Сеть XY Oracle: сеть криптографического определения на основе доказательств происхождения

Arie Trouw (Ари Трау)*, Markus Levin (Маркус Левин)†, Scott Scheper (Скотт Шепер)‡

Январь 2018

Введение

Благодаря растущему присутствию связанных, ориентированных на местоположение технологий, наша конфиденциальность и безопасность в значительной степени зависят от точности и достоверности информации о местоположении. Были предприняты различные попытки устранить необходимость в централизованных объектах, контролирующих поток данных местоположения, но каждая попытка основывалась на целостности устройств, собирающих эти данные в физическом мире. Мы предлагаем сеть без доверчивых криптографических местоположений, используя новую формулировку, основанную на цепочке доказательств нулевого знания, чтобы установить высокую степень достоверности данных о местоположении. Сеть XYO (XY Oracle Network) представляет собой абстракцию, которая обеспечивает многоуровневую проверку местоположения во многих классах устройств и протоколах. В его основе находится набор новых криптографических механизмов, известных как Доказательство происхождения & Связной свидетель, которые связывают все возможности технологии блокчеин и сбора данных в реальном мире в систему с прямыми приложениями.

---

1 Введение

С появлением основанных на блокчеин смарт-контрактов, не требующих верификации, потребность в услугах Оракула, который разрешает результаты контракта, значительно выросла. Большинство современных реализаций интеллектуальных контрактов полагаются на единый или агрегированный набор авторитетных оракулов для урегулирования результата контракта. В тех случаях, когда обе стороны могут согласовать полномочия и неподкупность указанного оракула, этого достаточно. Однако во многих случаях либо соответствующий оракул не существует, либо оракул не может считаться авторитетным из-за возможности ошибки или коррупции.

В эту категорию попадают оракулы. Определение местоположения физического предмета мира зависит от компонентов отчетности, ретрансляции, хранения и обработки данного оракула, все из которых имеют вероятность ошибки и могут быть повреждены. Риски включают в себя манипулирование данными, загрязнение данных, потерю данных и сговор.

---

*XYO Network, **arie.trouw@xyo.network**
†XYO Network, **markus.levin@xyo.network**
‡XYO Network, **scott.scheper@xyo.network**

Таким образом, существует следующая проблема: на достоверность и точность местоположения негативно влияет отсутствие децентрализованного оракула, не нуждающегося в верификации. Платформы, такие как Эфириум и EOS, широко используются из-за их способности безопасно взаимодействовать друг с другом в режиме первичного использования с участием эскронов для привлечения средств в форме ICO. Однако до этого момента каждая платформа полностью ориентировалась на мир онлайн, а не на физический мир из-за загруженной, коррумпированной целостности данных текущих информационных каналов.

Сеть XYO работает над концепцией, позволяющей разработчикам, пишущим смарт-контракты на платформах блокчеин, взаимодействовать с физическим миром, как если бы это был API. Сеть XYO - это первый в мире протокол оракула, который позволяет двум субъектам совершать сделки в реальном мире без централизованной третьей стороны. Наши статьи позволяют нам сделать проверку местоположения доверчивой для разработчиков, создав протокол с новыми вариантами использования, которые не были доступны до сегодняшнего дня.

Сеть XYO будет построена на существующей инфраструктуре более чем 1.000.000 устройств, циркулирующих в мире, которые были распределены через потребительский бизнес. Bluetooth и GPS-устройства XY позволяют ежедневным потребителям размещать физические следящие маяки на вещах, которые они хотят отслеживать (например, ключи, багаж, велосипеды и даже домашние животные). Если они ошибаются или теряют такой элемент, они могут видеть, где именно, просматривая его местоположение в приложении для смартфонов. Всего за шесть лет сеть XYO создала одну из крупнейших сетей Bluetooth и GPS в мире.

---

2 Предыстория & Предыдущие достижения

2.1 Доказательство местоположения

Концепция доказуемого местоположения существует с 1960-х годов и может быть датирована еще в 1940-х годах наземными радионавигационными системами, такими как LORAN [1]. Сегодня есть службы определения местоположения, которые стекают несколько сред проверки друг на друга, чтобы создать Доказательство местоположения посредством трехсторонней и GPS-услуг. Однако эти подходы еще предстоит решить наиболее важный компонент, с которым мы сталкиваемся сегодня в технологиях локации: проектирование системы, которая обнаруживает мошеннические сигналы и контролирует коррумпированность данных местоположения. По этой причине мы предлагаем, чтобы самая значительная платформа криптолокации сегодня будет той, которая больше всего фокусируется на доказательстве происхождения сигналов физического местоположения.

Удивительно, но концепция применения проверки местоположения на технологии блокчеин впервые появилась в сентябре 2016 года в DevCon2 Эфириум. Она была представлена Lefteris Karapetsas, разработчиком Эфириум из Берлина. Проект «Карапетсас», Сикорка, позволил развернуть смарт контракты на месте в реальном мире, используя то, что он назвал «Доказательством присутствия». Его применение мостового местоположения и мира блокчеин сосредоточивалось в первую очередь на случаях использования расширенной реальности; и он представил новые концепции, такие как вызов вопросов в доказательство своего местонахождения [2].

17 сентября 2016 года термин «Доказательство местонахождения» официально появился в сообществе Эфириума [3]. Затем он был дополнительно разъяснен разработчиком Фонда Эфириум, Мэттом Ди Ферранте:

«Доказательство местонахождения, которому вы можете доверять, честно является одним из самых сложных вещей для реализации. Даже если у вас есть много участников, которые могут подтвердить местоположение друг друга, нет никакой гарантии, что они не просто пойдут в любую точку в будущем, а так как вы всегда полагаетесь только на отчетность большинства, это огромная слабость. Если вам может потребоваться какое-то специализированное аппаратное устройство с технологией защиты от несанкционированного доступа, так что закрытый ключ уничтожается при попытке открыть его или изменить прошивку на нем, тогда вы, возможно, получите большую безопасность, но в то же время не похоже, что невозможно спутать сигналы GPS. Для правильной реализации этого требуется столько резервного и так много разных источников данных, чтобы иметь какую-либо уверенность в точности, это должен был быть очень хорошо финансируемый проект ». [3]

-Матт Ди Ферранте, разработчик, Фонд Эфириум

2.2 Доказательство местоположения: недостатки

Таким образом, Подтверждение местоположения можно понимать как использование мощных свойств блокчеин, таких как временное тиснение и децентрализация, и объединение их с устройствами, которые трудно обмануть. Подобно тому, как слабость смарт-контрактов сосредотачивается вокруг оракулов, которые используют один источник истины (и, следовательно, имеют один источник отказа), системы криптоопределения сталкиваются с одной и той же проблемой. Уязвимость в существующих технологиях криптоопределения вращается вокруг устройств, которые сообщают о местоположении объекта. В смарт-контрактах этот источник данных является оракулом. Истинные инновации, лежащие в основе сети XYO, сосредотачиваются вокруг доказательства местоположения, лежащего в основе компонентов нашей системы, для создания безопасного протокола шифрования.

---

3 Сеть Oracle XY

«Необходимость в сложной системе для дополнения GPS уже давно известна. GPS исключительно точна и надежна, но задержка, коррупция, кибератаки и другие формы помех, по-видимому, растут по частоте и серьезности. Это может привести к разрушительным последствиям для нашей жизни и экономической деятельности ». [4]

-Дана Говард, Президент Фонда PNT

3.1 О сети

Целью сети XYO является создание надежной, децентрализованной системы оракулов, которая устойчива к атакам и дает максимально точный ответ при запросе доступных данных. Мы достигаем этого путем набора абстракций, который значительно снижает риск спуфинга местоположения через цепочку доказательств без разглашения информации по компонентам системы.

3.2 Обзор сети

Наша система обеспечивает точку входа в протокол подключенных устройств, который обеспечивает высокую достоверность данных о местоположении через цепочку криптографических доказательств. Пользователи могут выдавать

транзакций, называемых «запросами», чтобы получить часть данных о местоположении на любой платформе блокчеин, обладающей интеллектуальной функциональностью контракта.[1] Агрегаторы из сети XYO затем прослушивают эти запросы, выданные по контракту, и берут ответы, которые имеют наивысшую точность от децентрализованный набор устройств, которые ретранслируют криптографические доказательства на эти агрегаторы. Эти агрегаторы затем возвращают эти ответы в интеллектуальный контракт после достижения консенсуса по ответу с лучшим результатом. Эта сеть компонентов позволяет определить, находится ли объект в определенной XY-координате в данный момент времени, с самой доказуемой, надежной уверенностью.

Сеть XYO имеет четыре основных компонента: **Стражи** (Сборщики данных), **Мосты** (ретрансляторы данных), **Архиваторы** (Хранилители данных) и **Дивинеры** (Агрегаторы ответов). Стражи собирают информацию о местоположении через датчики, радиоприемники и другие средства. Мосты берут эти данные у Стражей и предоставляют их Архиваторам. Архиваторы хранят эту информацию для анализа Дивинерс. Дивинеры анализируют эвристику местоположения у архиваторов, чтобы генерировать ответы на запросы и присваивать им оценки точности. Дивинеры затем передают эти ответы обратно в смарт-контракт (таким образом, Дивинеры служат в качестве оракулов). Оценка точности, названная «Целевой показатель происхождения», определяется набором доказательств нулевого знания (распространяемая информация без нарушения приватности), известных как «Доказательство происхождения цепи». Эта цепочка гарантирует получение двух или более данных из одного источника, не раскрывая никакой основной информации. Каждый компонент по пути запроса генерирует собственное доказательство происхождения, которое затем привязывается к каждому компоненту, к которому он передает данные. Доказательство происхождения - это новая формулировка, которая строит цепочку криптографических гарантий по пути ретрансляторов в сети, чтобы обеспечить высокую достоверность данных реального мира. Это доказательство происхождения цепи инкапсулирует уверенность, которую мы можем иметь в части данных местоположения, вплоть до самых первых устройств, которые собрали данные. В следующем разделе мы рассмотрим детпльно, как функционирует Доказательство происхождения.

Для создания децентрализованного консенсусного механизма среди Дивинеров, сеть XYO будет опираться на открытый, неизменный блокчеин, известный как **XYOMainChain,** который хранит транзакции запросов вместе с данными, собранными из Дивинерса и их ассоциированной оценкой происхождения. Прежде чем мы погрузимся в детали функциональности всей системы, мы четко определим обязанности каждого компонента в нашей сети.

3.2.1 Стражи

Стражи - свидетели местоположения. Они мониторят эвристику данных и ручаются за достоверность и точность эвристики, производя временные бухгалтерские книги. Самым важным аспектом Стражей является то, что они производят бухгалтерские книги, которые могут быть уверены в том, что другие компоненты получены из одного источника. Они делают это, добавляя Доказательство происхождения в цепочку ретрансляции криптографических доказательств. Учитывая, что сеть XYO является беззащитной системой, Стражи должны стимулировать предоставление информации о честном местоположении. Это делается путем

[1] Эфириум, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter- party, Monax and others

объединения компонента репутации с компонентом оплаты. Стражи награждаются Токенами Сети XYO (XYO), когда их информация используется для ответа на запрос. Чтобы увеличить их шансы быть вознагражденными, они должны создавать бухгалтерские книги, которые согласуются с данными других Стражей, предоставлять Доказательство происхождения идентифицировать себя как источник информации о местоположении.

3.2.2 Мосты

Мосты являются транскрипторами данных местоположения. Они надежно ретранслируют регистры регистров от Стражей Архиваторам до. Самый важный аспект Мостов состоит в том, что Архиватор может быть уверен, что эвристические регистры, полученные от Моста, никоим образом не были изменены. Второй самый важный аспект Моста состоит в том, что они добавляют дополнительное Доказательство происхождения. Учитывая, что сеть XYO является беззащитной системой, мосты должны быть стимулированы для обеспечения честной ретрансляции эвристик. Это делается путем объединения компонента репутации с компонентом оплаты. Мост награжден Токенами Сети XYO (XYO), когда информация, которую они передали, используется для ответа на запрос. Чтобы увеличить их шансы быть вознагражденными, они должны создавать бухгалтерские книги, которые согласуются с данными других Мостов и обеспечивают Доказательство происхождения, идентифицировав себя как передатчик эвристики.

3.2.3 Архиваторы

Архиваторы хранят информацию о местоположении, полученную от Мостов, в децентрализованной форме с целью хранения всех исторических записей. Даже если некоторые данные теряются или становятся временно недоступными, система продолжает функционировать, только с пониженной точностью. Архиватор также индексирует бухгалтерские книги, чтобы они могли легко вернуться в строку данных регистров, если это необходимо. Архиваторы хранят только необработанные данные и получают оплату Токенами Сети XYO исключительно за извлечение данных и их последующего использования. Хранение всегда бесплатное.

Архиваторы подключены к сети, поэтому запрос одного Архиватора приведет к тому, что Архиватор попросит другие Архиваторы предоставить данные, которых он не содержит. Архиватор может также хранить любую информацию в регистре, которая предоставляется в ответ на запрос. Это, скорее всего, приведет к созданию двух типов архиваторов: тех, которые в основном обрабатывают данные «облака» и тех, которые действуют на основе потребления данных из «облака». Архиватор со смешанным типом оперирования будет являться гибридом. Вариант хранения данных не применяется, но может быть легко выполнен через IPFS или другое децентрализованное решение для хранения. Каждый раз, когда данные передаются от одного Архитера к другому, добавляется дополнительное Доказательство происхождения для отслеживания оплаты, поскольку все Платежи получат оплату. Для поиска можно установить минимальный уровень уровня Доказательство, чтобы увеличить срок действия. Интересы Стражей, Мостов и Архиваторов должны быть выровнены, чтобы предотвратить дисбаланс данных.

3.2.4 Дивинеры

Дивинеры - самая сложная часть сети XYO. Общая цель Дивинера - получить наиболее точные данные для запроса из сети XYO и передать эти данные обратно эмитенту этого запроса. Дивинеры собирают данныk со всех применимых платформ блокчеин (Эфириум, Stellar, Cardano, IOTA итд) Для запросов, выпущенных для смарт-контракта XYO. Затем они находят ответ на запрос, напрямую взаимодействуя с Архиваторами, чтобы получить ответ с наивысшей точностью/достоверностью. Они осуществляют это, выбирая Свидетеля с лучшей цепью Доказательства происхождения. Дивинеры, получивший ответ с наилучшим результатом за самый короткий промежуток времени, сможет создать блок на главном XYO блокчеин (XYOMainChain) через Доказательство работы. Запросы имеют приоритет по размеру и сложности вознаграждения, поэтому чем больше XYO предлагается для ответа, тем выше приоритет будет у запроса.

Другие Дивинеры достигают консенсуса относительно действительности блока и подписывают блок в цифровом виде. Дивинер, который был адресом coinbase в этом блоке, затем отправляет транзакцию на

смарт-контракт, содержащий ответ, вместе с его точностью. Он также отправляет список других подписей Дивинеров, чтобы помешать злоумышленнику выдавать фальшивую информацию в блокчеин, выдавая себя за Дивинер. Затем смарт-контракт может подтвердить целостность этой информации, проверив список подписи полезной нагрузки.

3.3 Процесс работы сети от начала до конца

Теперь, когда обязанности каждого компонента ясны в самых мелких деталях, приведем пример работы системы от начала до конца.

1. **Стражи собирают информацию**
    - Стражи собирают эвристику местоположения реального мира и готовят свое собственное Доказательство происхождения, чтобы быть привязанным к узлам над ними.
2. **Мосты собирают информацию от Стражей**
    - Мосты собирают необходимые данные от онлайн-Стражей и присоединяют Доказательство происхождения к своей цепочке. Теперь мосты становятся доступными для Архиваторов в сети.
3. **Архиваторы регистрирует/собирает данные от Мостов**
    - Мосты постоянно отправляют информацию Архиваторам, которые затем хранятся в децентрализованных положениях вместе с эвристическим индексом местоположения.
4. **Дивинер ловит запрос от Пользователя**
    - Дивинеры ищут запросы, отправленные на смарт-контракт в Эфириум, и принимают решение о начале процесса формулировки ответа.
5. **Дивинер собирают данные от Архиваторов**
    - Дивинеры затем принимают решение о приеме запроса, извлекая необходимую информацию из сети Архиватора.
6. **Дивинер формулируют ответ**
    - Дивинер выбирает наилучший ответ на запрос из сети Архиватора, в которой содержится лучший исходный результат.
7. **Дивинеры предлагают блок с ответом**
    - Затем Дивинеры предлагают блоки на XYOMainChain, содержащие ответы на вопросы, запрос и Токен сети XYO (XYO), оплаченные через Доказательство работы. Другие Дивинеры в сети подписывают в цифровом виде содержимое блока, затем обновляется учетная запись коинбазы Дивинера, чтобы продемонстрировать Доказательство работы в системе после достижения консенсуса по действительному блоку.
8. **Дивинер отправляет результаты Автору запроса**
    - Дивинеры собирают ответ, Оценку происхождения цепи и набор цифровых сигналов и отправляют их на компонент адаптера, который надежно подключается к смарт-контракту XYO. Адаптер отвечает за то, чтобы целостность Дивинера не была скомпрометирована и отправляет набор ответов с цифровой подписью на смарт-контракт. Это происходит сразу после процесса создания блока. Затем на коинбазу Дивинера поступает оплата за выполненную работу.
9. **Компоненты сети XYO вознаграждаются за проведенную работу**
    - Компоненты, работавшие над созданием цепи «Доказательство происхождения» получают оплату за участие в получении ответа на запрос. Стражи, Мосты, Архиваторы и Дивинеры все награждаются за работу.

В случае, когда один и тот же запрос задается более одного раза, может быть получено более одного ответа, поскольку ответ, который создается в данный момент, основан на доступной эвристике, которую система может предложить в это время. Отправка ответа на блокчеин занимает два шага. Во-первых, необходимо провести анализ для определения наилучшего ответа на запрос. Если в системе генерируется несколько ответов, то узлы будут сравнивать ответы и всегда выбирать лучший ответ. Примером простого запроса может быть: «Где был узел в сети в определенное время в прошлом?»

3.4 Блокчеин как единственный источник правды

По своей сути Дивинеры просто преобразуют относительные данные в абсолютные данные. Они могут исследовать всю сеть Архиваторов, чтобы конкретизировать абсолютный ответ на запрос в сети XYO. Дивинеры также являются узлами, которые предлагают и добавляют блоки к XYOMainChain, и получают вознаграждение за их Доказательство работы. Поскольку сеть Архиваторов представляет собой хранилище необработанных данных, а блокчеин является хранилищем абсолютных обработанных данных, сеть может в конечном итоге использовать самую последнюю информацию о XYOMainChain для ответа на будущие запросы, а не полагаться на дорогостоящие вычисления через сеть Архиваторов.

Поскольку блоки на XYOMainChain хранят цепочку Доказательства происхождения и график компонентов, которые использовались для ответа на запросы, будущие Дивинеры могут исследовать эти абсолютные данные для достижения точных результатов при более низком использовании полосы пропускания. Таким образом, XYOMainChain постепенно станет самым важным источником правды системы. Тем не менее, сеть Архиватор по-прежнему будет необходима для поддержания самой свежей информации о эвристике местоположения, собранной Стражами.

3.5 Работа сети XYO для определения кандидатов с лучшим ответом

Мы определяем лучший ответ как единый ответ среди списка кандидатов, который получает наивысший балл оценки и имеет более высокий балл точности, чем минимальная требуемая точность. Оценка действительности основана на исходной оценке. Система знает, что такое самая высокая запись Оценка происхождения, которая будет составлять 100 процентов, пока не будет достигнут более высокий балл, который затем станет новым 100 процентов. Сеть XYO позволяет выбирать алгоритм наилучшего ответа для определения наилучшего ответа. Это создает расширение для будущих исследований альтернативных алгоритмов.

Когда данные исключаются из ответа из-за того, что он считается плохим или неправильным, эта информация будет распространена среди Архиваторов, чтобы они могли очистить эти данные от своих децентрализованных магазинов.

3.6 Начальная интеграция с общественными блокчейнами

Сеть XYO спроектирована как абстракция, которая может взаимодействовать с любым смарт-контрактом, способным, публичным блокчеин, таким как Эфириум, Bitcoin + RSK, EOS, NEO, Stellar, Cardano и другие. Чтобы взаимодействовать с сетью XYO, пользователи на Эфириум, например, могут выдать запросы нашему смарт-контракту XYO и заплатить в XYO Токен (ERC20). Узлы в нашем собственном XYO Блокчеин, называемые Дивинеры, постоянно будут опрашивать Эфириум и получать вознаграждение в собственной валюте XYO Блокчеин (также называемого XYO Tokens). В будущем мы сделаем индивидуальное преобразование от держателей нашего ERC20 токена в нашу собственную собственную валюту, чтобы предоставить нашим платформам комиссионные за транзакции, которые поддерживают требования к микроплатежам, необходимые для масштабируемых вариантов использования IoT. В этих случаях мы разрешаем пользователям отправлять запросы непосредственно на наш блокчеин, а не взаимодействовать через общедоступный смарт-контракт.

4 Доказательство происхождения

С физической сетью, состоящей из ненадежных узлов, можно определить определенность данных, которые были предоставлены краевыми узлами на основе доказательства нулевого знания, что две или более части данных были получены из того же источника. Используя эти наборы данных, в сочетании с рядом аналогичных наборов данных и знаниями по абсолютной позиции хотя бы одного узла, можно установить абсолютное местоположение другого узла.

4.1 Доказательство происхождения. Введение

Традиционные системы без верификации полагаются на закрытый ключ для подписания транзакций или контрактов в системе. Это очень хорошо работает с предположением, что узел в сети, который подписывает данные, физически и практически безопасен. Однако, если секретный ключ скомпрометирован, тогда способность доказать происхождение замирает.

При применении доверенных концепций к Интернету Вещей необходимо предположить, что краевые узлы в сети физически или практически не защищены. Это обуславливает необходимость идентифицировать граничные узлы без использования уникальных идентификаторов и вместо этого судить данные, созданные ими, как честные и достоверные без каких-либо знаний извне сети.

4.2 Суть Доказательство происхождения: Связной Страж

Доказательствоэк опирается на концепцию Связанного Стража. Учитывая, что ненадежный источник данных, используемых для разрешения цифрового контракта (оракула), не пригоден, мы можем существенно увеличить достоверность данных, предоставленных путем первого установления существования двунаправленного доказательства местоположения. Первичная двунаправленная эвристика местоположения – это приближенное понятие, поскольку обе стороны могут проверить наличие и диапазон взаимодействия путем координирования взаимодействия. Это позволяет доказать доказательство нулевого знания, что эти два узла находятся в непосредственной близости друг от друга.

Затем нам нужно определить уверенность в том, что узел свидетельства оракула в бездонной системе собрал данные, которыми он делится. В бездонной системе узел-свидетель может либо путем дефекта, либо повреждения создавать ложные данные. Неверные данные могут быть обнаружены и удалены просто, если они попадают за пределы допустимого диапазона для этой эвристики. Действительные, но неверные данные (т.е. Ложные данные) гораздо труднее обнаружить.

4.3 Однонаправленная и двунаправленная эвристика местоположения

Большинство данных, связанных с физическим миром (эвристический), являются однонаправленными. Это означает, что измеряемый элемент не может измеряться назад, что делает невозможным подтверждение достоверности данных однонаправленных эвристических данных. Двунаправленная эвристика - это та, где измеренный элемент может сообщать о своем собственном измерении обратно другой стороне, что делает возможной проверку. **Местоположение - редкая эвристика, поскольку она может быть двунаправленной, причем два пограничных узла сообщают друг о друге. Реальным примером этого могли бы быть два человека, которые находятся рядом друг с другом, занимаясь самоубийством, печатая копию для каждой стороны, а затем и подписывая автогонки. Этот процесс даст обеим сторонам доказательства**

близости. Единственный способ для этих двух людей получить эти «данные» будет от них вместе в одном месте.

Затем обсудим сетевые эффекты. Представьте себе систему, в которой каждый краевой узел должен постоянно производить эти «эгоисты», когда они путешествуют, и хранить их в связующем. Ожидается, что они также сохранят это связующее в последовательном порядке и никогда не смогут его удалить. Это устанавливает регистратор близости для каждого краевого узла, который может быть перекрестно привязан к рекордерам других граничных узлов.

4.4 Неограниченные узлы

Все узлы считаются Свидетелями, включая Мосты, Стражи, Архиваторы и узлы анализа. Это позволяет передавать любые данные от одного узла к другому. Эта концепция имеет название Связной свидетель.

4.5 Перекрестная ссылка

Анализ каждого набора селфи, создаваемых и связанных вместе каждым неограниченным узлом, позволяет системе получать лучший ответ на вопрос об относительной близости всех узлов, находящихся в сети. Если каждый узел сообщается открыто и точно, отображение всех относительных положений реберных узлов позволит достичь максимальной достоверности и точности: 100 процентов. И наоборот, если каждый узел является либо неверным, либо ошибочным, то определенность и точность могут приблизиться к минимуму 0 процентов.

Учитывая набор сообщенных данных и запрос относительно относительного положения одного из реберных узлов, может быть сгенерировано приближение позиции вместе с коэффициентами для уверенности и точности.

Учитывая тот же набор данных и тот же алгоритм анализа, каждый расчет должен приходиться на приближение одной и той же позиции и те же коэффициенты для уверенности и точности.

4.6 Диаграмма

S 'и S "(Рисунок 1) представляют собой Стража (краевой узел), которые собирают эвристику. При контакте друг с другом они обмениваются эвристическими данными и открытыми ключами. Оба строят полную запись взаимодействия и подписывают полученное взаимодействие. Затем подписанная запись становится следующей записью в обоих своих локальных регистрах (16 для S 'и 3 для S "). Это действие связывает двух свидетелей, находящихся в непосредственной близости друг от друга.

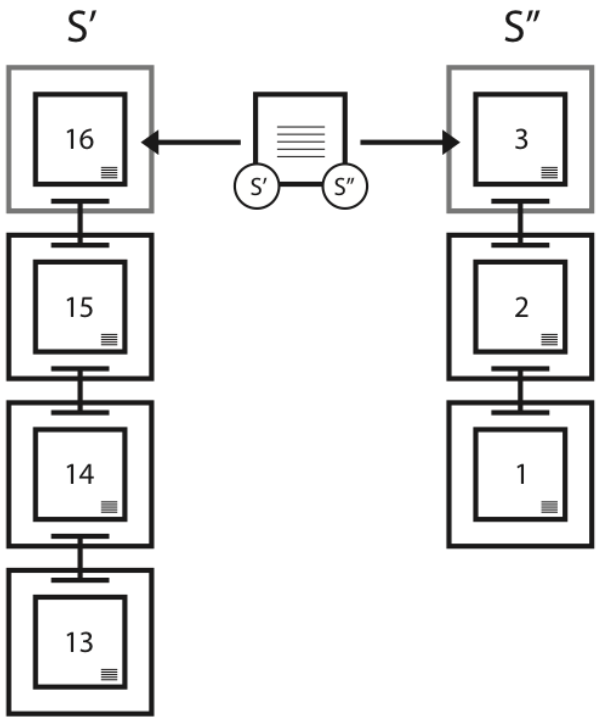

Рисунок 1. Пример привязки Свидетеля между двумя Стражами

4.7 Цепочки происхождения

Каждое происхождение ведет свою собственную книгу и подписывает ее, чтобы создать цепочку Доказательство происхождения. После того, как информация о цепочке происхождения Доказательство была разделена, она фактически является постоянной. Это происходит из-за того, что вилка, которая происходит после того, как доля заканчивается цепочкой, заставляет все будущие данные от свидетеля рассматриваться так, как если бы это было от нового свидетеля. Чтобы создать ссылку в цепочке происхождения Доказательство происхождения, источник генерирует пару открытых / закрытых ключей. Затем он подписывает как предыдущий, так и следующий блоки с одной и той же парой после включения открытого ключа в оба блока. Сразу после создания подписи секретный ключ удаляется. При немедленном удалении закрытого ключа риск кражи или повторного использования ключа сильно минимизируется.

Доказательство происхождения Цепи является ключом к проверке правильности ввода бухгалтерских записей в сеть XYO. Уникальный идентификатор источника данных не является практическим, так как он может быть подделан. Подписание частного ключа нецелесообразно, так как большинство частей сети XYO трудны или невозможны для физической защиты, поэтому способность плохого актера украсть закрытый ключ слишком осуществима. Чтобы решить эту проблему, сеть XYO использует переходные брелки. Преимущество их использования в том, что невозможно фальсифицировать цепочку происхождения данных. Однако, как только цепь сломана, она сломана навсегда и не может быть продолжена, превращаясь в остров.

Каждый раз, когда эвристический регистр передается в сети XYO, получатель присоединяется к своему собственному Доказательство происхождения, что делает цепочку Доказательство происхождения более длинной и генерирует проверку Доказательство происхождения. Доказательство происхождения Цепи и Доказательство происхождения Пересечения являются основными индикаторами, используемыми Дивинерами для проверки действительности бухгалтерских записей. Уравнение для репутации Ledger является фактически вычислением процента сети XYO, которое участвовало в создании ассоциированного с ним Доказательства происхождения. Теоретически, если 100% записей сети XYO связаны с Доказательство происхождения и затем полностью анализируются, вероятность того, что он действителен, составляет 100%. Если для анализа доступно 0 процентов записей сети XYO, то срок действия снижается до 0 процентов.

Для дополнительной безопасности открытый ключ для Chain Link не предоставляется до тех пор, пока вторая запись для него не станет доступной. Это также позволяет сохранить временный интервал между записями или другими данными в предыдущей или следующей ссылке.

4.8 Оценка происхождения цепи

Происхождение цепочки рассчитывается следующим образом (алгоритм по умолчанию):

- PcL = Доказательство происхождения Длина цепи
- PcD = Доказательство происхождения Цепная сложность
- Pc 'Pc "O = Доказательство происхождения Перекрытие цепей для ПК и ПК”

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O}$$

4.9 Дерево происхождения

Дерево происхождения используется для вычисления приблизительной действительности ответа. Он использует собранные данные для генерации идеального дерева, которое является деревом, которое наилучшим образом соответствует данным для данного утверждённого ответа. Если узел N находится в местоположении X, Y, Z, T, ошибка во всех данных в наборе должна содержать определенное значение. Чтобы вычислить эту ошибку, мы вычисляем: MIN, MAX, MEAN, МЕДИАНУ и СРЕДНЕЕ РАССТОЯНИЕ ОТ МЕДИАНЫ.

Учитывая набор S всех оценок s, Доказательство происхождения Chains Difficulty PcD и ошибку коэффициента ошибки, лучший ответ определяется следующим образом:

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

Другими словами, утверждённый ответ, который имеет самый высокий рейтинг наилучшего ответа, - лучший ответ. Используя дерево Доказательство, мы можем идентифицировать и обрезать невозможные ветви (выбросы).

4.10 Цепь переходных ключей

Использование временных закрытых ключей для подписи двух последовательных пакетов может объединить ряд пакетов данных вместе. Когда открытый ключ в паре с закрытым ключом включен в пакеты данных, получатель может проверить, что оба пакета были подписаны одним и тем же закрытым ключом. Данные в пакете не могут быть изменены без нарушения сигнатуры, гарантируя, что подписанные пакеты не были изменены третьей стороной, например мостом или узлом хранения.

4.11 Глубина ссылки

Как минимум, узел генерирует новую пару открытого/закрытого ключа для каждой ссылки в доказательстве цепи происхождения, которая имеет глубину связи 1. В таблице ссылок для данной записи могут быть N записей с каждой записью указав расстояние в будущем, когда будет добавлена вторая часть ссылки. Никакие две ссылки не могут иметь тот же порядок величины по шкале базового 2. Например, запись [1,3,7,12,39] будет разрешена, но [1,3,7,12,15] не будет.

Ссылка на канал глубины 1 создается, используется и удаляется при публикации предыдущего блока. Однако ссылки глубины больше 1 имеют свою пару, сгенерированную при подписании предыдущего блока, а вторая подпись не выполняется до тех пор, пока N блоков не будет позже, после чего будет удален частный ключ. По этой причине ссылки глубины более 1 всегда считаются менее безопасными, чем звенья глубины 1, но их можно использовать для повышения производительности и уменьшения потери данных за счет этой безопасности.

4.12 Фиксированный заказ

Ключевым элементом в определении последовательности регистров является порядок, в котором они были представлены. Учитывая, что устройство не может изменить порядок любого подписанного регистрационного документа Доказательство происхождения, абсолютный порядок может быть установлен путем совместного просмотра всех бухгалтерских регистров.

4.13 Предпоследнее издание

Первичный метод установления Доказательства происхождения основан на том факте, что Страж всегда сообщает свой второй к последнему блоку, не сообщая о последнем блоке. Это позволяет последнему блоку иметь подписанную ссылку на своего предшественника в качестве доказательства ссылки.

4.14 Пустые ссылки

Чтобы сделать цепочку Доказательство происхождения более безопасной, требуется, чтобы цепочка обновлялась не чаще одного раза в десять секунд и не реже одного раза каждые шестьдесят минут. В случае отсутствия новых данных, в цепочку будет добавлен пустой блок.

4.15 Диаграмма

По ходу течения времени слева направо (Рисунок 2), важность цепи Доказательства происхождения увеличивается. В любой момент времени производитель цепи будет предоставлять абоненту записи с затемненными границами, ожидая второго подписания записи, прежде чем сделать ее доступной. Например, в третьем столбце будут возвращаться только записи 2 и 1 как часть цепочки.

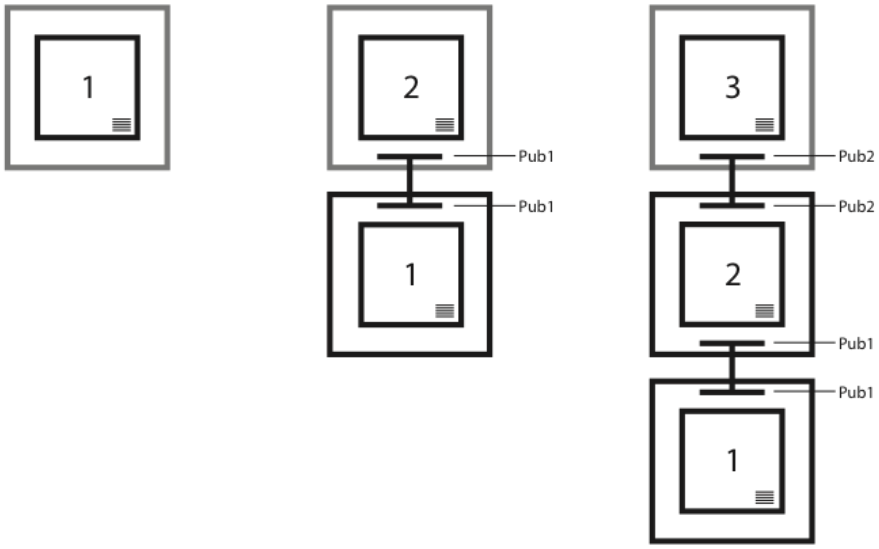

Рисунок 3. Пример включения ссылки в цепочке Доказательство происхождения.

4.16 Заключение

Учитывая серию пакетов данных, которые подписываются в последовательных парах с временными закрытыми ключами и включают парные открытые ключи, можно с абсолютной уверенностью определить, что пакеты поступают из одного и того же источника.

---

5 Меры предосторожности

5.1 Атака подставным Дивинером

Набор цифровых подписей отправляется на смарт-контракт XYO, потому что контракт должен проверить целостность Дивинера, который отправил ответ. Контракт может затем проверить другие Дивинеры, которые подписали этот список в пределах высокого доверительного интервала. Без этого ретрансляционный оракул будет единственным источником отказа и риска внутри системы

5.2 Атаки Стражей DDoS

Другой атакой, которую следует рассмотреть, является распределенный отказ в обслуживании (DDoS) среди узлов Стражей в определенном регионе. Злоумышленник может попытаться установить большое количество соединений с Стражами, чтобы предотвратить их передачу правильной информации или передачу какой-либо информации вообще на Мосты. Мы можем обойти эту проблему, требуя, чтобы маленькая криптографическая головоломка была решена любым, кто пытался подключиться к Стражу. Поскольку запрос не будет включать в себя очень большое количество подключений к Стражам, это не будет сильно влиять на ретрансляционную систему XYO и потребует от злоумышленника потратить большой объем ресурсов для успешной работы DDoS в нашей сети. В любой момент времени цепочка Доказательство происхождения может быть проверена кем угодно, поскольку она хранится на XYOMainChain. Это гарантирует, что если один объект по цепочке был скомпрометирован, точность ответа на запрос (исходный показатель цепочки) упадет до 0.0.

---

6 Экономика токенов XYO

Оракулы обладают значительным влиянием в сети и инфраструктуре для децентрализованных приложений, причем большая часть внимания сосредоточена на связности и агрегации авторитетных оракулов. Мы считаем, что для децентрализованных приложений необходимо обеспечить полностью децентрализованную и беспристрастную систему оракулов для достижения максимального потенциала.

6.1 Криптоэкономика сети XYO

Сеть XYO будет полагаться на маркер ERC20, называемый токеном XYO, который используется для стимулирования желаемого поведения обеспечения точного и надежного местоположения. Токены XYO можно рассматривать как «газ», необходимый для взаимодействия с реальным миром, чтобы проверить XY-координату заданного объекта.

Процесс работает следующим образом: держатель токена сначала обращается в сеть XYO с запросом (например, «Где моя посылка eCommerce с адресом XYO 0x123456789 ...?»). Затем запрос отправляется в очередь, где он ожидает обработки и ответа. Пользователь может установить желаемый уровень доверия и цену на газ XYO при создании запроса. Стоимость запроса (в токенах XYO) определяется объемом данных, необходимых для предоставления ответа на запрос, а также динамики рынка. Чем больше данных необходимо, тем дороже запрос и выше цена на газ XYO. Запросы к сети XYO могут быть очень большими и дорогими. Например, грузовая и логистическая компания может запросить сеть XYO, чтобы спросить: «Каково расположение каждого отдельного автомобиля в нашем парке? »

После того, как держатель токена XYO запрашивает сеть XYO и оплачивает стоимость необходимого газа, все участники Дивинеры, работающие над задачей, обращаются к соответствующим Архиваторам, чтобы получить соответствующие данные, необходимые для ответа на запрос. Данные получают от Мостов, которые первоначально собрали данные у Стражей. Стражи по существу являются устройствами или сигналами, которые проверяют местоположение объектов. Сюда входят такие устройства, как Bluetooth-трекеры, GPS-трекеры, отслеживание геолокации, встроенные в устройства IoT, технология спутникового слежения, сканеры QR-кода, сканирование RFID и многие другие. XY Findables впервые разработала и выпустила свой бизнес для Bluetooth и GPS, который позволил ему протестировать и обработать эвристику местоположения в реальном времени. Все усилия по развитию потребительского бизнеса XY Findables значительно помогли в разработке протокола блокчейнов сети XYO.

6.2 Вознаграждение независимости

Устройства сбора информации о местоположении представляют собой атомные блоки сети, и одно устройство может действовать как один или несколько из четырех компонентов системы. Однако было бы редкостью, особенно в большой сети XYO, если устройства брали на себя роль более двух из этих компонентов. Более того, регистр блокчеин, который имеет более независимое доказательство происхождения, будет автоматически вызывать больше доверия, поэтому существует криптоэкономическое наказание за устройство, действующее как несколько компонентов.

6.3 Вознаграждение постоянства

Стражам в сети XYO присваивается коэффициент стационарности для мониторинга движения на протяжении всего их жизненного цикла. Чем меньше Страж движется за определенный промежуток времени, тем большему количеству его данных можно доверять. Архиваторы отслеживают и анализируют эти коэффициенты стационарности при рассмотрении вопроса о том, какие Стражи направлять запросы.

6.4 Стимулирование использования Токенов

Система, в которой владельцам токенов рекомендуется не использовать свои жетоны, создает долгосрочную проблему для базовой экономики. Это создает экосистему с очень скудными запасами стоимости и вызывает естественный импульс, чтобы изобретать причины не использовать токен, а не повышать полезность и ликвидность. Недостаток ликвидности маркера часто игнорируется держателями токенов, потому что искусственный дефицит, созданный сдержанными токенами, создает кратковременные всплески, но вопрос в том, какова стоимость?

Проблема большинства криптоэкономических стимулов заключается в том, что основное внимание уделяется маркетологам, а вовсе не к пользователям токенов. Идентификатор XYO учитывает оба фактора, определяя идеальных и полезных участников рынка, которые хранят в памяти счета идеального состояния и действуют на него.

Модель маркера XYO стимулирует майнеров не просто предоставлять точные данные, но также знать, когда вообще не предоставлять данные. Конечный пользователь получает вознаграждение за транзакцию, когда низкая ликвидность сети по сравнению с высокой ликвидностью сети. Таким образом, экосистема XYO Токен обладает способностью оставаться сбалансированной, жидкой и надежной.

6.5 Характеристики XYO Токен

Открытая продажа токенов имеет многоуровневую структуру ценообразования, которая начинается с 1 ETH: 100 000 XYO и максимальная стоимость достигает 1 ETH: 33,333 XYO. Скоро будет опубликована подробная информация относительно нашей структуры ценообразования на основе объема и времени

- Платформа смарт-контрактов: Эфириум
- Тип контракта: ERC20
- Токен: XYO
- Название токена: Utility Токен сети XYO
- Адрес Токен: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Общая эмиссия: Конечная и ограниченная сумма, достигнутая после основной продажи Токенов
- Прогнозируемая капитализация токенов XYO: 48 млн. долларов США.
- Непроданные и нереализованные Токены: будут утилизированны после продажи маркеров. После окончания основной продажи никаких дополнительных Токенов XYO выпускаться не будет.

7 Случаи применения сети XYO

От простого до сложного, использование сети XYO имеет обширные приложения, охватывающие множество отраслей. Например, возьмите компанию eCommerce, которая могла бы предложить своим клиентам услуги по оплате по доставке премиум-класса. Чтобы иметь возможность предлагать эту услугу, компания eCommerce будет использовать сеть XYO Network и платформу XY (которая использует токены XYO) для написания смарт-контракта (т.е. на платформе Эфириума). Затем сеть XYO могла отслеживать местоположение пакета, отправляемого потребителю, на каждом этапе выполнения; от склада до курьера, вплоть до дома потребителя и каждого места между ними. Это может позволить розничным сетям и веб-сайтам электронной коммерции уверенным образом проверять, что пакет не только появился на пороге клиента, но и безопасно в их доме. Как только пакет будет подтвержден в доме клиента (определенный и подтвержденный определенной XY-координатой), отправка считается завершенной, и платеж поставщику будет выпущен. Таким образом, интеграция сети XYO в eCommerce позволяет защитить торговца от мошенничества, а также обеспечить, чтобы потребители платили только за товары, которые поступают в их дом.

Рассмотрим совершенно другую интеграцию сети XYO с сайтом обзора отеля, чья текущая проблема заключается в том, что их обзоры часто не доверяют. Владельцы гостиниц по-настоящему стимулируются для улучшения своих отзывов любой ценой. Что, если можно с большой долей уверенности сказать, что кто-то был в Сан-Диего, вылетел в отель на Бали и пробыл там в течение двух недель, вернулся в Сан-Диего, а затем написал обзор об их пребывании в отеле на Бали? Обзор будет иметь очень высокую репутацию, особенно если он был написан серийным рецензентом, который написал много обзоров с проверенными данными о местоположении.

---

8 Расширение сети XYO

Нам повезло, что у нас есть потребительский рынок, который успешно построил сеть в реальном мире с более чем одним миллионом (1.000.000) устройств Bluetooth и GPS. Большинство сетей определения местоположения не могут достичь этой фазы и достичь критической массы, необходимой для создания обширной сети. Сеть Стражей, которую мы создали, является только отправной точкой. Сеть XYO - это открытая система, в которой любой оператор устройств определения местоположения может подключаться и начинать зарабатывать XYO Токены.

Как правило, чем увереннее функционал Стражей в сети XYO, тем надежнее сеть. Чтобы далее развивать свою сеть, XYO взаимодействует с другими компаниями, чтобы усилить возможности Стражей за пределами своей собственной сети маяков XY Findables.

---

9 Выражение благодарности

Этот неофициальный отчет является результатом нашего решения сделать техническую документацию более краткой. Мы сделали это, опираясь на техническую документацию, содержащий только технические детали сети XYO. Мы создали эту зеленую бумагу, чтобы описать детали бизнеса, нашу стратегию и фон протоколов и протоколов местоположения. Мы благодарим Рауля Джордана (Гарвардский колледж, сотрудник Thie и советник сети XYO) за его предложение составить отдельную зеленую бумагу в первую очередь. Мы благодарим Кристин Сако за ее исключительную трудовую этику и внимание к деталям в ее обзоре. Проведя много времени и усилий, структурируя нашу техническую документацию, Кристин продолжала свою работу еще дальше, применяя те же самые лучшие практики к нашей зеленой бумаге. Мы благодарим Джонни Колашинского за компиляцию приложений для использования. Наконец, мы благодарим Джона Арану за его тщательный обзор и творческий вклад в наши усилия.

Литература (в оригинале)

[1] Blanchard, Walter. Hyperbolic Airborne Radio Navigation Aids. Journal of Navigation, 44(3), September 1991.

[2] Karapetsas, Lefteris. Sikorka.io.
http://sikorka.io/files/devcon2.pdf. Shanghai, September 29, 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof of location/. September 17, 2016.

[4] Goward, Dana. RNT Foundation Testifies Before Congress. US House of Representatives Hearing: “Finding Your Way: The Future of Federal Aids to Navigation,” Washington, DC, February 4, 2014.

Словарь понятий

точность
Мера уверенности в том, что точка данных или эвристика находится в пределах определенной погрешности.

Архиватор
Архиватор хранит эвристику как часть децентрализованного набора данных с целью хранения всех исторических регистров, но без этого требования. Даже если некоторые данные теряются или становятся временно недоступными, система продолжает функционировать, как раз с пониженной точностью. Архиваторы также индексируют регистры, чтобы при необходимости они могли возвращать строку данных регистра. Архиваторы хранят только сырые данные и получают оплату исключительно за извлечение данных. Хранение всегда бесплатно.

Лучший ответ
Мы определяем лучший ответ как единый ответ среди списка кандидатов-кандидатов, который возвращает наивысший балл оценки и имеет более высокий балл точности, чем минимальная требуемая точность.

Алгоритм наилучшего ответа
Алгоритм, используемый для генерации наилучших ответов, при выборе ответа Дивинером. Сеть XYO позволяет добавлять специализированные алгоритмы и позволяет клиенту указать, какой алгоритм использовать. Требуется, чтобы этот алгоритм привел к такому же результату при запуске на любом Дивинере с тем же набором данных.

Связной Свидетель
Связной Свидетель - это концепция, достигнутая благодаря существованию двунаправленной эвристики. Учитывая, что ненадежный источник данных для использования цифрового соглашения о контрактах (оракула) не является полезным, существенное увеличение достоверности данных, предоставляемых в результате создания такой эвристики. Первичная двунаправленная эвристика - это приближенное значение, поскольку обе стороны могут проверить наличие и диапазон взаимодействия путем координирования взаимодействия. Это позволяет доказать доказательство нулевого знания, что эти два узла находились в непосредственной близости друг от друга.

Мост
Мост - эвристический транскрипт. Он надежно передает эвристические регистры от Стражей до Дивинеров. Самый важный аспект Моста состоит в том, что Дивинер может быть уверен, что эвристические книги, полученные от Моста, никоим образом не были изменены. Второй самый важный аспект Моста состоит в том, что они добавляют дополнительные метаданные Доказательства происхождения.

уверенность
Мера вероятности того, что точка данных или эвристика свободна от коррупции или фальсификации.

крипто-местоположение
Область технологии криптографического местоположения.

криптоэкономика
Формальная дисциплина, которая изучает протоколы, регулирующие производство, распределение и потребление товаров и услуг в децентрализованной цифровой экономике. Криптоэкономика - это практическая наука, которая фокусируется на разработке и характеристике этих протоколов.

Дивинер
Дивинер отвечает на заданный запрос, анализируя исторические данные, которые были сохранены сетью XYO. Эвристика, хранящаяся в сети XYO, должна иметь высокий уровень доказательства происхождения, чтобы определить правильность и точность эвристики. Боевик получает и дает ответ, судя свидетеля на основании его Доказательства происхождения. Учитывая, что сеть XYO - это беззащитная система, Дивинеры должны быть стимулированы для обеспечения честного анализа эвристики. В отличие от Стражей и Мостов, Дивинеры используют Доказательство работы для добавления ответов на блокчеин.

эвристика
Точка данных о реальном мире относительно положения Стража (близость, температура, свет, движение итд).

оракул
Часть системы DApp (децентрализованное приложение), которая отвечает за разрешение цифрового контракта, обеспечивая ответ с точностью и уверенностью. Термин «оракул» происходит от криптографии, где он обозначает действительно случайный источник (например, случайного числа). Это обеспечивает необходимые ворота из уравнения криптографии в мир за пределами. Оракулы кормят смарт информацией о транзакциях из-за цепи (в реальном мире или вне сети). Оракулы - это интерфейсы от цифрового мира до реального мира. В качестве болезненного примера рассмотрим контракт на Завещание и погребение. Условия Уилла выполняются после подтверждения того, что наследодатель умер. Служба оракула может быть построена для начала выполнения завещания путем компиляции и агрегирования соответствующих данных из официальных источников. Оракул может затем использоваться в качестве фида или конечной точки для вызова смарт-контракта, чтобы проверить, умер ли человек.

Оценка происхождения цепи
Оценка, присвоенная цепочке происхождения, чтобы определить ее авторитет. Эта оценка учитывает длину, путаницу, перекрытие и избыточность.

Дерево происхождения
Набор данных записей регистров, взятых из различных цепочек происхождения, чтобы установить источник записи эвристической книги с определенным уровнем достоверности.

Доказательство происхождения
Доказательство происхождения - это ключ к проверке правильности ввода бухгалтерских книг в сеть XYO. Уникальный идентификатор источника данных не является практическим, так как он может быть подделан. Закрытие частного ключа нецелесообразно, так как большинство частей сети XYO трудны или невозможны для физической защиты, поэтому потенциал для плохого актера, чтобы украсть закрытый ключ, является слишком выполнимым. Чтобы решить эту проблему, XYO Network использует цепочку переходных ключей. Преимущество этого в том, что невозможно фальсифицировать цепочку происхождения для данных. Однако, как только цепь сломана, она сломана навсегда и не может быть продолжена, превратив ее в остров.

Доказательство происхождения цепи
Переходная цепочка ключей, которая объединяет ряд эвристических записей Связного свидетеля.

Доказательство работы
Доказательство работы - это часть данных, которая удовлетворяет определенным требованиям, трудно производить (а именно: дорогостоящая, трудоемкая итд), но легко для других проверить. Получение доказательства работы может быть случайным процессом с низкой вероятностью генерации, так что в среднем требуется тщательная пробная версия и ошибка, прежде чем будет создано действительное доказательство работы.

Страж
Страж (Сентинел) - эвристический страж. Он соблюдает эвристику и поручительства за достоверность и точность их создания временными книгами. Самый важный аспект Стража заключается в том, что он создает книги, в которых могут быть уверены, что Дивинеры можно найти из одного источника, добавив к ним Доказательство происхождения.

Смарт-контракт
Протокол, разработанный Ником Сабо до Биткойна, предположительно в 1994 году (именно поэтому некоторые считают его Сатоши Накамото, мистическим и неизвестным изобретателем Биткойна). Идея умных контрактов заключается в том, чтобы кодифицировать юридическое соглашение в программе и децентрализованные компьютеры выполнять свои условия, а не люди, которые должны толковать и действовать по контрактам. Смарт-контракты сворачивают деньги (например, эфир) и заключают контракты в одну и ту же концепцию. Будучи такими умными контрактами детерминистскими (например, компьютерными программами) и полностью прозрачными и читаемыми, они служат отличным способом замены посредников и брокеров.

Переходная цепочка ключей
Переходная цепочка ключей связывает ряд пакетов данных с использованием криптографии с временным ключом.

Не нуждающийся в доверии (trustless)
Характерная особенность, когда все стороны в системе могут достичь консенсуса в отношении канонической истины. Власть и доверие распределяются (или разделяются) между заинтересованными сторонами сети (например, разработчиками, майнерами и потребителями), а не сосредоточены в одном отдельном физическом или юридическом лице (например, в банках, правительствах и финансовых учреждениях). Это общий термин, который можно легко понять неправильно. Блокчеин фактически не ликвидируют доверие. Они сводят к минимуму количество доверия, требуемого от любого отдельного участника в системе. Они делают это, распределяя доверие между различными участниками системы посредством экономической игры, которая стимулирует участников к сотрудничеству с правилами, определенными протоколом.

Сеть XY Оракул
Сеть XYO Network.

Сеть XYO
Сеть XYO означает «XY Oracle Network». Она состоит из всей системы компонентов/узлов, включенных в XYO, которые включают в себя Стражей, Мостов, Архиваторов и Дивинеров. Основная функция сети XYO - действовать как портал, посредством которого цифровые смарт-контракты могут выполняться посредством подтверждений геолокации в реальном мире.

XYO MainChain
Неизменяемый блокчеин в сети XYO, в котором хранятся транзакции запросов вместе с данными, собранными от Дивинеров, и их ассоциированной оценкой происхождения.