Bridge Protocol: More sensitive decentralize price oracle machine

Content

1、Overview of Bridge Protocol

The smart contract and decentralized application (Dapp) on the Blockchain have interactive requirements for external data. Blockchain is a closed environment and there's no way to actively obtain real-world data outside it on the Blockchain mainly because the Blockchain fails to initiate Network call and the smart contracts on it passively receive data. And then the smart contract isn't "smart" which is the program which can reach trigger state only when the corresponding conditions are satisfied. In the meantime, the private key signature by contract participant(s) is necessary for final execution of smart contract and the smart contract fails in automatic execution. When the triggering condition of smart contract depends on the information outside the Blockchain, such information needs to be written into the record in the Blockchain. The information outside the Blockchain must be provided by the oracle machine at the moment.

The oracle machine is used to write the external information into the Blockchain to complete the data communication between the Blockchain and the real world. It allows the deterministic smart contract responding to an uncertain external world and is the only way for data interaction between the smart contract and the exterior and the interface of data interaction between the Blockchain and the real world.

The price oracle machine demands from the Blockchain network surge in the current stage (including gambling, stable currency, debit and credit, financial derivatives, futures, insurance and prediction market) The importance of the oracle machine becomes apparent and the new requirements against safety and efficiency of the oracle machine are put forward due to popularity of Uniswap, compound, etc.

The Bridge is aimed at proposing a safer extensible oracle machine network more sensitive to the price and more complying with market requirements in which everyone can participate to meet the current and future potential market needs.

2、Thinking about price oracle machine based on current solution

As for existing price oracle machines in the current stage (such as Bridge and Link) the Bridge Protocol team carries out a lot of analysis and actual call experiments as well as research and thinking for a long time.

For example, the Chainlink is a decentralized oracle machine network, solves the interoperability problem for Blockchain smart contract and safely connects it to the off-chain data source, Web API and traditional bank payment system. It is constituted by two independent parts-chain on the chain and

outside chain which must interact to provide the service. Most of the clients under the chain need to participate in the worst case if multiple rounds of message exchange occur, thus the performance and scalability of Chainlink are ordinary. Furthermore, the Matthew Effect, doing evil by collusion and targeted attack are easily incurred if the oracle machine is chosen on the basis of reputation which is the "semi-decentralization" source denounced by many people.

Due to Bridge, a great improvement in price oracle machines is made in comparison to other projects. New quotation oracle machines (including Bridge) solve partial problems, such as decentralization and being true and verifiable, but there is still a big gap in expansibility and sensitivity which will lead to many problems. For example, the decentralized derivative products falls into Defi products which are extremely sensitive to the price. The price difference within 1min will result in loss of RMB tens of millions which is a big test to all decentralized derivative project parties adopting such oracle machine and they have to choose the oracle machine.

The main tracks of existing products of Defi cover decentralized stable currency, debit and credit, exchange, financial derivative instrument, funds management, gambling, payment and insurance. Such Defi products are with very clear and urgent price oracle machine schemes which are safe, true, accurate and sensitive.

Based on the above study, we make the following judgments about Defi's available price oracle machines:

1、The oracle machine is expandable

2、The price is true

3、The price is sensitive

4、The price is safe and anti-attack

5、The price can be verified

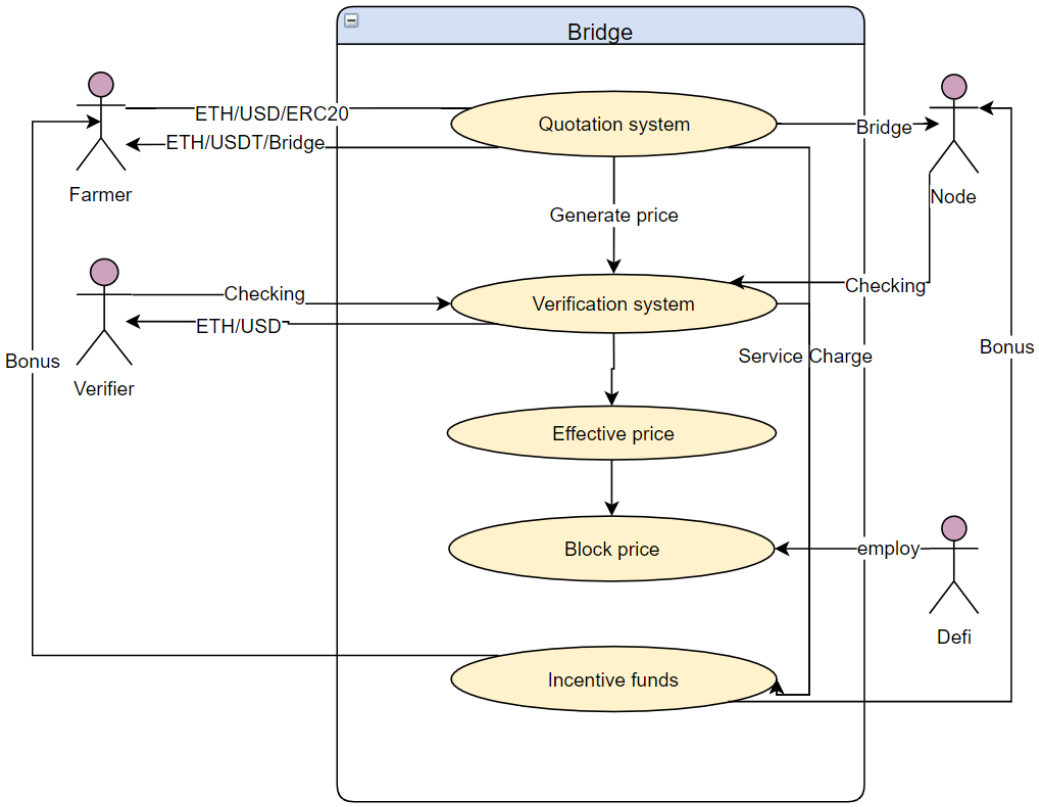
6、The network is distributed

7、Long-time operation

Therefore, Bridge proposes a price oracle machine solution with above-mentioned 7 points.

3、Bridge Protocol solution

3.1 Bridge Protocol framework



3.2 Quotation system

The quotation system is one of very important modules of Bridge. It is the first step of the information outside the Blockchain entering the Blockchain.

Generally, there's a very high threshold against the information outside the Blockchain entering the Blockchain, such as technology development, product design, data maintenance and API intervention.

The part on the chain and off-chain part are designed for DOS and LINK. The former is composed by system contract and management contract and the latter is the node with access permission mechanism which raises the threshold for participation.

We believe that the Blockchain should be open which everyone can participate in, so we have performed concise but not simple design for the quotation system after a lot of investigations and taking Blockchain participants' product experience into full consideration.

On the user end, we optimize the local wallet and quotation contract. The user only needs to shift the token price to the quotation contract in the form of asset pair. For example, the user deems ETH as proper price (such as 1ETH=400USDT) and shifts the assets for quotation to the quotation contract,

and then can complete the quotation when asset size is αETH and 400αUSD. The whole process is completely open without thresholds and every Blockchain participant can carry out quotation, ensuring the whole network is distributed. α refers to scale constant prescribed in the contract which is related to the quoted minimum assets.

On the contract end, the team conducts plenty of tests via test network and the professional safety team carries out safety audit and provides adequate security guarantees for all quotation participations.

3.3 Verification system

The verification system is an important module ensuring the price is true and accurate and bearing partial price sensitivity.

After the user submits the asset and price to the quotation contract, the verification system will work. When any verifier or verification node deems the price is inaccurate with arbitrage space, the ETH or USDT can be bought as per the user's quotation, only few transaction fee will need to be paid and the node verifier won't need to pay the transaction fee.

The mechanism ensures the quotation is the fair price in the market. This is because lots of verifiers will conduct arbitrage as soon as the excessive price deviation happens and the node verifier will also trade to make a profit when the GAS expense is covered by the arbitrage space even though the price deviation is low.

If the quotation isn't traded or completely traded within a period of time, the effective price will be generated. If the quotation is completely traded, the trader will need to conduct quotation anew. The process is the quotation verification period in the verification system.

Considering there will be product sensitive to transaction price in the Defi (such as financial derivative instrument) and for the purpose of minimizing the volatility as much as possible for the quoters in the rapidly fluctuating market, the verification system sets the price will be deemed as effective price if it isn't traded after the 20^{th} block from the quotation block which effectively improves the sensitivity of price oracle machine and lowers the participants' risk.

After the price verification period expires, the quoter's surplus assets and assets traded can be taken back at any time.

The verifier needs to offer a new price compulsively after the price of a quoter is executed according to the contract rules. If the quoter carries out quotation with price p with capital scale being Ω and the verifier A clinches a deal with quoter B at the price p, he needs to offer a price p1 to the contract whose scale is Ω1, but doesn't need to pay the commission without participation in mining. If the arbitrager A1 concludes a transaction based on

A quotation, he needs to offer p2 whose scale is Ω2 (the rest can be done in the same manner), as a result, a continuous price chain with 12 blocks as maximum quotation time interval is formed. p—p1—p2..., quotation asset chain is Ω—Ω1—Ω2...

3.4. Block price

Bridge price is recorded by blocks. Each block forms a price and each block may have multiple quotations. The block price is generated by the effective quotation in the block in an algorithm. This price is called block price or Block-Price. The block price includes the quotation p and the asset size Ω provided by the quoter.

Assuming that the effective quotation for a block is (p1,Ω1), (p2, Ω2), (p3, Ω3) …, the block price is $P=\sum pi*\Omega i/\sum \Omega i$. The former block price is followed in case of no effective quotation in the block.

3.5 Price sequence and volatility

When the first quotation block of Bridge is born, each block of Ethernet will correspond to a Bridge block price, thus forming a price sequence.

The price sequence is significant, such as providing average price for DeFi calls, including arithmetic mean price of N blocks, $Ps=\sum P/N$; or weighted average price of N blocks, $Pm=\sum P*Y/\sum \Omega$. Wherein $\Omega=\sum \Omega i$ is the above effective quotation.

It can provide volatility index for most derivative DeFi calls, such as the rolling volatility of 50 quotations or various volatilities defined by DeFi.

3.6 Secure price network

It is common that Internet and Blockchain network are under attack. Especially in the distributed Blockchain network, the successful attack brings huge benefits and small risks, so that network anti-attack ability becomes one of the important factors to judge whether the project can run for a long time.

There are many attack factors in the price network, such as huge Defi assets calling Bridge. Once the price fails, it may produce irreparable loss of assets. Secure price network of Bridge is well prepared for this.

When an attacker misaligns the desired price, or maintains a misalignment price for some time, the price mechanism may fail even at the expense of the price difference between the misalignment price and the market price.

Bridge guards against attacks by multiple means.

First, the price chain itself is a kind of anti-attack mechanism, that is, the attacker must leave a price and the assets corresponding to the price after attacking the price. This means that either a right price or an arbitrage space will be left after the attacker attacks. There must be verifiers on the market to

arbitrage interests and revise the quotation.

Second, to enlarge the attacker's costs the quotation size of all verifiers is arranged as follows: The transaction size of verifiers is Ω1 and the quotation size is Ω2=βx1. Wherein, β>1, that is, the verifier must quote at more than twice the size. Taking β=2 as an example, the initial quotation is Ω=10* ETH. In case of all transactions, Ω1=20, Ω2=40, Ω3=80... Attackers either expose great arbitrage opportunities to the market (size rises in series, and this attack is almost ineffective) or use extremely high-size assets to deal themselves on the basis of market prices to delay the chance of price adoption.

At present, at most 20 transactions may be quoted in each block of ETH. Distributed random access is implemented for quotation. Assuming each block has one transaction at the size of 10* ETH and the maximum quotation interval is 12 blocks, the asset size to be used is 2^12*25*10=1 million ETH in case of no price update of Bridge within 12 minutes through attacks. When β=3, the data approach the quantitative limit of ETH. The anti-attack property is beyond the reach of any centralized exchange.

3.7 Aggregate price oracle machine

A large number of assets of Ethernet are deposited on the network. Except for the higher demand of Ethereum on the price oracle machine, precipitated assets also need a price oracle machine for better circulation on the Ethernet.

For this purpose, Bridge provides aggregate price oracle machine to generate the on-chain price of any Blockchain asset, while keeping the safe, true, accurate and sensitive prices.

Any Blockchain participant may generate a quotation module of any asset using aggregate price oracle machine. The quotation module for each asset can be created only once.

The generation of the quotation module is determined by the on-chain auction. All Bridge Token for auction will be destructed.

3.8 Bridge Token ＆ node right Token

Name of main Token: Bridge TOKEN
Abbreviation: Bridge
Total quantity: 10 billion
Release mode: Mining (no pre-mining, no private placement)
Proportion: Mining 80%/node 18%/foundation 2%
Destruction method: Aggregate price oracle machine auction, etc.
Contract address:
Genesis block value:
Destruction address:

All data are verified on the chain. All Bridge Tokens on Bridge system are generated by mining without private placement, reservation or pre-mining. All costs will be returned to Bridge holder for incentive.

At the same time, Bridge Token in the aggregate price oracle machine system will be destructed. When the project develops and a large number of assets are deployed, the destroyed amount of Bridge will increase, which is the financial value of Bridge.

Bridge model has been completely decentralized without setting a threshold for anyone, which is similar to Bitcoin. Bridge protocol is updated by DAO, namely the proposer initiates community voting and passes and operates it in certain proportion.

There are 2 aspects of community voting, one for Bridge Token voting and the other for node right voting. This is the equity value of Bridge Token and node Token. voting rules will be published when the project accesses Cross Sea stage.

3.8 Incentive funds＆Bonus

The sources of Incentive funds are as follows:

1、1. Quotation charge paid by the quotation miner to the system;

2. Transaction charge for verifier;

3. 80% of expenses calling oracle machine;

4. Quotation charge contributed by aggregate price oracle machine system to Bridge Token system income pool (initial proportion is 40%).

On the whole, miners obtain Bridge by paying ETH commission and assuming price volatility risks in Bridge quotation network and aggregate price oracle machine network; Verifiers calculate the direct benefits based on the price deviations and assume the risks of transaction price. Therefore, the cost benefit of the verifiers is relatively clear. For miners, the mining model by quotation should be based on the economics.

We will return all ETHs contributed by the miners to Bridge holder. A model of automatic allocation is constructed in this process to give each Bridge intrinsic value. The value is verifiable on the chain. But the closed-loop of logic cannot be completed only relying on the quotation miner's ETH, which goes back to our original intention of building a price oracle machine: The price facts on the chain are fundamental to all DeFi products and the most important infrastructure for DeFi. Therefore, any DeFi developer or user shall be payable when calling Bridge-Price. Incentive funds are greater than the total cost contributed by the miners with the use of ETH network GAS added. Therefore, Bridge creates value for itself and ETH.

It can be understood that the overall value of Bridge is larger than the

overall cost. The cost is uncertain for each miner, which poses a possibility of transaction. Bridge owners of different costs deal in the context that the overall value is greater than the overall cost so as to reach an equilibrium state. This equilibrium is similar to that of the stock market.

4、Possible application scenarios of Bridge Protocol

Bridge is widely applied as a price oracle machine because price oracle machine is needed in most Defi.

Bridge Protocol will be of great significance to product design in the following aspects:

1. Defi product of mobile mining is mostly used by GAS on the existing ETH, which gain benefits by providing moving Ethereum DeFi products. At the same time, the products of Revenue aggregator emerge at the right moment.

The essence of revenue aggregator is equivalent to the smart pool of POW mining. In terms of product design, the accurate and sensitive prices should be quoted to calculate earnings.

2. The model of distributed futures, which introduces the liquidation of any third party, can enlarge the forward transaction size or directly capture the return of price fluctuation. It was impossible to design before. The general futures should perform forced liquidation by a centralized institution, but distributed futures do not take the risk of centralization.

3. Derivatives designed based on volatility of equilibrium prices are used to hedge or smooth derivatives risk. It becomes to design this product because of equilibrium price sequence on the chain.

The most basic product in financial domain or Defi hot product is taken as an example. The decentralized financial product design is realized by the introduction of Bridge-Price, which is different from the simplest point-to-point transaction. The whole DeFi develops fast due to the introduction of global variables. The reason why DeFi needs global variables is that the essence of finance is general equilibrium, not local equilibrium. It is not determined by a simple supply - demand relationship but based on the arbitrage mechanism of the whole market. It is not the law of commodity economy. So simple point-to-point trading cannot solve fundamental financial problems. The global variables that are similar to price sequence without centralized risk and with general equilibrium characteristics are needed. This variable cannot be introduced by centralization. Therefore, Bridge Protocol plan will become the fundamental infrastructure of the whole decentralized financial field.

5、Roadmap

Subgrade

This stage lays a solid foundation for the development of Bridge Protocol with contract deployment and Bridge Dapp online.

Pontoon

In this stage, Bridge Protocol operates stably and seeks for high-speed growth. More self-researched and cooperative Defi products & services will be provided based on Bridge Dapp.

Cross Sea

This stage is a long-term running stage of Cross Sea. The project is solely handed over to community governance and Bridge team is integrated into the community governance based on the community rules.

6. Risk Prompts

There is also risk in Bridge-Price similar to all financial products or financial services. Here's a simple description of Bridge-Price's reference risk. There may be other risks that are not described or recognized:

Because of the existence of minimum arbitrage space, there may be risks in the financial services with higher requirements for price difference accuracy when using Bridge-Price. Compensation must be made in the design.

The market arbitrage mechanism is not deeply explored, that is, the huge opportunities are ignored. This is the deepening of industry development that needs to be accepted and recognized by the market.

Although prices cannot be attacked, the price mechanism can be indirectly attacked by attacking Bridge. For example, above 51% Bridge will be occupied following Cross Sea stage, and the important parameters are modified to make the quotation mechanism invalid. This problem can be prevented by limiting key parameters and enhancing Bridge market size, so that it is difficult to achieve 51% attacks.

Risk of code vulnerabilities or major external changes will influence the price callers, such as vulnerability in Ethereum underlying code and Bridge system code, or significant changes in the external environment. This can be corrected by on-chain governance and contract splitting.