JOIN Protocol White Paper

Highly Reliable Oracle Protocol

Data in, trust out

2020-07

1. Preface

The term Smart Contract can be traced back at least to 1995, as the prolific interdisciplinary legal scholar Nick Szabo desbribed it: “a smart contract is a set of promises defined in digital form, which includes protocols allowing contract participants to execute them.” But long after Szabo proposed the theory, there was no clear path to practice until the birth of Ethereum.

With continuous attempts in the field of smart contracts, decentralized finance (DeFi) has created a challenging and exciting field: the future smart economy paradigm. The future smart economy will have the characteristics of decentralization, intelligence, equality, and liberalization. Based on the provided characteristics, the service can be used by anyone without obstacles or need for auditing, as long as it meets clearly defined requirements of smart contract.

Only when smart contracts are executed on a decentralized infrastructure (such as Ethereum) can it be ensured that the

implemented execution criteria will not be changed under interference from any party. Based on this reliable model of decentralization, individuals in the world can ignore the differences in geography, language, and culture, and reach a certain kind of cooperation or transaction, which leads to a further liberation of the entire human civilization. But the two-sidedness of smart contract also bring shackles to its development. Smart contracts need more data generated by human activities to build a ever richer smart economic paradigm. This requires a highly reliable way to transmit off-chain data, which is called "oracle".

JOIN Protocol is proposed to solve this problem, and is committed to creating a highly reliable oracle protocol for the future smart economy paradigm. JOIN Protocol has four major characteristics: 1) random and transparent block producing strategy, 2) complete game anti-cheating design, 3) native decentralized economic model, and 4) multiple data providing solutions. These characteristics are also the basis of a new generation of highly reliable oracles.

2. Architecture Overview

In the future situation of coexisting multiple chains, JOIN Protocol will be constructed by separating assets and business logic; assets will be managed by smart contracts on different public chains, and data collection and consensus logic will be achieved by a series of components-built oracle network cluster. Tokens will be issued on Ethereum and circulated on other public chains through reliable cross-chain technology.

JOIN Protocol has two node roles: oracle node and guardian node. The network protocol of oracle node(s) and guardian node(s) are the same, the former is used to provide the oracle data service and the latter is used to supervise oracle node(s). Guardian node(s) election is completely open, any candidate can join as long as the staking requirements are meet. Elected oracle node(s) can run guardian node(s) at the same time, and the two kinds of nodes together form a healthy and game-based oracle network.

In addition, viewed from structural perspective, JOIN Protocol can be divided into on-chain contracts and oracles network protocols. The interactive contracts on the chain includes: ranking contracts, result contracts, matching contracts, risk control contracts, arbitration contracts, etc.; oracle network protocol includes: efficient P2P communication network, threshold signature, data source collector, public chain adapter and other components.

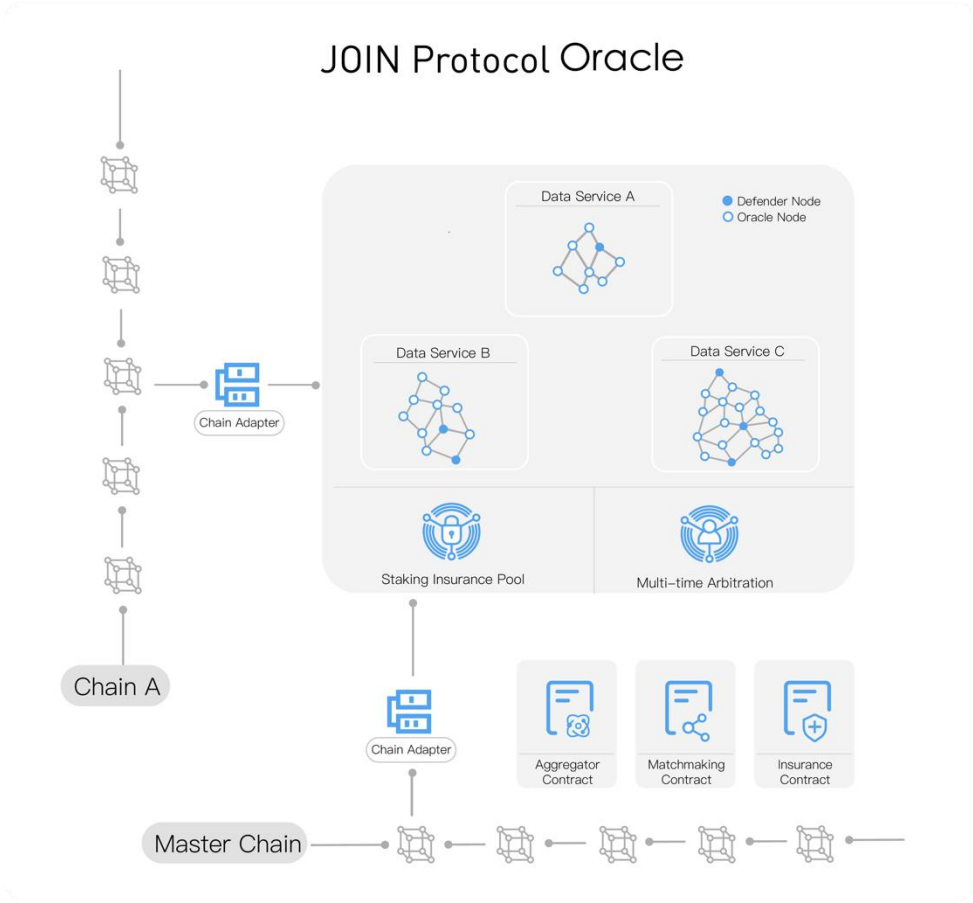

Figure 1 JOIN Protocol architecture diagram

3. Highly reliable oracle protocol

The smart contract using oracle service is represented by DeFi applications. DeFi requires the accuracy as well as the authenticity of data in order to obtain it in various scenarios with different reliable methods. JOIN Protocol is designed for such scenarios.

3.1 Random and transparent node block production strategy

"Trustworthy" is the fundamental condition for transactions in the real world. We cannot achieve any transaction without trust. Trust is so important, yet in many cases difficult to achieve. It often has to depend on the credibility of both parties to the transaction or on a trusted third party. In complex scenarios, this leads to increasing risks and costs. Some oracle services are designed based on the assumption of trusted or authoritative data sources. Such assumptions are theoretically risky and cannot guarantee the authenticity of the data provided by such sources.

Relying on an open consensus mechanism for proof of computing power, Bitcoin has become an example of a credible decentralized economy. With the attempts and verifications of other consensus mechanisms, PoS has become a relatively efficient and decentralized consensus mechanism. However, in order to avoid the potential systematic risk of the "giant whale", different public chains have made various adjustments based on their own situations.

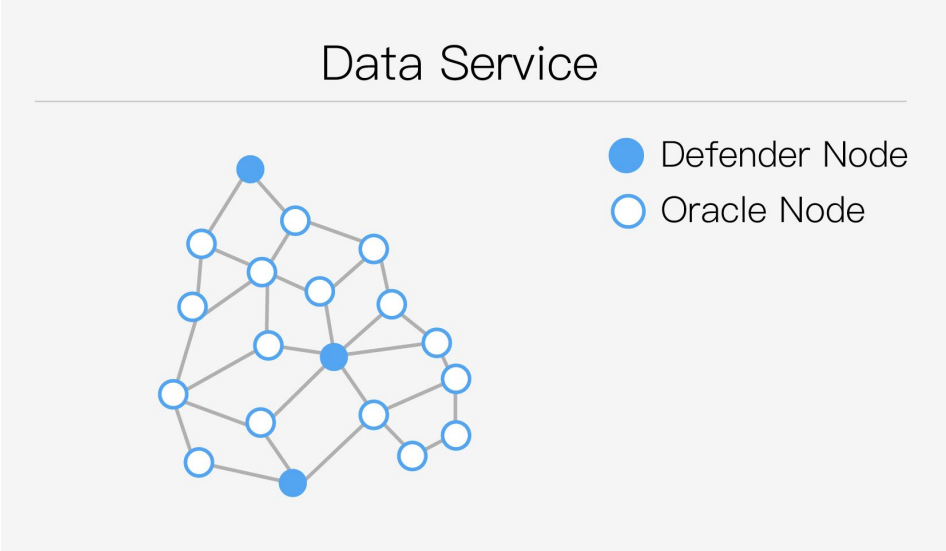

Figure 2 JOIN Protocol data service topology diagram

JOIN Protocol will use a PoS consensus mechanism with verifiable random functions to reach a credible consensus on oracle data. For an oracle data service, the oracle service

network will be formed by no less than 15 data providers with the highest staking amount, and the result only signatured by no less than 3/2n+1 nodes will become the result of the data service.

3.2 Anti-cheating design with complete game

The oracle machine is a concept introduced by the Turing machine model. Due to the halt problem and mathematical incompleteness, the introduction of this concept will lead to certain results that cannot be obtained by the standard Turing machine. In the Turing machine, the result is certain, but this feature of certainty can hardly be achieved in a oracle machine built on blockchain(s). The reason is that the blockchain itself is built on fault-tolerant logic. The certainty of input is not required, and even deception is tolerable, which is why the blockchain builds on the Byzantine fault-tolerant structure. Therefore, a blockchain oracle is essentially different from a traditional oracle.

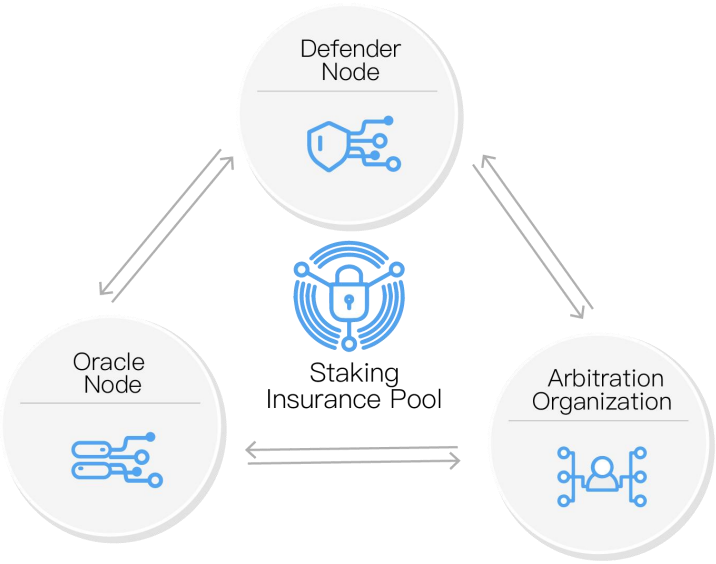

Figure 3 Role relationship of JOIN Protocol game model

Facing the problems of untrusted data providers, the simple deterministic calculation model is obviously powerless. For this reason, we introduce the game system model to solve these problems. In a nutshell, the oracle is not simply regarded as the information supply point of the system, but as a game model constructed by the participants of the game and the information user. And it aims to establish credible commitments through the introduction of a punishment mechanism and a multi-round game mechanism as well as to reach the Schelling point through the information selection mechanism of multiple information

supply points. As a result, the credibility of information will be improved. In addition, by introducing guardian nodes and adding rewards and punishments, the prisoner’s dilemma of data service providers further ensures credibility.

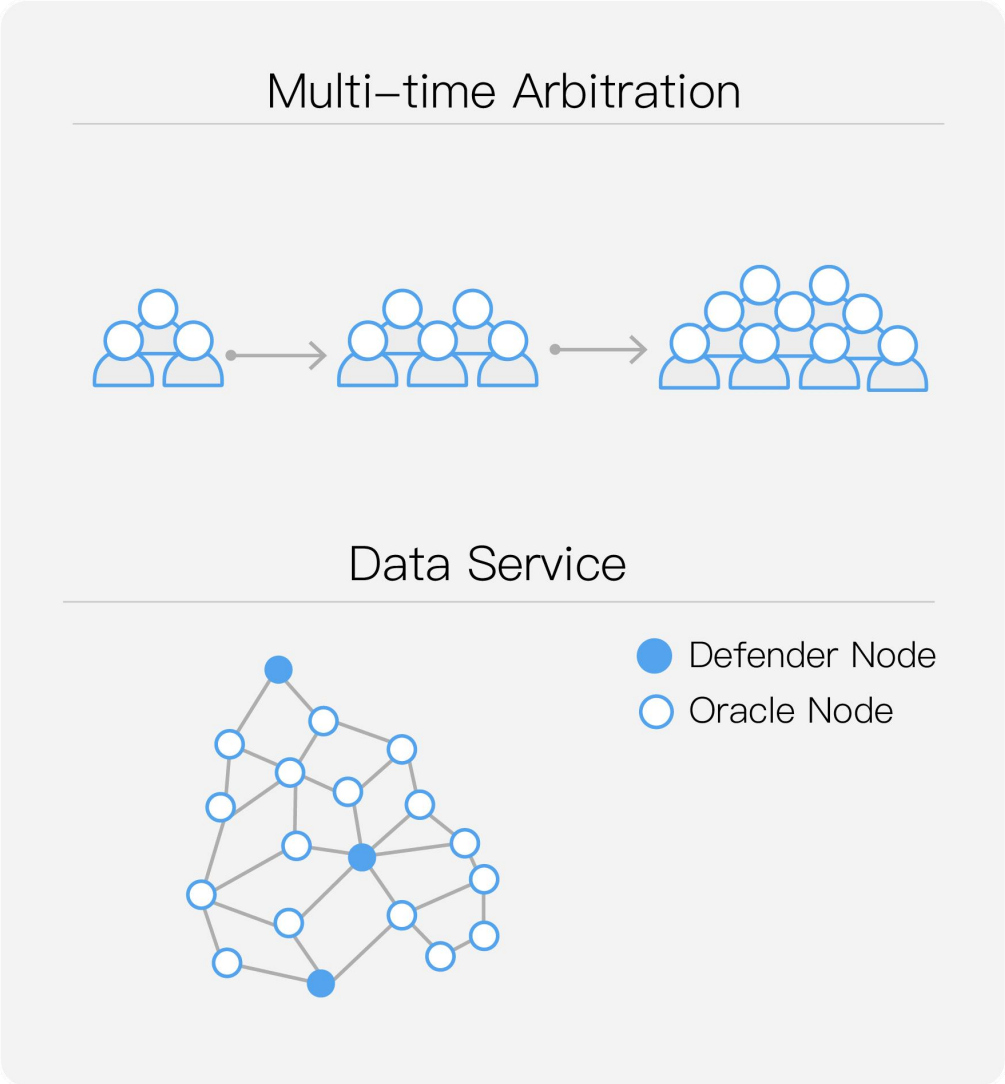

Figure 4 JOIN Protocol game model

The following discusses the cheating situation under this game model.

Assume that the data provider set is [dp1,dp2,...,dpi,....,dpn], where:

- The set contains a total of **n** elements
- Where **dpi** is the data provider numbered **i**
- For any data provider, assume that the number of times it has provided services is **Ki**
- The income of each data provided is **X**, the staking coefficient is **dr**, and the basic staking amount is **db**

For any data provider **dpi** providing this service, the total amount pledged is:

$$Ki*X*dr + db$$

The total staking amount in the entire data set of this type is:

$$Z = X*dr*\Sigma Ki+n*db$$

In a case where the oracle data is related to the allocation of asset(s) in amount of **Y**, when **Y=Z**, it can be achieved that even if the interested party(s) collude with all the data providers and cheat, victim(s) can get **100%** of their loss back after winning the arbitration.

In the statistical sense, the average time from application of data to discovery of data errors is called the "reaction period". For low-density data, **Y=Z** is the equilibrium point because of a longer reaction period; but for high-density data applications, since multiple allocations can be made during the reaction period, it is impractical to consider a single case only. The following assumes that **T** allocations can be made during the reaction period, then the single-time tolerable risk value is:

$$(X*dr*\Sigma Ki+n*db)/T$$

Assuming that the total amount involved in this asset allocation is **Y**, and for **n** data providers, their cheating income is **Y/n**. Regardless whether data users discover the problem or not, cheating is meaningful only when **Y/n>Z-X*dr*Ki+d**, otherwise honest reporting would be the best strategy. Further assuming that everyone has the same stake, then **Y/n=Z*(n-1)/n => Y=Z*(n-1)**, which means that in this sense, the balance point has risen to **Z*(n -1)**. Considering that the guardian node and each data provider can file a complaint, this will evolve into a typical multiplayer

prisoner's dilemma, and honest reporting will become the optimal strategy.

In the above model, only one game is considered. Since the system is essentially a model that repeats multiple games, in the long run, for oracle data providers with stable income, the cost of betrayal will be far greater than the theoretical value discussed above after part of their identity data information has been publicized. The provider’s characteristics as rivals will not change in multiple rounds of games.

The rules of the system are static and predictable for rational participants. Therefore, honest and fair participation is advantageous strategy. In addition, irrational participants will probably be punished in the system as well, thus enabling the entire oracle service to operate in a positive, healthy and efficient manner.

3.3 Native decentralized economic model

From the perspective of group behavior, the oracle can be regarded as a group cooperative behavior mode under which the task is executed by some while supervised by all. It is necessary to develop a set of incentive mechanisms to allow different roles to perform their duties.

The JOIN Protocol will have a "Staking Insurance Pool (SIP, Staking Insurance Pool)" mechanism. The role of the Staking Insurance Pool is to encourage the community to participate and to provide risk indemnity for small probability accidents.

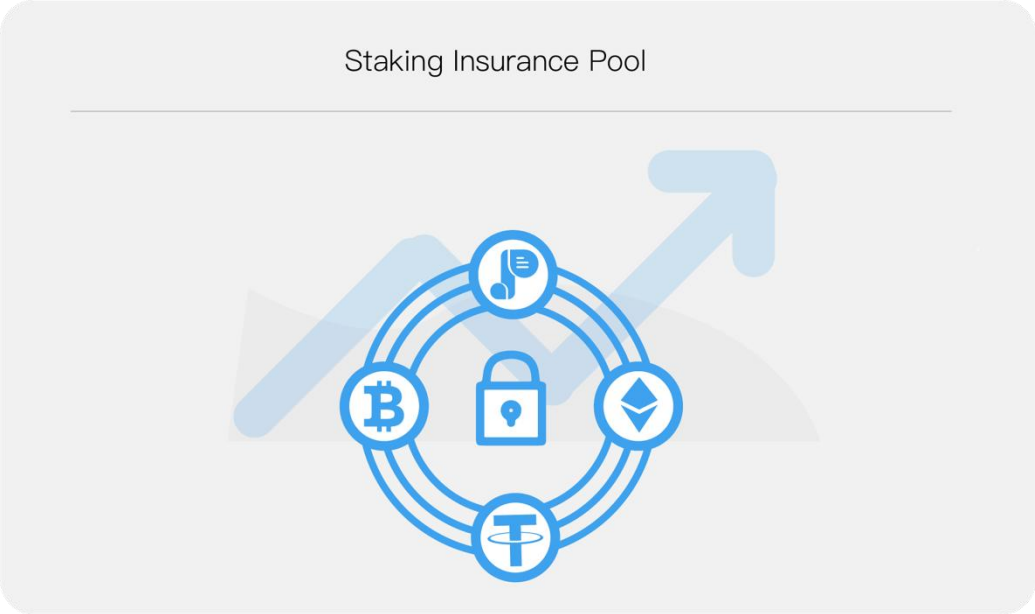

Figure 5 Multiple digital assets supported by Staking Insurance Pool

Staking insurance pool reward source:

- 20% of the data users pay will enter the insurance pool
- 38% of the total amount of JOIN tokens will be gradually released to the insurance pool

Staking insurance pool rules:

- There is no threshold, anyone can stake their JOIN tokens and get income
- The reward is allocated proportionally according to the amount of JOINs staked
- In case of accident, the insurance pool will use 1/3 of the tokens staked by data provider(s) to compensate the user(s)
- Cancellation of staking requires a 3-day payback period

The staking insurance pool itself is a decentralized intelligent economic model that can continuously promote the development and growth of the JOIN ecosystem.

3.4 Multiple data provision schemes

JOIN Protocol provides multiple ways to realize data allocation, which ensures that the oracle service is always available in complex calling scenarios.

3.4.1 Data directly written on the blockchain

Data provider(s) writes the data onto the chain first for the user(s) to read. In this way, some free external data can be provided. This scene data is open and has no access threshold, which can promote the diversity of the basic ecology of JOIN Protocol.

3.4.2 Monitor callback

The data provider(s) monitors the call event and actively pushes the data to the user through an on-chain manner.

This scenario will be the main form when public chain resources are relatively sufficient.

3.4.3 Off-chain callback

The data provider monitors the call event and actively pushes the data to the user through an off-chain manner. Compared with the 3.4.2 form, this form can avoid exposing any data on the chain and therefore secure privacy.

3.4.4 Completely Off-chain Interaction

The data interaction is completed off-chain, and the reliability of data is ensured by signature(s). This form relies on data verification through private key signature(s), which can avoid service unavailability caused by the shortage of public chain resources.

4. Data Market

Due to the differences in the technical solutions and capital investment of different teams, better oracle service providers will be more favored by the market after a period of competition. The data market of JOIN Protocol is not only an open store for oracle services, but also a content precipitation platform communicating with its users. The data market can perform intelligent analysis, classification, and ranking based on the statistical data on the chain according to different dimensions; users can also conveniently compare the oracle services of the JOIN Protocol and quickly find the data services that meet their demands. Users can also publish customized data requirements and then reward organizations with corresponding data resources in the community for such services.

5. Long-term technology strategy

5.1 Extension to multiple financial scenarios

The development of financial services is gradual and interlocking. Financial products can be divided into two categories: basic securities (such as stocks, bonds, etc.) and derivative securities (such as futures, options, etc.). Additionally, financial products can be divided into property rights products (such as stocks, options, warrants, etc.) and debt products (such as Treasury bills, bank credit products, etc.) according to the attributes of ownership.

Currently in the blockchain world, DeFi is still in its early stages of development. Compared with financial services in human life, it is still in need of richer infrastructure. This requires oracle to continuously promote the abstraction of industry scenarios and the specification of data services.

5.2 Trusted data provision based on zero-knowledge proof

With the development of encryption technology, credible private data will become an important form of blockchain oracle service. For this reason, JOIN Protocol will build a verifiable confidential data oracle service based on zero-knowledge proof . This service is mainly aimed at scenarios where data confidentiality requirements are high and data validity can be quickly verified, which makes the markets of private data on blockchain possible.

5.3 Smart Channel for IoT Data Transaction

With the accelerating implementation of 5G technology, a wealth of business scenarios will emerge. A large number of smart devices will generate tons of data, which will make more urgent the demand for data transaction under various scenarios, such as the climate data in a certain area, the information collected by wearable devices, etc. JOIN Protocol will launch smart channel(s) of data transaction for IoT industry, creating a complete technical solution and path from data generation to data consumption for IoT devices.

5.4 Whole chain risk control

Although the related game methods introduced by relying on the "staking model and multi-round game" can optimize the benign operation of the entire system, it may still face the most complicated cases and unpredictable situations despite their small probability. As a result, the security of the entire system must be further strengthened. In order to maximize the security of system, the design will consider the security of data and funds in the worst case of multi-round fraud. In extreme cases, data providers unified as a single entity to participate in the system, opening the possibility of committing multiple frauds in a short period of time. Under this situation, the simple consideration of a single-round game can no longer be adequate, thus the introduction of a risk control mechanism including a combination of time-limited freezing and delayed token allocation is required to solve the problem and guarantee the punishment of Evildoer(s).

6. Economic model

A good economic model design is the foundation for the stability and prosperity of the entire ecosystem. For JOIN, it goes a step further. The economic model of JOIN also plays the role of building and improving the security of oracle service. Since the entire oracle is built on the basis of game theory and the game relies on the prerequisite that the staking mechanism serves as the anchor point of punishment, the economic model of JOIN will adopt a combination of multi-token hybrid staking and staking-rate-based allocation to ensure and enhance the stability of punishment anchor, which leads to an enhanced deterrence and sensitivity to evildoer(s).

In addition, JOIN can not only motivate honest data providers by adopting a scheme that combines allocation strategies with game roles, but also promotes guardian nodes to supervise data providers. As a result, the reliability of data will be improved. The introduction of staking insurance pool mechanism will increase the staking rate of the entire ecology as well as provide compensation for building a secure system, pushing the safety of oracle to a whole new level.

While fully considering the role of economic models on safety of oracle, JOIN's incentive plan will also attract more people to participate in ecological construction. While realizing the enhancement of the oracle security, it also deepens the concept of decentralization and fairness. Everyone can be a participant of the oracle, everyone can be a safe contributor to the oracle, and everyone will also be a beneficiary of the oracle's incentives. Regardless of the value of JOIN or the safety of the oracle itself, this will undoubtedly form a virtuous circle.

As an oracle protocol that provides highly reliable data, JOIN Protocol embraces fairness and stability as its core concepts. The release strategy of JOIN token will take into account the amount of token staked and the frequency of oracle usage, and then adjust the daily release of tokens. The circulation of tokens has established a correlation with the activity of oracle usage, which makes the tokens in circulation reach a dynamic balance with the scale of use and difficulty of

acquisition, and further maintains the system stability and token value.

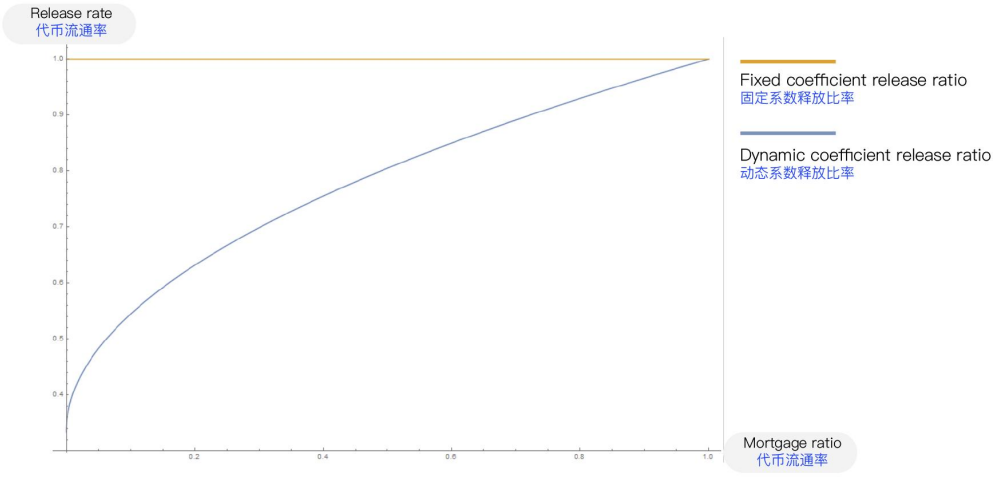

Figure 6 Comparison of release rate between fixed release and dynamic release

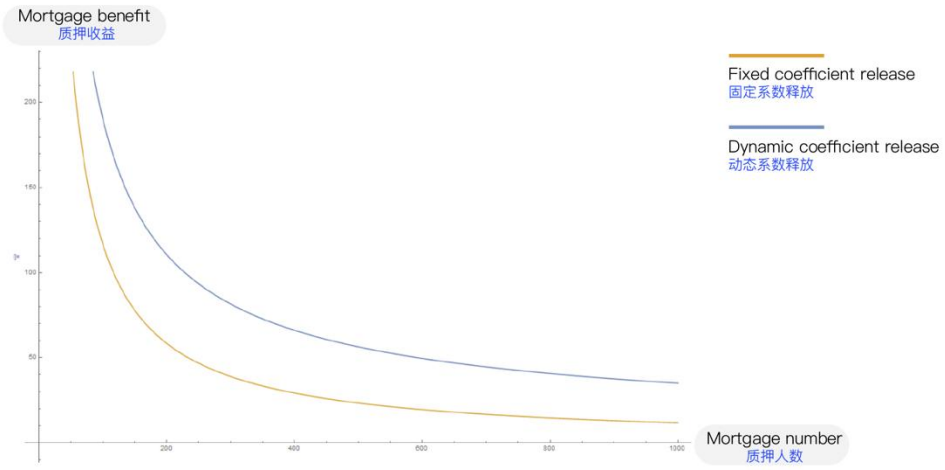

Figure 7 Comparison of return rates between fixed release and dynamic release

As shown in Figure 6 and Figure 7, the adjusted daily release rate will increase as the staking rate and call frequency increase. When more people participate in the oracle system, there will be nearly 2/3 of the adjustment space, which makes the mining revenue curve more flat and participant’s revenue less volatile. Consequently, the expectation of JOIN token value will be stabilized.

Token incentive scheme:

Name: JOIN

Total supply: 21,000,000

Allocation:

- 38% data providers incentives
- 38% staking insurance pool
- 10% data users incentives
- 10% genesis mining
- 4% ecological Fund

In addition to the ecological fund, 10% of the released tokens from data provider incentives, staking insurance pool, data users incentives and genesis mining will go into a project development fund.

Genesis mining will be allocated daily according to the proportion of locked Uniswap LP Token, including USDT-ETH, USDC-ETH, DAI-ETH, SUSD-ETH, JOIN-ETH (2 times reward), USDT-JOIN (2 times reward). Support for other currencies will be adjusted according to the results of community voting.

The ecological fund which will be used for incentives for arbitration and ecology construction will be released in accordance with the rules.

The function of daily allocation amount S is:

$$S = (2/3 * (F1*q*F2 + (1-q)*F1) + 1/3) * S0$$

among them:

- S0 is the allocation amount in the first cycle, with a value of 7000
- q is the adjustment coefficient, with a value of 0.1
- S0 will be halved every time half of the JOIN is released
- F1 = (s/t)^0.5; F2 = i/max_i
- s: JOIN staked amount
- t: JOIN total circulation

- i: the frequency of the current service being called, 5000 blocks are the statistical period
- max_i: latest maximum call frequency
- F2 value range (0, 1)

7. Conclusion

JOIN Protocol builds a multi-role game model, combined with technical solutions such as community staking mining, dynamic release model, etc., it can well solve the shortcomings current faced by other oracles. JOIN Protocol will become a new generation of highly reliable oracle standard protocol, creating a reliable data service network.

JOIN Protocol will become the basic platform for the data required by the future smart economy paradigm, making the value of blockchain technology move beyond currency attributes and expand into the area of constructing financial products and the formulating rules. This will solve or improve many real-world trust issues, thereby expanding the application boundary of blockchain.

8. References

[1]: Prisoner's Dilemma: John Von Neumann, Game Theory and the Puzzle of the Bomb

[2]: Jurišić, Marko, D. Kermek and M. Konecki, 2012, “A Review of Iterated Prisoner’s Dilemma Strategies,” Proceedings of the 35th International Convention MIPRO, 1093－1097.

[3]: －－－, 1994, Playing Fair: Game Theory and the Social Contract 1, Cambridge, MA: MIT Press.

[4]:－－－, 1997, “Rationality and Backward Induction,” Journal of Economic Methodology, 4: 23－41.

[5]: Verifiable Random Functions

[6]: Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme