Tower Research

White Paper

I. Overview

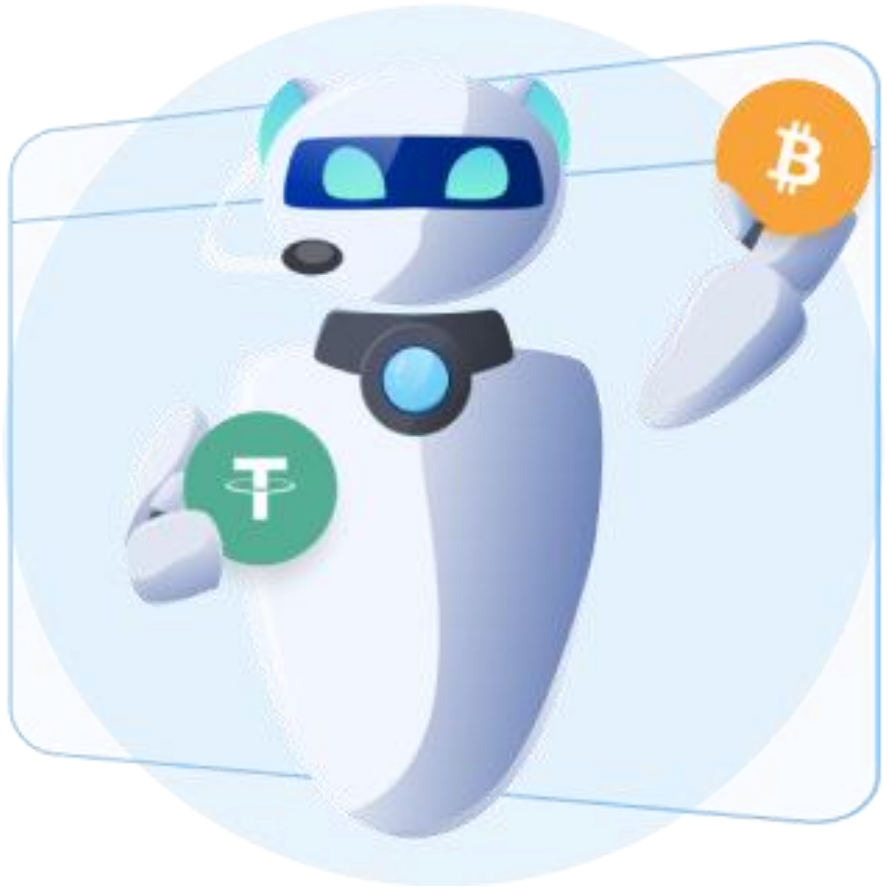
Tower Research Capital LLC, or simply Tower Research, is a high-frequency trading, algorithmic trading and financial services fund. It aims to create a decentralized trading platform (DEX) with community-based operations, transparent trading rules, and user assets controlled by themselves. The native token based on Tower Research is Tower Research, and the existing ERC20 Token form will be mapped to the native token on Tower Research according to the ratio of 1:1. Tower Research provides business solutions for cryptocurrency high-frequency trading and the financial industry with a more complete and unique blockchain business structure, and combines the token economy to give global trade greater vitality and participation.

2. Institutional Profile

Tower Research Capital is one of the oldest automated trading firms, founded by Mark Gorton and Alistair Brown in February 1998, Tower's in-house trading teams are independent of each other, accessing shared technical resources such as hardware, software and connectivity.) and resources such as business management, legal, compliance and risk management, and the core of the operation is the core engineering team, who own the architecture, implementation and optimization of the trading platform itself. This includes developing systems and tools for accessing market data, performing trend analysis, running trade simulations, order entry and management, real-time trade support, risk management and post-trade services. Deploy a variety of automated and quantitative strategies across a broad range of asset classes.

Tower employees are proficient in mathematics,

computer programming, physics, law, economics, engineering, finance and other academics. As of 2022, Tower has more than 1,000 employees in its global workforce. Albert An has been the company's CEO since 2019.



3. Tower Research

1. Accounts and Transactions

Tower Research is a basic account model, and each account natively supports multi-currency, so Tower Research supports multi-currency transfers. In order to prevent a large number of zombie accounts from consuming on-chain resources, Tower Research requires each account to be activated before it can be used. The specific activation method is to initiate a transfer transaction to the new account and deduct 1 Tower Research from the receivable Tower Research of the new account. As a feature fee for account activation. Each transaction can contain multiple messages, and each message can complete different operations, such as transfers, reward withdrawals, etc. Authentication of account permissions is performed by signature verification of the transaction. The signature algorithm is the ECDSA algorithm based on the secp256k1 curve. Tower Research supports

multi-signature transactions. The current multi-signature transaction adopts a method similar to the multi-signature in Bitcoin, that is, multiple signatures and public key information are included in the transaction. This method is easy to implement, but there are also problems of occupation and consumption of resources such as storage and computing.

Tower Research charges a transaction fee for each transaction, and only Tower Research can be used as a transaction fee. The transaction fee consists of two parts; the gas fee in the usual sense and the function fee. The gas fee is charged according to the number of bytes of the transaction, the number of signatures to be verified, and the number of reads and writes and the number of bytes stored in the store. The function fee is an additional fee for some specific operations. The operations that need to pay the function fee include: transactions in Tower Research to create new coins and create new trading pairs, transactions to start new

accounts, and transfer transactions with lock function. In addition, a commission will be charged proportionally according to the transaction amount in the matched transaction, and this part is also included in the function fee.

Tower Research plans to improve the way multi-signature transactions are constructed, by using an aggregated signature algorithm to compress multiple signature values/public keys. This approach saves on-chain storage space and reduces the number of signatures that need to be verified. Multi-signature transactions for n-ofn can improve the privacy properties of multi-signature transactions, because the aggregated public key and signature information can hide the entities involved in multi-signature transactions. On blockchains that support scripting systems, using Merkle to prove that multi-signature transactions for m-of-n can be achieve the same privacy protection effect. However, how to achieve the same effect without the script system still

needs further investigation. The biggest challenge facing the aggregate signature algorithm is to ensure security under the Plain Public Key Model under the premise of the existence of Rogue Public Kev attacks. Rogue Public Key exploits this fact, allowing attackers to concoct legitimate aggregated signatures without the knowledge of other parties involved. There are two common solutions, requiring the participant to prove that he really has the corresponding private key (KOSK, Knowledge of Secret Key) or requiring the participant's public key to be cascaded in front of the message to be signed. The practice of requiring KOSK proofs to be difficult to operate in practice and cascading public keys will partially offset the efficiency improvement effect of the aggregated signature mechanism. Under the Plain Public Key Model, participants do not need to prove that they hold the private key corresponding to the declared public key. The MuSig multi-signature mechanism and the bilinear pair-based BLS signature mechanism

designed by Blockstream researchers can meet the security requirements and do not have the drawbacks of the above two methods.

2. Decentralized financial aggregators

The so-called Defi represents the entire field of decentralized finance, and the ecological traffic entrance of DeFi is the aggregator. Decentralized finance or DeFi has taken root in the blockchain industry and is now undoubtedly the hottest field in the cryptocurrency market. There is no sign of

slowing down. Tens of thousands of DeFi users are now using Decentralized Exchanges (DEXs) for trading, swapping, staking, mining liquidity and yield farms, with the bulk of the activity taking place on exchanges that use the Automated Market Maker (AMM) model . Of these separate AMMs, Uniswap and SushiSwap have been the main targets in search of the best yields, mainly due to the concentration of liquidity there, which in turn drives the largest trading volume (since it is the day of trading activity that ultimately generates revenue) .

One of the main issues facing DEX traders right now is the high slippage that can occur when swapping - that is, orders are executed at a lower price than expected. This is simply because, if swapping within a single liquidity pool of a single DEX, the price or bid-ask spread may change between requesting an order and making the swap.

So there are two ways to solve this problem through aggregation. Aggregators like 1inch automatically execute

orders from liquidity sources connected to it according to the best way determined by its protocol. This could end up being one order or split into multiple orders. Aggregators like linch simply aggregate liquidity from different DEXs so that whenever a trader exchanges from its platform, the protocol calculates the best crypto price from all the DEXs it is connected to and from It determines the best liquidity pool to execute. This usually means that your orders are split and distributed across multiple DEXs. This typically results in lower slippage compared to exchanging on a single DEX.

On average, this can be a good way to exchange, but then traders will not be able to choose a source of liquidity for themselves and will have to trust the protocol to execute trades as needed. Furthermore, traders cannot actually compare sources on such aggregators, and automatic calculations of gas prices may be overestimated. However, it should be noted that token interactions in DeFi can be very

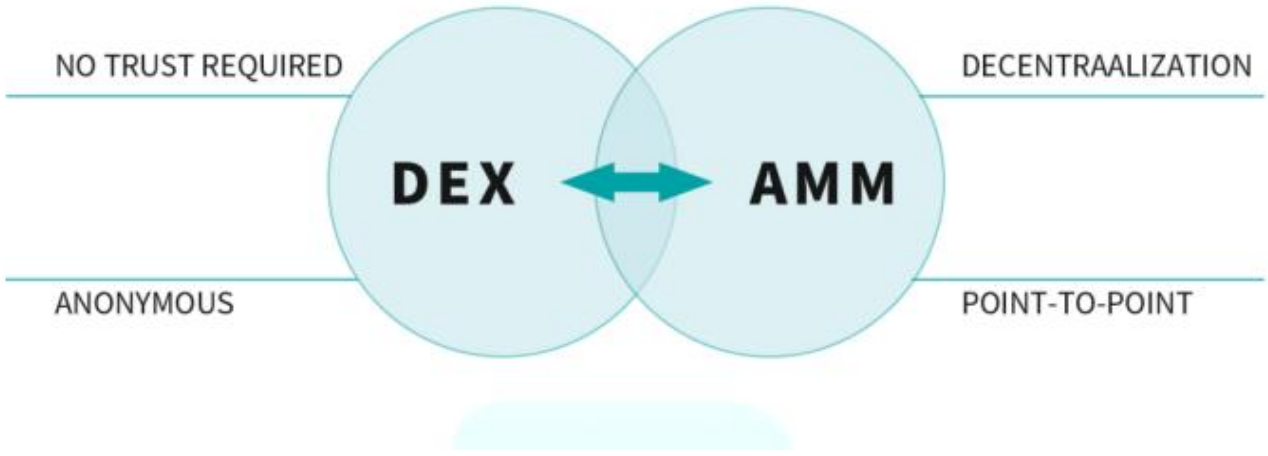
complex. Smart contracts are automatically routed through multiple platforms, so execution costs can add up quickly.

This makes little sense in times of high gas fees (and when isn't a period of high gas fees?), splitting an order into multiple orders and multiplying by gas fees makes little sense - so, in the congested times of Ethereum from 2020, Regardless, 1inch tends to choose a source for a single order. Another way, as our own aggregator PlasmaFinance does, is to just aggregate data. This method will display all the different DEXs and connected protocols, allowing users to view the prices that are immediately available for themselves and exchange at the desired DEX. You can even set your own slippage tolerance and trade deadline to your liking, which gives you precise control over how much slippage you are willing to risk and how long you are willing to wait for swap conditions.

In this way, professional arbitrage traders can switch

from one source of liquidity to another source of liquidity on the same aggregator very quickly. Once PlasmaFinance integrates with the likes of Binance Smart Chain and Polkadot, you can even choose to exchange across networks. In fact, we plan to integrate other aggregators like 1inch, and you can even swap our other aggregators if you prefer to swap aggregates automatically.

Aggregators don’t force you to choose, it allows you to see every opportunity DeFi has to offer. You can still choose to trade from or provide liquidity to a single source of liquidity if you wish, but it's good to know that you have all the options in front of you in an easy and simple way.



3. Liquidity mining

Before the advent of decentralized finance and DeFi platforms, users could only obtain liquidity by exchanging some assets. But DEX exchanges offer cryptocurrency holders a new way to generate income by adding cryptocurrencies to a public pool. In this article, we will explain what liquidity mining is, how it works, how it allows users to make money, and take a closer look at the risks of this new scheme.

Liquidity has three main properties:

Speed: It determines the execution speed of the order. If liquidity is too low, delays can occur and limit orders can take hours, days, or even weeks to execute. Try placing a limit order on an exchange at the current price and record the time to check how long it takes to execute. Then try to sell it again. For highly liquid currency pairs, the execution of orders can take anywhere from a few seconds to a few milliseconds. It is necessary to distinguish the liquidity of platforms and trading

pairs. Binance is one of the most liquid cryptocurrency exchanges ever, but it also has weak trading pairs such as DENT/USDT or IDEX/USDT. In other words, even the largest platforms have low liquidity pairs.

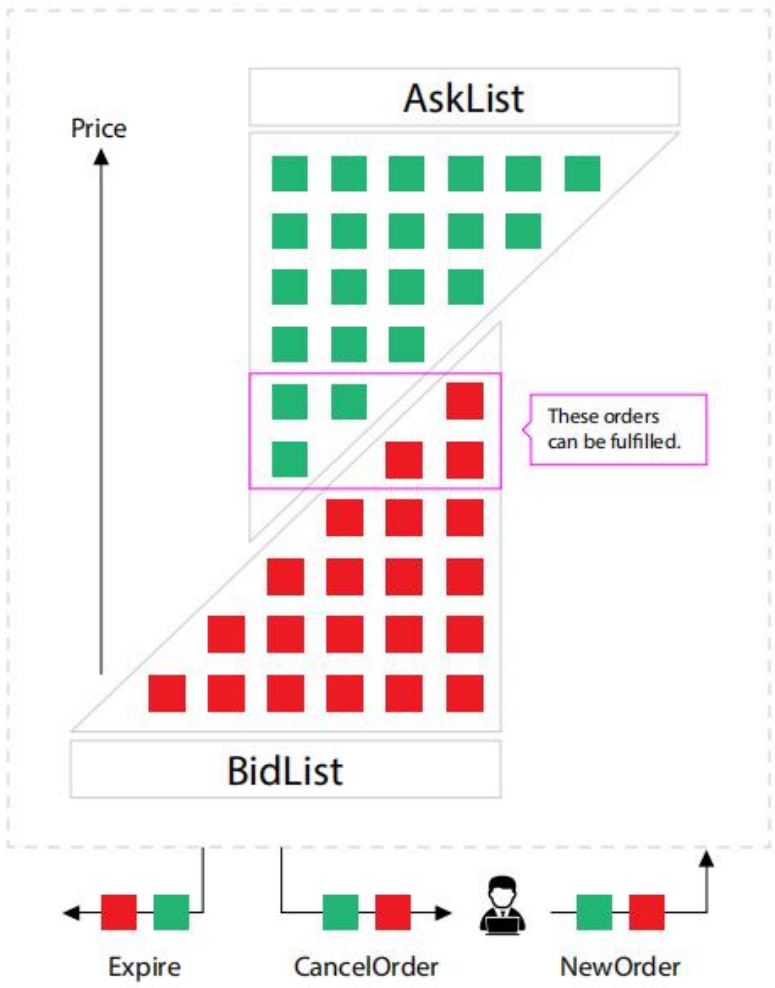
Spread: A high spread or gap between buy and sell orders in the order book indicates low liquidity. Low spreads mean that you can buy or sell an asset with minimal losses almost instantly. If liquidity is high, the spread is usually no more than one-tenth of the asset's market value.

Slippage: The essence of slippage is that illiquid pairs not only cannot guarantee that orders will be filled quickly, but that they will also be filled. Slippage means that even when an order is placed (for example, a stop-limit order) it cannot be guaranteed to be executed in the presence of high trading activity on the exchange: during periods of high price volatility. The paradox is: at first, orders go unfilled for a long time, but then there is a sudden influx of traders, resulting in unmet

demand or supply.

4. Deal matching

Like mainstream decentralized exchanges, we use order book-based matching methods, as shown in the following figure:



The order book contains a list of sell orders (AskList) and a list of buy orders (BidList), with sell orders marked in red and buy orders marked in green. Sell orders always want to push the price up, and buy orders always want to push the price down. Currently, only market orders are supported, and limit orders are not supported. If the price of sell one and buy one does not cross, the market is not filled.

The internal organization method of AskList and BidList is that they are sorted by price first, and orders with better prices are ranked first and are eligible to be traded first; while orders with the same price are packaged and put on the chain earlier, that is, older ones. Eligibility for priority transactions. In the figure, sell orders with lower prices are ranked at the top of the queue (bottom) in AskList, while buy orders with higher prices are ranked at the top of the queue (top) in BidList.

When the price of the sell one and the buy one cross, the

buy orders with a higher price than the sell one and the sell orders with a lower price than the buy one will be sorted by price and then by age, and traded one by one. The sell orders and buy orders circled by the purple squares in the picture are all eligible to participate in the sorting, and may eventually be traded. Whether they can all be traded in the end depends on the total amount of sales and purchases among them. Users can submit new sell orders or buy orders to the order book through the NewOrder transaction, and can also cancel orders issued by themselves in the order book at any time. Both Good Till Expire (GTE) orders and Immediate Or Cancel (1OC) orders are automatically removed from the order book when they expire. The former will expire at midnight UTC after the preset age is reached, and the preset age can be extended by paying more feature fees. IOC orders will expire in the next block after entering the order book (i.e. there is only one chance to be matched).

Off-chain matching, orders are always accepted by the server one by one, and they can be sorted in full order on a first-come-first-served basis. The most important difference between on-chain matching is that orders are packaged and uploaded to the chain in batches, and orders within the same block cannot be sorted on a first-come-first-served basis. In order to ensure that the orders within the same block are treated equally, we adopt the method of "call auction": in each round of matching, a single execution price is calculated for all the buy and sell orders that can be traded. The principles for determining the strike price are:

(1) Maximize transaction volume.

(2) Minimize the remaining amount. If more than one price can achieve the same volume, the price that minimizes the remaining volume is selected. Remaining volume refers to the remaining unfilled amount of an order at an acceptable execution price.

(3) Market pressure. If multiple prices can meet the requirements of steps 1 and 2 above, then first determine which direction the market is currently pressure on the underlying price. If the remaining amount is positive, the buyer is under pressure and choose a higher price; if the remaining amount is negative, the seller is under pressure and choose a lower price.

(4) When there is a positive residual amount and a negative residual amount at the same time, the execution price of the last transaction is the reference price, and the price closest to the reference price is selected.

Whether it is a centralized exchange or a decentralized exchange, it is necessary to deal with the problem of front-running. Front-running transactions refer to obtaining information about transactions in advance with the help of technical advantages or market advantages, predicting changes in transaction prices in advance, and executing

transactions that are beneficial to them, which often causes other participants in the market to suffer losses. For example, in a centralized exchange scenario

In this way, the exchange can see more global transaction information, so that before matching the transaction, it can concoct the optimal trading strategy for itself according to the current market situation and give priority to the transaction for profit.

Tower Research's DEX public chain is designed to naturally prevent preemptive transactions. First, based on the second-level block generation speed of Tendermint, the time window for preemptive transactions is very small; secondly, in a P2P network, it is difficult to fully understand which orders will be included in the next block; third, call auctions The price generation mechanism makes the preemptive transaction have no obvious advantage compared with other transactions in the same block. Therefore, it is very difficult for ordinary

users to profit from front-running.

As a Validator, it has the right to decide which orders to add in the next block. It can include its own specially designed orders in the block by means of "censorship attack", instead of those orders that conflict with its own orders. In order to encroach on the interests of other traders. However, all data and execution logic on DEX are public. If Validator frequently conducts censorship attacks on other people's transactions and inserts transactions that have not been broadcasted by the entire network, then its behavior will be easily observed. . This would damage its credibility, eventually causing the principal to withdraw its support.

A possible improvement is through the "Commit-Reveal" mechanism, which allows users to selectively delay the reveal of the order's contents (for example, 2~3 blocks later), so that when the validator packs the next block, it cannot be seen. All the state of the current trading system also makes it more

difficult to construct profitable front-running trades. The Tower Research team will continue to conduct in-depth research on the issue of front-running trading and provide more complete solutions in the future.

5. Automated market making

At present, exchanges widely use the matching method of order books. To achieve a transaction, there needs to be a demand for buying and selling at the same time, and the AskList and BidList on the order book must have an intersection. For currencies with good liquidity, such as BTC, because the order to buy one or sell one is very large, if you want to buy and sell a certain amount, you can basically meet the demand on the exchange, but some currencies with little attention have insufficient liquidity Support large buy and sell orders. Based on this situation, many projects will choose market makers to increase their liquidity. Market makers maintain market liquidity through the market making system.

They compensate for the cost of the services provided by the appropriate price difference between the buying and selling quotations and earn profits. . The high cost of market making is a major problem faced by Token issuers. On the one hand, exchanges have to charge fees, and on the other hand, market makers have to make profits. These are the costs of increasing liquidity. In addition, market makers still have to rely on real trading volume. Although market makers are all program-based, when there is a large number of unilateral buy and sell orders, the market-making capabilities that traditional market makers can provide are very limited.

Tower Research Chain will use automated algorithm market making on the DEX public chain to meet the liquidity of tokens, mainly based on two automated market making protocols: Bancor and UniSwap. Tower Research will expand the Bancor protocol and UniSwap to make it more Adapt to the decentralized exchange, better provide sufficient liquidity,

and ensure the reasonableness of its price. Market makers no longer specify transaction prices when providing liquidity, but only provide funds.

The Bancor protocol can realize a token trading network with decentralized liquidity. The protocol does not rely on bilateral demand matching, and uses connectors to realize an asynchronous price mechanism. The price formula of Token is:

price=connectorBalance/(smartTokenSupply *CW),

where the connector weight (CW) affects the sensitivity of smartToken price to smartToken supply. Users can buy Tokens from the connector at any time at the automatically calculated price, or sell Tokens to the connector at any time at the automatically calculated price.

UniSwap is also a decentralized token exchange protocol. Uniswap completely gets rid of the concept of limit orders. UniSwap will make a market based on the constant product market maker model to bring everyone's liquidity together.

UniSwap will gradually increase the price of tokens with the increase of transaction buy orders, and will gradually decrease the price of tokens with the increase of transaction sell orders. Through the algorithm, a decentralized exchange system that does not require pending orders and does not require market depth can be realized. The core idea of constant product is: x*y=k, where x is the amount of Base Currency, v is the amount of Quote Currency, and k is the product of the two amounts. When k is guaranteed to be a fixed constant, the larger the x value, the smaller the y value; the smaller the x value, the larger the y value.

6. Profit model

(1) Trading profit:

Trading profit is a major source of profit for Tower Research. After Tower Research goes online, all parties involved in financial product transactions will conduct various transactions, and Tower Research can be converted into

currency, and the handling fee generated during the transaction process will be used as profit. Transaction process Each transaction is given a priority, which is determined by the historical time, amount and number of "inputs". Transaction requests with high fees will be prioritized.

The Tower Research project can also access tasks issued by other blockchains, and generate corresponding virtual coins through its own transaction computing power to generate value.

(2) Service profit model:

After the issuance of Tower Research, all business activities based on blockchain technology, business entities must consume tokens to support the operation of platform nodes. Organizations or individuals who use tokens need to obtain tokens in the form of mining or buying coins. Service profit is mainly obtained from three ways:

If the third-party application platform wants to join the

Tower Research traceability service platform, it must charge a certain franchise fee, which will inevitably consume a certain amount of tokens; at the same time, the third-party application platform will consume tokens whether it is reading or writing the chain. If a third-party application platform wants to obtain the data of users of this platform, it must consume a certain amount of tokens. When users use a third-party application platform on the traceability service platform to obtain information to generate behavioral data, query products or exchange assets are equivalent to mining behavior, and the traceability service platform will pay tokens for the user's contribution. And if users need to use the value-added services provided by the trading system, such as joining members, they also need to consume a certain amount of tokens. When more users use the third-party applications in the traceability service platform to push the token price up, the platform will gain more profit and

appreciation.

7. System operation management mode

For Tower Research, system equipment operations include several categories:

(1) Standard Tower Research node;

(2) Cloud access node;

(3) Cloud storage nodes;

(4) Tower Research trusted gateway;

(5) External data source storage pool;

(6) Tower Research service equipment.

A standard Tower Research node can be considered as a basic network device that supports the Tower Research control chain and at least one data chain, supports the data storage of the related chain, and can execute the corresponding data chain smart contract. The device should have the ability to run the Tower Research virtual machine, and be able to execute the Tower Research model functions

defined by the Tower Research control chain and the corresponding data chain.

Cloud access node. It is a node developed by Tower Research for the convenience of each mobile terminal device, and this node can provide the ability of a Tower Research node for each access object. Any mobile client can access the cloud by logging into the cloud in a secure encryption way, and obtain various capabilities of the Tower Research node.

The cloud storage node is the Tower Research block data backed up by Tower Research in the cloud in real time. This data is written into the cloud in real time by the Tower Research genesis node; this data is only for the convenience of users to check offline, not as the consensus basis of all nodes. It belongs to Tower Research accessory tool. Users can verify the validity of the data chain offline by obtaining the entire data verification and signature. Since the cloud storage node data does not need to be stored in the order of the

blockchain, it can be stored in a traditional database format, such as MySQL, to facilitate offline query and verification for users.

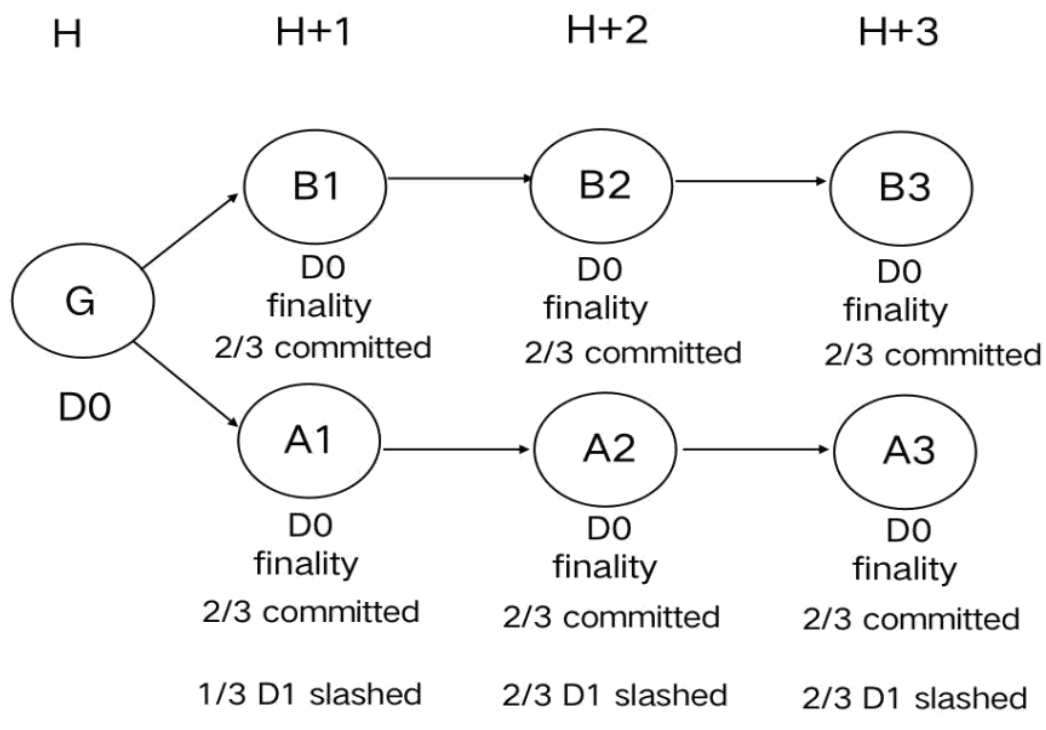
The Tower Research trusted gateway is the main device used to communicate with external data sources. The device will obtain the external data sources required by Tower Research through Tower Research, and pass the Tower Research audit to determine the confidence level. When the Tower Research node uses the data, it will determine the reliability of the final data according to the consistency of each independent node, and give the credit evaluation of each node. In addition, the trusted gateway can support the expansion of Tower Research and user plug-ins to achieve deeper integration of online and offline. The external data source storage pool, the data source storage content is the external data obtained by the trusted gateway, and all data have passed the Tower Research audit. The storage pool will

also be used for the storage of users' private data, which can only be accessed by specific users through secure encryption. Any file in the storage pool can use the built-in engine to verify the file signature without directly reading the content, so as to determine whether the file has been tampered with. Due to the importance of this storage pool, Tower Research will deploy multiple distributed storage pools, and each pool will be organized in the way of data blockchain. Only when the data content of each distributed storage pool is agreed can the block be written. Tower Research service device, which contains two functions:

①It can serve the optimization of the entire system structure and the parameters of each Tower Research model;

②Initiating various Tower Research services on Tower Research can not only use Tower Research as a whole to serve external users, but also call nodes in Tower Research to serve various users. The Tower Research service device is an

auxiliary device of Tower Research, and any node can also build this device by itself.。



4. Tower Research 应用

1.Typical characteristics of blockchain technology

Blockchain is an integrated innovation of information technologies such as distributed data storage, point-to-point transmission, trust consensus algorithm, and encryption algorithm in the Internet era. It has the characteristics of pan-centralization, trust consensus, information cannot be tampered with, and openness. In business situations that require a high degree of mutual trust.

Tower Research pan-centralized operation:

Pan-centralization, also known as "decentralization", is one of the biggest advantages of the blockchain technology system. The blockchain system is based on the distributed system structure and uses encryption algorithms to establish trust relationships between distributed nodes, thereby forming a decentralized distributed system. In a decentralized system, the entire network no longer needs a centralized third-party

intermediary, and the rights and obligations of any node are equal. The damage or loss of any single node in the system will not affect the operation of the entire system. The data blocks in the blockchain system are jointly maintained by all related nodes. Therefore, cross-border payment based on blockchain technology can ensure the transparency of the transaction information between the two parties in a pan-centralized mode, and reduce the risk between the two parties. risk of information asymmetry.

Tower Research uses mathematical algorithms to build trust relationships: trust is like the invisible and intangible oxygen in daily life. It is the basis for transactions in the market economy and the core of financial business. Without trust, no international transaction would be possible. Blockchain technology uses a set of consensus-based mathematical algorithms to establish a network of "trust" between transaction parties.

Every transaction that occurs in the Tower Research system is publicly released to other participating nodes in the system. All nodes participate in the verification together, confirm the authenticity of the transaction, and write the verified transaction record into the blockchain. The use of blockchain technology to build a transaction information that both sides of the trade jointly participate in the verification and maintenance of to ensure the authenticity and reliability of delivery information and capital payment information can greatly reduce the risk of payment and settlement between import and export parties in financial transactions.

Tower Research information cannot be changed: in the blockchain system, once the information is verified and added to the blockchain, it will be permanently stored, unless it can be supported by more than half of the verification nodes in the system at the same time, the modification of data by a single node is invalid, so the data stability and reliability in the

blockchain system are extremely high. In international payment, once the importer completes the cross-border payment, the information cannot be changed, which can ensure the authenticity and validity of the import and export trade information in the pan-centralized mode.

The Tower Research system is completely open: the blockchain system is open, and the operating rules of the entire system are open and transparent. Data exchange between each node in the entire system does not require mutual trust, except that the private information of the transaction parties is encrypted. In addition, any participating node can query the data in the blockchain through the open interface, so the entire system information is highly transparent, and nodes cannot be deceived. This completely open feature can ensure the open and effective operation of financial transactions.

By analyzing the characteristics of Tower Research

technology, it can be seen that blockchain technology is very suitable for cross-border payments in financial transactions. Building a cross-border payment model based on blockchain can greatly reduce the risk of cross-border payment, improve the efficiency of cross-border payment, and save the cost of cross-border payment.

2. Tower Research's cross-border payment solution based on blockchain technology

Tower Research uses the blockchain network to add traditional financial institutions, foreign exchange market makers, liquidity providers, etc. to the payment network to build a payment gateway. Through the payment gateway, the flow of digital assets on the blockchain can be connected with the real legal currency, so that the legal currency can be converted into digital assets on the blockchain, which is convenient for subsequent payment transfers. Through the network connector in the blockchain payment network,

traditional market makers, remittance banks, remittance banks and other institutions can be connected, eliminating intermediate transaction links and realizing point-to-point fast and low-cost payment.

3. Tower Research's cross-border payment advantages based on blockchain technology

Tower Research's new model of cross-border payment based on blockchain, compared with traditional wire transfer payment, makes full use of the advantages of blockchain technology, directly conducts point-to-point payment between the two parties, and participates in payment verification together, which reduces the risk of cross-border payment, There are obvious advantages in improving cross-border payment efficiency and saving bank resources.

4. Tower Research reduces cross-border payment risks

In traditional wire transfer payment, the biggest risk is that there is no guarantee that the importer's capital payment

and the exporter's goods delivery information are true and valid. After the importer passes the bank wire transfer, he cannot understand the intermediate payment link in detail, nor can he intervene in the transfer payment of funds, nor can he know the exporter's delivery information in time. Therefore, the two sides of the trade can only conduct transactions based on the commercial credit of both parties. transaction risk.

Tower Research's cross-border payment based on blockchain technology connects all nodes involved in payment and settlement, including importers and exporters, through blockchain technology to jointly maintain payment transaction information and participate in consistency verification. After the importer pays through the blockchain, if the real and valid exporter's delivery information is not received, then in the consistency verification process, the importer will deny the payment information, and the exporter will not be able to

receive the remittance . Therefore, through blockchain payment, all parties involved in the transaction jointly maintain transaction records and participate in the verification of transaction information, which greatly reduces the payment risk in financial transactions.

Tower Research improves the efficiency of cross-border payment: In traditional wire transfer payment, the wire transfer of the importer is ultimately completed by the bank. Inter-bank payments are often done by central counterparties, and each intermediary counterparty has a local database that acts as an authoritative general ledger that records all account balances and transaction flows. In such a transaction with intermediate participants, two complex business processes must be processed: First, all banks involved in the payment must reconcile the transaction information and synchronize all transaction information to the intermediate settlement party. Second, the central counterparty will only execute the final

payment after offsetting the debit and credit of different accounts. Therefore, in traditional cross-border payments, very complex transaction processing is required.

Tower Research adopts the solution of blockchain payment. Since all participating nodes in the blockchain network jointly maintain the verification information to ensure the consistency of information, there is no need for complex information synchronization and reconciliation in blockchain payment, which greatly improves the Efficiency of cross-border payments.

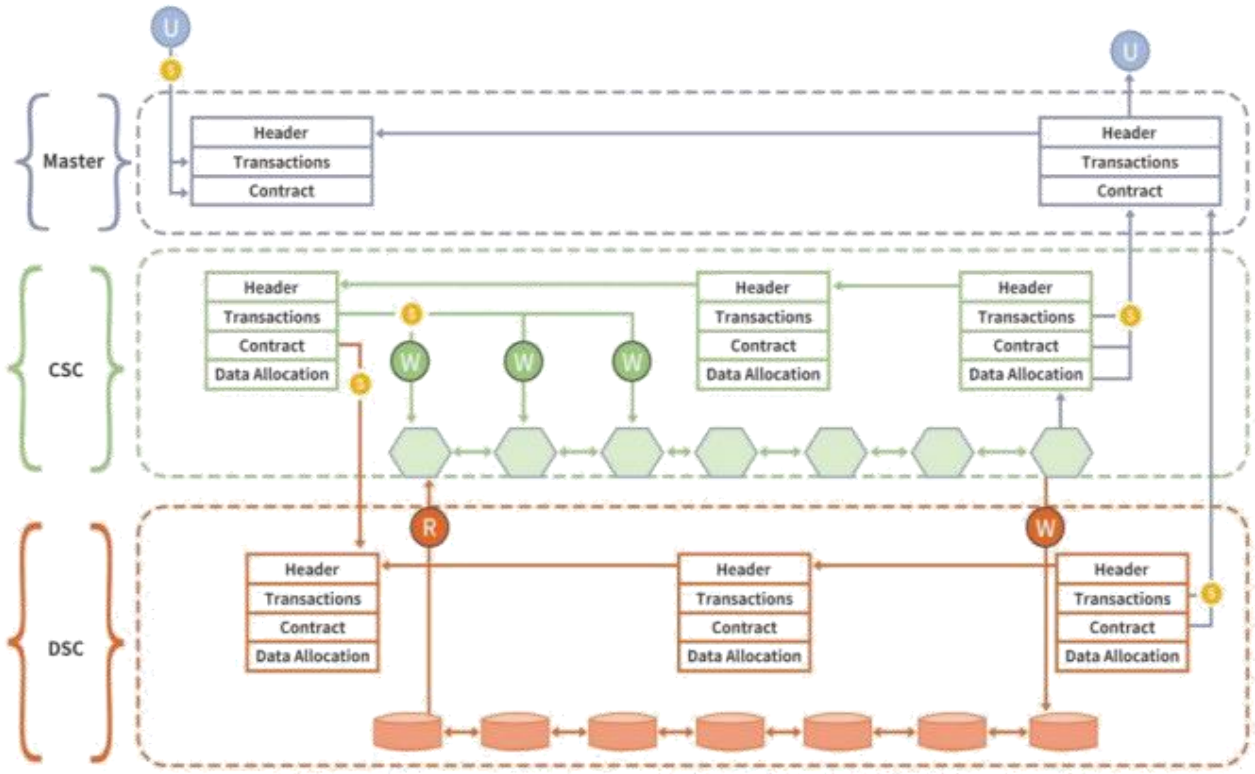
Tower Research saves banking resources: In traditional cross-border payments, inter-bank payments use an authoritative central transaction party to settle payments for both lenders and borrowers. In order to minimize the counterparty risk, each bank must establish a set of payment network for the affiliated bank and set up a separate reserve account for each affiliated bank, so a large amount of reserves

are required for cross-border payments. In the blockchain payment system, different banks can be implemented based on the alliance chain, so that when the exchange payment is made between different currencies, it can get rid of the participation of the intermediate affiliated banks and directly make real-time payments;

In Tower Research's blockchain-based payment platform, each bank only needs one reserve account, which saves the reserve capital that would have been stored in the intermediary transaction party, and increases the resources that can be allocated to its own banking business. The solution becomes even more attractive when a large number of banks are involved in the network. Therefore, cross-border payments based on blockchain technology can greatly save banks' resources.

To sum up, the decentralized technology adopted by Tower Research blockchain payment means that both parties

of the transaction no longer need to rely on a central organization to be responsible for fund settlement, but directly transfer value based on a consensus mechanism algorithm that does not require trust coordination. Therefore, Tower Research blockchain payment provides a better solution for cross-border payments than traditional wire transfers.。



5. Disclaimer

This document is for informational purposes only, and the content of the document is for reference only, and does not constitute any investment advice, invitation or offer for the sale of stocks or securities by Tower Research and its shareholders. Any actions related to this white paper shall not be deemed participation in the public offering, including requesting access to the white paper or sharing the white paper with others. Participating in the public offering means that the participants have reached the age standard, have full capacity for civil conduct, and fully understand all risks.

Thanks For Watching