Computer mathematical statistics optimization of conversion between blockchain integral and Token

Xin Wang¹, Zhitao Li²*, Xiaoling Li³

¹WeBank Institute of FinTech, Shenzhen University, Shenzhen, Guangdong 518060
²College of Mathematics and Statistics, Shenzhen University, Shenzhen, Guangdong 518060

*Corresponding author: 2018132124@email.szu.edu.cn

Abstract. Block chain in recent years is a new technology for the development of faster, it is mainly based on the principle behind the underlying distributed network structure, and based on the distributed, not tampered with, the nature of the traceability chain blocks in recent years has gradually become the financial and monetary financial attributes such as very strong support, therefore block chain in the extremely rich in recent years. Object of this paper is aimed at token chain integration or the block chain between trade and exchange rate problems, these problems can be described as two token between how to automatically by means of the chain of integral exchange and trading, and solve the middle block chain will appear black swans, slippage is too large, the problem of liquidity dried up.

Keywords: Market maker, Exchange Rate, Token.

1. Introduction
In recent years, the world's attitudes towards Bitcoin have fluctuated, but blockchain technology, one of the underlying technologies of Bitcoin, has received increasing attention. In the process of Bitcoin formation, blocks are storage units one by one, recording all the communication information of each block node within a certain period of time. Each block is linked by a random hash (also known as a hash algorithm). The next block contains the hash value of the previous block. With the expansion of information exchange, a block and a block are successively connected. The result is called blockchain. Blockchain refers to a distributed, shareable, public ledger that can be trusted through a consensus mechanism and can be checked by every participant, but no centralized single user can control it, and it can only be revised according to strict rules and open protocols. It has the following properties:

1.1. Decentralization
In the current system design or application development, the central server is considered to realize all the information exchange and data storage. But in block chain, by building the structure of the distributed system and the open source licenses, let all of the participants involved in the data record and verify, then spread through distributed to various nodes, even if some nodes to attack or damage, will not affect the integrity of the entire database and information updates, the equivalent of each participating nodes are "the center".
1.2. Trust
In the traditional Internet mode, information matching verification and trust accumulation are carried out through trusted central nodes (such as housing registration system) or third-party channels (such as Alipay), so it cannot realize the decentralization of value transmission. Those that can be decentralized must not need credit endorsement.

1.3. Timestamp
Block refers to all the information (including data and code) generated in a certain period of time is packaged and generated. The page capital of each block contains the index information of the previous block, which is linked end to end to form a chain. Therefore, the addition of block (complete history) and chain (complete verification) forms a timestamp (complete history can be traced), which stores all the historical data in the system, provides retrieval and search functions for each data, and can trace the origin with block chain structure and verify each stroke [1].

1.4. Asymmetric encryption
Blockchain uses asymmetric encryption algorithm through mathematical consensus mechanism, that is, a "key pair" is used in the process of encryption and decryption. The two keys in the "key pair" have asymmetric characteristics: one is that only the other key can be unlocked after encrypting with one of the keys; Second, after one of the keys is published, others cannot calculate the other key according to the public key.

1.5. Intelligent contract
Since the block chain can realize point-to-point value transfer, the introduction of programmability will enable the embedding of corresponding programming scripts during the transfer between the two parties, so as to deal with some unpredictable transaction patterns in this way of intelligent contract, ensuring that the technology can continue to be effective in the continuous use.

Now almost all the blocks and especially on the etheric fang blockchain, how to carry out the integral exchange is offline can be combined with online one way, while the existing block chain in the middle of the most divided into market makers curve, constant and, constant product and so on, and these ways among different scenarios, there are many in appropriate characteristics, therefore, how to build a satisfy an era of existing stable currency, and to make the whole block chain integration is not been beset by liquidity, is a hot spot of society, A bad curve will lead to problems in two directions: 1) liquidity cannot be satisfied because liquidity is easily exhausted in a short period of time; 2) the sliding point is too high and there are too many arbitrage opportunities, which makes the whole decentralized exchange fluctuate too much when short-term liquidity funds are low and price instability is easy to occur [2].

Object of this paper is aimed at token chain integration or the block chain between trade and exchange rate problems, these problems can be described as two token between how to automatically by means of the chain of integral exchange and trading, and solve the middle block chain will appear black swans, slippage is too large, the problem of liquidity dried up is proposed based on running, LMSR typical market makers outside of the curve of the new solution, better let blockchain points for smoot, become the online prediction machine. These curves and mechanisms are collectively referred to as CFMM mechanisms. In order to solve the problem of corresponding slippage, we further discussion, how to optimize the curve, thus making the liquidity and slippage problem have been solved, finally puts forward a new framework curve, so as to make the chain block in the future to the curve of the center market problem is solved, make corresponding users from entering the market risk, that makes the market constantly improve.

Impact Statement Among traditional market makers model, in order to achieve the purpose of liquidity, use of is to reduce slippage of large range to maintain the liquidity of the protection, maintain the ecological market makers, but for most of them are stable currency trading today, we will further consider the effect of slippage, so in this paper, the curve of the building within a wide range of the
slippage of low impact, maintain the need of the current situation and the use of hyperbolic tail state further maintain the liquidity demand, make lower slippage, higher liquidity.

The main influencing factors are determined by the slope of the curve and the speed and range of slope change. Therefore, the further optimization of the curve of mathematical function is mainly aimed at the quick response and range of slope change, in which the speed affects its sliding point and the range affects its liquidity.

2. Review of historical models
This part mainly introduces the market-making models owned by blockchain decentralized exchanges in the past, as well as their advantages and disadvantages.

2.1. Constant sum market-making function
The formula for the constant sum market-maker function is:

\[ x + y = D \]

Define \( x, y \) is the price of token.

As the name implies, a market maker with a constant sum is represented by the sum between two integrals as a fixed constant, which is a barter idea and the first famous market maker function.

Its picture is shown in Figure 1.

![Figure 1](image)

**Figure 1** Constant sum market-making function

The figure above shows that we started out with five integrals A and five integrals B, and in the middle of this line of constant absolute value 1, the exchange rate between integrals A and B is always 1:1, namely 1A = 1B. This looks perfect, but there are two very fatal problems:

1) Liquidity is exhausted. Under the premise of no intervention, the number of one party can easily be reduced to zero, making the whole liquidity pool ineffective.

2) Unable to adapt to the changing exchange rate, if the points A, B and external market targeting, the points A and B will not be fully 1:1 targeting, and such fluctuations will lead to the arbitrage crisis in the middle of the flow pool.

To solve the defect of compensating for constant and function, we consider the way of constant product.
2.2. Constant product market maker function

The formula for the constant product market-maker function is:

\[ xy = \left( \frac{D}{Z} \right)^2 \]

In fact, the product function is the hyperbolic function seen in daily life. Such a function will never change to 0 at the tail of x and y axis, so it has a good liquidity protection ability. Its picture is shown in figure 2.

![Figure 2 Constant product market maker function](image)

Here describe to overlay curves, we can find that hyperbolic the most intuitive reflect the relationship between the supply and demand and price, when a certain integral infinite close to x or y, one party tokens of flow has less and less, and its price becomes infinity, number is the exchange rate between the two token, which is between the hyperbolic slope, we can find that through constant product solves the constant and, in the form of two fatal problems, but lack of the introduction of an additional problem, cannot adapt to the current relatively stable points for the scene.

Stable integral /token is stable in most cases, and is close to 1:1. Hyperbolic function will introduce a very large slide point, and even in a small trading volume, there will be a large fluctuation of the price exchange rate, so it cannot meet the exchange scenario requirements of a large amount of stable integral/token.

In order to further the usability of the combination between the two scenarios, whether we can combine two functions their advantages to join a new function among - stable exchange rate, output, very low point, can automatically adjust the transaction exchange rate and a steady stream of liquidity to protect, in fact, from the image we are looking for is a constant and function and constant product function between a kind of function curve, namely to be able to in the middle section close to constant and straight line, and can be in the end like hyperbolic constantly close to the axis, so we put forward the function, through expression of the two together.

3. Newly constructed curve

The formula for the constant sum market-maker is:
\[ xy + (x + y) = D + \left(\frac{D}{2}\right)^2 \]

Its picture is shown in Figure 3.

**Figure 3** Newly constructed curve

In this curve, we found that the constant and the emergence of the liquidity dried up in the intermediate part is solved the problem, but because of the weight is not accurate, resulting in a little bit far place can appear liquidity problems or dried up, so that the division of fixed by fifty percent in a way that the weight has some shortcomings.

We find that it is not particularly close to the line, so we give the function of constant sum by means of weights.

Tail not inherit and continue the hyperbolic curve edge, no way to provide unlimited liquidity, so we use a similar limit inference of thinking, namely in the initialization point (D/2) as the center, in the middle range curve is extremely close to a straight line, so the coordinates of the product to less than the constant volume of hyperbolic, but the farther (D/2) point near the middle, the closer to the center of hyperbolic product, and in the unlimited extension of x and y, x y far less \((D/2)^2\) tend to be zero.

To further by liquidity reflects changes in the curve, we use an D variable expand, with the distance between x and y, we can get, to make further close to the straight line, curve considering as liquidity provided by inflation rate, prevent due to the increasing liquidity of synthetic curve is not close to the linear constant lost.

Get the formula:

\[ 4A(x + y) + D = 4AD + \frac{D^3}{4xy} \]

4. **Model Influence**

What problems do these solve:

1) Impermanent loss optimization: the corresponding loss optimization is obtained through calculation, which is obviously lower than the previous one:

Nondestructive interests is to provide process, due to the liquidity into the pool when no fee income, in the face of the volatility of the market and exchange rate changes will be arbitrageurs taking certain assets, their proportion in the pool of assets less, but when the exchange rate to return to, loss and vanished, and generally volatile loss to below level based on the exchange rate [3].
2) If the assets are not invested in a rational proportion, the curve is more suitable for improper data input, so that the price stability can be protected and the overall ecological stability and harmony can be maintained [4].

3) Slippage protection, through the diagram can be found, in a stable currency interval point is very small, by way of illustration, we can find that, In the middle of the large amount of the stability of the exchange process, the exchange rate is close to 1, so in most of the slippage between the scope of the size is very small, but only in very rare situation below, in order to maintain liquidity to meet, we will be in a certain currency among the declining process makes curve close to hyperbola, liquidity and the corresponding protection.

4) Liquidity protection. By making infinite cases, we find that the retention of liquidity can be compared with the case of constant sum. We find that the newly constructed curve can never be exhausted, so there is always liquidity, so the newly constructed curve will solve these problems.

5. **Experiment**
The experiment is mainly verified by curve comparison.

Look at the Figure 4.

![Figure 4 The experiment of newly constructed curve](image)

We can see from the table, the vertical line of the method to determine by doing it, we can know that the stable currency in large scope under the condition of big deals, in the end we provide curve can better more close to the constant and the function of trajectory, It shows that the stability of the us within a wide range of currency trading among similar problems has better performance.
Correspondingly, as shown in figure 5, using horizontal dividers to process and analyze the curve at the end of the X-axis, the newly optimized curve is more favorable in terms of liquidity provision compared to the curve of constant sum and base weight, which is practical for the current small currency.

6. Conclusion
By optimizing the change rate of slope, which increases with the increase of a certain asset, and the stagnation of the front part of slope, the corresponding liquidity problem and the sliding point of currency price are optimized. Model to solve the existing block chain trade among the two important problems, the mobility and stability, through curve fitting, and the weight of inflation rate to join, make into a large range price stability, extreme liquidity eternal block chain automatic market makers, provides a new solution for decentralized trading.

References
[1] Chen Miaomiao. Research on the influence of blockchain on auditing techniques and methods in the era of big data [J]. China Collective Economy, 2021 (09): 162-163.
[2] Tsai Jason Sheng Hong, Hsu Wen Teng, Wei Chao Lung et al. Universal prediction-based adaptive fault estimator applied to secure communication [J]. Applied Mathematical Modelling, 2014, 38(19)
[3] Ning Huansheng, Farha Fadi, Ullah Ata et al. Physical unclonable function: architectures, applications and challenges for dependable security [J]. IET Circuits, Devices & Systems, 2020, 14(4)
[4] Yan Chang, ShiBin Zhang, Jian Li et al. Robust EPR-pairs-based quantum secure communication with authentication resisting collective noise [J]. Science China Physics, Mechanics & Astronomy, 2014, 57(10)