ACY Finance WhitePaper

Writtened by **ACY Core Contributers**

0 Introduction

ACY Finance is an anti-robot DEX. ACY invents Flash Arbitrage, a protocol level implementation that executes to reduce the arbitrage activities of miners and other kinds of arbitrage robots in each transaction.

Our smart contract will split user's swap transaction into multi-route arbitrage transaction inside the same swap transaction. Users can then automatically profit from the arbitrages, enjoy the lower price slippage and more stable price. Without big enough arbitrage opportunities, arbitragers including the miners' bots will be disinterested in swap transactions from our platform.

What's more, Flash Arbitrage is executed using a mathematical model to calculate the most optimal routes during runtime, aka during transaction execution. Unlike 1inch and other platforms where they calculate the routing solutions before they do the swap transaction, ACY Finance has no delay and is more accurate for its protocol level implementation of the algorithm.

Flash Arbitrage is a creation invented to help promote a fair competition for users by ACY Finance. Which is why we wanted our solution to be Anti-MEV but also Anti-corruption to fight against the robots. In this new world created by ACY, the interest of both Traders and Liquidity Providers will be appreciated.

1 Background

1-1 Arbitrage

DEX is the crown jewel in the field of Defi. Starting from AMM of Uniswap V2, users on blockchain can initiate asset transactions anytime without worrying about the absence of transaction counterparties. This greatly enhances the liquidity of assets on the chain as well as user-experience. However, the problems brought about by AMM are trading slippage and impermanent loss, which is embodied in the close relationship between the price fluctuation of trading pairs and the volume of liquidity funds. Once liquidity is insufficient, users will bear considerable losses.

Who benefited from the losses? The answer is the arbitrageurs. In an ideal state, users exchange token A for token B, and the price should remain the same regardless of the way and route of exchanges. However, that is not the reality. If only one transaction pair is used for token exchange, the AMM algorithm will raise the price to a very high position because of the limited amount of liquidity funds in the transaction pair. If the user exchanges token B at this price, the arbitrageur would exchange token A for token B through other channels, and then sell at this price.

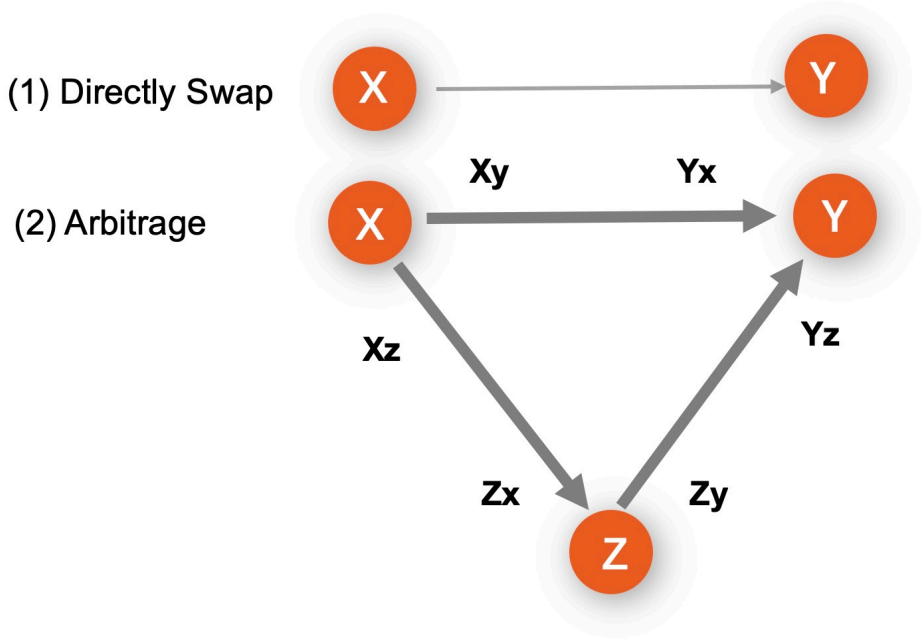

Fig. 1 Triangular Arbitrage in DEX

A considerable amount of profits can be gained this way. As shown in the figure below, the arbitrageur can frequently find arbitrage opportunities brought by the price difference between different trading pairs and obtain profits. In fact, the source of these profits is the losses borne by users who trade through DEX.

1-2 MEV

In the past, MEV robots were invincible and the interests of users and liquidity providers were damaged. How is it possible for Miner Bots to extract values from our transactions? The essential reasons for the on-chain attack lies in the design of the blockchain.

The first reason is the mempool design of the blockchain. After users have submitted their transactions to the network, these transactions are not directly appended to the block. Instead, they will be buffered in the mempool. Therefore, the transactions inside mempool are pending transactions. This is where miners do harmful behaviors because miners are given the access to monitor and review the transaction inside the mempool, then they can select the ones they preferred to execute in gas-priority order, which should have been the case. But MEV is the rule breaker, it refers to the value miners can obtain from exploiting their power to determine the arrangement of transactions in a block, often at the expense of users.

Secondly, the time gap between each block generation opportunities for the attackers. According to Etherscan, the current average block generation time of Ethereum is 13s, which means miners are given more than enough time to reorder, insert, or drop transactions to initiate front-running, back-running, sandwich, time zone and etc attacks to gain MEV.

1-3 Single Asset Liquidity

Some DEX began to try to avoid such losses through the mechanism of Single Asset Liquidity Providing. All tokens can form trading pairs with tokens issued by DEX, and subsequently create a network of a star topology.

However, the key of Single Asset Liquidity Providing lies in the tokens issued by DEX. The price fluctuation and issuance model of this token will seriously affect the normal operation of the whole DEX ecosystem. Flaws in mechanism design will also lead to hacker attacks. In addition, there are mechanisms to introduce other exchange prices through Oracles (such as Uniswap V3, etc.), but these complex mechanisms can not balance the trading slippage and impermanent losses well.

1-4 Our Proposing Solution

The best solution is to allow users to take advantage of the arbitrage opportunity each time after the swap transaction. However, this is difficult to achieve. On the one hand, not every user has enough time and ability to complete the arbitrage transaction by himself; on the other hand, it is difficult for users to seize the opportunity before professional arbitrageurs.

Fortunately, the atomicity of smart contracts solves the second problem. If users' normal transactions and arbitrage transactions are both placed in one single transaction to call a contract function, no other users can insert the transactions into them.

By splitting the swap transaction into multiple smaller routes using different liquidity pools, the price slippage on swap transactions will be lower and price will be more stable.

2 Relative Work

There are some projects trying to solve these problem. Uniswap propose the "Slippage Tolerance" and "Minimum Receive Token" to prevent the sandwich attack, which can protect the revenue of the trader.

For the arbitrage attack, 1inch tried to solve this problem with PathFinder algorithm.

The idea lies in allocating the source tokens input by users to different paths and exchanging them with the target tokens, which can effectively avoid the price fluctuation and arbitrage space caused by token exchange on a single path.

1inch uses a more complex dynamic programming algorithm to solve the multi-path allocation problem of token. Due to the limitation of gas fee, this part of calculation can only be performed in the way of view function (without consuming gas fee). After the calculation is completed, the result is sent to the function for a specific token swap process. In this way, the path searches and exchange execution are split into two executions, during which market fluctuations and even malicious attacks may cause the exchange to be not a good solution, which brings potential risks to traders.

The Flash Arbitrage proposed by ACY puts the path searches and exchange execution in one transaction, and ensures that the exchange executed is a good solution to the search at that time. In order to solve the gas fee problem, the Flash Arbitrage does not adopt the dynamic programming algorithm, but models the whole problem as an optimization problem in mathematics, and quickly obtains an approximate solution through the mathematical model.

3 Flash Arbitrage

The specific scheme of FlashArbitrage is shown in the following figure. Instead of the direct exchange for the target token by users, the ACY contract is automatically split into multiple paths to exchange the target token. The liquidity equivalent to this exchange is the sum of the liquidity of all relevant paths, which can help users obtain arbitrage gains and greatly reduce the trading slippage.

To maximize the arbitrage profit, we establish a model to calculate the ratio of different routes.

3-1 Mathematical Walkthrough

Assume we want to use ΔX to exchange ΔY. One of the Triangular Arbitrage opportunity is to use some token X to exchange for some token Z, and subsequently exchange this for some Y.

The optimal relationship is given as following:

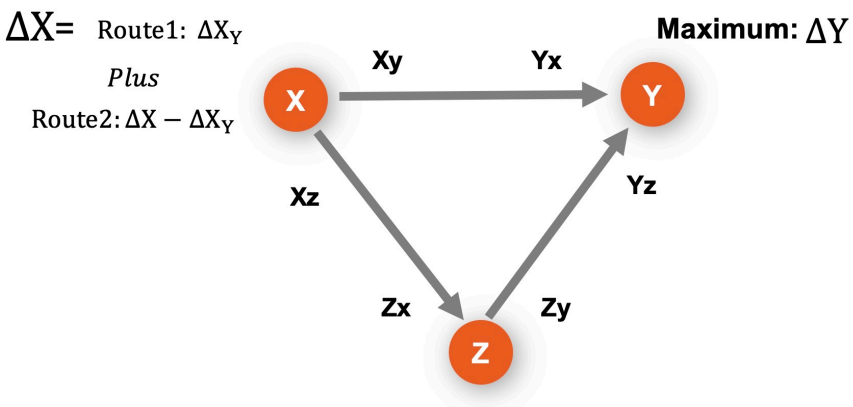

Fig.3 The Optimal Distribution

Variables are given below:

$\mathbb{Z}_x$: Total Z token amount in the X/Z pool

$\mathbb{Z}_y$: Total Z token amount in the Y/Z pool

X_z: Total X token amount in the X/Z pool

Y_x: Total Y token amount in the Y/Z pool

X: Total X token amount in the X/Y pool

Y: Total Y token amount in the X/Y pool

C: 1 - TransactionFees

P: The price of **X** per **Y** by using ΔX to exchange ΔY in X/Y pool

P_{arb}: The price of x per y by using ΔX_z to exchange ΔZ_x in X/Z pool, and subsequently using this to exchange ΔY_z in Y/Z pool

$$\Delta Z_x = Z_x(\Delta X_z)C/(X_z + C\Delta X_z)$$
$$\Delta Y_z = Y_z(\Delta Z_y)C/(Z_y + \Delta Z_y C)$$

Set $\Delta Z_x = \Delta Z_y$,

$$\Delta Y_z = Y_z C\Delta Z_x/(Z_y + C\Delta Z_x)$$
$$\Delta Y_z = \frac{Y_z C(Z_x C\Delta X_z)/(X_z + C\Delta X_z)}{Z_y + C(Z_x C\Delta X_z)/(X + C\Delta X_z)}$$
$$\Delta Y_z = \frac{Y_z(C^2 Z_x)\Delta X_z/(X_z + C\Delta X_z)}{Z_y + (C^2 Z_x)\Delta X_z/(X + C\Delta X_z)}$$

Set $R = (C^2 Z_x)\Delta X_z/(X_z + C\Delta X_z)$

$$\Delta Y_z = \frac{Y_z}{(Z_y/R) + 1}$$
$$P_{arb} = \frac{C\Delta X_z}{\Delta Y_z} = \frac{C\Delta X_z[(Z_y/R) + 1]}{Y_z}$$
$$P = \frac{C\Delta X}{\Delta Y} = \frac{X + C\Delta X}{Y}$$

No arbitrage theory: $P_{arb} = P$

$$\frac{C\Delta X_z[(Z_y/R)+1]}{Y_z}=\frac{X+C\Delta X}{Y}$$
$$C\Delta X_z[(Z_y/R)+1]=\frac{X+C\Delta X}{Y/Y_z}(1)$$
$$\frac{Z_y}{R}+1=\frac{Z_y(X_z+C\Delta X_z)+C^2Z_x\Delta X_z}{C^2Z_x\Delta X_z}$$
$$\frac{Z_y}{R}+1=\frac{(Z_yX_z/\Delta X)+Z_yC+C^2Z_x}{C^2Z_x}(2)$$

By Inserting the result from equation (2) into equation (1) we can get

$$\frac{Z_yX_z+(Z_yC+C^2Z_x)\Delta X_z}{CZ_x}=\frac{X+C\Delta X}{Y/Y_z}$$
$$\frac{Z_yX_z}{CZ_x}+\frac{(Z_yC+C^2Z_x)}{CZ_x}\Delta X_z=\frac{X+C\Delta X}{Y/Y_z}$$
$$\Delta X_z=[\frac{X+\Delta X}{Y/Y_z}-\frac{Z_yX_z}{CZ_x}]\frac{Z_x}{(Z_y+CZ_x)}(3)$$

Equation (3) gives the proportion of token X that should be exchanged into token Z and then into token Y. Moreover, $\Delta X_{total}=\Delta X_a+\Delta X_b+\ldots+\Delta X_z$, while A, B, ..., Z are the tokens used in arbitrages. Based on the aforementioned equations, the optimal solution of flash arbitrage can be solved for.

3-2 Multi-Routing Flash Arbitrage

In the basic version, we consider only one intermediate currency, only one hand is turned, and the arbitrage space can be completely smoothed out. In the Pro version, we use a different mathematical modeling approach to solve optimization problems that allow for multiple intermediate currencies and situations where the arbitrage space cannot be completely smoothed out. That is, in the Pro version, we provide a global optimal solution that guarantees traders a minimum slip point consistent with the theoretical value

4 Tokenomics

In ACY's design, most of the gains from Flash Arbitrage are returned to users, and the remaining part rewarded to liquidity providers. In this way, compared with similar DEXes such as UniSwap, PancakeSwap and SushiSwap, ACY can provide lower trading slippage on the one hand, higher liquidity mining return rate on the other hand, and quickly attract users and liquidity providers to join ACY Finance.

4-1 Token Distributions

Our **200,000,000 (200Million)** ACY Tokens are distributed as follows:

1. **20% for Contributors** - 40,000,000 (40 million)*These tokens are rewards for the hard work of the developers, designers, managers, and other team members behind ACY Finance.*
2. **15% for ACY Foundation** - 30,000,000 (30 million)*ACY Foundation is a non-profit organization to facilitate decentralised decision-making within ACY Finance. Funds are used to realise community suggestions for the project, which have received approval from the board.*
3. **20% for Institutional Investors** - 40,000,000 (40 million)*Institutional investors are companies or organisations, such as Venture Capitals, who hold our tokens through private sales.*
4. **15% for Marketing** - 30,000,000 (30 million)*These include IDOs and airdrops. We are currently holding our first IDO with Hippo Finance, with several others in the pipeline. Airdrops will be streamed until all allocated funds are exhausted.*
5. **20% for Providers and Users** - 40,000,000 (40 million)
   Transaction Fees for liquidity providers are distributed in ACY Tokens. Users and Liquidity Providers also have another source of income which is from our Flash Arbitrage, which could be multiple times of the income from liquidity mining. More details of Flash Arbitrage revenue can be found below.
6. **10% for Ecosystem Fund** - 20,000,000 (20 million)
   This provision is to reflect our commitment to the development of our project's ecosystem by integration or collaboration. Use case examples are sponsorships for hackathons, bounty awards for bug finding or solving, and grants for developer communities.

4-2 Flash Arbitrage Revenue

Recipient	Percentage	Token
Trader	30%	Target Token
	10%	ACY
Liquidity Provider	20%	LP trading pair, Each 10%
	10%	ACY
Staker	20%	10% ETH & 10% BTC
Ecosystem Fund	10%	5% ETH & 5% BTC

- Flash Arbitrage Revenue will be distributed to Traders (40%), Liquidity Providers (30%), Stakers (20%), and Ecosystem Fund (10%).
- 50% of Flash Arbitrage Revenue will remain in the trading pair tokens, 20% is used to purchase ACY tokens, the remaining 30% is used to purchase ETH & BTC.

4-3 Transaction Fee

Directly goes to Liquidity Provider, 0.3% of each transaction.

5 ACY DAO Governance Model

At ACY Finance, we value the independence and fairness of a decentralized governance network, and therefore we endorse a Staking DAO governance model to govern the ACY Decentralized Autonomous Organization (heretofore remarked as the ACY DAO).

5-1 ACY DAO Overview

The main purpose of the ACY DAO Governance Model is to provide a regulatory structure to govern the ACY DAO in a manner that fulfils the three objectives we believe are critical to achieving fair, independent, and resilient community.

1. Community Empowerment: To ensure our community has the opportunity and ability to be fairly represented on topics meaningful and relevant to themselves.
2. Transparency: To ensure maximum viable transparency on all voting as well as the post-vote execution of decisions.
3. Security & Stability: To ensure that the previous two objectives can be carried out whilst maintaining an adequate level of security and stability for ACY Finance

5-1-1 ACY Broad and Meaningful Representation

ACY holders are the centrepiece of ACY Finance, and so in order to best reflect the interests and values of our community, we have designed the key governance structure around the ability to have inputs from our member.

For example ACY holders will vote on deciding how the Flash Arbitrage Revenue will be allocated to maximize growth.

By receiving constant inputs from the community, we ensure that we not only empower our members with the ability to make fundamental decisions on our parameters for various scenarios, we will also ensure that the strategies we adopt will be more robust and sustainable with the ultimate goal of driving long term growth.

5-1-2 Transparency and Stability

The ACYDAO is designed for maximum viable transparency, network stability and quick recovery in cases of emergencies. The ACY team will serve as the current maintainer of the ACYDAO. We believe it is important to build the system to be as verifiable as possible while being transparent and clear about our role in the DAO.

All processes and data will be stored and processed on-chain where feasible. For example, once the voting for flash arbitrage revenue allocation ratio is concluded, it will be executed on-chain and no one will be able to change that. Where it is not practical, there will be a set of robust off-chain community and governance processes to ensure that DAO decisions are followed through.

Given that ACY is an important part of the decentralized infrastructure, network stability is crucial for the hundreds of DApps and reserves that depend on us. To reduce spamming and abuse, the ACY team will take on certain key roles, including putting up proposals for voting, protecting against malicious activities.

It is important to note that changes can be monitored by the community since these operations will be done fully on-chain where feasible.

5-1-3 Evolving Governance

As the current DAO maintainer, we take the role of facilitating discussions, driving open and transparent decision making, and executing (and following through) the formal DAO processes very seriously.

If we perform this balance well, our legitimacy will continue to grow, participation will increase, and the community's understanding of the key operations will be sufficient to allow us to gradually move more operations towards DAO votes, including network features, technical upgrades or protocol upgrade decisions.

We believe that this progressive decentralization achieves the main goals of **broad representation, transparency, resilience, and network stability** — and we would love to work with the community to continuously improve both the on-chain and off-chain processes as we continue to evolve.

5-2 Staking, Voting, And Reward

In this section, we describe the key concepts and mechanisms behind staking and voting, as well as provide an example of how these work together. Staking, voting, and claiming of rewards all require gas.

5-2-1 Staking

Staking ACY Tokens will give users the ability to vote for governance, Earn Rewards from Governance Profit, Enjoy our Pro version Access (1000 ACY Tokens).

5-2-2 Epochs

Staking and voting are done in epochs, which just means fixed periods of voting time, denominated in Ethereum block times. One ACYDAO epoch period will last about 2 weeks before the next one begins.

The benefits of this short epoch period are faster reward distribution and DAO conclusion (hence faster decision-making). The cons are that there needs to be at least one voting campaign every 2 weeks, resulting in more work for the ACY team, as well as more frequent participation required from ACY Token stakers.

In every epoch, there will be one or more campaigns, and each campaign will have several options. It is important that voters vote for all the campaigns since they only receive rewards for campaigns that they voted in.

5-2-3 Delegation

We expect busy stakers to delegate their voting power to 3rd party “pools” to vote on their behalf, with these pools being able to dictate their fees and independent voting decisions. Since they are expected to share in the rewards. and their voting decisions will be fully transparent on-chain, they are expected to both be proactive in voting as well as communicating on the rationale of their decisions.

This is an important part of the ACYDAO setup, and we expect to have a range of options for ACY Token stakeholders, both in terms of their preferred method of delegation as well as types of staking partners.

5-2-4 Reward Distribution For Individual ACY Holders

The reward distribution is designed to incentivize stakers to vote in **all the campaigns**.

After every epoch, there will be BTC & ETH set aside for voting rewards(More details in the next section). The total amount of rewards is decided by a few main factors: flash arbitrage revenue decided in the previous epoch, and proportion of revenue allocated for voting rewards. The revenue allocation ratio are decided by the ACYDAO.

As an individual ACY Token staker, your share of the rewards received after the epoch will be determined by your voting points (the amount of ACY you have staked during the epoch x the number of campaigns you voted on), in proportion to the total voting points of all ACY Token stakers.

Name	Calculations
Available Rewards	Flash Arbitrage Revenue * Ratio allocated to rewards
Your Voting Points	Your ACY staked * Numbers of Campaigns Voted On
Your Share	Your Voting Points / Voting Points of All Stakers
Your Reward	Your Share * Available Rewards

Assuming you (and all the other stakers) voted for all the campaigns in that epoch, your share will be proportionate to your ACY staked vs. the total amount of ACY staked by all. If you as a ACY staker did not vote, you would not receive any rewards. If you only voted for one but not all the campaigns in that epoch, you would receive less than what you actually could have.

5-2-5 Rewards in BTC and ETH

The Rewards will be presented to users in BTC and ETH, we will purchase BTC and ETH. Because Our Flash Arbitrage is actual protocol profits we generated from our swap transactions, the revenue will be used to purchase the most iconic tokens in crypto, BTC and ETH, and use it to reward our stakers.

5-3 Staking And Delegation Options

One of the most important considerations is to make ACYDAO participation as easy as possible. We want to allow ACY stakers who are unable or have limited resources to participate in every ACYDAO vote to still receive rewards for staking, while providing the resources for others to vote on their behalf.

At launch, there will be several options for users to stake, vote or delegate, depending on their ability to participate and their preferences for the type of experience they prefer (for example between custodial and decentralized solutions).

5-3-1 dao.acy.finance: The Default DAO Interface

The default way to stake and vote ACY is through our main ACYDAO interface. The ACYDAO will be hosted on the domain dao.acy.finance and this will be the main staking and voting interface for the ACY Finance community to participate in governance.

To stake ACY and vote on the ACYDAO, ACY holders will need to connect their wallet and spend gas on all on-chain actions.

5-3-2 Delegating your ACY voting power to Staking Pools or someone else

ACY stakers who do not wish to vote, but still want a share of rewards, can delegate their ACY voting power to a 3rd party address/ “pool master” who will vote on their behalf. They will be able to do so on the official ACYDAO.org interface.

ACY holders retain full control of their ACY and will be able to be withdrawn or re-delegated anytime. They have to delegate their full stake (no partial stake) and can only delegate their stake to one pool at any time.

The Flash Arbitrage rewards will be given to the 3rd party pool master. The pool master will then need to calculate the reward allocated to each of their pool members and have a mechanism for them to claim their rewards after. Although ACYDAO does not track or manage the distribution of the rewards, rewards due to individual members are fully recorded on-chain.

6 Roadmap

Our Platform has aimed to provide the best in class DEX product for our users, and the roadmap is as follows:

- Testnet version: This is the version with the basic capability of doing swaps and liquidity adding on the platform. It will come along with our ACY DAO platform for early governance participants to govern our platform.
- Mainnet Version: This Mainnet version will be launched after our perfection with all the feedbacks during the testnet period. It will be fully capable of launching flash arbitrage swaps and users will earn benefits with the platform by enjoying the stable pricing and extra arbitrage incomes.

- Pro Version: The Mainnet version will be equipped with basic version of Flash arbitrage which is Bi-routing Flash Aribtrage. The Pro version will equiped with the most optimized flash arbitrage solution using multi-routing Flash Arbitrage algorithm. To access to pro version, the users will be required to hold 1000 ACY tokens.
- IDO capability: IDO pipeline will be implemented in this milestone, and we would welcome all projects to do IDO on our platform after a reviewing session on ACY DAO.
- API/SDK for users and projects: Our Project will never stop at just developing our ecosystem, we would love to provide our services to other projects and platforms to build on top of us.

7 Conclusion

The open and transparent nature of blockchain brings security and traceability to users, while exposing users' privacy to malicious attackers. On the other hand, miners get block rewards and handling fees through submitting transactions, and the transaction order is not much different in the UTXO transaction model of Ethereum. However, under the model of Ethereum smart contract, the different transaction order will lead to different contract execution. But this was not exposed in the early stage, so Ethereum did not give corresponding improvement measures. With the popularity of DeFi, there are a lot of profit margins, and miners' right to order transactions becomes more important.

ACY believes that miners can get corresponding profits when they finish packing and executing transactions, but it is inappropriate to get excess profits by adjusting the order. For chain data with the same amount of computation and storage space, it is not appropriate for miners to treat them differently because of different token values. Just as we require the Internet to meet the principle of "net neutrality", Internet operators (ISPs) provide equal services to network customers and information flows without discrimination. We should also require blockchain miners to provide equal services for user transactions, which ACY guarantees to a certain extent through agreements. If miners don't change, ACY will change miners.