EVANESCO

Whitepaper

Ver 0.8

INTRODUCTION

Evanesco is based on Polkadot ecology, committed to building the next generation of decentralized new privacy financial ecology protocol family in a fair and reliable way. Relying on the underlying secure privacy network, mainstream cross chain adaptation mechanism, powerful privacy transaction engine and standardized privacy exchange as a service (PEX as a Service), it can build a more equitable ecology network of privacy finance.

The open, transparent and difficult-to-tamper characteristics of the block chain have accelerated the emergence of modern decentralized finance, but in some fields these characteristics are not suitable for the development of financial activities, such as transaction information of large encrypted currency. Whether it is in the cryptocurrency or the traditional financial field, it is very sensitive to the transfer of large-value assets. The transfer information of top Exchange`s address can even affect the market direction. For both parties, it is more hoped that the key transaction amount can be concealed. The privacy transaction process reduces the impact on the market.

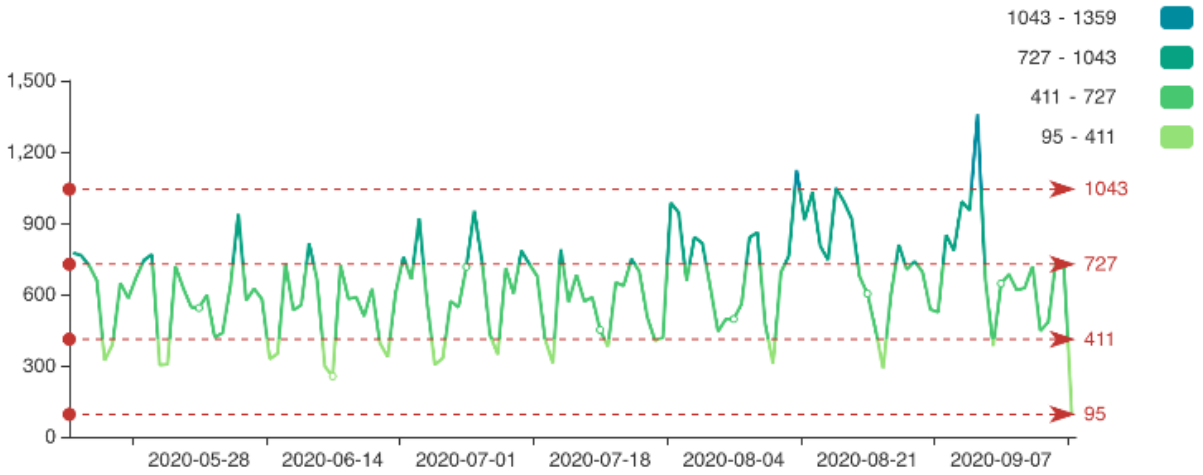

Fig.1 BTC Whale Trading Monitoring Data (TokenView)

The OTC centralized platform will also involve people's physical information. The transaction information of the counterparty can be obtained by analyzing each transaction on the chain of stablecoin and the OTC display information in the same period. It is necessary, in a complete financial ecology, to block the transfer of assets on this chain through private transactions to protect OTC information of both parties to the transaction.

Problems such as insufficient liquidity, traceability of transactions and visibility of account book owners during decentralized transactions exist in most standard and non- fungible assets in the current encryption ecology. A complete decentralized financial network must has a privacy layer. Users are concerned about income risks and account transaction privacy the most in using any finance-related application. Especially when DeFi leads modern finance, the privacy layer, will be an item of standard configuration.

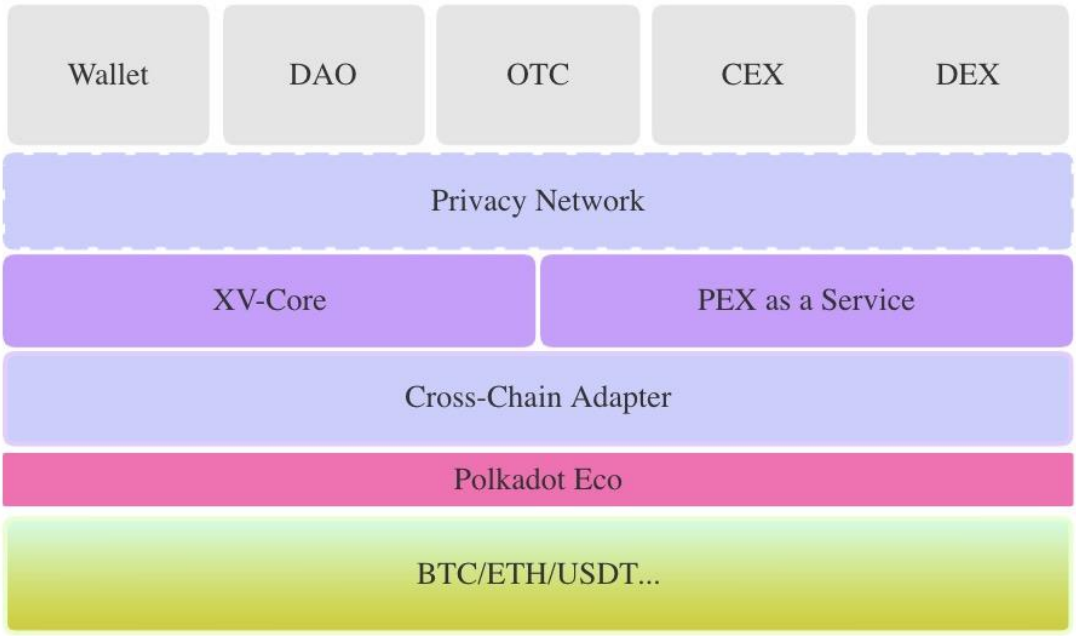

Fig.2 Evanesco Model

Evanesco's vision is to build the next generation of financial ecology in a fair and reliable way. Based on privacy network and privacy transaction

technology, it will be committed to breaking through the protocol stacks of public chains, private transaction and DeFi, breaking the liquidity boundary of encrypted assets, and building a robust DeFi operation platform. With the private P2P network, friendly and standardized trading interfaces will be provided for various encryption ecological access, and the privacy transaction liquidity be shared with Polkadot ecosystem, other public chains, exchanges, wallets, OTC, DAO and other encryption ecology.

Content

WHY POLKADOT?

Technical Potential

Polkadot's architecture separates state storage and calculation, and achieves the final results through relay chain. Parallel chain can be refined and customized for different scenes, the most suitable consensus algorithm can be selected according to the characteristics of the project itself, which can be independently formed into a chain, so that the imagination can be fully utilized in the application, and no technical limitations.The inherent cross-chain characteristics make Polkadot ecology naturally prepared for interconnection, allowing professional chains to engage in professional businesses, while offering access to traffic to other parallel chains. However, the financial ecology that best fits the block chain technology requires multi-party cooperation. EVA expects to rely on Polkadot 's strong ecological potential to bring privacy economic liquidity to all aspects of the ecology. It is also prospected that through Polkadot 's friendly chain governance mode, it will automatically upgrade itself iteratively on the chain, improve decentralized governance, and realize a fairer and more reliable ecological vision.

Combination with DOT

Evanesco, as a separate public chain, set up a private communication network to start POW mining in its early days. When the consensus node of PoS layer starts to operate, it becomes a parallel chain of Polkadot.

Evanesco Parallel Consensus will use Polkadot`s algorithm in the PoS layer of GPOW, Masses of validation members will be introduced into the pledge layer of GPOW to take part in transaction verification, docking with relay chain and cross-chain communication. The pledge of the initial PoS layer is EVA, and a certain proportion of DOT pledge will be accepted after accessing the Polkadot, thereby introducing community liquidity to develop together with the entire Polkadot ecology.

TECHNICAL FRAMEWORK

Evanesco is based on the privacy layered network, and protects the privacy of users' asset behaviors by constructing privacy assets and privacy transactions. The security of distributed ledger depends on the powerful parallel consensus system of PoW + PoS, and private transactions need more support of basic hash rate. Therefore, it is fairer and more consistent with ecological expansion to distribute new token assets according to hash rate. The PoS pledge consensus layer based on Polkadot supports EVA and DOT and introduce Polkadot ecology, so that the community can take a larger part in the project, form a joint force, and move forward together iteratively. At the bottom of the technology, privacy protection is introduced into the intelligent contract platform by expanding the bottom privacy transaction module of the virtual machine, making full use of the extensive and rich ecological communities already formed by other public chains, incorporating high-quality projects and carrying out privacy transformation to serve Polkadot ecology.

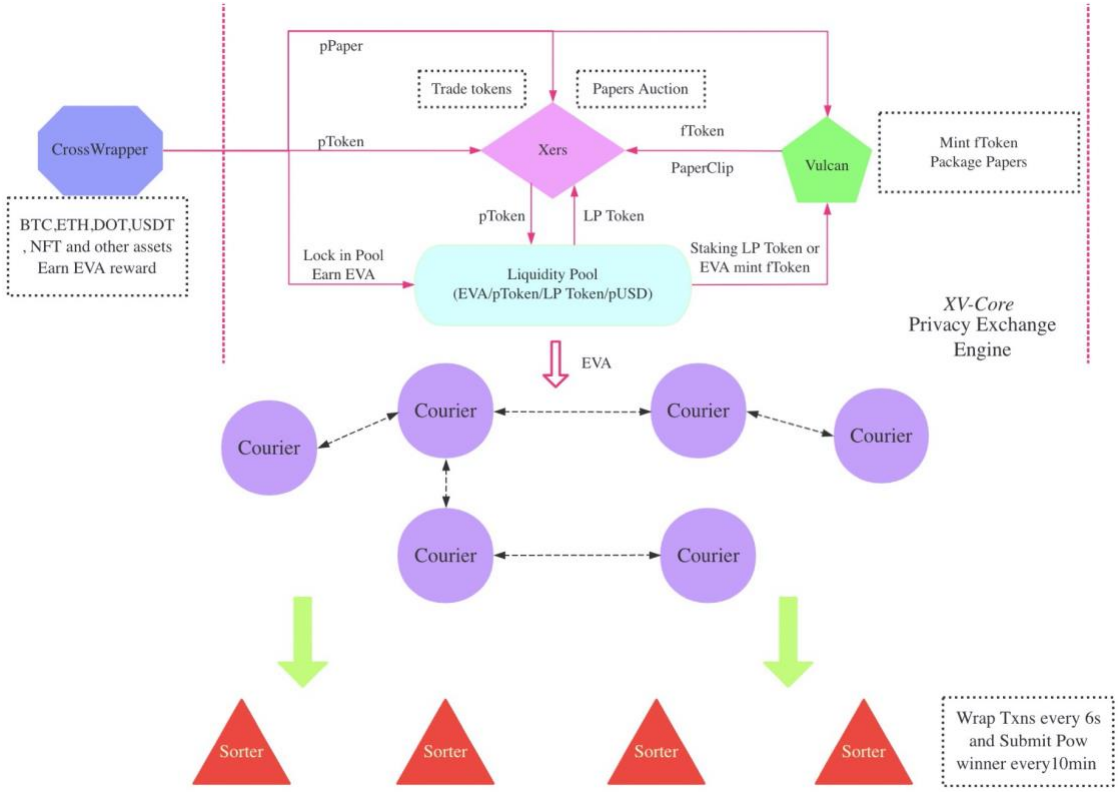

Fig.3 Operation Mechanism of Evanesco Economy

Role

- **Service user**: Users of the whole financial ecology can be ordinary individuals who use token in various trading markets, OTC dealers, CEX and DEX operators, DAO and other entities that require private trading, asset synthesis, DEFI and other functions.

- **CrossWrapper**: To adapt to various cross-chain frameworks, package and relay cross-chain asset transactions, extend PEX services to the outside, and earn token according to services.

- **Sorter**:To be responsible for verifying private transactions, packing transactions within 6-second intervals for quick block generation,

selecting the correct POW block-generating person and earning coin casting sharing.

- **Courier**: It is the core component of XV-Core to provide network services such as transaction or data distribution, collection and block generation required by users in Evanesco infrastructure. POW mode achieves block generation to earn revenue.

- **P-DAO**:Evanesco's unique decentralized privacy governance mechanism is a participant in the decentralized governance of overall ecological services.

Privacy Cascade Network

The bottom layer of EVA runs on the privacy layered network, providing development and privacy communication services for the entire network routing layer. Through the construction of a hierarchical decentralized P2P network, EVA combines the open PoW mining network with the privacy trading network, fairly balancing fairness and privacy security.

OPEN NETWORK

P2P network is a distributed application architecture that distributes tasks and workloads among Peers. It is a network form shaped by peer-to-peer computing model in the application layer. EVA technical team forms a P2P model for developing the network. In its function, the specific performance is as follows:

1. TCP/UDP/QUIC transmission protocols have pluggability;
2. Real-time bidirectional streaming mechanism based on QUIC/TCP and Protobuf;
3. Kademlia-based DHT node detection and discovery mechanism;
4. Node identification and signature based on Ed25519;
5. Support Gossip protocol;

Based on the fairness and optimization of network transmission efficiency. Mining network will be established in open network and will be transmitted through a private network when submitting transactions to verifiers. Miners can also generate blocks through private network broadcast, but the influence of network delay and node size on the verifier's selection of block-generator should be considered.

PRIVACY NETWORK

Privacy network is responsible for the transmission of private transactions or the routing of special data in EVA network. By deeply combining the basic P2P model in the development network with the classical network privacy protocols TOR and I2p, the location information of both parties to the transaction is hidden without exposing the information.

Onion routing is implemented by encrypting the application layer of the communication protocol stack, and the nesting mode is similar to onion layer by layer. TOR encrypts the data, including the target IP of the next node, many times and passes it on a virtual route composed of randomly selected TOR relays. Each TOR relay decrypts only enough packets to identify which relay the data comes from and send it to the next relay. The relay then

repackages the data and broadcasts it. The last relay node decrypts the innermost encryption and sends the original data, but is not aware of the source IP address. When a user connects to the TOR network, their network traffic will pass through multiple global servers, each of which will delete the information of the previous server, so that the last exiting node will not know where the network originates.

I2P adopts a one-way tunnel to communicate. In I2P, there are two channels between the client and the server. The data directions of the channels are from the client to the server and from the server to the client respectively. According to the characteristics that Tor directory server addresses are prone to be attacked and centralized, I2P organizes all qualified nodes as per Kademlia algorithm to form I2P network database to share functions similar to directory servers in Tor network. Nodes present different logical distributions every day due to date changes. Client and server establish their own input tunnels and output tunnels according to the logical distribution in the communication process. As the logical distribution changes constantly, the cost of monitoring and intercepting links is extremely high.

EVA's privacy network is mainly aimed at clients sending transactions to Sorter consensus layer. The establishment steps are as follows:

1. Sorter and Carrier layer nodes will establish a normal open network to complete the block generation confirmation of PoW;
2. The nodes will establish DHT databases of their adjacent points at the network layer according to the K-bucket algorithm, and set up internal data tunnel routes, which default to 3 hops, in which each Sorter node will form routes with several Carriers;

3. After the client or Carrier node packages the private transaction, it locates the access point of data tunnel routing through DHT table and sends the transaction to the access point node;
4. Each data tunnel is established as per TOR protocol. In principle, all private transactions are transmitted from the tunnel to Sorter and broadcast at the consensus layer;
5. The tunnel has a re-planning time. If the planning time arrives and data is being transmitted, the tunnel will be re-planned after a period of delay.

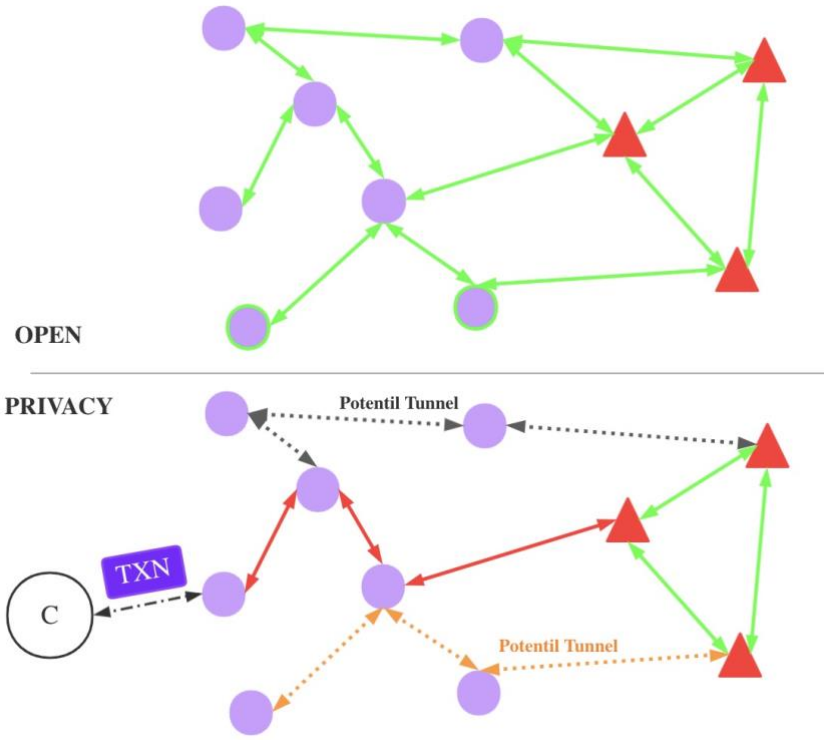

Fig.4 Two-layer Privacy Network Model

GPoW(GRANDPA over PoW)

In order to provide a decentralized, more efficient and consistent consensus system for the entire financial ecology, EVA uses GPoW

consensus algorithm to perform token generation and final consistency identification.

GPoW consensus includes two layers of consensus mechanisms, which are nested, influence each other and play different roles. GPoW algorithm not only provides almost real-time, asynchronous and safe finality similar to GRANDPA algorithm, but also can fairly distribute new tokens according to PoW, enabling a wider range of communities to go in for the construction of the whole ecology.

The basic steps of the GPoW consensus are:

1. When the whole network starts, the network miners start to run PoW algorithm and transmit data based on the privacy cascade communication protocol.
    a. In the case of transaction or routing data, public or cascaded private transmission is set based on transaction settings
    b. In the case of a PoW block, it is publicly broadcast to nearby network nodes
    c. On average, the network miner calculates a PoW block and broadcasts it every 10 minutes

2. The two-layer Sorter network packages the broadcast transactions into blocks, and determines the final consistency of the whole chain according to GRANDPA protocol.
    a. In the case of transaction data, the block-generating person is obtained according to the drawing algorithm, and the block is generated and determined as final (second level)

b. In the case of a PoW block, the most suitable block is determined according to the content of the block broadcast by the block-generating person and the finality is determined (10 minutes)

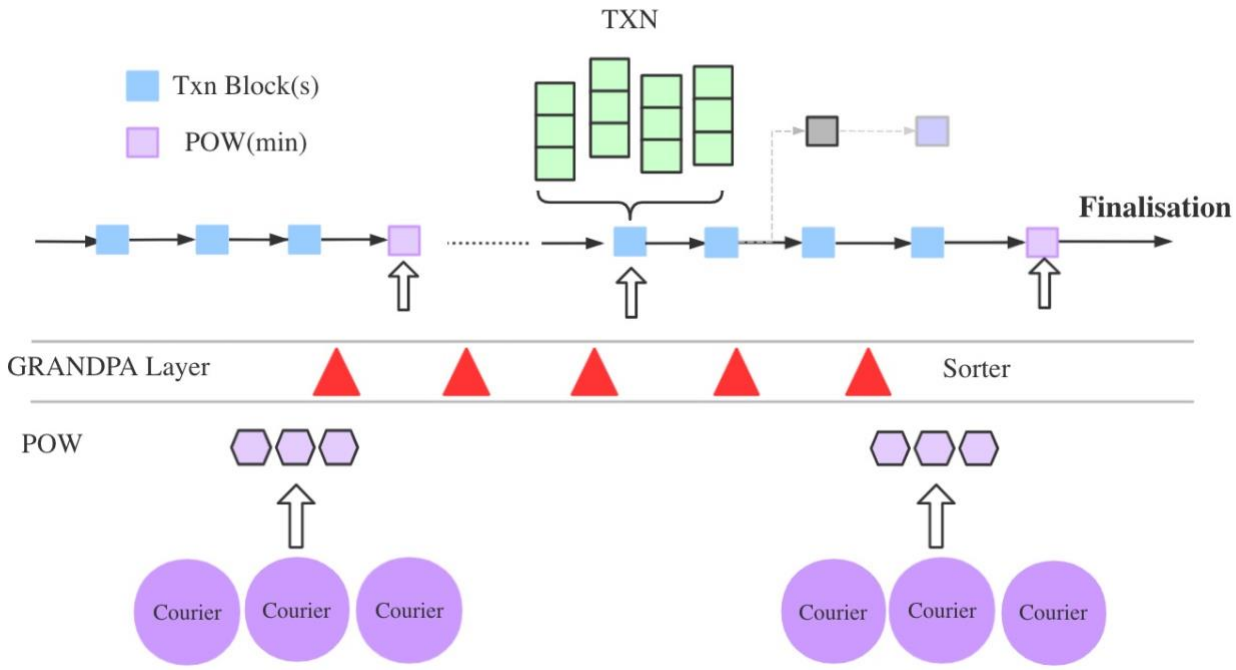

Fig.5 GPoW Parallel Nested Consensus

MINTING FAIRNESS AND CONSISTENCY CONFIRMATION

Classic encrypted currency projects such as BTC and ETH have proved that proof of work (PoW) is an excellent economic model to deal with denial of service attacks and other service abuse. It requires the initiator to perform a certain amount of operations, which of course means that it needs to consume certain time and resources. Many projects for long have adopted proof of stake (PoS) to replace PoW because of the huge consumption of resources.

However, PoW and PoS mechanisms have their own advantages from the perspective of EVA. PoW's mechanism of distributing the token

certificates generated by mining to miners makes it easy and cost-free to obtain new users to join the network. The ownership of the decision-making power of hash rate is highly related not only to economic ability, but also to the recognition of the project by the community. However, PoW also has problems such as too long time of transaction determination and chain bifurcation. As the bottom value center of financial ecology, long waiting and unexpected rollback make it difficult for the ecology to stabilize and expand. PoS ecology use pledge promises to lock in liquidity in a certain period afterwards, which is also a kind of PoW. It not only saves hash rate resources, but also has the advantages of fast block generation, fast convergence of finality and ideal global consistency. The disadvantages of PoS lie in the potential centralization risks and the inability to promise long-term efforts to contribute workload. In GPoW miner could vote for the validators, and the consensus integrated PoW's fair token distribution mode and the fast finality and final consistency of GRANDPA algorithm to realize the vision of building the next generation of financial ecology more fairly and credibly.

SELF-DRAWING BLOCK GENERATION

Before Evanesco uses GRANDPA algorithm to make final judgment, it is required to select some block-generating persons, issue Proposals to transactions and POW blocks, and then all verifiers will cast their final votes. EVA uses the Verifiable Random Function (VRF) to determine the block-generating person and priority. VRF has been applied as a mature election algorithm in many projects, such as Algorand, Filecoin, Dfinity, Cardano and so on.

Regardless of the kind of BFT consensus mechanism, Leader and Committee complete the release of blocks and make consensus resolutions.

For example, for the dPoS BFT of EOS, fixed 21 BPs take turns to serve as the Leader and Voter and Zilliqa joins the Committee through PoW to adopt PBFT consensus algorithm. These more intuitive Byzantine consensus algorithms all have a common feature, that is, everyone can see who the Leader of the next block is and which the Committee responsible for consensus is. This creates a possible risk that these block producers and Committee members are easy targets for DDOS or bribery.

In order to solve this potential EVA risk, EVA uses VRF to hide the steps of Leader Selection and GRANDPA to solve the Committee problem.

It can be simply put as follows: The general BFT selects Leader and Committee fairly and openly at the beginning of each round, while EVA discloses random numbers at the beginning of each round. Each Sorter can take his own private key to claim a prize, and the winner can become the Leader of the next round. However, no one knows who will generate the block until the block-generating person identifies himself, that is, no one can predict the next Leader.

The process of validation by the block-generating person is as follows: VRF can generate a verifiable set of pseudorandom random numbers Y and proofs ρ from the private key (S_K) and message (X). Anyone can check whether the random string is really the holder of the private key corresponding to the public key through the verification function. Since the Sorter also pledges EVA as a commitment before becoming a verifier, the amount of pledged EVA will also be considered during verification, and which nodes will be used as the block-generator and the order of block generation will be determined according to the corresponding proportion.

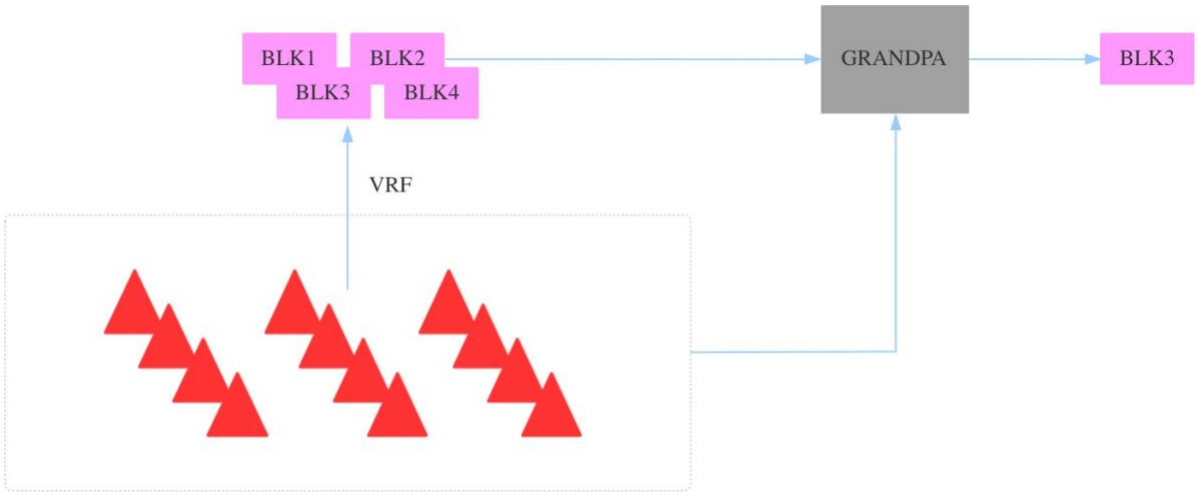

Fig.6 VRF+GRANDPA Consensus Mechanism

Polkadot adopts GRANDPA (Recursive Ancestral Prefix Protocol Based on GHOST) as the final deterministic accessory, which separates block generation from the final determination of blocks EVA utilizes a weighted GRANDPA decision-making mechanism, which means that more EVA are pledged to have a bigger say in decision-making.

CONSENSUS VOTE

Sorter's composition is not static and requires the community to vote, instead of relying on the amount of pledge.

In GPoW algorithm, Sorter node has the following two governance roles:

- Alternate node: Consensus group nodes that are not selected as consensus nodes by Carrier.
- Consensus node: The node that is voted to run VRF+GRANDPA consensus and responsible for consensus generation of block.

Alternate nodes and consensus nodes together form a large number of consensus groups.

If the node expects to participate in the consensus, it will pledge a certain EVA during the pledge period, and then initiate access request. After the qualification of the node is approved by the intelligent contract, the node is added to the candidate node list, that is, the node needs to start connecting with the existing consensus node and keep online.

During the consensus election period, PoW miners begin to vote on candidate nodes. Each PoW block can vote for several nodes, and the voting can be repeated, which is subject to the PoW block generation.

When the last PoW block is generated in the consensus election period, the PoW node is added with a re-election transaction to initiate the consensus re-election. Certain consensus nodes are selected according to the number of votes. When the number of reserved nodes is not enough, the consensus node is selected from large to small pledges in the list of candidate nodes. If nodes that are already in the consensus group expect to continue to participate in the consensus, they need to initiate access requests to the contract while maintaining the pledge.

Privacy Transaction

At present, block chain account models are roughly divided into two categories: UTXO-based and Balance-based accounts. There are a variety of block chain platforms that hide transaction amounts for UTXO-based block chain, similar to Zcash and Monero. This kind of block chain only hides the amount of each transaction and involves no concept of balance. For block chain based on the balance accounts, the Balance of each account will be updated in real time. When a transaction occurs, the amount paid cannot exceed the payer's current balance. After payment, the balance of payer and

payee is updated. However, for the block chain platform based on Balance, transactions take place, and the balances of all accounts are recorded on the block chain in clear text.

THEORY

Evanesco has implemented the balance hiding technology based on Balance account by constructing scope proof, and introduced zero knowledge proof technology into the intelligent contract system, which allows transactions between open accounts and private accounts, and transfer and audit between different accounts. Even if the network miners decrypt the encrypted network layer and view the transaction data Payload, the specific transaction information cannot be decrypted due to the private transaction agreement.

Open accounts are also called OAC in EVA. All transactions constructed by OAC are public. Privacy accounts are called PAC. Transactions constructed by PAC are private. Only the payee can get to know the payment amount, but they shall be verified by intelligent contracts.

- PAC holds the user's balance commitment. During each payment, the payer forms a commitment of the payment amount, then deletes the commitment of the payment amount from the payer's balance commitment and adds the commitment of the payment amount to the payee's balance commitment. What is always recorded in the transaction is the commitment of the balance and the commitment of the payment amount, thus no balance and payment amount are exposed.
- The scope proof of the payment amount will be added to the transfer transaction to ensure that the payment amount is not negative; The

scope proof of the new balance commitment guarantees that the payment amount does not exceed its original balance.

- In order to convince the payee that the commitment of the payment amount is indeed correct, the payer uses the payee's public key to record the payment amount and the corresponding random number in the transaction in the form of ciphertext. In this way, the payee after seeing the transaction can decrypt the payment amount and the corresponding random number. As long as the commitment calculated by these two numbers is equal to the "commitment of the payment amount" recorded in the transaction, the "commitment of the payment amount" is proved to be correct, and the payee calculates his balance according to the random number.
- Through the means of aggregation commitment, point-to-point chain transactions can be carried out, and only a small amount of aggregation zero knowledge proof will be submitted, which can greatly improve the business carrying capacity and reduce friction costs.

TRANSACTION PROCESS

The following is a brief illustration of the transaction process using an example of OAC transfer to PAC account:

ID_1 stands for OAC, and $\overline{ID}_2$ for PAC. ID_1 pays $\overline{ID}_2$ in private way $\overline{a}_1^b$

Input: a_1^{old} , $\overline{a}_1^b$, $ID_1, \overline{ID}_2$, $\overline{CM}_2^{old}$, $\overline{pk}_2$

(a_1^{old} is the public balance before payment by ID_1 ; $\overline{a}_1^b$ is the amount to be paid in private way; $\overline{CM}_2^{old}$ is the commitment of $\overline{ID}_2$ to pay the previous balance; $\overline{pk}_2$ is the public key of $\overline{ID}_2$)

Select random number $\overline{r}_1^b$, calculate $\overline{CM}_{\overline{r}_1^b} = \overline{r}_1^b H$, and generate zero knowledge proof $\pi^{zk}_{CM_{\overline{r}_1^b}}$ of $\overline{CM}_{\overline{r}_1^b}$ on H discrete logarithm. Calculate $\overline{CM}_1^b = \overline{a}_1^b G + \overline{r}_1^b H$, $\overline{CM}_2^{new} = \overline{CM}_2^{old} + \overline{CM}_1^b$

The public key $\overline{pk}_2$ of $\overline{ID}_2$ is used to encrypt $\overline{r}_1^b$ to get $c = Enc_{\overline{pk}_2}(\overline{r}_1^b)$

Calculate $a_1^{new} = a_1^{old} - \overline{a}_1^b$

Output Tx ={ $a_1^{new}, \overline{a}_1^b, \overline{CM}_1^b, \overline{CM}_{\overline{r}_1^b}, \pi^{zk}_{CM_{\overline{r}_1^b}}, \overline{CM}_2^{new}, \mathrm{ID}_1, \overline{ID}_2$ }

Validator audits Tx as follows：

Input: Tx, $a_1^{old}, \overline{CM}_2^{old}$ makes the following judgment:

（1）$\overline{CM}_1^b = \overline{a}_1^b G + \overline{CM}_{\overline{r}_1^b}$ can be judged using $\overline{a}_1^b$

（2）Is $\pi^{zk}_{CM_{\overline{r}_1^b}}$ valid?

（3）$a_1^{old} = a_1^{new} - \overline{a}_1^b$?

（4）$\overline{CM}_2^{new} = \overline{CM}_2^{old} + \overline{CM}_1^b$?

If all the above judgments are correct, Tx goes on-chain.

Encryption Economy

With an eye to realize Evanesco's long-term goals, Evanesco's network ecology will be composed of different roles, including core network clusters, asset mapping, private transactions, asset synthesis and other functions. Evanesco's economic model also designs incentive and punishment measures for various ecological services and realizes decentralized governance mode. Evanesco boasts a fairer decentralized financial ecological model, which arranges a more sound infrastructure and richer ecological driving force for the next generation of financial ecology.

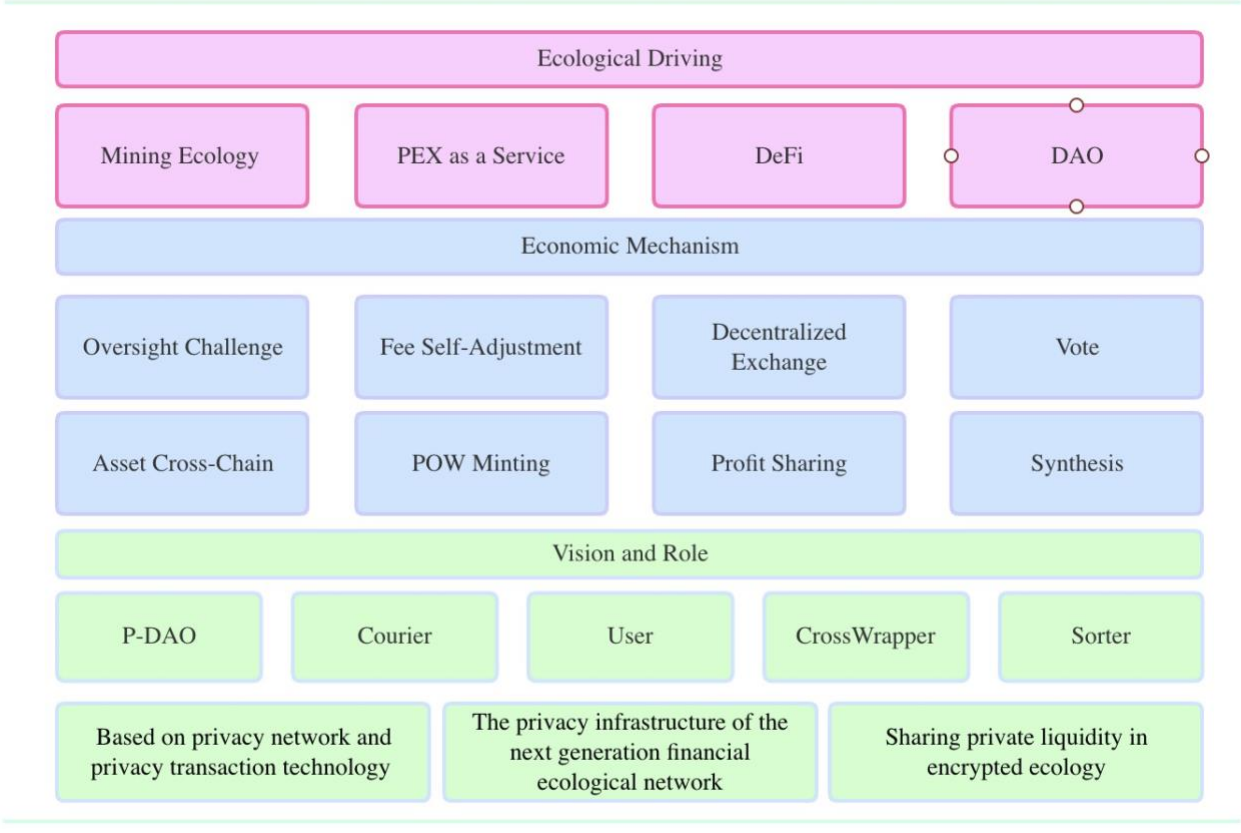

Fig.7 Evanesco Encryption Economy Framework

Financial Ecology

With a view to construct a fairer and more decentralized full-privacy financial transaction network, Evanesco has embraced the concept of cross-chain gateway and privacy transaction engine. Intending to expand the community ecology, the privacy transaction engine runs on the network mining machine Courier as a core component, completes the bottom-level transaction confirmation including decentralized transaction and asset synthesis transaction, and earns block generation rewards and handling fees.

ASSET CROSS-CHAIN

Evanesco will not develop its own cross-chain scheme, but will be compatible with and adapt to the existing cross-chain mechanism under the Polkadot ecology. We believe that this will reduce the development difficulty and cycle, make better use of the Polkadot ecology and cut the homogenization of the project. For example, WBTC on Ethernet network is accepted as standard BTC asset mapping. BTC, ETH and USDT will be used as cross-chain assets in the initial stage of the project, and selected as cross-chain assets in the later stage by EVA holders.

CrossWrapper is responsible for the cross-chain adaptation layer, mapping the external link token to pToken, or mapping the Ethernet NFT asset to pPaper. Cross-chain behavior will create EVA handling fee for CrossWrapper.

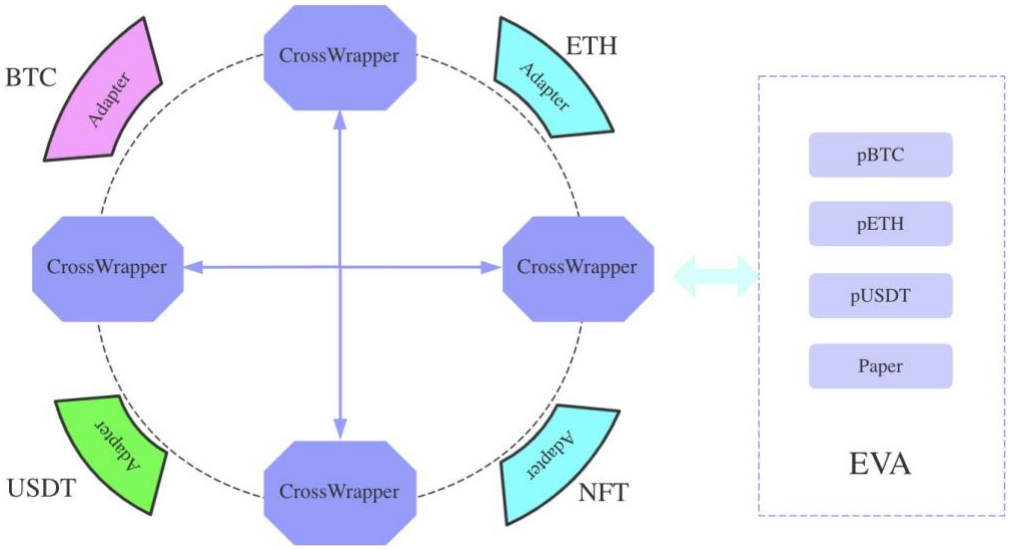

Fig.8 CrossWrapper Adaptation Layer

Each cross-link routing adaptation is completed by several or dozens of nodes that pledge EVA in intelligent contracts. These nodes have the power to supervise evil behavior of other nodes.

DECENTRALIZED EXCHANGE

The Xers module is responsible for asset exchange, starting with pToken, LP Token and EVA as the main trading pairs. pToken can participate in Xer transactions, lock in or provide liquidity, and obtain transaction fees of EVA and LP Token. Xers is also responsible for the auction and deal making of pPaper and synthesis bill PaperClip.

Fig.9 Xers Cluster Architecture

Xers is not a DEX, but a set of DEXs formed to implement business. These DEXs implement different functions and render interfaces for other DEXs to retrieve data. At the beginning of the project, asset transaction Xer and PAPER auction Xer will be run. PaperClip, which is partially packaged with pToken or LP Token, will compare prices from the asset Xer to make an asset value estimate. The price control index of a package of tokens is also adjusted by reading asset Xer and externally linked Oracle data.

ASSET SYNTHESIS

LPToken and EVA can be pledged into the asset synthesis engine Vulcan to synthesize fToken, such as a stable currency, or using a prophecy machine to track external assets, or synthetic gold, which will provide liquidity to Xers.

fToken's borrowing fees will be 100% returned to the pledger, and Sorter and CrossWrapper's service mortgage EVA in Vulcan is synthesized into fToken, so Sorter and CrossWrapper will also receive borrowing income.

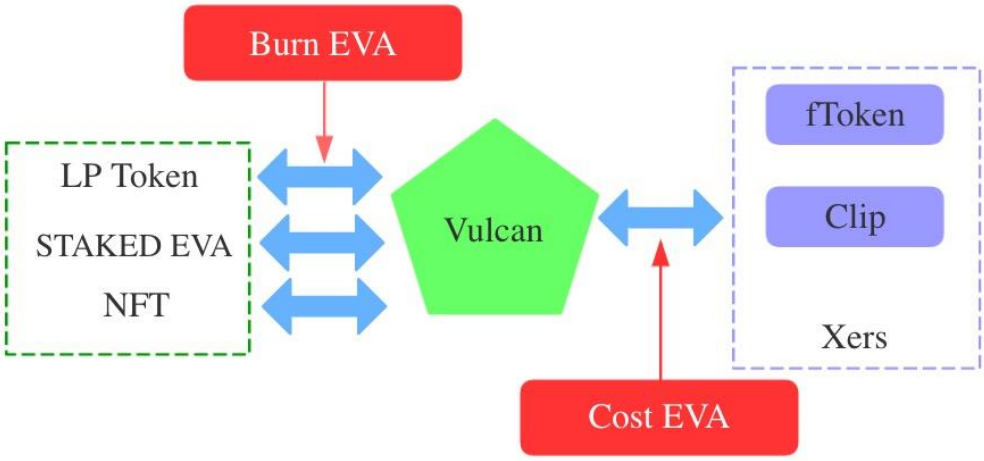

Fig.10 Vulcan Asset Synthesis Mechanism

Since a certain proportion of EVA will be consumed in each asset synthesis process, the holders of EVA across the network share the liquidity locking reward brought by destroying these EVA. Cross-chain pPaper can also synthesize PaperClip through Vulcan and join Xer for auction and other transactions. Synthesizing and dismantling PaperClip requires consumption of EVA.

Economic models

MINTING AND TRANSACTION FEE

EVA is a network-wide governance token and also a transaction fee token. 85% of the total amount is generated by miner Courier's mining. Courier is responsible for the verification and private routing of the transaction, and can obtain POW coin casting reward and transaction fee sharing.

EVA consumption scenarios include miners' verification transactions, private routing, cross-chain entrustment fees, liquidity locking and various asset synthesis actions.Be a Sorter or CrossWrapper requires pledging EVA as service collateral.

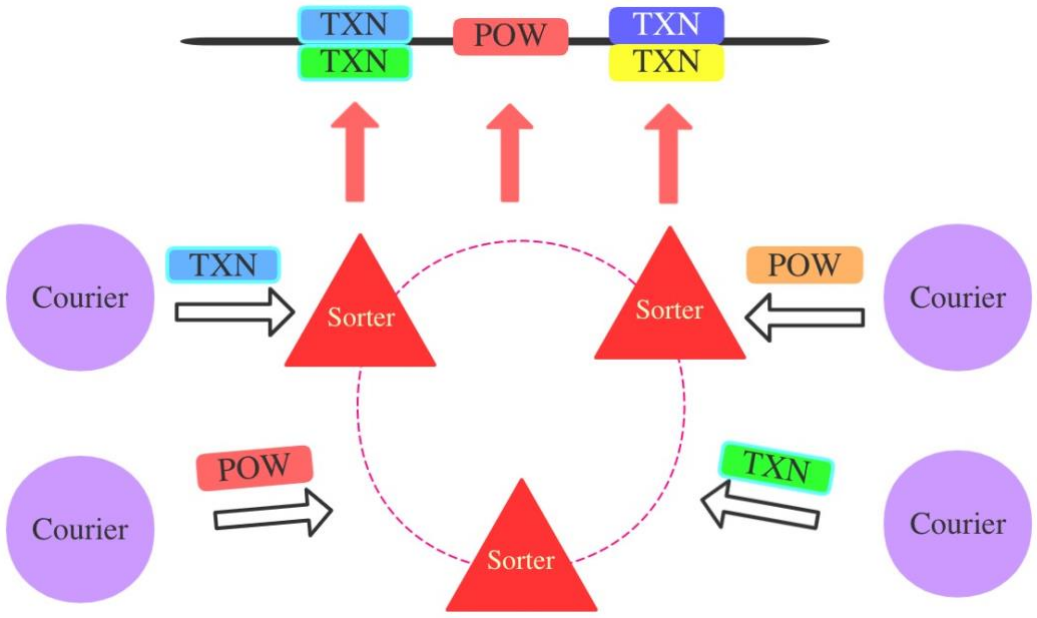

Fig.11 POW+POS Mixed Block Generation Mechanism

Sorter packages the whole network transaction every 6s and broadcasts to earn the transaction fee sharing, and submits to the POW winner for block generation and earns the POW coin casting sharing every 10 minutes.

All kinds of behaviors in Evanesco ecology require payment of friction fees and transaction fees. The roles involved in ecological operation can get corresponding transaction fee sharing.

- Privacy transaction fees will be transferred to all routing Carriers and Sorters.
- Xer Asset transaction fee, PAPER auction fee and PAPER view fee will be obtained by LP liquidity provider based on shares.

- The cross-chain adaptation fee is transferred to the CrossWrapper node that executes the service.
- a certain proportion of EVA will be burned in each asset synthesis process.

NETWORK FEE SELF-ADJUSTMENT

As a means to decouple the strong correlation between token price changes and system friction fees in encryption economy ecology, Evanesco has set up a full-network rate self-adjustment algorithm.

The system fee have an intermediary consumption standard (ICS) in each consumption scenarios, and each ICS corresponds to an automatically floating EVA rate. For example, if the transaction fee is 10ICS, it corresponds to ICS=0.00001 EVA in default. EVA and package token index are counted and ICS is adjusted in the sliding window. If the package token index rises, ICS will fall.

The calculation formula of the package token index is similar to the following formula, and the specific parameters would be announced after precise calculation.

1. Assume that *υ*BTC(i) is used to represent the EVA/BTC transaction consideration at time i, i.e.:

$$\upsilon BTC(i) = \frac{EVA(i)}{BTC(i)}$$

2. Then the package token index at time i is:

$$f(i) = a * \upsilon BTC(i) + b * \upsilon ETH(i) + c * \upsilon DOT(i) + d * \upsilon USDT(i)$$

Where a, b, c and d are adjustment coefficients.

3. The rate of ICS is the ratio relationship between f(i-1) and f(i):

$$\lambda(i) = \frac{a * vBTC(i-1) + b * vETH(i-1) + c * vDOT(i-1) + d * vUSDT(i-1)}{a * vBTC(i) + b * vETH(i) + c * vDOT(i) + d * vUSDT(i)}$$

For example, if the package token index rises by 10% in the 14-day sliding window, ICS will reduce by about 9%, reducing the cost of system friction. If f(i) falls by 10% within the statistical time, ICS will rise by 11.1%, increasing subsidies for ecological roles.

The absolute value of ICS, adjustment coefficient and even adjustment formula can be modified by DAO voting.

Governance

OVERSIGHT CHALLENGE

The behaviors of all roles will be under the supervision of similar roles in Evanesco ecology. If any evil behavior is found, other roles will launch fraud challenges and submit the evil behavior to the chain arbitration together with environmental variables. If the evil behavior is confirmed, the roles will temporarily or permanently lose the rights and interests of ecological participation.

If any Carrier submits the transaction without performing more than three hops of routing actions as required by the protocol, his account number will be prohibited from participating in the transaction for a period of time, and other Carriers will be disconnected from the node because they cannot normally route the transaction.

Another example is that if the cross-chain node intentionally exceeds the normal lock time without releasing pToken or broadcasts illegal

messages during adaptation, the pledged EVA will be deducted and kicked out of the CrossWrapper cluster.

VOTE

Holding or mortgaging EVA or DOT allows participation in voting on Evanesco governance. It includes but not limited to the following:

- Future cross-chain asset expansion;
- Courier and Sorter's transaction fee sharing proportion;
- Xers partial privacy disclosure;
- Transaction and auction rates;
- Selection of asset synthesis trading pairs;
- Modification of synthesis parameters;
- ICS adjustment and package token index adjustment
- Voting on technology development proposals

In the future, we will also explore the establishment of a private crowdfunding incubation DAO to incubate Polkadot ecological projects in a decentralized way.

Ecological Scenarios

As the new financial ecological protocol, EVA has four ecological driving forces:

- Mining
- PEX as a Service
- DeFi
- DAO

EVA's four ecological driving forces are not independent to promote community development but through integration and innovation, showing the advantages of hash power, community, decentralized finance and DAO in the following aggregation scenarios:

Full Privacy Lending Market

By transferring external assets across the chain into EVA and synthesizing special assets for decentralized lending business, users who inject liquidity can obtain the same income as their injected asset shares, without exposing the quantity and source of pledged assets. Moreover, users in Vulcan cannot spy on each other's assets. Privacy contracts verify various lending activities while ensuring the consistency of global asset data.

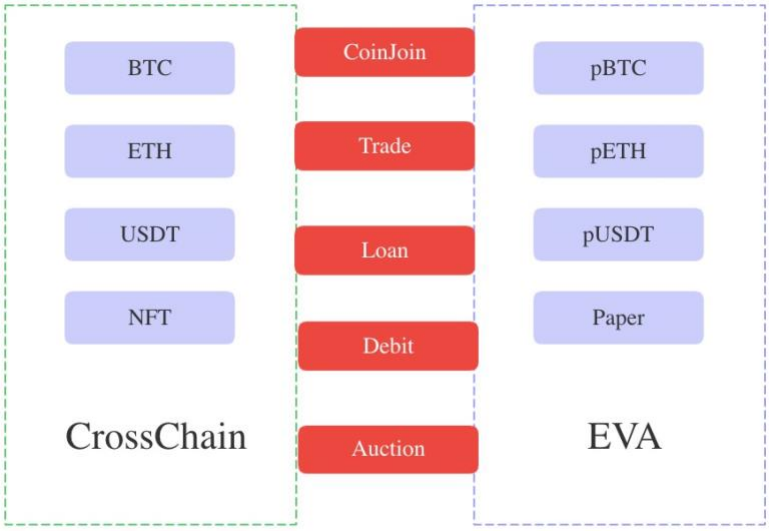

Fig.12 EVA Privacy Financial Markets

Hash Rate Capitalized Privacy Trading Market

Carrier, as the main role of the privacy transaction engine and the generation of token certificates, is the most important role in EVA. The safe, stable and efficient ecological circulation of the network involves a large number of POW mining machines to participate. And a large amount of EVA will be mined by miners, including all the assets of the foundation and EGC in the later period. Therefore, miners have a great say in the community.

We could takes the average hash rate in the past 14 days as the evaluation standard, and NFT bills with hash rate are replaced in combination with electricity and network costs, which are traded or circulated in DEX. In the course of the transaction, NFT holders receive most of the resulting block generation rewards.

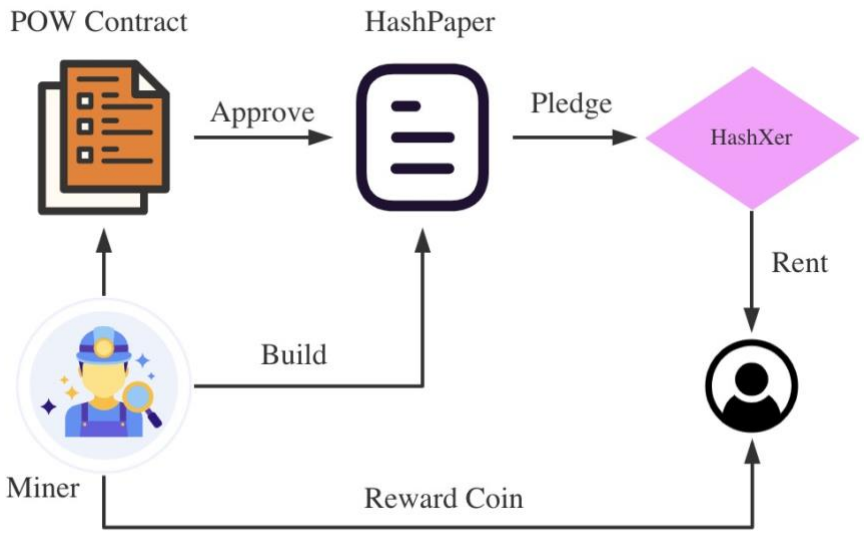

Fig.13 EVA Hash Rate Capitalization Market

PEX Value-Added Service Provider

Evanesco endows privacy liquidity to OTC, wallet, exchange and aggregated trading services. The conversion, diversion and collection of interface-based encrypted asset liquidity lead to the intelligent service of private transactions. Evanesco will not involve the community ecology of OTC, wallet, exchange and various aggregated trading service providers, but only provide the link service between the application layer and the infrastructure layer. The service will also be provided by many community nodes to maximize the ecological benefits.

Privacy exchange value added service providers can aggregate privacy liquidity in EVA and provide users with transaction combinations in multiple encrypted currencies, multiple channels and multiple delays by linking wallets, OTC market makers, CEX, etc.

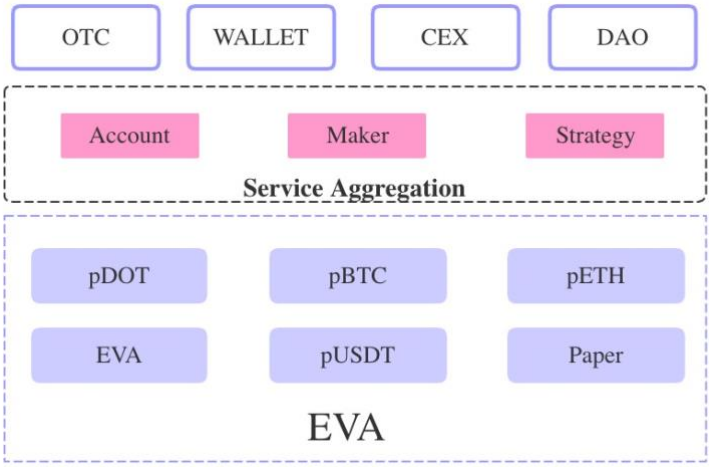

Fig.14 PEX Value Added Services

DAO Privacy Crowdfunding Incubation DAO

EVA can pool the strength of the community, transform cross-chain assets, EVA, synthetic assets, etc. through privacy pledge agreements, The DAO would incentives for the early incubation of Polkadot related projects. These projects for incubation are selected through the community, and screened and guaranteed by the community members. If the incubation is successful, the community members will receive a certain proportion of project incentives. All DAO members will receive the project incubation income in proportion.