ECONOMY WHITEPAPER

2020/5

Crust Economic Model & Asset System Draft

1. Overview
2. Economic Design Goal
3. Crust Participants
    3.1 Validators
    3.2 Candidates
    3.3 Guarantors
    3.4 Users
4. Crust Token
    4.1 Token Functions
    4.2 Generation and Burning
    4.3 Token Values
5. Economic Model
    5.1 GPoS Consensus Design
    5.2 Gas Fee Composition
    5.3 Penalty Mechanism* (unfinished)
6. Trading Market
    6.1 Storage Resources Market
        6.1.1 File Storage Service
        6.1.2 File Retrival Service
        6.1.3 Fishing Task
    6.2 Computing Resources Market
    6.3 Token Trading Market
7. On-chain Governance
8. References

1. Overview

As a decentralized cloud system, Crust serves as a distributed network that is public and open to everyone to participate freely. This system was incubated by the Foundation, and it will eventually be self-governed by the community after the growth period. In this system, whether it is a cloud service provider or demander, or various interested parties who maintain the system, they can freely enter and exit under the premise of following the system agreement. Crust's economic model can maintains the interests of all parties and guarantee the development of the entire Crust system.

2. Economic Design Goal

The goal of Crust economic design is to keep the interests of all participants increase in the same direction as the value growth of the Crust system. On the one hand, it is essential to protect the rights and benefits of all participants; on the other hand, it is also necessary to maintain the stability of the Crust system. That is, each participant will contribute to the Crust system while pursuing their interests.

To achieve the goal of Crust economic design, we will consider from the blow several aspects:

How to ensure the security of the Crust protocol

How to keep the sustainable development of the Crust system

How to protect the interests of participants

How to manage the interests of the participants and the value of the Crust system in the same direction

Before describing the design of the Crust economic model, let us first analyze the model of the existing distributed system:

Bitcoin, as one of the earliest blockchain protocols, uses native tokens to incentivize nodes to verify transactions, and also applies PoW consensus to coordinate competition between nodes. In Bitcoin's economic model, early block rewards act as the primary way to protect the interests of nodes. After the block reward decreased in the later period, the fee income has become the essential method to guarantee the node's interest. There are two commonly accepted functions of Bitcoin: value storage and circulation payment. Regarding value storage, users expect to hold or increase the value of tokens, so they pay more attention to the security and deflation policies of the Bitcoin network protocol; regarding circulation payment, users employ the peer-to-peer value transmission function of the Bitcoin network, which is similar to the fiat currency payment function, so they pay more attention to Bitcoin transaction fees and value volatility. On the premise of without changing the existing bitcoin economic model, value storage defends the interests of users. In this kind of user-led network, transactions will not happen so much; so in the long run, it is difficult to retain the operation of the node while ensuring network security. This will affect the sustainable development of the entire system.

Ethereum is the largest smart contract platform, and its native token is used to pay for computing services. Similar to Bitcoin, after the block reward reduced, service fees may become the primary way to preserve the interests of nodes. The difference is that there are more users involved in circulating payment in the Ethereum network, and its monetary policy is not fixed yet and is now an inflation policy. The planned ETH2.0 system changes

the consensus of Ethereum to PoS and is designed to protect the node's interests with sustainable inflation. However, inflation will affect the value of the token and its economic model will try to balance this relationship as much as possible.

After studying the models of other distributed projects, Crust proposed the Crust economic model and asset system according to its characteristics.

3. Crust Participants

There are multiple parties in the entire Crust system, and they have different needs. According to the way each role participates, we divide them into validators, candidates, guarantors, and users. The users mentioned in this article mainly refer to users involved in storage and computing resources. At Layer 2 there will be other different user roles, such as a token market maker.

3.1 Validators

The validator is a node that generates blocks and includes blocks in a package in the Crust network to maintain the entire blockchain network. According to the GPoS (Guaranteed Proof of Stake) consensus of the Crust network, the validator node needs to stay online and have sufficient storage resources and workload as a guarantee to staking the corresponding amount of CRU tokens (the native tokens in the Crust network described in detail in the next chapter). So the validator node is also a node that provides storage resources. The validator nodes participating in the network can obtain the rewards for the packaged blocks individually and share the reward of each cycle of the blockchain, but also needs to bear the risk of being slashed. The validator can also obtain profits by selling storage resources on the storage trading market.

3.2 Candidates

The candidate is a node that competes in the Crust network to become a validator but does not qualify for verification. Like the validator node, the candidate also needs to stay online and possess storage resources and workload as a guarantee to staking the corresponding amount of CRU tokens. The difference from the validator node is that the candidate node does not participate in the generation of the block, and cannot receive the exclusive reward for the block generation. Candidate nodes can obtain the reward share of each cycle of the blockchain, and at the same time, they can also exchange storage resources on the storage trading market to obtain revenue. Candidates and validators are not fixed, their identities may change every cycle, which mainly based on the staking number of tokens at the end of each cycle.

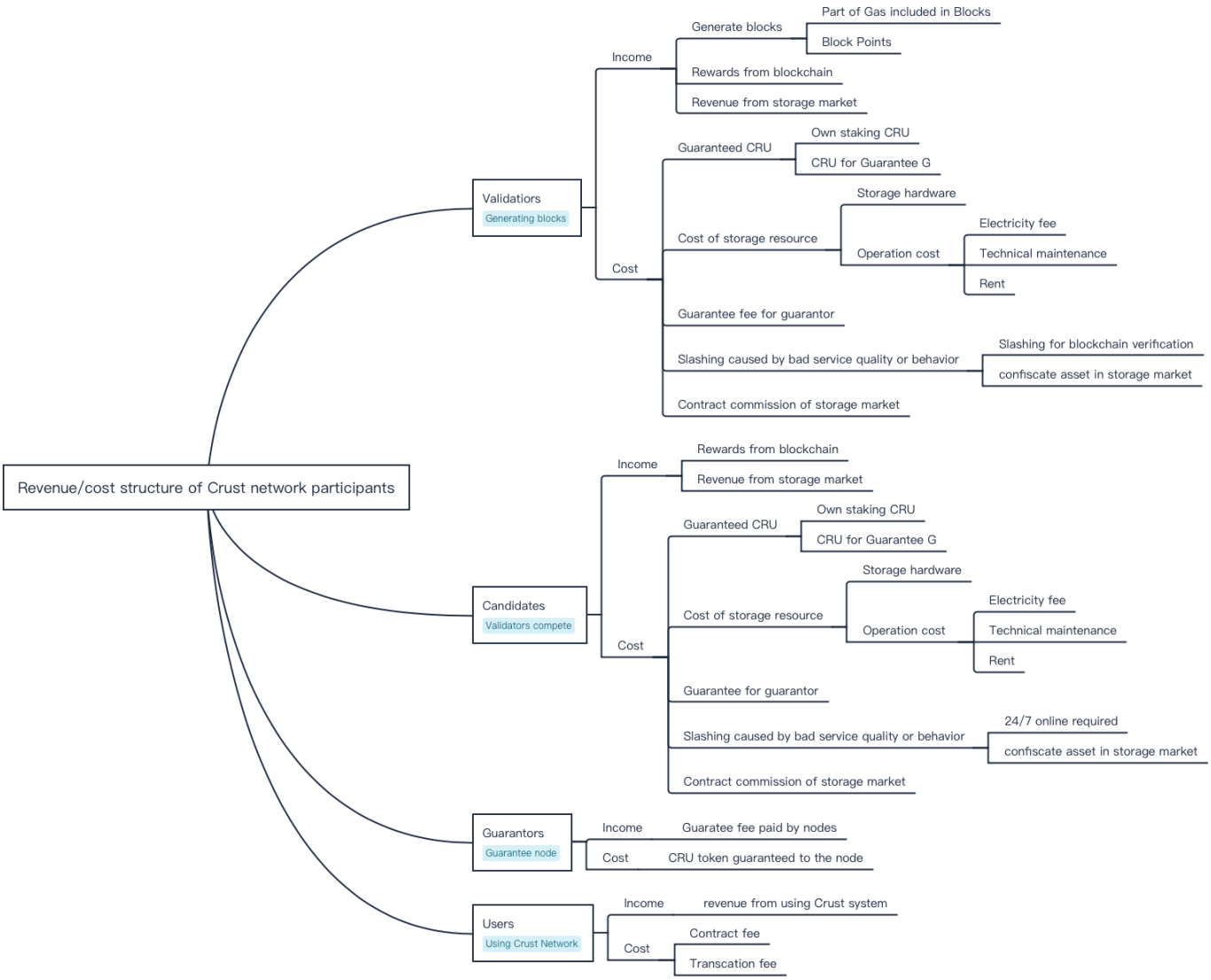
3.3 Guarantors

The guarantor is an account provided by any one or more nodes in the Crust network. Accounts with CRU tokens can become guarantors, and their CRUs can be used as guaranty assets. The guarantor can obtain guarantee income from the node, and shall also bear the penalty risk of its guaranteed nodes in proportion.

3.4 Users

Users apply Crust network resources, mainly refer to those who involved in storage and computing resources, and who can also use CRU tokens or other token assets supported in the Crust network to purchase resource services.

The revenue/cost structure of each participant is as follows:



4. Crust Token

The native token CRU in the Crust network is a utility token representing the value of the entire network, similar to ETH in the Ethereum or DOT in the Polkadot.

4.1 Token Functions

In the Crust network, the CRU token mainly has the following functions:

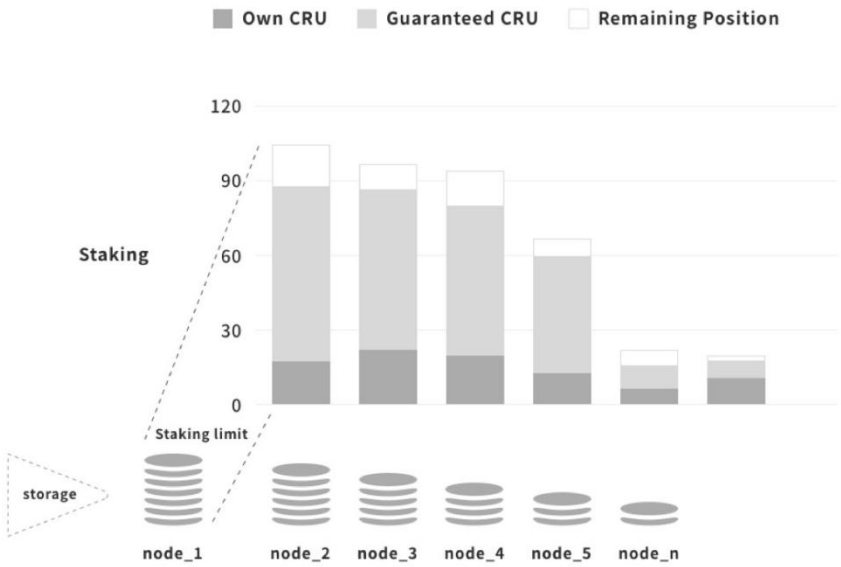
1. Staking to maintain the GPoS consensus of the Crust network
2. Used to guarantee the selected nodes
3. Serving as contract guarantee and commission for providing resource services
4. Serving as a transaction fee for using the network
5. Used to purchase resource services
6. Used for election and voting of on-chain governance mechanism, and vote on proposals

The blockchain consensus in the Crust network is GPoS consensus, which is called Guaranteed Proof of Stake. GPoS is a kind of PoS consensus mixed with PoW. The

mechanism combines PoW resource fairness and the high performance of the PoS chain. Similar to the existing PoS project, the node needs to use the CRU token for staking to compete for the right to generate blocks. The difference is that the node also needs to have storage resources or workload as a guarantee. Only with the guarantee amount can the corresponding number of CRUs be staked. Under this mechanism, two types of assets, storage resources, and CRU tokens are required to become a node, combining the advantages of a resource-based (such as Bitcoin) and a token-based (such as Cosmos) consensus mechanism can more effectively ensure the security of the network. If you want to attack the Crust network consensus, in addition to having a large proportion of CRU tokens, you also need to be able to control a sufficient amount of storage resources. This design will make the difficulty of the attack particularly high.

Nodes can also allow other guarantors to stake CRU as a guarantee under the premise of having a storage resource and workload guarantee. That is, the staking CRU on the node can be own or from other guarantors. When the guarantor applies the CRU to guarantee a node, the number of the guaranteed CRU and the CRU staked and owned by node runner will add up into the total staking CRU on the node. To attract guarantees, nodes will pay for the guarantee. And the guarantee fee rate is set by the node runner. On the one hand, the guarantor chooses a certain ratio of income he is willing to accept when guaranteeing the node. On the other hand, the guarantor also needs to bear the corresponding rate of risk as the node being punished. If the node is penalized by the system for triggering the penalty mechanism, a certain part of the guarantor ' s staking will be deducted according to the agreed guaranteed ratio. Under this mechanism, the guarantor will tend to choose to stake on the nodes with good faith and service quality. Finally, it will become the market to determine a balance between guaranteed income and penalty.

The operation of GPoS consensus is shown in the following figure:



As a network protocol for storing underlying data, Crust provides the function of trading storage resources. CRU tokens are used as contract guarantee funds in this trading market to protect the order of the trading market.

Similar to other blockchain projects, the CRU token will not only be used as a transaction fee for using the network, similar to Gas in Ethereum but also directly used to purchase resource services in the network.

The governance mechanism of the Crust system will allow the use of CRU tokens to conduct parliamentary elections on the chain and take a vote on proposals.

4.2 Generation and Burning

There are two ways to generate CRU tokens: one is generated at one time when the main network is initiated; the other is generated as blocks are produced.

The number of genesis blocks as Crust initiated main network: 20,000,000 CRU

Mainly used in the following aspects:

7,000,000 CRU Community development # Including Lockdrop, Worklock, etc.

1,000,000 CRU Used for Crust ecological construction

4,000,000 CRU Transfer to a professional investment institution**

4,000,000 CRU Reward the technical team

4,000,000 CRU Crust Foundation reservation

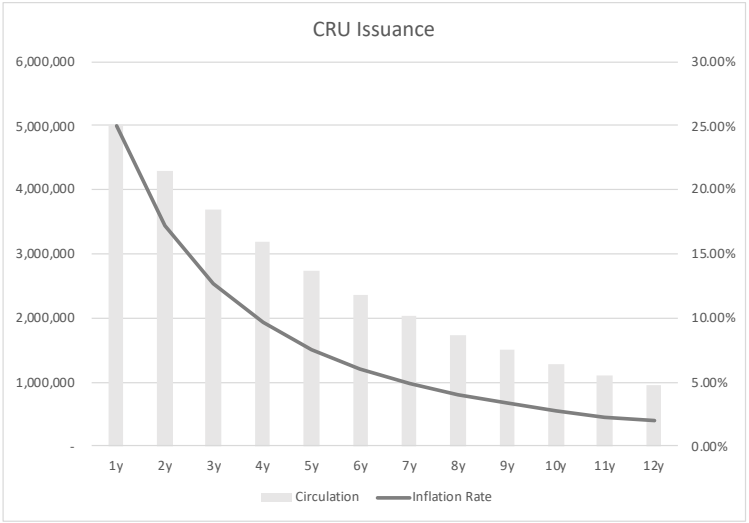
The tokens generated by the block have rewards every cycle, and the points can also be redeemed for rewards. The rewards are mainly for participating nodes in the network to maintain the security of the network protocol. And encourage participation in the network at an early stage. The total distribution method is as follows:

First Year 5,000,000 CRU

From the second year onwards, it will be reduced by 12% each year, and will not decrease until the inflation rate of the whole network reaches 2.8%. The specific data is as follows:

Chart:

Time	Issuance	Inflation Rate
1y	5,000,000	25.00%
2y	4,400,000	17.60%
3y	3,872,000	13.17%
4y	3,407,360	10.24%
5y	2,998,477	8.17%
6y	2,638,660	6.65%
7y	2,322,020	5.49%
8y	2,043,378	4.58%
9y	1,798,173	3.85%
10y	1,582,392	3.26%



If the service quality of the node is unstable or node is found with malicious behavior, it will face the confiscation of the staked CRU. Some of the confiscated tokens will be directly burned, and some will be placed in the Treasury account as a reserve. Some of the fees

incurred by transactions in the network will be directly burned, and the rest will be allocated to the nodes that generate blocks.

4.3 Token Values

CRU is a utility token of the Crust network, its value depends on the Crust network. Its value was correlated with the size of the Crust network, and demand for CRU increased as the Crust network was used by a large number of users. There are two main ways for CRU to capture network value. One is to lock or occupy when it is used, thus reducing the total amount of circulation. For example, deposit for storage and retrieval services, payment for purchase of storage services, voting for governance on the chain, Staking in the consensus mechanism, and so on; The other is that it will be burned when used, thus reducing the total amount of token, such as some transaction fees.

5. Economic Model

The main problem solved by the Crust economic model is to reasonably distribute the interests of various parties under the premise of ensuring the security of the network protocol. The economic model can incentivize various participants to join the network, but also make the system stronger, safer, and more valuable. And can maintain the sustainable development of the system by using CRU as the value bearing and value circulation.

5.1 GPoS Consensus Design

Besides maintaining network security, the design of GPoS also seeks to optimize the workload under PoW as much as possible to match the actual market demand, so that the workload becomes meaningful (Meaningful Proof of Work). When CRU is used as staking to maintain the GPoS consensus of Crust network, nodes need to have storage resource guarantees to obtain a staking limit. There is a conversion rate X between the storage resource and the CRU quota, that is, how many units of CRU quota a unit of storage resource can generate. The design of X is devided into two phases in the system. In phase 1, the node can obtain a quota of 20 cru per TB. Storaging meaningful data can get extral 10% quota. So the node can get 22 cru quota per meaningful data. The formula is:

$$X = 20 \times (1 + 0.1 \times Z \times M)\ cru/TB$$

*M: Effective storage ratio, that is, the ratio of the meaningful storage data of the

*Z: Qualified user index coefficient

Meaningful storage data means the data comes from users by sighing contract in storage market. Among them, a qualified user refers to a user who signs a contract with a node and the contract is within the validity period. Qualified user index coefficient refers to the effective of meaningful data, that means qualified users should be more than 30, the meaningful data quota can take effect.

With Crust network growth, when the Staking Rate of CRU get 50%, it will come into phase 2, in this phase:

$$X = \mathrm{R} \times (1 + Y \times Z \times M) \times \frac{Amount_{cru}}{\mathrm{Storage}}$$

*X: Conversion rate between storage resources and CRU quota

*M: Effective storage ratio, that is, the ratio of the meaningful storage data of the node to the total capacity provided by itself

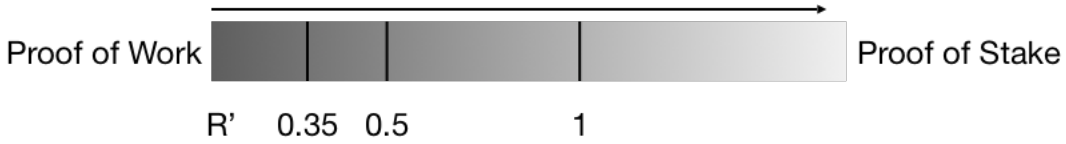
*Amount_cru: The total number of CRU tokens in the whole network

*Storage: Total storage resources of the entire network

*R: Conversion rate

*Y: Coefficient of effective storage ratio

Meaningful storage data means the data comes from users by sighing contract in storage market. In this design, we stipulate R '= R × (1 + Y × Z × M). The R 'coefficient represents the upper limit of CRUs that can be staked in the system. When the coefficient is designed to be low, the economic characteristics of GPoS consensus will be closer to the PoW consensus. At this time, the security of the network is mainly guaranteed by storage resources, and the distribution of benefits will flow to these nodes; When the R 'coefficient is designed to be high, the economic characteristics of the GPoS consensus approach PoS. The security of the network is mainly guaranteed by the staked CRU token in the network, and more of the benefits will be allocated to the account holding CRU. As shown below:



We set R = 0.5, Y = 0.1 and Z = 1 (when the number of qualified users> = 30; if the number of qualified users <30, then Z = 0), so we get

$$X = 0.4 \times (1 + 0.25 \times 1 \times M) \times \frac{Amount_{cru}}{\text{Storage}}$$

Under this setting, when the storage nodes are empty, the total staking quota accounts for 40% of the entire network's circulating CRU; if the hard disk space is full of valid files, the staking quota accounts for 50% of the entire network. For nodes, improving effective data storage is more economical than increasing storage resources, and will incentivize nodes to make storage as meaningful as possible.

After analyzing the staking ratio of existing PoS projects, the generally accepted safety coefficient is about 0.35 ~ 0.66. That is, the locked tokens in the PoS system account for 35% to 66% of the total. In actual projects, the staking ratio range can be 0.15 ~ 0.85. It is determined by the stage of the project and the staking yield. The following table shows the staking situation of cosmos and tezos projects:

Projects	Staking Ratio	Inflation Rate	Consensus
cosmos	73%	7%	BPoS
tezos	78%	5%	LPoS

The conversion ratio setting only specifies how many CRUs the entire network can stake. The number of CRUs participating in staking is related to the yield of participation. From the data of the Cosmos and Tezos projects in the above table, it can be seen that in the early stage of the projects, when the functionality of the token was not exerted, users tended to stake the token in the system to earn dividends. When the yield is 6% ~ 8%, the staking ratio can account for about 75%. In the Crust system, when the price of the token is low, the node runners will not blindly expand the storage resources, which is similar to all PoW projects; when the value of the token is recognized, it will bring a price increase, and the staking ratio

will decrease accordingly. Node expansion of storage resources to increase the CRU staking limit will not directly bring benefits back, this will weaken the node's willingness to expand. If the value of the token is due to the development of the storage market, the node's revenue in the storage market will drive it to increase storage resources. This design allows the supply of resources to change according to market demand, rather than simply relying on the increase in token prices.

After passing through the block reward period, the inflation rate of the token in the Crust network will remain at a relatively stable ratio and will affect the staking ratio of the entire network. The specific design is as follows:

Perpetual Inflation Rate: 2.8%

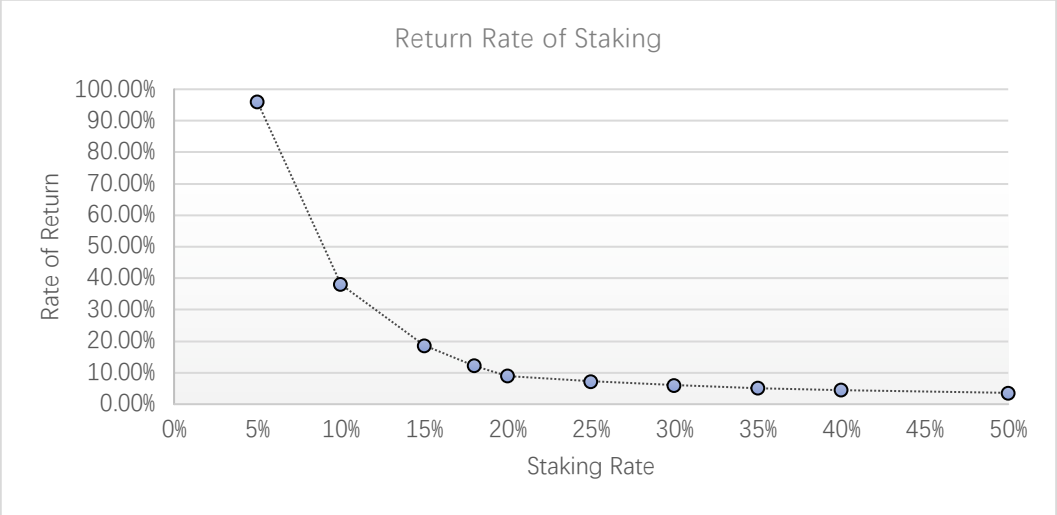
Inflation rate when the staking ratio is below 20%: $2.8\% + \left(1 - \frac{\text{staking_rate}}{0.2}\right) \times 0.04$

For the Staking ratio, our expected short-term target is 50%, about 35% in the medium term, and 20% to 35% in the long term. Because the security of the network will decrease rapidly after being lower than 20%, we designed the compensation for the income when the staking ratio of the entire network is lower than 20%.

The average staking rate r of the whole network is:

$$\mathrm{r} = \frac{0.028 + \left(1 - \frac{\text{staking_rate}}{0.2}\right) \times 0.04}{\text{staking_rate}}$$

The rate of return is as follows:



In the Crust system, the CRU staked at the node can come from the node itself or can be by the guarantor. We further analyze the return on investment of participating in the network as a node runner or guarantor:

We define the ROI (Return On Investment) of the validators as:

$$ROI = \frac{Rv + Re + Rs - Fg - Fs}{C_node + Cm + Vcru}$$

*C_node: The hardware cost invested for the node to participate in the network

*C_m: Hardware maintenance cost for the node

*V_cru: CRU value of node own staking

*R_v: Block generation reward (which includes transaction fees and block points included in the block)

*R_e: Reward distribution of each cycle of blockchain

*R_s: Storage Market Revenue

*F_g: The guarantee fee paid by the node to the guarantor

*F_s: The cost of the node being confiscated

Compared with the validators, the candidates do not have the job of generating blocks, so it does not have to bear the penalty risk of generating blocks and enjoy the R_v income. The asset cost categories invested by the node runners include hardware equipment, power costs, labor costs, site costs, and CRU token assets; revenue includes CRU tokens and the various types of assets that can be independently determined in the trading market, which are mainly divided into fiat currency-denominated assets and CRU token assets. Since storage resources have independent trading markets, their ROI can be separately calculated as:

$$ROI = \frac{Rs}{C_{_node} + Cm}$$

Compared with the existing cloud storage vendors, the ROI of storage resources will ultimately be determined by the market. Considering that the storage market is not perfect early in the system, R_s should be small. Therefore, the Crust system has designed a higher R_e to protect the node's revenue, and R_e will gradually decrease as the system grows. After R_e is reduced to a stable ratio, the node has an independent ROI calculation through the staked CRU token, where the validator is:

$$ROI = \frac{Rv + Re - Fg - Fs}{Vg + Vcru}$$

*V_g: CRU value guaranteed by the guarantor for the node

The candidate's ROI is:

$$ROI = \frac{Re - Fg}{Vg + Vcru}$$

The staking ROI between the validator and the candidate is closely related to the average staking rate r of the entire network. Because the inflation of the system accounts for a large proportion of the node's revenue. When the proportion of handling fees and commission income in the trading market increases, the ROI can be significantly improved.

If do not consider the cost of being confiscated, the guarantor's ROI is:

$$ROI = \frac{Fg}{Vg}$$

As the guarantor 's investment with CRU tokens, the income is also CRU tokens. When the asset variety is the same and the investment return rate is measured in CRU tokens, the rate of return will be determined by the market. The rate of return can refer to that of the entrusted voters in the Cosmos and Tezos projects.

5.2 Gas Fee Composition

In the blockchain network, the typical resources and the corresponding fees are designed as follows:

Limited block size, it charges gas fees by calculating the number of bytes occupied by each transaction;

The limited generation time of the block, the time consumed by different transactions can be obtained by calculation or performance test;

On-chain storage resources usually have two modes of one-time payment and leasing. The one-time payment occurs during processing transaction and it evaluates this fee during development. The leasing model also considers the length of time that a transaction occupies on the chain, and will clear the corresponding state after the timeout.

In the design of the Crust system, the gas fee is composed of the following parts:

Total gas fee = basic fee + (byte fee + weight fee) × (1 + dynamic adjustment rate) + tip

The basic fee is the fee to be paid for each transaction; byte cost = cost per byte × number of bytes. The system will give an initial cost configuration, which can be updated as the system upgrades. The dynamic adjustment rate is a rate adjusted according to the proportion of block resource usage. When the utilization rate of network resources is high, transaction fees will increase; when the utilization rate of network resources is low, transaction fees will be reduced. Tipping is a fee determined by the sender of the transaction. When the network is particularly congested, tips can be added to give priority to packaging transactions.

The basic fee will be directly burned, and other fees will be paid to the nodes that package the block. The basic cost of burning will allow the tokens in the system to enter deflation.

5.3 Penalty Mechanism* (unfinished)

6. Trading Market

The first phase of Crust will complete the storage resource trading market, allowing storage resource providers and storage resource users to trade in this market, and will further introduce the computing resource market in the future.

6.1 Storage Resource Market

In the storage resource market, storage resource providers serve as nodes in the Crust network, including validators and candidates; storage resource users are users with data storage demands, including users of Web2 centralized cloud storage, and users with big data storage need in the Web3 ecosystem decentralized network.

To meet storage service requirements, resource providers need to be online 24/7. We have designed corresponding mechanisms in the network access protocols for validators and candidates and put forward further requirements for nodes being online in the trading market. Unlike the online requirements for nodes in the GPoS consensus (for details, please refer to the introduction of GPoS consensus), storage service response, and blockchain verification work separately, so nodes need to have additional locked CRU to guarantee storage services, We call this locked CRU Guarantee G, and the system stipulates the minimum G is 10 CRU. For users, there is no online requirements.

6.1.1 File Storage Service

In a typical storage transaction, users generally rent a period of storage space and pay for the corresponding rent service. This fee P will be locked in the network when the trading

contract takes effect and will be unlocked in batches and paid to the nodes that provide storage space. To ensure that during this period, the nodes that sell space can guarantee the quality of service, the system will request the nodes that provide storage space to lock a certain amount of CRU token assets as contract guarantee money G. This guarantee money G cannot be released until the service is terminated. Only the Crust native token CRU can be used as the guarantee G, and the fee P can be an asset that the node is willing to accept. It can be a CRU, a stable currency, or other token assets, but it shall be exchangeable with the CRU in the token trading market. During the contract period, the user cannot cancel the contract order. The storage node can apply for termination of the contract, but it needs to deduct the corresponding proportion of the security deposit. Initial setting in Crust network:

$$\boldsymbol{Vg} \geq \sum Vp$$

*Vp: Market value of users payment P

*Vg: Total market value of node guarantee G

That is, when the transaction contract takes effect, according to the token price in the trading market, the guarantee G value of the storage node in the transaction market needs to be greater than the CRU to which the fee P can be exchanged (excluding the handling fee), and the minimum guarantee G is 10 CRU. When the contract is generated, 0.5% of the contract price will be drawn from the guarantee as a contract commission to enter the reward distribution pool of the next cycle of the blockchain. The minimum value of the contract commission is the transcation fee for generating trading contracts on the chain. If the storage node applies for termination of the contract in advance, the remaining fee P will be refunded to the user, and a part of the guarantee will be confiscated by the system. (## About the penalty mechanism of the storage market, the design to be improved)

6.1.2 File Retrieval Service

Similar to the file storage service, users can initiate a retrieval service request for a file on a node and pay **Pr** for this service, which will generate a retrieval contract. The node can receive this fee **Pr** after completing the user retrieval service. Similarly, 0.5% of the contract price will be withdrawn from the Guarantee G as the contract commission to enter the reward distribution pool of the next cycle of the blockchain. The minimum value of the contract commission is the transcation fee for generating the retrieval contract on the chain. Different from the storage contract, a part of the payment fee **Pr** of the retrieval contract will be sent to a specific account **A**. If the user sends the identification of retrieval file to the chain, it can take back the assets sent to the specific account. The purpose of this is to encourage users to verify the retrieved files.

6.1.2 Fishing Task

The Crust network design Fishing Task mechanism to check whether the node provides File Retrieval Service. A random user who selected by VRF(Verifiable Random Function) can take the random task, and it can get a reward form specific account **A** when it complete the retrieval task.

6.2 Computing Resources Market

Crust Network will support the decentralized cloud computing in the future. Unlike the storage market, computing resource services generally do not support long-term staking assets, but users directly pay for computing services in the form of gas fees. The design of this trading market will be updated in subsequent versions.

6.3 Token Trading Market

To better serve all participants in the Crust network, a decentralized token trading market is provided in the Crust network. In this token trading market, multiple types of tokens can be exchanged with CRU. Because Crust is developed based on the Substrate framework of Polkadot ecology and will be connected to the Polkadot network in a parallel chain, it can easily accept the exchange of other types of tokens and CRU in the ecology.

In the above, we mentioned that the participating users in the storage market include Web2 centralized cloud storage users and users in the Web3 ecosystem who have decentralized big data storage demands. Traditional Web2 users as consumers will prefer to use currency with stable value to purchase storage services, such as stable coins; Web3 ecological users can also easily use their project tokens to purchase storage services. The nodes that provide storage resources can also choose the assets they are willing to accept to price the service. When the assets paid by the user are different from the assets accepted by the node, the token trading market can provide real-time token transactions and only need to pay a certain fee.

7. On-Chain Governance

Crust uses Substrate technology to build an on-chain governance mechanism. The main applications related to the economy are the processing of funds in the Treasury account, as well as possible future proposals for system improvements. When the network is running, nodes may be confiscated for some reason. This operation may be misjudged because of the imperfect network. We hope to correct such an error through a channel. The voting function of on-chain governance allows CRU token holders to participate in the construction of the network. The on-chain governance mechanism is still under development.

8. References

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] Ethereum “A Next-Generation Smart Contract and Decentralized Application Platform” 2014

[3] Polkadot: Vision for A Heterogeneous Multi-Chain Framework 2017

[4] Cosmos: A Network of Distributed Ledgers 2016

[5] John Maynard Keynes “The General Theory of Employment, Interest, and Money” 1936

[6] What is Tezos https://tezos.com/get-started

[7] Filecoin: A Decentralized Storage Network 2017