

**Децентрализованный
рынок разведки
киберугроз.**

Table of Contents

PolySwarm за 60 секунд	03
Общие сведения	04
Обновление рынка разведки	06
угроз безопасности нового типа	06
Участники	07
Рынки предсказаний, Арбитры и опосредованный консенсус	10
Определение достоверности	12
Инструменты	13
Вознаграждение за верность	15
Комиссионные сборы	17
Детали протокола	19
Жизненный цикл Вознаграждения	20
Жизненный цикл предложения	23
Репутация	25
Регистр работников	27
Конфиденциальность артефакта	27
Дополнительные рынки	29
План развития	30
Продажа токенов	34
Заявление об ограничении ответственности	37
Заключение	37

PolySwarm за 60 секунд

PolySwarm — децентрализованный рынок разведки угроз безопасности, основывающийся на смарт-контрактах Эфириум и блокчейн-технологии.

PolySwarm стимулирует внедрение инноваций в антивирусное и автоматизированное пространство разведки киберугроз с оборотом 8,5 миллиардов долларов США в год¹ и имеет точные экономические стимулы, поощряющее своевременную иверную разведку угроз безопасности, связанных с файлами, сетевым трафиком и URL-адресами.

PolySwarm определяет экосистему для нахождения угроз безопасности в режиме реального времени, затрагивающую предприятия, потребителей, поставщиков и экспертов по обеспечению безопасности в различных районах мира. Эксперты разрабатывают и улучшают «микро-механизмы», которые проводят автономную разведку последних угроз безопасности, стараясь превзойти механизмы конкурентов. «Доказательством работы» PolySwarm является точность определения угрозы безопасности: рынок вознаграждает экспертов, обеспечивших наилучшую защиту предприятий и пользователей.

В сравнении с сегодняшним специализированным рынком, PolySwarm снизит порог вхождения, обеспечит более широкие варианты покрытия, воспрепятствует дублированию усилий и создаст возможность для взаимодействия между поставщиками продуктов и экспертами по разведке угроз безопасности.

С экономической точки зрения, PolySwarm является специальным элементом, требующем наличие навыков, на рынке предсказаний² с тысячами микро-механизмов («рабочих систем»), исследующих последние изменения вредоносных программных средств со скоростью машины и без участия человека.

PolySwarm разрабатывается компанией **PolySwarm Pte. Ltd.**, финансирование обеспечивается продажей ERC20-совместимых служебных токенов **Nectar** («NCT»).

Благодаря применению служебных токенов, PolySwarm устраняет экономическую выгоду от спекулятивных действий с Nectar,

¹ Jefferies Cyber Security Primer. 18 января 2017 года.

² https://en.wikipedia.org/wiki/Prediction_market

вознаграждая лишь добросовестных участников рынка путем [сбора и распределения Комиссионных сборов \(подробнее см. на р. 6\)](#) между активными участниками, показавшими положительный результат.

Общие сведения

Сегодня для защиты от развивающейся враждебной кибердеятельности предприятия используют смесь из антивирусных программ, систем разведки угроз безопасности и механизмов классифицированного динамического анализа. Пользователи должны оценивать преимущества и недостатки каждого предлагаемого решения и определить для себя, какое решение менее всего повредит их среде.

Сегодняшний рынок препятствует развитию решений, которые бы обеспечили широкое покрытие угроз безопасности.

Решения сегодня фокусируются на зоне комфорта угроз безопасности — прямом экономическом результате деятельности сегодняшнего рынка.

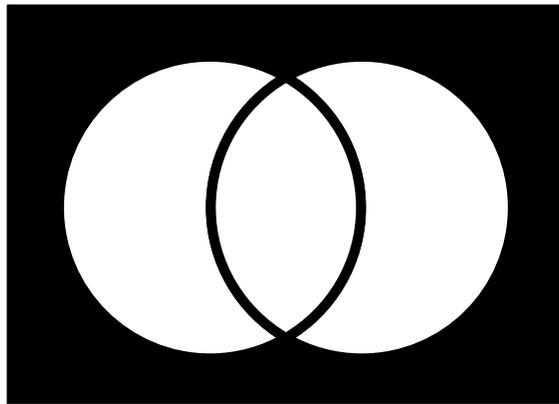


Рисунок А: Черным прямоугольником выделены все возможные угрозы безопасности, с которыми может столкнуться Предприятие; в окрестностях представлены антивирусные программы №1 и №2, соответственно.

Легко (и возможно оправдано) проигнорировать антивирусное решение, не способное обнаружить вредоносную программу WannaCry³, но таким действием сегодняшний рынок эффективно поощряет дублирующую

деятельность поставщиков — несостоятельность рынка, создающую дублирующие затраты. Это является классической проблемой сложившейся ситуации в целом.

Сейчас представьте поставщика, который решит разработать решение, выходящее за пределы зоны комфорта. Если зона комфорта будет определяться угрозами безопасности, с которыми сталкивается большинство предприятий, то такому поставщику будет непросто реализовывать свою продукцию. Как вы убедите потенциального клиента в том, что он столкнется с вредоносными программными средствами, обнаружить/предотвратить/изолировать которые сможете только вы?

В конечном счете, защитники не способны смешивать и сочетать большое количество сегодняшних решений, создание комбинаторного покрытия не подходит для многих сценариев.

В отличие от этого, PolySwarm разовьет экосистему с широким покрытием, которое будет обеспечиваться тысячами «микро-механизмов», управляемыми экспертами по безопасности их разных регионах мира.

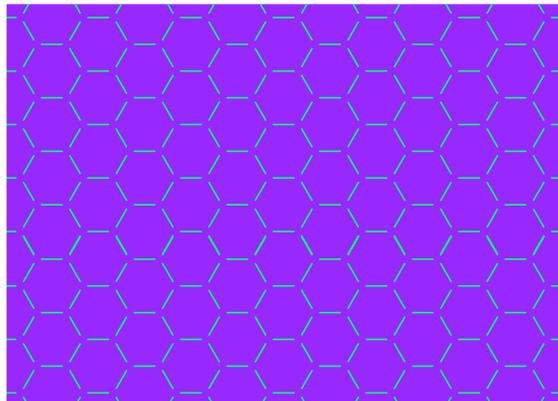


Рисунок В: PolySwarm разовьет экосистему с широким покрытием угроз безопасности.

PolySwarm обеспечит легальный поток дохода для экспертов по безопасности.

Когда местная экономика не способна предоставить хорошо оплачиваемую и добросовестную работу, некоторые эксперты по безопасности начинают заниматься разработкой вирусов-вымогателей, поддерживать работу программ-ботов или применять свои навыки в каких-либо иных дурных целях. PolySwarm предлагает независимую от региона проживания альтернативу: не связанное никакими

обязательствами вознаграждение за добросовестную работу. Эксперты будут состязаться между собой за создание более надежной сетевой защиты.

PolySwarm обращает особое внимание на пользователей.

Рынок PolySwarm направляет экономические стимулы туда, где это наиболее важно: на верное определение злых умыслов (на «разведку угроз безопасности»). Верность определяется новейшим процессом, который мы называем [Опосредованным консенсусом \(подробнее см. на стр. 10\)](#).

Короче говоря, PolySwarm предоставляет пользователям временный доступ к обширной базе решений по обеспечению безопасности, разработанных путем краудсорсинга. Требуется быстро отфильтровать подозрительный файл? Просто воспользуйтесь PolySwarm™.

Обновление рынка разведки угроз безопасности нового типа



NCT-токены PolySwarm («NCT») формируют основу нового рынка, представляющего новейшие инструменты для получения своевременных и верных утверждений наличия злых умыслов в файлах, сетевом трафике и URL-адресах, в совокупности именуемых Артефактами. Структура этих новых инструментов позволяет напрямую стимулировать внедрение инноваций в пространство по разведке угроз безопасности с циклом обратной связи, основывающемся на верных результатах.

PolySwarm использует Комиссионные сборы для блокировки спама и стимулирования добросовестного и активного рыночного участия. Комиссионные сборы определяются по типам транзакций, которые могут использоваться в целях спама, а затем распределяются между активными участниками экосистемы; людьми, предоставляющими Артефакты и определяющими достоверность наличия или отсутствия в них злого умысла. Такое участие измеряется в «скользящем» окне, где более старые вклады в работу рынка «устаревают», это стимулирует принимать непрерывное участие в работе рынка.



Предприятия



Эксперты



Посредники



Арбитры

PolySwarm 1.0 (и настоящий документ) фокусируются только на логическом определении (зловредный/безопасный элемент), но команда разработчиков PolySwarm имеет более обширные планы, чем логическое определение зловредных элементов. Во время разработки PolySwarm 1.0 команда проведет исследование методов стимулирования процесса создания метаданных по артефактам, например, определения вредоносных семейств и того, как ключевые концепции PolySwarm, например, структура рынка с использованием смарт-контрактов, опосредованный консенсус и фокусирование на информационной безопасности, могут помешать работе других соответствующих рынков, например, рынка вознаграждений за нахождение ошибок в программном обеспечении⁴.

Перед тем, как представить инструменты PolySwarm, мы хотели бы рассказать о классах участников, которые будут использовать их.

Участники

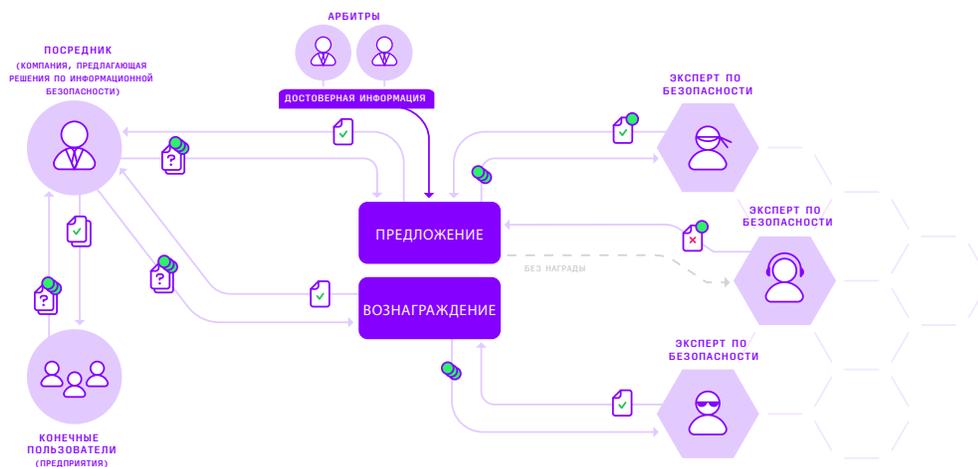
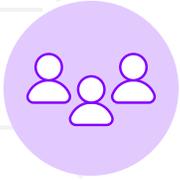


Рисунок С: Обзор жизненных циклов Вознаграждения и Предложения PolySwarm.

⁴ «NasckerOne, но децентрализованно, под псевдонимом и без юридических обременений. На основе блокчейн-технологии.» Не рассматривается в настоящем документе.



Конечные пользователи: Корпоративные и домашние пользователи с подозрительными Артефактами. Конечные пользователи смогут участвовать на рынке PolySwarm посредством Вознаграждений и Предложений (подробнее об этом см. далее) и извлекать своевременные и верные классификации злых умыслов.



Эксперты по безопасности («Эксперты»): Эксперты по вредоносным программным средствам и декомпилированию. Эксперты анализируют последние подозрительные Артефакты и поддерживают работу механизмов определения злого умысла (рабочие системы), подключенных к PolySwarm. Эксперты берут на себя ответственность за «Утверждения», публичные заявления о результатах проведенного ими анализа Артефакта на наличие в нем злого умысла. Эксперты, предоставившие верные Утверждения, получают вознаграждение (в виде NCT-токенов) за свои усилия.

Вознаграждение определяется фактическим объемом работы, выполненным ключевыми участниками. Элементарность — это хорошо, но не всегда, если речь идет о рынке PolySwarm. Технически, PolySwarm смог бы работать только с указанными двумя классами участников. Реалистически же этого не выйдет, так как большинство **конечных пользователей** предпочтут отдать на сторону рутинное взаимодействие с рынком PolySwarm. Прежде чем продолжить, необходимо представить **посредников** (еще одних участников рынка) и определенный подкласс таких посредников.



Посредники: Компании, облегчающие конечным пользователям процесс получения выгоды от работы с рынком PolySwarm. Посредники собирают традиционные фиатные средства (например, плату за подписку) и подозрительные Артефакты со своих клиентов (конечных пользователей) и размещают на рынке **Вознаграждения** и **Предложения** от лица своих клиентов. Посредник несет ответственность за разбор утверждений нескольких Экспертов, создание простого Вердикта по **вредоносности** или **безопасности** рассмотренного элемента и дальнейшее предоставление Вердикта своим клиентам.

Такой тривиальный и возможно наивный подход необходим для простого упрощения утверждений, предоставленных Экспертами. Маловероятно, однако, что такой алгоритм сможет успешно конкурировать с байесовским анализом⁵, не говоря уже о привлечении эксперта. Мы ожидаем, что существующие антивирусные компании и фирмы, выполняющие разведку угроз безопасности, примут участие на рынке PolySwarm в качестве ранних посредников, тем самым улучшив свои собственные решения, благодаря фильтрам PolySwarm для подозрительных Артефактов.

Что касается пользователей, то обновление до средств защиты с поддержкой PolySwarm станет простой задачей: просто выберите надежного посредника и оплатите подписку.

Репутация Посредника основывается на успешном определении достоверности в прошлых Вердиктах. Посредники мотивированы опубликовывать свои Вердикты из-за свойственного им желания создать хорошую репутацию и привлечь новых клиентов, а также получить скидку на Комиссионные сборы рынка (подробнее об этом см. далее). Такие публичные вердикты позволят создать «оценочную карту» посредников, где можно будет оценить реальную мировую эффективность с учетом несинтетических Артефактов с данными, которых просто нет на сегодняшнем рынке⁶.

Арбитры Посредники высшего эшелона, отвечающие за определение достоверности в отношении злого умысла. Определенное количество посредников (число определяется объемом созданных Комиссионных сборов) будут считаться «Арбитрами».



Во время процесса развития, PolySwarm назначит Арбитрами существующих поставщиков решений по разведке угроз безопасности с хорошей репутацией, которые будут готовы часто взаимодействовать с командой PolySwarm, содействовать в определении и устранении ошибок платформы и оказывать помощь в привлечении внимания к новой экосистеме.

Как только PolySwarm 1.0 будет готова к запуску, этим Арбитрам необходимо будет поддерживать рыночные объемы Арбитров высшего эшелона, чтобы сохранить свои статусы.

⁵ Алекс Кантчелиан и др. «Лучшая достоверность по выявлению вредоносных элементов: Техника оценки ярлыков поставщиков антивирусных продуктов». Материалы 8-ой конференции ACM по искусственному интеллекту и безопасности. ACM, 2015 год.

⁶ Самый ближайший аналог — Comparatives AV (<https://www.av-comparatives.org/>).

Рынки предсказаний, Арбитры и опосредованный консенсус

В экосистеме PolySwarm Эксперты по безопасности разрабатывают микро-механизмы, конкурирующие между собой в быстром и верном исследовании подозрительных артефактов. Это исследование выполняется на машинной скорости до установления достоверных данных по злому умыслу артефакта.

Такая структура имеет нечто общее с рынками прогнозирования, например, вознаграждение прошлых утверждений на основании их верности, но она также имеет два важных отличия:

- 1. Для верной классификации артефакта не требуются будущих данных.** «Правильный» ответ на вопрос является ли артефакт вредоносным можно будет определить с уверенностью сразу после того, как этот артефакт станет доступен рабочим системам. PolySwarm имеет структуру, основывающуюся на навыках, в которой ничего не остается без внимания⁷.
- 2. Определение достоверности всегда требует экспертной оценки.** Это контрастирует с «универсальной наблюдательностью» рынков предсказаний (включая рынок Аугур)⁸, которые опираются на участников без навыков и ведут запись событий по мере их появления.

Средство №1 — средство сдерживания азартных игр PolySwarm⁹.

Элемент №2 представляет техническую задачу: каким образом лучше всего стимулировать органы управления для постоянного создания достоверной информации? Ответом PolySwarm является класс Арбитров, а процесс мы именуем опосредованным консенсусом.

⁷ В теории. На практике по крайней мере 2 события могут внести неопределенность: (1) арбитры неправильно определили достоверность статуса в результате чего награда была передана неверным экспертам, (2) анализ, выполненный экспертом, является верным согласно установленной достоверности, но эксперт не согласен с рамками злого умысла – семантический вопрос за пределами PolySwarm. Рекламная вредоносная программа или просто потенциальное нежелательное приложение? Ни одна из переменных не уменьшает коренным образом характер экосистемы PolySwarm, основывающийся на навыках.

⁸ <https://augur.net/>

⁹ Артефакты со злым умыслом на платформах с приложениями по гаданию, заключению пари, игре в азартные игры или платформах с другими пари, основывающимися на шансе, неблагоприятны для всех, PolySwarm специально разработан быть максимальной жестким к такому применению платформ.

Опосредованный консенсус представляет собой типовую парадигму проектирования, которая, как мы надеемся, найдет себе применение в других рыночных проектах по проектированию. Короче говоря, опосредованным консенсусом является процесс рыночного проектирования, в котором подгруппе участников присваивается критическая задача. Эти участники:

1. Обладают соответствующей квалификацией для решения такой задачи (обладают опытом).
2. Имеют свои интересы, связанные с жизнеспособностью рынка (исключая трагедии общего пространства).

Мы создали класс Арбитров для преодоления этих ограничений. По своему определению, к классу Арбитров относятся наиболее активные посредники в экосистеме PolySwarm в любой момент.

Как и посредники, Арбитры связаны договорными обязательствами со своими клиентами для создания Вердиктов из утверждений Экспертов по безопасности. Клиенты доверяют им и пользуются их автоматизированной и, если необходимо, человеческой экспертной оценкой. Эти компании уже имеют личную заинтересованность в публичном документировании верности своей работы (позиция №1).

Являясь наиболее активными посредниками, Арбитры могут достичь наибольших благ, выполняя добросовестную работу, или рискуют больше всего пострадать, работая недобросовестно в экосистеме PolySwarm. Их наибольшая заинтересованность в благополучии экосистемы связывает их финансовые интересы с жизнеспособностью рынка (позиция №2).

Мы разработали Комиссионные сборы для обеспечения дополнительной защиты от нарушений Арбитров, например, для защиты от сговора Арбитра и Эксперта по безопасности.

Определение достоверности

Большая часть подробностей процесса арбитражного голосования была намеренно оставлена на данный момент без определения. Это было сделано по одной простой причине: особенности процесса вынесения арбитражного решения основываются на особенностях практически всех других процессов PolySwarm, где мы ожидаем некоторых изменений.

С учетом вышесказанного, мы ожидаем, что следующие проектные решения высокого уровня будут полезными в этом процессе:

1. Арбитры достигают консенсуса по достоверности **большинством голосов.**
2. Голоса являются неотъемлемой частью **полной цепочки Эфириум** (множество голосов на цикл), что экономит время и финансовые средства (газ в Эфириум) для экосистемы PolySwarm.
3. Для стимулирования участия **Арбитры награждаются Комиссионными сборами за голосование по достоверности злого умысла артефактов.**
4. **Арбитры могут воздержаться от голосования** по любому определенному артефакту. Арбитры могут сделать это в случае, если, например, сочтут себя некомпетентными для определения злого умысла определенного артефакта.
5. При необходимости, **право голосования Арбитра может быть передано дополнительному Посреднику (в порядке объема)** для обеспечения кворума при определении достоверности.
6. В случае необходимости, **мы ожидаем, что участники будут оспаривать определения Арбитров доступными на сегодняшний день способами:** в блогах или технических статьях, описывающих злой умысел или безопасный характер артефакта, который орган управления, например, Арбитр, по ошибке отнес к другой категории: внешний общественный цикл обратной связи.

Команда PolySwarm итеративно проработает особенности арбитражного голосования и схемы стимулирования во время процесса разработки. Мы ожидаем, что ранняя обратная связь с Арбитрами поспособствует решению этих задач.

Темы исследования включают, но не ограничиваются:

- Минимальным количеством Арбитров для кворума
- Процедурой арбитражного сдерживания (для случаев, когда кворума невозможно достичь)
- Соответствующей процедурой вознаграждения
- Стимулом для своевременного определения достоверности, например, только первые X проголосовавших Арбитров получают вознаграждение
- Штрафами за неучастие, например, Арбитры должны проголосовать по вопросу достоверности X% артефактов в определенное временное окно, иначе статус Арбитра будет аннулирован
- (По необходимости) дополнительными средствами сдерживания, направленными против антистимулов

Инструменты

PolySwarm предлагает два ключевых инструмента для конечных пользователей и посредников¹⁰, которые помогут повысить эффективность рынка разведки угроз безопасности:

Предложения Polyswarm: Запросы направляются напрямую Экспертам по безопасности с хорошей репутацией для получения их прогноза по злему умыслу. PolySwarm предоставляет отлаженный доступ к тысячам разработчиков, тем самым обеспечивая традиционный обмен информацией с нетиповыми участниками. Такое взаимодействие обеспечивается Raiden-каналами предложений¹¹ (подробнее см. далее). После того, как каналы будут установлены, Предложения начинают создавать миллисекундную задержку для исследования артефакта.

ПРЕДЛОЖЕНИЕ

¹⁰ В дальнейшем Конечные пользователи и Посредники совместно именуется «Посредниками». Конечные пользователи могут действовать в качестве собственных Посредников. Мы ожидаем, что некоторые крупные предприятия примут участие таким образом.

¹¹ <http://raiden.network/>

Вознаграждения Polyswarm: Постер «Разыскивается» в стиле дикого запада с сопутствующим содержимым Артефакта (например, Разыскивается: Этот Артефакт: вредоносный или безопасный? Награда: 1000 NCT-токенов). Эксперты по безопасности создают себе имена (укрепляют репутацию), успешно соревнуясь между собой за Вознаграждения. Прямых аналогов этому нет на сегодняшнем рынке.

Предложения являются наиболее близким аналогом сегодняшнего рынка антивирусного сканирования по запросу пользователя и работают с миллисекундной задержкой.

Посредники передают Предложения и Артефакты напрямую выбранным Экспертам по безопасности, в некоторых случаях заключается соглашение о неразглашении. Эксперт решает принять ли Предложение или нет, основываясь на своей компетентности в подготовке верного Утверждения по предоставленному Артефакту. Эксперты могут отказаться от Предложения, чтобы не портить свою репутацию, если будут не уверены в своей способности предоставить верное Утверждение. Если Эксперт принимает Предложение, то он берет на себя обязательства предоставить свое Утверждение по злему умыслу в установленные временные рамки. Токены и вознаграждения регулируются и осуществляются исключительно распределяемыми смарт-контрактами.

Выпуск Предложения требует наличия определенной информации об Экспертах, наилучшим образом подходящих для анализа необходимого Артефакта. Для облегчения поиска Эксперты рекламируют свои навыки посредством списков в Регистре работников PolySwarm — аналоге регистров Ethereum dApp¹², таким образом они создают себе репутацию, успешно участвуя в Вознаграждениях аналогичного типа.

Вознаграждения дешевле, чем Предложения и не требуют осведомленности об определенных Экспертах, но Вознаграждения подходят не для всех.

¹² См. [Регистр работников](#) на р. 27 для подробной информации.

¹³ То, что является истиной в PolySwarm 1.0, необязательно останется истиной в будущих версиях платформы. [См. раздел Конфиденциальность артефакта.](#)

Во-первых, Вознаграждения должны являться частью блока Эфириум, что происходит, приблизительно, раз в 15 секунд, и требует наибольших затрат времени при такой схеме. Во-вторых, для размещения Вознаграждения необходима публикация Артефакта¹³. В конечном счете, постеры «Разыскивается» в стиле дикого запада не будут эффективны, если не будут размещаться в публичном месте и со всей известной информацией. Таким же образом, Вознаграждения представляют собой публичные, «умные» (как в смарт-контракте) обязательства вознаградить поставщиков информации, которая приведет к помещению Артефакта на карантин или его освобождению. Благодаря Вознаграждениям формируется критический элемент в цикле обратной связи, который устанавливает достоверность.

Вознаграждение за верность

В отличие от сегодняшнего рынка, PolySwarm предлагает точные вознаграждения, основывающиеся лишь на верности разведки угрозы, что мотивирует Экспертов проводить улучшения, направленные исключительно на обнаружение угрозы (минимальные ложноположительные и ложноотрицательные результаты), и позволяет посредникам извлекать максимальную пользу для своих клиентов. PolySwarm определяет верность как достижение согласия между Утверждениями Экспертов и решением Арбитров по достоверности.

Цикл обратной связи определяется Вознаграждениями PolySwarm. Каждое Вознаграждение награждает Эксперта, предоставившего верное Утверждение, и штрафует Эксперта в случае предоставления неверного — одновременно избегая появления стимулов к сговору между Посредниками и Экспертами¹⁴. Предложения PolySwarm обеспечивают удобные средства, позволяющие достичь типовых деловых двухсторонних отношений, но никак не влияющие на результирующую верность.

Достоверная информация производится и поглощается на рынке PolySwarm следующим образом:

1. Посредник назначает Вознаграждение за Артефакт, оплачивая Комиссионный сбор.
2. Различные Эксперты предоставляют свои Утверждения по этому

¹⁴ Это включает потенциальный интерес сговора между Экспертами и Арбитрами, голосующими за собственные Вознаграждения. Структура Комиссионных сборов PolySwarm исключает случаи, когда Арбитр вносит сомнение в полученную достоверную информацию, а Эксперт, находящийся в сговоре с ним, получает Вознаграждение, превышающее по размеру затраты Арбитра на внесение такого сомнения на рынок.

Артефакту до окончания периода предоставления утверждений по Вознаграждению. Каждое Утверждение предоставляется вместе с суммой NCT-токенов, выбираемой Экспертом («Заявка») и отображающей уверенность Эксперта в своем Утверждении. Комиссионный сбор составляет процент от предоставленной суммы Заявки. Утверждения являются конфиденциальными до окончания периода предоставления утверждений.

3. Посредник выносит свой Вердикт, учитывая Утверждения Экспертов, если находит их подходящими, и передает его клиенту. Посредник мотивирован опубликовывать свой Вердикт, чтобы создавать себе хорошую репутацию и привлекать новых клиентов, а также получать скидку на Комиссионные сборы рынка (подробнее об этом см. далее).
4. Позднее (например, через 7 дней после размещения Артефакта в Вознаграждении), Арбитрам предоставляется возможность определить голосованием является ли Артефакт вредоносным или безопасным. Такая достоверная информация, определяемая позднее, НЕ БЛОКИРУЕТ ВОЗМОЖНОСТЬ ВОЗВРАТА ВЕРДИКТОВ ПО АРТЕФАКТУ. Другими словами, Посредникам не нужно (и они не должны) дожидаться определения достоверности для того, чтобы вернуть результат клиенту.
5. Кворум Арбитров определяет достоверный статус Артефакта. Подробности такого голосования по процессу конверсии достоверности еще не определены. Возможно системой голосования будет простое голосование большинством голосов или пропорциональное голосование большинством голосов (например, основанное на объеме рыночного участия). Эти особенности будут определены на этапе разработки прототипа.
6. После установления достоверности, согласно смарт-контракту Вознаграждения происходит награждение NCT-токенами Экспертов, предоставивших верные Утверждения. Сумма переданных NCT-токенов пропорциональна сумме Заявки Эксперта относительно общего пула верных Заявок.

Сначала может показаться, что здесь хорошо подойдет классический рынок предсказаний: Эксперты предоставляют Утверждения, после чего эти Утверждения сравниваются с достоверной информацией с последующим вознаграждением или штрафованием в зависимости от верности. Неприятностью для PolySwarm является то, что классические рынки предсказания косвенно предполагают источник достоверной информации, которые могут быть проверены всеми участниками. Рынок предсказаний, где задается вопрос, кто победит на выборах или превысит ли цена золота определенную отметку к определенной дате, легко регулировать, так как все участники смогут

проверить предоставленные данные после завершения периода, охватываемого прогнозом. Кто победил на выборах? Превысила ли цена на золота установленную отметку?

Определение злого умысла подозрительного Артефакта требует специальных знаний и опыта, которые неравномерно распределены между участниками PolySwarm. Эта задача имеет свой аналог на рынках предсказаний, затрагивающий медицинские диагнозы¹⁵, когда врачи привносят в решение вопроса различный накопленный опыт и знания.

PolySwarm возлагает определение достоверности на Арбитров. На сегодняшнем рынке роль Арбитра эффективно играют традиционные антивирусные компании. Эти компании «голосуют» (и несут публичную ответственность) за «достоверность» через такие сервисы как, например, VirusTotal. Арбитры на рынке PolySwarm определяются исключительно рыночным участием, предлагая новым игрокам возможность внести свой вклад в ход событий.

Таким образом, мы верим, что этот процесс правильно стимулирует Арбитров выделять средства на проведение должного исследования при определении достоверности в интересах рынка в целом.

Эта концепция элитной группы «устанавливающих» достоверность может применяться и в других сферах. Мы ожидаем, что другие оценят возможности этого механизма для других токенов-платформ, где требуются специальные знания для получения достоверной информации.

Комиссионные сборы

Комиссионные сборы определяются для различных транзакций на рынке PolySwarm и необходимы для достижения двух целей:

1. **Повышение эффективности работы рынка PolySwarm посредством стимулирования действий, влекущих за собой минимальную стоимость газа Эфириум.** Фиксированные Комиссионные сборы применяются к сделкам на PolySwarm для предупреждения поведения, приводящего к созданию излишних транзакций (включая спам-транзакции) и, соответственно, влекущего за собой лишнюю газовую стоимость на рынке. Необходимость PolySwarm рассчитывать Комиссионные сборы независимо от стоимости газа в Эфириум является одной из нескольких причин, почему создание NCT-токенов необходимо для обеспечения существования рынка PolySwarm.

2. **Награждение активных участников рынка PolySwarm пропорционально их (добросовестному) участию.** Комиссионные сборы присуждаются участникам, активно использующим экосистему PolySwarm посредством предоставления Артефактов (посредники, размещающие Вознаграждения) и определения достоверности в отношении умыслов Артефактов (Арбитры, достигающие кворума по достоверности статуса).

Во время развития сети, команда PolySwarm будет симулировать структуры оплаты Комиссионных сборов, приведенные выше, повторяя эти симуляции по мере необходимости для создания наилучших рыночных условий.

Комиссионные сборы за размещение Вознаграждений, оплачиваемые посредниками

Когда посредник размещает Вознаграждение на рынке PolySwarm, к средствам в смарт-контракте применяются следующие Комиссионные сборы:

1. **Фиксированный Комиссионный сбор за размещение.** Это фиксированный Комиссионный сбор побуждает посредника группировать несколько Артефактов в одном Вознаграждении, тем самым понижая нагрузку сети и стоимость газа для всех.
2. **Комиссионный сбор, пропорциональный сумме Вознаграждения.** Вознаграждения с изначально большими суммами Вознаграждения несомненно привлекут к участию больше Экспертов. Этот пропорциональный сбор используется для сопоставления Комиссионного сбора с интересом Экспертов (и нагрузкой сети).

Комиссионные сборы за Утверждения, оплачиваемые Экспертами

Когда Эксперт предоставляет свое Утверждение в отношении Вознаграждения, к средствам на смарт-контракте применяются следующие Комиссионные сборы:

1. **Фиксированный Комиссионный сбор за Утверждение.** Этот фиксированный сбор устраняет стимул для подачи повторных утверждений, которые могут замедлить скорость работы сети.

2. **Комиссионный сбор, пропорциональный сумме Заявки.**

Подключение Канала предложения: Комиссионные сборы Посредника

Предложения возникают в Raiden-каналах, устанавливаемых напрямую между Посредниками и Экспертами. Когда Посредник и/или Эксперт решат создать свой Канал предложения в блокчейне, следующий Комиссионный сбор рассчитывается смарт-контрактом Канала.

1. **Процент от суммы NCT-токенов нетто передается по каналу.**

Комиссионный сбор определяется токенами Посредника после открывания канала. Когда канал закрывается, этот Комиссионный сбор возвращается Посреднику пропорционально неиспользованным токенам канала.

Детали протокола

Здесь приводятся подробности по Вознаграждениям, Предложениям, Утверждениям и Вердиктам, связанным с работой PolySwarm. Вознаграждения и Предложения в совокупности именуется Списками PolySwarm. Заявление Polyswarm: Вознаграждение, Предложение, Утверждение или Вердикт.



Вознаграждения



Предложения



Утверждения



Вердикты

Жизненный цикл Вознаграждения

Для размещения Вознаграждения на рынке Посредник регистрирует Заявление посредством вызова смарт-контракта Вознаграждения PolySwarm.

Заявление о Вознаграждении содержит следующее:

1. **GUID Списка:** Глобальный уникальный идентификатор Списка.
2. **Идентификационные данные Посредника.** Определяются подписью на Заявлении, доступной для проверки любым лицом, владеющим адресом Посредника (открытые ключи формируются из адресов).
3. **Комиссионный сбор за размещение Вознаграждения.** Этот Комиссионный сбор формируется фиксированной суммой + процентом от Суммы Вознаграждения (см. раздел «Комиссионные сборы» выше). Скидка доступна, если Посредник позднее публично предоставит Вердикт.
4. **Сумма Вознаграждения.** Эта сумма размещается в смарт-контракте вместе с Комиссионным сбором за размещение Вознаграждения и передается Экспертам, предоставившим верные Утверждения (или возвращается, если Эксперты не были найдены). Эта сумма схожа со сборами за совершение транзакций на Эфириум или Биткоин платформах и используется для привлечения внимания к Вознаграждению.
5. **Криптографическая контрольная сумма Артефакта.** Изменяемая, но в настоящее время SHA256. Используется для уникального определения Артефакта.
6. **URI-идентификатор Артефакта.** Артефакты не хранятся в цепочке из-за расходов на хранение. Мы ожидаем создания дополнительного рынка для хранения и доставки Артефактов¹⁶, а также того, что некоторые Посредники решат хранить копии всех собранных Артефактов на этом рынке для проведения конкурентного анализа в будущем.
7. **Крайний срок Утверждения:** Крайний срок для подачи

Утверждения. Посредник может менять длительность периодов анализа, учитывая свои требования для конкретного Артефакта. Для проведения более глубокого анализа Артефактов несомненно потребуется больше времени (а также большая сумма Вознаграждения для привлечения внимания), в то время как анализ других Артефактов возможно выполнить в короткие сроки.

После появления Вознаграждения в списке, Эксперты определяют свои возможности для работы с Артефактом, а также то, является ли указанная сумма привлекательной для них. Эта ожидаемая сумма вознаграждения представляет собой функцию их интервала уверенности интервала в отношении злого умысла Артефакта.

Эксперты, согласные принять участие, подают Заявки по своим Утверждениям, представляющие уровень их уверенности (и границы риска). Сумма Вознаграждения вместе с общей суммой всех неверных Заявок присуждается верным Заявкам пропорционально их сумме по отношению к общей сумме верных Заявок.

Взгляните на следующий пример (Комиссионные сборы не учтены для простоты):

1. Посредник размещает Вознаграждение с суммой 2 NCT-токена. Эти 2 NCT-токена помещаются в смарт-контракт Вознаграждения. На данный момент они составляют всю сумму награды для Экспертов, предоставивших верные Утверждения.
2. Эксперты А и В после изучения Артефакта решают утвердить, что он является *безопасным*. Они размещают заявки на 5 и 3 NCT-токена по своим Утверждениям, соответственно.
3. Эксперты С и D после изучения Артефакта решают утвердить, что он является *вредоносным*. Они размещают заявки на 1 и 4 NCT-токена по своим Утверждениям, соответственно.
4. Через некоторое время Арбитры устанавливают достоверность и определяют, что артефакт является *вредоносным*. Таким образом, Эксперты А и В предоставили *неверные* Утверждения, а Эксперты С и D *верные*.
5. Сумма Вознаграждения вместе с Заявками, размещенными Экспертами А и В образуют всю сумму награды, которая будет пропорционально разделена между Экспертами С и D. Сумма награды составит $2 + 5 + 3 = 10$ NCT-токенов.
6. Эксперт С подготовил верное Утверждение и ее Заявка составляла $1/5$ от общей суммы верных Заявок. Эксперт С получит сумму своей Заявки вместе с частью награды: $1 + 1/5 * 10 = 3$ NCT-токена.

7. Эксперт D подготовил верное Утверждение и его Заявка составляла 4/5 от общей суммы Заявок. Эксперт D получит свою заявку вместе с частью награды: $4 + 4/5 * 10 = 12$ NCT-токенов.

В Утверждениях Вознаграждения содержится:



1. **GUID Списка + Криптографическая контрольная сумма:** Уникальная ссылка на Список Вознаграждения.
2. **Идентификационные данные Эксперта:** Также определяются подписью на Заявлении.
3. **Комиссионный сбор по Утверждению:** Этот сбор представляет собой фиксированную сумму + процент от суммы Заявок (см. раздел «Комиссионные сборы»)
4. **Сумма Заявки.**
5. **Утверждение:** Логическое определение «Вредоносный» или «Безопасный» по отношению к умыслу Артефакта. Утверждения хранятся в тайне до истечения срока подачи Утверждений по Вознаграждению. Мы намереваемся использовать слепые обязательства + этап раскрытия для достижения этой цели.
6. **(Дополнительные) метаданные:** Информация, полученная во время создания Утверждения и предложенная Посреднику в качестве дополнительной для применения при расчете Вердикта (например, информация о семействе вредоносного программного обеспечения). Эксперты могут добровольно предоставлять эту информацию для того, чтобы выделить себя и привлечь предложения в будущем.

Посредник оценивает Утверждения после их получения и подготавливает свой Вердикт о том, является ли Артефакт «вредоносным» или «безопасным». Посредник предоставляет свой Вердикт клиенту в качестве окончательного отклика по статусу Артефакта. Посредник может также опубликовать Вердикт (и имеет стимул сделать это для получения скидки по Комиссионному сбору) до завершения его срока действия.

Общественные Вердикты содержат следующее:



1. **GUID Списка:** Уникальная ссылка на Список.
2. **NCT-идентификационные данные Посредника.** Также определяются подписью на Заявлении.

3. **Вердикт:** Логическое определение «вредоносный» или «безопасный» по отношению к умыслу Артефакта.

Через некоторое время Арбитры достигают кворума по достоверности статуса Артефакта. Достоверность статуса сравнивается с мнениями Экспертов и за верные Утверждения начисляются NCT-токены.

Жизненный цикл предложения



Если Посредник решает передать Предложения выбранному Эксперту, он открывает Raiden-канал с этим Экспертом.



Это осуществляется путем создания смарт-контракта **Канала Предложения** с Экспертом, включающего следующее:

1. **Идентификационные данные Посредника и Эксперта.**
2. **Сальдо канала:** Максимальная нетто-сумма NCT-токенов, которую Посредник готов передать Эксперту при закрытии канала (с учетом Комиссионных сборов).



После установления Канала Предложения Посредник передает Эксперту ноль или более Предложений. Каждое Предложение включает следующее:

1. **GUID Списка:** Глобальный уникальный идентификатор Списка.
2. **Сумма Списка.** Эта сумма не должна превышать сальдо смарт-контракта Канала Предложения (за вычетом Комиссионных сборов).
3. **Криптографическая контрольная сумма Артефакта.**
4. **URI-идентификатор Артефакта.** По желанию возможно шифрование Артефакта под идентификационные данные Адресата или Артефакт может иметь другую защиту для обеспечения конфиденциальности.

5. **Крайний срок реагирования:** Крайний срок Отклика на Предложение (см. ниже).
6. **Крайний срок Утверждения:** Крайний срок для Утверждения по этому Предложению.

Если предоставляется вместе с Предложением, Эксперт (Адресат) может выбрать, начать взаимодействовать с Предложением или нет. Адресат определяет для себя, стоит ли начинать оценку этого Артефакта за Предлагаемую сумму в выделенный промежуток времени.

Будущие дела Адресата основываются на его способности предоставлять верные результаты. Если Адресат не уверена в своей способности обеспечить верный результат в выделенный промежуток времени (например, Артефакт является типом файла, который Адресат не способна проанализировать), она может отказаться от Предложения.

Если Адресат решит отказаться от Предложения, то она либо выпускает «отклоняющее» Заявление о заинтересованности, либо ждет истечения крайнего срока для реагирования. Лучшим для Адресата является быстро отклонить предложение, чем ждать истечения крайнего срока для реагирования, так как Посредники ценят Экспертов, не заставляющих их ждать истечения крайнего срока для реагирования для определения следующих действий.

Если Адресат примет Предложение, она выпускает «принимающее» Заявление о заинтересованности до истечения крайнего срока для реагирования.



Заявления о заинтересованности содержат следующее:

1. **GUID Списка + Контрольная сумма:** Уникальная ссылка на Список.
2. **Обязательство по реагированию:** Логические «принимаю» или «отклоняю», определяющие, готов ли Адресат начать работу с этим Предложением и принять на себя обязательства по подготовке Утверждения до истечения крайнего срока предоставления Утверждения по этому Предложению.

Как только Адресат примет Предложение, он будет обязан до истечения соответствующего крайнего срока предоставить свое Утверждение по этому Предложению.



Эти Утверждения содержат следующее:

1. **GUID Списка + Контрольная сумма:** Уникальная ссылка на Список.
2. **Утверждение:** Логическое определение «вредоносный» или «безопасный» по отношению к умыслу Артефакта.
3. **(Дополнительные) метаданные:** Информация, полученная во время создания Утверждения и предложенная Посреднику в качестве дополнительной для применения при расчете Вердикта (например, информация о семействе вредоносного программного обеспечения). Эксперты могут добровольно предоставлять эту информацию для того, чтобы выделить себя и привлечь предложения в будущем.

После того, как Эксперт передаст свое Утверждение Посреднику, Посредник подпишет Raiden-сообщение об обязательстве передать сумму Предложения, после чего риски Эксперта будут ограничены лишь полученными аналитическими данными. После чего, общая сумма размещается в блокчейне и Канал предложения закрывается.

В отличие от Вознаграждений, Предложения не имеют цепного механизма обратной связи по вопросам достоверности. Вместо этого, Адресаты, не предоставившие Утверждения до истечения установленного срока или предоставившие неверные Утверждения (что будет определено анализами вне цепочки позднее), могут больше не привлечь других предложений. Следовательно, поддержание своей репутации схоже с циклом обратной связи вне цепочки, где давление рынка используется для поддержания добросовестной работы Адресатов.

После закрытия Канала предложения происходит сбор комиссии. Как и другие Комиссионные сборы, эти сборы передаются активным участникам рынка. Комиссионный сбор обеспечивается смарт-контрактом Канала предложения, отклоняющим установление Каналов предложения, не соответствующих требованиям.

Репутация

В отличие от других токенов-платформ (например, Аугур) **PolySwarm не старается формализовать понятие репутации и встроить его в рыночные транзакции.**

Причина этого довольно проста: невероятно сложно прогнозировать, какие результаты обработки данных ценят различные участники; и каким образом выполняется их оценка. То, что наилучшим образом подходит для Посредника А может не лучшим образом подходить для

Посредника В, бесполезно пытаться наладить их работу с таким допущением. Вместо этого, механизм PolySwarm просто передает виды данных или создает стимул для их раскрытия, что несомненно делает вклад в создание репутации.

Алгоритмы создания репутации скорее всего будут сохраняться в секрете, аналогично алгоритмам перегона Утверждения в Вердикт. Посредники будут дифференцировать себя, взаимодействуя с наиболее подходящими Экспертами для выполнения работ по Артефактам. Эксперты будут дифференцировать себя, поддерживая положительную историю правильных Утверждений после определения их достоверности. Кроме этого, посредством предоставления метаданных, например, информации по семейству вредоносного программного обеспечения, к которому, по их мнению, принадлежит исследованный артефакт.

Прототип Посредника, подлежащий разработке, будет перегонять различные результаты обработки данных в простые «баллы» репутации и понятную цветовую схему. Такой контрольный способ перегонки несомненно будет полезен многим, но он может быть также заменен на другой или изменен для соответствия потребностям участников. Вероятно Эксперты захотят внедрить систему репутации для оценки Посредников, но ожидается, что бизнес-логика такой системы будет еще сложнее и будет существенно отличаться среди участников.

Контрольный «демон» PolySwarm будет «разрушать» старые данные, поддерживая «скользящее окно» для репутации участников. Мы верим, что такой подход с использованием «скользящего окна» необходим для исключения блокировки новых участников рынка.

Мы ожидаем использования следующих результатов обработки данных в базовой реализации Посредника:

1. **Верность Утверждения** (относительно достоверности и/или анализа вне цепочки).
2. **Частота и среднее время отклика для Вознаграждений и Предложений.** В случае с Предложениями, Посредники смогут выбрать публикацию сводных данных, обычно доступных только в Канале предложения. Посредники могут поощрять Экспертов, проявляющих быструю и постоянную заинтересованность.
3. **Возможность сохранять конфиденциальность Артефактов, поставляемых с Предложениями.** Вероятно это гибридный рыночный/внерыночный анализ.

Посредники смогут просматривать прошлые Вердикты своих конкурентов и пытаться находить в них ошибки (например, Посредник А заявил, что образец является безопасным, но фактически он был определен

вредоносным). Эксперты могут принимать меры, направленные на избежание ведения дел с Посредниками, чьи условия должного исследования в общем невозможно реализовать или эти условия часто невозможно применить при каких-либо конкретных обстоятельствах (например, Посредник А часто относил документы Microsoft Word не к той категории, что привело к тому, что определенные Эксперты стали избегать проведения анализа документов Microsoft Word для Посредника А). Другими словами, среди других входных данных, Эксперты могут быть заинтересованы в верности Вердиктов, подготавливаемых Посредниками.

Потребители будут вероятно опираться на обобщенные Отчеты для потребителей, веб-сайты или публикации со сравнениями, например, AV-Comparative, которые будут публиковать сведения по каждому Посреднику, возможно с указанием примерных вводных данных с известным выявленным злым умыслом и проведенной проверкой.

Регистр работников

Эксперты в экосистеме PolySwarm будут, во многих случаях, пользоваться автоматизированными рабочими системами. *Работники* — это системы, автоматически реагирующие на появляющиеся Вознаграждения и *Предложения*, возможно направленные на особые типы файлов или сетевой трафик. На рынке PolySwarm будет доступен децентрализованный Регистр работников для упрощения процесса поиска предложений для Экспертов.

Мы разработаем общий интерфейс и дескрипторный язык для публичной регистрации Работников. Эти элементы будут взаимодействовать с Регистром PolySwarm, смоделированным по примеру первоначального регистра Ethereum dApp. Регистр работников PolySwarm будет включать описания особых навыков Экспертов (например, «Я разбираюсь в двоичных кодах Mac OS Mach-0» или «Я работаю с документами Microsoft Word»).

Конфиденциальность артефакта

Конфиденциальное раскрытие Артефактов посредством инструмента *Предложение* является первоклассной особенностью рынка PolySwarm. Однако, без дополнительных мер предосторожности, Посредникам, использующим *Предложения*, возможно всегда придется доверять

мотивированности и техническим способностям Экспертов по безопасности, направленных на отражение нападающих.

Мы ожидаем, что это условие доверия повлечет за собой рост числа дополнительных рынков и новейших способов применения технологий, направленных на сокращение консолидированного доверия. Далее приведены несколько примеров инструментов, созданных в верхней части PolySwarm для обеспечения требований, связанных с конфиденциальностью.

Минимизация доверия посредством Intel SGX

Intel SGX — это новая технология, изначально поставляемая вместе с семейством процессоров Skylake. На высоком уровне SGX обеспечивает нечеткие вычислительные среды внутри «анклавов». Содержимое блоков памяти анклавов SGX недоступно для другого программного обеспечения и пользователей одной системы, независимо от уровня доступа. В контексте PolySwarm, SGX анклавы позволяют Экспертам сканировать Артефакты, не раскрывая их содержимое Исследователю и не предоставляя исследованных данных кому-либо еще. Технология SGX обещает понизить уровень взаимного доверия между Посредниками и Экспертами.

Эксперты смогут использовать аккредитованные (и аттестованные) SGX анклавы для работы с Артефактами и их исследованными данными, и создать Утверждение, которое можно будет предоставить Посреднику. Существуют некоторые технические препятствия, которые еще следует преодолеть, но мы уверены в том, что SGX можно будет использовать в анклавах для целей бутстреппинга. Дальнейшие итерации PolySwarm смогут позволить Посредникам стать авторами будущих заявлений о «SGX Вознаграждениях» на рынке PolySwarm с раскрытием Артефактов только анклавам с бутстреппингом.

Консолидация доверия посредством Посредников по SaaS (Сканирование как услуга)

Эксперты смогут передавать вычислительные задачи третьим сторонам по ряду причин, которые могут относиться к PolySwarm или нет. Например, мы ожидаем, что множество Экспертов будут использовать AWS, Google Compute Engine, Azure или другие вычислительные сервисы по запросу для пропорционального изменения своего Утверждения согласно потребностям PolySwarm рынка. Это не является по существу PolySwarm-мотивированным вычислительным решением.

Мы ожидаем, что стимулы, характерные PolySwarm для SaaS предприятий будут расти естественным путем. В контексте конфиденциальности, участники будут создавать SaaS компании, которые будут выступать в качестве доверительных третьих сторон

между Посредниками и Экспертами, поддерживая исполнение ими соглашений о неразглашении. Эти SaaS компании будут стремиться той же цели, что и SGX анклав — защищать Артефакты от Экспертов и исследованные данные от Посредников.

Посредники смогут понять, что намного проще доверять доверительным сторонним SaaS предприятиям, имеющим репутацию в обществе, чем большому числу Экспертов, личности которых могут быть не установлены. Такие Посредники станут авторами большего количества Предложений, которые будут адресованы SaaS предприятиям, а не напрямую Экспертам.

Дополнительные рынки

Рынок PolySwarm создаст потребность в формировании дополнительных рынков. Один из таких рынков (Сканирование как услуга) ранее обсуждался в контексте предоставления дополнительных средств управления конфиденциальностью. Ниже приведены некоторые дополнительные ожидаемые рынки.

Посредники

Этот рынок очевиден и тщательно рассмотрен в настоящем документе. Многие потребители решат вести дела с рынком через Посредника, но работа через Посредника не является строгим требованием.

Услуги по публикации Артефактов

Посредник должен обеспечить доступность Артефакта Экспертам при размещении Вознаграждения или Предложения на рынке. Предприятия, размещающие Артефакты, смогут предоставлять эту услугу, обеспечивая плавное участие в использовании. Их клиентами станут Потребители и Посредники. Мы также ожидаем, что многие Посредники начнут предлагать услуги по публикации Артефактов.

Услуги по отслеживанию репутации

Три бюро кредитной информации в Соединенных Штатах пользуются доверием банков и поддерживают регистра учет «фактов», относящихся к индивидуальной благонадежности. Рынок PolySwarm обеспечит аналогичное требование; одни участники рынка захотят

оценить благонадежность других участников по разным причинам, которые были ранее обсуждены. Вероятен рост услуг, связанных с отслеживанием благонадежности участников, данные будут использоваться для понижения рисков контрагентов.

План развития

Ниже приведены предварительные этапы развития PolySwarm. Каждый этап: (1) предложит новый функционал (2) предоставит документацию и испытания, обеспечивающие транзакции Посредника, Эксперта и Конечного пользователя.

PolySwarm имеет четкое преимущество развития по сравнению с такими сетями как Биткоин и Эфириум, которые обязаны всегда сохранять все транзакции. После установления достоверности или открытия Канала предложения в цепочке, Посредники и Эксперты получают все, что им необходимо от этой сделки: исследованные данные по Артефакту и NCT-токены, соответственно. Такая элементарность дает нам запас и позволяет вносить ранее несовместимые изменения до релиза версии 1.0 бесплатно и без нарушений консенсуса, свойственных другим сетям.

V0.1 Альфа (30 апрель 2018)

Альфа-версия PolySwarm будет фокусироваться на подготовке прототипа комплексного потока операция для Вознаграждений после успешной продажи токенов. Этот первоначальный релиз позволит команде PolySwarm заняться процессом бутстреппинга всерьез. Посредники и Эксперты смогут совершать транзакции в тестовой сети PolySwarm («testnet»). В тестовой сети будут доступны основные смарт-контракты Вознаграждений, что позволит Посредникам размещать Вознаграждения, Экспертам предоставлять Утверждения и Посредникам выносить Вердикты.

Мы ожидаем, что во время альфа-этапа будет выполнено следующее:

- Смарт-контракт «Менеджер предложений», удерживающий Суммы предложений и комиссионные сборы, принимающий Утверждения, публикующий Вердикты и награждающий Экспертов, предоставивших верные Утверждения
- Размещение Артефактов и их перемещение на склад вне PolySwarm и с него (например, S3 или IFPS)

- Прототип алгоритма выбора Арбитров после истечения срока Вознаграждения
- Базовые реализации для публикации Вознаграждений, отклика на Утверждения и определения достоверности Арбитрами

V0.2 Бета (31 май 2018)

Бета-версия PolySwarm сфокусируется на предоставлении поддержки Предложений PolySwarm по Raiden-каналам. Предложения создаются для обеспечения высокопроизводительной, по сравнению с Вознаграждениями, оценки Артефактов и это требует устройства более эффективного блокчейна для каждой транзакции. В бета-версии PolySwarm будут использоваться смарт-контракты. Мы ожидаем реализации этого функционала с помощью прямых, одноранговых, Raiden-каналов между Посредниками и Экспертами в тестовой сети.

Мы ожидаем, что во время бета-этапа будет выполнено следующее:

- Каналы предложения
 - Децентрализованное установление канала
 - Отправка нескольких Предложений по одному каналу
 - Размещение NCT-токенов при закрытии канала
- Базовая реализация для создания Предложения и отклика
- Базовая реализация для обеспечения уведомлений об определении достоверности Арбитрами и отклик
- Сбор Комиссионного сбора и смарт-контракты по дистрибуции
- Исследование и определение доверия (в NCT-токенах), требуемого для особого объема Артефакта
- Комплект инструментов для разработки Предложения/ Вознаграждения: интегрированная среда для тестирования и реализации для Экспертов и Посредников, автоматически обслуживающая Вознаграждения и Предложения

V0.3 Гамма (30 июль 2018)

Гамма-версия PolySwarm сфокусируется на предоставлении возможностей для установления необходимых контактов, что упростит сотрудничество между Посредниками, Экспертами и Арбитрами. Эксперты смогут указывать свою квалификацию в Работниках, настроенных на определенные виды Артефактов. Мы ожидаем, что Эксперты получат возможность использовать Работников в рекламных целях в Регистре PolySwarm. Регистр работников позволит Посредникам без риска находить Работников до выхода стабильной версии платформы (в гамма-версии продолжится использование тестовой сети PolySwarm).

Кроме того, в этом релизе будет выполнено улучшение и расширение инструмента для Вознаграждения с учетом опыта его работы в альфа- и бета-версиях. Например, мы ожидаем, что для Вознаграждений станет полезна возможность запроса Утверждений, являющихся конфиденциальными для других Экспертов и раскрываемых только после истечения срока подачи Утверждений.

Мы ожидаем, что во время гамма-этапа будет выполнено следующее:

- Язык описания работника (WDL), описывающий возможности анализа артефакта и атрибуты авторства Эксперта (для репутации)
- Децентрализованный регистр для поиска работников и их возможностей.
- Конфиденциальность Утверждений по Вознаграждениям до истечения установленного крайнего срока
- Завершение выбора Арбитра, отклик и комплексный цикл обратной связи по Вознаграждению

Мы ожидаем, что гамма-версия платформы будет включать все ее возможности.

Polyswarm 1.0 (Q4 2018)

Стабильная версия PolySwarm будет фокусироваться на устранении ошибок, допущенных в гамма-версии PolySwarm до перехода с тестовой сети (тестовые токены) на реальный рынок PolySwarm.

Сверхплановой целью, если это позволит время и финансирование, в стабильную версию будет встроена конфиденциальность первого класса посредством ограничения аудитории Вознаграждения.

Polyswarm V2.0 (Q2 2019)

Второй стабильный релиз PolySwarm в настоящий момент имеет две цели: расширить Предложения и Вознаграждения для обработки большего числа типов Артефактов (например, URL-адресов и сетевых потоков) и упростить применение PolySwarm для Предприятий и Домашних пользователей.

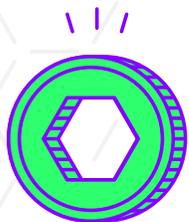
Расширение количества типов Артефактов в последующей версии PolySwarm должно позволить работать с, например, автоматизированными попытками фишингового определения URL-адреса пользователя с прямым размещением Вознаграждений и Предложений в информационном наполнении.

Расширение защит PolySwarm напрямую до конечного предела является главной целью последующих версий платформы. Мы предполагаем разработать базовую реализацию Пакета защитных средств для оконечных устройств с открытым исходным кодом, который будет автоматически блокировать вредоносные артефакты, основываясь на данных PolySwarm. Мы считаем эту открытую структуру ключом к расширенной адаптации конечных пользователей.

Возможности в будущем

Последующие релизы PolySwarm будут отображать развивающийся ландшафт угроз и использование сети в мире. Мы видим несколько возможностей, предоставляемых PolySwarm, для следующих функций, которые способны обеспечить пользу для сети и достичь конечной цели по обеспечению защиты конечных пользователей:

- Гибкая конфиденциальность Артефакта
 - Основная: Артефакты выборочно раскрываются Экспертам или поставщикам SaaS
 - Продвинутая: Артефакты никогда не раскрываются кому-либо за пределами SGX анклавов полностью гомоморфных механизмов
- Новые инструменты (например. предоставление по подписке данных по угрозам)
- Предоставление контейнеров Работников конечная тока-резидент, заменяющих собой сегодняшние пакеты защитных средств для конечных точек.



Продажа токенов

Техническое развитие, заинтересованность сообщества и информационная осведомленность участников для экосистемы PolySwarm будут обеспечиваться компанией PolySwarm Pte. Ltd. на финансовые средства, полученные с продажи токенов.

Токены будут обмениваться участниками за разведку угроз. NCT-токены приводят в действие все основные элементы PolySwarm: Размещение Вознаграждения, установление/освобождение/замена Канала предложения, регистрация Утверждения и определение достоверности. Благодаря продаже служебных NCT-токенов, курсы обмена для NCT на разведку угроз получают преимущество перед более крупным ETH рынком благодаря своей обособленности, обеспечивая активное участие в PolySwarm без учета колебаний ETH.

В этом разделе предоставлен обзор высокого уровня экономики токенов PolySwarm В случае расхождения между этим документом и Соглашение по продаже токенов («Соглашение») последнее будет иметь преимущественную силу. [Соглашение по продаже токенов доступно в сетевом варианте.](#)

План-график

В настоящее время PolySwarm Pte. Ltd., занимается реализацией программы предварительных продаж токенов для приглашенных участников. Открытая продажа NCT-токенов запланирована для квалифицированных покупателей на 20 февраля 2018 года в 19:00 по Гринвичу. Продажа будет прекращена 22 марта 2018 года в 19:00 по Гринвичу.

Требования к покупке

NCT-токены можно будет приобретать исключительно за Эфир (ETH). Потенциальным покупателям рекомендуется обеспечить достаточную сумму ETH до начала продаж.

При продаже токенов будут применяться правила «знай своего клиента» (KYC) с уникальным техническим механизмом для привязки покупок к результатам обработки данных KYC, включая, без ограничения: Страна происхождения, адрес электронной почты, полное имя, IP-адрес и принятие условий Соглашения по продаже токенов.

Ограничения/лимиты

Создание токенов прекратиться после завершения периода их продажи.

Общее количество NCT-токенов будет определено во время периода продажи.

Максимальное количество токенов ограничено. Ограничение основывается на ограничении максимального финансирования в долларах США, цене NCT (в ETH) и текущем курсе обмена ETH к доллару США. См. веб-страницу по продаже токенов, чтобы узнать об ограничениях по NCT, стоимости, траншевом финансировании и многом другом.

Размещение

70 % NCT-токенов будет реализовано во время периода продаж.

50 % из оставшихся 30 % будут «сброшены» предприятиям, поставщикам и Экспертам по безопасности, заинтересованным в оказании помощи для запуска экосистемы PolySwarm. Получатели выбираются по собственному усмотрению PolySwarm Pte. Ltd.

Оставшиеся 15 % токенов будут использоваться PolySwarm Pte. Ltd. в целях обеспечения наилучшей адаптации экосистемы PolySwarm. В качестве наглядного примера, токены могут предлагаться за участие в хакатонах PolySwarm. Это распределение будет осуществлено по собственному усмотрению PolySwarm Pte. Ltd.

Распределение

Мы предвидим, что сумма ETH, полученная с продажи служебных токенов Nectar PolySwarm («NCT»), будет распределена следующим образом:



- **54,51 %** – Разработка протоколов и программного обеспечения
- **3,00 %** – Офисные расходы
- **4,06 %** – Эксплуатационные накладные расходы (поездки, проживание и т. д.)
- **14,49 %** – Юридические расходы
- **13,62 %** – Маркетинговые расходы
- **10,32 %** – Налоговые расходы

Команда PolySwarm ожидает понижения юридических расходов в 2019/2020 финансовом году. Остаток будет отнесен к маркетинговым расходам, накладным расходам и заработной плате разработчиков.

Налог 10,32 % является небольшим, но это небезосновательно. Так лучше для участников: больше финансирования будет выделено напрямую на развитие и продвижение PolySwarm.

Заявление об ограничении ответственности

Цель настоящей брошюры — предоставление технической информации для будущих владельцев токенов. Продажа токенов PolySwarm будет финансировать разработку начальных прототипов и испытание экономических инструментов, представленных здесь. Мы предполагаем, как и любой рассудительный участник, что информация, представленная в настоящем документе, может меняться на этапе разработки стабильной версии платформы и во время периодов испытаний. Интересы PolySwarm Pte. Ltd. и покупателей токенов вместе направлены на создание жизнеспособного рынка, который по-настоящему сможет изменить индустрию разведки угроз безопасности

Заключение

PolySwarm — это новейший рынок и связанный с ним ERC20 токен (NCT), который создается для изменения индустрии разведки угроз безопасности посредством внедрения новых методов взаимодействия между экспертами по безопасности, поставщиками и предприятиями. Команда PolySwarm проведет запуск токена для финансирования разработки программного обеспечения и развития сообщества вокруг этого нового рынка.

Надеемся, что вы присоединитесь к нам для защиты пользователей со всех сторон (**All Angles™**).

