Whitepaper

ALPHA TAKER™

On-chain algorithmic asset management platform

May 11, 2022, Kyiv, Ukraine

by Eduard Ohanesian

donthodl@alphataker.com

https://github.com/AlphaTaker/main

ABSTRACT

The document details the economy of the AlphaTaker token, including the ecosystem structure that enables investors to embrace an algorithmic capital management, comprehensive in its safety. The document contains examples of investment strategies and dApps implementation drafts for EVM blockchains.

Increases in DEX liquidity, as well as the development of high-performance Blockchains and L2 solutions, persist as relevant trends. A similar level of trust extends to oracles and cross-chain bridges with a clear economic model. These factors contribute to favorable and popular trading DEX strategies that had been excessively vulnerable to transaction costs and liquidity strains. It is anticipated that strategies effective in decentralized contexts would expand in the future, while marketing opportunities would increase. Therefore, AlphaTaker provides investors with instruments for the creation of automated investment strategies using EVM blockchains. The DAO management enables AlphaTaker to issue tokens based on available trading algorithms, shape strategy portfolios, and generate synthetic assets with a desired risk profile and profitability. Moreover, the autonomous performance and CEX absence provide investment security and risk structure transparency, typical of DeFi applications.

PROBLEM

If crypto investors lack strategies for asset management or passive market making in the DeFi field, they have to resort to external marketplaces. Trend-informed strategies require investors' regular participation or a trustee involvement, which might create a risk of financial loss. The execution infrastructure might become another source of problems even upon the introduction of automated trading implemented without outside assistance because infrastructure contains encrypted keys. Acceptance of such risks remains unparalleled and effective in active speculative trading, arbitrage opportunities, and HFT trading. Aside from the continuous management of non-market risks, technology and arbitrage traders manage a limited capital. However, if the situation involves significant capital amounts with less rigorous management, exclusion of any non-market risks must become a pressing problem.

Before providing the solution overview, I offer several examples of targeted investment strategies.

Examples

1. The ETH purchasing strategy of Bitcoin-miner capitulation: the strategy requires the data on the cost of energy in stablecoin, the network complexity, and BTC open-market costs. The strategy rests on the fundamental connection between a product price and production costs. The approach demands no frequent deals.
2. The BTC arbitrage strategy of the S2F model: the strategy requires the data on the Bitcoin network complexity, block reward amount, and the market price of Bitcoin.
3. The BTC purchasing strategy of the weekly candlestick: the strategy requires the OHLC data on BTC currency pairs.

The provided examples do not follow high-frequency patterns, as the approaches exhibit tolerance to transaction costs and have capital-intensive features. Such asset management strategies perform ideally under conditions without trust, outside a regulated environment, and without investor anonymity loss.

SOLUTION

All deals occur based on strategy algorithms programmed into smart contracts. Smart contracts manipulate data and indicators available in the blockchain through a system of independent oracles that earn a reward for the delivery of market data (or present as marketplaces). The execution of smart contracts falls on participants who monitor the emergence of strategic trading signals, compete for transaction queuing, and earn a reward for completion. A strategy can be modeled by an investor through a strategy constructor and saved as an NFT, as well as a strategy can be purchased or copied in the strategy marketplace.

As such deals have an inherent non-arbitrage pattern, the problems of insufficient liquidity and trading activity disclosure are irrelevant for this class of investment strategies.

Economic structure of the solution

Unfortunately, it is impossible to provide technological guarantees that would solve all problems. For example, the issue of data falsification by oracles persists. For this reason, certain cases have security controls facilitated by the economic game with clear and transparent rules to the extent that effective behaviors naturally lead to a system of checks and balances necessary for the protection from economic cyber-attacks. The efficiency guarantee of the approach focuses on the avoidance of complication and excessive optimization susceptible to exploitation by hackers.

Data market

Participants responsible for transaction expenses provide the blockchain system with relevant data and indicators. Such participants are data providers, as they enter the data in the blockchain through the system of smart contracts that assume the role of oracles for other contracts. The Ethereum network contains multiple oracles, with Chainlink being the best known one that guarantees data authenticity in various ways and that has been labeled as the most trustworthy oracle by the blockchain community. DEX - MakerDAO, Uniswap, and Schelling prediction markets might also represent market data oracles. With custom indicators, like Black box, or individual data feeds applied, a simple AlphaTaker oracle can be used. The solution entails the entry of data at any frequency at the data provider's discretion. However, the simplest strategies (and the above-mentioned strategy examples) have no significant need for the delivery of market data more often than once a day. Data providers fix a fee and earn a reward from users for these services in cases when the data rendered prove relevant.

The more relevance the data demonstrates, the more compensation a data provider receives. Some data providers might not compensate for transaction costs and might cease to exist. Nevertheless, other data providers would justify their services on multiple occasions and would continue investment in reputation/frequency/reliability. Multiple oracles might use the constructor of investment strategies, hedging against cyber-attacks on oracles or against the disappearance of the data provider. Such circumstances form the data market.

Strategy market

Every strategy represents an NFT token that describes the rationale behind an investment decision. On the one hand, a strategy entails resorting to oracles, and on the other hand, to DEX liquidity providers. Strategy creation occurs with the help of a graphical constructor or, directly, with code. Strategies might exhibit different levels of complexity, employ external indicators, or analyze indicators independently. Strategies might be safer, with the use of the data from multiple providers, or strategies might be less safe, with trust given to a single data provider. Different approaches focus on market order changes, market order dilution for DEX applications, or the use of DEX liquidity aggregators. These factors make strategies more or less expensive from the perspectives of execution and development. With execution costs, available data, and signal frequency taken into account, strategies might include targeted AUM estimated by the strategy designer. This challenge anticipates the involvement of experts who design or audit strategies. Additionally, the situation requires the participation of investors who can select strategies among the available ones, purchase strategies, like Black box, and copy strategies with an open-access code. These factors shape the NFT strategic market.

Mining market

The conventional CEX trading determines that the stakeholder controlling the trading logic also executes orders. The present approach divides the two roles. Order execution entails the invocation of a smart contract without the opportunity to introduce changes to the trading logic. The deployment of a smart contract (in EVM blockchains) is impossible to time; therefore, the smart contract invocation and the payment for its deployment are available to anyone willing to complete the task. The first miner, who invokes a strategic smart contract with its deployment resulting in the dispatch of trading orders, receives the reward. Investors do not pay for ineffective contract invocation that leads to transaction costs, but fails to change trading positions.

Participants, who implement trading strategies and compete with each other for the opportunity to complete a transaction for a reward, are known as miners. Additionally, a miner selects a time frame when the production cost within the network is lower than a reward amount. The process generates the mining market.

Actors

Investor/Fund/DAO

The participant who manages algorithmic portfolios. Exactly this stakeholder allocates funds for strategy management and compensation of mining services by the means of including a required number of AlphaTaker tokens in the portfolio balance (an analogy to fuel). The investor manages multiple portfolios, as each portfolio has a single trading strategy attached to it. The investor can generate trading strategies independently or purchase/copy existent ones made by designers. The identified stakeholder is a buyer in the strategy market.

Strategy designer (optional)

The participant who creates algorithmic strategies with the help of a web-constructor or an embedded programming language. The stakeholder has the best understanding of the system complexity and offers the ability to locate rational solutions based on the safety profile and AUM strategy.

Data provider

Data provider is the participant who records the off-chain data in the oracle's contract. The stakeholder can deliver two data types, namely the baseline data and indicators. The former type refers to the verifiable original data, the authenticity of which can be confirmed. The latter type refers to indicators, aggregated data, and Black box trading signals. Such data cannot be verified due to the complexity of statistical analysis and their encrypted nature.

Miner

The participant who deploys the strategy, executing the network commission arbitrage and earning a reward for completion.

Technical description

A generalized approach rests on the maximization of the benefits of the developed blockchain ecosystem without an increase in community-accepted compromise amounts. The application of industry standards and popular products enables the development focus maintenance and improves UX.

The NFT-styled strategy presentation provides for the launch of the strategy market based on existent marketplaces. The DAO-specific fund presentation ensures the use of available DAO constructors with respective, high-quality instruments of corporate management. The use of well-known oracle platforms creates access to existent data markets for strategies based on simple calculations. The following elements are part of the AlphaTaker system.

Test environment deployed in the BSC (BNB network)

Blockchain part

■ Oracle	(Contract) 0x9D22818E275eCfc4315C41FBA9039d13187c542d
■ NFT strategy	(Contract) 0x5e67787795209D2A2d24d0524B32F9678a7c661A
■ Portfolio	(Contract) 0x84C1aF42F03B0D3808D1Ce3120dd779521665D22

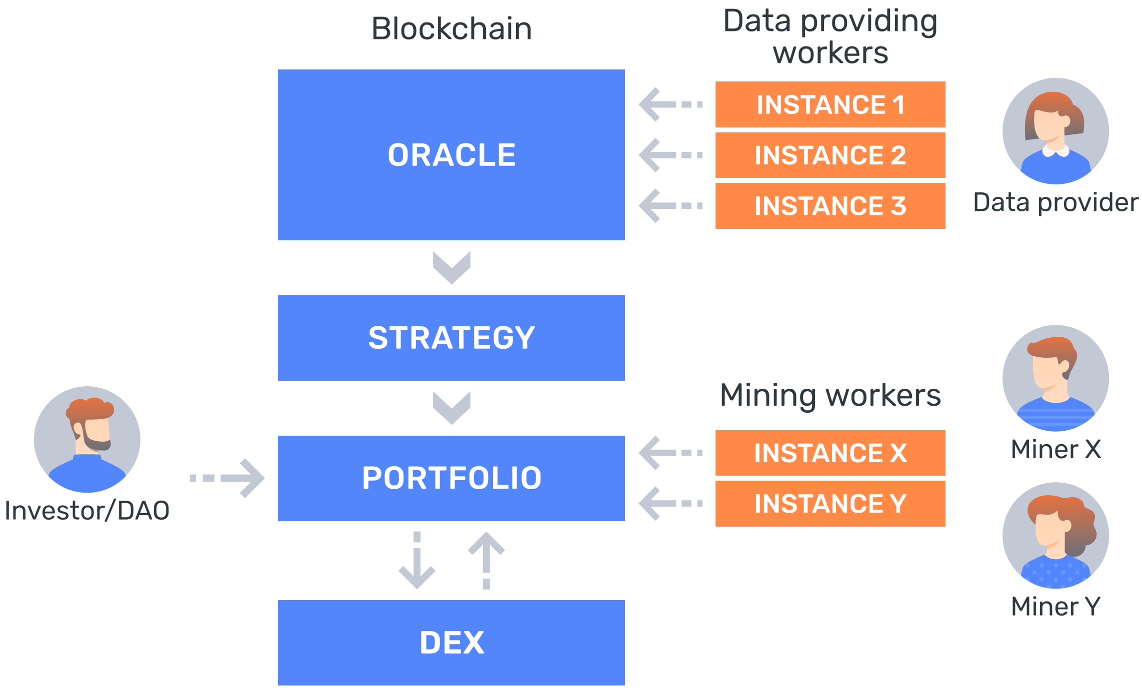
Web-management (todo)

- Strategy constructor
- Portfolio manager (https://bscscan.com/address/0x84C1aF42F03B0D3808D1Ce3120dd779521665D22#writeContract)
- Blockchain explorer of the market data and strategies

Workers

■ Data provider (oracle)	(Address) 0x13e14084D4721615f2f48B5E40De8bF51DDECB95
■ Miner	(Address) 0x13e14084D4721615f2f48B5E40De8bF51DDECB95

Architecture



The code provided below is a schematic. The reference code of the test environment is available at the Github repository of the AlphaTaker project.

Oracle

The oracle contract allows storing the data for a data provider and querying data for the strategy contract.

```
contract Oracle{
    function write(name, value) {
        _indicators[name] = value;
    }
    function read(name) {
        return _indicators[name];
    }
}
```

Strategy

The strategy implements the oracle querying and token exchange under DEX management, containing the trading logic and computational strategies necessary for effective functioning.

```
contract Strategy{
    function setOracle(address oracle_address) {
        _oracle = oracle_address;
    }
    function execute() returns(string) {
        new_price = (_oracle).call("read(string)", "btc-usd-price");
        if (new_price > old_price){
           buy_success = (_dex).call("exchange(address, address)", _tokenA, _tokenB);
           if (!buy_success) return "Token A buy fail";
        }else if (new_price < old_price){
           buy_success = (_dex).call("exchange(address, address)", _tokenB, _tokenA);
           if (!buy_success) return "Token B buy fail";
        }else{
            return "Indicator not updated";
        }
        old_price = upd;
        return "Success";
    }
}
```

Portfolio

The contract implements portfolio management: token deposit/withdrawal and strategy management specifications, as well as interface realization for strategy execution by miners.

```
contract Portfolio{
    function setStrategy(address strategy_address) {
        _strategy = strategy_address;
    }
    function claimToken(address token_address, uint256 amount) {
        call_success = (token_address).call("transfer(address, uint256)", _owner, amount);
    }
    function execute() {
        call_success = (_strategy).call("execute()");
        reward_amount = spent_gas() * k;
        if (call_success) (reward_token_address).call("transfer(.)", msg.sender, reward_amount );
    }
}
```

Strategy constructor

The constructor represents a web interface that allows for programming algorithms by mousable graphical means on the principle of "What You See Is What You Get." The interface produces a JSON-document that offers a complete description of the investment strategy. The JSON-document can be relayed in the program code and, furthermore, in the binary code of a smart contract. The capabilities of the programming strategy are limited by the scheme of the interface and the document that prevents the realization of any desired strategy logic. The scheme also enables the verification of the contract's binary code in terms of alignment with the document, while the document can be verified in terms of alignment with the web-interface, instrumental in its creation. Therefore, the process demonstrates evidence about the strategy safety upon the contract's generation with the help of a trustworthy interface. Dependent on a scheme, a different functionality of the constructor might be prohibited and allowed. Multiple graphical web interfaces might be realized for a single scheme.

An arbitrary contract can be verified by means of loading the JSON-document that produced it with the indication of the scheme version, the processor version, and solidity compilator (if processing occurred in solidity) that were used in its production. The document itself describing a strategy should not necessarily be stored in the local dataset, but the address dataset should pass an assessment by being publicly available and represent a following table.

Verified NFTs

Network	Contract	SCHEME	Translator	Compiler
BNB	0xea674fdde714fd979de3ed f0f56aa9716b898ec8	v1.0	v1.0	v0.8.7+commit.e28d 00a7

Consequently, the strategy and its trading logic can be covert and represent a Black box in the form of a smart contract or, conversely, be open and available for modification if the JSON-document created in the constructor is published in open access.

Data provider worker (Oracle client)

The worker is launched in several non-competitive but identical replicas in separate environments with the application of dissimilar endpoints for the same market data acquisition. As the worker stores the market data in the blockchain, different replicas employ different BC balances and BC-node addresses. The element makes broad opportunities available for the mitigation of technological risks.

```
function update_oracle(feed_name, value){
  var options = { gasLimit: 150000, gasPrice: ethers.utils.parseUnits(5, 'gwei') };
  oracle.estimateGas.write(feed_name, [value], options).then(function(tx) {
      options.gasLimit = tx;
      oracle.write(feed_name, [value], options);
  });
}
function get_Binance_price(symbol){
  request.get({url: Config.binance_api+'/api/v3/avgPrice?symbol='+symbol, json: true},
function (error, response, body) {
    if (!error && response.statusCode == 200) update_oracle('btc-usd-price', body.price);
  });
}
setInterval(function(){
  get_Binance_price('BTCUSDT')
}, 24h);
```

Mining worker

The worker is launched in multiple competitive replicas. To receive a reward, the first worker often checks the blockchain status of the contract and implements the strategy when the transaction completion leads to the desired result (i.e., remuneration with reward tokens). Frequent checks of the blockchain status and transaction results exert pressure on the BC node; thus, the worker uses a personal parking node or employs a third party's infrastructure for a fee.

```
function mining(){
  var options = { gasLimit: 150000, gasPrice: ethers.utils.parseUnits(5, 'gwei') };
  portfolio.estimateGas.execute().then(function(tx) {
    options.gasLimit = tx;
    portfolio.execute(options);
  });
}
setInterval(function(){
  mining();
}, 5s);
```

TOKEN

Strategy implementers sustain transaction costs related to the blockchain network commission. Transaction prices in EVM networks depend on two factors, namely the calculation amount necessary for the contract execution and the unit price for the node computational power. The latter factor is prone to variability that assists in managing the probability of a rapid block transaction containment and transaction precedence in the node storage pool. The former factor is constant and broadly known. AlphaTaker fixes a reward in its own tokens in direct ratio to the volume of "gas" needed for the worker to complete a transaction. The token price is market-regulated between token consumers (i.e., algorithmic portfolio holders) and sellers (i.e., miners, oracles, and project investors). The AlphaTaker token shares a fundamental connection with a "gas" price in the network and represents "fuel" essential to the ecosystem operation.

The following process overviews the simplest circulation cycle of the AlphaTaker (AT) token between actors, the investor and the miner, with market making services used and for the strategy that entails a reward of 1AT upon its execution:

- MM offers 1AT for $10 and purchases it for $9
- Investor purchases 1AT for $10 and deposits it in the portfolio contract
- Miner does not execute the contract because the network transaction price is set at $14
- Miner executes the contract when the network transaction price decreases to $7
- Miner receives 1AT and sells it to MM for $9
- MM offers 1AT for $10 and purchases it for $9, etc.

$ distribution as a result of one cycle

MM	Miner	Network validators	Algotrader
+1$	+2$	+7$	-10$

The investor (algotrader) paid $10 for the strategy execution instead of $7 that could have been paid, had the investor assumed the role of a miner. However, the investor paid $10 instead of $14 that could have been paid, had the investor followed the strategy in a trivial manner (without a miner-executed BC analysis). Therefore, the investor paid the miner $2 for the service of the autonomous strategy implementation, as well as for the transaction cost optimization. Miner competition reduces the prices of mining services for investors even more.

The cycle repetition contributes to the MM's increase in the USD holdings, without an increase in AT holdings, which forces the MM to raise the AT market price. The tendency occurs even in the circumstances of a permanent number of strategies and a stable demand for AT.

AT demand stimulation and price increases are possible by the means of token withdrawal from the cycle in favor of other participants, who hold the token without using it within the ecosystem. The introduction of a deflation mechanism is possible by the means of imposing fees on auxiliary investor transactions with the subsequent burning of the fees.

FEES

The following options present as possible AT token fees:

- A fee for the NFT strategy issue (interface interaction)
- Success fee
- Execution fee, etc.

DAOS

The selection of a strategy that manages the asset portfolio requires responsible decision-making. The strategy has full access to portfolio resources, including the possibility of complete funds withdrawal. Relevant security guarantees manage the portfolio and strategy adjustment. A system of bridge contracts based on Shamir's Secret Sharing and other multisignatures act as security controls. In cases of collective ownership of managed funds, the DAO decentralized management architecture enables decision-making by voting, with different approaches to consensus protection. As a platform for the generation of algorithmic portfolios, AlphaTaker envisions DAO-creation platforms and various MultiSig wallets as its partners.

DEXS

As a platform for the generation of taker liquidity, AlphaTaker envisions AMM and DEX protocol developers as its partners.

MULTICHAIN

As an element of the DeFi infrastructure, AlphaTaker envisions new and old EVM blockchain projects, focused on an increase in transactions and participants in their network, as its partners.

Ethereum	Fuse	HECO	Shiden	XDC Network
Polygon	Oasis	BNB Chain	BitTorrent	
Fantom	Optimism	Avalanche	CoinEx	
Moonbean	Celo	Aurora	Boba	
Astar	Metis	Moonriver	OKC	

DEVELOPMENT PROSPECTS

1. Social trading
   - Automated copy trading as repetition of a single alpha by multiple portfolios
   - Diversification as aggregation of many alphas within one portfolio
2. Market data research and the delivery of indicators, like Black box
3. Issue of algorithmic token and derivatives

LIMITATIONS

Although I am writing about investment strategies, it is probable that investors would want to increase the frequency of deals cutting their own return on investment and ensuring the profit for the entire ecosystem described above, including BC validators responsible for the contract system validity. Thus, it is more appropriate to discuss “trading” strategies. However, I believe that the system is not designated for these purposes.

Additionally, the relay of oracle market decisions as indicators is one of the weaknesses of custom oracles. Therefore, the Black box data provider becomes a certain private manager that receives opportunities to manipulate markets to its advantage, which creates arbitrage by automated copy traders and eliminates arbitrage with the help of the provider’s funds.

Moreover, inefficacy might emerge in any other unknown market scenario that occurs as a result of the rising complexity of investment strategies. AlphaTaker leaves such cases to the market's discretion and arbitration.

CONCLUSION

Although the significant security and high transaction prices render the blockchain infrastructure unappropriated for active low-margin operations, the community has engaged in the enthusiastic pursuit of innovative solutions related to the intelligent level of compromise for the creation of decentralized markets and the inexpensive exchange in the permissionless environment. These solutions operate in technological and economic dimensions alike. Industry trends include the emergence of market making algorithms that are more efficient in terms of transaction workload, as well as blockchain networks focused on high productivity alongside low-priced transactions. Economic compromises, like stablecoins, oracles, and cross-chain bridges, proved their sufficiently high reliability and the capacity to deliver benefits that surpass application risks. The tendency of market regulation and KYC enables the protection of the economic consensus models from the most dangerous attacks, imparting even more resilience to the DeFi infrastructure. The financial DeFi infrastructure will evolve in the future toward added complexity alongside the emergence of new financial instruments, including derivatives. The capital management will also complexify, as managed finance amounts will increase, with the token value similarly rising and ensuring such management.