Millionaire

Millionaire White Paper

Build a DeFi, NFT, GameFi-based ecosystem and general certification incentive model

MAI Ecological Development Foundation • 2021

Millionaire

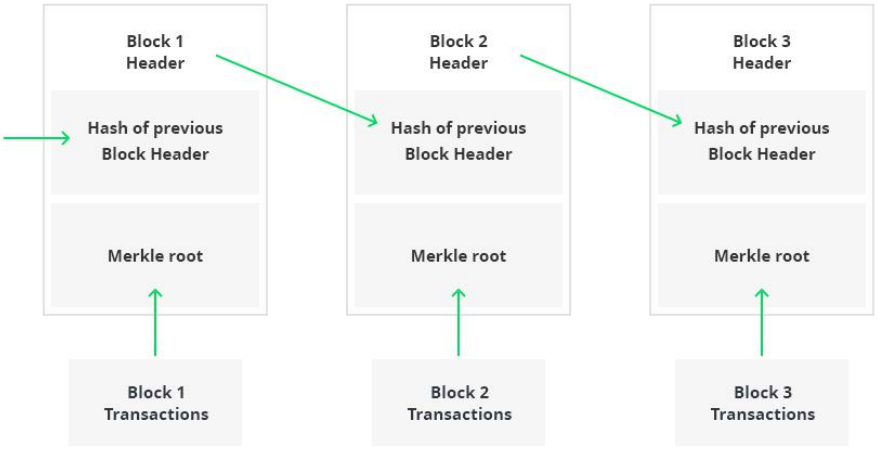
catalogue

Chapter I Overview of the Development of the Blockchain Industry and the Crypto Market

1.1 Blockchain technology and the crypto digital market

The distributed accounting technology of blockchain can enable all parties to establish trust at the technical level, and have the potential to become the infrastructure to build the future free circulation network of value, that is, to form the value Internet.Although the widespread arrival of the value Internet is still unknown, but from today's development situation, some value LAN has been gradually formed.In fact, in some specific areas, several partners or industrial chain participants are jointly building blockchain trust networks, and this value LAN is already in the process of implementation, no longer just a concept.From value LAN to value Internet a possible evolution path is: similar to the development of the Internet, the early is an independent, formed by each industry according to its own needs of local value circulation network, later driven by cross-industry value exchange demand, gradually form a large-scale, common value free circulation network.

Trust, in 2021, is even more valuable.Under the impact of the epidemic, the global environment has increased, the original social order has been disturbed, and the international political and economic situation have also changed significantly. The thinking of anti-globalization has further spread. The lack of confidence in other countries and the vulnerability brought by the too concentrated supply chain have become increasingly severe.In this context, blockchain's value, as a machine to convey trust, has been more visible.From the point of results, blockchain technology with distributed, peer, etc, difficult to tamper with, transparent mechanism, in the trust, help industry realize digital transformation, build digital economy infrastructure and liberation of data productivity play the natural advantages, gradually need some cross-border, cross-industry, cross-industry cooperation distributed commercial application scenarios in the useful, market scale and corresponding rapid growth.



At present, blockchain technology is called by many large organizations as a major breakthrough technology that completely changes the way businesses and organizations operate. The technical basis of the blockchain is a distributed network architecture. It is precisely because of the maturity of distributed network technology that the decentralized, weak-centered, sub-centered and shared, consensus, and shared organizational structure and business structure can be effectively established. .

In 2008, the birth of Bitcoin opened the door to the era of blockchain and encrypted digital assets. Due to the subversive design of "decentralization", in the past ten years, blockchain technology has taken the lead of the times, and has been raised to a strategic height by countries all over the world. It has been commercialized in many fields such as finance, trade, credit investigation, traceability, games, and investment. Good progress has been made in the implementation. According to CoinMarketCap, as of 2021, there are more than 11,000 types of encrypted digital assets in the world, and the asset scale reaches trillions of dollars at its peak. Compared to April 2013, the total scale of encrypted digital assets was only 1.5 billion US dollars. In the past few years, the market value of encrypted digital assets has grown hundreds of times.

According to statistics, the number of investors in encrypted digital assets is conservatively estimated to exceed 300 million. Although encrypted digital assets have achieved phased development, looking at the global economy and traditional financial markets, encrypted digital assets still have a huge market space in the future. First of all, the trend of asset digitization has

taken shape. The Internet of Things, big data, artificial intelligence, and asset security requirements promote asset digitization. In the future, all assets will be digitized and can be used in the network.

Secondly, the gradual maturity of blockchain technology and cryptocurrency has brought inspiration to the national economic system. At present, many countries have issued national cryptocurrencies. The International Monetary Fund believes that central banks should consider issuing cryptocurrencies, while the United States, China, and Europe The central bank has indeed maintained close attention and active research on cryptocurrencies. At present, the investor penetration rate of encrypted digital assets is still extremely low. Compared with investments in stocks, real estate, and gold, encrypted digital assets have more investment value under the trend of asset digitization. In the era of digital economy, cryptocurrency will take on a more important role.

- Can reduce the risk of capital trust. Blockchain technology has the characteristics of open source and transparency. Participants of the system can know the operating rules of the system, verify the authenticity and integrity of the contents of the ledger and the history of the ledger structure, and ensure that the transaction history is reliable and has not been tampered with, which is equivalent to The accountability of the system is improved, and the trust risk of the system is reduced. For example, the blockchain can evade the current frequent thunder explosions, road running and other incidents that occur.

- It can improve the efficiency of fund payment, transaction and settlement. On the blockchain, the process of transaction confirmation is the process of clearing, settlement and auditing. The blockchain uses distributed accounting, all transactions are displayed in real time on a spreadsheet platform similar to the global sharing, and real-time clearing, greatly improving efficiency. Blockchain can increase efficiency to the minute level, which can reduce settlement risk by 99%, thereby effectively reducing capital costs and systemic risks.

- Can effectively prevent failures and attacks. The traditional financial model is centered on financial institutions such as exchanges or banks. Once the center fails or is attacked, the overall network may be paralyzed and transactions may be suspended. The blockchain is supported by many

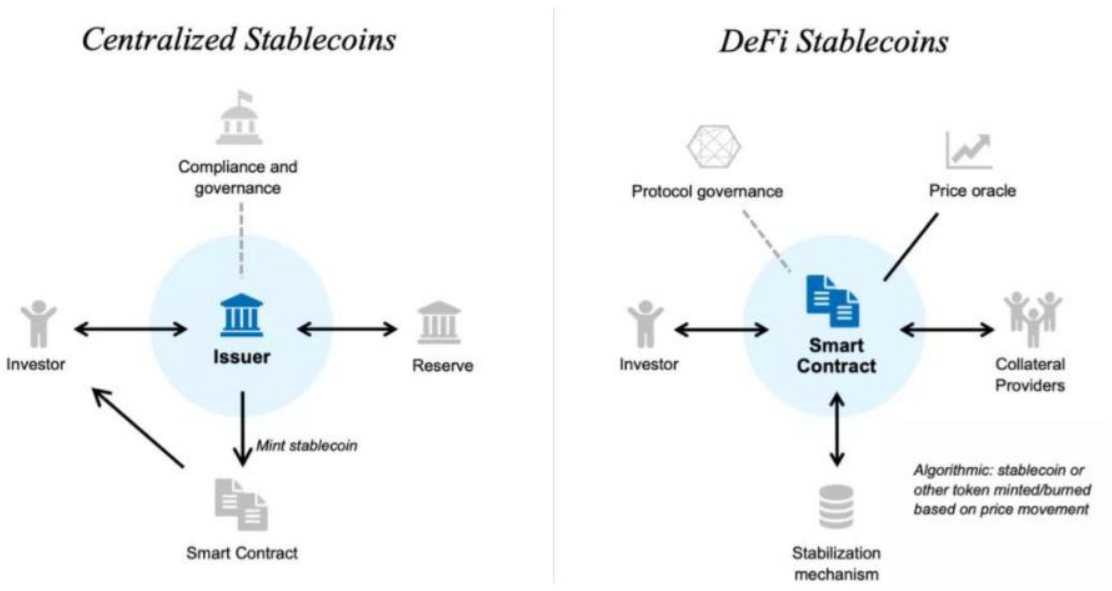
Millionaire

distributed nodes and computer servers on the peer-to-peer network. Any part of the problem will not affect the overall operation, and each node saves a copy of the blockchain data. Therefore, the built-in business continuity of the blockchain has extremely high reliability and fault tolerance.

- Able to improve the level of automation. Since all files or cryptocurrency assets can be embodied in the form of codes or ledgers, by setting the data processing program on the blockchain, smart contracts and automatic transactions may be realized on the blockchain. For example, a smart contract can write a set of financial contract clauses into the agreement to ensure the automatic execution of the contract and default payment.

1.2 The continued boom of the DeFi

DeFi (Decentralized Finance) is decentralized finance, a financial behavior operating on the underlying blockchain system such as ETH Ethereum.DeFi uses smart contracts to enable digital assets to rebuild traditional financial order in blockchain networks and generate synergies with each other.DeFi uses smart contracts to enable digital assets to rebuild traditional financial order in blockchain networks and generate synergies with each other.Typical applications include quantitative, market-making, lending, insurance, swap, liquidity mining, derivatives, machine gun pool, clearing and settlement and so on using digital assets.



Corresponding to the centralized finance of CeFi (Centralized Finance), DeFi decentralized finance has the characteristics of code neutral and open source, decentralized operation, no centralized supervision, and decentralized autonomy:

• Code neutral and open source: DeFi projects running on the blockchain are openly running in the blockchain network and the code is open source. Every smart contract interaction and open source code can be browsed in the block at any time

• Public access on the device. The mainstream project code on the chain is audited by a code audit company to avoid backdoors, bugs and other vicious events that affect the healthy operation of the system. Most of the code for traditional Internet applications is not fully open source.

• Decentralized operation: Refers to DeFi projects that can be run on miner nodes distributed across the world on the blockchain main network, unlike traditional Internet applications, which need to run on a centralized server owned by the company. Decentralized blockchain nodes are more resistant to risks. As long as there are mining machines around the world for mining and accounting for this public chain, the blockchain network can operate normally.

• Non-centralized supervision: The blockchain network application runs on countless blockchain nodes, and the main network of the project does not need to be reviewed by a centralized organization, which makes innovation more free and faster to develop. Without supervision, the DeFi network completed the on-chain reconstruction of the traditional financial system in just half a year, and tried various innovations on the original basis. On the other hand, decentralized supervision also makes investors less protected. The DeFi network has gradually grown in a decentralized organizational form during accidents such as hackers and loopholes.

• Decentralized Autonomous Organization (DAO, Decentralized Autonomous Organization): Most of the top blockchain network applications use decentralized autonomy to manage major projects and development paths. Any community member can initiate a proposal, and all users who hold digital assets can vote on the development direction of the project based on their holdings. DAO is similar to a shareholder meeting initiated 24 hours a day and 365 days without interruption.

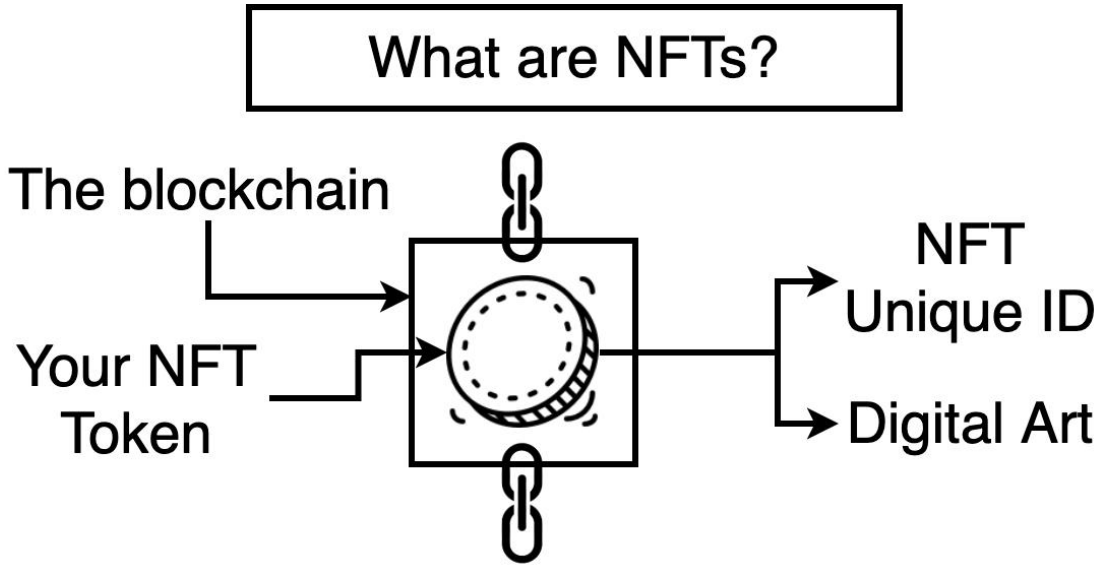
The concept of DeFi began to rise in 2014-2017. In 2018-2019, various

decentralized lending and other DeFi projects were gradually launched. In January 2021, as the Bitcoin bull market attracted market attention, it became popular. The DeFi lock-up volume exceeded US$80 billion in April 2021. The stock of digital assets in the DeFi network has exceeded 100 billion U.S. dollars in May 2021, accounting for about 5% of the overall volume of digital currencies, and there is a trend of further acceleration.

1.3 The rise of the NFT field

As DeFi continues to thrive, blue ocean trends are emerging, most typically NFT.

NFT, English is all called Non-Fungible Token, Chinese translated as a "nonhomogenized token", a cryptocurrency using blockchain technology, which can be understood as an advanced version of Bitcoin.Simply put, NFT is a virtual asset that places specific information on the blockchain through encryption to prove the only copyright and to buy and sell through an online trading platform.Unlike Bitcoin, NFT has inseparable, irreplaceable and unique characteristics. Its records on the blockchain cannot be tampered with or copied, and the transaction records are publicly visible, so NFT cannot be imitated.



For example, when a painting transforms into the NFT form, then it cannot be changed and produces a certain number of tokens to prove its scarcity.The creator, the painting's creation date, and other information will be forever recorded in its NFT s, and even if someone copied or copied it, others can determine it as true or false.To sum up, NFT is the use of blockchain technology to transform the abstract fact of "holding ownership of a commodity" into "tokens" that can be priced and change hands, and is recognized by the world and cannot be changed.

The history of NFT dates back to 2017.In that year, Ethereum launched 10,000 CryptoPunks pixel heads, each being different. People holding Ethereum cryptocurrency could get them for free and get second-hand market transactions.Half a year later, Ethereum launched the blockchain mini-game "Cryptokitties" (crypto).Each cat has its own number, cannot be copied or stolen, gameplay similar to the QQ penguin, unlike the cat you spend time and money "captive" always belongs to you and will not disappear because of the game suspension.

In 2018, the NFT ecosystem gradually developed.Trading platforms such as OpenSea, MillionaireerRare, Rarible, Nifty Gateway rise, and with the rise of NFT, there are various NFT trading platforms, among which Ethereum operates the largest MillionaireerRare and OpenSea, attracting more customers.

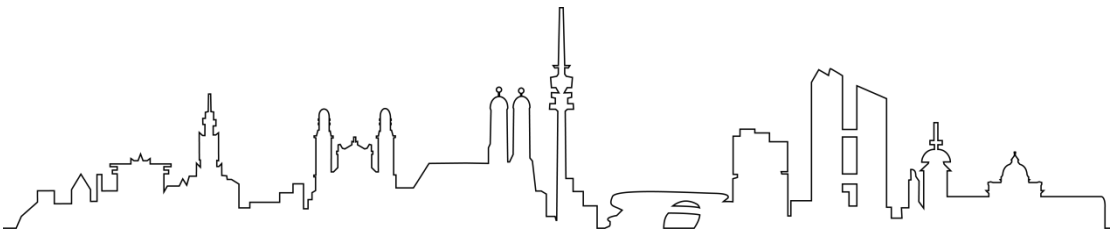
By 2019, brands like Nike, F1, sensing business opportunities, were getting involved in the NFT market.In 2020, NFT began to apply in other areas, including

authentication, fixed asset backup, and even use as a crypto collection to increase collection value.

In 2021, the NFT market finally saw explosive growth.According to the CryptoArt.io shows NFT with the strongest competition at the beginning of the year, with more than $2 million in March; as of August 1,8.21 million artworks were sold as NFT, with a total value of about $683 million, or 260,000 Ethercoin ETH.Not only Musk, Jack Dorsey and other technology giants have grabbed the market, but some well-known artists have also entered NFT, a lot of art works sold at high prices.

At present, we can now clearly see that NFT's main application areas include games, art, domain names, collectibles, virtual assets, reality assets certification (STO), especially art and games pay more attention in the market.Some game props and art are naturally unique and inseparable, just coupled to the NFT, so the NFT can effectively prevent the counterfeiting and fraud of such items.

In the context of global digital transformation, NFT will play an irreplaceable role in the future blockchain ecosystem, and may even become the key driving force and cornerstone for many industries to realize the transformation of the digital economy.For the exchange, how to be under the new wind outlet



1.4 GameFi driven by NFT

The earliest application of the word GameFi was outside of encryption, an innovative financial services company designed to use interesting ways to improve corporate employee efficiency, and since then, the original incompatible words of Game (game) and finance (Finance) have begun to be inextricably linked.

GameFi refers to presenting financial products in the way of games and

gamification of DeFi, such as using NFT equipment to improve revenue and introduce battle mode. Compared with traditional liquidity mining, GameFi projects are more interactive with users and more interesting.

When the word GameFi comes to encryption, it means not just "Game+Finance」, but" Game+DeFi」.People in DeFi world have no longer satisfied with traditional mining projects. With the boring waiting after pledLP, they began to integrate mining into the game, which not only lowers the threshold for new people, but also brings more interest to liquid mining.

When it comes to GameFi, NFTFi, has to mention that many liquidity mining projects led by MEME introduced the NFT, market in an unprecedented way at that time, which also caused a period of FOMO boom.However, MEME's way of obtaining points through pledge and then exchanging NFT is too monotonous and simple, which is also an important reason for the short duration of the NFTFi boom.The advent of GameFi solved the problem, giving NFT more practical value through gamified settings, making them no longer just items hanging on OpenSea waiting for sale.

GameFi is attracting more people into DeFi space.The fun of gamification attracts users who don't want to understand the complex technology of the DeFi project. They don't have to understand the code, logic and mechanics of the DeFi project, just figure out how the "game" is played, neither brain-burning nor boring.Second, GameFi gives retail investors more opportunities to enter.Traditional mining projects depend on the proportion of LP provided in the whole pool, so large households who enter early will often earn a lot of money, while retail investors have little income and risk the risk of free losses caused by large selling.Turning mining projects into "games" offers more benefits for retail investors.

The integrated development of DeFi, NFT and GameFi, the Millionaire(Monopoly) project, is committed to building a complete value ecology for global users in the blockchain era, and hopes that this ecology can guarantee users' free will and personal value, especially time value.At the same time, we will realize the interconnection between independent ecology, build a bridge between each continent, so that human beings can understand the new business world built by blockchain from a new dimension.

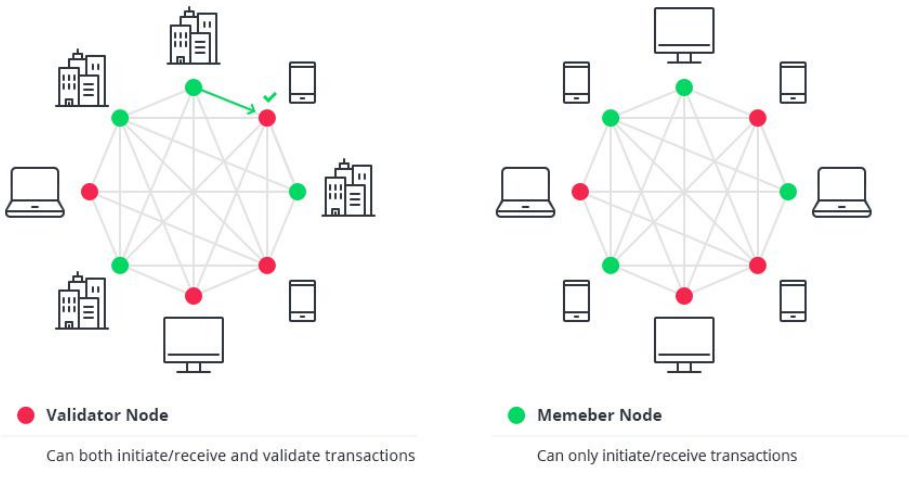
Chapter II Millionaire Project Overview

2.1 Project profile

Millionaire Chinese Monopoly is a DeFi, NFT, GameFi-based ecosystem and certification incentive model created by the MAI Ecological Development Foundation and the world's top blockchain community and team.

Millionaire aims to build a more innovative and better expanding financial platform based on DeFi+NFT+GameFi.Through a full range of basic functions and diversified economic model, create more asset exchange autonomous management system, establish a perfect DeFi ecosystem, provide complete decentralized financial infrastructure, become the king of aggregate trading in the field of DeFi, create more possibilities for the value of the existing cryptocurrency to flow, let more people share the interests under the background of blockchain technology development!

In order to realize the ultimate freedom of digital assets, professional to promote the rapid development of DeFi+NFT+Gamefi, to create a truly distributed "digital financial service ecosystem", so that blockchain technology and digital asset applications can be popularized in a wider range, Millionaire according to the research on existing technologies.In terms of ecological construction, Millionaire covers the most valuable applications of DeFi, NFT and GameFi, such as liquidity pool, real estate tycoon GameFi games, pledge lending, NFT transaction services, etc., to meet the all-range of increasing value needs of users.



☑ Millionaire design objectives:

Multi-asset exchange: Millionaire can connect the existing major digital authentication networks (such as Bitcoin, Ethereum, BSC, HECO, SOL, etc.), and complete asset exchange without changing the original chain mechanism.The newly generated digital pass network can also be accessed to Millionaire at extremely low cost.

Provide privacy protection for transaction: both parties can choose privacy protected transactions in Millionaire,, provide privacy protection for digital asset transfer and transactions, and provide anonymity protection for digital asset holders.

With ductility of scenarios: Millionaire can become a distributed platform for various digital certificate exchange; can conduct deposit and loan business of different digital certificates; can complete transactions of digital assets through digital pass; and can issue and trade new digital financial assets.By improving the ease of use, security and revenue, Millionaire will lower the threshold for small-money users to participate in DeFi.Compared with other DeFi forms, Millionaire continues to innovate the product design and mechanism while preferably aggregating the DeFi product portfolio to optimize the revenue.

☑ Millionaire technological innovations include:

- At the communication level of the underlying P2P network nodes, combined with the advantages of the existing Tor-based anonymous communication network and the blockchain-based distributed VPN, the original hidden P2P communication network is realized, and the method for anonymous access of nodes is designed and realized. The private encrypted communication protocol greatly enhances the anonymity of nodes in the underlying communication network, ensuring that the communication between nodes is difficult to track and crack.

- At the underlying data structure level, a new data structure is adopted, and an enhanced directed acyclic graph (DAG)-HashNet (HN) is adopted to achieve asynchronous and parallel event consensus verification and improve the scalability of the system sex.

- At the level of the distributed consensus mechanism, a safe and efficient consensus mechanism is designed. On the basis of the enhanced DAG HashNet consensus and the Byzantine negotiation (BA-VRF) consensus of the random selection function, an autonomous consensus mechanism is formed with high concurrency, The fast transaction confirmation speed can quickly build an ecosystem for different application scenarios.

- At the level of anti-quantum attack, a new anti-quantum attack cryptographic algorithm is adopted. By replacing the ECDSA signature algorithm with an integer lattice-based NTRUsign signature algorithm, and at the same time replacing the existing SHA series algorithm with the Keccak-512 hash algorithm, the quantum calculation is reduced. Threats posed by rapid development and the gradual popularization of quantum computers.

- At the level of anonymous transactions, combined with the characteristics of the existing encrypted virtual currency, through the one-time key and ring signature technology, designed anonymity and privacy protection methods with extremely high cost-effectiveness and excellent security, and support zero-knowledge proof as Select functions to meet the privacy protection needs of different application scenarios.

- At the smart contract level, through the realization of the Moses Virtual Machine (MVM), it supports declarative non-Turing complete smart contracts and advanced Turing complete smart contracts for the Moses language. The advantage lies in better Supports off-chain data access, supports third-party asset issuance, and can be implemented in actual application scenarios in the form of public chains, alliance chains, and private chains.

- At the cross-chain communication and multi-chain integration level, the relay chain technology is used to implement the cross-chain communication and multi-chain integration functional modules as a single layer of Overlay, which can maintain the independence of cross-chain operations and reuse the Millionaire foundation. Various functions of the chain.

- At the level of ecological incentives, a comprehensive use of multiple Token distribution methods and methods, and support for mining for ecological incentives.

- At the industry application level, through the development of JSON-RPC industry common interfaces such as circulation payment, data transmission, data search, and contract invocation, it supports various upper-level applications.

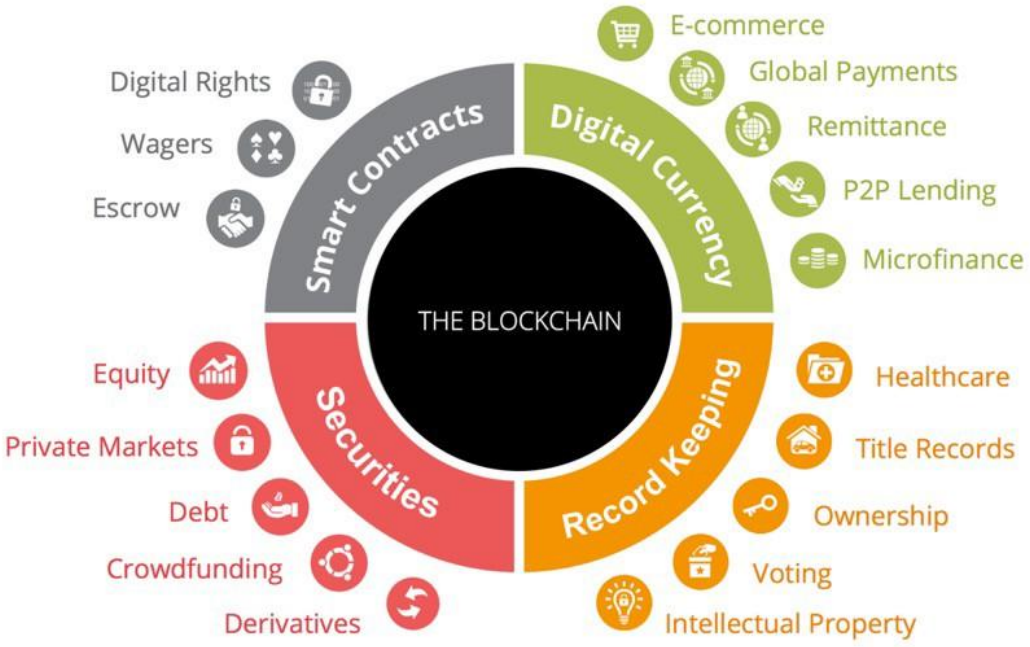
2.2 Mission and Vision

Based on blockchain technology, the prospect of digital currency and the value of DeFi, NFT, GameFi innovation, Millionaire grasps the opportunity of The Times in order to realize a new financial ecological construction of digital asset and real asset transactions.In order to jointly launch the application carrier, in order to better

let the community understand the purpose of the block commercial application ecosystem established by the community, Millionaire shares the purpose and beliefs of the Millionaire with the super nodes and the community:

The goal of Millionaire is to build a fair and open comprehensive application system using blockchain technology.Solve the trust and fairness problems faced by finance, payment, liquidity, pledge lending, and entity business, consumption, entertainment, supply chain, finance, so as to make the whole competitive environment more fair, open and efficient.

Millionaire's mission is to build a complete value ecosystem for global users in the blockchain era, and to hope that this ecology can guarantee users' free will and personal value, especially time value.Millionaire hopes to achieve communication between independent ecosystems, build a bridge between each continent, so that humans can understand the new business world built by blockchain from a new dimension.



- Digital asset empowering entity: Through the infrastructure platform of blockchain technology provided by Millionaire, the token economy will empower the entity, allowing digital assets to lay the foundation for the circulation of the real economy.

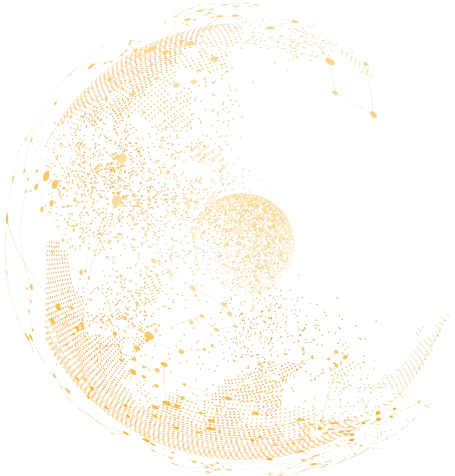
- Release currency rights: Millionaire releases currency rights through liquidity and pledge, so that everyone has exclusive rights to their participation.

- Asset securitization: Millionaire hopes to empower traditional entities through blockchain + new finance, so that more assets can be securitized and generalized.

- Distributed business applications: Millionaire believes that in order to create huge new economic opportunities and new business value for the world's physical businesses, the only way to integrate Millionaire's consensus and openness into low-cost global business applications.

- Autonomous communities: Millionaire firmly believes that more and more decentralized community management methods will be used in the commercial development of various industries around the world, and the formation of autonomous communities will allow more people to report to the group and achieve higher value.

- Integrate commercial applications with inclusive finance: Millionaire believes that traditional applications should be developed globally and should be merged with digital currency and finance, so that chain business symbiosis can become a global wealth opportunity.



2.3 Value logic and technical pursuit

1）Value logic

Millionaire's value logic is based on its core technical advantages and the breadth of application scenarios. In the development process of Millionaire, the stages of digitization, data assetization, and asset sharing involved in the development process require safe and efficient basic functions as support. To this end, the basic functional modules not from the research public chain will provide functional support including digital asset registration, blockchain wallets, and data traceability queries.

Based on the idea of digital economy + business integration, Millionaire will integrate the data of major players in all major industries and fields to jointly create a digital economy traffic highland. By building a shared network of machine trust, it will solve data access, encrypted transmission, sharing, and data access. Trust transactions, storage and other issues, realize the safe on-chain of business data and assets around the world, promote more business individuals to join the alliance, carry out data integration, maximize the value of data, and jointly create a borderless data circulation, value open sharing, and business industry collaboration Innovative digital economy alliance.

In this process, Millionaire will go through the development process from the digitization of everything, to the assetization of data, and then to the sharing of assets.

- Dataization of everything: through blockchain distributed data storage, global individuals, enterprises, and institutions are combined to realize the storage of data and assets on the chain to create a massive database;

- Data assetization: through encrypted storage and peer-to-peer transactions, the privatization of data rights and the use of public ownership, in the form of Millionaire tokens, realize the barrier-free circulation of digital assets;

- Asset sharing: build a safe and credible digital economy alliance, realize the optimal allocation of resources within the alliance, reduce resource integration costs, improve efficiency, stimulate social productivity, and jointly build a digital economic value ecosystem.

In order to achieve this goal, Millionaire will comprehensively utilize cutting-edge technologies such as blockchain, big data, Internet of Things, and AI to realize the safe chaining of global industrial data and assets, promote the integration of industrial data, and connect physical value through massive data to create global value The Internet realizes the integration of the "five flows" of business, capital, information, logistics, and user flows, so as to allow all entities in the alliance to create greater value and jointly build an open, shared, collaborative and innovative, and sustainable digital economic alliance Ecology.

2）Millionaire's technical pursuit

In the future, Millionaire will develop the underlying API of the blockchain to realize the docking of application scenarios and realize the superposition of digital assets, so as to solve commercial problems and build a bridge-like application platform that can dock assets in the physical world. The Millionaire blockchain system has realized a brand-new blockchain architecture, optimized consensus mechanism, adopted distributed computing design ideas, independently developed a distributed storage system, and solved the I/O performance bottleneck problem of the blockchain in storage. Can save a lot of storage overhead for users. Newly designed and developed from the bottom of the operating system, aiming to achieve the performance expansion of commercial-level distributed blockchain systems. Millionaire provides a high-performance, secure, stable and reliable blockchain infrastructure. Therefore, the technical pursuit of the system includes the following aspects:

- Improve transaction speed: By optimizing key links such as signature algorithm, ledger structure, data operation, serialization, consensus mechanism, and message diffusion, the Millionaire blockchain system will achieve rapid transaction verification in seconds. Meet the user experience of most blockchain application scenarios.

- Increased data storage: The blockchain double-entry accounting model has been continuously used in the system and accumulated a large amount of data, resulting in a decrease in operating speed. The Millionaire blockchain system will implement a separate storage and table storage mechanism to achieve massive data storage.

- High throughput: The essence of blockchain is a distributed shared

accounting technology, and its distributed characteristics are mainly reflected in distributed consistency rather than distributed concurrent processing. In order to ensure data consistency and prevent the Byzantine Generals problem, certain specific links can only be executed serially, not parallel. Through long-term testing and optimization practices, the processing performance of the Millionaire blockchain system will further greatly increase transaction throughput.

- Fast synchronization of node data: The Millionaire blockchain system will develop a mirroring mechanism, which can periodically mirror local ledgers to implement a convenient rollback mechanism. Under a unified consensus, mirror tags can be designated for rollback; at the same time, the new addition is shortened. Nodes join the cycle of operation, and only need to synchronize the latest mirroring and a small number of recent transaction collections to integrate into the network and participate in consensus verification.

- Increase scalability: The block chain structure of the Millionaire block chain system will meet the needs of different business areas and improve the system's scalability and maintenance efficiency. It can be used to mark assets and asset transfers, can also provide non-tamperable multi-dimensional event records, and can also be used for traceability to track the circulation process of items.

- Permission control strategy: The Millionaire blockchain system will provide two types of permission control strategies for writing and reading data information. Data information write permissions, multiple users are set up under the same account, and corresponding permissions are set for different operations to meet the use scenarios of multi-party signature control. Data information read permission, users can grant and revoke single user or user group operation permissions on data, and user groups can be flexibly configured by users. The data includes user account information, transaction information, etc. The granularity can be refined to each attribute field of the transaction or account.

2.4 Commercial landing plan

Under the guidance of the core values of the DeFi, NFT, GameFi concept, Millionaire will make a perfect decentralized +NFT+GameFi ecosystem for users and developers through the blockchain network and the certification incentive mechanism.Therefore, Millionaire provides more exclusive features in ecological service support.Including:

1) Game asset issuance

Millionaire has a self-service game and asset issuance portal, mortgage basic Token and value measurement, and digital asset value protection.

- Self-service game and asset issuance portal: Millionaire opens a self-service asset issuance portal to qualified users. Users can design their own issuance plans and connect with their own game programs through open APIs.

- Mortgage basic token and value measurement: Millionaire requires that the issuer of the asset must hand in a certain percentage of the basic token as collateral for the issuance of digital assets by default, so as to ensure the initial value and credit of the issued assets. At the same time, forming a transaction pair with the basic Token is also an indicator of asset value measurement.

- Digital asset value protection: Millionaire uses methods such as forced liquidation to ensure that digital assets with unexpected risks can stop loss in time. Liquidation users can get a certain percentage of Token compensation through asset collateral to control the scale of loss.

2) Game asset trading

Millionaire has a secure and free decentralized trading platform composed of multiple high-performance nodes. The nodes can be expanded and adjusted at any time to provide users with all-weather, real-time, safe and stable free matching transactions or directional transaction services. The cross-regional acceptance gateway group provides currency exchange and consumption services for circulating game assets. In addition to providing automatic

acceptance system construction services for game manufacturers, Millionaire also accepted them as node service providers to jointly maintain the trading network.

3) Democratic gaming environment

- Fair and open game environment: All game data on Millionaire, including the reward probability of game props, random event parameters in the game, player matching balance value, etc., all inherit the non-tamperable characteristics of the blockchain system, and benefit from the underlying framework The high-efficiency processing power brought about perfectly solves most of the unfair problems of game platform transaction efficiency and game oligopoly.

4) Multi-asset access

Millionaire will establish a new asset circulation and inflow mechanism, which will evaluate the assets that are already in circulation on the market and request circulation in the Millionaire DAPP, evaluate the number of users, and vote on a sample of users to determine whether to admit new assets, all new assets The access of the company will be based on the maximum guarantee of the safety of user assets.

5) Multiple incentive system

Millionaire aims to establish a high-quality DeFi, NFT, and GameFi ecosystem, with activity and contribution as a measure of the number of users benefiting. At the same time, through the generation, circulation and value fission of NFT, it gives users the maximum return on the value of income. All business activities on Millionaire need to be driven by basic Tokens. These Tokens are recovered by the system in the form of fees and deposited in the fund pool for rewards to users who have contributed and active to the entire system and the entire network. Ways include but are not limited to: issuing assets, actively participating in transactions, providing node support for the entire network, and actively operating communities.

6) Asset value protection

When asset issuers issue assets on the Millionaire DAPP, they need to use the base Token for value collateral for the amount of the asset issued. This collateral ratio is usually a certain percentage of the initial total value of the issued Token. This design is to prevent this asset from being affected by the project. Suddenly, a bubble bursts and bursts under circumstances such as suspension, capital withdrawal, etc., causing the holders to suffer excessive losses. The purpose of this design is to ensure that Millionaire has the ability to repay the digital assets purchased by users under any circumstances, and once the asset value falls below the limit due to market fluctuations and other reasons, the asset will be forced to liquidate by the system. Reduce the loss of the holder.

7) System security

Millionaire provides users with automatic matching and targeted transaction services. The mutually redundant nodes cooperate with the connection quality detection/link selection program, making Millionaire sufficiently high-performance, safe and robust, and able to effectively resist access pressure, theft risks and node failures.

- Redundant security: Nodes are deployed in multiple countries and regions, and third-party node operators are accepted to provide safe, stable and uninterrupted transaction services.

- High performance: Millionaire's theoretical throughput can reach 1,000,000 TPS, which is enough to support asset trading behavior and game applications on the chain.

Chapter III The Ecological Plate of Millionaire

Millionaire ecology covers the most valuable applications of DeFi, NFT and GameFi, such as liquidity pool, real estate tycoon GameFi games, pledge lending, NFT transaction services, etc., to meet the all-range of increasing value needs of users.

3.1 DeFi Ecological Plate

Millionaire will provide users in DeFi with aggregate trading services including SWAP, mining, machine gun pools, lending to provide liquidity support to markets including autonomous ecology.

1) Millionaire SWAP

Millionaire SWAP will be building the most secure, stable, and efficient digital currency value network for its users worldwide, providing the best digital currency AMM services.The Millionaire[Automatic Market Maker (AMM)] model, in which two certain amounts of encrypted assets are put into a smart contract, automatically calculates the transaction price of the token based on the automatic market maker algorithm.

The gist of the algorithm is that the product of the number of two assets exchanged remains as a constant, the constant product market maker.Represents by formula, x*y = k,x and y are the number of tok ens in the liquidity pool, and k is the product.To k eep k constant, x and y can only reverse each other.At the same time, liquidity providers that provide liquidity to automated market makers (AMM) may see their pledged tokens losing value.This risk is called [impermanence loss].Simply put, impermanence loss is the value difference between token holding in AMM and holding in their own wallet.This happens when the price of the token in the AMM deviates in any direction.The greater the deviation, the greater the impermanence loss.

The self-developed matchmaking system can handle millions of transactions per second.In addition, in order to meet the diversified needs of users, Millionaire

SWAP has not only developed an advanced matchmaking system for currency trading, but also opened up safe and efficient C2C trading services for users to build a continuous, transparent, low-friction and non-discriminatory trading environment with blockchain technology and pass-proof economic model.

In addition, Millionaire SWAP pays attention to improving user experience at the same time, will also upgrade platform technology, improve the ecological system, with scientific and efficient management operation, accumulate distributed ecological resources and energy and the energy output to the whole industry, finally by the application of the whole ecology, eventually form a cycle can assign, continuous development, to establish a global users without trust and highly decentralized financial infrastructure.

2）Liquidity polymeraggregate mining

The provision of Millionaire mobility is based on DeFi based aggregate mining.Through the integration of liquidity mining, mortgage lending, aggregate mining and other modes, the aggregate liquidity pool will be established to provide value support for contracts, leverage and automatic market making.At the same time, generate encrypted integrated digital index synthetic assets through decentralized data contracts, and allow external access to key data and any other API functions to reduce the entry threshold of DeFi and enable users to obtain high returns without exposure to volatile asset exposure and active capital management.

Millionaire takes the mode of mobility aggregate mining, realizing user convenience, low cost and high yield participation.Liquidity mining, mortgage, pledge mining, trade mining, etc can create more vitality for DeFi, and Millionaire is strictly select the chain of the safest highest yield mining projects, and automatically put the money into the highest yield mining pool, the income regularly issued and with Millionaire token reward, to encourage users to provide higher liquidity for the market.

Millionaire liquidity aggregate mining can maximize the benefit rate of user collection, save user mining costs, and high token incentives.Previously, it was difficult for both SUSHI, CRV and YAM, users to grab the head mine, which means that the earnings are greatly reduced.For the broader retail investors, due to the high mining cost, can not participate, basically can only buy in the secondary market, for large households "dig —— to lift —— to sell" to take over.In addition, there are some mining projects with loopholes, smart contracts are not audited,

and security cannot be guaranteed.This severely hit user confidence and motivation for liquidity provision.

The way of Millionaire is to conduct automatic liquidity aggregate mining through the mode of intelligent contract, and realize automatic income distribution. First, to solve the risk of centralization, the other is to solve the problem of transparency of income distribution.

3) Millionaire machine gun pool

The literal translation of Valut in English should be called the vault, but the circle is more inclined to call it a machine gun pool. Millionaire Valut is an intelligent revenue aggregator (Earn Collection), based on the DeFi protocol that automatically implements the best revenue strategy configuration. It can help investors obtain the best returns in the market with one click, thereby greatly reducing the entry barriers for ordinary investors, and at the same time reducing the loss of income caused by information asymmetry.

Millionaire Valut has obvious advantages. It can eliminate the complicated contract operations of liquidity mining and save users high gas fees. You only need to recharge assets to the Millionaire Vault smart contract as an agent, and you can recharge/withdraw with one key to get the best profit in the market. .

- Linear release of capital weight: In order to prevent large accounts from diluting other people's income by quickly depositing and withdrawing funds, all income will be evenly released within 24 hours after each deposit of funds, and T+1 is more in line with supervision And anti-money laundering requirements.

- Automatic rebalancing of revenue strategies: According to the current market conditions, the Millionaire machine gun pool will automatically switch strategies. For a certain currency, users do not need to withdraw the currency and recharge to the new pool to get the highest profit in the current market. The only pool for each currency is the Vault with the highest profit currently on the market.

- Supported currencies: Millionaire Vault will support mainstream currencies including ETH, DAI, BUSD, USDT, WETH, USDC, etc., with a total APR of more than 70%.

The Millionaire machine gun pool is essentially a capital pool that contains

strategies to maximize asset returns. The machine gun pool strategy is much more active than the Millionaire standard protocol, which can only lend coins. In fact, most machine gun pool strategies can do multiple things to maximize revenue. This may involve providing collateral and borrowing other assets (such as stablecoins), providing liquidity and charging transaction fees, or mining other tokens and selling them for profit. Each machine gun pool follows a strategy voted by the Millionaire community.

4) Pledge lending

In the Millionaire pledge loan agreement, users realize continuous financing through the risk classification of the pledge target.After the platform provides initial liquidity, the market maker locked LP Token as a pledge in the Millionaire protocol, thus continuous liquidity buying.When the user provides liquidity in the Millionaire and sets a large range, the value fluctuation of the liquidity coin based on the liquidity target is small.

If the supplier edges the LP Token, in Millionaire, the pledge will be significantly improved in extreme conditions, which will also make the booster pool system more stable: when the project tokens rise sharply, do reasonable risk warning, and when the tokens fall sharply, do a good job of risk buffer.Millionaire can eventually allow high-quality assets to rise for a long time, and non-performing assets gradually decline and are eliminated.

In the platform, in order to achieve more accurate risk pricing, it is necessary to grade the risk, so as to form a fixed income classification fund.In addition to the initiator of the project (IP), two main classes of engagement roles are required, divided into significant participants (GP) and fixed-income participants (LP).

Both roles will provide ongoing funding input to the project, and GP, as a direct investor in the project, will exchange all the principal into project tokens, and LP funds will be used as leverage for GP to help the project achieve greater value growth.

Millionaire allows IP to pledge high-quality assets, which adds a layer of security for GP and encourages large GP inflows.Each GP inflow goes into Vault to store LP's risk reserves and profits.With the increase of Vault capital volume, LP's willingness to invest is also gradually enlarged.As follows:

LPw ∝ Vault ∝ IPcol * GPturnover * IPltv

GPturnover ∝ GPw

in:

• IPcol is the pledge of IP

• IPltv is the current pledge rate of IP

• GPturnover is the turnover rate of GP

• GPw is GP’ s willingness to invest

• LPw is the investment willingness of LP

• Vault is the reserve

It can be seen that through effective signal transmission, the underlying asset with a smaller IP pledge volatility effectively drives the capital capacity of LP. As the most important part of the market feedback loop, LP capital will exert a positive multiplier effect. If the project is a non-performing asset, because GP participants have replaced their base currency with project tokens, the volatility rate of the GP leveraged target will be much higher than that of the IP pledge. At this time, the GP may fall due to the price of the project’ s assets. And was the first to be cleared out. The remaining GPs are more willing to enjoy the pledge after the IP is cleared, thereby reducing the turnover rate. This time directly led to the shrinking of Vault's increments, which greatly reduced the LP's investment willingness, which in turn caused inferior projects to be gradually cleared.

LPw ∝ IPcol * GPturnover

GPturnover ↓ ⇒ LPw ↓

Such transmission mechanism can not only make Millionaire operate healthily, become a scavenger of non-performing assets, but also convey a lot of effective market information, as an external feeding data for Millionaire risk pricing, to provide decision feedback to investors and liquidity providers.

3.2 The NFT Ecological Plate

Millionaire's NFT ecosystem segment will provide global users with services including NFT auction, NFT creation, and NFT fragmentation transactions, based on solving the pain points of the industry.

1）Industry pain points

With the popularity of NFT, various platforms have emerged one after another, which has also left the entire market in a state of barbaric growth. Generally speaking, the existing NFT trading market has the following pain points:

- Credit issues: Practical issues such as the lack of a credit system in the field of personal IP. The creator's creation track and achievements cannot be preserved fairly, and there is the possibility of tampering.

- The cost of a centralized platform is high: For a centralized system, a centralized third party is required between the project party and the IP provider. This increases the corresponding cost. In order to ensure the normal operation of the platform, some platforms will transfer these fees to the commission of the project party, the price of the game or the product, and ultimately, the user must pay.

- Unprotected copyright: On traditional platforms, content piracy, lack of innovation, a vicious circle, copyright cannot be confirmed, and it is difficult to confirm the rights. Seriously infringes on the interests of creators.

- Centralized power: centralized platforms have risk behaviors such as tampering with transaction records, user assets, user levels, number of community participants, reading records, digital currency, etc., especially modifying the amount of digital currency, which will directly lead to the devaluation of user assets, and ultimately Cause the user's loss, even the third-party platform's own loss.

- Fake traffic and single evaluation system: The value considerations of traditional platforms for creators mainly rely on the single evaluation system of reading volume (participation volume), number of rewards, and user

evaluation, which is easy to be brushed and lacks credible reference value. In order to improve their own popularity and traffic, some individuals are forced to perform behaviors such as checking the number of people, the number of rewards, and the evaluation. As a result of spam content on the list, the platform lacks an intelligent anti-spam mechanism and anti-swipe mechanism. Therefore, it is very important to provide users with a fair, fair and innovative evaluation system.

- Insufficient liquidity in the NFT secondary market, and too high GAS: The scarcity of NFT is suitable for a series of applications that reflect unique value, but it is also because of its uniqueness and irreplaceability (uniqueness) that it is difficult to evaluate the value , Which makes it difficult to realize the free trading of NFT artworks and creates liquidity problems. Therefore, the current NFT and homogenized tokens (ERC-20, etc.) show a gap of multiple orders of magnitude in transaction volume, and the transaction cycle is too long, which ultimately restricts the circulation of NFT assets.

- NFT primary market to be explored: Due to the nature of NFT, it is unable to subscribe to the primary market through Token distribution. It can only circulate in the secondary market through auctions, transfers, and the sale of a single NFT. Due to the lack of early funds and investors in the primary market for NFT assets (such as investment institutions, promoters, collectors, art funds, etc.), this type of assets (works) is restricted in dissemination and marketing, and ultimately makes high-quality NFT assets in Difficult to discover early.

2) Millionaire NFT Market Solutions

Millionaire will help high-quality projects, users, investors, and related institutions conduct primary issuance, trading and circulation of NFT assets. Through Millionaire, users or players can buy NFTs before they flow into the secondary trading market, thereby gaining a better entry price or the priority right to experience the project earlier. For example, users can directly participate in market subscriptions on the Millionaire platform in order to get a better entry price or the priority right to experience the project earlier.

In terms of secondary market liquidity, the Millionaire secondary market will rely on the huge flow of the community to help users solve the problem of secondary market liquidity. On the Millionaire platform, buyers and sellers can

trade freely on the NFT secondary market.

In terms of GAS fees, compared with general NFT trading platforms, Millionaire has no user threshold and no issuance restrictions. At the same time, Millionaire transaction has zero handling fee, which perfectly solves the problem of excessive GAS fee. In addition, for the NFT minted on Millionaire, the data is stored in a decentralized storage network, which ensures the durability and immutability of the data.

The advantages of Millionaire's solution are: a one-stop trading platform, no Gas fee for NFT casting, decentralized storage, low thresholds and clear fees.

- Millionaire is a cross-chain, cross-category, and cross-project NFT comprehensive investment platform. This comprehensiveness provides users with one-stop transaction services, and also concentrates user traffic, bringing more exposure to products. Regardless of which NFT users want to purchase or browse, relevant business needs can be met on Millionaire.

- There is no gas fee for minting NFT on Millionaire. Only when the user successfully sells the product, the minted NFT will be listed on the chain and the gas fee will be charged.

- The data content of the NFT minted on Millionaire is stored in a decentralized storage network, which guarantees the durability and immutability of the data.

- Compared with a trading platform that focuses on a single NFT field, Millionaire has no user threshold and no issuance restrictions. At the same time, Millionaire only charges a very small portion of the transaction fee, and the fee model is clear.

In the future, relying on first-mover advantages and continuous accumulation of network effects, Millionaire will surely become a comprehensive NFT investment platform covering the widest range of categories and the most digital products. With its diversified ecology, Millionaire will continue to cultivate in the field of NFT transactions. , And form an irreplaceable dominant position.

3) The NFT auction platform

Millionaire will build the NFT items and value product auction service ecosystem to provide a brand new, dependable business model and platform for artists, players, investors, and collectors.Millionaire NFT Item and Value Product auctions are based on DApp, developed by Ethereum to provide NFT creation, trading and circulation infrastructure.Millionaire also set up a special NFT investor protection fund, to include: investment and layout head NFT platform and works, hatch top head NFT artists, for traditional top artists into NFT bridge, sponsored galleries, organize art exhibition or publishing, set up awards, support art creation and art criticism and establish related art collection.

For the real world, the biggest advantage of the Millionaire NFT sector is to create new value for the physical industry.Help art and collection to obtain better liquidity, from the capital end, to solve the difficult retail funds to enter the core difficulties.For the world on the chain, Millionaire NFT+ value items also bring a brand new concept category to all digital currency investors.At present, the growth dividend of the NFT industry can be seen to the naked eye. For all investors, the best posture for participation is to enter the Millionaire NFT ecology in order to share the dividend of industrial development.

4) NFT authoring Platform

Millionaire is building a NFT creation platform for everyone, hoping to drive the creator economy to a new level for creators to enjoy permanent royalty, revenue sharing and affordable coin fees.Millionaire will provide low-cost underlying systems and cross-chain agreements for global artists and NFT institutions with low-performance blockchain technical support. If only need to focus on work creation, artists can enjoy the high liquidity of DON incremental user market to empower their NFT works, and fully obtain value benefits from the NFT wave.

Millionaire by linking NFT artists / institutions and users, become an important channel of NFT concept popularization, market education and liquidity expansion, and provide the artists, ordinary users and professional NFT institutions platform, low coin, work display and sales experience, promote the popularization and promotion of NFT, jointly explore the infinite possibilities of NFT in the field of artistic value and application, let everyone become NFT artist!

5) NFT fragmentation trading platform

Users can fragment one or more of the NFT assets they own on Millionaire's NFT fragmentation trading platform.Automatic market maker (AMM) and liquidity mining (Liquidity Farming) were introduced on the basis of NFT fragmentation.

NFT holders can create MToken,MToken by depositing their own ERC-721/ERC-1155 standard based NFT in and locking in a smart contract is a ERC-20 token with circulation set by the creator, a MToken containing one or more collections of NFT collections.

Purpurchaser can gain partial ownership of the NFT collection (determined on the MToken holding quantity) by purchasing MToken.NFT collectors can bid on individual NFT,MToken holders in the NFT collection collection to vote on whether to accept the highest bid.When a percentage of votes agreed to accept the highest bid (set by the creator when creating the MToken), the NFT is unlocked and the highest bidder can claim the holder of the NFT,MToken with pro rata proceeds from the sale of the NFT.

MToken is essentially governance tokens that give holders the right as well as share the proceeds.To gain more revenue, the model encourages MToken holders to be active in voting when the bid for the NFT collection reaches the expected valuation, and also gives MToken holders the incentive to promote the collection, giving NFT the chance to get a higher bid.Millionaire's NFT fragmentation trading platform will provide two price transactions and auction methods for global NFT works.In NFT works or other NFT platforms created on Millionaire platform, NFT works charged to Millionaire NFT fragmentation trading platform can be displayed and traded in a full way. The sales income will directly become the income of the creators, and a small part of them will be included in the Millionaire fund and used for the creation support of the creators signed on the platform.

3.3 The GameFi Ecological Plate

Millionaire's GameFi Ecology section will contain services such as NFT+GameFi, Play-to-earn.The first application of Millionaire's GameFi ecosystem is the —— real estate tycoon, who will detail the game's revenue gameplay.

NFT+GameFi

The Millionaire game ecology and GameFi system aim to establish an NFT+GameFi application platform and a high-value chain game revenue ecology. Adhering to the concept of deep application of the DeFi+NFT+GameFi concept, Millionaire will open a new era of value internet. Thanks to the advantages of continuous development and innovative technology, extensive commercial applications, and refined governance, Millionaire is competitive in the following aspects:

• Increased player participation, can modify or optimize the game: Every player can participate in the improvement and upgrade of the overall game. Players who have obtained game governance tokens can upgrade and improve the game by voting to obtain a better gaming experience. Players and games have higher interaction and stickiness.

• Chain games have no central control and no unified operation center: it is not owned by a certain company. Players and developers jointly maintain the game. It is completely driven by the market. The higher the popularity and the better experience, the higher the game player. For games placed on the blockchain, the computing company that was originally developed cannot fully grasp the development trend of the game, or close the game.

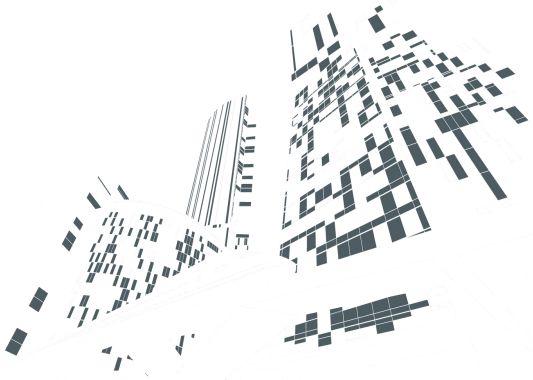
• Play-to-earn can realize odd loose control: Playing and earning is the biggest selling point of the Millionaire game. It not only enjoys the game, but also tokens and equipment, props, NFTs, etc., which can all be sold in the blockchain market .

• Distributed decentralization: Since every node and miner in the Millionaire blockchain must follow the same accounting transaction rules, and this rule is based on cryptographic algorithms rather than credit, and each transaction requires the approval of other users in the network, so , Millionaire's decentralized trading system does not require a third-party intermediary structure or endorsement by trusted institutions.

• Immutability and encryption security: The Millionaire blockchain adopts a one-way hashing algorithm. At the same time, each newly generated block advances strictly in time linear order. The irreversibility of time leads to any attempt to invade and tamper with the data and information in the blockchain. Behaviors are easily traceable, leading to rejection by other nodes, which can limit related illegal behaviors.

In addition, Millionaire will provide more users and third-party developers with a high-performance, highly scalable blockchain game basic service aggregation platform, which has the ability to quickly build upper-level application services and meet the application scenarios of large-scale users. Based on the team's continuous technological breakthroughs and innovations, Millionaire has formed a series of technical features and advantages in terms of performance, scalability, security, and operation and maintenance. That is, with the support of the underlying technology, the Millionaire mainnet can provide developers on Dapp with an easy-to-use and complete blockchain game infrastructure, including a visual development kit and an on-chain ecological environment. Developers do not need to pay attention to blockchain technology. The realization of the block chain game can be completed directly in a graphical manner, with a low threshold, and quickly and efficiently.

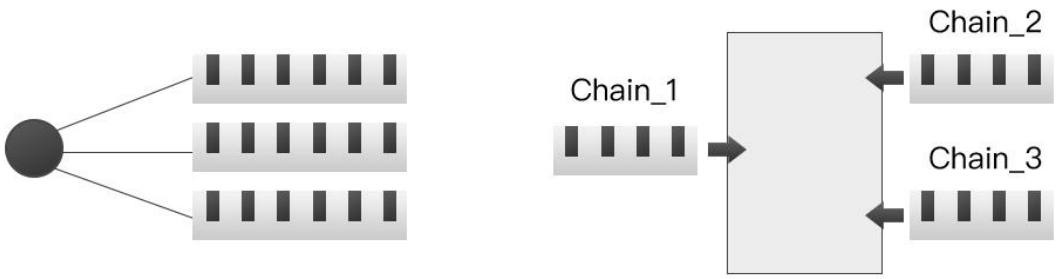
Millionaire hopes to provide players with a fair, just, and open game environment in which data is transparent, rules are transparent, there is no background manipulation of item drop rates, and consumption is maliciously induced. At the same time, Millionaire hopes to carry the value fission of the digital asset economic model through the NFT+GameFi model.



Chapter IV The Technical System of Millionaire

4.1 Platform performance

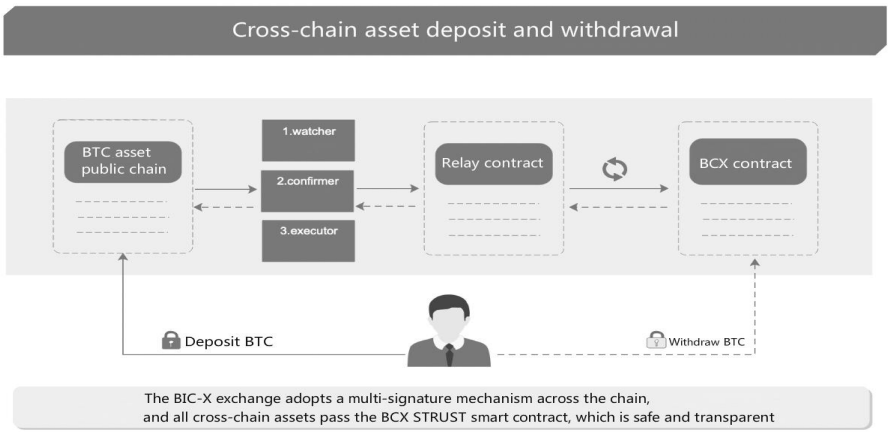
Millionaire supports dynamic adjustment of network topology for dynamic node addition and active exit.At the same time, users can also choose better performance non-Byzantine consensus agreement according to their own needs to improve the operation efficiency of the whole blockchain.In order to cope with diversified business scenarios, meet information security needs, and improve business throughput, Millionaire blockchain supports multi-chain architecture.Unrelated businesses run on multiple parallel blockchain, which provides Millionaire with linear expansion capabilities for the business.The interoperable Millionaire between multiple chains adopts the relay chain mode, participating in the relay chain nodes in various directions, and the results were confirmed after consensus.



Millionaire adopts a micro-service processing architecture, which supports horizontal scaling and dynamic capacity expansion, and realizes massive transaction processing and data storage.Through testing and analysis, it is found that the password module and the contract module have the performance bottleneck.In order to reduce the impact of this problem, the password module and contract module are divided into separate stateless micro services, so that targeted horizontal expansion of password and contract micro services in handling massive transactions.As the processing of data increases, the performance of the K-V

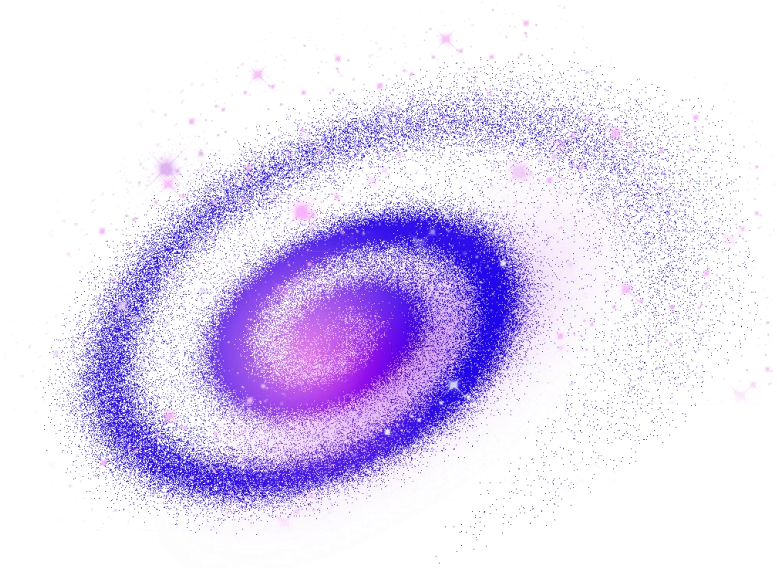
Millionaire

database gradually decreases, and the trend becomes more obvious.To solve this problem, it abstracts the K-V memory module in the consensus node as a microservice and implements the storage dynamic routing synchronization with the consistency HASH algorithm in the API gateway.



Flexible data storage structure is adopted to support hot and cold data separation;

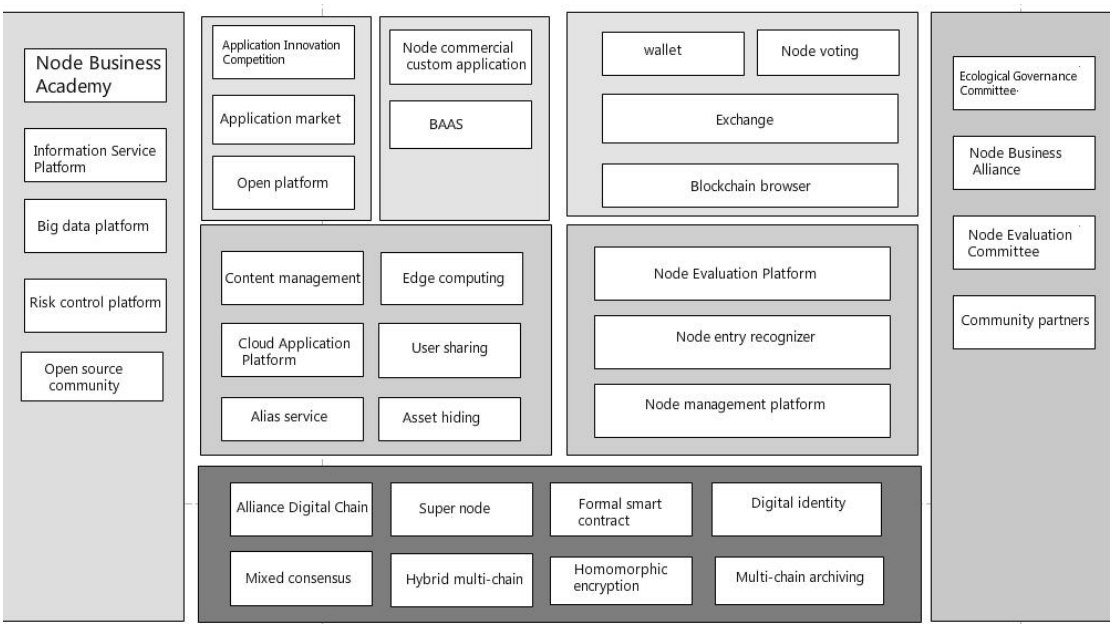
Support the dynamic addition and exit of nodes, realize the high availability of the system, and ensure the uninterrupted business operation.



4.2 system function

The Millionaire employs a universal event-driven model framework.The Actor model accessing AKKA gives a higher abstraction of the concurrent model.Light-weight transactions are used to achieve fine-grained component multiplexing at the event level.

The message queue + cache is used to timely absorb the abnormal situation in the business processing, and adopt various monitoring mechanisms to respond to the abnormal business in time.



- Support enterprise data governance;
- Support event-driven business collaboration model;
- Support multiple ledgers to manage data on the chain according to business dimensions.

1) Ecological safety

- Pluggable password algorithm, can flexibly formulate corresponding password system;
- The platform implements multiple sets of cryptographic algorithms by default, including national cryptographic algorithms and hardware encryption devices.

2) Smart contract

- Support reusable smart contracts;
- Support the debugging function of the smart contract language.

3) Application compliance

- Support CA-based account authentication;
- Support the access of supervisory nodes;
- Support data filing.

4.3 system architecture

Millionaire adopts a top-down design approach, first focusing on the design of blockchain protocols to solve data standardization and multi-chain connectivity in applications; second, defining a general component model of specific blockchain system, realize loose coupling and interggable functional components, solve the requirements of customized extensions in the application; finally, provide a specific blockchain platform implementation and related tools and development packages to quickly realize commercial-level blockchain applications.

1) Blockchain protocol

As the top-level architecture design, the Millionaire blockchain protocol defines the data format standards of the blockchain, including data standards in

four aspects: ledger status, historical proof, ledger operation set, and contract instruction set.

2) Component model

The "component model" is the framework model of the logical components of the blockchain and the implementation framework of the Millionaire blockchain protocol. It includes four components: consensus network, ledger, persistence engine, and contract engine.

3) Service model

The "service model" is the concrete realization of the upper-level blockchain protocol and component model, which is composed of gateways, services, node networks, SDKs, and a set of tools.

4.4 Account agreement

The ledger agreement is a standard model defined from the perspective of data, including two definitions:

The standard format of ledger data consists of two parts:

- "Ledger status" indicates the current real-time data content;
- "History proof" indicates the characteristics of the ledger data and the characteristics of the data change history.

The standard format of instructions for reading and writing ledger data consists of two parts:

- "Ledger Operation Set" defines the standard expression of the type of write operation to the ledger data and the standard format of the parameters;
- "Contract instruction set" defines a standardized contract language instruction format.

The purpose of defining the ledger protocol is to allow the data on the chain to be exchanged, verified, stored and used in a standardized manner, which can span the blockchain network implemented by different technologies, regardless of the specific data storage implementation.

1) ledger status

The term "status" here is a concept in the computer field, where it represents the state of the blockchain system at a certain moment, which is composed of the business data saved by the system and the control attributes of the system's operation.

The "ledger status" of the Millionaire blockchain is composed of "identity", "KV data", "authority", and "contract code".

- "Identity" is represented by a "blockchain address (Address)" and the corresponding asymmetric key pair/certificate;
- "KV data" is the form of account book data, which is uniquely identified by the key, and the content is recorded by the value;
- "Contract code" represents the logic of state changes, expressed in a sequence of contract instructions;
- "Permission" is the access control code of "Identity" to "KV Data" and "Contract Code".

2) Ledger operation set

"Ledger Operation Set" is to define a common standard for cross-chain interoperability, including standard codes for "types" and standard formats for "parameters". Typical operations include:

- Identity registration
- Status data read and write
- Contract deployment
- Contract call

- Permission settings

3) Contract instruction set

Blockchain defines the control and conversion logic of business status in the form of contract language. By designing a standardized contract language instruction set, various complex business logics can be expressed in a general way, which has nothing to do with specific programming languages. On the one hand, following the standard contract instruction set, the blockchain system can have good versatility; on the other hand, developers can write smart contracts in different programming languages, which reduces the learning threshold and meets the requirements of different teams' technology stacks.

4.5 Component model

The Component Model is a logical functional module design that is the logical framework for implementing the ledger protocol.The standardized interface of the components is defined, so that the blockchain system implementation following the component model has loose coupling and interpolable features.

1) Consensus network

The current typical consensus algorithms mainly include PoW, PoS, PBFT, Raft, Paxos, etc. Through comparison, it is found that these algorithms can abstract the following stages in the operation process:

- Transaction proliferation;
- Transaction sequencing;
- Call the transaction execution program;
- Consensus on the results of transaction execution;
- Submit consensus results.

The differences of various consensus algorithms are reflected in the different implementation strategies adopted at different stages.

• The PoW and PoS algorithms do not use the atomic broadcast protocol when transactions are proliferated and sorted. At the same time, the leader node is selected in a randomized manner to perform the sorting, so transactions may be randomly discarded.

• The Raft and Paxos algorithms perform atomic broadcasting and sorting of all transactions, but they do not deal with Byzantine errors during the consensus process.

• The PBFT algorithm performs atomic broadcasting and sorting of all transactions, and handles Byzantine errors in the consensus phase. It does not support dynamic node adjustment.

Starting from the characteristics of industry-oriented commercial-level application scenarios, we select an algorithm similar to the POW+POS mechanism, and optimize on this basis, providing deterministic transaction execution, Byzantine fault tolerance, and dynamic node adjustment characteristics. Millionaire's consensus network components are designed in accordance with the idea of modularization, and are encapsulated based on the above general stages, abstracting scalable standard interfaces.

2) Ledgers and contracts

The ledger state is separated from the contract, and the identity-based access control protocol is used to restrict the access to the state of the contract. This design pattern that separates data and logic is a typical anemia model, which can provide stateless logic abstraction for upper-level business logic.

3) Persistent storage

Defining the persistence format of ledger information as more concise KV format data makes it possible to use mature NoSQL databases to achieve persistent storage. Based on the current mature mass data storage solution on the NoSQL database, the blockchain system can support mass transactions.

4) Contract engine

The contract engine consists of two parts. The front end includes the contract high-level language specification and its tool chain, and the back end is a lightweight contract intermediate code execution environment. All operations on the account book are implemented through the API provided by the account book component.

4.6 service model

The service model function module of Millionaire is divided into four parts: blockchain gateway, blockchain node service, blockchain consensus network, and supporting tools.

1) Blockchain gateway

"Blockchain Gateway" is designed as a lightweight gateway system, usually deployed in the network environment of participants, providing functions including:

- Private key management: provide fully localized private key custody function;
- Privacy protection: use end-to-end encryption to achieve privacy protection;
- Protocol conversion: Provide a lightweight HTTP Restful Service and a blockchain node API that adapts to the TCP protocol.

2) Blockchain node service

The application-oriented general functional components provided on the basis of the blockchain basic network aim to provide the reuse of general functions, including:

- Application-oriented account management;
- Account authentication and authorization;
- Object-oriented ledger data access framework;
- Event notification mechanism;
- Smart contract management.

3) Blockchain consensus network

A network composed of consensus nodes, based on P2P networks and consensus algorithms, ensures that transaction data remains consistent between nodes.

4) Tools

A set of supporting tools, including SDK, data management, installation and deployment tools, and monitoring services.

4.7 Improved NFT asset Agreement

1) Improved data structure of non-homogeneous digital assets (NFT)

Non-homogeneous digital assets (NFT) is a type of digital asset used in distributed accounting networks. The asset instance is unique. By optimizing the structure of non-homogeneous digital assets (NFT), it can serve more flexibly For blockchain online games.

Millionaire redesigned the data structure and added custom data storage to accommodate possible game data and expanded content. At the same time, key processes such as consensus, witness, and block production are adjusted accordingly to match the new data structure. The item data in Millionaire is only fully recorded in the block data when it is generated and attribute changes. During ordinary transactions and circulation, only the hash pointer is recorded to ensure that the volume of the block data will not increase too quickly due to long-term transactions. .

2) Data separation of assets and contracts

Homogeneous, non-homogeneous assets (NFT) and smart contract data are stored separately on the chain. There will be a large number of continuous transactions in Millionaire's network. It is necessary to reduce the computational cost of asset analysis and circulation as much as possible. The separation of assets and contracts can realize the separate analysis and execution of contracts and the operation of necessary results on the chain.

Under the design of separating the storage of assets and contract data, the asset owner has all the rights of the asset, and the operation of the asset can only be completed by the owner's authorization. It can avoid the occurrence of damage to asset properties or calling others ' assets by modifying the content of the contract due to the non-separation of the asset contract, and it is easier to achieve cross-chain acceptance of non-homogeneous assets (NFT) without considering the constraints of contract factors. Therefore, assets Separation from the contract is a safer design.

3) Security guaranteed by modern cryptography

The full name of ECC algorithm is Elliptic curve cryptography (elliptic curve cryptography), which was proposed by Neal Koblitz and Victor Miller in 1985.

Modern cryptography technology is a cryptography technology based on mathematical principles. It has been widely used in a variety of industries in the Internet field. Common symmetric encryption technologies include AES encryption used by WiFi and asymmetric encryption algorithms (public and private key cryptosystems) RSA, ECC, etc., among which ECC (Elliptic Encryption Algorithm) is a commonly used encryption algorithm in the blockchain field. These algorithms use mathematical principles to design an encryption and decryption system with unacceptable solution consumption to prevent encryption from being compromised. Under the premise that the key is not obtained correctly, attempts to crack such encryption algorithms will take too long to implement due to the large amount of calculation (usually it takes nearly a hundred years to try to crack/guess the key system). Lose the value of cracking behavior.

4.8 Price oracle

The marginal price of the t moment (marginal price, excluding handling fees) provided by Millionaire can be calculated with the reserves of asset a divided by the reserves of asset b.

$$p_t = \frac{r_t^a}{r_t^b}$$

If this price deviates (beyond the commission fee), the arbitrageur deals with Millionaire to return the price to normal, so the price provided by Millionaire tends to track the price of the asset in the relevant market.This means that it can be used as an approximate price prediction.

Millionaire calculates and records the price before the first transaction in each block (that is, the last price of the previous block).That price is harder to manipulate

than prices within a block.If an attacker submits a transaction (transaction) that attempts to manipulate the price at the end of the block, other arbitragers can submit another transaction (transaction) for an immediate reverse transaction.A certain miner (or an attacker with enough gas to fill the entire block) can manipulate prices at the end of the block and they have no particular advantage unless they can dig out the next block with special arbitrage advantages.Specifically, Millionaire tracks the cumulative sum of prices at the beginning of each block interacting with the contract, to accumulate the price.Each price is weighted by the time of the block above the updated price, according to the block timestamp.This means that the value of the accumulator at any time (when updated) is equal to the sum of the spot price per second in contract history.

$$a_t = \sum_{i=1}^{t} p_i$$

To calculate the time-weighted average price from time t1 to t2, an external caller can check the value of the accumulator for t1 and t2 time, subtracting the posterior value and divided by the number of seconds elapsed during the period.

$$p_{t_1,t_2} = \frac{\sum_{i=t_1}^{t2} p_i}{t_2 - t_1} = \frac{\sum_{i=1}^{t_2} p_i - \sum_{i=1}^{t_1} p_i}{t_2 - t_1} = \frac{a_{t_2} - a_{t_1}}{t_2 - t_1}$$

The predicted users can choose the start and end time of this interval.Choosing longer intervals can cost attackers to manipulate prices higher, although this can cause price changes to lag.

One complication: Should we use asset B to calculate the price of asset A or the price of asset B?Although the spot price of A calculated with B is always the reciprocal of the spot price calculated with A, the average price of A at a certain period is not equal to the reciprocal of the average price of B calculated with A.

For example, if the USD/ETH price is 100 in block 1 and 300 in block 2, the average price is 200 USD/ETH, but the ETH/USD is 1 / 150 ETH/USD (because the contract cannot know which asset users want to use as an account unit, Millionaire tracks two prices.

Another complication: Is it possible for someone to send an asset to a transaction pair contract to change its balance and marginal price, but does not

interact with it and so does not trigger a price update.If the contract simply checks its own balance and then updates the prophecy, the attacker can manipulate the price by sending assets to the contract before the contract first calls in the block.If the block of the last transaction was X seconds ago, the contract mistakenly multiplied the new price by X, before accumulation even if no user has traded with that price.To prevent this problem, the core contract caches its capital reserve after each interaction, updating the price predictions with the cached capital reserve without the current capital reserve.

4.9 Flash Swaps

In traditional mode, users who buy ABC with XYZ need to send XYZ to the contract before they can receive ABC.This way is inconvenient if users need ABC to get the XYZ, they pay for.For example, users may buy XYZ, with ABC in other contracts to hedge the price on the platform, or they may sell collateral on Maker or Compound and return it to the platform.

Millionaire adds new features to this, allowing users to receive and use assets before payment, as long as they complete the payment in a transfer of the same atom.The swap function calls an optional user-specified callback contract, between which the user-requested tokens are transferred out and enforced as constant.Once the pullback is completed, the contract checks the new balance and ensures that it is unchanged (adjusted for the payment fee).If the contract does not have enough money, it will roll back the full transaction.

Users can also return the same tokens to the Millionaire funding pool without completing the swap.This efficiently allows anyone to quickly borrow any assets from the Millionaire funding pool.

4.10 Protocol fee

The Millionaire includes extremely low protocol fees that can be turned on or off and, if opened, are sent to the feeTo address specified in the factory contract.

Initially, feeTo was not set and no fees was charged.A pre-specified address feeToSetter can call the setFeeTo function on the Millionaire factory contract and set the feeTo address.feeToSetter can also call setFeeToSetter itself to modify the feeToSetter address.

If the feeTo address is set, the protocol charges a 5pb fee, taking 1 / 6 of the 30bp fee from the liquidity provider. Traders will pay 0.3% fees on all transactions, 83.3% fees to the liquidity provider, and 16.6 fees to the feeTo address.

The total fee collected can be calculated using the increase since the last fee collection (k is a constant product).The following formula gives the accumulated charges between t1 and t2 as a percentage of liquidity in the t2 time capital pool:

$$f_{1,2} = 1 - \frac{\sqrt{k_1}}{\sqrt{k_2}}$$

If fee is enabled before time t1, the feeTo address should receive an cumulative fee for 1 / 6 of the t1 to t2 time period.Therefore, we want to cast new liquidity tokens to the feeTo address, among them.

We want a sm to choose to meet the following relationship where s1 is the total circulation share (outstanding shares) at t1 moment:

$$\frac{s_m}{s_m + s_1} = \phi \cdot f_{1,2}$$

After the transformation, which will be replaced by, the solution is given to

$$s_m = \frac{\sqrt{k_2} - \sqrt{k_1}}{(\frac{1}{\phi} - 1) \cdot \sqrt{k_2} + \sqrt{k_1}} \cdot s_1$$

Let, and get the following formula

$$s_m = \frac{\sqrt{k_2} - \sqrt{k_1}}{5 \cdot \sqrt{k_2} + \sqrt{k_1}} \cdot s_1$$

Assuming that the initial depositor deposited 100DAI and 1ETH in the transaction pair, it received 10 shares.After a period of time (if no other depositors participate) they turn the money out, then there are 96DAI and 1.5ETH, of transactions with the above formula:

$$s_m = \frac{\sqrt{1.5 \cdot 96} - \sqrt{1 \cdot 100}}{5 \cdot \sqrt{1.5 \cdot 96} + \sqrt{1 \cdot 100}} \cdot 10 \approx 0.0286$$

4.11 Multi-chain, cross-chain system

In recent years, the popularity of the blockchain has brought about the prosperity and development of the DAPP ecosystem, but as we all know, most DAPPs are facing the same dilemma: the existing blockchain performance on the market simply cannot meet the high concurrency and large Scale application requirements. The specific manifestations are as follows:

• The immutability of the blockchain itself must exist in some applications, but the increasing amount of ledger data makes the blockchain network nodes bloated and heavy, consumes storage resources extremely, and causes storage expansion.

• The homogeneity of blockchain node types is serious, and the execution speed is relatively slow, resulting in transaction scale and transaction speed far from reaching the requirements of high concurrency and high response speed for commercial applications.

• Existing smart contract programming requirements are high, business expression ability is insufficient, and there is no suitable solution for large and medium-sized enterprise applications.

Therefore, Millionaire designed a high-performance underlying platform that supports multi-chain and cross-chain to solve the problem of parallel computing.

1) Multi-chain architecture

The existing blockchain platforms are basically single chains, that is, the entire blockchain network has a unique main chain, but single chains often do not meet actual production standards in practical applications.

First of all, in terms of performance, the performance bottleneck problem of the single chain has not been solved so far. The public chain represented by Ethereum still has the problem of transaction blocking, resulting in long-term transaction delays. In addition, the application layer tends to be more complicated. Requirements, such as business isolation of related businesses. Multi-chain derivative chains will appear under one main chain, sharing part of the business pressure of the main chain. In addition, business isolation can also be achieved through the derivative chain, such as the art traceability business and the transaction business as two different derivatives. The chain performs business processing, which not only meets the complex business needs of the application layer, but also improves the performance of the blockchain network to a certain extent.

Millionaire intends to solve the compatibility problem of different public chains through the cross-chain of Ethereum. Developers can call Millionaire's smart contracts in different public chains. However, it is conceivable that in the technical cooperation of public chains, it is easy to be restricted by the poor performance of

public chains. Therefore, Millionaire adopts the "relay node technology" to divide the link by adding relay nodes. Improve link capacity and efficiency.

In addition, Millionaire solves the problem of non-interoperability of community data through cross-chain technology, and avoids the situation of public chain data closure. In addition, due to the existence of cross-chain characteristics, Millionaire supports cross-chain calls for non-native tokens, such as ETH/ERC20, HT, and EOS tokens, which makes the platform more cross-platform.

In Millionaire, there are several traceability chains, and the game chain is the most basic function of Millionaire, and it is also the easiest part of it.

2) Cross-chain information exchange

Millionaire uses IPLD (InterPlanetary Linked Data) as the cross-chain data exchange structure. IPLD is a standard data model proposed by the Protocol Laboratory (IPFS team). IPLD is a distributed Web data model that connects all data through encrypted hashes, and Make it easy for data exchange and linking.

IPLD components include:

- CID: Self-describing content addressing identifier for distributed systems.

- IPLD tree: A cross-protocol data model based on JSON, Protobu, and path navigation, designed to facilitate interoperability with pluggable format-related parsers.

- IPLD Resolvers: IPLD resolvers can introduce new systems into the IPLD protocol.

It can be seen that IPLD is mainly responsible for the definition of data, namely naming, file data exchange and other functions. In addition, IPLD can treat all hash-linked data structures as a subset of the unified information space, and connect all data with hashes. The data model is unified as an IPLD instance. Therefore, in terms of cross-chain, IPLD can be used as the middle layer of data exchange to realize data exchange between different blockchains and realize cross-chain data intercommunication.

Chapter V MAI General Certified Economic Model

5.1 Distribution of MAI

MAI is a value token circulating in the Millionaire ecosystem and a functional token used on the platform. Its value attribute combines DeFi, NFT and GameFi. This is an interesting and practical one that is widely used in the circulation of various value assets. Designed virtual currency. At the same time, MAI tokens also provide support for the Internet of Everything of DeFi, NFT and GameFi, realize the tokenization incentives of data and assets, and create a new high-value token for global users and investors.

MAI circulation: 1 billion

MAI release rules: 10% per year for all allotments, with a gradual decrease of 10% per year from the second year onwards.

MAI is the governance token of the entire Millionaire. All ecology is developed around MAI, which is used to participate in account records, transfers and payments in DeFi and more applications in the future. In addition, MAI will also take on more roles in the future ecology, maintaining the overall ecological balance while stabilizing the fluctuations in the value of digital currency. As a new generation of DeFi, NFT, and GameFi high-value assets, MAI tokens can seize the commanding heights of the world through various advantageous mechanisms and the use of market gaps. MAI will also realize efficient circulation in the platform ecological scene.

5.2 MAI incentive and circulation model

MAI can be obtained from official task rewards, resource rewards, from the exchange of secondary assets, or through mining. MAI circulates in the Millionaire ecosystem, such as DeFi mining, NFT mining and trading, and Play-to-earn. Users can contribute and earn income in a variety of ways, and can also be converted into other secondary assets.

The incentive methods of MAI include but are not limited to:

• Value creation: including (A) contribution to the creation of digital assets. For a single digital asset, the amount of platform incentives issued is proportional to the value of the asset created by participants, and inversely proportional to the lifetime of Millionaire and the value of the total assets of the system. The total amount of incentives has an upper limit; (B) The contribution of creating the value of digital assets, that is, the creation of assets reaches a certain fee and the scale of asset circulation can obtain MAI. For a single digital asset, the amount of incentives issued is proportional to the total asset circulation of the asset created by the developer;

• Platform contribution reward: Users who contribute to the MAI community can get MAI. In the initial stage, we distributed MAI based on the historical contribution of the developer community. In the later period, the platform will adopt various forms such as bounty tasks and free assets to encourage developers to develop new functions, upgrades, bug fixes, and tests on the platform. This part will be allocated from the platform foundation’ s asset reservation and platform division;

• Asset Circulation: Sell prop assets acquired in Play-to-earn to get MAI. This part of the incentives is related to the Play-to-earn gameplay and economic system, and is determined by the Play-to-earn developers and market rules. In principle, the platform does not impose rules and quantity restrictions;

• Behavioral incentives: A variety of effective behaviors in Millionaire, the community and the platform Play-to-earn will be converted into MAI according to a certain degree of contribution. For example, users register platform accounts and participate in various interactions in the community to obtain MAI. The platform

confirms whether the user's behavior is effective by analyzing the dimensions of access validity, information integrity, and behavioral rationality, and provides MAI incentives. The number of incentives in this part is directly proportional to the interactive content, inversely proportional to the total number of users on the platform, and the duration of the platform. There is an upper limit on the total amount of incentives;

- Contribution rewards for MAI consensus work.

After users obtain MAI, MAI will have a wider area of circulation. MAI can be exchanged with all digital currencies on the exchange, and MAI is settled with global legal currency. MAI supports circulation and payment in all aspects of the ecology, such as receipt and payment, transfer, legal currency transactions, deposits, withdrawals, voting for listings, STO gateways, coin distribution, mortgages, public welfare, game malls, etc.

In addition to circulation in the Millionaire ecosystem, it will also be circulated in third-party applications developed based on Millionaire technology and exist as the only value token. This will accelerate the circulation rate of MAI, add more circulation value attributes to scarce MAI, and increase the overall value and price. For players, MAI can be used for game consumption. At the same time, it can also be used as a basic means of cross-border payment, thus bringing more benefits to itself. When MAI is connected with global mainstream platforms, players can enjoy the broader global convenience brought by MAI.

MAI usage scenarios include but are not limited to:

- Exchange development resources from third-party developers;

- Exchange value-added services such as developing functional components from the platform;

- Buy game gold coins and prop assets from Play-to-earn or asset circulation platforms. Based on the asset rights management mechanism of the platform, a certain fee is paid to the developer for each transfer of the props in its complete life cycle;

- Post reward tasks in the community, initiate and participate in voting on community affairs.

In the future, through continuous improvement of application business model exploration, MAI will adapt to more diversified business needs and meet data sharing across business chains. This means that MAI has sufficient commonality and standards for data recording methods and can express various structures. And unstructured information, and can meet the cross-chain requirements required by the expansion of business scope. And this provides more value flow basis for the versatility of MAI.