Abstract

This paper presents a new blockchain protocol called Troy Network, a non-custodial and decentralized protocol for global trading and settlement, aiming to build the infrastructure of the decentralized finance (DeFi) ecosystem in blockchain industry, by combining Layer 1 and Layer 2 technologies. Troy Network is an infrastructural protocol for the trading and settlement of crypto-assets (including but not limited to BTC, ETH, EOS), which inherited the advanced features of high security from public blockchain and high speed, high frequency, high privacy from the state channel technologies. It acts as the prime broker for the member exchanges to access the liquidity of the other participating mainstream exchanges (both centralized and decentralized) and merchant nodes in the network, providing customers (such as institutional investors and high-net-worth clients) with one-stop and full-stack brokerage services including but not limited to deal-making, margin trading, asset management, data analytics services and other value-added services, etc.

Troy Network will implement the function of exchange and payment of cross-chain crypto assets in the near future as the technology of cross-chain protocol (COS-MOS or Polkadot, etc.) or cross-chain state channel technology evolves into a more mature level.
1. Background

1.1 A New Era of Crypto-assets

It has been more than a decade since the birth of Bitcoin launched a new era. During the decade from 2008, Bitcoin community has gradually grown from the crypto geek circles to the global mainstream society. Meanwhile, the price of bitcoin has risen as time flies, from the time when 10,000 bitcoins can only buy two 25-dollar pizzas to the time that price hit the peak of $20,000 per bitcoin during 2017-2018. Back then, Warren Buffett has publicly claimed bitcoin as “rat poison”, but now the founder of Tesla, Elon Musk, has support for bitcoin on Twitter. After years of up and down, bitcoin has become the world’s first globally recognized decentralized cryptocurrency which has been in stable and safe operation for more than 10 years.

There have been many disputes about cryptocurrencies along the way. Typical example, mainland China has completely banned the Initial Coin Offering, along with all the trading and brokerage of cryptocurrencies within the country. However, crypto-assets, represented by bitcoin, have shown increasingly robust vitality and growing influence across the world. Since 2018, the mainstream society has finally begun to embrace the crypto industry. Bitcoin futures exchange Bakkt, subjected to the ICE from the United States has successfully raised more than 180 million dollars in the bear market and currently the futures exchange LedgerX has been approved of the spot currency settlement of bitcoin futures contracts. The crypto-assets trust funds Grayscale is managing more than 220,000 BTC, and JPMorgan has launched their JPM Coin as a settlement tool internally. Facebook also launched its financial platform Libra (includes stablecoin a kind of stablecoin backed by a package of low volatility assets and stable fiat currency). Crypto-assets are stepping into the mainstream of society, from the shadow of the world to the center of the stage.

1.2 The Trading Ecosystem of the Crypto-assets

In the current stage of blockchain development, as most of the blockchain projects are still searching for application scenarios or in the slow infrastructural construction, trading is the center of circulation for crypto assets. In the circulation ecosystem of crypto-assets, the primary market can hardly form a large-scale trading market due to the lack of liquidity, thus the secondary market is the core of the trading ecosystem. Generally, exchanges can be roughly divided into centralized exchanges and decentralized exchanges according to their features.

Among crypto exchanges, centralized exchanges integrate trading, custody and settlement, providing users with good user experiences (excellent trading depth, trading speed, advanced trading tools etc.), therefore centralized exchange is more popular among regular users. However, according to the data from CoinMarketCap, currently there are more than 2,600 cryptocurrency assets in the world. In fact, Etherscan data shows that the number of token contracts on Ethereum is close to 30,000, which corresponds to the large
number of exchanges and trading pairs to serve. According to incomplete media statistics, there are more than 10,000 cryptocurrency exchanges in the world and most of them are centralized exchanges. However, centralized exchanges have been criticized for their opacity and centralization:

1) Fake Trading Volume
Centralized exchanges often falsify and wash trading data to fill liquidity traps and lure users to trade, often resulting in losses of users’ assets.

2) Opacity and Centralization
Centralized exchanges have all the access and rights to the data of the trading happening on their platforms, so that they can maliciously abuse their privileges to create numerous profit opportunities thanks to their God perspective. So some exchanges will be a referee as well as a sportsman in the same game and harvest the retail traders by various illegal methods, such as illegally issuing extra tokens, carrying out insider trading or manipulating the price.

3) Ignorance of Security Management
There are too many risk exposure in the centralized exchange, such as the closed-source code, the asset custody process that too many people get involved in. These processes are often opaque and centralized, which is easy to cause a lot of security bugs. Taking the famous “Mt. Gox” as an example, 850,000 bitcoins were stolen from Mt. Gox and then the exchange broke down in 2014, casting a shadow over the whole crypto industry. But in the end, most of the stolen bitcoins were stolen by their own staffs rather than getting hacked by outsiders.

Considering the disadvantages of centralized Exchange, Decentralized Exchange (DEX) won the appreciation, thanks to the decentralized and open characteristics. DEX aims to build a decentralized blockchain platform to remove middlemen and provide users with a point-to-point trading experience directly. DEX will be evolved into an open brokers commercial model in the future. In contrast to CEX (Centralized Exchange), DEX is rooted in the excellent features of blockchain, which has the following advantages:

1) Privacy Protection
One of the main benefits of DEX is privacy and anonymity. In DEX, transaction and account control was achieved by cryptography technology (the public and private key pairs) and there is no need to complete KYC for users who want to trade in DEX, in contrast that most centralized exchange always force the users to do KYC and AML before trading. In DEX, users only need to sign up to get the username and password (not necessary), then import the existing wallet or create a new wallet on blockchain. After that, they can begin to trade and get a global 24/7/365 service. This feature provides a perfect trading platform for users who value privacy and want to remain anonymous.

2) Censorship-resistance
Since there is no centralized entity to monitor trading and order execution in DEX, this mechanism will ensure that it is more resistant to censorship and can effectively prevent centralized attacks by hackers. In addition, it can also prevent malicious shutdown and censorship of exchanges by authorities.
3) Security

Although the safety level of DEXs is different, unlike CEX, the attack from hackers cannot focus on all the on-chain non-custodial wallets to steal users' money, so DEX can provide better security for users. In addition, DEX uses a decentralized settlement mode, which greatly reduces the possibility of hackers using the settlement process to attack. Users can also use escrow programs to ensure that funds are fully managed during the trading process. In the worst case, even if DEX stops running, users can wait for the escrow program to stop and regain control of their assets.

4) Versatility and Flexibility

In DEX, users can technically trade any asset as long as there are buy and sell orders, without exchange listing the trade pairs. This characteristic of free exchange and trade provides a broad development space for its business. For example, if the accumulated vouchers tokens cannot be used up, users can exchange them with other useful tokens automatically through DEX, or even convert them into a better liquidity crypto-currency.

5) Anti-manipulation

Centralized exchanges are often criticized by the manipulation behaviors, such as counterfeiting trading volume, closing token withdrawing, restricting trading to interfere user's trading behaviors, and even manipulating the trading market through malicious price manipulation. In a DEX, no one could control the order book, which can effectively reduce the possibility of trading manipulation.

The exploration of decentralized exchanges is not a new topic. Most mainstream exchanges, including Coinbase and Binance, have developed their own DEX. However, all the current decentralized exchanges cannot meet users' trading needs very well, nor have they gained good market acceptance. Some of the pain points of the current decentralized exchange are as follows:

1) Poor User Experience

Because DEX is the trading happening on the blockchain, its account addresses are the same as the typical public and private key used in the blockchain. The keys are lengthy, meaningless random string, which is not conducive to users' memory and preservation. In addition, the trading steps are very different from the regular financial trading habits, which causes bad user experience.

2) High Latency, Low Efficiency and Poor Scalability

DEX needs to execute on the chain when it works, so that it takes more time to call smart contracts, reach consensus and execute trading orders than a centralized exchange does. If there is a network jam, the trading speed will be further reduced or even unusable. Given the extensibility bottleneck of the current public chain, DEX is also difficult to support the trading behavior of high density and large number of users. For example, IDEX, the famous decentralized exchange, has been unable to use due to surging trading volume for many times.

3) Simple, Basic Trading Tools

So far, DEX can merely support simple pending orders, withdrawal orders and direct trading, but cannot support entrusted trading, stop-limit order, market price trading and other complex trading functions.
4) Poor Liquidity
Users are not willing to trade on DEX due to poor user experience, primitive trading tools and shallow trading depth. Additionally, due to poor scalability of the public blockchain, DEX does not support large-number high-frequency trading, which is not conducive to market makers that can provide trading depth. Furthermore, many DEX did not fully consider the incentives for market makers at the beginning of design. Therefore, trading mainly relies on the natural coincidence of trading, which leads to poor natural depth and liquidity.

5) Lack of Fiat Currency Entrance
DEX is limited to trading between crypto assets, and there is no exchange gateway between fiat currencies and crypto-currencies. So it is less attractive to users who used to trade by fiat currencies.

From the perspective of the development logic of blockchain industry, although there will be an industry pattern that centralized exchanges are the main and decentralized exchanges are the auxiliary in the short and medium term. However, with the improvement of the whole industry’s infrastructure, decentralized exchanges will certainly occupy a place in the blockchain ecosystem. But the final form of the decentralized exchange isn’t necessarily the shadow of the centralized exchange and should be a decentralized protocol layer which integrates trading (bidding and non-bidding), custody and settlement function, can be easily integrated in the Internet applications and Dapps’ backend, being able to connect centralized and decentralized exchange market and depth at the same time.
2. Project Design

2.1 Project Positioning and Design Principles

Troy Network is aiming to build a world-class financial platform based on the mature fundamental infrastructural blockchain, to serve all professional financial institutions as the most advanced crypto assets trading platform, and to provide any kind of commercial applications with full-functional trading tools, by aggregating the liquidity of all major global crypto exchanges and inheriting the advantages of DeFi financial service (decentralized, borderless, trustless).

With our deep understanding of the crypto market and rich trading experience in the past, we firmly believe that with more and more traditional financial institutions entering into the crypto market with their large scale of investment, the market capacity will be expanded aggressively. At the same time, along with the advancement of blockchain, more application scenarios will be further developed. As the market scale keeps expanding, the number of exchanges and trading markets worldwide may experience an explosive growth, institutional investors and high-net-worth users will be in need of service facilities similar to the traditional stock brokers to reduce investment costs, lower irrelevant risks and improve the efficiency of investment. On the other hand, with the landing and expansion of blockchain application ecosystem, tokens based on many vertical application scenarios is bound to need a protocol layer that can quickly find market supply and demand, realize lightning exchange and trading for merchants and users due to liquidity restrictions.
This project aims to create a decentralized global trading and settlement network protocol, which combines Layer 1 and Layer 2 technologies to meet the requirements of asset security, performance, privacy, decentralization and other characteristics, so as to create an epoch-making new digital asset protocol. This project’s ultimate goal is to provide one-stop decentralized brokerage services including deal-making, financing, asset management, data services and other value-added functions by aggregating the trading depth of mainstream exchanges (centralized and decentralized) and merchants nodes.

Therefore, the basic functions of the protocol will achieve the following design objectives:

1) Build a decentralized trading and settlement network in the mode of “application + protocol”;
2) Strengthen application layer commercial barriers (operations, resources and traffic, etc.), reducing the hard fork risks;
3) Connect and aggregate the liquidity of centralized and decentralized exchanges;
4) Break through the scalability bottleneck of the current decentralized exchanges;
5) Cross-chain interoperability, compatible with a variety of native tokens;
6) Built-in dark pool trading features, which can support the dismantling and execution of block trade.

2.2 Design Principles

1) Decoupling with underlying public chain protocol;
2) Combining Layer 1 and Layer 2 solution;
3) Implementing multi-chain interoperability;
4) Providing open interface;
5) Offering non-custodial account system.
2.3 System Framework and Basic Features

In Troy Network, the whole system architecture consists of four layers, including the public chain protocol layer, the off-chain trading layer, the settlement network layer and the application layer. The brief introduction is as below:

1) Public Chain Protocol Layer
   As the base layer of Troy Network, the public chain protocol layer will provide basic security for the assets in Troy Network. If necessary, Troy Network will develop a highly customized underlying public chain for trading. The characteristics of public chain layer are as follows:

   Robustness and Compatibility
   The Troy Network is designed to decouple with the underlying public chain to maintain the robustness and improve the compatibility of the whole system. When the underlying public chain has major upgrade or hard fork, Troy Network can easily stay compatible with the new chains. In addition, we will develop dedicated connectors for main underlying public chain protocols, such as all EVM-compatible public chains can be quickly integrated into Troy Network via the EVM public chain connector.

   Cross-chain Interoperability and Universality
   The blockchain assets in the future must have the characteristics of cross-chain interconnection. Therefore, in order to be compatible with more asset categories as much as possible, Troy Network will integrate mainstream cross-chain protocols(such as COSMOS and Polkadot) into the system, so as to effectively expand Troy Network's business ecosystem.
2) Off-chain Trading Layer

In order to improve users' trading experience and further enhance the privacy protection, Troy Network will deploy a off-chain trading protocol on the underlying public chain, which adopts Layer 2 technologies as the keystone. In the off-chain trading layer, Troy Network will actively apply the mature off-chain scalability technology to the trading process, such as state channel technology. Up to now, state channel technology is one of the most mature technologies in this field. Relying on state channel technology, it will be able to realize point-to-point rapid trading and settlement all over the world. Typical state channel technologies include bitcoin lightning channel, Raiden Network and Celer Network, etc. More importantly, state channel technology combining with data encryption technology can also open up exclusive private channels for users, thus providing high-net-worth customers and institutional investors with faster, safer and more private trading services.

3) Settlement Network Layer

Troy Network users are dispersed around the world, and the exchanges (centralized or decentralized) all over the world have different compliance requirements about the KYC and AML for trade users. Therefore, we designed our settlement layer to automatically match the most suitable settlement service providers for users and provide automatic compliance verification. The settlement service providers will be able to earn service fees by providing compliance and trading verification, which further encourages other compliant entities to join Troy Network. For non-compliant trading categories and exchanges, the layer will only carry out necessary trading verification, rather than the relatively time-consuming compliance verification.

4) Application Layer

The Application layer will provide Troy Network and trading users with rich interactive interfaces and application services (such as exchanges, data analysis, financing services, games, etc.). Trading users can only use Troy Network's trading and other value-added services through the application layer interface. Application in the application layer, can support the decentralized implementation, either can support the application of centralized function calls (through specialized trade interaction interface). The decentralization application is the keystone of the application layer, such as DEX 's plug-in can provide trading services independently, also can provide the centralized or decentralized applications with token conversion function.

2.4 Troy Trade

In Troy Network, trading is the footstone of all functions and value-added services. As a decentralized protocol for trading and settlement , in order to facilitate the implementation of the financial application protocol, we will first develop a new open broker system, Troy Trade, based on Troy Network.

Troy Trade, which combines the advantages of both centralization and decentralization modes, is the first landing application of the Troy Network protocol, and would evolve into one of the interfaces of Troy Network. Features of Troy Network are as below:
1) Non-custodial Account System
Trading will happen in the state channel, and all the states of trading will be kept off-chain. In essence, users’ assets will be custodied on the chain, protected from centralized organizations. This solution can effectively avoid the security risk caused by centralized management.

2) Decoupling with Underlying Protocols
This feature mainly refers to the functions of the exchange that decoupled with the underlying public chain protocol and matching protocol, allowing the application layer to be compatible with the multiple versions of underlying protocol (multi-version protocol before and after forking), even if the underlying protocol is forked, it will not affect the functions of the upper protocols/applications.

3) Cross-chain Interoperability
This feature mainly refers to the ability to implement cross-chain trading (assets swapping), which is realized in two ways: first, cross-chain asset exchange can be implemented through underlying cross-chain platforms, such as COSMOS or Polkadot, or through other mature cross-chain technologies, such as Atomic Swap; Secondly, the cross-chain state channel can bridge multiple chains and achieve cross-chain trading.

4) Supernodes
In Troy Network, the supernode can be classified into different types according to the services they provided. For instance, Broker-dealer supernode provides open primary broker service to match off-chain trading with high efficiency and serves as a high functional relay hub; Liquidity backer supernode provides financing services for the users of the platform; Oracle supernode provides data analysis and information support for trading users and trading system.

Troy Trade is the first applications in Troy Network. It is also the first comprehensive supernode in the network, providing customers(such as institutional investors and high-net-worth clients) with one-stop full-stack brokerage services including but not limited to deal-making, financing, asset management, data services and other value-added services, etc. Troy Trade provides three different trading modes for users: regular trading, the Bancor based trading and the lightning trading channel. Three modes share one common concept of “trade off-chain, settle on-chain”, with the specific details as follows:

1) Regular Trading
Trading can only be conducted in the listed trading pairs in the exchange. TROY(the native token of Troy Network) Trading markets will be the first to be open, and then gradually open other markets.

2) The Bancor-algorithm-based Trading
This trading mode is mainly designed for low-liquidity currencies in business activities. Merchants provide reserve tokens and realize automatic exchange or trading of tokens without the need of counterparties through smart contracts. For example, merchants issued moon cake vouchers to provide discounts in Mid-Autumn festival, but the validity period is only one week. In this case, it is unrealistic to expect the market to naturally form a mature counteroffer. So merchants can create a bancor-based trading pair to provide customers with exchange and trading services. Troy Network will provide
Consensys member Simon DE la Rouviere elaborated in an essay on Curation Markets that bonding curves exist in the following basic hypothesis:

- Users can purchase (cast) new tokens (such as A project token A) from smart contracts with designated tokens (such as ETH), and ETH will be retained as a reserve pool in smart contracts without being sent to any teams or individuals.
- The purchase price is determined by an algorithm curve, which is mainly determined by the quantity demanded for token A of the current project.
- The user can sell token A back into the public reserve pool of the smart contract (destroy the token) at any time, but the selling price is determined by the selling curve.

Under this premise, tokens will be issued entirely determined by the real demands of the market. Therefore, according to the bonding curve hypothesis, the price of tokens will increase with the increase of the supply of tokens. When defining Bancor token price and supply through the bonding curve, it is necessary to ensure that the bonding curve could be applied to any feasible function which can be easily integrated, such as power function, Sigmoid function, mixed function, etc.

Taking the most general power function as an example, the bonding curve is assumed to be:

\[ y = mx^n + b \]

Among them,

- \( Y \) is the token price;
- \( X \) is the token supply;
- \( M \) is the slope parameter;
- \( N \) is the exponential parameter;
- \( B \) is the initial price.

You can fine-tune the slope and price range of the function by fine-tuning \( m \), \( n \) and \( b \) numerically. In the actual implementation process, supposing that it is necessary to know the amount needed to pay for the purchase of \( k \) tokens when the supply has released \( a \), then the calculus area of the function in the supply interval shall be changed as follows:
Consensys member Simon DE la Rouviere elaborated in an essay on Curation Markets that bonding curves exist in the following basic hypothesis:

Users can purchase (cast) new tokens (such as A project token A) from smart contracts with designated tokens (such as ETH), and ETH will be retained as A reserve pool in smart contracts without being sent to any teams or individuals.

The purchase price is determined by an algorithm curve, which is mainly determined by the quantity demanded for token A of the current project.

The user can sell token A back into the public reserve pool of the smart contract (destroy the token) at any time, but the selling price is determined by the selling curve.

Under this premise, tokens will be issued entirely determined by the real demands of the market. Therefore, according to the bonding curve hypothesis, the price of tokens will increase with the increase of the supply of tokens. When defining Bancor token price and supply through the bonding curve, it is necessary to ensure that the bonding curve could be applied to any feasible function which can be easily integrated, such as power function, Sigmoid function, mixed function, etc.

Taking the most general power function as an example, the bonding curve is assumed to be:

\[ S = \int_a^{a+k} (m \times x^n + b) \, dx \]

\[ = \frac{m}{n+1} (a+k)^{n+1} + b(a+k) - \left[ \frac{m}{n+1} a^{n+1} + b \times a \right] \]

\[ = \frac{m}{n+1} [(a+k)^{n+1} - a^{n+1}] + b \times k \]

\[ = \frac{m}{n+1} a^{n+1} \left[ \left(1 + \frac{k}{a}\right)^{n+1} - 1 \right] + b \times k \]

When it is necessary to calculate the capital held in smart contracts, the above equation can be calculated from 0 to [a+k], as follows:

3) Lightning Trading Channel (Ring Matching)

This method of trading is suitable for quick exchange between any two tokens with sufficient trading depth and volume (initially limited to the same trading market). In order to reduce the complexity of
token trading path and the risk of market fluctuations, it is necessary to lock the orders of both trading pairs. This trading method requires the fixation of price in exchange for rapid trading (the default price error percentage should be set when trading), which may bring a certain amount of risks to the users. In order to reduce the complexity of ring matching, tokens A and B are required to have their own trading pairs with TROY respectively. The basic mechanism of ring matching is that TROY bridges between trading capitals, enabling the smooth exchange between random two tokens even if they do not have direct trading pairs between themselves.

In summary, Regular Trading mode aggregate the liquidity of mainstream exchanges (centralized and decentralized exchanges) in order to serve the trading of mainstream crypto-assets; Lightning Trading Channel mode is designed for the user who needs to quickly buy high liquid crypto-currency; The Bancor-algorithm based trading is a trading mode designed to serve the long tail market. However, it is worth mentioning that although the Bancor algorithm can provide a trading market for low-liquidity currencies, it cannot create liquidity out of thin air. In most cases, it will mainly rely on the liquidity provided by reserve tokens (such as the reserve pool provided by merchants).
2.5 Comparison between Troy Trade and Other Mainstream Exchanges

The following table compares Troy Trade with the existing exchange system, and the results are shown in the following table:

<table>
<thead>
<tr>
<th>Trading Tools</th>
<th>Cost</th>
<th>Speed</th>
<th>Trusted</th>
<th>On-chain</th>
<th>Attack-resist</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binance</td>
<td>low</td>
<td>fast</td>
<td>trusted</td>
<td>no</td>
<td>no</td>
<td>Partially yes</td>
</tr>
<tr>
<td>Coinbase</td>
<td>low</td>
<td>fast</td>
<td>trusted</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Shapeshift</td>
<td>Relatively high</td>
<td>Relatively slow</td>
<td>trusted</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Etherdelta</td>
<td>high</td>
<td>slow</td>
<td>Trustless</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>IDEX/DDEX</td>
<td>Relatively low</td>
<td>Relatively slow</td>
<td>Trustless</td>
<td>mixed</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>0xProject/looring</td>
<td>low</td>
<td>Relatively slow</td>
<td>Trustless(partially)</td>
<td>mixed</td>
<td>Partly yes</td>
<td>no</td>
</tr>
<tr>
<td>Kyber Network</td>
<td>Relatively high</td>
<td>slow</td>
<td>Trustless</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Troy Network</td>
<td>Extremely Low</td>
<td>Ultra-fast</td>
<td>Trustless</td>
<td>mixed</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

From the comparison of the characteristics in the table, it can be found that Troy Trade has an overwhelming advantage in terms of trading cost, trading speed, security and compliance. Among them, the trading cost and speed mainly depend on the support of the off-chain state channel technology, while the security is mainly guaranteed by the Layer 1 underlying public chain (such as ETH). Compliance is ensured through the settlement network layer and the foundation's compliance operations.
3. The Participants of Troy Network

The participants in Troy Network are:

1) Trading users, who can choose the Regular Trading mode, Bancor-algorithm based trading mode or Lightning Trading mode.

2) Broker-dealer, the broker-dealer acts as a settlement service provider, providing trading verification and automatic compliance verification services, providing services for trading requiring compliance or high trading verification threshold, aiming to lower trading threshold and costs to improve trading efficiency.

3) Market Maker, who needs to provide market trading depth and liquidity for specific trading pairs. This role is generally required to be provided by the vendor.

4) Relayer. The decentralized Network composed of Relayers shall be mainly responsible for timely updating and locking orders. Orders can only be completed in the order book of Relayer Network, and orders can only be cancelled after they are deleted from the order book. Relayer nodes are divided into ordinary nodes and supernodes. Among them, the supernode needs staking TROY tokens for a specific period, and its main function is to confirm and update orders. The order information can be quickly shared among supernodes to reach consensus through PBFT algorithm. Ordinary nodes do not need to
The participants in Troy Network are:

1) Trading users, who can choose the Regular Trading mode, Bancor-algorithm based trading mode or Lightning Trading mode.

2) Broker-dealer, the broker-dealer acts as a settlement service provider, providing trading verification and automatic compliance verification services, providing services for trading requiring compliance or high trading verification threshold, aiming to lower trading threshold and costs to improve trading efficiency.

3) Market Maker, who needs to provide market trading depth and liquidity for specific trading pairs. This role is generally required to be provided by the vendor.

4) Relayer. The decentralized Network composed of Relayers shall be mainly responsible for timely updating and locking orders. Orders can only be completed in the order book of Relayer Network, and orders can only be cancelled after they are deleted from the order book. Relayer nodes are divided into ordinary nodes and supernodes. Among them, the supernode needs staking TROY tokens for a specific period, and its main function is to confirm and update orders. The order information can be quickly shared among supernodes to reach consensus through PBFT algorithm. Ordinary nodes do not need to stake TROY tokens, but are responsible for the synchronization of trading records and to challenge suspicious trading records for bonus. If trading system bugs are found, 50% or above of the punished nodes’ staking tokens will be redistributed to the challenger after confirmation; otherwise, ordinary nodes will be put into the blacklist and banned by the system within a certain period of time.

5) Liquidity backer mainly provides Liquidity capital carriers (such as financing services) for trading networks, and reduces economic costs of broker-dealers/makers.

6) Information Feeder: it provides basic analysis of trading data on-chain and off-chain to users and profits from the subscription fee.
4. Token Economic Model

In Troy Network, the native token TROY is designed as the medium of value circulating as the blood in this organic network. Furthermore, TROY also acts as the gas fee unit when users call up the trading and settlement functions. TROY merely functions as utility token, which has no characteristics of any forms of security nor promises any returns derived from the token itself. Its functions are embodied in the following aspects:

1) Functions as the medium of value circulating as the blood in this organic network;
2) Provides workload reward of Relayer network to encourage timely and accurate updating, broadcasting and synchronizing orders;
3) Serves as relay medium for the exchange of unconventional token trading pairs in ring matching;
4) Acts as the gas fee unit when users call up the trading and settlement functions;
5) For staking in Relayer Network.
5. Development Roadmap

Considering the limitations of the feasible functions of current blockchain infrastructures, Troy Network will develop suitable strategies to adapt to the needs of different developing stages, our roadmap is as below:

Step 1:
Based on centralized Troy Trade, establish mature prime broker business ecosystem. At this stage, the project will provide services to users in a centralized system, exploring and verifying the feasibility of the business model, in order to reserve resources and technical support for the next step.

Step 2:
Implement the basic decentralized trading and settlement functions based on Ethereum. This phase will only open the ERC20 token trading market and is designed to verify the decentralized technical solutions.

Step 3:
After the technical solutions based on BTC and ETH being proved correct and mature, we will launch trading and settlement services based on EOS/Tron/Cosmos/Polkadot and other public chain platforms. This empowers our community influence and expand application scenarios of Troy Network, at the same time provide basic cross-chain support.

Step 4:
Develop Troy Network Instant components (APIs), in order to integrate the functions into various centralized or decentralized application easily;
Improve the functions of off-chain trading layer, by adopting mature off-chain channel technologies (such as bitcoin lightning network and Celer Network, etc.);
Improve Troy Network's cross-chain and dark pool trading functions.