfirmed message m1 when generating a new block.

2. When Alice's balance is less than the transfer amount (ie, the fourth line in the above algorithm is satisfied), and Alice and Bob belong to the same chain, the committee member records the message processing $\sigma_a = (m\ 1 : m_2)$ in the block. This means that processing m1 produces m2 (line 6 of the above algorithm). At the same time, message m2 is marked as an internal relay message and is executed on the block. In this case,10 is deducted from Alice's balance (line 5 of the above algorithm) and 10 is added to Bob's balance i (line 9 of the above algorithm).

3. When the 4th line in the algorithm is satisfied, and Alice and Bob are from different chains, $\sigma_a = (m\ 1 : m_2)$ is also marked on the chain. At the same time, the committee member marks m2 as an external relay message on the block and sends m2 to the destination chain, Bob's chain. n this case, Alice's withdrawal operation (line 5 of the above algorithm) is executed. The external relay message m2 will be executed in the same way in Bob's chain.

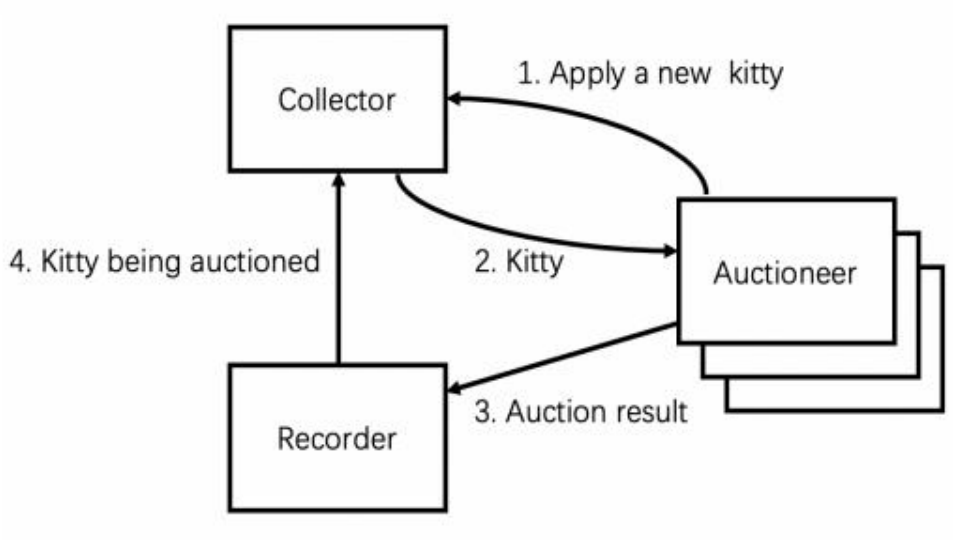
4. When Alice's balance is less than the transfer (that is, the fourth line of the above algorithm is not satisfied), $\sigma_a = (m_1 : \emptyset)$ is recorded on the block. In this case, the balance of Alice and Bob will not change.

For each account i, we use σ_i to represent the order in which the messages are processed and the message is generated. Therefore, when the three accounts are on the same chain, we have $\sigma_a = (m_1 : m_2), \sigma_b = (m_2 \mid m_3 : m_4), \sigma_c = (m_4)$, as shown in Figure 10, and record the message processing $\sigma = (\sigma_a, \sigma_b, \sigma_c)$ in the block. The node can then get the same state through σ. The only thing to do is to reach a consensus on σ (block) because the order in which the messages are received affects the behavior. For example, Bob's order of processing messages m2 and m3 can be reversed to obtain another valid message processing procedure $\sigma' = ((m_1; m_2), (m_3 \mid m_2), \emptyset)$. When the three accounts are on different chains, the message processing process σ_a, σ_b and σ_c is separately recorded on the corresponding chain to complete the two transfers.

We noticed that the transfer is confirmed in the first phase. As long as the message m1 is included in the block in the first phase, Bob can determine that the transfer has been confirmed. Bob can wait for billing and withdrawals. Cross-chain transfer can achieve the same confirmation speed as intra-chain transfers through this process

4.5.5 . Ether cat program based on parallel model

In the previous section, we provided an example of a payment application. Our model also supports any complex logic. We will take the Ether cat too as an example. The Ether Cat is a very popular electronic pet game based on the Ethereum smart contract. In the game, players can buy and sell Ether cats. However, when many kittens are auctioning, they will block the Ethereum network. Based on our model, a multi-chain solution to solve the network congestion problem is designed.



We designed three types of accounts: collectors, auctioners, and loggers, as shown in the image above. The collector is responsible for collecting all auction requests from the seller. The auctioneer will auction the kittens. The recorder is responsible for calculating the auction results.

The auctioneer requests the collector for the kitten auction firstly. When the auctioneer receives the kitten, it can auction the kitten and send the auction result to the recorder. Finally, the recorder records the auction results and tells the collector if the kitten has been auctioned. Auctioneers can be placed on different chains. The workload of such auction can be split in multiple independent and parallel chains, which greatly improved the efficiency and scalability. A single kitten may attract many people to participate in the bidding, which is called the "hot cat" problem. In this case, the auction of hot cats can be held by different auctioneers. Bidders can choose any auctioneer to bid. Finally, all auction results will be aggregated and sent to the recorder. According to the rules, the recorder selects the winning bidder of the hot cat.

4.5.6 Optimization

We have designed some optimization methods to reduce communication costs and account storage.

- Avoid duplicate storage. Each account has the same general handling for some specific messages. These public methods are designed by the system and do not need to be designed by each account.

- Reduce communication costs. Communication costs can be reduced by merging a bunch of messages of the same type. For example, if there are 10 "add" messages sent to the same account, they can be combined into one "add" message.

The "single account hotspot" problem, which means a single account involves a large number of messages, can be easily solved by the collaborative design of the upper application. This is similar to the "hot cat" problem, and many frequently used accounts can be placed on multiple chains.

Our models are more flexible and efficient than other methods that are also used for concurrency. However, when developing with this model, developers need to clearly consider the scale of how to cross-chain communication, otherwise, multiple cross-chains are likely to offset the efficiency generated by parallelism.

5.Core Engine of Blockchain Commercialization

Thinkey has opened up a new path for the perfect combination of blockchain technology development and real business. In this section, we will elaborate on how Thinkey accelerates the commercialization of blockchain from the perspective of blockchain infrastructure, landing of commercialization, empowerment of traditional businesses, and formation of a common value network.

5.1 Blockchain infrastructure

Cost of decentralization transaction in 2009

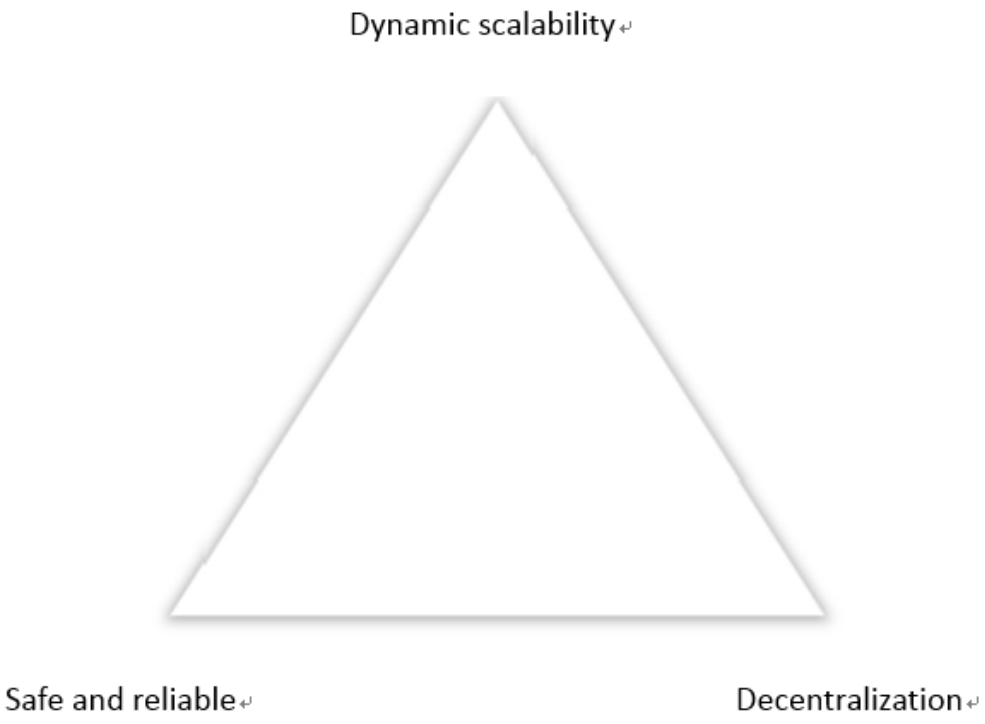
Smart contract in 2014

Blockchain infrastructure in 2018

Since the birth of Bitcoin, the blockchain has matured with the development of over the past decade, but today, there is still no common technology underlying and unified technical standards. The lack of uniform standards has restricted the accumulation of talents or the collaboration between business entities in blockchain industry. There are also many blockchain companies with the ideal of changing the world, however, after they issuing the currency, the development of it is stagnant and contrary to the initial heart for the lack of the support from suitable technology.

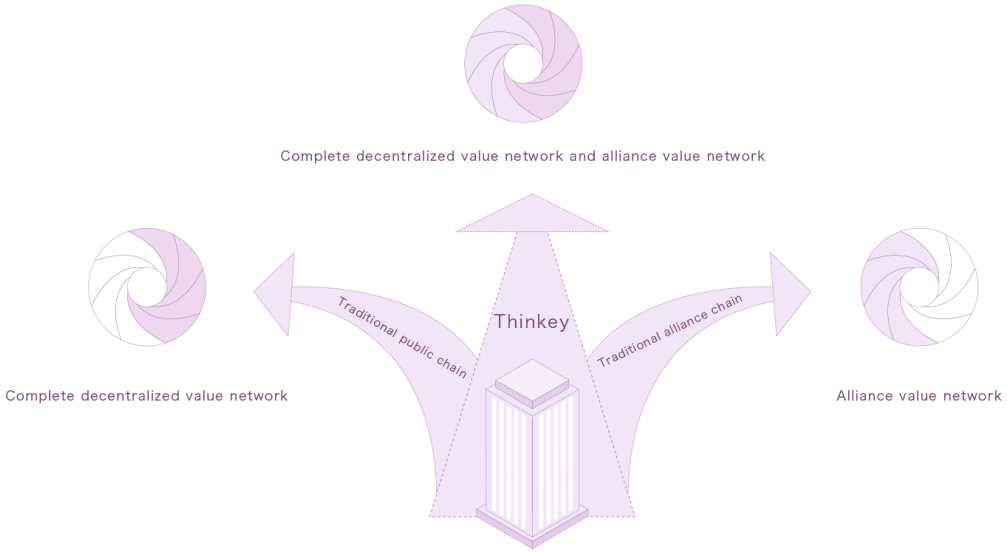
Thinkey has empowered the world's leading public chain, alliance chain, and privacy protection technologies to developers by adhering to an open, inclusive and mutually beneficial mentality to enable to developers to find their initial heart and welcome their dream without the limitation of technology through developing their own industry public chain, alliance chain or application based on Thinkey.

5.2 Landing of commercialization



Thinkey has supported horizontal and vertical bidirectional dynamic expansion through hierarchical multi-level architecture and self-developed hierarchical consensus protocol stack technology under the condition of ensuring the security and consistency of the whole system, which fundamentally solved the problem that “triangle is impossible” in blockchain. Based on the solving the problem that “triangle is impossible” in blockchain, Thinkey also innovatively proposes an Actor-based account system that perfectly supports high-concurrency processing of complex tasks, which enables the blockchain to carry large-scale transactions more efficiently and support the application running of massive user scale. And make it possible to land a blockchain commercial project that was originally limited by technology maturity.

5.3 Traditional commercial Thinkey+

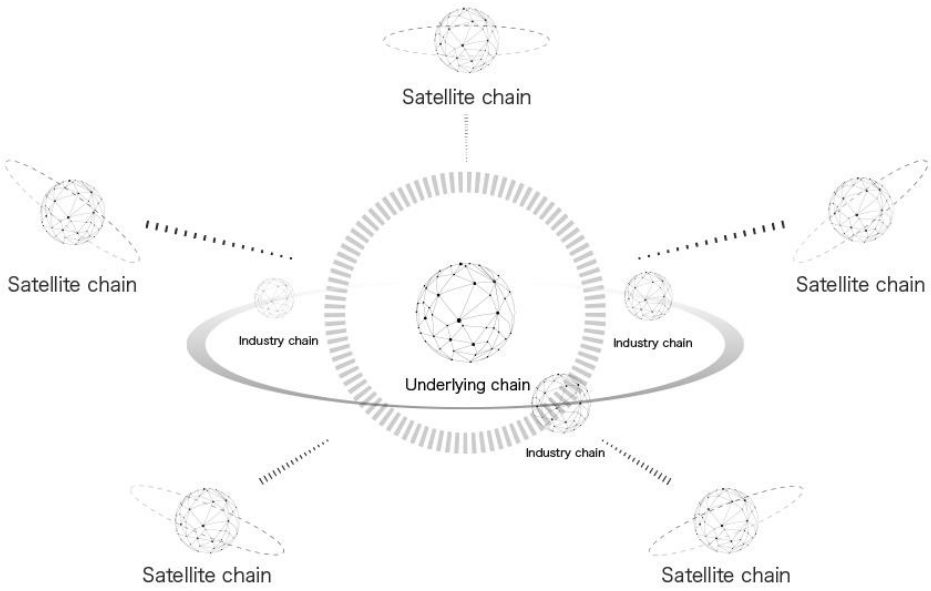


Traditional business faces the dilemma of traditional public chain and traditional alliance chain when it meets the traditional blockchain technology wave and carries out blockchain + transformation: if they select the completely decentralized scheme of public chain, the businesses may worry about the security of their data. If they select the alliance value network of the alliance chain, their value has not been maximized. The unique characteristics of Thinkey's support for both the public chain and the alliance chain make the business entity no longer entangled in the dilemma of subversive innovation and progressive innovation,t here is no need for them to worry about missing the business opportunities brought about by the new technology wave becausethey are too conservative.\

With the underlying facilities of the Thinkey blockchain, business entities can split their business according to their own business needs, they can put a part of the strict confidential business into a credible alliance chain and put another part of the business that needs a larger scope of circulation into the public chain, which can meet the needs of confidentiality and liquidation at the same time.When there is business content adjustment, they can also switch between the public chain and the alliance chain according to the needs of their business. The landing path of blockchain technology for

commercial entities will be greatly shortened due to the emergence of Thinkey, which will attract more industry entities to participate in the blockchain transformation.

5.4 Value network



The entire value network of Thinkey can be understood to be composed of the underlying chain + scalable satellite chain of Thinkey. Industry chain can be built on the underlying chain of Thinkey, and satellite chain is alliance chain. If it is an industry public chain, its underlying security is consistent with the underlying public chain of Thinkey and other industry public chains on it, and the value can be directly passed. If it is alliance chain, the underlying security is inconsistent and the value delivery process need to be guaranteed by additional protocol. Developers can develop DAPP directly on the Thinkey underlying public chain, or they can develop DAPP on the industry public chain, as well as capture part of the value of the satellite chain already linked to Thinkey. Developers can also develop DAPP on the satellite chain and pass part of the value between different satellite chains through Thinkey.

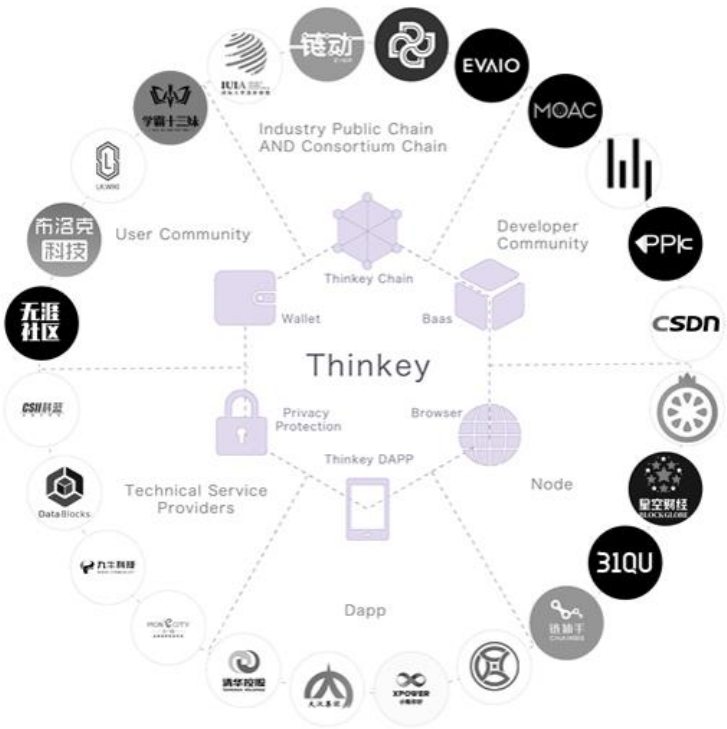
6. Thinkey commercial ecosystem

The design principle of Thinkey is built on real commercial. Its technical characteristics determine its ability to combine with real business, and can also support large-scale high-concurrency commercial projects. This section explains the Thinkey ecosystem growth path from the Thinkey commercial ecosystem and the Thinkey commercial eco-booster.

6.1 Thinkey commercial ecosystem

Thinkey business ecosystem includes the blockchain application like Thinkey public chain, alliance chain, privacy protection, DAPP, wallet, browser, etc. It also provides convenient, friendly, efficient and safe developing, testing, deploying and operating environment to large-scale commercial application like industry public chain, industry alliance chain, decentralized application and the community of developers.

Thinkey can be compared to a mutual trust commercial collaboration engine, which has spawned a commercial environment that is trustworthy and secure for all participants in the ecosystem. In such a commercial environment, the collaborative friction between all business entities will be greatly reduced, which make all business collaboration more efficient and reliable.



6.2 Thinkey eco-booster

The market has long proved that it is impossible to realize the large-scale commercial landing of blockchain by simply playing the financial attributes of the blockchain and encouraging the early participant. Thinkey has done a lot of practical and theoretical research in the fields of finance, e-commerce, marketing, games, AI, IoT, etc., and is committed to providing the underlying technology infrastructure while providing traditional information technology interoperability and large-scale commercial application path for ecosystem participants. And build a new financial underlying.

6.2.1 Decentralized finance of Thinkey

DeFi, decentralized finance, is one of the best landing scenarios for blockchain technology. The core principle of DeFi is to provide a new, unlicensed financial services ecosystem without any central authority that anyone in the world can use. In this ecosystem, users are the custodians of their own assets,they have complete control and ownership of their assets, and they are free to enter all decentralized markets on the market. DeFi's most important vision is to pass all assets to the world, to achieve borderless transactions in the global market, and to create a more open financial system. On the one hand, the development of Defi's business will subvert the existing financial industry's organizational structure and business model, and achieve “going to the bank

for massed-financing and self-financing”; on the other hand, it will increase the mainstream digital currency liquidity and expand the value recognition, which will eventually become stable "Currency" and build a new business and financial system. Which provides viability for true inclusive finance, turning the credit of everyone and every business into wealth- Bank the Unbanked, Serve the underserved.

6.2.3.1 How does Thinkey boost the development of DeFi

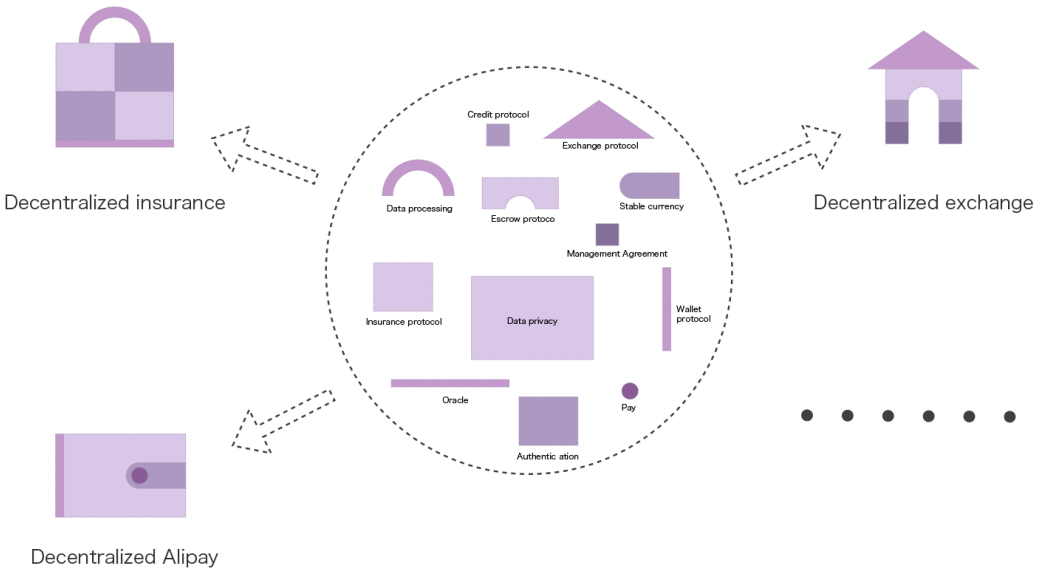
The current DeFi is still in its infancy, but its development space is unthinkable. In order to successfully change the future with DeFi, it is not only necessary to develop a wealth of valuable application products, but also used by a large-scale use of billion-level users, and the absolute security of almost "zero error". As the global trusted clearing layer, Thinkey aims to provide a low-cost, efficient payment settlement system to the world to meet the high efficiency payment and transaction and guarantee the absolute security of the entire distributed bookkeeping and build the infrastructure of distributed finance.

- Support the internet-level mass applications and users

Decentralized financial products are often demanded by the public, such as decentralized insurance, decentralized lending, and so on. Thinkey uses a layered, multi-level architecture to support unlimited expansion of performance, storage and applications. All industries can develop DeFi applications that meet market needs on the basis of Thinkey based on their own business, and achieve high-efficiency lending, transactions and payment for a large number of users.

- Flexible combination of protocol

The key innovation of DeFi is to modularize the basic elements of finance and to achieve the commercialization of trust through this modularity. Thinkey itself will develop a series of basic protocols like wallet, payment, identity authentication, asset issuance, and introduce more and more open financial protocols. The application layer can from the protocol layer required by the combination and achieve the landing of application according to the genes of its own team and the discovery of market opportunities. For example, a decentralized exchange can be implemented by a combination of a wallet agreement, a loan agreement, an escrow agreement, and an exchange agreement.



- Safe and reliable

The DeFi business involves the trading and storage of a large number of digital assets, and its security issues are particularly important. Thinkey uses a layered consensus protocol stack to ensure all aspects of protocol, contract, data, and network securit

- Good user experience

Def is essentially a type of application that helps users solve problems and create value, and needs to ensure a good user experience. Thinkey has dynamic and scalable computing storage capacity, TPS can easily scale to 10W, and the confirmation time is short, which can solve the network congestion problems effectively. Thinkey adopts ultra-low fee mode, which does not pass the burden of calling network resources to users. And Thinkey uses a variety of methods to store data, which can be quickly read and processed in the face of massive data.

6.2.3.2 The ecosystem significance of DeFi to Thinkey

Kevin Kelly said that finance should evolve into a way of life for people. Only by truly integrating finance into all aspects of people's lives can we truly make finance different from the usual, and eventually complete the transformation. In the future human business activities, more and more commodities will be created through blockchain open collaboration organizations, including more and more digital products such as culture, entertainment, games, etc., and the financing demand generated in the process of commodity creation will

be solved by the financial business on the chain, and ultimately pay through the blockchain "currency". This will be a subversive change in the human business and financial system. Thinkey decentralized finance offers this possibility. The goal of decentralized finance is not to decentralize itself, but to make the business more open and fair. The development of DeFi will positively promote the development of the Thinkey ecosystem:

- Attract more developer

The diversity of DeFi application scenarios and expectations for future high growth will attract a large number of developers and project developers to develop based on the framework and modules provided by Thinkey.

- Attract a large number of users

DeFi has no entry barriers, and there is no need to worry about privacy being reviewed and utilized. The advantages of open and transparent data make users more widely engaged and grasp the way of wealth distribution and growth in the new era. The ever-expanding user base is spurring the development and landing of more meaningful and valuable applications.

- Efficient endowment

DeFi is the blood of the trusted world digital economy, which can promote the development of DAPP and application public chain based on Thinkey. In the Thinkey ecosystem, various applications are interconnected and integrated, which enables the flow of funds, information flow, trust flow, and logistics under the chain to accelerate the wonderful bloom of the distributed business world.

6.2.2 Decentralized user system of Thinkey

A trusted collaboration network based on Thinkey, Thinkey's real ID system, and Thinkey's trusted settlement system are bound to trigger a new marketing revolution. The main driving factor of the value growth of the current business entity has been transformed into the value growth of its own users, and the technology provided by Thinky makes it possible to store the value of the user in various distributed networks and complete the integration in the end. Which provides a feasible user value management model that we defined as CVM (Customer Value Management).

CVM can also be understood as a new user loyalty revolution, which can asset all the user's behavior, and can collect and permanently store the user's value. We will provide each user with a private value store (excluding assets, it will also contain some core private data).

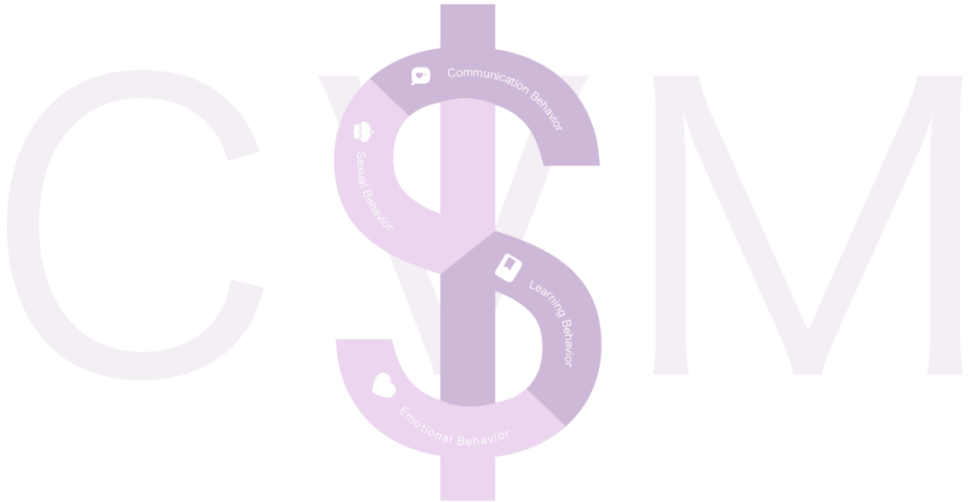
Under the new marketing system, the traditional pull and retention models have changed dramatically:

• Gradually transforms the original business entity's actively infiltrates and motivates, the user's passively accept into the user's own value growth drive. Users will be more autonomously added to the value network (also defined as a community) because their personal value is recognized.

• Gradually transforms the maintaining and motivating more unilateral subjects from the original business entity into the common value community formed by continuous interaction between users and business entities. The users become more loyal because of the precipitation of value.

As the common value of users and business entities grows, they push their value networks to transfer value between each other. Moreover, this kind of interaction is on the bottom of the business environment of mutual trust, so that the most basic marketing activities such as traffic exchange and advertising become unnecessary to worry about traffic traps and settlement risks.

Future product services will continue to upgrade, but marketing is always an inevitable problem for business activities. The mutual trust marketing network based on Thinkey technology will greatly reduce marketing costs and cover more widely.



6.2.3 Distributed e-commerce of Thinkey

Distributed e-commerce refers to the construction of a trusted and equal supply and demand network based on Thinkey blockchain technology. In this trusted network, the behavior of each participant is capitalized according to the consensus criteria, and at the same time, independent collaboration and exchange of values can be carried out in accordance with the rules of consensus.

With the rise of social e-commerce and the deep excavation of private domain traffic in recent years, it seems that there is no e-commerce market with structural innovation. In fact, from the macro perspective of both supply and demand:

- **Supply end：** Industry network collaboration has not yet been formed, and efficiency can be improved through integration.

- **Demand end：** Consumer demand has shifted from the mass to the individual, and individual consumption has spawned a flexible supply chain.

Starting from the point of supply and demand, Thinkey's distributed e-commerce core objectives are:

1. Integrate the supply end through blockchain technology to form a collaborative supply network: in the various aspects of idea, production, processing, pricing, sales (pre-sale, official sales), each participant will cooperate independently and determine the final benefit based on the value of the contribution.

2. Based on the consensus-based standard, the user's behavior is assetized and stored in the blockchain to form a new value network. The continuation of value can protect the user's personality and stimulate personality.

3. Because of the common value body, and then the user (demand side) and the supply side are more deeply bound, the smart contract can guarantee the distribution of interests between different participants.

In such a new mutual trust distributed e-commerce network, the cooperative friction of each participating role is greatly reduced, thereby greatly improving efficiency and reducing trust costs. At the same time, Thinkey's new marketing revolution also gives new business potential to the entire e-commerce network, so that the value of each role is more rationally distributed and stored continuously to achieve their own ability upgrades and role transformation:

- User：promoted from simple consumers to value investors, consumption is investment. Such consumption can be direct money, social relationship assets, behavioral assets, and so on.

- **Server：**(sales, customer service, content producers) divide the labor more professional, division of labor, everyone engages in product service work that is more in line with their personality. The service experience, created content, and business data of the server are capitalized and stored in a wider value network, which break the service boundary of the server.

- **Brander owner：** Brands are a consensus asset with economic value. In the new mutual trust business environment, the brand owner and the user jointly create and maintain the brand and share the brand revenue, so that the growth path of the brand is shortened and more stable.

- **Manufacturer：** It is possible to grasp the data in the entire supply and demand network more realistically and comprehensively, so as to realize on-demand production and on-demand customization. Which ensuring sufficient production efficiency and extremely low waste while staying close to the individualization of consumers.

- **Developer:** The data is separated from the program, and the data ownership is returned to the user itself. The developer's profit model is transformed from the original profit model that collects user data to a new model that synergistic users to create value together.

With the gradual improvement of the subjective status of user value, the evolution of the model of distributed e-commerce is simultaneously promoted:

In a distributed e-commerce network based on Thinkey's mutual trust, S refers to a super supply chain platform integrated through blockchain technology. This integrated S2B2C is no longer a simple variant of B2B2C, but a true technology-based and data-driven collaborative network ecosystem. The traditional supply chain is linear thinking. Such a supply chain cannot cope with the three core conflicting indicators of low cost, fast response and high customization. Only the structure of the trusted network has sufficient flexibility to achieve dynamic optimization of these three indicators. The building of industrial value

synergy network through the blockchain is impossible for any single entity in the industry. The value of the platform is the formation of the network and the underlying architect. From the perspective of empowerment, it breaks through the "transaction" thinking of the traditional franchise system and realizes the symbiosis and win-win of all kinds of small B in S and the industrial chain. As the value of users grows, the roles of users becomes more and more important and the users gradually becomes the dominant player on the entire supply and demand link.

This evolutionary model does not mean that all resource-led formats are directly overturned. It has been a form of a fusion model for a long time. Only in the distributed e-commerce network built by Thinky, each role can conduct mutual trust and cooperation on a larger scale to jointly create a larger community of business value.

6.3. Thinkey token

The native digital cryptographically-secured utility token of Thinkey (Thinkey token) is a transferable representation of attributed functions specified in the protocol/code of Thinkey, designed to play a major role in the functioning of the ecosystem on Thinkey, and intended to be used solely as the primary utility token on the platform.

Thinkey token is a non-refundable functional utility token which will be used as the virtual crypto "fuel" for using certain designed functions on Thinkey, providing the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on Thinkey. Computational resources are required for running various applications and executing transactions on Thinkey, as well as the validation and verification of additional blocks / information on the blockchain, thus providers of these services / resources would require payment for the consumption of these resources (i.e. "mining" on Thinkey) to maintain network integrity, and Thinkey token will be used as the platform currency to quantify and pay the costs of the consumed computational resources. Thinkey token is an integral and indispensable part of Thinkey, because without Thinkey token, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on Thinkey. Users of Thinkey and/or holders of Thinkey token which did not actively participate will not receive any Thinkey token incentives.

Thinkey token does not in any way represent any shareholding, participation, right, title, or interest in the Foundation, the Distributor, its affiliates, or any other company, enterprise or undertaking, nor will Thinkey token entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. Thinkey token may only be utilised on Thinkey, and ownership of Thinkey token carries no rights, express or implied, other than the right to use Thinkey token as a means to enable usage of and interaction within Thinkey.

Thinkey token are designed to be consumed/utilised, and that is the goal of the Thinkey token sale. In fact, the project to develop Thinkey would fail if all Thinkey token holders simply held onto their Thinkey token and did nothing with it.

In particular, it is highlighted that Thinkey token: (a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any affiliate; (b) does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of its affiliates), or its revenues or assets, including without limitation any right to receive

future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to Thinkey, the Foundation, the Distributor and/or their service providers; (c) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss; (d) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment; (e) is not a loan to the Foundation, the Distributor or any of its affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of its affiliates, and there is no expectation of profit; and (f) does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of its affiliates.

The contributions in the token sale will be held by the Distributor (or its affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale. To the extent a secondary market or exchange for trading Thinkey token does develop, it would be run and operated wholly independently of the Foundation, the Distributor, the sale of Thinkey token and Thinkey. Neither the Foundation nor the Distributor will create such secondary markets nor will either entity act as an exchange for Thinkey token.

7. Team

WEI DAI

Distributed algorithm expert Ph.D. of Interdisciplinary Information Institute of Tsinghua University. More than ten years of network security Internet industry, years of experience inbig data and cloud computing, and explore blockchain industry for many years. He has won 1 national science and technology progressaward and 8 provincial and ministerial awards,and he is the leader of 863 national major

STEPHEN GUO

Senior architect of blockchain, rich practical experience in blockchain architecture and R&D, 18 years of system architecture experience SOHU, Aspire Chief System Architect

ICE SUN

PH.D. of Systems Engineering, blockchain expert, deeply involved in the design of several blockchain projects. Have a deep insight into the research and valuation of blockchain projects.

CHENJIANG LIU

Double degree in software engineering and mathematics in Beijing University of Aeronautics and Astronautics. Senior Product Operations Specialist and he is good at hacker growth.

SHAN CHEN

Master of Cross Information Institute, Tsinghua University, Ph.D. in the password and security of Georgia Tech, he has in-depth study in blockchain security and encryption computing.

HOWARD FU

Graduate from Yaoban, Tsing University,Ph.D. of Cross Information Institute, Tsinghua University. Random algorithm experts, he has in-depth research on blockchain consensus and cross-chain algorithms, and published many top international random algorithm articles.

AGAN

Graduated from Beijing University of Aeronautics and Astronautics, he had served as a service development leader in ST Electronic, Singapore. CTO of a community finance project in Master Financial Services Group, leader of R&D in Following Learning Group, technical partner of Internet Vehicle Insurance. And he had created the Beauty of Words APP.

OECAN

Senior blockchain development engineer, DAPP expert, involved in multiple blockchain projects, imTube blockchain technology leader, years of embedded development experience, years of lottery game development leader.

MILEN MARINOV

Master of Marketing and Management, Aston University, Birmingham, UK.He has worked at Land Rover UK and is the co-founder of three financial and marketing start-ups. He has rich experience in global investment and haves provided consulting and training for well-known enterprises such as ICBC, CITIC Construction and COFCO.

YAJING WANG

TaiG Jailbreak's Global Community Leader, partner of Digital Money Fund ChainVC, and co-founder and COO of former Singapore Digital Currency Exchange YEX .

YUHONG LIU

Professor of Santa Clara University.researcher of blockchain privacy Protection.

ZHAOQUAN GU

Undergraduate and PhD of Yaoban, Tsing University.Postdoctoral fellow of Hong Kong University Professor of Guangzhou University. Algorithm design experts, including distributed algorithms, artificial intelligence, blockchain algorithm experts, Microsoft scholars, Xiangjiang scholars.

DONGXIAO YU

PhD and postdoctoral fellow of the Department of Computer Science, Hong Kong University. Professor of Shandong University. Expert in international distributed algorithms, graph algorithms, mechanism design and blockchain mechanisms, Microsoft scholar.

Adviser

GORDON MATTEY

Bachelor of Science in Business Information Systems, University of Portsmouth, UK (First Class Honours), product project management specialist, Mindhouse's founder and CTOhe has served as Chief Product Officer of Spirl, Vice President of Ticketmaster Products, Senior Product Director of Yahoo, Senior Engineer of Oracle, and EIR Consultant of DNA Fund.

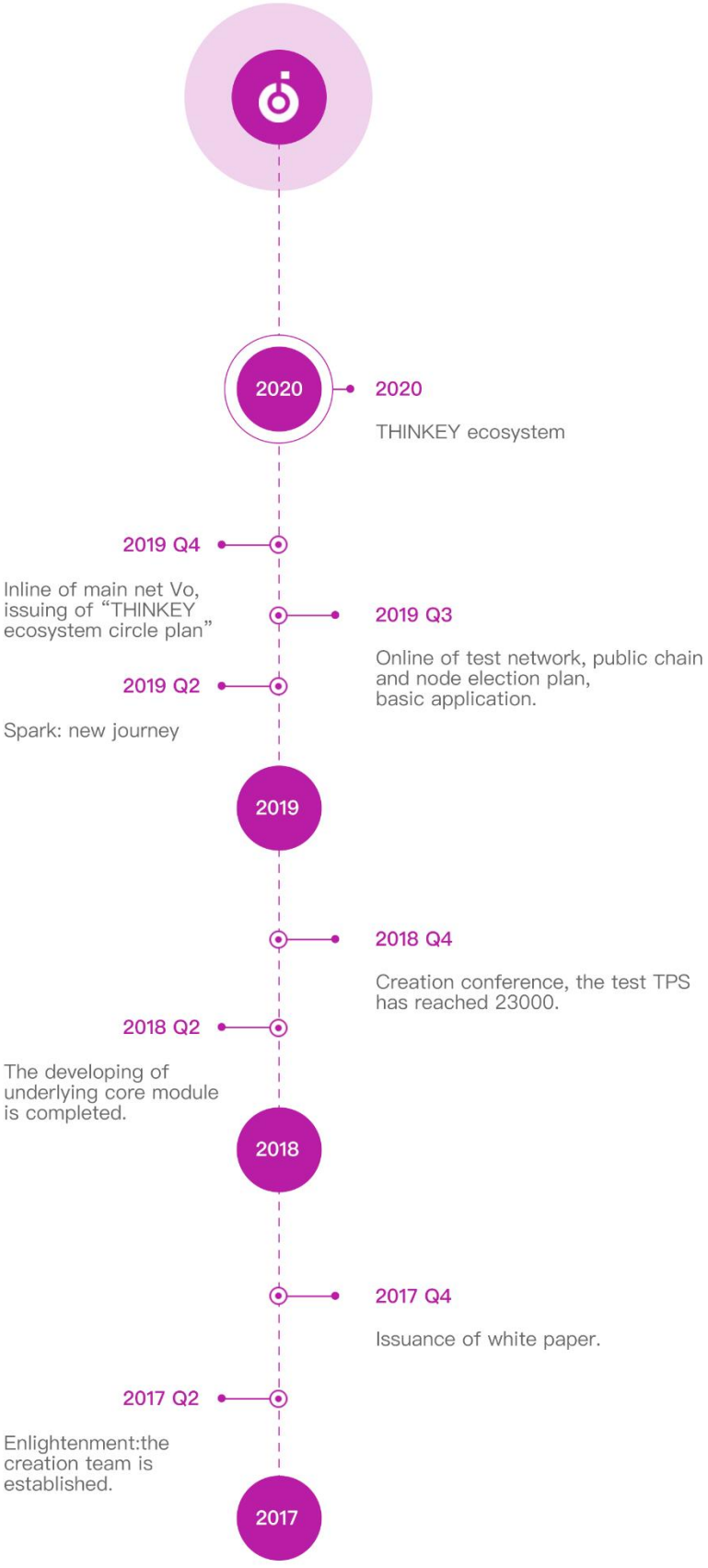
JEFFREY J. CHANG

Established Crossroads Cabinetry, the first online custom luxury cabinet e-commerce company in the United States, and co-founded Clarent Corporation, the first IP Phone Company listed on the NASDAQ . He has worked in key technical management positions of IBM, Schlumberger and Unisys .

GRAHAM SANDERSON

With more than 30 years of experience in cutting-edge enterprise software, he has extensive expertise in distributed systems, concurrency, optimization, performance and system level programming. Worked as a CTO for VAST (Big Data/AI) and a senior engineer at IBM, Lombardi and Trilogy. Master of Science in Electrical Engineering and Information Science,

8. ROADMAP


2020
2020
THINKEY ecosystem
2019 Q4
Inline of main net Vo, issuing of "THINKEY ecosystem circle plan"
2019 Q3
Online of test network, public chain and node election plan, basic application.
2019 Q2
Spark: new journey
2019
2018 Q4
Creation conference, the test TPS has reached 23000.
2018 Q2
The developing of underlying core module is completed.
2018
2017 Q4
Issuance of white paper.
2017 Q2
Enlightenment:the creation team is established.
2017

9. Agreement of Thinkey

527 years ago, Christopher Columbus led three ships and 90 sailors bravely sailed and found the New World, which greatly expanded the space and boundaries of human survival and development.

57 years ago, John Fitzgerald Kennedy eloquently said: we will send humans to the moon in the next decade. We choose to land on the moon, not because it is simple, but because it is difficult. Since then, the pace of human exploration has entered the moon.

11 years ago, Nakamoto published Bitcoin: A peer-to-peer Electronic Cash System that allowed tens of millions of people to participate in this social experiment covering "currency, technology, economy, governance, organization". Despite its limitations, it opens the door to the world of blockchain for us. Today, Thinkey, whose mission is to create an open, equitable, credible and prosperous distributed business ecosystem, is born. Thinkey's bigger dream is to connect the world, coordinate the world, and more people with dreams through blockchains to do valuable, meaningful, innovative, and creative things together. Today's Thinkey is just a nobody, but we never despise our dreams, because every great cause starts from a small point. And Thinkey will one day become great, because every one who join it is committed to making the world more open, more equal, more credible, and more prosperous! In this great era full of opportunities and uncertainties, you just want to be a bystander, a "prophet", a loser, or a true promoter, participant, creator. At the huge crossroads of the times, you have to choose to be the "sportsman" who is brave in the forefront of the tide or the "ostrich" who is resigned to death. Fortunately, after encountering Thinkey, you can listen to your inner voice and make choices for yourself, your small step may become a big step in the whole world.

10. Risks

You acknowledge and agree that there are numerous risks associated with purchasing Thinkey token, holding Thinkey token, and using Thinkey token for participation in Thinkey. In the worst scenario, this could lead to the loss of all or part of the Thinkey token which had been purchased. IF YOU DECIDE TO PURCHASE Thinkey token, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:

1. Uncertain Regulations and Enforcement Actions: The regulatory status of Thinkey token and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including Thinkey token and/or Thinkey. Regulatory actions could negatively impact Thinkey token and/or Thinkey in various ways. The Foundation, the Distributor (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, a cautious approach will be applied towards the sale of Thinkey token. Therefore, for the token sale, the sale strategy may be constantly adjusted in order to avoid relevant legal risks as much as possible. For the token sale, the Foundation and the Distributor are working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

2. Inadequate disclosure of information: As at the date hereof, Thinkey is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to Thinkey, it is not absolutely complete and may still be adjusted and updated by the Thinkey team from time to time. The Thinkey team has no ability and obligation to keep holders of Thinkey token informed of every detail (including development progress and expected milestones) regarding the project to develop Thinkey, hence insufficient information disclosure is inevitable and reasonable.

3. Competitors: Various types of decentralised applications and networks are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying Thinkey token and/or Thinkey and attempt to re-create similar facilities. Thinkey may be required to

compete with these alternative networks, which could negatively impact Thinkey token and/or Thinkey.

4. Loss of Talent: The development of Thinkey greatly depends on the continued co-operation of the existing technical team and expert consultants, who are highly knowledgeable and experienced in their respective sectors. The loss of any member may adversely affect Thinkey or its future development. Further, stability and cohesion within the team is critical to the overall development of Thinkey. There is the possibility that conflict within the team and/or departure of core personnel may occur, resulting in negative influence on the project in the future.

5. Failure to develop: There is the risk that the development of Thinkey will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or Thinkey token, unforeseen technical difficulties, and shortage of development funds for activities.

6. Security weaknesses: Hackers or other malicious groups or organisations may attempt to interfere with Thinkey token and/or Thinkey in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Foundation, the Distributor or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of Thinkey token and/or Thinkey, which could negatively affect Thinkey token and/or Thinkey.

Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to Thinkey token and/or Thinkey by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

7. Other risks: In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your purchase, holding and use of Thinkey token, including those that the Foundation or the Distributor cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Foundation, the Distributor, its affiliates and the Thinkey team, as well as understand the overall framework, mission and vision for Thinkey prior to purchasing Thinkey token.

11. Reference

1. Amdahl, Gene M. “Validity of the single processor approach to achieving large scalecomputing capabilities.” In Proceedings of the April 18-20, 1967, spring joint computer conference, pp. 483-485. ACM, 1967.

2. Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." In OSDI, vol.99, pp. 173-186. 1999.

3. Hewitt, Carl, Peter Bishop, and Richard Steiger. "A universal modular actor Formalismfor artificial intelligence." In Proceedings of the 3rd international joint conference onartificial intelligence, pp. 235-245. Morgan Kaufmann Publishers Inc., 1973.

4. Hill, Mark D., and Michael R. Marty. "Amdahl's law in the multicore era." Computer41, no. 7 (2008): 33-38.

5. Jogalekar, Prasad, and Murray Woodside. "Evaluating the scalability of distributedsystems." IEEE Transactions on parallel and distributed systems 11, no. 6 (2000): 589-603.

6. Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov."Ouroboros: A provably secure proof-of-stake blockchain protocol." In AnnualInternational Cryptology Conference, pp. 357-388. Springer, Cham, 2017.

7. Maymounkov, Petar, and David Mazieres. "Kademlia: A peer-to-peer informationsystem based on the xor metric." In International Workshop on Peer-to-Peer Systems, pp. 53-65. Springer, Berlin, Heidelberg, 2002.

8. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

9. Pass, Rafael, and Elaine Shi. "Rethinking large-scale consensus." In 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp. 115-129. IEEE, 2017.

10. Schneider, Fred B. "Implementing fault-tolerant services using the state machineapproach: A tutorial." ACM Computing Surveys (CSUR) 22, no. 4 (1990): 299-319.

11. Stoica, Ion, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan."Chord: A scalable peer-to-

peer lookup service for internet applications." ACMSIGCOMM Computer Communication Review 31, no. 4 (2001): 149-160.

12. 12. Thomas, Dave. Programming Elixir≥ 1.6: Functional|> Concurrent|> Pragmatic|> Fun. Pragmatic Bookshelf, 2018.

13. 13. Al-Bassam, Mustafa, Alberto Sonnino, Shehar Bano, Dave Hrycyszyn, and George Danezis. "Chainspace: A sharded smart contracts platform." arXiv preprint arXiv:1708.03778(2017).

14. Corbett, James C., Jeffrey Dean, Michael Epstein, Andrew Fikes, Christopher Frost,Jeffrey John Furman, Sanjay Ghemawat et al. "Spanner: Google's globally distributed database." ACM Transactions on Computer Systems (TOCS) 31, no. 3 (2013): 8.

15. Daian, Phil, Rafael Pass, and Elaine Shi. "Snow white: Robustly reconfigurable consensus and applications to provably secure proofs of stake." In Iacr, pp. 1-64. 2017.

16. Eyal, Ittay, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. "Bitcoin-ng: A scalable blockchain protocol." In 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), pp. 45-59. 2016.

17. Gilad, Yossi, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich "Algorand: Scaling byzantine agreements for cryptocurrencies." In Proceedings of th e 26th Symposium on Operating Systems Principles, pp. 51-68. ACM, 2017.

18. Hanke, Timo, Mahnush Movahedi, and Dominic Williams. "Dfinity technology overview series, consensus system." arXiv preprint arXiv:1805.04548 (2018).

19. Hewitt, Carl. "Actor model of computation: scalable robust information systems." arXiv preprint arXiv:1008.1459 (2010).

20. Kogias, Eleftherios Kokoris, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. "Enhancing bitcoin security and performance with strong consistency via collective signing." In 25th {USENIX} Security Symposium ({USENIX} Security 16), pp. 279-296. 2016.

21. Kokoris-Kogias, Eleftherios, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. "Omniledger: A secure, scale-

out, decentralized ledger via sharding." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 583-598. IEEE, 2018.

22. Li, Chenxing, Peilun Li, Wei Xu, Fan Long, and Andrew Chi-chih Yao. "Scaling nakamoto consensus to thousands of transactions per second." ar Xiv preprint arXiv:1805.03870 (2018).

23. Luu, Loi, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. "A secure sharding protocol for open blockchains." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security , pp. 17-30. ACM, 2016.

24. Pass, Rafael, and Elaine Shi. "Thunderella: Blockchains with optimistic instantconf irmation." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 3-33. Springer, Cham, 2018.

25. Thomas, Dave. Programming Elixir≥ 1.6: Functional|> Concurrent|> Pragmatic|> F un. Pragmatic Bookshelf, 2018.

26. Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger."Et hereum project yellow paper 151 (2014): 1-32.

27. Zamani, Mahdi, Mahnush Movahedi, and Mariana Raykova. "RapidChain: Scaling blockchain via full sharding." In Proceedings of the 2018 ACM SIGSAC Conferenc e on Computer and Communications Security, pp. 931-948. ACM, 2018.