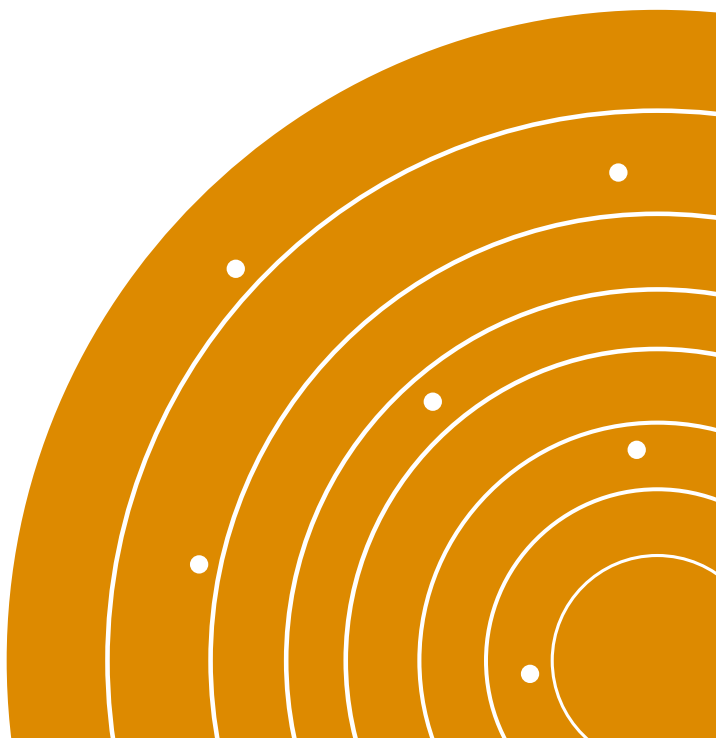
btSwap

a better way to trade your crypto

Decentralized Liquidity Mining

Exchange Based on AMM



Contents

Abstract

Initial Decentralized Exchange (DEX) Offering is very popular recently, which is similar to Initial Coin Offering (ICO) in 2017. This is mainly due to the recent hype of Decentralized Finance (Defi) and the market cycle of cryptocurrency. In most of existing DEX platforms, liquidity providers are only rewarded with transaction fees, and the platform does not issue its own tokens, so it is difficult to mobilize the enthusiasm of traders or liquidity providers. Therefore, we propose the type of DEX model -- btSwap.

btSwap is a protocol that allows automatic token exchange based on Ethereum. It is completely decentralized and designed around usability, gas efficiency, censorship resistance, low transaction fee. It is developed in the form of a liquidity pool with automatic market making (AMM).

At the same time, btSwap has also improved on the DEXes developed using AMM model such as Bancor, and allowed the listing of coins with no strings attached (Bancor and others require staking platform coins).

On the basis of AMM, it has added liquidity mining functions, which would stimulate users' enthusiasm for participation and create arbitrage opportunities, so that users can continue to stay on the platform and achieve sustainable cycle.

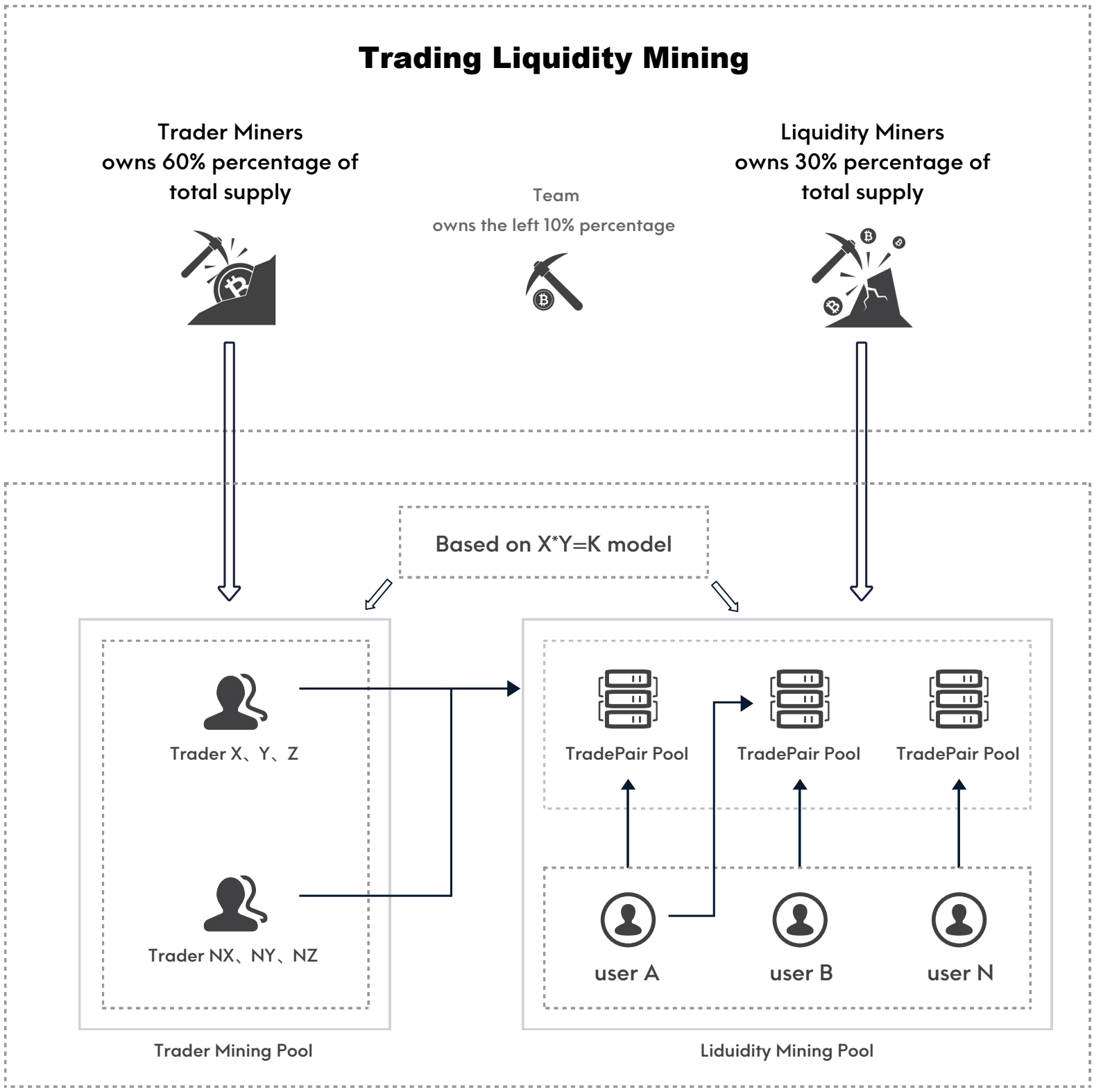
1. Overview

1.1 btSwap Idea

btSwap is an automatic market-making decentralized exchange based on the concept of liquidity pools. It is similar in function to some DEXes on the market; however, it adds the element of liquidity mining. In other words, as long as a transaction is performed, a certain amount of tokens will be generated and sent to the traders.

The essence of liquidity pool is to provide unlimited liquidity. As long as the user wants to trade, they can sell the cryptocurrency at any time instead of only supporting one-way market, so it is called AMM (automatic market making). Of course, it also has certain flaws -- in the case that the price goes to the extremes, the price curve would be steeper. In general, AMM has great potential and value, and is the embryonic form of future human-machine exchanges.

Liquidity mining is a process of equal distribution of tokens, which can attract users that are interested in the project to form an ecosystem, and continue a positive cycle. btSwap will generate new tokens according to each block of Ethereum, halve it every 4 years, and realizing complete decentralization.



1.2 Design Idea of Logo

The design concept of the logo uses the elements of "bee".

There are two huge groups in nature that are always awe-inspiring, one is ants and the other is bees. We all know that with the hard work of bees, delicious honey is available. Therefore, we hope btSwap community members can mine diligently like bees and reap their own achievements.

In addition, it is the swarm thinking mentioned in Kevin Kelly's "Out of Control"-decentralized super organisms, distributed management, just like the several characteristics of the blockchain.

The essence of bee colony thinking is a decentralized super organism. There is no mandatory central control system. Tens of thousands of bees gather together to form a new organism. The power of a bee colony will not emerge from the individual actions of one, two, or dozens of bees. Only when there are enough members, the point-to-point link and mutual influence between members will release a very powerful effect, and exponential growth will appear when the quantity changes to the qualitative change.

The rule of the bee colony relies on the wisdom of the populaces, the information sent back by the little bees, and then the action plan is decided through discussion and voting. For example, where do bees gather honey? They are all relying on the information sent back by the worker bees (in the form of dancing). They will see who dances enthusiastically, and then send a few more waves of bees to investigate. After verifying that they are correct, the swarm starts to act. This is the essence of a democratic system, a thorough distributed management.

Based on the above characteristics, we regard "bee" as the primary element of the logo. It shows that btSwap is completely decentralized. At the same time, it is necessary to rely on community members to play their own roles, whether it is a trader or a liquidity provider, to play its greatest value in this system, thereby creating our own wealth.

2. Token Introductions

2.1 Token Information

Token name: BT (BtSwap Token)

Total Token: 1 billion

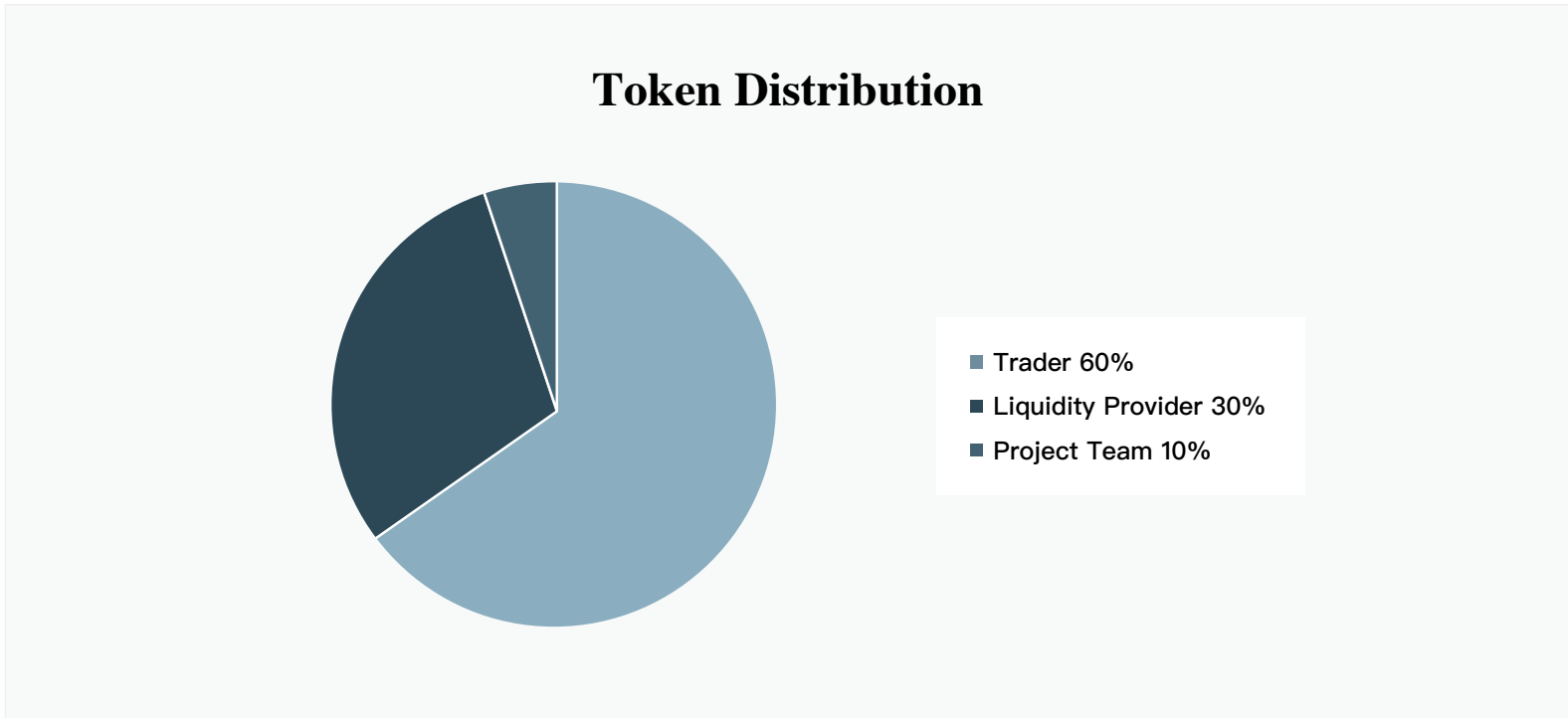
Block generation cycle: consistent with Ethereum (based on its smart contract operation)

Initial reward: 3 coins per block

Halving cycle: every four years

2.2 Token Economic Model

The total supply of btSwap is 1 billion. The project follows "zero pre-mining, zero airdrop", and all tokens are generated by transaction mining and providing liquidity. Among them, 10% of the mining output is allocated to the project party for technology research and development and community promotion of the project. The remaining 90% of tokens are allocated to users who provide liquidity and make transactions for the btSwap, of which 60% are allocated to traders and 30% are allocated to market makers who provide liquidity.



Through this method of liquidity mining, the output of tokens is relatively slow, so the project does not design a lock-up mechanism. btSwap halves mining every four years. After the mining output ends, the community will determine the proportion of transaction fees and continue to maintain the normal operation of the system.

The notes of liquidity mining include the following:

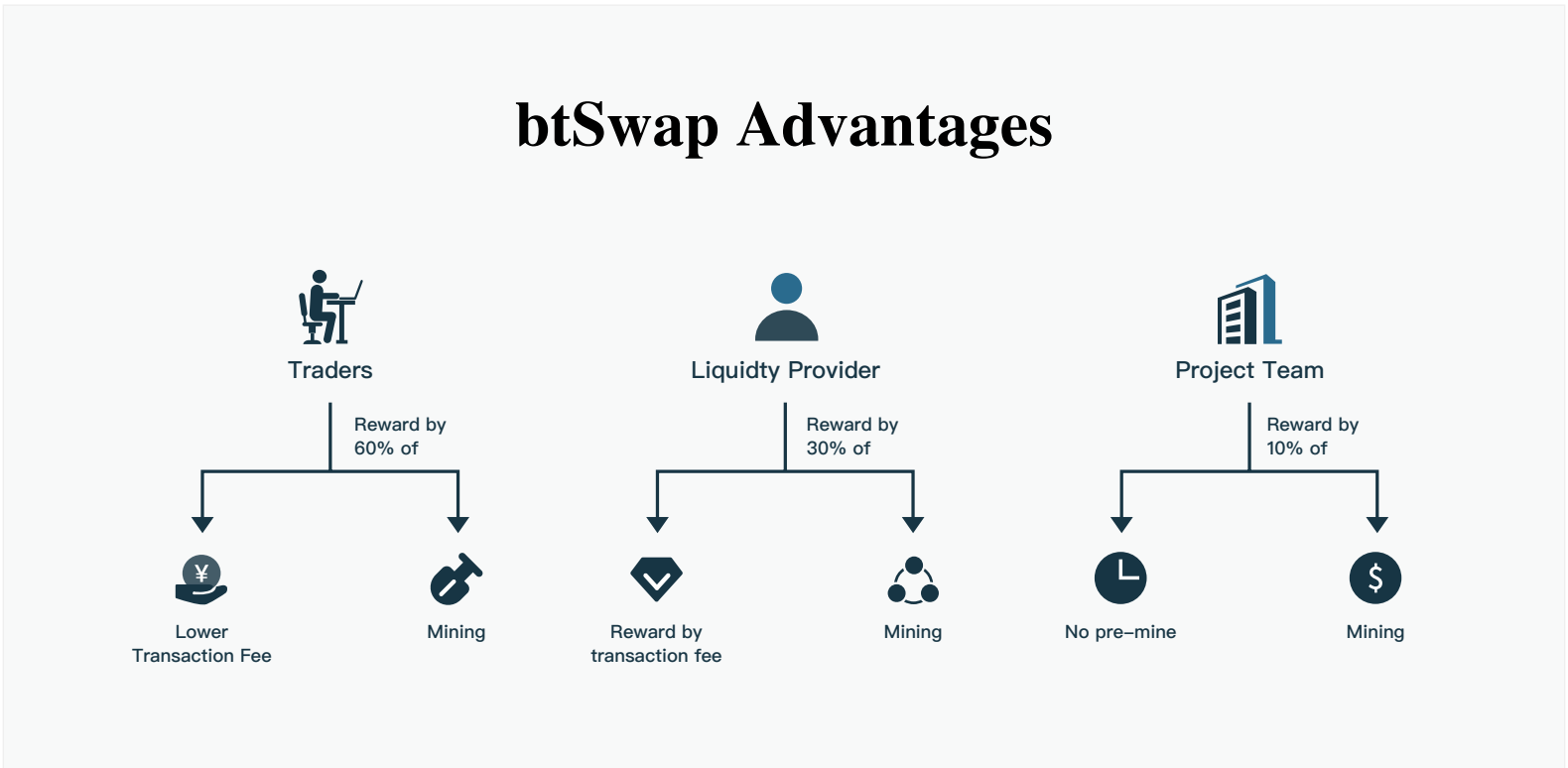
- For traders, in addition to the low-cost transaction fees at btSwap, they can also get 60% of the total tokens generated through transaction mining, so they have great motivation to come to trade;

- For liquidity providers, in addition to transaction fees, btSwap also rewards an additional 30% of mining output to them. This powerful incentive will also stimulate them to actively increase liquidity;

- The project party has completely zero pre-mining, and the initial holdings are zero, just like the community and other investors;

- One-fifth of the transaction fee will be reserved for the project party for repurchase, platform construction, and ecological construction. Among them, 50% is used for repurchase until the total amount is reduced to 21 million;

- Not all currencies that list on btSwap can be liquidity mining. It needs to be voted by the community and mortgages a certain amount of tokens. If the currency is involved in deception, the mortgaged token will be destroyed, which is equivalent to deflation of the total circulation.



The specific mining mechanism is detailed in Chapter 3.

2.3 BT Value

BT can be used for community governance of btSwap and make decisions on major events in the community. For example, voting to determine the proportion of transaction fees, deliberation of other important regulations, and the decision to achieve deflation on the regular repurchase and destruction of tokens, etc., please refer to the announcement for details.

3. Mining Issuance

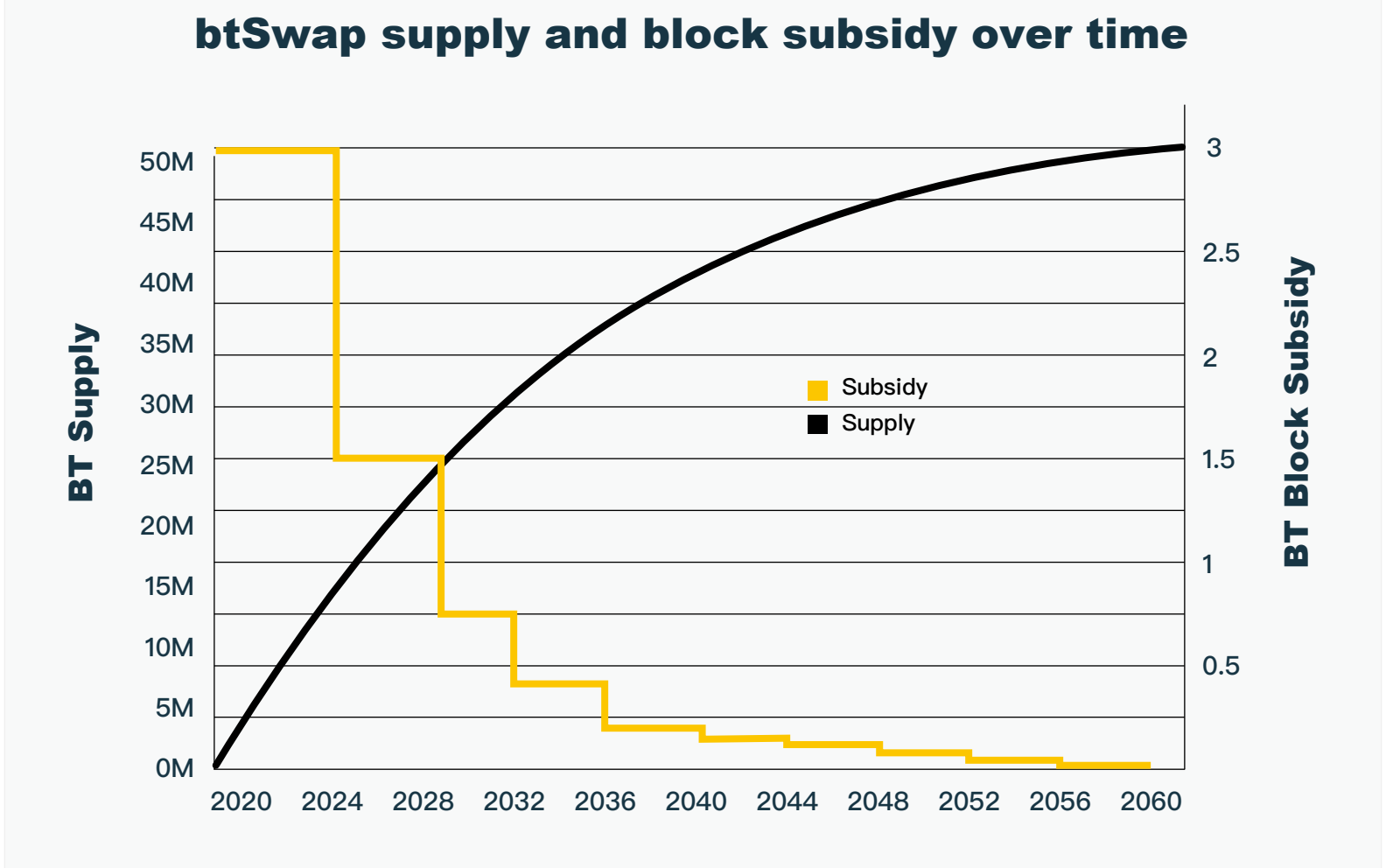
The block generation cycle of btSwap is consistent with that of Ethereum. When Ethereum produces a block, btSwap will mine and issue 3 tokens; at the same time, every 8,409,600 blocks (calculated according to the current Ethereum block production rate, the duration is about 4 years) will be halved. Therefore, it can be calculated that the upper limit of the total Token is about 1 billion.

The tokens produced in each block will be distributed to Trader, Liquidity Provider (LP) and project teams in a certain proportion.

3.1 Halving Rules

As we all know, Bitcoin halves every 210,000 blocks (which is what we often call four years) to avoid currency inflation. Therefore, after referring to the Bitcoin halving concept, we designed the following halving rules:

- Every 8409600 blocks (at the current rate of Ethereum block production, it is about 4 years) is a stage;
- In the first stage, each block reward (that is, mining output) is 3 BT;
- After each stage, the reward is halved. For example, in the second stage (starting from the fifth year), each block reward is 1.5 BT;
- After 84096000 blocks (at the current rate of Ethereum block production, it is about 40 years), there will be no more rewards.



Therefore, by calculating in this way, it can be concluded that the total mining reward is about 1 billion which is also the total amount of BT.After the halving reward is over, the block reward will be replaced by the handling fee as the main incentive method to guide the normal operation of the entire ecosystem.

3.2 Transaction Mining

In order to incentive traders to make transactions, 60% of the BT output of each block will be rewarded to traders. These rewards will be produced in a trader Mining Pool , each Trader allocates a certain proportion of shares according to the proportion of its trading volume in the total trading volume.

3.2.1 Pool share

To facilitate understanding, we define several parameters:

* userVolume: Indicates the transaction volume currently owned by a user in the BT system, that is, the share the user owns, priced in eth, and the unit is 1e18;

* totalVolume: Represents the total transaction volume of the BT system, that is, the total share;

* totalTMPBalance: Represents the total amount of BT in the current traderMiningPool. (Each block produces a fixed amount, see chapter 3.1 for details)

Therefore, the total amount of BT currently held by a user in the mining pool is:

$$balance[user] \equiv \frac{\text{userV}olume}{totalVolume} * \text{totalTMPBalance}$$

3.2.2 Withdrawal share

According to the formula, we can infer the user's withdrawal behavior. For example, if the user withdraws X tokens, the user's token in the mining pool will be changed to:

$$balance[user] \equiv \frac{\left(userVolume - \frac{X * totalVolume}{totalTMPBalance} \right)}{totalVolume - \frac{X * totalVolume}{totalTMPBalance}} * (totalTMPBalance - X)$$

It can be concluded from the formula that after the user withdraws, the userVolume will be reduced, and the totalTMPBalance will also be reduced simultaneously.

3.2.3 Transaction Mining

From the above, we can know that as long as a user generates a transaction, the User Volume will be increased, more tokens will be produced. Then how is the mining reward calculated during the transaction process?

For example, assuming that user's newly added transaction Volume is Current Volume, its latest balance is:

$$balance[user] \equiv \frac{userVolume + currentVolume}{totalVolume + currentVolume} * totalTMPBalance$$

According to this formula, we can know that as the transaction volume increases, the user's new mining rewards will gradually increase, but at the same time the growth rate will gradually decrease (the denominator totalVolume becomes larger).

Since BT will mine and issue new tokens in each block, totalTMPBalance will always increase. That is to say, for token holders, if no new users join the transaction to increase the new transaction volume (that is, the totalVolume remains unchanged), then its balance will continue to increase. Therefore, assuming that there is no new transaction from the last transaction of the user to the current block, the balance of the user in the mining pool is:

$$balance[user] \equiv \frac{\text{userV}olume}{totalVolume} * (\text{totalTMPBalance} + (block.number - previosBlockNumber) * Award)$$

* block.number represents the current block height.

* previosBlockNumber represents the block height of the user's last transaction.

* Award represents the number of BT rewards for each block in the current stage, such as the first stage Award=3

To sum up, if a user keeps making his User Volume significantly higher at a certain moment (Total Volume will also become higher), and then withdraw his share of BT from the mining pool, this is reasonable because the transaction is Need to consume handling fees. At the same time, if the totalTMPBalance in the pool is large, users will also have the motivation to withdraw cash in time to avoid this situation.

3.3 Liquidity Mining

For Liquidity Provider, in addition to all the transaction fees, they will also receive 30% of the amount of mining output. These rewards will be produced in a mining pool called LPMiningPool (liquidity provider mining pool), each LP occupies a certain share of it according to the proportion provided by its liquidity. This process is called liquidity mining.

The principle of liquidity mining is similar to transaction mining,
but the calculation mechanism is completely different. In the BT system, there will be a total liquidity pool priced by the product of eth*blockNumber, and each Liquidity Provider will increase a certain share after providing liquidity, reduce the share after withdrawal.

3.3.1 Introduction to Liquidity Share

First of all, we need to give a definition of liquidity share. In the BT system, a user's liquidity share is: The amount of User's deposit equivalent to eth multiplied by the existing duration, expressed by the formula:

$$userLiquidityShare \equiv \frac{userEthBalance * (block.number - lastDepositBlockNumber)}{totalLiquidity}$$

It can be seen from the formula:

*userEthBalance represents the amount of eth-based of the user’s deposit liquidity

*lastDepositBlockNumber represents the block height of the user's deposit liquidity

*block.number-lastDepositBlockNumber represents the number of blocks the user has experienced since the last deposit to the current moment

*TotalLiquidity means the sum of userLiquidity of all users (here is just a visual display, see chapter 3.3.2 for actual code implementation):

$$\text{totalLiquidity} \equiv \sum_{user1,user2...userN} \text{user}Liquidity$$

Therefore, the BT balance of a user in the liquidity mining pool is:

$$balance[user] \equiv \frac{\text{userLiquidity}}{totalLiquidity} * \text{totalLPSupply}$$

*totalLPSupply represents the total amount of BT in the current LPMiningPool. (Each block produces a fixed amount, see chapter 3.1 for details)

It should be noted here that only trading pairs that have been voted and approved by the system will be included in the effective liquidity mining pool and share the income of liquidity mining; all mining shares are priced in ETH.

At the same time, because some trading pairs are relatively unpopular, it is difficult to convert into ETH pricing. Also, it is designed in order to avoid too

small transaction volume and large capital precipitation, which will lead to malicious mining that is unfair to other miners. btSwap sets up an oracle mechanism: in other words, the price of all liquidity priced in ETH is updated by the oracle. The price of the oracle has nothing to do with the transaction price and only affects mining. Therefore, even if the update is not timely, it will not affect the transaction business and has no perception or impact on users.

3.3.2 Provide liquidity (deposit)

When liquidity is provided, the lastDepositBlockNumber will be updated, and this will cause the user's userLiquidity to change (see the 3.3.1 formula for details), so the BT withdrawal action of "withdraw liquidity" will be triggered first, and then all the current liquidity rewards of the user have been withdrawal， this is equivalent to the first deposit for the user this time.

First of all, the provision of liquidity will trigger the trading contract to mint ERC20 tokens. This is some of the logic of other DEXs, so the description will not be repeated here.

Then, if it is not the first time that liquidity is provided, the user’s rewards to the present will be calculated and transferred. The calculation formula is shown in the user’s share in Chapter 3.3.1. At the same time, since the user's liquidity share has been reduced to 0 (because the rewards has been distributed and transferred), the total Liquidity needs to be deducted simultaneously:

$$\text{totalLiquidity} \equiv \text{totalLiquidity} - \text{user}\mathit{Liquidity}$$

Furthermore, as mentioned earlier, while providing liquidity, the lastDepositBlockNumber will be updated to the current block height block.number.

Finally, come to the calculation link:

- Update the user's liquidity balance (note that it is not a share) userEthBalance is the current deposit amount; if it is not the first deposit, userEthBalance = balanceOf(pair)*Ratio, that is, the equivalent amount of transaction pair eth multiplied by the user The proportion of the liquidity pool in the trading pair;

- Update the totalLiquidity. This calculation will be more complicated, because the value will be recalculated every time the liquidity is deposited and withdrawn, that is to say, the block height and the total amount of the system that provided (or withdrawn) liquidity will be saved. According to section 3.3.1, the calculation formula can be drawn:

$$\text{totalLiquidity} \equiv \text{total}Liquidity + (block.number - \text{lastDepositBlockNumber}) * lastBlockTotalEthBalance$$

*lastBlockTotalEthBalance: Indicates the total balance of the liquidity pool denominated in eth during the last liquidity deposit and withdrawal.

So in simple terms, providing liquidity logic mainly does two things:

- If it is not the first time to provide liquidity, calculate the BT rewards of the user's previous liquidity and transfer;

- Update lastDepositBlockNumber, totalLiquidity, lastBlockTotalEthBalance, etc.

Because during the btSwap transaction process, there are fees accumulated and distributed to the user’s share, and the price of the transaction pair will continue to change, so the user’s liquidity balance is changing, and userEthBalance does not update the record, that cause the liquidity balance to be not equal to userEthBalance. The processing for this situation is as follows:

- When users withdraw liquidity (including the logic of providing liquidity that needs to be withdrawn first and then dividends), regardless of the handling fee, the essence is to withdraw its share, and we will first clear its share before recalculating when processing Liquidity, so the userEthBalance can be directly used to calculate the share dividend. Note: The userEthBalance may have changed at this time (because of price changes), but for the liquidity share, the previous userEthBalance is still used;

- When the dividend is completed, the price of the trading pair may have changed at this time, then recalculate the userEthBalance of the user. So although there are fees accumulated in the share, it has no effect on the calculation;

- Due to changes in the price of the trading pair, there will be a certain amount of arbitrage space. For example, the price was 1eth:300token a week ago, and a user deposited 1eth; a week later, the price became 1eth:1200token. According to the calculation of the formula x*y=k of btswap, we can know that the actual balance of the user in the transaction pair at this time is: 0.5eth:600token. Therefore, the actual userEthBalance of the user at this time should be 0.5eth, but we ignore this logic and still calculate it at 1eth (see Article 1), but if the liquidity is deposit and withdraw, it will be recalculated

For example:

Trading pair: ETT/ ETH

Initial price: 1ETH = 1000ETT

userA deposited 1eth and 1000ett for the first time on July 25 to provide liquidity, at this time x*y=1*1000=1000(k) userB sold 1000 ett on July 26, and the remaining liquidity pool is 0.5eth and 2000ett,
x*y=0.5*2000=1000(k)

Assuming that userA plans to deposit 1eth and 4000ett liquidity on July 27th, it needs to pay dividends first. The calculation steps are:

- The userEthBalance of userA is 1eth before the dividend, and the lastBlockTotalEthBalance is also 1eth. But it should be noted that in the liquidity pool, he actually only has 0.5 eth. This is because the price has changed and ett's price decreased doubled;

- According to the previous article, after the dividend is completed, userA's liquidity share has been cleared at this time, so its userEthBalance = balanceOf(PairEthBalance)*Ratio is recalculated. Since there is only one user A in the pool, Ratio=1, and balanceOf (PairEthBalance) is the balance of eth in the trading pair, which is 0.5+1=1.5eth;

- The lastBlockTotalEthBalance also needs to be updated at this time, first deduct 1eth, then add 1.5eth.

According to the example, we can find that if the user does not deposit and withdraw liquidity, it is very beneficial to him, because his balance in the liquidity pool has only 0.5 eth left, but when calculating the dividend, it is still priced at 1 eth. This is also reasonable, because the user initially recharged 1eth, and he contributed to the liquidity pool.

3.3.3 Withdraw liquidity (withdraw)

Withdrawing liquidity is an inverse function of providing liquidity, which triggers the following logic:

- Calculate all the bonus points of the user up to the present
- Tranfer Dividends to users
- According to the amount withdrawn by the user, transfer the corresponding token or eth to the user, and destroy its liquidity share
- Calculate the user's latest liquidity balance (not share) based on the amount withdrawn by the user
- Update lastDepositBlockNumber and totalLiquidity and balance (the method is the same as in chapter 3.3.2)

Most of the steps here are mentioned in chapter 3.3.2, for example, when dividends are paid to users, totalLiquidity needs to be deducted, etc., which will not be repeated here.

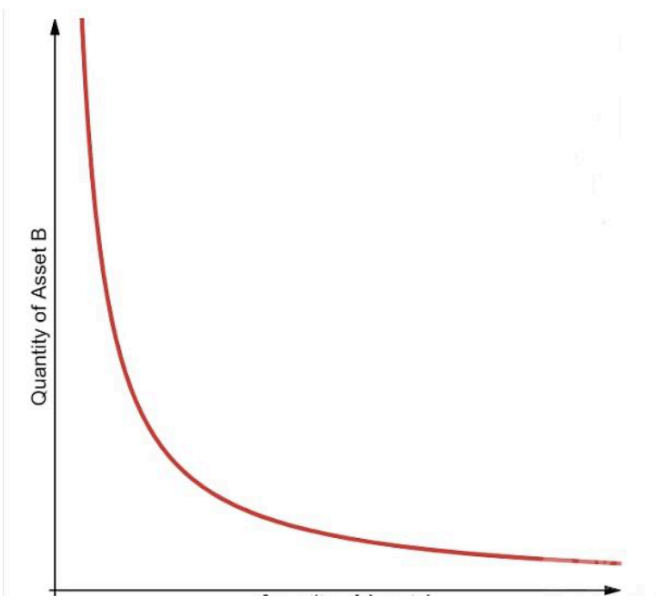
4. Technical parts

4.1 Introduction to Constant Product AMM

The market maker (MM) is the entity responsible for providing prices on the exchange, otherwise there will be a lack of liquidity if there is no trading activity. Market makers buy and sell assets from their own accounts, with the ultimate goal of making profits. Their trading activities create liquidity for other traders and reduce trading slippage.

Automatic Market Makers (AMM) use the algorithm "Money Robots" to simulate price behavior in markets such as DeFi. Although different decentralized exchanges have different designs, AMM-based DEX has always had the largest liquidity and the highest average daily trading volume.

The Constant Product Market Maker (CPMM) is based on the function x*y=k, which determines the price range of two tokens based on the available quantity (liquidity) of each token. When the supply of X increases, the supply of Y must decrease, and vice versa, to keep the product of k unchanged. When a curve is drawn, the result is a hyperbola in which liquidity is always available, but as the price gets higher and higher, the ends will approach infinity.



From Bancor to Uniswap to Curve, and to our btSwap, AMM technology is providing new possibilities for any digital asset to obtain instant liquidity. AMM not only creates prices in previously illiquid markets, but it also does so in a highly secure, accessible and non-custodial manner.

Although AMM has experienced explosive growth, innovations around higher capital efficiency, multiple asset pools, and temporary loss reduction have created the necessary foundation for attracting larger liquidity providers from traditional markets.

4.2 Transaction mining and liquidity mining

DeFi transaction mining and liquidity mining are mainly products that use Ethereum blockchain. It provides liquidity for the DeFi products on the Ethereum to obtain revenue. To put it simply, certain token assets can be deposited for mining. Liquidity mining on Compound mainly involves depositing tokens or lending tokens on it, so as to obtain rewards of COMP tokens.

Liquidity mining on Balancer is to provide liquidity for the token pool of the transaction. For example, to provide liquidity for the BAL-WETH pool, the liquidity provider can deposit BAL and WETH at a certain ratio (such as 80:20) and then according to certain rules, obtain BAL tokens and related transaction fees.

Here, we must first clarify the difference between transaction mining and liquidity mining in the btSwap system:

- Transaction mining: The tokens rewarded to traders who generate transaction behaviors in the btSwap system are equivalent to the income obtained from the consumption of gas fees through trading;

- Liquidity mining: The tokens rewarded to LPs that provide liquidity in the btSwap system are equivalent to providing token assets to obtain income;

Therefore, according to this definition, the above compound belongs to transaction mining, and Balancer belongs to liquid mining. But btSwap isa combination of the two, and there is no pre-mining.

4.3 BT mining arbitrage

According to section 3.2, we can know that the BT balance of a user in the mining pool is constantly changing, and the main factors of change are: transactions generated by oneself and transactions generated by others (total transaction volume), and total supply (Continuous mining output).

Therefore, we can draw the following scenarios:

- After user A generates a transaction, there is no new transaction. If no new users generate transactions, their pool share remains unchanged, but the BT balance continues to increase (mining output);

- If other users generate transactions, but the transaction rate is slower than the mining output, the user’s balance in the mining pool will increase;

- If other users generate transactions, and the transaction volume increases rapidly, the user's balance in the mining pool will decrease.

Therefore, users can keep the BT without withdrawal to increase its value when the transaction volume grows slowly, or quickly withdraw it in the scenario of rapid transaction volume growth to ensure the maximizationof their own profits.

Conversely, if a user finds that the trading pool has a large balance, he can initiate a large-value transaction to quickly occupy a certain share of the mining pool and withdraw, thus maximizing the benefits.

These all belong to the existing BT mining arbitrage space, which is specifically selected and handled by the user.

4.4 On-chain oracle

Blockchain can interact safely and transparently on chain through smart contracts. However, blockchain is not the Utopia. After all, blockchain needs to interact with real-world data. In many scenarios on the blockchain, smart contract applications must obtain information sources outside the chain and perform data interaction inside and outside the chain to trigger their logical judgments.

ChainLink is currently the leader of the oracle track. Its customers include the world's top Internet companies such as Google and Oracle, as well as many projects in the industry. Its operating mechanism is that 21 off-chain nodes provide quotations, and submit the data to the smart contract on the chain, aggregate data within the contract, and obtain the final quotation data. Therefore, its biggest problem may be that the quotation mechanism is controlled by the reputation of the node and the pledge token, which is easy to be manipulated.

Another well-known oracle project is NEST, which can be understood as a decentralized game theory mechanism to achieve quotation. The NEST oracle program adopts a new idea of reverse verification. Quotation miners need to use real money to participate in the quotation, instead of uploading price data to the on-chain contract, so it is more decentralized and less easy to be manipulated.

Therefore, the essence of the on-chain oracle is the price after the game between traders. From this point of view, btSwap is a natural price prediction machine that can provide very real-time and accurate transaction price changes.

Therefore, btSwap plans to increase the oracle function after the traffic is gathered to provide real, timely and effective prices for projects on the chain that require quotation.

5. Summary

According to the above introduction, we can know that the user's withdrawal in btSwap is no different from Uniswap and Bancor, but the transaction mining and liquidity mining functions have been added, and the transaction fee has been reduced (initially 0.02%), Therefore, users are more motivated to trade here and provide liquidity.

At the same time, the initial stage of the project is completely zero pre-mining, and all tokens are slowly produced through mining. The fee ratio is also corrected by the oracle machine through the later token voting, so that the token will slowly generate ecological management value.

To sum up, btSwap is a highly innovative DeFi project that combines the advantages of the current DEXes on the market and the characteristics of the centralized exchange platform currency.

6. Disclaimer

- All examples of data, announcements, income and profits in this document are for reference only, or represent industry averages, and do not constitute a guarantee for user participation results and investment.

- Digital asset investment is a new investment model with various risks. Potential investors need to carefully evaluate investment risks and participate within their own risk tolerance. Once investors participate in the investment, they understand and accept the risks of the project, and is willing to personally bear all corresponding results or consequences for this.

- This document and any other documents or materials provided are only for the purpose of conveying information. They are not intended as and should not be regarded as the basis for any investment decision, or specific advice, consultation or solicitation, and should not be construed as any sale, purchase or subscription invitation, and shall not be interpreted in this way.

7. Reference

- Bitcoin Whitepaper:https://bitcoin.org/bitcoin.pdf
- Ethereum Whitepaper:https://ethereum.org/en/whitepaper/
- Uniswap Whitepaper:https://uniswap.org/whitepaper.pdf
- Bancor Whitepaper: https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf
- AMPL:https://www.ampleforth.org/