Diffusion Dao

Economic crony type DAO organization

Content :

Foward

In 2022, the world will accelerate into the era of digital economy, and the field of cryptocurrency has penetrated into the multi-dimensional aspects of the society, the powerful organizational and economic capabilities of the crypto ecosystem applications led by the Ethereum ecosystem are rising, DAO and DEFI have also become the most outstanding applications in the entire cryptocurrency field. However, the rather objective evaluation shows that the current DEFI products and DAO still have deficiencies, and the room for improvement is still huge.

Significant changes have taken place in both theoretical and practical research on monetary policy since 1990. On the theoretical side, macroeconomics is moving towards a new synthesis. Traditional Keynesian elements are integrated into the real business cycle (RBC) paradigm, resulting in the development of a new generation of monetary business cycle models that allow the analysis of monetary policy and its relationship can be carried out within a unified dynamic stochastic general equilibrium (DSGE) framework. This new model is generally referred to as the new Keynesian (newkeynesian, NK) model. We will adopt this framework so that the overall ecology can obtain an "optimal currency model" under this framework. We will study the core value support in the current cryptocurrency, and achieve the "optimal" goal through a series of models and algorithm support, At the same time,

through algorithmic deduction, the core idea is that no matter how the central financial agreement changes, it should target "inflation".

We believe that the core solution of DEFI1.0 mainly focuses on the reproduction of financial scenarios, that is, the application of financial products, we believe that there is a big gap between the profitability of the first generation DEFI products and the market value of their tokens, there are many main reasons for the increase in the market value of such tokens, market environment, investment enthusiasm, capital operation, and etc.

Let's take a look at the DAO organization again:

The DAO first emerged as a project called The DAO, which aimed to attract venture capital. Launched in the Ethereum ecosystem in June 2016, it attracted $150 million capital through crowdfunding, unfortunately, it was hacked immediately, and $50 million worth of cryptocurrency was stolen. Over the next few weeks, the effects from the hacked incident were retroactively eliminated by means of an Ethereum "hard fork", and the lost money was recovered as a result. Most ethereum miners and clients then switched to this new fork mechanism to apply this emergency remedy as a prevention solution. However it also caused the largest fork of the Ethereum public chain, and the Ethereum classic model came into existence. As a result of this mistake, a utopian organizational structure fell, but it developed a distributed autonomous organization, an organization embodied in open and transparent computer code, only controlled by shareholders of an organization not

by the central government. Its financial transaction records and procedural rules are stored in the blockchain, and this idea of organization, with code acting as law, to exist in the world.

The performance of token itself is very similar to that of stocks in the traditional market. The definition of a stock is that a stock or capital stock is a marketable security through which a company limited by shares allocates its ownership. As a company limited by shares needs to raise long-term funds, the stock is issued to investors as part of the ownership certificate of the company's capital, and become shareholders to receive dividends (stock dividends or/and cash dividends), sharing the profits from the company's growth and potential capital appreciation from the volatility of the trading market; but also bearing the risks of the company's operating errors. We can find the similarities between the token and stock in the definition: a company in traditional finance is similar to the originating team of a cryptocurrency, the company's fundraising is in the form of IDO and ICO in the field of cryptocurrency, and the part of the ownership certificate obtained by traditional financial investors is very similar to the token itself.

However, we all know that tokens are completely different from stocks, the volume of the cryptocurrency market is growing rapidly, and the rapid expansion of funds in this field is a rare miracle in the history of human finance. Interestingly, it seems that in the cryptocurrency space investors don't care about the intrinsic value of the tokens themselves, that is where traditional financial judgments fail in this

context, when an investor invests in a cryptocurrency he does not even need to know who issued the token, perhaps he is more concerned with the smart contracts themselves, or just a liking to a KOL tweet. Today, when we are faced with an industry that has grown to the trillion dollars level, it is necessary for us to seriously treat and analyze this phenomenon with more research and academic spirit. There are some that are almost equally applicable to other famous tokens, we believe that there are many factors in the composition, the factors are as follows :

1. With excellent benefits like Bitcoin for example

2. Nearly perfect anonymity to satisfy the individual's psychological needs for privacy

3. The convenience of the issuers

4. Low threshold for investment and editing

5. Huge space for innovation

6. The background of globalization

7. ...

The above factors all constitute the rapid expansion of the field, we will abstract the important factors into one of the factors that can determine the development of a decentralized financial system, while we will use more mature macroeconomic models to fix the problems that have been found, and then create an economic crony DAO organizational structure supported by a central financial protocol. We know that web 3.0 is coming, and it will change the world, across both civilizations and regions. We hope to empower the existing cryptocurrency

field with a rigorous mathematical model and make the ecological value more rational, not only using reliable mathematical financial tools, but by objectively increasing the elements of the information economy, web3.0 can have a more reliable economic system to support the soul of the digital space when it arrives.

Diffusion abstract elements

Here we abstract only the quantifiable factors, which we will make use of in the following.

1. Attention factor: The market value of almost all tokens is directly related to their topicality and attention, and tokens that continue to maintain a high market value will not get rid of the "attention" factor, we will collect "attention" data from mainstream platforms.

2. The transfer coefficient of the transfer factor, that is, the market value of any token is directly related to its invocation, whether it is the native token of the public chain or the ERC20 token created in the public chain, the frequency of its transfer invocation will be a measure of a token or ecosystem an important indicator of the value.

3. Diffusion coefficient is a very important indicator of Diffusion. It directly shows the increase in the number of valid 0x addresses of DiffusionDAO, which will be an important economic indicator of DiffusionDAO.

Definition

First we need to clarify the important definitions:

  1. Central financial protocol series:

A series of smart contracts deployed in the public chain system that determine the development of the economic system, the functions of which are defined as follows:

A，Minting

B，All tokens circulating in the ecosystem need corresponding contracts to be minted

C，DFS

DFS is the core of the financial system TOKEN of DFS, that is, the abbreviation of diffusion, which is based on the core protocol diffusion ERC20 to achieve minting, which is not a stable currency, from the "optimal monetary policy" model, the market price of DFS will infinitely approach the floor price. The goal of the protocol in the short term is to mint as many DFS as possible, thereby causing "inflation" of the system.

D，PFUS

PDFS is the private token of Diffusion ecosystem, buying Bonds in Difussion to unlock, the exchange rules are as follows:

$$BUY\,1\,DFSBonds：PDFS = DFS$$

E，Current deposit

Current deposit means that holders of DFS can store their own DFS in the

central financial protocol and obtain DDFS. The emergence of DDFS is to

reduce the complexity of manual pledge. DDFS cannot be traded, but can

be replaced by DFS at any time.

$$DFS = DDFS$$

F， Fixed Deposit

Fixed deposit means that holders of DFS can store their own DFS in a

central financial protocol and receive FDFS. The emergence of FDFS is to

reduce the complexity of manual staking, FDFS can be withdrawn at any

time, however, the amount of DFS that can be obtained will be less than

the expected amount, and the interest rate is the current deposit rate on

the day.

Maturity：

DFS=FDFS

G， FS

It is an algorithmic stable coin issued based on DRF held by the central

financial protocol, which is 1:1 with USD in terms of price.

H， Loan

Central Financial Protocol will provide a range of lending products led by

DFS.

I， Rebase

Refers to the interest rate per cycle in the central financial agreement, which

is controlled by the DSGE model, divided into two categories, one is the

current interest rate and the other is the fixed-term interest rate, fixed term interest rates vary by time and amount.

J, Reserve bonds

The central financial agreement will sell its own bonds to increase treasury assets. Reserve bonds refer to a series of bonds issued by the central financial agreement that are sold at stablecoin prices, buyers can obtain bonds at a lower price than the secondary market by purchasing bonds.

K, Liquid Bonds

Liquid bonds refer to the LP obtained by users after the decentralized exchange provides liquidity, which can be used to purchase DFS, same principle as the purchase of reserve bonds.

L, Central Bank

The central bank refers to the central agreement of the entire agreement, which is used to reserve core assets and is an important support for the Diffusion ecosystem.

M, RFV

RFV is a risk-free asset, it refers to an asset with no uncertainty in its future rate of return. Its standard deviation is 0, the actual rate of return will always equal the expected rate of return. The treasury will have a larger weight to reserve RFV.

N, BCV bond control variable

An adjustment mechanism for bond prices that controls the bond's discount

rate, expectations are determined by the DSGE model.

O， PCV

The amount of funds controlled by the protocol refers to the sum of all assets controlled by the central financial protocol. The more funds, the better for the ecosystem.

P， POL

The liquidity of the protocol refers to the number of LPs owned by the protocol. The more LPs, the better for the ecosystem.

Q， TVL

Total Value Locked, the total locked value refers to the total value of the digital assets mortgaged by users in the project. People often use the growth of TVL to refer to the upward movement of token projects.

R， TWAP

The time-weighted parity price, the time-weighted average price, are both the average price.

2， Definition of Ecological Indicators

A， Media Traffic

B， KOL interaction index

C， The number of addresses owned, defined as the DAO population

D， Spending Power

Observation of payment conditions in the DAO community

E， DAO Activity

Refers to the number of times the protocol in the DAO organization related to Diffusion is used.

F，External system cooperation

Depth of ecological cooperation with other cryptocurrency systems and expected returns.

G，Technical Shock

Refers to the emergence of a new agreement to compete with the ecosystem itself.

3，Organizational Structure

A，citizen

That is a valid 0x address to interact with Diffusion.

B，Dao

DiffusionDAO is a decentralized self-organization jointly managed and governed by many citizens.

C，Governance

Every important decision of Diffusion will be participated and decided by citizen. DiffusionDAO will continue to initiate the Governance issues to be decided by citizen voting.

D，GFUS

It is encapsulated by DFS as GDFS for decision-making and voting.

E，Ecological contribution value

Refers to how many times a central financial agreement is mobilized by the

address associated with the address, such as increasing the PCV of the central bank contract.

F，Ecological Fund

Diffusion will periodically take out funds from the DAO organization fund to incentivize the development of the protocol.

G，Shake Hands

A cooperative relationship can be formed between addresses, and addresses with a handshake agreement can promote each other to establish a form of mutual help. For example, when buying bonds, addresses with a handshake agreement will get more DFS.

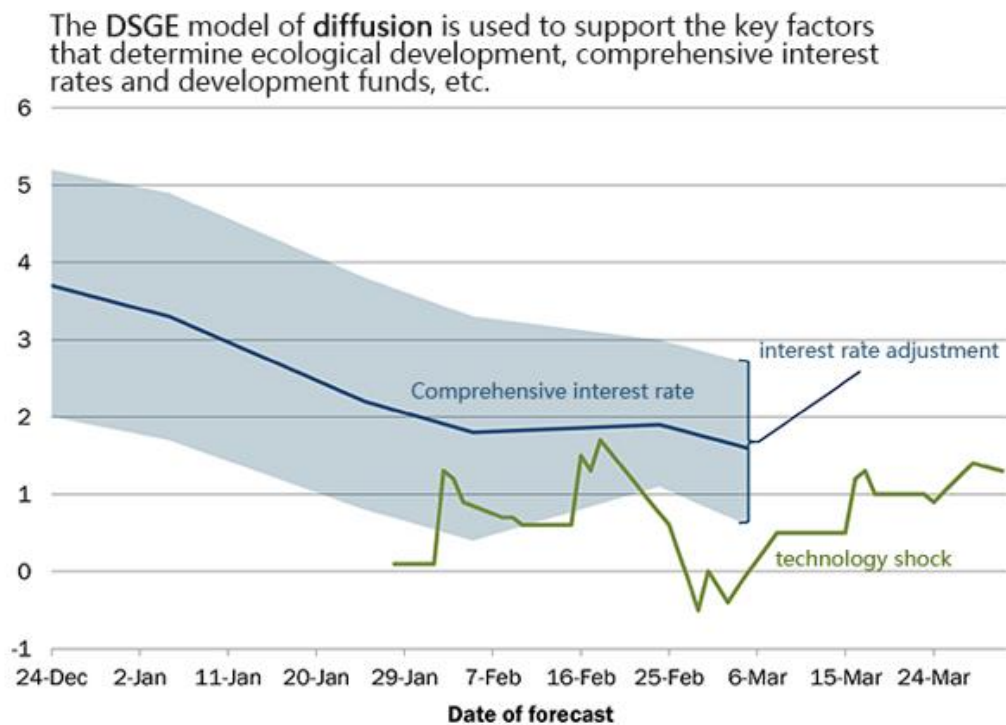## 4. DAO Organization Protocol Series

1，   MakeDiffusion Capital-protected Crowdfunding:

Diffusion will support capital-protected crowdfunding, due to the general lack of intrinsic value support and defined "attention" elements in existing DAO crowdfunding, although many DAO organizations are innovations worthy of encouragement and learning, but for investors of DAO projects that use valuable assets such as ETH for crowdfunding, this is dangerous, because investors are likely to lose their valuable assets in exchange for a bunch of empty air tokens. This often puts investors in a dilemma, that is, they do not want to miss out on a very good investment opportunity, but they can also lose money because of it. The specific execution process is as follows:

Diffusion DAO

Diffusion's first official DAO organization tool is called MakeDiffusion, a set of protocols that enable capital-protected crowdfunding. The functions are defined as follows:

A，MakeDiffusion is a set of DAO crowdfunding protocols that can be freely initiated by anyone, with a user-friendly graphical interface, ones can design their own DAO with interactive features including:

B，Project name, project introduction, project number, official website link, twitter link, disorder link, project funding planning

C，Funding cycle target, including funding target (usd series, ETH, FS) and the time of the planned crowdfunding.

D，Token Keeping

E，Incentives

Tokens awarded for each payment amount will be reduced by this percentage with each new funding cycle, and a higher discount rate will incentivize supporters to pay their project fees in advance

The DSGE model of **diffusion** is used to support the key factors that determine ecological development, comprehensive interest rates and development funds, etc.

F, Restricted Movement

Limit on payments and tokens minting

G, Description of Funding Objectives

1, You can set the type and proportion of the expected income assets of your DAO project. It should be noted that if the pre-received funds are in the USD series or ETH, 1% of the funds will go to the central bank of Diffusion and become the protocol profit. If the prepaid funds are DFS, you cannot receive DFS directly, but the packaged MDFS can be replaced with DFS after a fixed time, the ratio is the time when FS was received as follows:

$$MFS=FS*frebase^n$$

N is the fixed deposit rate of the Diffusion agreement on the day of collection, after

the fixed deposit date expires, crowdfunders will be able to use MFS to exchange FS for project running funds, at the same time, investors will get the project's tokens and the same amount of FS as the investment.

2, Cooperative game protocol

DFS holders can enter the CGDiffusion community to interact with various games and exchange of opinions. When entering CGDiffusion, the user's FS will be replaced with CGDFS for participating in the game, CGDFS can replace FS, however, CGDFS has different levels of ability indicators, the energy indicator of CGDFS is 0 at the time of creation, that is, the ratio of the amount of exchange for DFS is 1:0. The energy indicator is upgraded every 8 hours, and the energy upgrade time is consistent with the rebase cycle of Difussion's central financial protocol. Every time you upgrade CGFS, you can exchange for more FS. The highest level of energy value can be selected by the user, the higher the level, the stronger the exchange ability of CGDFS. The conversion formula is as follows:

Case A: The energy value of CGFS is 100

FS=CGFS* Energy value* fixed deposit rate

Case B: The energy value of CGFS is less than 1 and greater than 0

FS=CGFS* Energy value* demand deposit rate

If the game has a quiz game loop, the loser will lose CGFS, when the CGFS is exchanged, the guessing party will get an equal amount of FS to buy CGFS, and the winner will get CGFS.

Formula

1. One of the most important components of any organization is its members. However, there are no native members in DIffusion. All members participate based on the public chain system. Their identification cannot be based on the "address" headed by 0x, we need to use 0x's contractual interaction with Diffusion as a criterion to judge a member of "DIffusion", which is very similar to the behavior of "applying for a green card" in the physical world.

Attention: the degree of attention in the digital space is defined as: N_t

Invocation degree: the number of times the related smart contract is called: Q_t

Diffusion: a phased policy indicator that encourages cooperation between 0x addresses in the ecology: D_t

1. For 0x members (it needs to be explained here that all the following 0x are people who already "hold green cards") the typical 0x preference involves four factors, the composite consumer commodity C_t, the actual interest-earning currency balance M_t/P_t, the bond which can be purchased B_t, the labor supply N_t, and the leisure $1 - N_t$.

Assuming that the life of 0X is infinite, then 0X seeks to maximize the intertemporal utility as follows:

$$E_0\left\{\sum_t^{\infty} \beta^t u\ (C_t,\ M_t/P_t,\ N_t)\right\}$$ (2.1)

In the formula, β is the subjective discount factor, E_t is the expected operator, and $u\ ()$ represents the single-period utility function. It is additive with respect to

its three independent variables, and CES is taken for each independent variable:

$$u\ (C_t, M_t/P_t, N_t)\ = \frac{C_t^{1-\sigma}}{1-\sigma} + \frac{(M_t/P_t)^{1-\emptyset}}{1-\emptyset} - \frac{N_t^{1+\eta}}{1+\eta} \qquad (2.2)$$

In the formula, σ and $\emptyset$ are the reciprocal of the intertemporal substitution elasticity of consumption and money, respectively, η is the inverse of the elasticity of labor supply, and the composite consumer commodity C_t is the differential digital asset generated by the DAO organization protocol, these DAOs are distributed in a size equal to 1 on a continuum, C_t is defined as:

$$C_t = \ (\int_0^1 c_t(i)^{\frac{\varepsilon-1}{\varepsilon}}\ di)^{\frac{\varepsilon}{\varepsilon-1}} \qquad (2.3)$$

In the formula, $c_t\ (i)$ is the commodity i, i$\in$[0.1] produced by DAO, and ε is the inverse of the elasticity of substitution between different commodities i. The 0x decision making issue can be handled in two stages. First, the optimal behavior of 0x to buy a composite commodity is to minimize the cost when purchasing individual commodities that can reach the level of this composite commodity, secondly, 0x makes the optimal choice for C_t, M_t, N_t according to the given cost of purchasing any level of C_t. We first discuss the problem of minimizing the purchase cost of C_t, the decision making for 0X is to minimize the purchase cost of C_t, through the selection of individual commodities $C_t\ (i)$:

$$\int_0^1 P_t\ (i)c_t(i)di$$

The restrictions are:

$$(\int_0^1 c_t(i)^{\frac{\varepsilon-1}{\varepsilon}}\ di)^{\frac{\varepsilon}{\varepsilon-1}} \geq C_t$$

where $P_t\ (i)$ is the price of commodity i. Let Ψ_t denote the Lagrangian

multiplier on this constraint, then the first-order condition on commodity i is:

$$p_t(i) - \Psi_t \left(\int_0^1 c_t(i)^{\frac{\varepsilon-1}{\varepsilon}} di \right)^{\frac{\varepsilon}{\varepsilon-1}} c_t(i)^{\frac{-1}{\varepsilon}} = 0$$

Arranging the above formula to get:

$$c_t(i) = \left[\frac{p_t(i)}{\Psi_t} \right]^{-\varepsilon} C_t$$

According to formula (2.3), we can get:

$$C_t = \left(\int_0^1 \left[\left(\frac{p_t(i)}{\Psi_t} \right)^{-\varepsilon} C_t \right]^{\frac{\varepsilon-1}{\varepsilon}} di \right)^{\frac{\varepsilon}{\varepsilon-1}} = C_t \left(\frac{1}{\Psi_t} \right)^{-\varepsilon} \left(\int_0^1 p_t(i)^{1-\varepsilon} di \right)^{\frac{\varepsilon}{\varepsilon-1}}$$

With Ψ_t as:

$$\Psi_t = \left(\int_0^1 p_t(i)^{1-\varepsilon} di \right)^{\frac{\varepsilon}{\varepsilon-1}} \equiv P_t$$

In the formula, P_t represents the total consumer price index, and it can be

seen that the Lagrangian multiplier Ψ_t for minimizing the purchase cost of C_t is the

total consumer price index. Therefore, the optimal demand for commodity i can

be expressed as:

$$c_t(i) = \left[\frac{p_t(i)}{P_t} \right]^{-\varepsilon} C_t$$

There are two types of financial assets in the existing economic system:

interest-bearing currencies and central financial agreement bonds with a single-

period nominal interest rate i_t. 0x owns a DFS of M_{t-1} and a nominal bond of

$(1 + i_{t-1})B_{t-1}$ at the beginning of period t, and gets $W_t N_t$(W_t is the diffusion value)

at period t income from work and the nominal interest rate D_t; at the end of

period t, 0x keeps M_t's DFS and buys B_t's bonds, and spends the rest on C_t.

According to the definition of (1.4) total price index, the 0x intertemporal budget constraint expressed in real value can be expressed as

$$\frac{W_t N_t}{P_t} + \frac{M_{t-1}}{P_t} + \frac{(1+i_{t-1})B_{t-1}}{P_t} + D_t = C_t + \frac{M_t}{P_t} + \frac{B_t}{P_t} + T_t \,. \tag{2.6}$$

The second stage of the 0x optimization strategy problem is to maximize (2.1) by choosing C_t, N_t, M_t, B_t in combination with the above solvency constraints, and the following four optimization conditions can be obtained:

$$\frac{W_t}{P_t} = C_t^{\sigma} N_t^{\eta} \,. \tag{2.7}$$

$$\frac{M_t}{P_t} = C_t^{\frac{\sigma}{\phi}} \left(\frac{1+i_t}{i_t}\right)^{\frac{1}{\phi}}. \tag{2.8}$$

$$C_t^{-\sigma} = \frac{\beta(1+i_t)}{1+E_t\{\pi_{t+1}\}} E_t\{C_{t+1}^{-\sigma}\} \,. \tag{2.9}$$

Equation (2.7) gives the optimal condition of the consumption-leisure trade-off of 0x; qquation (2.8) gives the equilibrium condition of the portfolio of 0x, which also represents the money demand function of 0x; (2.9) is the time-span optimization condition of 0x Euler equation, ie. π_{t+1} is the inflation rate between period t and period t+1. So Diffusion's IS-LM model (Investment-Saving / Liquidity preference-Money supply model, investment-saving/liquidity preference-money supply model) is as follows:

$$x_t = -\varphi \ (i_t - E_t\pi_t) + E_t x_t + g_t \tag{2.10}$$

Equation (2.10) is called the DIsffusionIS curve. In the formula, $\varphi = \frac{1}{\sigma}$, g_t follows an AR(1) process:

$$g_t = v g_{t-1} + \hat{g}_t, \ 0 \le v \le 1 \text{ where } \hat{g}_t \text{ is white noise.}$$

2. Phillips curve

DAO is a decentralized self-organization, which can be completely matched with

our ecosystem, or it may be an external ecological access to the core financial protocol, however, the 0x of the external ecology is not the same as the 0x that holds the "green card", so the formula here refers to the existence of the "green card" that interacts with the DAO.

To maximize attention and diffusion, DAO is subject to three constraints. The first constraint reflects the demand function that the existing 0x exists.

$$c_t(i) = \left[\frac{p_t\ (i)}{p_i}\right]^{-\varepsilon} C_t \quad (2.5)$$

The second constraint is the marginal utility function of the DAO,

2.2.11DAO

The attention is set to A_t, and the call degree is T_t

$$E_0\left\{\sum_t^{\infty} u\ (A_t,\ T_t)\right\}$$

In the formula, u is the Lagrangian coefficient of A_t and T_t.

3. Optimal monetary policy for the answer

Objective Function

The central financial agreement objective function transforms the behavior of the target variable into a measure of the individual welfare level, which leads to the choice of policy, our dynamic model seeks to maximize the utility of OX, while making each 0x diffusion value tend to be larger, with the highest attention and the largest diffusion value in the short term. In turn, it is positively promoting the expansion of Diffusion.

Inflation Rate: Present Value Floor Price: V_n Present Value Market Price: : V_{n+1}

Current floor price: $V_t$et current market price: V_{t+1}

Current value floor price: current value of total treasury asset value T_s / current market circulation L_n

Current to immediate circulation growth: L_{n+1}

Spot minimum floor price: $V'_{t+1} = T_s/(L_n + L_{n+1})$

Inflation rate: $K = ((V_n - V_{n+1})/(V_t - V_{t+1})) / (V_t - V_{t+1})$

HighestiInflation rate: $K = ((V_n - V_{n+1})/(V_t - V'_{t+1})) / (V_t - V'_{t+1})$

$$\max -\frac{1}{2}E_t\{\sum_{k=0}^{\infty}\beta^k[\alpha x_{t+k}^2 + \pi_{t+k}^2 + D_t + C_t]\} = U(t) \quad (3.1)$$

4. fs minting

$fs_{supplyGrowth} = fs_{bonders} + fs_{deposit} + fs_{protocol\ contribution\ value} + fs_{dsge} + fs_{dao}$

5. bonder

$bonder_{price} = 1 + premiusm$

$premiusm = dsge(RFV)$

$dsge\ (RFV) = \max -\frac{1}{2}E_t\{\sum_{k=0}^{\infty}\beta^k[\alpha x_{t+k}^2 + \pi_{t+k}^2 + D_t + C_t]\}$

$bondPayout_{reserveBond} = marketValue_{asset}/bondprice$

$bondpayout_{lpBond} = marketValue_{lpToken}/bondprice$

6. YPY

$APY = (rebase)^{1095}$

Rebase = deposit amount* Index

Index = $U(t)$

7. Backing per FS

$FS_{minimunmarket\ value} = (treasuryBalance_{RFV} + treasuryBalance_{SDR})*(1+20\%*three\text{-}factor\ index)$

$RVF = RVF_{reserveBond} + RFV_{lpBond}$

SDR = value asset + Ecological cooperation assets

RVF$_{reserveBond}$=assetSupplied

RVF=FSLPBond = 2qrt(constantProduct)*(%ownership of the pool)

D$_{x=}$attention factor=Number of interactions on social platforms*N

N=Collection quantity

N$_x$=The number of social platform interactions of N similar products on the

collected list

attention factor=$(N * D_x)/N_x$=A$_x$

transfer coefficient=The number of contract calls of the central financial protocol

Con$_{x=}$Number of contracts on central financial agreements

Citizen=buy bonds and have term deposits

Citizen$_x$= number of citizens

CCO$_x$=*The number of product contract calls obtained*

transfer coefficient=$(\frac{\text{Citizen}_x}{\text{Con}_x})/CCO_x$=TC$_x$<=1

8. In the three-factor calculation formula Max TC$_x$=1=TC′

Diffusion coefficient(DFSC)=Record the sum of the handshake increments in the

172800Ethereum block height

IN$_x$=The number of citizens in the initial block

EN$_x$=Number of citizens of the end block

$$\text{DFSC}(\text{IN}_x, \text{EN}_x) = (\frac{\text{IN}_x}{\text{EN}_x})^{\frac{1}{4}} - 1$$

In the three-factor indicator formula Max DFSC =1 = DFSC′

three-factor index=(DFSC′ *60 + TC′ *20 + A$_x$ *20)%