HALO Network

Whitepaper V2

ABSTRACT

The DEFI revolutionary wave is leading the development of digitalization globally. We are at the best era of blockchain development. According to CoinGecko, which published the <2021 Q1 Digital Asset Industry Quarterly Report DeFi Part>, the overall market cap of DeFi has reached $96 billion in the first quarter of 2021.

Despite the fact that ethereum is still the main battlefield of the DeFi ecosystem, there are many applications that have been expanding to other chains. BSC continues to attract many quality projects to its strong BSC ecosystem due to its low fees.In addition, the popular Polkadot, although the main network is still not running, many DeFi applications are still planning to launch on Polkadot due to its strong community power.

Solana, on the other hand, proposes a unit-chain delegation proof-of-interest protocol that solves the problem of handling a single trusted time source in a distributed network. it also attracts a group of high traffic applications due to its better operability and faster network speed.

It also attracts a group of high attention applications due to its better operability and faster network speed.

Leveraging the experience of other projects, HALO proposes a highly available, rapidly reusable and agile iterative blockchain architecture that is fully compatible with Ethereum, meaning that Ethereum development tools and DEFi products can be seamlessly migrated and merged into HALO ecosystem.

Looking at the product perspective, the HALO ecosystem aims to serve innovative DEFI applications, we will be providing a service-oriented, easy-to-deploy DEFI framework in the form of scenario components, including DeFi tools, infrastructure, NFT, games, wallets, DApp applications. The HALO ecosystem will be developed in eight main areas and nearly 20 sub-sectors,

including DEX, derivatives, transaction analysis visualization, lending, stocks, synthetic assets, stable coins, OTC, etc.

From the technical point of view, large number of base layer enhancements have been optimized by HALO. By using HALO's powerful development framework, development tools and DEFI components, developers can quickly develop DEFI products to meet the requirements, and conduct version iteration and validation with agile development mode.

Table of Contents

1. Introduction

1.1 Visions

HALO Network is dedicated to establish a HALO Infinity decentralized financial system that aims to a highly efficient HPOS consensus mechanism, a more transparent dual-transaction model and a robust & secure oracle machine. HALO Network provide scalable components for liquidity management, on-chain and off-chain scenario convergence, to form the underlying financial infrastructure tools for the rapidly growing DEFI ecosystem in order to fulfill the needs of the evolving DEFI innovation.

1.2 Core Values

HALO is dedicated in creating a highly efficient and modular DEFI base layer as below：

- On the basis of large-scale DEFI application scenario, the HPOS block generation rate is faster than the Ethernet time, about 5 seconds or less, and it can handle more than 1000 transactions per second with multi-node cluster.

- HALO SWAP adopts innovative transaction management with bimodal liquidity:

  -Optimized AMM liquidity management with constant product market making x*y=k;

  -Implement HMM trading model to improve price acquisition accuracy and capital efficiency.

- Proposed a lower cost and more efficient cross-chain intermediate solution based on the EVM smart contract engine.

- Constructed with decentralized oracle machine, providing the most extensive oracle machine data source support, supporting on-chain aggregation and off-chain price aggregation, providing extensive quotation model, including quartile price, average price, and optimal price, TWAP, and credit price.

1.3 Principles

In order to achieve a scalable and reusable high-performance financial public chain, HALO Network will follow the following design principles:

- **Decentralization**

  All parties involved in the HALO Network are equal. Neither HALO Labs, nor users nor the community, none has any exclusive right. All matters pertaining to the HALO network will be determined by voting, and requires of more than 50% up vote to be approved. Voting rights will be determined by the quantity of HO one's hold.

- **Compatibility**

  According to the network effect and Matthew Effect, we believe that the Ethereum ecosystem will be further expanded and optimized. HALO Network will be designed to be as compatible as possible with Ethereum, for example, it will also be based on Ethereum Virtual Machine(EVM), using the structural, object-oriented (encapsulation, inheritance, polymorphism, interface, abstract contract) features of the Smart Contract Solidity language, and also supporting Web3.JS / Truffle.

- **Scalability**

  Many underlying functions and structures are similar between blockchain services in the same domain. It is never a good approach to develop every system from scratch. HALO Network supports innovative DEFI application which is service-oriented, easy-to-deploy DEFI framework in the form of scenario components.

- **Interoperability**

  Interoperability is the most fundamental requirement for the new generation of DEFI. The main reason for poor interoperability is that the underlying protocols of each project are not standardized, the diversity leads to isolation between chains.

HALO Network can provide standard communication mechanism, network protocol, asset communication, and service terminology to facilitate the interoperability of different parallel chains. A logical hierarchy is established to create layers of modules that handle the same functions, the layers able communicate with each other through a service language. However, cross layers are not able to communicate directly. Thereby shielding the differences in heterogeneous and consensus algorithms, governance structures, block structures, etc.

- **Trustworthy Isolation**

  The minimum security mechanism and trusted computing module within the chain are clearly defined, the security boundary is also established to distinguish the boundary between trusted and untrusted. Maximum security is ensured through a clear unified security interface and the use of reference monitoring, where access paths can be confirmed and verified to ensure security and trustworthiness

1.4 DEFI Approaches

HALO Network is committed to provide developers with iterative development and backward compatible DEFI components. According to the principles of independence, low cohesion, high integration and public modules, it is divided into the following modules：

- **HALO Infrastructure Module**

  HALO INFRA：HALO Core, HALO VM, HALO Oracle, HALO Storage, HALO Data etc.

- **HALO DEFI Components**

  HALO SEEE： HALO SWAP, HALO Bridge, HALO HOUSD, HALO P2P, HALO STOCK, HALO OTC etc.

- **HALO Governance Module**

  HALO DAO： HALO Pledge, HALO Reward, HALO Burning, HALO Mint, HALO Merger etc.

2. HALO Network Technology Core

2.1 Dual Exchange Transaction Mechanism (HMM & AMM)

2.1.1 Drawbacks of AMM Automated Market Maker

The AMM liquidity management in liquidity and price stability based on the constant product market making formula: x*y=k, which has intrinsic drawbacks in that:

① It works well only with high liquidity pools. It is easy to have a deviation between the actual exchange ratio and the price especially when the depth of the liquidity pool is relatively small or the amount of funds to be exchanged is relatively large

② The on-chain price is confirmed by the smart contract of the transaction. The slippage problem may occurs when the chain is busy.

For Example:

Suppose the ETH/DAI pool has 10 ETH and 10,000 DAI, and the initial market is 1 ETH = 1000 DAI. The pool is balanced when the internal price of the pool is equal to the market price. When users want to buy 20 ETH, the pool will not be able to accept the transaction of 20 ETH, which causes the stability problem of ①; when the market price fluctuates greatly during the block confirmation of ETH, it causes the slippage problem of ②.

2.1.2 HMM Node Market Makers

In order to avoid price distortion, HALO SWAP introduces the HMM (Node Market Maker Model) based on the AMM market maker model. The combined operation of AMM and HMM improves the liquidity and capital utilization, reduces fluctuations and brings the trading value closer to the actual price.

HMM is the transaction of user with HMMPOOL and HOLPPOOL. The transaction prices are quartile prices of COINBASE-HUB, BITMAX-HUB,

HUOBI-HUB, BLNANCE-HUB, ASX-HUB, NDX-HUB, etc. in HALONODE. The query price data of the oracle machine is the white list of transactions.

2.1.3 Quartile Price of HMM

The HMM node market maker model quartile prices rank the oracle feed prices from lowest to highest, forming a price series a1, a2, a3 ...an then the three quartiles Q1, Q2, Q3 will be obtained.
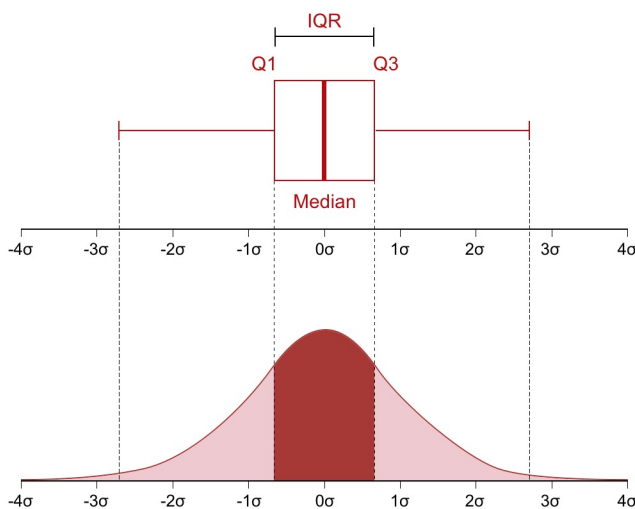
$$Q1 = (n+1)/4$$

$$Q2 = 2(n+1)/4 = (n+1)/2$$

$$Q3 = 3(n+1)/4$$

n indicates the number of nodes of the oracle machine

Set the price of AMM be P.We have the following format.

According to the AMM model.

Q1 ≤ P ≤ Q3,P falls inside the median price box.

According to the HMM model.

P < Q1 & P > Q3,P falls outside the median price box

2.1.4 HMM Initial Pool

The initial HMM funding is used to provide the AMM with liquidity and price stability during the initial opening of the market. This allows AMM to maintain a stable flow of liquidity from the beginning. According to the DAO governance policy, each HMM pool will be initially backed by HALO tokens. Thus, we define the initial pool of HMM funds P0, P1, P2, and the initial funding DE of the HMM is denoted by:

P0=DE (single coin pool, P0 is a single coin)

P1+P2=DE (dual coin pool, P1 and P2 are currency pairs)

The initial DE pool should not be too large or too small. A large DE pool impacts the security of the entire HO token ecosystem, while a small DE pool does not achieve the effect of maintaining stability. Therefore, we use the HMM monitoring contract, HALODE, to monitor and adjust the pool size.

2.1.5 HMM Monitoring Contract, HALODE

The HALODE contract monitors the capital level of the HMM pool within a time period of 3 or 5 seconds. When the fund level is excessive (e.g. greater than 3 times the initial DE price) within a certain period, the HALODE contract will freeze the excess DE (more than 3 times the initial DE) until the DE has been maintained at about 3 times the initial amount.

When the HALODE contract monitors that the HMM pool is less than or equal to 1 times the initial amount of DE, the HALODE contract will release from the frozen DE to replenish the HMM Pools until the DE exceeds 1 times the initial amount.

2.2 HPOS Consensus Algorithm

Consensus protocol is the most significant core of a blockchain system.

Consensus mechanisms are all suffer from CAP problems, namely consistency, availability and partition fault tolerance, which are hardly to be guaranteed at the same time. In addition, it is also necessary to ensure that all nodes are integrity and consistent to avoid forking. The consensus mechanism is extremely important for HALO, which is committed to be the foundation layer of DEFI and pursues the goals of high accessibility, fast reusability, and agile iteration.

Therefore, HALO has optimized a consensus mechanism for large-scale applications, called HPOS, in order to meet the needs of the large-scale financial transactions.

2.2.1 Objectives of HPOS

- Faster block generation rate than Ethereum, e.g. 5 seconds or even less.

- High TPS, More than 1000 transactions per second.

- Multiple nodes online, allowing up to 99 HALO-NODEs to be online at the same time.

- Compatible with Ethereum, the hardware configuration in setting node is almost identical to Ethereum.

- Equipped with an on-chain governance mechanism based on token pledge.

- Oracle machine feeding mechanism in the contract layer.

2.2.2 Optimization of Clique PoA algorithm

The core algorithm of HPOS is stripped of the Ethash algorithm. Instead, it optimizes the Clique PoA algorithm. HPOS Clique relies on the order of authorized HPOS Nodes signers to generate blocks, which can be elected by authorized signers (with more than 50% of the votes cast) to add new signers and eject the authorized signers. The consensus engine HPOS Clique has smoother choking time and will not be affected by the 51% attack.

At the same time, the minimal work is done on the core data structures to maintain as much as the existing compatibility to the Ethereum client.

HPOS allows anyone who is a token holder to vote to become a HALO-NODE through a node election. HALO-NODE can produce blocks on behalf of voting users and share the production reward with the voters.10% of the production reward will be directly awarded to the node, and the voting users will share the remaining 80% weighted equally based on the number of votes.

The node rewards are all contributed from transaction fees.

2.2.3 HSTAKE, a fair authentication algorithm

HALO Network allows up to 99 HALO-NODEs to be online at the same time. The online situation is updated in real time depending on the voting ranking, node network stability and hardware performance. In the node authentication algorithm, HPOS introduces a time-based fair authentication algorithm HSTAKE.HSTAKE fair authentication can be equivalent to a rule that：Any nominator holding at least 1/n of the total shares is guaranteed to have at least one set of validators whom they trust be elected.

HSTAKE uses the principle of equal opportunity. HPOS restricts the issuance of blocks by an authenticated node to a maximum of one block in each consecutive SIGNER_LIMIT block. In other words, only SIGNER_COUNT - SIGNER_LIMIT certified nodes can participate in block issuance in each round, so that certified nodes have equal opportunities to issue blocks and it also effectively avoid malicious nodes from continuously issuing blocks.

The equal opportunity principle of HSTAKE is also reflected in the overlay of difficulty, that is, each node will determine this node as "inturn" node when issued, if it is an "inturn" node, the difficulty of the block generated by that node is "K", otherwise it is "1". Only one node will be an "inturn" node in each round.
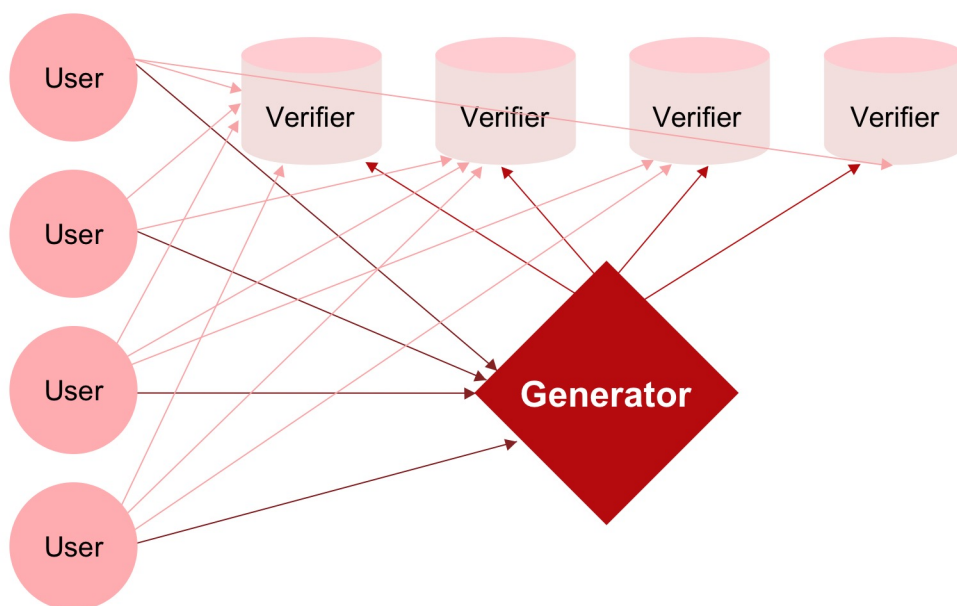
2.2.4 Proof of time series

HALO Network is expected to produce a block not more than 5 seconds, and each block will have only one HALO-NODE will be authorized to produce. If the authorized node is not able to produce the block in time, the next node will be authorized to produce it. At the same time, the node that is not able to update in time will be demoted, and the node with too low weight and high voting rate may not be able to go online.

At any given time, a HALO-NODE node will be nominated as the validator to produce a HALOTIME sequential, which provides the network read consistency globally and a validated timestamp hash. This HALO-NODE validator processes user messages on a first-in-first-out basis so that other nodes in the system can process them efficiently in order to maximize throughput. The HALO-NODE validator will first refresh the execution transaction in RAM, then publish the transaction as well as the final state signature to the replica node of verification. The validator will perform the same transaction on its copy of state and publish the signature of its computed state as a confirmation. The confirmation of the publishing serves as a vote for the consensus algorithm
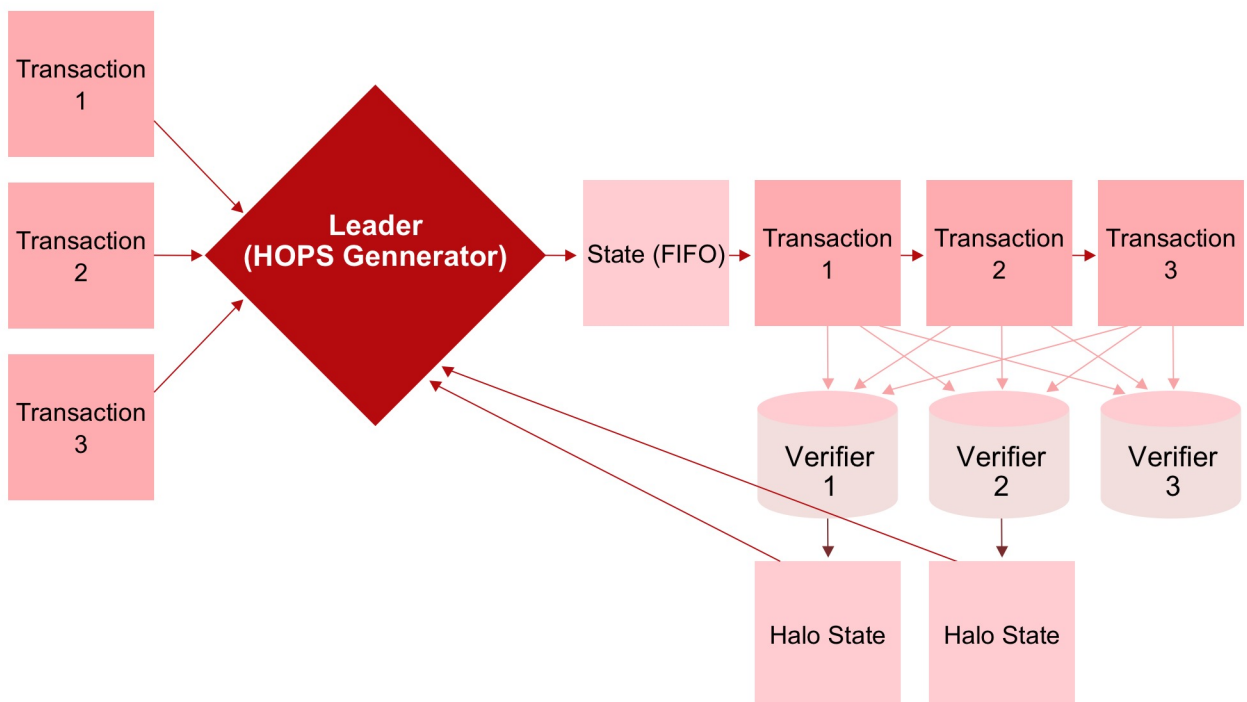
2.2.5 Anti-attack prevention

HPOS is capable of protecting against the mainstream attacks on the POS, the following are some of the attack prevention mechanisms, more prevention details in the Yellow paper.

- **Spam Prevention**

  Spam is a malicious user who can create many replicator identities and send malicious proofs to the network.   To facilitate the speed of authentication, encrypted data and the entire merekle tree need to be provided by the node to the rest of the network when requesting for authentication. However, the HPOS replication proof allows authentication of any other additional proofs, thus such attacks can be avoided.

- **Partial Erasure Prevention**

  In Partial Erasur, an attacker is able to copy node as well as to wipe some data away from the node. However, the number and randomness mechanism of HPOS authentication will make the attack become difficult. For example, if a user intends to remove one byte from each 1mb block with storage of 1TB data. By sampling one byte per every megabyte, it is possible to match any erased byte 1-(1- 1/ 1000000)1,000,000- 0.63 that has conflict. After 5 attempts, the possibility of having conflict is 0.99.

- **DOS Attack Prevention:**

  DOS attacks are not only happening on networks and systems, but also on consensus algorithms. By creating a large number of valid replicator identities, attackers create opportunities for denial-of-service attacks on the network. To limit DOS attacks, the consensus protocol of HPOS can select a replication target, where replication proofs that satisfy the required characteristics (e.g., availability) are rewarded.

2.3 Cross-chain Intermediate Layer Protocol

2.3.1 HALO Bridge Protocol

There are many kinds of cross-chain technologies that are constantly being extracted and applied. Cosmos is essentially a blockchain system that allows a single cryptocurrency (e.g., Bitcoin) to be linked to more external transfers using a two-way peg approach to create a framework, but the sidechain solves the problem of Extensibility rather than Scalability. Fundamentally, Cosmos carries out trustless inter-chain communication through the main hub chain. However, this inter-chain communication is limited, which only allows the transfers of digital assets, but not arbitrary information. Then, the parallel chain framework was proposed by Polkadot, The network is unified by a relay chain to manage the consensus of the network, whereby all the parallel chains share the same level of security. However, the cost of joining a parallel chain is relatively high, and the resources on the parallel chain is limited.

HALO proposed a lower cost but high efficiency cross-chain solution, HALO Bridge Protocol. It is a cross-chain middle layer concepts based on EVM smart contract engine. The transaction and consensus process of HALO Bridge Protocol are all happened in the smart contract, which is secure, transparent and reusable. The HALOer, refers to the users who participate in consensus voting, they have the right to vote on each cross-chain transaction through hardware multi-signature. The token freezing and extra issuance can only be executed after consensus have been agreed upon.

The HALO Bridge is a product of the HALO Bridge Protocol, which currently supports Ether, BSC and other cross-chains.

2.3.2 Cross-Chain Process

With the introduction of the intermediate chain layer, the cross-chaining process from ERC to HALO, for example, is simply as described as follows:

① The user deposits the ERC tokens in the Bridge contract of ERC

original chain, input the target chain marker, specifying the target chain and the target address.

② HALO intermediate chain, monitor_chain, monitors the chain data every second, once the special target chain logo is detected and confirmed, the forward_chain will be triggered immediately.

③ Forward_chain triggers the mint method in the Bridge contract of the target chain through the consensus of the intermediate chain. The corresponding quantity of ERC token will be issued and transferred to the target address.

④ In the process of deposit, users need to pay the native gas fee of the original chain for cross-chain transaction fee, for example ETH, DOT, EOS. HALOER will receive a portion of the fee as a reward by OER will receive a portion of the fee as a reward by performing consensus tasksperforming consensus tasks.

2.3.3 Penalty Interest mechanism

The HALO DEFAULT, the contract that is responsible for recording the blocks missed by each validator. Once the DEFAULT metric exceeds a predefined threshold, the validator's block reward will not be transferred to HALO for distribution. Instead, it will be shared with other better validators. In this way, the bad validators will gradually exit, as their delegator will receive less or no reward. If the data continues remains at a higher threshold level, the validator will be penalized and will be forwarded back to HALO. In HALO, the validator's staked assets will be penalized by 40%.

2.3.4 Distributed Private Key Management

In order to keep the chain as decentralized as possible, the transactions of the HALO Bridge Protocol intermediate chain are managed using a distributed key mechanism. The distributed private key control controls the private keys of various assets through distributed nodes by mapping the original chain assets to the cross-chain. The core contract of distributed keys is in HALO HUB.

HALO-NODE will be authorized to manage segmented keys at the time of go-

live, with M segments, respectively

(SK1,,,,SKm), and the number of nodes is N (Node1,,,Noden).

M and N are linearly related, if M is too large, the key security is high but inefficient, if M is too small, the key security will be reduced, while the case of nodes offline has to be considered as well. In order to balance security and efficiency, the following formula is available:

$$M = N-2 \qquad (2 < N <= 20)$$
$$M = INT(N/2) \qquad (20 < N < 100)$$
$$M = 50 \qquad (N >= 100)$$

The RECVMID contract of HALO intermediate chain monitors the data on the chain every second and merges the data of cross-chain blocks. When a node produces a block, if there is a cross-chain transaction demand for the corresponding block, it will be handed over to the block production node to initiate a cross-chain transaction. The transaction content will be validated by other nodes and the corresponding cross-chain transaction will be initiated when more than 67% of the nodes approve the validation. During the whole process, the private keys are stored in different HALO-NODEs in the form of "SK1 ,,,,SKm", and the data interoperability between the complete chain and the side chain is supported. All the keys segment are stored as backups in consideration key loss problem.

2.3.5 HALO BRIDGE-HOBG Transfer Contract

Taking the HALO BRIDGE as the example, the HALO BRIDGE-HOBG (Halo Bridge) transfer contract mainly consists of

Existing: send_to_side_chain and recv_from_side_chain

New: monitor_chain and forward_chain two contracts

HALO BRIDGE-HOBG (HALO Bridge) to convert HALO OS related token to ETH, BTC and other assets. For example:

Users can complete the transfer of ETH token of Ethernet network and HRC-ETH of HALO network through Halo Bridge.

Users only need to pay the transaction fee charged by the Ethernet network

to get 1:1 ratio of HRC-ETH in the HALO network, the HRC-ETH can be used for trading, and can also be converted back to ETH token with 1:1 ratio via HALO Bridge. The transaction will be completed by HALO-NODE through HALO HUB. The HALO HUB will charge the corresponding fees charged by the Ethernet network without paying Additional fees.

In consideration of the fact that most projects may decide to issue coins on Ethereum first and then switch to HALO, HALO has designed a mapping bridge contract for Ethereum, which supports the merging and mapping of token on Ethereum chain to HALO chain.

For example: TOKEN A is issued on Ethereum chain and due to the evolution of the project it is necessary to switch to HALO chain, as TOKEN B. There are several options available:

- BridgeMap: A is fully mapped to B, A is destroyed, B is activated.

- BridgeCross: A cross-chain to B, A is locked, B is activated.

- BridgeMix: A and B are merged in proportion to their tokens.

2.4 HALO Oracle

2.4.1 Data Source

HALO offers a decentralized data oracle that connects smart contracts such as Defi to external data and APIs, which inclusive

- Top 30 digital currency pairs

- Top 100 Stocks

- Commodity prices

2.4.3 Quotation Node

5 ≤ number of quotation nodes ≤ 30

If the offering node is less than 5, an error will be reported.

If the offering node is greater than 30, the best price will be calculated by the quotation algorithm.

2.4.4 Convergence mode

HALO oracle supports both on-chain and off-chain convergence

- **On-chain Convergence:**

  Nodes submit and converge data to the on-chain contract to obtain the best data.

- **Off-chain Convergence:**

  Trusted data is first converged off-chain to obtain the best data before uploading to the chain. According to the experiment, the reliability and stability of off-chain convergence is at least 30% higher than on-chain convergence.

2.4.5 Safety Assurance

Node Credibility: High credibility means higher security.

- **Pledged tokens:**

  The security is proportional to the amount and duration of tokens pledge. The larger and longer the tokens had pledged, the higher the security.

- **Deviation:**

  Price deviation within 10% is considered safe, deviation of 10% to 20% is warning level, deviation of more than 20% is considered as not safe.

2.4.6 Quotation Model

- **Average price:**

  The average price of all nodes.

- **Optimal price:**

  Assuming the number of nodes is N, removes the highest price and the lowest price, the optimal price is the average price of the remaining nodes.

- **TWAP average price:**

  The cumulative weight of each node, if all the nodes have the same weights, then the average price will be the average price of all nodes.

- **Credibility price:**

  The credit price is limited by the credit value, K. The value K is taken as a percentage between 0 and 1, where K1 is the lowest credit, K2 is the highest credit, The K1 and K2 parameters are adjustable in the backend.

- **Quartile number:**

  All models of HMM are quartile sensitive prices.

3. Decentralized Applications

HALO is designed based on a rapidly replicable technology layer by introducing DEFI scenario components to build an agile and iterable DEFI product. It meets the diversified financial needs of the digital economy such as trading, custody, OTC, stable coin, lending, pledge, stock, insurance, etc. HALO is highly scalable with the capability to freely combine and expand the DEFI financial components to meet technical and market needs.

HALO's scenario DEFI components are:

- Fully compatible with Ethereum, DEFI applications on Ethereum can be mapped to HALO with almost no hassles.

- Service oriented architecture deployment, HALO system is pre-defined to cover DeFi, tools, infrastructure, NFT, games, wallets, DApp applications, and R&D, eight major areas of the ecosystem. Which includes.

- DEX, derivatives, transaction analysis and visualization, lending, synthetic assets, stable coins, etc.

- With high scalability and the ability to freely integrate and expand DEFI financial services according to market needs. It has the ability to consolidate and merge the governance system.

3.1 HALO SWAP

HALO SWAP is the foundation for the DEFI component. The SWAP component is standalone to facilitate for other DEFI applications. As mentioned earlier, HALO SWAP supports two trading models: the HMM nodal market maker model and the AMM automated market maker model.

For example, using quartile prices of Q1 and Q3. When the liquidity pool prices are out of the Q1 and Q3 boxes, the HMM mode will be triggered to obtain greater liquidity and accurate price.

Inspired by the Uniswap V3, HALO SWAP optimizes the liquidity mode component (for both HMM and AMM modes), as following:

- Supports Virtual Reserves, which provides pools of funds with a fixed product curve for specified interval liquidity.

- Support the minimum cost calculation for interval granularity-Tick. By using relative values of capital and price relative values to calculate the liquidity.

- Adding a function called Hybrid Liquidity Accuracy Control to the x*y=k curve, to boost the capital efficiency to 500 to 4000 times.

- Multiple LP rates are available (0.05%, 0.30% and 1.00%). By using these settings, it is possible to set higher rates on more risky pairs (ETH/DAI) and lower rates on less risky pairs (USDC/DAI).For example, set a 0.05% handling fee for less volatile assets, 0.3% for HALOETH/HALODAI pairs which has higher trading volume but also higher volatility, and 1% for other assets.

- The traders and LPs are offered with a new feature, Range Orders, which is an upgrade of the Limit Orders on the Exchange. Its purpose is to compensate the current Market Orders.

- Users can top up an asset within a set price range. If the asset enters the range set by the user, the asset will be gradually exchanged for another asset of the trading pair. If the price of the asset exceeds the price range, it will be exchanged for another type of asset.

3.2 HALO Stablecoin

The HALO stable coin (represented below by currency code HOUSD) is issued by staking digital assets on the HALO stablecoin contract. HALO Labs launch the HOUSD mainly to address the decentralized access of more localized fiat currencies into contracts within the HALO Network and then to other blockchain networks, to obtain the localized financial capabilities on the smart contracts in the HALO Network and the cross-chain asset contracts.

HALO stablecoin is not a single digital asset, but a series of digital assets. V1 version will release the following stable currency:

HALO stablecoin is not a single digital asset, but a series of digital assets. V1 version will release the following stable currency:

- HOUSD - U.S. dollar $
- HOEUR - Euro €
- HOCNY - CNY ¥
- HOGBP - BriΘsh pound £
- HOJPY - Japanese yen ¥
- HOINR - Indian rupee ₹
- HOTWD - New Taiwan NT$
- HOHKD - Hong Kong dollar HK$
- HOKRW - South Korean won 원

- ◆ HOSGD - Singapore dollar S$
- ◆ HOMYR - Malaysian ringgit M$
- ◆ HOIDR - Indonesian rupiah Rp
- ◆ HOVND - Vietnamese dong ₫
- ◆ HOAUD - Australian dollar A$
- ◆ HOCAD - Canadian dollar C$
- ◆ HOZAR - South African Rand R
- ◆ HOAED - UAE Dirhams
- ◆ HOTHB Thai Baht ฿
- ◆ HORUB Russian Ruble ₽

- ● **Supply and Destroy (Burn) of HOUSD**

  The Initial issuance of all the stable coins is 0, and each token is issued by the user through a coinage contract. The V1 coinage function supports all the currencies of Halo Bridge. The coins are minted according to the real time exchange rate based on the HALO-HUB-ASX-HUB (Australian Exchange – FX Trading Data Tray). The staking assets that are used for minting their coins will be decentrally managed through contracts to ensure asset security.

  Users can exchange HOUSD for other digital assets at a real-time exchange rate, and the HOUSD will be destroyed after exchange.

- ● **HOUSD Economics**

  HALO Lab believes that the current stablecoin market lacks a consumer-oriented application. Most stablecoins are digitizing the U.S. dollar. Therefore, HALO Labs launched the HALO Stablecoin, which is mainly for the digitization and localization of localized currencies. Stablecoins are more easily accepted by users on the consumer side.

  For example, in Russia, if merchants accept digitized U.S. dollars,

merchants also need to accept the exchange rate risk between the ruble and the U.S. dollar. In the case of largescale transactions, it is difficult for merchants to use it normally, but Merchants will easily accept HORUB. Merchants can convert HORUB to other digital assets at the actual exchange rate or convert it to cash through HOOTC at any time after receiving the payment from HORUB.

- **The Advantages and Risks of HOUSD**

  The decentralized nature of HOUSD will free it from regulatory and political Risk. HOUSD can be used as value-stored tool to avoid exchange rate risk.

  Due to the algorithmic logic of the contract, the HALO stable coin may have a risk less than 1:1 staking assets. For example, when the user mortgages one ETH at the ETH price of 1,000 US dollars to get 1,000 HOUSD, there is 1 ETH in the pool. If the user is at the ETH price of 2,000 US dollars in the redemption operation, the staking assets will face the situation that the redemption cannot be completed. If this extreme situation occurs, HOLPPOOL digital assets will be used to make up the 1:1 staking assets, and the user will not face this risk.

3.3 HALO Loans

HOP2P 1.0 Pledged Lending

HALO's HOP2P 1.0 component product realizes decentralized pledged lending. HALO HOP2P 1.0 sets up a lending liquidity pool. User deposits funds into the liquidity pool, and lenders lend funds from the pool. In terms of risk control, HALO HOP2P 1.0 lending process is operated by smart contracts on the chain without human operation and intervention, eliminating the need for the complex credit risk control mechanisms used in traditional financial institutions.

- Borrowed funds must first be pledged, and the borrowed funds must be less than the value of the collateral, i.e.: Lend fund< Pledged Fund

- In consideration of liquidation risk, cryptocurrency volatility risk, and to avoid triggering any systemic risk, HALO HOP2P 1.0 sets Loan-To-Value (LTV). Each reservation has a specific Loan value (LTV), which is calculated as a weighted average of the different items that make up the LTV of the underlying collateral.

HALO HOP2P 1.0 Loan-To-Value (LTV) is the ratio of loan-to-value to pledge value, with a maximum LTV is between 60% and 80%.

HALO HOP2P 1.0 Borrowing position supports two interest rate models, fixed rate and variable rate. Borrowing The borrowing time is open-ended, i.e. there is no specific repayment time requirement and it can be paid back at any time (partially or full). Subsequent lending models with a time frame are avaiable, such as 7 days, half a month, one month, three months, half a year and one year.

HALO HOP2P has a risk control mechanism to avoid the risk of violation and the systemic risk caused by extreme market conditions.

- **Settlement Mechanism**

  Settlement of a borrowing position may be triggered when prices are volatile. A settlement event occurs when the price rises the collateral falls below a threshold LQ, called the settlement threshold, Meeting this ratio triggers a liquidity bonus, which provides an incentive for liquidators to purchase collateral at a discount. Each pool has a specific liquidation threshold, using the same methodology as LTV. The average settlement threshold, La, is calculated using a weighted average of the settlement thresholds of the collateral to perform this operation dynamically. The borrowing position at any point in time is characterized by a risk control factor function, H f , which is a function of total pledged loans.

$$H_f = \frac{SUMCollateral * L_Q^a}{SUMBorrows + SUMFees} \quad when \quad H_f < 1$$

- The lending targets are selected from digital currencies with high trading volume and good liquidity. The selection of lending bids will managed by HALO DAO.

- Price warning to avoid flash lending loopholes and extreme cases of intense price fluctuations. Risk control will be triggered when price deviation exceeds 20%.

- Setting up an insurance fund for compensation in extreme cases.

HOP2P 2.0 Credit Lending

HALO's HOP2P 2.0 protocol introduces real-world credit lending.The credit lending model is applicable to a wide range of lending scenarios, such as project-specific funds lending, credit consumer lending, etc. Its protocol is based on the user profile provided by the liquidity pool, decentralized credit assessment. Combined with peer-to-peer aggregation and liquidity pool management for intelligent matching, it promotes risk control and liquidity matching for credit lending.

HOP2P 2.0 framework is suitable for real estate NFT, consumer lending, credit lending and other scenarios which allow to credit-backed, reduced collateral rates, and even supports zero-collateral credit lending scenarios.
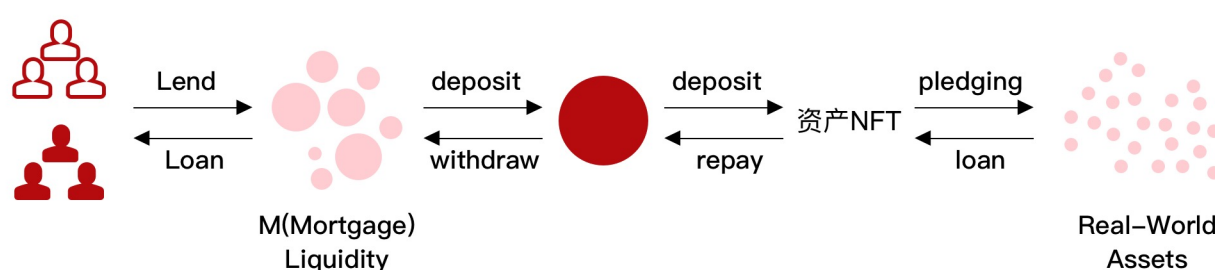
Through the HALO Pooled loans pool, companies or "asset originators" can provide financing by pledging real-world assets such invoices, property deeds as a NFT, then uses these NFTs as collateral in its loan pool to finance its assets. HALO will offer two interest rates for decentralized investors, including fixed rates and default risk rates.

3.4 HALO STOCK-HOSTK

HALO stock contracts are decentralized equity trading contracts realized through the HOSWAP — HMM model. Since the HALO-NODE V1 version oracle machine of HALO - NODE only supports the NASDAQ stock exchange,the whitelist of HALO stock contract in the version V1 is NASDAQ stock. The naming rule for individual stock token is to add the prefix HRC - before the stock code. For example, the stock code of Apple Inc. in NASDAQ is AAPL, then the token in the HALO stock contract is named HRC-AAPL, meaning the trading with HOSTKPOOL and HOLPPOOL.

3.5 HALO OVER THE COUNTER-HOOTC

The HALO counter transaction contract is a multi-currency decentralized over the counter (OTC) transaction contract launched for the HALO stablecoins. Users can realize the exchange of decentralized legal currency and digital assets through the contract. The contract realizes the default in the transaction process through the new DAO model. For regulatory actions such as arbitration and information authentication, users need to provide over 50% mortgage digital assets to use the contract. If there is a breach of contract, 3-9 verification nodes will conduct arbitration. If there is no default, the transaction will be automatically completed after 72 hours. The node needs to provide a certain amount of HO staking to HPOS-NODE, and the corresponding HPOS-NODE is certified as a verification node.

HAOL emphasizes ecological development and will support global HALOers to develop more ecosystem in terms of technology, funding, market and community. HALO will technically providing integrated development tools, SDK interfaces and initiating marathon hacking project competitions. Establishing a dedicated token fund to support quality HALO projects.To provide more exposure to eco-users for globalized markets and communities.

4. Tokenomics

The HALO Network will issue governance tokens for decentralized governance and mining rewards. Currency code: HO, with a total circulation of 21million. Following the principle of decentralization, the distribution of HO will be used for HOLPPOOL (HALO DAO) construction and liquidity mining. HALO Labs will not receive HO distribution and only receive the HPOS-NODE block production rewards during the election process for unopened node.

4.1 Token Distribution

CONTRACT	ISSUING METHOD	NUMBER OF TOKENS
HOLPPOOL	Genesis	10,000,000
HOSWAP	Yield Farming	11,000,000
HOP2P		
HOFP2P		
HOSTK		
HOFE		
HOOTC		

HO is only issued via the contract. The reward is issued through the user's participation in the contract, there is no other allocation method.

4.2 HALO Genesis

To meet the early HO circulation and the construction of HOLPPOOL (HALO DAO), the HALO Network will simultaneously launch the HALO Genesis when the HALO Network is launched The Genesis Group will be the earliest HALO Network adopters. Participation in Genesis requires an ETH commitment to minted with initial total 10,000,000 HO via contract. The initial minted ratio is 1ETH:10,000HO. Early adopters of the GENESIS will witness an upside of

100 times from the initial offering. The cost of each successful minted 1000 HO coins will increase by 0.00001ETH, the 10,000,000th HO will upside of 100 times from initial offering. Each 2000 HO will be destroyed if no tokens minted every 60 minutes after the Genesis event launched and the timer will restart after destruction. The theoretical Genesis period is between 1 day to 208 Days. Committed ETH obtained from the Genesis event will support the early stability of HALO by being sent into HOLPPOOL (HALO DAO). HOLPPOOL (HALO DAO) supports the early liquidity of HOUSD, HOSWAP, HOP2P, HOFP2P, HOSTK, HOFE and HOOTC and the theoretic loss of HOUSD, HOSTK and HOFE contract.

For Example:

The 0th to 1000th HO are worth 0.0001 ETH each, The 1001-2000th HO is 0.000101ETH each, The cost of ETH will increase by 0.000001 when every 1000 HO staked or destroyed. By analogy, the minting cost of the last 1000 HO is 10.099ETH:1000HO.

4.3 Node Reward

There is no reward for node production blocks before the HALO Network starts the node election. HALO Labs will initiate the first community proposal-the block reward adjustment proposal before the node election starts. The content of the proposal is to modify the block reward to 3. 00342857HO.The proposal will pass if more than 67% of votes cast each time. If the proposal is not passed, the block reward will be adjusted and re-voted. If the proposal passes the HALO-NODE (Super Node), new HO will be produced. It is expected that HALO-NODE in the first year (Super node) will get about 2.1 million HO.

5. Conclusion

HALO Network is designed and developed based on comprehensive experience that has been universally proven over a long period of time. It is an improved (Incremental) optimization of the existing public chain architecture. It proposes a dual transaction model of HMM and AMM with more liquidity support, a cross-chain middleware HALO Bridge driven by smart contracts and HPOS Consensus for large-scale DEFI application, aiming to provide a secure, reliable, infinitely scalable and agile iterative ecosystem for the blooming DEFI.HALO Network represents the fundamental progress of blockchain technology in decentralized finance, and it is a part of expandable global blockchain system. HALO Network represents the innovation and progress of blockchain technology in the decentralized financial vertical field.