Whitepaper

AlphaTaker™

On-chain algorithmic asset management

May 11, 2022

by

Eduard Ohanesian

Kyiv, Ukraine

donthodl@alphataker.com

https://github.com/AlphaTaker/main

Abstract

Этот документ объясняет экономику токена AlphaTaker, устройство экосистемы, которая позволяет инвесторам организовать в широком смысле безопасное, алгоритмическое управление капиталом. Документ содержит примеры инвестиционных стратегий и черновики реализации dapps для EVM блокчейнов.

Рост ликвидности DEX, а также развитие высокопроизводительных БЧ и L2 решений являются трендами. Как и доверие к оракулам и кроссчейн бриджам с понятной экономической моделью. Это создает благоприятные условиями для трендовых торговых стратегий на DEX, которые ранее были слишком чувствительны к транзакционным издержкам и нехватке ликвидности. Вероятно, в будущем класс стратегий, эффективно работающих в децентрализованном окружении, будет еще шире, а рыночные возможности еще больше. Поэтому AlphaTaker предлагает инвестору инструменты создания автоматических инвестиционных стратегий на EVM-блокчейнах. Под DAO управлением AlphaTaker позволит выпускать токены обеспеченные торговыми алгоритмами, формировать портфели стратегий, создавать синтетические активы с нужными параметрами риска и доходности. При этом, автономное исполнение и отсутствие CEX, обеспечивают защищенность инвестиций и прозрачную структуру рисков, характерную DeFi приложениям.

Problem

Если криптоинвестору не достаточно стратегий удержания актива, или пассивного маркетмейкинга в сфере DeFi, он вынужден иметь дело с внешними торговыми системами. Стратегии следования тренду требуют регулярной активности инвестора, или участия доверенного управляющего, что может стать источником риска потери средств. Даже автоматизировав торговлю собственными силами, инфраструктура исполнения может оказаться источником проблем, поскольку на ней находятся секретные ключи. Для активных спекуляций, арбитража и HFT принятие такого рода рисков все еще остается безальтернативным и эффективным. Технологические трейдеры и арбитражеры помимо того, что администрируют нерыночные риски непрерывно, они также управляют ограниченным капиталом. Но если речь идет о крупных размерах капитала с менее интенсивном управлением, в этой ситуации исключение любых нерыночных рисков становится, пожалуй, проблемой номер один.

Прежде чем изложить решение этой проблемы, приведу несколько примеров целевых инвестиционных стратегий.

Examples

1. ETH стратегия покупки капитуляции Биткоин-майнеров - необходимы данные о стоимость электроэнергии в stablecoin, данные о сложности сети и о стоимости BTC на открытом рынке. Стратегия основана на фундаментальной связи цены товара и его стоимости производства. Не нуждается в высокой частоте сделок.

2. BTC стратегия арбитража модели S2F - необходимы данные о сложности сети Биткоин, размере вознаграждения за блок, рыночной стоимости Биткоина.

3. BTC стратегия покупки закрытия недельной свечи - необходимы данные OHLV валютных пар с BTC..

Приведенные примеры стратегий не являются высокочастотными, они толерантны к транзакционным издержкам и являются капиталоемкими. Такие стратегии управления активами идеально существуют в условиях без доверия, без регулируемой среды и без потери анонимности инвестора.

Solution

Все сделки происходят согласно алгоритмам стратегий, запрограммированным на смарт-контрактах. Смарт-контракты оперируют данными и индикаторами доступными в блокчейн через систему независимых оракулов, получающих вознаграждение за поставку рыночных данных (или являющихся рынками). Исполнением смарт-контрактов занимаются участники, которые отслеживают появление торговых сигналов стратегий, конкурируют за место в очереди и получают вознаграждение за их исполнение. Стратегия может быть подготовлена как самим инвестором при помощи конструктора и сохранена как NFT, так и может быть приобретена или скопирована на рынке стратегий.

Поскольку сделки заведомо не являются арбиражными, то проблемы нехватки ликвидности и проблема раскрытия торговой активности не являются актуальными для такого класса инвестиционных стратегий.

Economic structure of the solution

К сожалению, не возможно предоставить технологические гарантии решения всех проблем. Как, например, проблему фальсификации данных оракулами. Поэтому в ряде случаев безопасность обеспечивается экономикой игрой, правила которой настолько просты и прозрачны, что эффективное поведение участков само собой создает балансы и противовесы, необходимые для защиты от экономических атак. Залогом работоспособности такого подхода является избегание усложнений и избыточной оптимизаций, слабостями которых могут пользоваться хакеры.

- **Data market**

Данные и индикаторы поставляются в систему блокчейн участниками, которые берут на себя затраты по выполнению этих транзакций. Такие участники являются провайдерами данных (Data provider), они записывают данные в блокчейн через систему смарт-контрактов, которые для других контрактов являются оракулами. В сети Ethereum существует множество оракулов, наиболее известный из которых Chainlink, который обеспечивает подлинность данных совершенно разнообразными способами и по мнению блокчейн сообщества наиболее заслуживает доверия. Оракулами рыночных данных также могу выступать DEX - MakerDAO, Uniswap и рынки предсказаний согласно Schelling. В случае использования кастомных индикаторов типа **Black box** или же собственных фидов данных, можно использовать простой оракул AlphaTaker. Данные могут быть записаны с любой частотой на усмотрение Data provider. Однако, для простейших стратегий (и примеров стратегий описанных выше) нет большой необходимости поставлять рыночные данные чаще, чем раз в сутки. За эти услуги Data provider устанавливают плату и получают вознаграждение от пользователей данных, в случае, если их данные оказались востребованы. Чем более востребованы эти данные, тем больше награды получает Data provider. Могут существовать Data provider, которые не окупают транзакционные издержки и прекратят существование. Но также будут и те, кто окупаются многократно и продолжит инвестиции в репутацию/частоту/надежность. Конструктор инвестиционных стратегий может пользоваться множеством оракулов, хеджируя риски атак на оракулы или исчезновения Data provider. Таким образом возникает рынок данных.

- **Strategy market**

Каждая стратегия является NFT токеном, который описывает логику принятия инвестиционного решения. Стратегия включает в себя обращение с одной стороны к оракулам, с другой стороны к поставщикам ликвидности DEX. Создание стратегий происходит при помощи графического конструктора, либо непосредственно кодом. Стратегии могут быть сколь угодно сложными, они могут пользоваться внешними индикаторами, либо рассчитывать индикаторы самостоятельно. Стратегии могут быть более безопасными, с использованием данных множества Data provider, либо менее безопасными с доверием к одному Data provider. Возможно управление маршрутами ордеров, дробление ордеров для исполнения на разных DEX или использование агрегаторов DEX ликвидности. Все это делает стратегии боле или менее дорогими с точки зрения исполнения, а также с точки зрения разработки. С учетом затрат исполнения, используемых данных и частоты сигналов,

стратегии могут иметь целевой AUM, рассчитанный дизайнером стратегии. Такая сложность предполагает участие специалистов, которые разрабатывают стратегии, либо способны выполнять их аудит. А также участите инвесторов, которые могут выбирать стратегии среди существующих, покупать стратегии типа **Black box**, или копировать стратегии с открытым кодом. Таким образом возникает NFT рынок стратегий.

- **Mining market**

В классической биржевой торговле на CEX исполнением приказов занимается тот, кто контролирует торговую логику. В данном подходе эти роли разделены. Исполнение означает вызов смарт-контракта без возможности внесения изменений в торговую логику. Выполнение смарт-контракта (в EVM блокченах) не возможно поставить на таймер, поэтому вызов смарт-контрактов и оплата их исполнения будет предлагаться любому желающему. Тот, кто первый вызвал смарт-контракт стратегии и его выполнение завершилось отправкой торговых приказов, тот и получает вознаграждение. Неэффективные вызовы контракта, которые приводят к транзакционным издержкам, но не приводят к изменению торговых позиций инвестора не оплачиваются. Участники, которые занимаются исполнением торговых стратегий, конкурируют друг с другом за возможность первым выполнить транзакцию с вознаграждением называются майнерами (Miner). При этом Miner подбирает момент времени, когда стоимость исполнения в сети ниже, чем размер вознаграждения. Таким образом возникает рынок исполнения.

Actors

- **Investor/Fund/DAO**

Участник, который администрирует алгоритмические портфели. Именно он аллоцирует свои средства под управление стратегий и оплачивает услуги Miner путем размещения необходимого количества токенов AlphaTaker на балансе своих портфелей (аналог топлива). Инвестор управляет множеством портфелей, к каждому из которых привязана одна торговая стратегия. Инвестор может самостоятельно создавать торговые стратегии или покупать/копировать готовые у дизайнеров. Он является покупателем на рынке стратегий.

- **Strategy designer (optional)**

Участник, который создает алгоритмические стратегии с использованием web-конструктора или на встроенном языке программирования. Он лучше всех ориентируется в сложности системы и способен находить рациональные решения исходя из профиля безопасности и AUM стратегии.

- **Data provider**

Data provider это участник, который записывает офф-чейн данные в контракт оракула. Он может поставлять данные двух типов - исходные данные и индикаторы. Первый тип - проверяемые оригинальные данные, подлинность которых можно удостоверится. Второй тип - индикаторы, агрегированные данные, или торговые сигналы **Black box**. Такие данные не возможно доказать сверкой в силу сложности их расчета, или их скрытой природы.

- **Miner**

Участник, который приводит стратегию в исполнение, выполняя арбитраж комиссии сети и платы за исполнение

Technical description

Общий подход заключается в том, чтобы максимально использовать преимущества развитой экосистемы блокчейн, без увеличения размера компромиссов, которые приняты сообществом. Использование отраслевых стандартов и популярных продуктов позволит сохранить фокус разработки и улучшить UX. Представление стратегии в виде NFT позволяет запустить рынок стратегий на базе существующих маркетплейсов. Представление фонда в виде DAO позволяет использовать существующие DAO конструкторы с соответствующими, качественно разработанными инструментами корпоративного управления. Использование известных платформ для оракулов открывает доступ к существующим рынкам данных для стратегий, основанных на простых вычислениях. Следующие элементы являются частью системы AlphaTaker.

Test environment deployed in the BSC (BNB network)

Blockchain part

- Оракул: (Contract) 0x9D22818E275eCfc4315C41FBA9039d13187c542d
- NFT стратегии: (Contract) 0x5e67787795209D2A2d24d0524B32F9678a7c661A
- Портфель: (Contract) 0x84C1aF42F03B0D3808D1Ce3120dd779521665D22

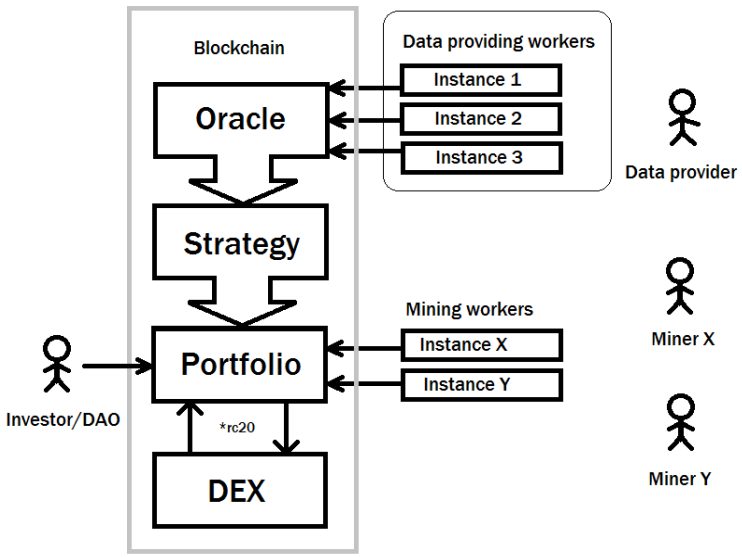
Web-management (todo)

- Конструктор стратегий
- Менеджер портфеля (https://bscscan.com/address/0x84C1aF42F03B0D3808D1Ce3120dd779521665D22#writeContract)
- БЧ-обозреватель рынка данных
- БЧ-обозреватель стратегий

Workers

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

Architecture



Приведенный ниже код является схемой. Референсный код тестового стенда доступен в Github репозитарии проекта AlphaTaker

Oracle

Контракт оракула разрешает запись для поставщика данных и чтение для контракта стратегии

```
contract Oracle{

    function write(name, value) {
       _indicators[name] = value;
    }

    function read(name) {
        return _indicators[name];
    }

}
```

Strategy

Стратегия реализует чтение оракула и обмен токенов под управлением на DEX, а также содержит торговую логику и необходимые для работы стратегии вычисления

```
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

Контракт реализует управление портфелем: ввод/вывод токенов, задание стратегии управления и реализует интерфейс для майнеров для выполнения этой стратегии

```
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(address, uint256)", msg.sender, reward_amount );
    }

}
```

Strategy constructor

Конструктор представляет собой web-интерфейс, который позволяет программировать алгоритмы графическими средствами при помощи мыши по принципу «что видишь, то и получаешь». Интерфейс производит JSON-документ, который полностью описывает инвестиционную стратегию. Этот JSON-документ способен быть однозначно транслирован в программный код, а затем и в бинарный код смарт-контракта. Возможности программирования стратегии ограничены схемой интерфейса и документа, которая не позволяют реализовать любую желаемую логику стратегии. Также схема позволяет верифицировать бинарный код контракта на предмет соответствия документу, а документ верифицировать на предмет соответствия web-интерфейсу, при помощи которого он был создан. Таким образом обеспечивается доказательства того, что стратегия безопасна и создана при помощи доверенного web-интерфейса. В зависимости от схемы может быть запрещена и разрешена различная функциональность конструктора. Для одной схемы может быть реализовано множество графических web-интерфейсов.

Произвольный контракт может быть верифицирован путем загрузки JSON-документа из которого он произведен с указанием версии схемы, версии транслятора (и версии компилятора solidity, если трансляция происходит в solidity), которые использовалась при его создании. Сам документ, описывающий стратегию, не обязательно должен быть сохранен в локальной базе данных, однако база данных адресов успешно прошедших проверку должна быть публичной и представлять собой следующую таблицу

Verified NFTs				
Network	**Contract**	**SCHEME**	**Translator**	**Compiler**
BNB	0xea674fdde714fd979de3edf0f56aa9716b898ec8	v1.0	v0.1	v0.8.7+commit.e28d00a7

Таким образом, стратегия и ее торговая логика могут быть скрыты и представлять собой **Black box** в виде смарт-контракта, либо наоборот открыты и доступные для модификаций, если JSON-документ, созданный в конструкторе размещен публично.

Data provider worker (Oracle client)

Запускается в нескольких не конкурирующих, но повторяющих друг друга экземплярах в раздельном окружении с использованием неодинаковых точек доступа получения одних и тех же рыночных данных. Поскольку воркер пишет рыночные данные в блокчейн, разные экземпляры используют разные БЧ-балансы и используют разные адреса БЧ-нод. В этой части доступны широкие возможности уменьшения технологических рисков.

```
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

Исполнитель запускается в множестве конкурирующих экземпляров. Для получения вознаграждения первым воркер часто проверяет состояния контракта в блокчейн и выполняет стратегию, когда совершение транзакции приводит к желаемому результату (к выплате токенов вознаграждения). Частая проверка состояния блокчейн и проверка результатов транзакции создает нагрузку на БЧ-ноду, поэтому исполнитель имеет свой парк нод, либо использует платную инфраструктуру третьей стороны.

```
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

Исполнители стратегий несут транзакционные издержки, связанные с комиссией сети блокчейн. В EVM сетях стоимость транзакции примерно связана с двумя факторами - объем вычислений, необходимый для выполнения контракта и стоимость единицы вычислительной способности ноды. Второй фактор вариативен и позволяет управлять вероятность скорого включения транзакции блок и приоритет транзакции в пуле памяти нод. Первый фактор постоянный и заведомо известен. AlphaTaker устанавливает вознаграждение в собственных токенах, которое прямо пропорционально объему "газа", необходимого для того чтобы исполнитель выполнил транзакцию. Цена токена регулируется рынком между потребителями токена - держателями алгоритмических портфелей и продавцами - майнерами, оракулами и инвесторами проекта. Токен AlphaTaker фундаментально связан со стоимостью газа в сети и является "топливом" для работы экосистемы.

Так выглядит простейший цикл обращения токена AlphaTaker (AT) между актерами Investor и Miner, при использовании услуг маркетмейкера и для стратегии, выполнение которой вознаграждается 1AT:

1) MM предлагает 1AT за 10$ и покупает за 9$
2) Инвестор покупает 1AT за 10$ и вносит на контракт портфеля
3) Майнер не выполняет контракт, так как стоимость транзакции в сети 14$
4) Майнер выполняет контракт, когда стоимость транзакции в сети опустилась до 7$
5) Майнер получает 1AT и продает его MM за 9$
6) MM предлагает 1AT за 10$ и покупает за 9$ etc

В результате одного такта распределение $			
MM: +1$	Майнер: +2$	Валидаторы сети: +7$	Инвестор: -10$

Инвестор заплатил 10$ за выполнение стратегии вместо 7$, которые он бы заплатил, если бы выполнял ее вместо майнера. Но также он заплатил 10$ вместо 14$, которые бы он заплатил, если бы исполнял свою стратегию тривиально (без анализа БЧ, который делал майнер). Таким образом инвестор оплатил 2$ майнеру за услугу автономного исполнения стратегии, а также за оптимизацию транзакционных расходов. При конкуренции майнеров услуги исполнения становятся еще дешевле для инвестор.

Повторяя этот цикл, у ММ растет долларовый запас, но не растет запас AT, что заставляет ММ поднимать рыночную стоимость AT. Это происходит даже при постоянном, не увеличивающемся числе стратегий и не увеличивающемся спросе на AT.

Стимулирование спроса на AT и рост цены возможны путем вывода токенов из этого цикла в пользу других участников, удерживающих токен, а не использующих его внутри экосистемы. Внедрение механизма дефляции возможно путем обложения сборами вспомогательных транзакций инвестора с последующим сжиганием этих сборов.

Fees

Возможны следующие варианты сборов в токенах AT:

1. Плата за выпуск NFT стратегии (взаимодействие с интерфейсом)
2. Плата за успех
3. Плата за исполнение etc

DAOs

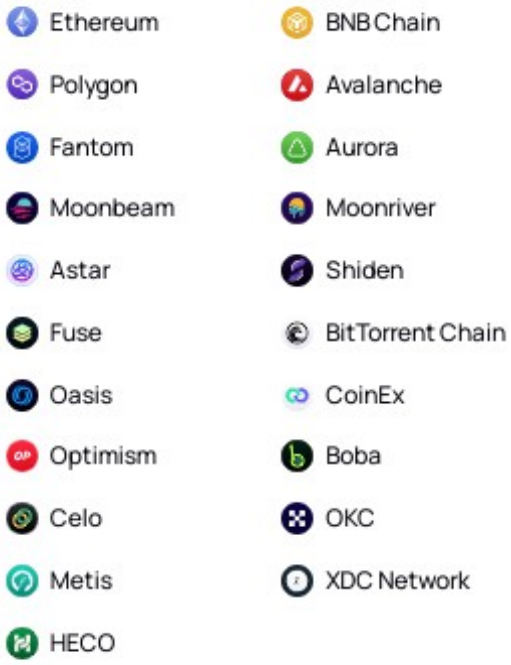
Выбор стратегии, которая управляет портфелем активов, является ответственным решением. Стратегия имеет полный доступ к средствам портфеля, включая возможность полного вывода средств. Разумно обеспечить необходимые гарантии безопасности управляющим портфелем и настройку стратегии. Это возможно делать через системы промежуточных контрактов, реализующих защиту Шамира и иные виды мультиподписи. В случае когда управляемый капитал является коллективной собственностью, используется децентрализованная архитектура управления DAO с возможностями принятия решений путем голосования с различными видами защиты консенсуса. AlphaTaker как платформа для создания алгоритмических портфелей видит своими партнерами платформы для создания DAO и различные multisig wallets.

DEXs

AlphaTaker как платформа для создания тейкерской ликвидности видит своими партнерами разработчиков AMM и DEX протоколов.

Multichain

AlphaTaker как элемент инфраструктыры DeFi видит своими партнерами новые и старые EVM БЧ-проекты, стремящиеся наполнять свои сети транзакциями и участниками



Development prospects

1. Социальный трейдинг
    1. Автоследование - повторение одной альфы многими портфелями
    2. Диверсификация - агрегация множества альф в рамках одного портфеля
2. Исследование рыночных данных и поставка индикаторов типа **Black box**
3. Выпуск алгоритмических токенов и деривативов

Limitations

Хотя я пишу об инвестиционных стратегиях, вполне вероятно, что инвесторы будут хотеть увеличивать частоту сделок, урезая собственную доходность и обеспечивая прибыль всей описанной выше экосистемы. Включая валидаторов БЧ, на которых развернута система контрактов. Более корректно говорить в этом случае о "торговых" стратегиях. Но я считаю, что система предназначена не для этого.

Также слабым местом в части кастомных оракулов является трансляция в качестве индикаторов собственных торговых решений. Таким образом, поставщик данных **Black box** становится чем-то в роде частного управляющего и получает возможности манипулировать рынками в свою пользу — создавая арбитраж автоследователями и устраняя его при помощи своего капитала.

Также неэффективность может возникать в любых других неизвестных рыночных ситуациях, возникающих в результате роста сложности инвестиционных стратегий. AlphaTaker оставляет такие случаи на усмотрение и арбитраж рынка.

Conclusion

Не смотря на то, что инфраструктура блокчейн в силу своей высокой защищенности и высокой стоимость транзакций не предназначена для активных маломаржинальных операций, сообщество активно ищет оригинальные способы решения как при разумном уровне компромисов организовать децентрализованные рынки и недорогой обмен в permissionless окружении. Эти решения находятся как в технологической так и в экономической плоскости. Появление более экономных с точки зрения транзакционной нагрузки алгоритмов маркет-мейкинга, а также блокчейн сети развернутые с фокусом на выокую производительность при низкой стоимости транзакций, являются трендами индустрии. Экономические компромиссы в виде stablecoin, оракулов и бриджей доказали достаточно высокую прочность и способность приносить выгоду превышающую риски их использования. Тенденция к регуляции рынка и KYC позволяют защитить экономические модели консенсуса от наиболее опасных атак, придавая инфраструктуре DeFi еще больше устойсивости. В будущем финансовая инфраструктура DeFi будет развиваться в сторону усложнения, появления новых финансовых инструментов, в том числе производных. Управление капиталом также будет усложняться, объемы средств под управлением будут расти, как и будет расти ценность токенов, обеспечивающих такое управление.