KEY PERSPECTIVES TO UNDERSTAND DEFI

Chuanwei David Zou,
Chief Economist of Wanxiang Blockchain

How will the DeFi ecosystem evolve? What logic will the evolution follow? In addition to the skill of writing smart contracts, what other tools should DeFi developers master? This article answers these questions from eight key perspectives:

1. Financial functions;
2. Discrete-time finance;
3. Trustless environment;
4. Oracles and information;
5. Liquidity;
6. Arbitrage;
7. Incentives;
8. Risks and interconnections.

1. Financial Functions

Some researchers refer to mainstream financial institutions to understand DeFi, for example, what should be the form of banks, securities firms, and insurance companies in the DeFi field. This analogy is actually not precise enough, because DeFi is built according to financial function modules. This involves the relationship between financial institutions and financial functions.

Financial development has two main lines that are entwined and rising like double-stranded DNA. One is financial function and the other is financial institution. Zvi Bodie and Robert Merton put forward six basic financial functions. They believe that financial functions are more stable than financial institutions, and the form of financial institutions depends on the financial functions they perform. Their insights also apply to DeFi (Table 1).

DeFi projects have very good assemblability. Multiple DeFi projects can be assembled together to achieve complex and diverse financial functions, which can be close to mainstream banks, securities firms, and insurance companies.

Financial function	**DeFi field**
Payment and settlement	Stablecoins
Resource integration and equity segmentation	Staking and liquidity tokens
Resource transfer across time and space	DEX (including automatic market makeror AMM) and DeFi lending
Risk management	DeFi insurance and derivatives
Information provider	Oracles
Incentive solution	Token governance

Table 1: DeFi and financial function modules

2. Discrete-time Finance

Mainstream finance is continuous-time finance, and the unit of time is generally hours, days, weeks, months, quarters, and years. DeFi is discrete-time finance, and the unit of time is the update frequency of the public blockchain - block time.

Discrete time and TPS limitations have a comprehensive and profound impact on DeFi. First, the amount of DeFi activities is naturally restricted by the physical properties of the public blockchain. Second, the efficiency of information synchronization and arbitrage are affected on and off the blockchain. Third, the efficiency of price discovery and risk clearance are also affected.

Continuous-time finance is easier to analyze because it can use mathematical tools such as calculus. The analysis method of discrete-time finance is:
Discrete-time finance = approximation of continuous-time finance + the influence of public blockchain TPS and latency

In discrete-time finance, the time value of money still applies. Although block time is a random variable, the interest theory of mainstream finance can still be introduced into DeFi. Basic concepts and tools such as present value, future value, discount factor, simple interest, compound interest and non-arbitrage pricing are applicable to DeFi.

3. Trustless Environment

No matter what role DeFi participants assume, they are essentially addresses in the public blockchain. The public blockchain offers a trustless environment. Addresses are essentially anonymous, identity-less and reputation-less.

The trustless environment is the foundation of DeFi's openness and permissionlessness. But in a trustless environment, enforcement of addresses' obligations in financial contracts relies on over-collateralization and staking, rather than their creditworthiness. How to understand over-collateralization and staking?

First, over-collateralization and staking are important channels for public blockchains to capture value from DeFi. Without this mechanism, value interaction between the public blockchain and DeFi may be ineffective.

Second, over-collateralization locks in liquidity, which is equivalent to converting the credit risk of addresses into the liquidity risk of the collateral. In DeFi and mainstream finance, risks do not disappear, they just change a form.

Third, because of over-collateralization, the risk pricing efficiency of DeFi lending is very low. The DeFi lending rate does not include a risk premium for the borrower and has nothing to do with the creditworthiness of the borrower.
Fourth, in MakerDAO, over-collateralization guarantees that Dai (essentially CDP liabilities) from different Collateralized Debt Positions (CDPs) have the same intrinsic value. No matter who initiates the CDP, and no matter what kind of collateral the CDP adopts, as long as the over-collateralization rules are followed, Dai is equivalent to each other.

Fifth, staking is a commitment mechanism for stakeholders. This has been fully reflected in the PoS consensus algorithm to solve the Nothing-at-stake problem.

Financial activities are inseparable from trust. Trust can reduce the uncertainty about the future and is essential for reducing the transaction costs of financial activities. This is true for both mainstream finance and DeFi. Blockchain is trustless, essentially transforming trust in people and institutions into trust in algorithms and smart contracts.

4. Oracles and Information

There are two consensus mechanisms regarding blockchain. The first is consensus algorithms such as PoW and PoS, which form a consensus on token status and token transactions. The second is Oracle, which form a consensus on the off-chain information and read the information into the blockchain. Oracle is the basis for information synchronization and arbitrage on and off the

chain. Whichever consensus mechanism applies, it means entropy reduction (that is, elimination of chaos), and energy input is required. The goal of Oracle design is to minimize the ratio of error to cost.

There are many design schemes for Oracle, but they can be roughly divided into two types. The first type of Oracle is based on reputation and voting, represented by ChainLink. The second type of Oracle is based on trading and arbitrage, and the arbitrage mechanism allows Oracle quotations to converge to the market price.

From the perspective of communication engineering, no matter what form it takes, DeFi Oracle sample the continuous off-chain signals at discrete points in time, and then read the discrete signals into the public blockchain (Figure 1).

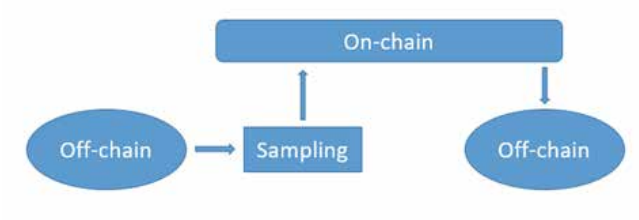

Figure 1: Sampling process of Oracle

5. Liquidity

Liquidity reflects the possibility of selling assets at a reasonable price within a reasonable time. Obviously, the liquidity of transactions on the blockchain is restricted by its TPS. Liquidity is the product of interaction between buyers and sellers. The higher the confidence of both parties, the greater the liquidity. For most commodities, rising demand will stimulate supply by pushing up prices. However, because liquidity is related to the confidence of buyers and sellers, the supply may be the least when it is most needed.

For investors, liquidity is a commitment mechanism that provides confidence about whether a transaction can be completed and at what price. There are two main types of commitment mechanisms. The first type is reputation-based commitments, such as market makers in the limit order book. The second type is algorithm-based commitments, such as automatic market makers. Under the same conditions, products that can provide better liquidity are more attractive to DeFi investors.

Liquidity has agglomeration effect. For multiple liquidity pools, their combined liquidity will exceed the sum of their respective liquidity. This is the same as the risk diversification effect, which is the basic law of finance - the risk of the a portfolio is less than the sum of its components.

6. Arbitrage

There are many driving factors for financial development, such as regulation and technology, but the fundamental driving force is arbitrage. When any financial market or product is first launched, because the pricing mechanism is not sound, there will always be arbitrage opportunities and will attract arbitrageurs. Driven by arbitrageurs, the pricing mechanism will be corrected, and the financial market and products will gradually be improved. With such a cycle, financial development can continue to move forward.

Arbitrage converges prices, but it takes time and cost. For any Oracle based on trading and arbitrage, once the Oracle's quotation deviates from the market price, it means an arbitrage opportunity, but the arbitrageur needs to pay a cost to execute the arbitrage strategy. Therefore, arbitrageurs will carefully weigh the arbitrage benefits and costs, and will execute the arbitrage strategy only when the Oracle quotation deviates from the market price by a large enough extent. The execution of the arbitrage strategy will correct the deviation of the Oracle quotation from the market price until the arbitrage strategy is no longer economically attractive. The higher the arbitrage efficiency, the smaller the Oracle quotation deviation.

Arbitrage is derived from the basic needs of human nature and is a universally applicable mechanism design. Arbitrage only requires people to be rational, to seek advantages and avoid disadvantages, and to maximize their own interests, without knowing whether they are good or bad. In the decentralized environment of DeFi, the incentive and coordination role of arbitrage is more important. For example, MakerDAO collateral liquidation is based on arbitrage design.

7. Incentives

Incentive mechanism design should make DeFi an infinite game, instead of a finite game. Community self-organization and self-upgrading are the keys to the evolution of DeFi. Community members should be able to get their own benefits from DeFi. In other words, in the design of DeFi incentive mechanism, one cannot expect a certain type of participant to always subsidizing others. This problem is common in the blockchain field. For example, if the block reward is not considered, or the block reward drops to a very low level, can the transaction fees received by PoW miners make up for the mining cost? For another example, can the user's payment for an Oracle to make up for the cost of the Oracle?

The above issues all involve the provision and financing of public goods in a decentralized environment. To solve these problems, we must refer to the economic theory of public goods.

8. Risks and Interconnections

The core of DeFi is making profits via taking risks, which mainly includes market risk, liquidity risk, technical risk and credit risk. Market risk comes from fluctuations in the price of crypto assets. In DeFi, the widespread application of over-collateralization and staking converts the credit risk of addresses into the liquidity risk of the collateral. The technical risks of DeFi are much more prominent than those of mainstream finance, which may come from loopholes in smart contracts or from the limitations of public blockchain TPS. Risks can be transferred, shared, hedged, converted and diversified, but they will never disappear.

DeFi projects are interconnected and combined through channels such as information, funds, and risks, which helps to develop the DeFi ecosystem in a bottom-up approach, but lacks an overall plan and accumulates risks. In particular, the more basic projects in the DeFi ecosystem, although they have "moat", the more likely they are to introduce a single point of failure risk.

Many researchers sort out the DeFi ecosystem according to different business types, but it is even more necessary to draw an overall "risk map" for the DeFi ecosystem. In the future, before the DeFi project goes live, in addition to smart contract audits, financial risk audits should also be done. ■

Dr. Chuanwei David Zou
Chief Economist of Wanxiang Blockchain

Previously, Dr. Zou held various positions in China Investment Corporation (CIC) and Nanhu Finance Corporation from 2006 to 2015. Dr. Zou received Ph.D. in Economics from Tsinghua University, Mid-Career MPA from Harvard University, M.A. in economics and B.S. in Statistics from Peking University. In 2015, Dr. Zou was a winner of the 1st Sun Yefang Prize for Financial Innovation (China's top prize for economists) and the 5th China Soft Science Prize for his research on fintech. In 2013, 2014 and 2017, his books were selected into the lists of "financial books of the year" by China Business Network. In 2019, Dr. Zou was nominated as one of the "top 10 institutional economists of the year" by China Business Network.