Гидро Рэйндроп

Открытая Аутентификация На Блокчейне

Январь 2018

Содержание

Введение

Блокчейн и Эфириум

- Разработка на основе Эфириума
- Деревья Меркла
- Смарт контракты
- Виртуальная Машина Эфириума

Открытый журнал

- Открытый журнал для частных систем
- Архитектура для принятия

Рэйндроп

- Состояние финансовой безопасности
- Взлом компании Equifax
- Добавление блокчейн слоя
- Гидро Рэйндроп
- Детальное рассмотрение
- Открытие Рэйндропа обществу
- Пример использования – Рэйндроп с OAuth 2.0

Риски

Заключение

Введение

HYDRO (далее, ГИДРО): Этимология – от др.-греч. ὕδωρ – (hudro-) – вода.

Гидро позволяет новым и существующим частным системам (private systems) беспрепятственно интегрировать и еще лучше использовать неизменяемую и прозрачную динамику открытого блокчейна (public blockchain) для повышения безопасности приложений и документов, управления идентификационной информацией, а также для работы с транзакциями и искусственным интеллектом.

В этом документе, будет показано, как частные системы, такие как API, могут использовать открытый блокчейн Гидро для повышения безопасности через открытую аутентификацию (public authentication).

Предлагаемая технология называется “Рэйндроп” – транзакция выполняемая через смарт контракт, который публично проверяет доступ к частной системе, и может дополнить существующие приватные методы аутентификации. Данная технология призвана обеспечить дополнительную безопасность для важных финансовых данных, которые все чаще подвергаются риску от взлома и нарушений.

Первоначальная реализация Рэйндропа осуществлена на платформе Hydrogen API. Этот модульный набор API команд доступен предприятиям и разработчикам по всему миру для создания прототипов, сборки, тестирования и развертывания сложных финансовых технологических платформ и продуктов.

Рэйндроп будет доступен мировому сообществу разработчиков в качестве программного обеспечения с открытым исходным кодом, который позволит разработчикам интегрировать Рэйндроп с любым REST API.

Блокчейн и Эфириум

Гидро реализуется на сети Эфириума. Но прежде, чем представить больше деталей о проекте, важно объяснить некоторые фундаментальные идеи о блокчейне и Эфириуме.

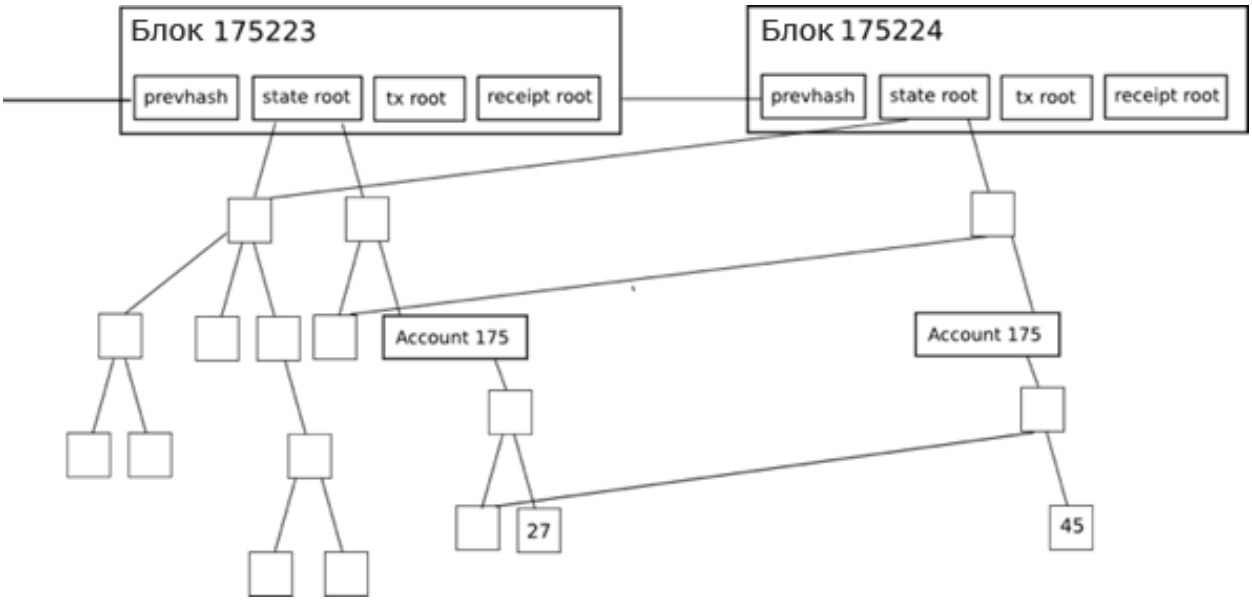
Разработка на основе Эфириума

Подобному тому, как и многие приложения, например Snapchat, были построены с помощью Swift и других инструментов предлагаемых поверх платформы Apple iOS, так и блокчейн приложения могут быть реализованы на основе Эфириума. Корпорации Snap не надо было создавать iOS, вместо этого, она использовала ее в качестве инфраструктуры для запуска социального медиа приложения, меняющую правила игры.

Проект Гидро обладает сходными свойствами. Он опирается на тысячи разработчиков по всему миру, которые работают над тем, чтобы сделать базовую технологию блокчейн быстрее, сильнее и эффективнее. Гидро поддерживает эту постоянно улучшающуюся инфраструктуру, разрабатывая ориентированные на конечный продукт средства взаимодействия, использующие технологию блокчейн, которые могут предложить ощутимые преимущества для приложений финансовых услуг.

Деревья Меркла

Деревья Меркла используются в распределенных системах для эффективной проверки данных. Они эффективны, потому что используют хэши файлов вместо самих файлов. Хэши - это способы кодирования файлов, гораздо меньше по размеру, чем сам файл. Каждый заголовок блока в Эфириуме содержит три дерева Меркла для транзакций, поступления и состояний.



Источник: Merkling in Ethereum, Vitalik Buterin, основатель Эфириума.

Это облегчает клиенту получение проверяемых ответов на такие запросы, как:

- Существует ли данный аккаунт?
- Каков текущий баланс?
- Была ли эта транзакция в определенный блок?
- Произошли ли сегодня по этому адресу определенное событие?

Смарт контракты

Ключевой концепцией Эфириума и других сетей основанных на блокчейне, являются *смарт контракты.* Это самостоятельно исполняющиеся блоки кода, с которыми могут взаимодействовать несколько сторон, что устраняет необходимость в доверенном посреднике. Код смарт контракта можно рассматривать как аналогию правовых положений в традиционном бумажном контракте, но он позволяет получить гораздо более широкие функциональные возможности. Контракты могут иметь правила, условия, штрафы за несоблюдение или инициировать другие процессы. При срабатывании, контракты выполняются так, как это было первоначально указано при развертывания публичной цепочки, предлагая встроенные элементы неизменяемости и децентрализации.

Смарт контракты являются жизненно важным инструментом, для разработки на основе инфраструктуры Эфириума. Основная функциональность блокчейн слоя Гидро достигается с помощью пользовательских контрактов, о чем будет сказано далее в этом документе.

Виртуальная Машина Эфириума

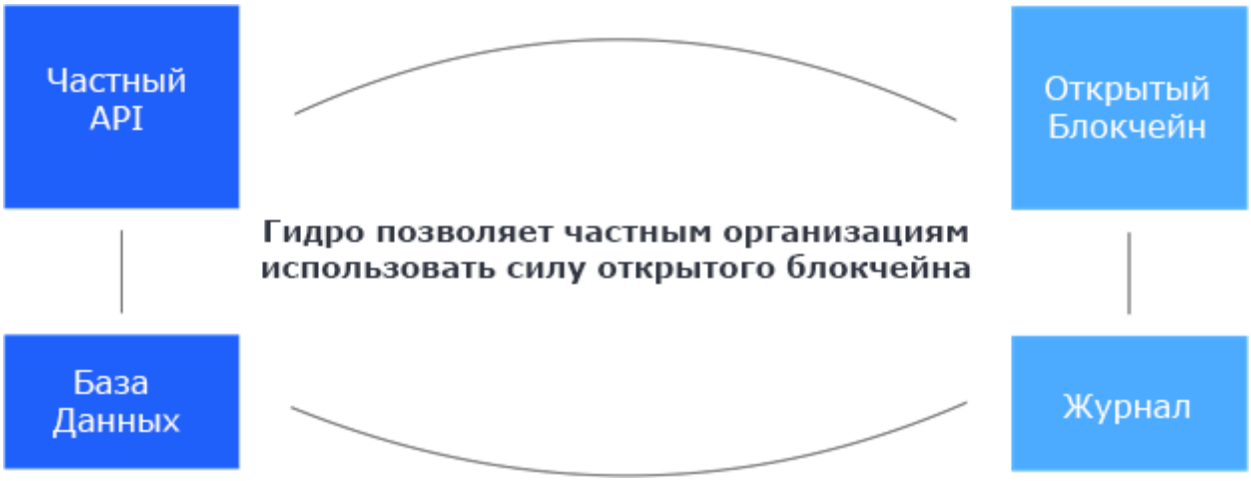
Виртуальная Машина Эфириума (ВМЭ) является средой исполнения для смарт контрактов Эфириума. ВМЭ помогает предотвратить DoS-атаки, гарантируют что программы остаются не обладающими состоянием, и обеспечивает связь, которая не может быть прервана. Действия ВМЭ связаны с затратами, называемыми *газом*, количество которых зависят от требуемых вычислительных ресурсов. Каждая транзакция имеет максимальное количество газа, отведенное ему, известная как *лимит газа*. Если газ, потребляемый транзакцией достигнет предела, то она прекратит свое выполнение.

Открытый журнал

Открытый журнал для частных систем

Системы, которые обеспечивают работу платформ финансовых услуг, веб-сайтов и приложений, часто могут быть описаны как носители потока данных – они отправляют, получают, хранят, обновляют и обрабатывают данные для объектов, с которыми они взаимодействуют. Из-за характера этих данных и финансовых услуг в целом, эти системы часто представляют собой сложные операции на частной и централизованной основе. Расчет на частные структуры, в свою очередь, дает возможность получить различные преимущества в плане безопасности, прозрачности и повышения эффективности, путем интегрирования внешних средств, возможности которых превосходят те, которые предоставляет внутренняя система.

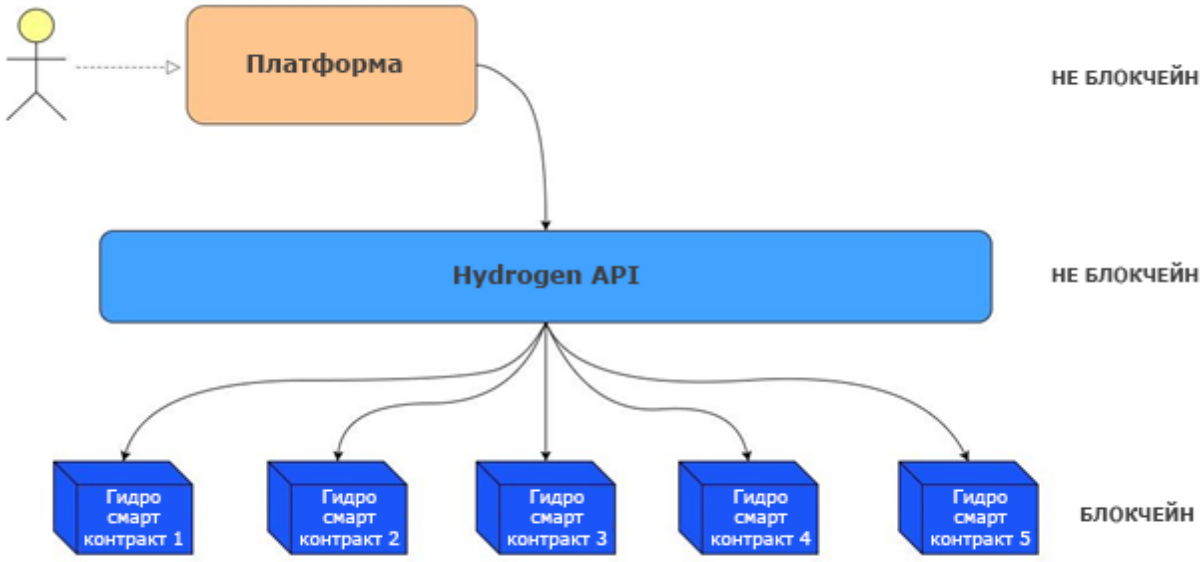
Так обстоит дело с платформой Hydrogen API. Гидро стремится использовать вышеупомянутые преимущества, позволяя пользователям Hydrogen взаимодействовать с блокчейном способами, которые надежно интегрируются в фундаментальную частную экосистему Hydrogen.



Открытые операции на основе блокчейна, могут возникнуть до, во время или после частных операций. Взаимодействие между частными и открытыми элементами может использоваться для проверки, регистрации, записи или улучшения процессов в экосистеме. Идеал этой модели - сделать процессы более надежными, используя преимущества блокчейн технологии, в особенности там, где она может оказывать наиболее позитивное воздействие. Хотя этот гибридная структура не может быть применима ко всем платформам, Гидро фокусируется на том, что бы быть полезной в тех случаев, когда это возможно.

Архитектура для принятия

Гидро отличается от многих существующих проектов на основе блокчейн, поскольку она может существовать независимо и на разных уровнях, сочетаясь с новыми или существующими системами, не требуя при этом системных изменений. Гидро стремится не заменять, а расширять имеющиеся функции. Платформы и организации, которые используют Hydrogen API, автоматически получают доступ к блокчейну.



Спектр платформ финансовых сервисов, которые смогут воспользоваться Hydrogen, широк. Эти платформы могут обеспечивать практически любую функциональность, предоставлять любое количество запатентованных сервисов, обеспечивать любые приватные действия с данными и развертываться в любом окружении. Это обеспечивается модулярной структурой Hydrogen, которая синергична с Гидро и действует, как дополняющее его вспомогательное средство.

Рэйндроп

Служба аутентификации на основе блокчейна, построенная на основе публичного журнала Гидро называется “Рэйндроп”. Она обеспечивает отдельный, неизменяемый, глобально прозрачный уровень безопасности, который проверяет, что запрос на доступ исходит из авторизованного источника.

Частные протоколы аутентификации, такие как OAuth 2.0 предлагают различные уровни надежности и полезности для целого ряда различных существующих вариантов использования. Нет необходимости конкурировать с этими протоколами или пытаться заменить их – Гидро предлагает способ улучшить их, включив принцип работы блокчейна в качестве компонента процедуры аутентификации. Это может добавить полезный уровень безопасности, помогающий устранить уязвимости системы и предотвратить компрометацию данных.

Прежде чем рассматривать технические аспекты Рэйндропа, сначала взглянем на проблему, которую он пытается решить.

Состояние финансовой безопасности

Начало цифровой эры привело к росту количества уязвимостей, что особенно важно для финансовых сервисов. Финансовые платформы часто являются шлюзами для большого количества частных и конфиденциальных данных, таких как идентификационные номера государственных органов, учетные данные пользователей и истории транзакций. Ввиду исключительной важности этих данных, несанкционированный доступ к ним приводит к катастрофическим результатам.

Фирма Trend Micro исследуя отрасль, опубликовала доклад, в котором говорится что украденная персональная идентификационная информация (ПИИ) продается в Deep Web всего за 1$, сканы документов таких как паспорта за 10$, а банковские учетные данные всего за 200$, что делает распространение похищенных данных все более хаотичными и не отслеживаемым.

К сожалению, существующая финансовая система не имеет безупречную репутацию, когда речь заходит о предотвращении, диагностике и передаче данных о нарушениях ее клиентам.

- Согласно недавнему исследованию "The 2017 Identity Fraud Study", проведенному компанией Javelin Strategy & Research – В 2016 году, 16 млрд долларов было украдено у 15,4 млн жителей США из-за сбоев финансовых систем в области защиты ПИИ.
- В Апреле 2017 года, компания Symantec опубликовала доклад "Internet Security Threat Report", где приведены оценки, согласно которым, за 2016 год было похищено 1,1 млрд различных фрагментов ПИИ.
- Отчет "2016 Year End Data Breach Quickview", опубликованный компанией Risk Based Security, сообщает, что в 2016 г. во всем

мире произошло 4149 нарушений сохранности данных, указывая 4,2 млрд случаев.

- "2017 Thales Data Threat Report – Financial Services Edition" – международный отчет, который делают IT-специалисты по профессиональным услугам – указывает, что 49% организаций оказывающие финансовые услуги в прошлом понесли потери от нарушений безопасности, 78% тратят больше ресурсов для собственной защиты, но 73% запускают новые инициативы связанные с искусственным интеллектом, интернетом вещей и облачными технологиями, не обеспечив заранее соответствующих решений безопасности.

Взлом компании Equifax

29 июля 2017 года, компания Equifax - агентство кредитных отчетов работающее 118 лет на территории США, была взломана. 143 млн. персональных данных клиентов, включая номера социального страхования, были подвергнуты риску. Данные, касающиеся кредитных карт 209 тыс. клиентов, были скомпрометированы.

Какая была причина этому нарушению?

Она исходила от одного серверного приложения, использованного компанией Equifax. Struts является фреймворком с открытым исходным кодом для разработки веб приложений на языке Java, принадлежащий организации Apache Software Foundation. CVE-2017-9805 является уязвимостью в Apache Struts, связанную с плагином Struts REST, который использует обработчик XStream для обработки XML полезных данных. При эксплуатации, она позволяет хакерам находящимся удаленно и непрошедшим проверку подлинности, запускать вредоносный код на сервере приложений, чтобы взять машину под свой контроль, либо проводить с нее дальнейшие атаки. Эта уязвимость была исправлена организацией Apache за 2 месяца до взлома Equifax

Apache Struts содержала недостаток в плагине REST Plugin XStream который срабатывает, когда программа небезопасно десериализует XML запрос. Говоря более конкретно, проблема заключалась в методе toObject() класса XStreamHandler, который не накладывает никаких ограничений на входящие данные при использовании XStream десериализации в объект, что приводит к возникновению уязвимостей произвольного выполнения кода.

Даже если этот REST плагин был скомпрометирован, должно ли это иметь значение? Существует ли способ использовать технологию блокчейн для защиты финансовых данных тех 143 млн. клиентов, в то же время полагаясь на действующие REST API и системы основанные на Java?

Добавление блокчейн слоя

Очевидно, что целостность финансовых шлюзов, обрабатывающие данные, может быть улучшена. Давайте рассмотрим, как дополнительный уровень безопасности достигается через Гидро.

Основополагающие механизмы консенсунса сети Эфириума обеспечивают транзакционную достоверность, поскольку участники совместно обрабатывают транзакции, которые должным образом подписаны. Это обстоятельство приводит к децентрализации и неизменяемости, но, что более важно, она обеспечивает вектор для смягчения последствий несанкционированного доступа к шлюзу, который обрабатывает конфиденциальные данные.

При использовании Гидро, аутентификация может быть основана на транзакционных операциях блокчейна. Например, API сможет проверять разработчиков и приложения, требуя от них инициировать определенные транзакции, с конкретными полезными данными, между конкретными адресами в блокчейне, как предварительное условие для инициации стандартного протокола аутентификации.

Гидро Рэйндроп

Дождь (Рэйн) состоят из водяных капель, диаметр которых находится в диапазоне от 0,0001 до 0,0005 сантиметров. При обычном ливне, выпадают миллиарды таких капель, у каждой из которых случайный размер, скорость и форма. Поэтому нельзя достоверно предсказать точную структуру дождя. Аналогично, каждая аутентификационная транзакция Гидро является уникальной и практически невозможно, чтобы она произошла случайно – вот почему мы называем их Каплями Дождя (Рэйндропы).

Платформы финансовых услуг обычно используют проверку микроплатежами для проверки учетных записей клиента. Данная концепция проста: Платформа делает небольшой платеж на случайную сумму на банковский счет, о котором клиент заявляет, что он принадлежит ему. Для того, чтобы доказать, что пользователь действительно владеет этим счетом, он или она должны возвратить обратно этот платеж платформе, который затем проверяется. Единственный способ, который пользователь может знать действительную сумму (помимо угадывания) – это иметь доступ к банковскому счету, о котором идет речь.

Проверка на основе Рэйндропа с Гидро является аналогичной. Вместо того, чтобы отправлять пользователю сумму и возвращать ее обратно, мы определяем транзакцию и пользователь должен выполнить ее из известного ему кошелька. Единственным способом, которым пользователь может провести подтвержденную транзакцию, является доступ к кошельку, о котором идет речь.

Используя Рэйндропы, как система, так и пользователь, имеющий к ней доступ, могут отслеживать попытки авторизации в неизменяемом открытом журнале. Эта основанная на блокчейне транзакция отделена от основных

системных операций, происходит в распределенной сети и зависит от владения закрытыми ключами. Поэтому, она служит полезным вектором валидации.

Детальное рассмотрение

В процессе Гидро аутентификации участвуют 4 объекта:

1. Аксессор (Accessor) – сторона, пытающая получить доступ к системе. В случае Hydrogen, аксессор - это финансовое учреждение или приложение использующее Hydrogen API для своей основной цифровой инфраструктуры.
2. Система (System) – система или шлюз, к которым пытается получить доступ аксессор. Для Hydrogen, этой системой является сам Hydrogen API.
3. Гидро (Hydro) – модуль, который используется Системой для связи и взаимодействия с блокчейном.
4. Блокчейн (Blockchain) – распределенный открытый журнал, который обрабатывает транзакции Гидро и содержит смарт контракты Гидро, в который информация может быть помещена, извлечена или иным образом обработана.

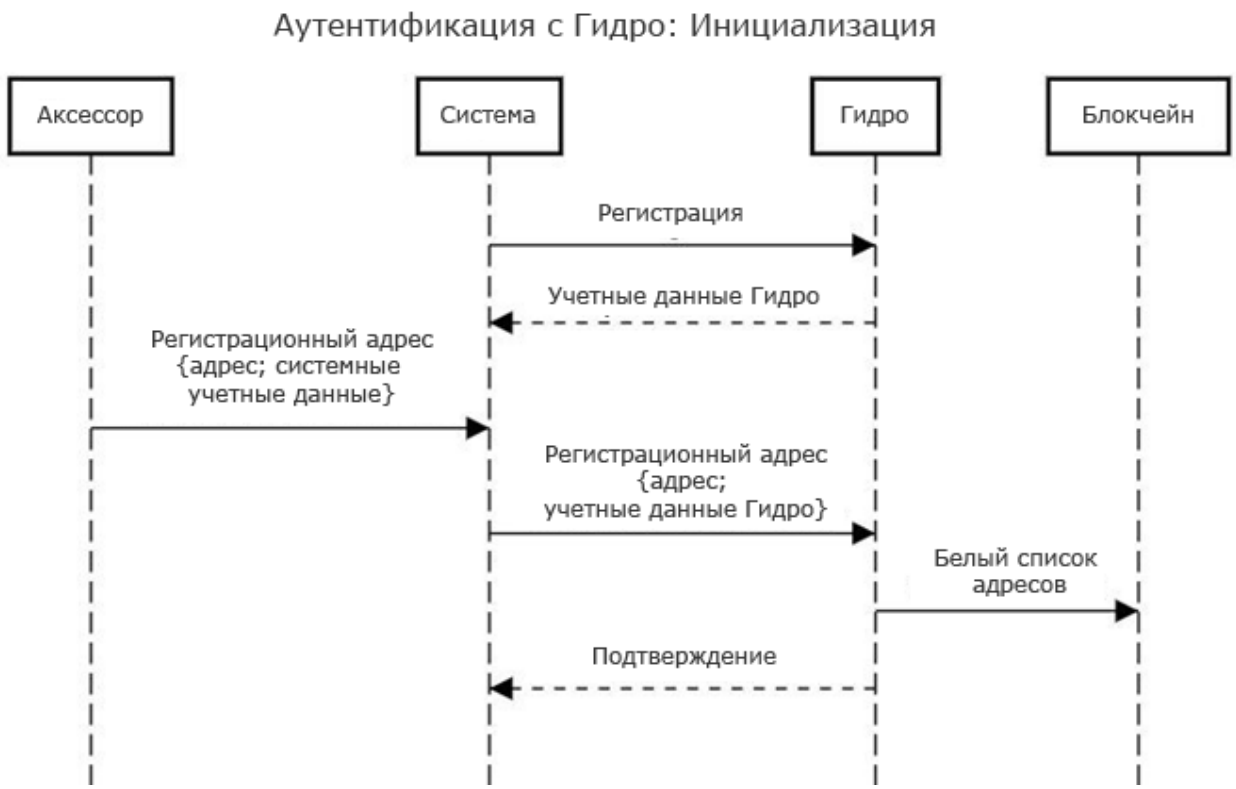
Каждый Рэйндроп, в целом, представляет собой набор из пяти параметров транзакции:

1. Отправитель (Sender) – Адрес который должен запустить транзакцию.
2. Получатель (Receiver) – Конечный пункт транзакции. Это соответствует вызову методу в смарт контракте Гидро.
3. ID – Идентификатор, связанный с Системой.
4. Количество (Quantity) – Точное число Гидро для отправки.
5. Вызов (Challenge) – Буквенно-цифровая строка, сгенерированная случайным образом.

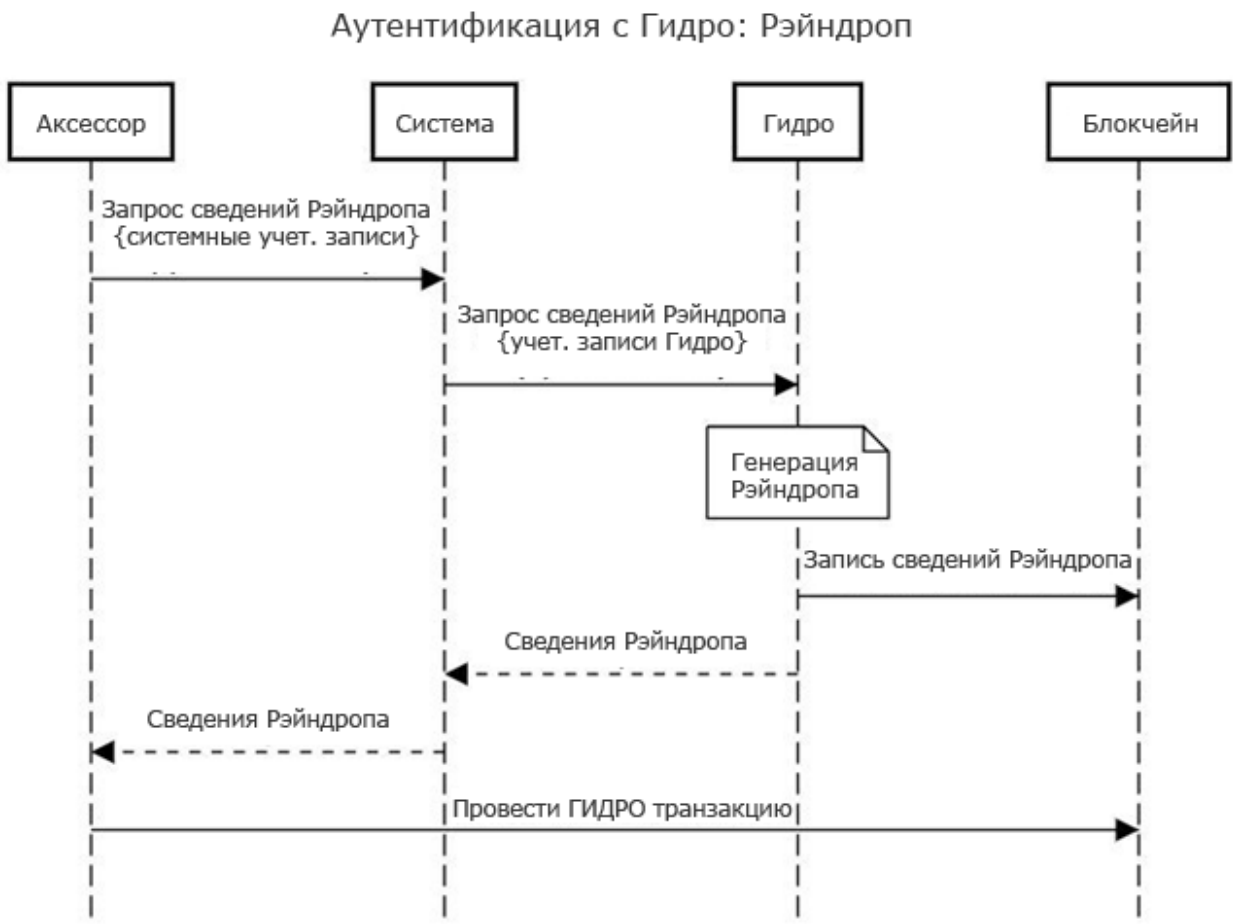
Ниже приводится схема процесса аутентификации, которую обычно можно разделить на 3 этапа:

1. Инициализация
2. Рэйндроп
3. Валидация

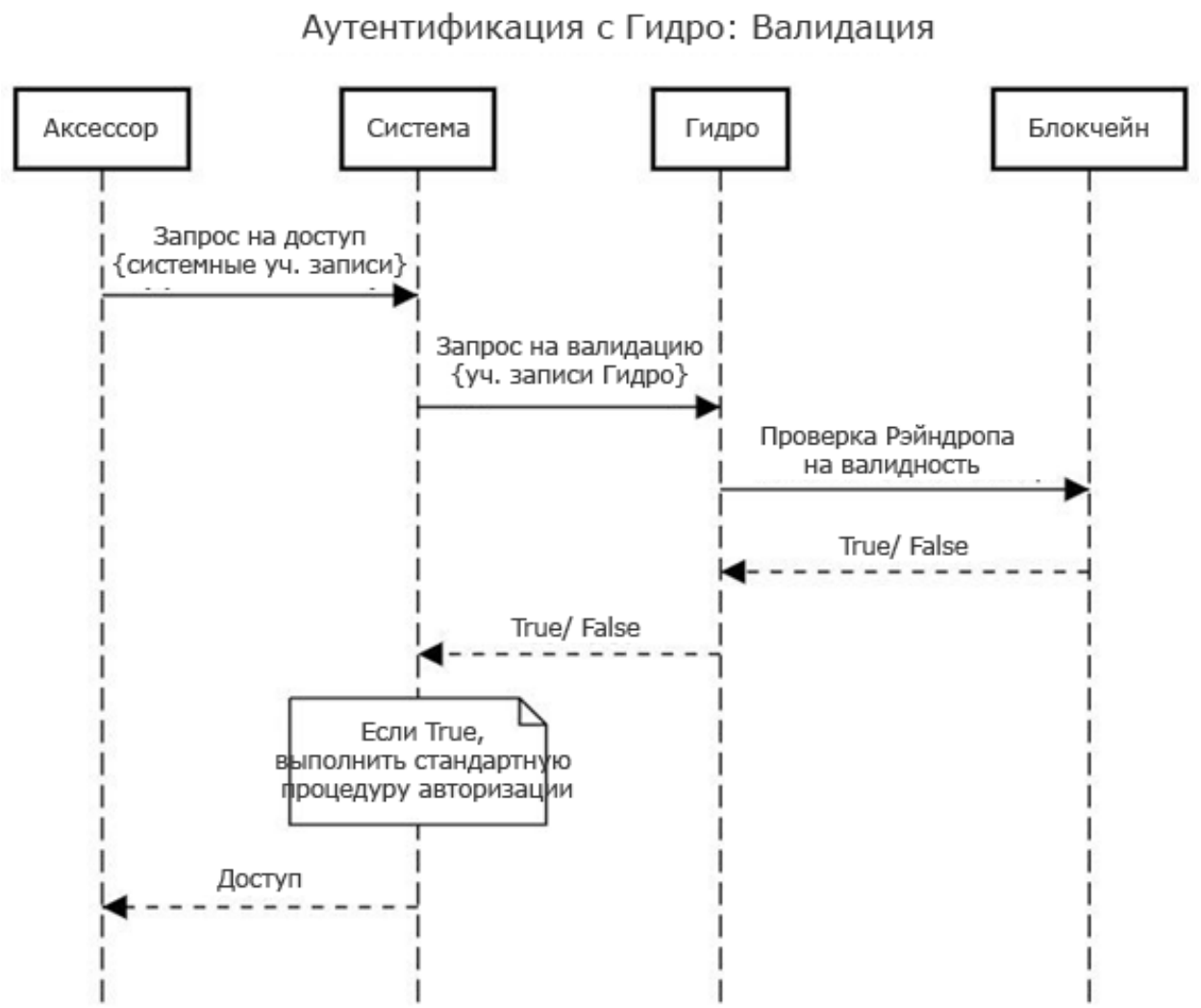
Инициализация начинается с регистрации Системы (например, Hydrogen) для использования Гидро и получения учетных данных, что позволяет системе связываться с блокчейном через модуль Гидро. Системой управляет Аксессор (например, финансовое учреждение), который регистрирует публичный адрес, а затем передает зарегистрированный адрес в Гидро. Этот адрес без изменения записывается в блокчейне в белый список, хранящийся в смарт контракте Гидро. Система получает подтверждение о том, что адрес был занесен в белый список, что можно проверить как общедоступные событие, которое всем видно. Регистрация в системе требуется единственный раз, а занесение в белый список – один раз для каждого Аксессора.



После того, как Инициализация завершена, запускается ядро аутентификации Гидро. Аксессор, который должен выполнить Рэйндроп транзакцию, запускает этот процесс, запрашивая подробные данные Рэйндропа из Системы, а Система перенаправляет запрос на Гидро. Гидро генерирует новый Рэйндроп, сохраняет определенные сведения в блокчейне, не изменяя их, и возвращает уже подробные данные Аксессору через Систему. Аксессор, имеющий всю необходимую информацию, проводит транзакцию с зарегистрированного адреса, обращаясь к методу смарт контракта Гидро. Если адрес не занесен в белый список, то действие отклоняется, а если занесен, то оно записывается в смарт контракт. Важно отметить, что эта транзакция должна происходить вне Системы, напрямую от Аксессора к Блокчейну, так как она должна быть подписана закрытым ключом Аксессора (к которому должен иметь доступ только Аксессор).



Наконец, заключающим этапом является Валидация. Здесь, Аксессор официально запрашивает доступ к Системе через ее установленные механизмы. Перед выполнением какого-либо стандартного протокола аутентификации, Система запрашивает у Гидро, выполнил ли Акссесор валидную Рэйндроп транзакцию. Гидро взаимодействует со смарт контрактом, проверяет на достоверность его, и отвечает пометкой – true/false. Система может решить, как она должна действовать на основе этой пометки. Например - если false, то запретить доступ, если true, то предоставить доступ.



Если мы будем рассматривать основные учетные данные Системы – или любой другой существующий протокол Системы, который имеется в наличии – как один из факторов аутентификации, важно, что уровень Гидро обеспечивает полезный второй фактор. Изучая два основных вектора атаки, мы можем легко подтвердить его пользу:

- Вектор 1 – Злоумышленник крадет основные учетные данные Системы у Аксессора
  - Злоумышленник пытается получить к Системе с помощью валидных учетных данных.
  - Система совместно с Гидро определяет – была ли сделана валидная транзакция на блокчейне.
  - Гидро возвращает false, и Система запрещает доступ.
- Вектор 2 – Злоумышленник крадет закрытый ключ от кошелька Аксессора
  - Злоумышленник пытается провести Гидро транзакцию с зарегистрированного адреса, без необходимых параметров Рэйндропа.
  - Злоумышленник не может сделать валидную блокчейн транзакцию.

- Злоумышленник также не может запросить доступ к Системе без соответствующих учетных данных Системы.

Очевидно, что Злоумышленник должен завладеть как основными системными учетными данными, так и закрытым ключом от кошелька Аксессора, чтобы получить доступ к системе. В связи с этим, Гидро успешно добавляет дополнительный фактор аутентификации

Открытие Рэйндропа обществу

Не смотря на то, что блокчейн сервис аутентификации был спроектирован чтобы защитить экосистему Hydrogen API, он широко применим к различным платформам и системам. Чувствуя, что другие потенциально могут извлечь выгоду из этого уровня верификации, мы открываем его для использования.

Точно также, как Hydrogen будет внедрять его в качестве предварительного условия доступа к своей экосистеме API, так и любая система может добавить его к существующим процедурам и протоколам. Любая платформа – API, приложение, корпоративный софт, игровая платформа и т.д. – может использовать Hydro для аутентификации. Официальная документация будет доступна на сайте GitHub для тех, кто хочет включить этот блокчейн слой в инфраструктуру аутентификации или REST API.

Пример использования – Рэйндроп с OAuth 2.0

Существуют десятки способов использования Рэйндропа для частных организаций. Закрытые API, базы данных и сети создали сложные системы токенов, ключей, приложений и протоколов за последнее десятилетие, пытаясь защитить конфиденциальные данные. Например, Google, стал одним из самых популярных поставщиков на рынке, при помощи приложения Google Authenticator. Как было сказано ранее - нет необходимости заменять существующие протоколы.

В качестве примера использования, рассмотрим кратко, как Hydrogen реализует Гидро аутентификацию в качестве уровня безопасности в своем собственном общем API фреймворка безопасности:

1. Партнеры Hydrogen API, во первых, должны иметь белый список IP адресов собственных различных окружений.
2. Партнеры должны делать запрос на внесение публичного адреса Гидро в белый список.
3. Все вызовы к Hydrogen API и передача данных шифруется и передается через HTTPS протокол.
4. Партнеры должны завершить валидную Гидро Рэйндроп транзакцию с зарегистрированного Гидро адреса.
5. Партнеры должны использовать OAuth 2.0 валидацию. OAuth (Open Authorization) – это открытый стандарт для аутентификации и авторизации на основе токенов. Hydrogen поддерживает типы доступа - “Учетные данные владельца ресурса” и “Учетные данные

клиента”, и каждый пользователь API должен предоставлять учетные данные для запроса аутентификации.

6. Если ни один из пяти вышестоящих пунктов не нарушается, то партнеру Hydrogen выдается уникальный токен, который проверяется и верифицируется при каждом вызове API.
7. Токен будет действовать 24 часа, после чего партнер должен снова подтвердить себя.

Если какой-либо из этих пунктов нарушается, то доступ пользователя к API немедленно блокируется. Хакер не сможет обойти эти факторы безопасности, угадывая случайным образом символы, т.к. существуют триллионы уникальных комбинаций.

Блокчейн аутентификация Гидро является важным компонентом протокола безопасности Hydrogen. Команда Hydrogen призывает партнеров к установке кошельков с мульти-подписями, и хранить закрытые ключи в нескольких защищенных местах независимо от других учетных данных, чтобы не было единственной точки уязвимости. Правильно защищенный кошелек с мульти-подписями не только трудно похитить, но в силу открытости блокчейна также быстро распознать любую кражу, т.к. это связано с безопасностью API.

Любой может отслеживать попытки аутентификации в смарт-контракте Гидро, что означает, что время платформ которые были скомпрометированы месяцами, могут уйти в прошлое. Теперь, попытки взлома API могут быть прерваны с большой оперативностью из-за способности обнаруживать неожиданные попытки авторизации в реальном времени, из любой точки мира.

Риски

Также, как и в любой зарождающейся технологии, например, как в ранние времена социальных сетей, электронной почты и потоковых приложений (который были зависимы от dial-up подключения), очень важно, чтобы основная команда разработчиков тщательно отслеживала новые разработки в скоростях транзакций и объемах Эфириума. Не могли бы вы представить, чтобы YouTube пытался запуститься в 1995 году? Или чтобы Instagram впервые предлагался на Blackberry?

Основные разработчики Эфириума, такие как Виталик Бутерин и Джозеф Пун в работе "Плазма: Расширяющиеся Автономные Смарт Контракты" ("Plasma: Scalable Autonomous Smart Contracts"), предложили улучшить протокол Эфириума:

> *Плазма является предлагаемым фреймворком для более интенсивного и принудительного исполнения смарт контрактов, которые могут масштабироваться до значительного количества обновления состояний в секунду (потенциально миллиарды), что позволить блокчейну иметь возможность представлять большое количество децентрализованных финансовых приложений, по всему миру. Стимулируется продолжение автономной работы этих смарт контрактов за счет платежей за сетевые транзакции, что в конечном итоге зависит от базового блокчейна (например, Эфириума) для обеспечения перехода состояними транзакций.*

Другие проекты, такие как Raiden Network, предложили решение масштабирования вне цепочки, предназначенное для ускорения транзакций и низких комиссий. В то же время, Рэйндроп **будет минимально нагружать** фреймворк Эфириума, поэтому масштабируемость является небольшим риском для успеха технологии.

Заключение

Неизменяемость открытого блокчейна предлагает новые способы повышения безопасности закрытых систем, таких как API.

Этот документ освещает 3 важные вещи:

1. Открытый блокчейн может внести свой вклад в финансовые услуги.

2. Гидро Рэйндроп может повысить безопасность частных систем.

3. Существует непосредственные применения Гидро Рэйндропа в рамках платформы Hydrogen API.

Команда Гидро считает, что новая структура может стать стандартной инфраструктурой безопасности для новых моделей смешанных частных и публичных систем, которая принесет пользу всем заинтересованным сторонам в сфере финансовых услуг и за ее пределами.

Источники:

Ethereum; Merkling in Ethereum

Trend Micro; What Do Hackers Do With Your Stolen Identity?

Javelin Strategy & Research; The 2017 Identity Fraud Study

Symantec; *Internet Security Threat Report*

Risk Based Security; 2016 Data Breach Trends - Year in Review

Thales; 2017 Thales Data Threat Report – Financial Services Edition

Apache.org; Apache Struts 2 Documentation - S2-052

Joseph Poon and Vitalik Buterin; Plasma: Scalable Autonomous Smart Contract