DAOSWAP Whiter Paper

DAOSWAP: DEX for DAO Organization

The Internet is forming a monopoly and decentralized finance (DEFI) is creating an endless bubble! What is the future of the Internet, and where is the way out for DEFI?

DAOSWAP's core team believes that the future of the Internet is in blockchain, the future of blockchain is in DEFI, and the future of DEFI is the fusion of DEX (Decentralized Exchange)+NFT(Non-fungible Token)+DAO (decentralized autonomous organization).

Because only blockchain can provide liquidity for value not just information, and the foundation of value liquidity is DEFI and DEFI cannot be landed without the integration of DEX+NFT+DAO.

1, The future of the Internet is in blockchain

We spend an average of six hours a day on the Internet, sending messages, browsing news & pages, transferring files, watching videos, sending emails etc. What we do on internet is transmitting information. This is also the greatest value of the Internet, bringing disruptive ways of information interaction to human beings. For last decade humans have generated more data than the total of human history.

The value generated by our activities on the Internet gathering into an ocean of "Internet", but only a very few groups (centralized platforms and companies of all kinds) can profit from this ocean. They have built the dam of Internet monopoly, forming a "dammed lake" of digital value in which only they can use and capture the traces of people's behavior without compensation.

Today, the Internet has reached a bottleneck in its development, because:

1. Internet only solves the problem of information interaction, and its infrastructure all built on a centralized system, which makes it impossible to solve the "double spending" problem. The value generated by information is monopolized in the hands of a few centralized groups, and they are forming an age of surveillance capitalism.
2. The value of assets such as money, property, cars, stocks, intellectual property, insurance, accounts receivable, etc., cannot be freely transferred on the Internet. For example, if I want to transfer my money to the other side of the world, I need to go through a series of centralized clearing and settlement systems before I can do so. Not to mention that I want to

transfer my property to another person across the ocean, which will be a long and frustrating process.

The future of Internet development lies in blockchain because it solves the problem of decentralized information and value transfer.

After the financial crisis in 2008, blockchain exploded with great vitality during constant blows. The fundamental reason is that it makes information and value flow freely in the world of data and has **opened the first entry in the dam of digital value.**

2, The future of blockchain is in DEFI

The boom in blockchain must be predicated on the boom in decentralized finance (DEFI) because:

1. Digital value needs to flow in the " dammed lake" where digital value has been gathered for decades. The failure of P2P is a typical proof.
2. Blockchain is the best choice for value flow, and the most direct manifestation of value is finance.

Blockchain is to today's world as the Internet was to the world in 2000. Business models based on information such as blogging, social networking and e-commerce have just proven its success, and the prosperity of the Internet today is built based on the prosperity of these fields first.

DEFI is also proving its success in the field of blockchain, and the future prosperity of blockchain will certainly be based on the prosperity of DEFI, which is the **second opening in the dam of digital value.**

3, The future of DEFI is the fusion of DEX+NFT+DAO

Finance is to serve the real economy through financial instruments, but capital in today's DEFI is not serving economy, only speculation. If this situation not improved, DEFI will only become a "bubble machine" to produce numerous bubbles without market rules.

How to solve the dilemma? First of all, the real economy is divided into two categories: traditional real economy and digital economy, the traditional real economy digitalization has a long time to go, while the digital economy is born in the digital world with digital value. Therefore, from the category point of

view, DEFI's main service target will be the digital economy, and the digital economy must build on three major foundations:

1. Digitization of asset (NFT).
2. Collaborative models of value creation (DAO).
3. Decentralized exchange market (DEX).

3.1, Digitization of asset (NFT)

BTC, ETH, UNI and other fungible crypto digital currencies (FT) represent equity, similar to stocks, options, currencies, etc. They are all fungible. There is no difference between your 1 BTC and my 1 BTC, they can be exchanged one for one.

In addition to economic activities, more assets are embodied in the form of property rights, such as property, land, digital copyrights, codes, etc., which are all non-fungible. One of your estates and one of my estates cannot is completely different and cannot be exchanged one for one. The property rights of these assets in the data world cannot be expressed in FT, they need unique, tamper proofing and self-evident credentials.

This is what we are going to say about non-fungible tokens (NFT), which have unique, tamper proofing, tradable, traceable, and programmable properties that allow them to effectively represent the property rights of arbitrary assets in the digital world.

In this way, we can freely exchange property rights in the digital world. With the digital property rights, DEFI will have the actual "subject matter" to serve the digital economy through financial instruments like mortgages and guarantees.

3.2, Collaboration model of value creation (DAO)

Most successful projects in the blockchain today like BTC, Ether, Uniswap, etc., were not created by companies, and over 90% of the Internet's infrastructure was not invented by companies neither. They were all invented by a group of community contributors who collaborate with each other not through a company, but through an open-source community model.

The corporate system can no longer meet the value creation of the digital economy, a new model is needed to organize contributors to create value. This open-source community model has two major fatal flaws:

1. No governance mechanism, loose cooperation, the contribution generated cannot be quantified.
2. No protection mechanism, open-source results were freely used by company and profit from it, but open-source contributors almost no revenue.

Open-source communities have suffered from this drawback for decades, and it is in this context that the decentralized autonomous organization (DAO) model was born, i.e., a decentralized model to collaborate, self-govern, contribute and be able to make a profit. The DAO model is also becoming the mainstream form of value creation in the digital economy

3.3, Decentralized exchange market (DEX).

While value flows in the real world are conducted through centralized platforms such as NASDAQ, SSE, and SZSE, the digital economy requires new decentralized trading venues due to the liquidity of its value and the decentralization of its subjects. And such decentralized exchanges (DEX) have also matured in recent years.

In summary, the prosperity of the digital economy cannot be separated from freely flowing assets (NFT), new forms of collaboration (DAO) to continue generating value and decentralized exchanges (DEX).
The fusion of DEX+NFT+DAO will be the **third opening in the dam of digital value.**

4, DAOSWAP, DEX for DAO organization

NFT and DAO are not new concepts, they have been developed for several years and they rely on the building of many blockchain foundations such as public chain computing, public chain storage, tokens, decentralized governance mechanisms, DEFI, etc. The reason NFT and DAO started to explode in 2021 is because we:

- Saw the gradual maturation of public chains such as Ether.
- Saw the unstoppable momentum of cryptocurrencies and algorithmic currencies such as BTC.
- Saw the emergence of public chain storage technologies such as FIL, SWARM, etc.
- Saw the boom of autonomous market maker (AMM) DEX such as Uniswap.
- More importantly, we have seen DAO and NFT begin to have the

possibility of making blockchain truly landed, and the Internet of value for the real digital economy is taking shape.

It will take time for DAO and NFT to mature, and when the melons ripen and fall in 3 or 10 years, those who can really catch these melons can only be the infrastructure providers mentioned above, because they have paved the way, so they can harvest. These infrastructures are built with very high technical, resource and cognitive entry.

Open-source communities have been popular since the 1990s, and everyone gathered for the same dream, which is to be free to start and survive without relying on centralized means such as companies. They are the germ of DAO organizations, but due to the failure to solve the basic problems of contribution quantification, governance decentralization and financial liquidity, open-source communities have been in the embarrassing situation of only contribute but no gain.

The explosion of DEX in 2018 lighted the dream of this group of people, the emergence of DAO has made the route clearer and made it possible to quantify contributions as financial liquidity.

3, Brief Introduction

Daoswap is a financial platform based on AMM, applying multiple chain technology and compatible for polymorphic assets. Our vision is: 1, Build

DEFI for everyone; 2, Build DEFI for real economy. Our roadmap is to applying DEX+DAO+NFT, solve the problem of “Human Resource” and “Finance” for startup DAO projects. Daoswap created ALP+AMM to make go public before start business come true.

The core contributors of DAOSWAP are from this group of people who had dreams about DAO in the early days, and with their respective professional accumulation in the fields of finance, blockchain and sociology. They integrate DEX+DAO+NFT to realize the dream of going public before starting a business.

DAOSWAP's core contributors that is, idealistic dream makers, but also realistic practitioners, want to achieve the future dream must lay a good foundation in the present. The following three steps of dreaming cannot be missing.

- DEX: first from DEX to pave the way for a decentralized financial base more conducive to NFT, DAO organizations.
- NFT: then compatible with the full range of assets such as NFT to expand the financial base.
- DAO: finally provide DAO organizations with innovative contribution that is mining mechanism to achieve listing before starting a business, what you do is what you get.

DAOSWAP 1.0 starts with financial base DEX, ecologically Ether-based fusion of multi-chain and second-layer technology, and liquidity with self-action market model. Fundamentally solve the liquidity problem, subvert the traditional order-book exchange model and all the rights of centralized trading, open all the rights to project parties, and truly use blockchain to provide a guaranteed liquidity market for innovative projects.

Most exchanges maintain an order book and facilitate matches between buyers and sellers. DaoSwap smart contracts hold liquidity reserves of various tokens, and trades are executed directly against these reserves. Prices are set automatically using the constant product (x*y=k) market maker mechanism, which keeps overall reserves in relative equilibrium. Reserves are pooled between a network of liquidity providers who supply the system with tokens in exchange for a proportional share of transaction fees.

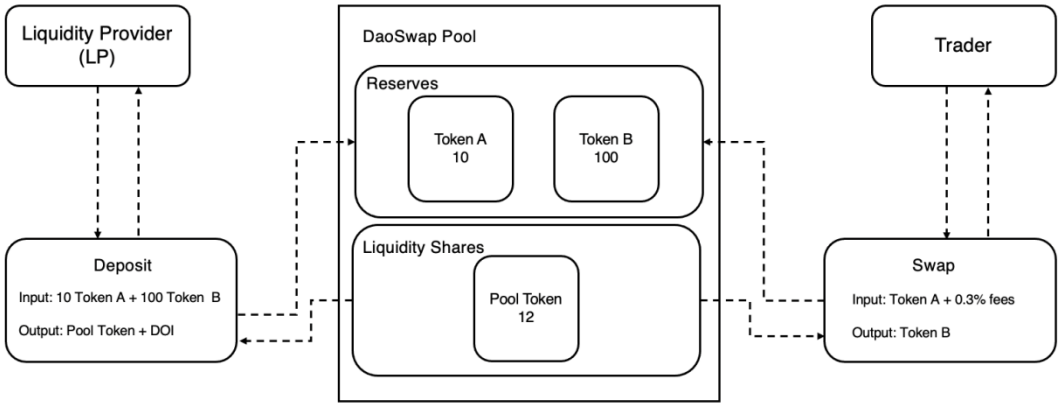
The decentralized applications (DApps) by DaoSwap are initialized or built on the Ethereum blockchain, a distributed ledger. This will lead to the exclusion of the influence of unauthorized persons. The copy of transaction details and investment data is available in every node on the blockchain that is present in the nooks and corners of the world. This will eliminate forced shutdown or censorship of the DaoSwap system. And also, an important thing to note is

since investment details are distributed among thousands of users(nodes) there is no possible way to tamper your data. If anyone needs to modify, the data in every single node has to be overwritten which is practically impossible. This is why DaoSwap is secured over the traditional investment systems.

1, Multi-chain integration
Ethernet main network is the main one, integrating HECO, BSC, and the latest layer 2 technology to provide full chain ecological services.
2, Serve entities
The first automatic liquidity ALP model, compatible with the governance of DAO projects, the flow of NFT, tapping the long tail demand of Defi, and truly serving the entity's native digital economy.
3, Efficient and low cost
Achieve centralized efficiency and decentralized security, with fees as low as 0.01 USDT.
4, Decentralized autonomy
The project runs in community autonomy mode, all code is open source and published, and the whole chain is decentralized.

Who is supporting us?
Gitcoin
Medium
Uniswap

4, How DaoSwap works



DaoSwap is an *automated liquidity protocol* powered by a constant product formula and implemented in a system of non-upgradeable smart contracts on the Ethereum blockchain. It obviates the need for trusted intermediaries, prioritizing **decentralization**, **censorship resistance**, and **security**. DaoSwap is **open-source software** licensed under the GPL.

Each DaoSwap smart contract, or pair, manages a liquidity pool made up of reserves of two ERC-20 tokens.

Anyone can become a liquidity provider for a pool by depositing an equivalent value of each underlying token in return for pool tokens. These tokens track pro-rata LP shares of the total reserves and can be redeemed for the underlying assets at any time.

Pairs act as automated market makers, standing ready to accept one token for the other as long as the “constant product” formula is preserved. This formula, most simply expressed as `x * y = k`, states that trades must not change the product (`k`) of a pair’s reserve balances (`x` and `y`). Because `k` remains unchanged from the reference frame of a trade, it is often referred to as the invariant. This formula has the desirable property that larger trades (relative to reserves) execute at exponentially worse rates than smaller ones.

In practice, DaoSwap applies a 0.30% fee to trades, which is added to reserves. As a result, each trade actually increases `k`. This functions as a payout to LPs, which is realized when they burn their pool tokens to withdraw their portion of total reserves. In the future, this fee may be reduced to 0.2%, with the remaining 0.1% withheld as a protocol-wide charge as further incentive.

Because the relative price of the two pair assets can only be changed through trading, divergences between the DaoSwap price and external prices create arbitrage opportunities. This mechanism ensures that DaoSwap prices always trend toward the market-clearing price.

5, Ecosystem Participants

The DaoSwap ecosystem is primarily comprised of three types of users: liquidity providers, traders, and developers. Liquidity providers are incentivized to contribute ERC-20 tokens to common liquidity pools. Traders can swap these tokens for one another for a fixed 0.30% fee (which goes to liquidity providers). Developers can integrate directly with DaoSwap smart contracts to power new and exciting interactions with tokens, trading interfaces, retail experiences, and more.

In total, interactions between these classes create a positive feedback loop, fueling digital economies by defining a common language through which tokens can be pooled, traded and used.

Liquidity Providers

Liquidity providers, or LPs, are not a homogenous group:

- Passive LPs are token holders who wish to passively invest their assets to accumulate trading fees.
- Professional LPs are focused on market making as their primary strategy. They usually develop custom tools and ways of tracking their liquidity positions across different DeFi projects.
- Token projects sometimes choose to become LPs to create a liquid marketplace for their token. This allows tokens to be bought and sold more easily and unlocks interoperability with other DeFi projects through DaoSwap.
- Finally, some DeFi pioneers are exploring complex liquidity provision interactions like incentivized liquidity, liquidity as collateral, and other experimental strategies. DaoSwap is the perfect protocol for projects to experiment with these kinds of ideas.

Traders

There are a several categories of traders in the protocol ecosystem:

- Speculators use a variety of community-built tools and products to swap tokens using liquidity pulled from the DaoSwap protocol.
- Arbitrage bots seek profits by comparing prices across different platforms to find an edge. (Though it might seem extractive, these bots actually help equalize prices across broader Ethereum markets and keep things fair.)
- DAPP users buy tokens on DaoSwap for use in other applications on Ethereum.
- Smart contracts that execute trades on the protocol by implementing swap functionality (from products like DEX aggregators to custom Solidity scripts).

In all cases, trades are subject to the same flat fee for trading on the protocol. Each is important for increasing the accuracy of prices and incentivizing liquidity.

DaoSwap Team and Community

The DaoSwap team along with the broader DaoSwap community drives development of the protocol and ecosystem.

6, Swaps

Token swaps in DaoSwap are a simple way to trade one ERC-20 token for another.

For end-users, swapping is intuitive: a user picks an input token and an output token. They specify an input amount, and the protocol calculates how much of the output token they'll receive. They then execute the swap with one click, receiving the output token in their wallet immediately.

In this guide, we'll look at what happens during a swap at the protocol level in order to gain a deeper understanding of how DaoSwap works.

Swaps in DaoSwap are different from trades on traditional platforms. DaoSwap does not use an order book to represent liquidity or determine prices. DaoSwap uses an automated market maker mechanism to provide instant feedback on rates and slippage.

As we learned in Protocol Overview, each pair on DaoSwap is actually underpinned by a liquidity pool. Liquidity pools are smart contracts that hold

balances of two unique tokens and enforces rules around depositing and withdrawing them.

This rule is the constant product formula. When either token is withdrawn (purchased), a proportional amount of the other must be deposited (sold), in order to maintain the constant.

7, Pools

Each DaoSwap liquidity pool is a trading venue for a pair of ERC20 tokens. When a pool contract is created, its balances of each token are 0; in order for the pool to begin facilitating trades, someone must seed it with an initial deposit of each token. This first liquidity provider is the one who sets the initial price of the pool. They are incentivized to deposit an equal *value* of both tokens into the pool. To see why, consider the case where the first liquidity provider deposits tokens at a ratio different from the current market rate. This immediately creates a profitable arbitrage opportunity, which is likely to be taken by an external party.

When other liquidity providers add to an existing pool, they must deposit pair tokens proportional to the current price. If they don’t, the liquidity they added is at risk of being arbitraged as well. If they believe the current price is not correct, they may arbitrage it to the level they desire, and add liquidity at that price.

Pool tokens

Whenever liquidity is deposited into a pool, special tokens known as *liquidity tokens* are minted to the provider’s address, in proportion to how much liquidity they contributed to the pool. These tokens are a representation of a liquidity provider’s contribution to a pool. Whenever a trade occurs, the 0.3% fee which is levied is distributed *pro-rata* to all LPs in the pool at the moment of the trade. To receive the underlying liquidity back, plus any fees that were accrued while their liquidity was locked, LPs must burn their liquidity tokens.

Liquidity providers can also choose to sell, transfer, or otherwise use their liquidity tokens in any way they see fit.

Why pools?

DaoSwap is unique in that it doesn't use an order book to derive the price of an asset or to match buyers and sellers of tokens. Instead, DaoSwap uses what are called Liquidity Pools.

Liquidity is typically represented by discrete orders placed by individuals onto a centrally operated order book. A participant looking to provide liquidity or make markets must actively manage their orders, continuously updating them in response to the activity of others in the marketplace.

While order books are foundational to finance and work great for certain use cases, they suffer from a few important limitations that are especially magnified when applied to a decentralized or blockchain-native setting. Order books require intermediary infrastructure to host the orderbook and match orders. This creates points of control and adds additional layers of complexity. They also require active participation and management from market makers who usually use sophisticated infrastructure and algorithms, limiting participation to advanced traders. Order books were invented in a world with relatively few assets being traded, so it is not surprising they aren't ideal for an ecosystem where anyone can create their own token and those tokens usually have low liquidity. In sum, with the infrastructural trade-offs presented by a platform like Ethereum, order books are not the native architecture for implementing a liquidity protocol on a blockchain.

DaoSwap focuses on the strengths of Ethereum to reimagine token swaps from first principles.

A blockchain-native liquidity protocol should take advantage of the trusted code execution environment, the autonomous and perpetually running virtual machine, and an open, permission less, and inclusive access model that produces an exponentially growing ecosystem of virtual assets.

It is important to reiterate that a Pool is just a smart contract, operated by users calling functions on it. Swapping tokens is calling `swap` on a Pool contract instance, while providing liquidity is calling `deposit`.

Just how end-users can interact with the DaoSwap protocol through the Interface (which in turn interacts with the underlying contracts), developers can interact directly with the smart contracts and integrate DaoSwap functionality into their own applications without relying on intermediaries or needing permission.

8, Fees

Liquidity provider fees

There is a 0.3% fee for swapping tokens. 0.2% is split by liquidity providers proportional to their contribution to liquidity reserves. 0.1% is split by all TOI holders according to the number of tokens they hold.

Swapping fees are immediately deposited into liquidity reserves. This increases the value of liquidity tokens, functioning as a payout to all liquidity providers proportional to their share of the pool. Fees are collected by burning liquidity tokens to remove a proportional share of the underlying reserves.

Since fees are added to liquidity pools, the invariant increases at the end of every trade. Within a single transaction, the invariant represents `token0_pool / token1_pool` at the end of the previous transaction.

9, Pricing

How are prices determined?

As we learned in Protocol Overview, each pair on DaoSwap is actually underpinned by a liquidity pool. Liquidity pools are smart contracts that hold balances of two unique tokens and enforces rules around depositing and withdrawing them. The primary rule is the constant product formula. When a token is withdrawn (bought), a proportional amount must be deposited (sold) to maintain the constant. The ratio of tokens in the pool, in combination with the constant product formula, ultimately determine the price that a swap executes at.

How DaoSwap handles prices

In DaoSwap V1, trades are always executed at the “best possible” price, calculated at execution time. Somewhat confusingly, this calculation is actually accomplished with one of two different formulas, depending on whether the trade specifies an exact *input* or *output* amount. Functionally, the difference between these two functions is miniscule, but the very existence of a difference increases conceptual complexity. Initial attempts to support both functions in V2 proved inelegant, and the decision was made to **not provide**

any pricing functions in the core. Instead, pairs directly check whether the invariant was satisfied (accounting for fees) after every trade. This means that rather than relying on a pricing function to *also* enforce the invariant, V2 pairs simply and transparently ensure their own safety, a nice separation of concerns. One downstream benefit is that V2 pairs will more naturally support other flavors of trades which may emerge, (e.g. trading to a specific price at execution time).

At a high level, in DaoSwap V2, *trades must be priced in the periphery*. The good news is that the library provides a variety of functions designed to make this quite simple, and all swapping functions in the router are designed with this in mind.

Pricing Trades

When swapping tokens on DaoSwap, it's common to want to receive as many output tokens as possible for an *exact input amount*, or to pay as few input tokens as possible for an *exact output amount*. In order to calculate these amounts, a contract must look up the *current reserves* of a pair, in order to understand what the current price is. However, it is *not safe to perform this lookup and rely on the results without access to an external price*.

Say a smart contract naively wants to send 10 DAI to the DAI/WETH pair and receive as much WETH as it can get, given the current reserve ratio. If, when called, the naive smart contract simply looks up the current price and executes the trade, it is *vulnerable to front-running and will likely suffer an economic loss*. To see why, consider a malicious actor who sees this transaction before it is confirmed. They could execute a swap which dramatically changes the DAI/WETH price immediately before the naive swap goes through, wait for the naive swap to execute at a bad rate, and then swap to change the price back to what it was before the naive swap. This attack is fairly cheap and low-risk, and can typically be performed for a profit.

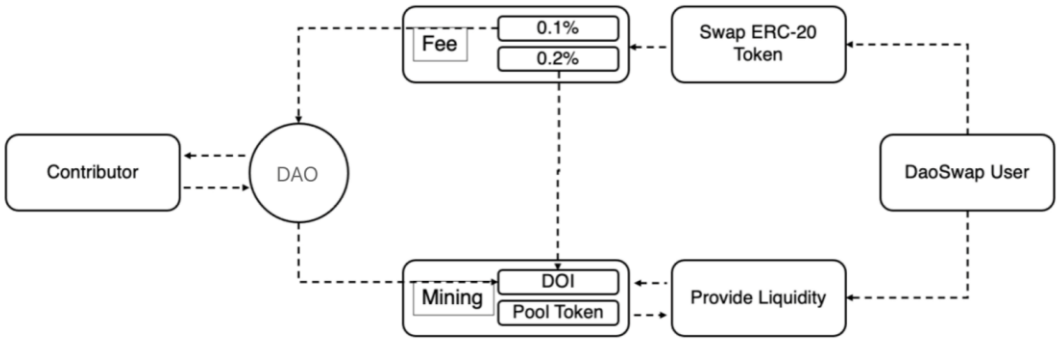
To prevent these types of attacks, it's vital to submit swaps *that have access to knowledge about the "fair" price their swap should execute at*. In other words, swaps need access to an *oracle*, to be sure that the best execution they can get from DaoSwap is close enough to what the oracle considers the "true" price. While this may sound complicated, the oracle can be as simple as an *off-chain observation of the current market price of a pair*. Because of arbitrage, it's typically the case that the ratio of the intra-block reserves of a pair is close to the "true" market price. So, if a user submits a trade with this knowledge in mind, they can ensure that the losses due to front-running are tightly bounded. This is how, for example, the DaoSwap frontend ensure trade safety. It calculates the optimal input/output amounts given observed intra-

block prices, and uses the router to perform the swap, which guarantees the swap will execute at a rate no less that `x`% worse than the observed intra-block rate, where `x` is a user-specified slippage tolerance (0.5% by default).

10, Tokenomics

DAO

DaoSwap minted DAO to server the purpose for community-led growth, development, and self-sustainability, enabling shared community ownership and a vibrant, diverse, and dedicated governance system, which will actively guide the protocol towards the future.



DAO Allocation

- 10 billion in total
- 25% to DaoSwap community members
- 25% to community treasury
- 50% to team and linear release

DAO holders will have immediate ownership of:

- DaoSwap governance
- DAO community treasury
- The protocol fee share

11, Disclaimer

This material should not be taken as the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions. Trading digital assets involves significant risk and can result in the loss of your invested capital. You should ensure that you fully understand the risk involved and take into consideration your level of experience, investment objectives and seek independent financial advice if necessary.