Force Network: Набор Децентрализованных Интернет-Протоколов v0.1

Michael Dye

20 июня 2018 г.

Аннотация

В этой статье мы представляем новую структуру для децентрализованных интернет-протоколов под названием «The Force Network». Эта сеть будет анонимной, масштабируемой, гибкой и позволит пользователям получать доступ к данным и услугам в конфиденциальной и устойчивой к цензуре манере. Основополагающий utility-токен, Force Coin (FOR), служит для многих целей, начиная с механизма стимулирования доставки услуг и их качества и заканчивая инструментом для соглашения по одновременному согласованию сети, а также служит в качестве безопасного средства передачи ключей шифрования между участвующими узлами. Force Network предоставит людям возможность получать доступ к информации и защищенным сетям в любой точке планеты, даже в условиях самых репрессивных режимов, позволяя информации свободно существовать без возможности ее удаления и без несанкционированных манипуляций.

I Введение

Force Nertwork стремится быть полностью анонимным, масштабируемым и гибким набором протоколов, которые предлагают устойчивый к цензуре доступ к данным и сетевым услугам. Мы называем этот набор протоколов Децентрализованными Масштабируемыми Сетевыми Службами (DSNS). Команда Force разработает базовый utility-токен, называемый Force Coin (FOR), инфраструктуру распределения сети, а также систему, которая позволит сетевым узлам предоставлять постоянно расширяющийся перечень различных сетевых протоколов. Независимые разработчики смогут создавать приложения, использующие Force Network поверх платформы любой третьей стороны. После успешного завершения подключения к Force Network, подключение к применимым сервисным сетевым узлам будет ощущаться так же, как подключение к физической локальной сети (LAN).

В то время, как централизованные сети подвержены цензуре, ограничениям доступа к контенту и отдельным точкам сбоя, их преимущество перед децентрализованными сетями заключается в том, что они находятся в лучшем положении для фиксирования постоянных ресурсов высокого уровня с полным резервированием при сбое и более доступны из-за их централизованной природы планирования. Поскольку Force Network будет децентрализованной сетью, где участие поставщиков услуг будет добровольным, мы изложим предлагаемое нами решение касаемо продолжения стимулирования указанных поставщиков с целью поддержания услуг на долгосрочную перспективу для предотвращения прерывания работы службы с последующим ухудшением опыта пользователей.

Первым осуществленным протоколом будет Протокол Передачи Гипертекста (HTTP). Это означает, что любой человек сможет подключиться к Force Network, используя настраиваемую структуру веб-браузера, находящуюся прямо в кошельке. Данный браузер будет кросс-платформой для мобильных и настольных устройств и будет взаимодействовать, как с нашей сетью, так и с обычным Интернетом, но с той лишь разницей, что контент из сети децентрализованных сетевых узлов будет распределен с использованием сквозного шифрования. При использовании Force Network, загруженный или скаченный контент не будет доступен для расшифровки для сторонних субъектов, какими, например, являются провайдеры интернет-услуг.

Распределенным, конфиденциальный интернет

- это только начало. Force Network также стремится разрешить сетевым узлам принимать у себя любой заранее определенный сетевой протокол. Сетевые узлы Force Network будут сгруппированы согласно протоколу, который они предоставляют (Распределенная Услуга Hive, или DSH), а также согласно уровням доступа, которые применяются на сетевом уровне.

Примерами протоколов, поддерживаемых сетью, являются:

- МежПланетная Система Файлов (IPFS);
- Децентрализованные, Виртуальные, Конфиденциальные Сети (DVPN);
- LAN-игры;
- Электронная почта и безопасный обмен сообщениями, возможно, протокол HushList;
- Медия стриминг;
- Услуги Сети по Доставке Контента (CDN);
- Нетворкинг Интернета Вещей (IoT).

II Ключевые Моменты Конкурентной Дифференциации

Force Network разработан, как крупномасштабная децентрализованная сеть, где участникам предлагается предоставлять и потреблять широкий спектр сетевых услуг надежным, конфиденциальным и безопасным способом. Force Network нацелен на достижение этих целей посредством экономического поощрения. Чтобы сеть стала самостоятельной и успешной с самого начала, она должна продемонстрировать свое преимущество перед другими решениями, которые работают в аналогичной сфере.

В интересах оценки рыночного потенциала услуг Force Network и ее способности нарушать текущий ландшафт, мы создали список из нескольких ключевых моментов, которые, по нашему мнению, являются сильными отличительными качествами по сравнению с действующими конкурентами и которые будут поддерживать долгосрочную деятельность Force Network.

1. Полная конфиденциальность сети и шифрование данных. Force Network - единственная монета протокола, которая полностью конфиденциальна, зашифрована сквозным шифрованием и содержит контент, который устойчив к атакам вне сети. Force Network прилагает большие усилия для обеспечения того, чтобы:
   - IP адрес клиента никогда не раскрывался напрямую;
   - IP-провайдеры контента никогда не раскрывались напрямую;
   - данные не могли быть обратно прослежены клиентом или хостом;
   - данные не могли быть расшифрованы каким-либо посредником.
2. Полностью независима от традиционных, технически ограниченных решений. Другие проекты пытаются обеспечить децентрализованный интернет, используя обычные веб-браузеры. Несмотря на то, что использование уже установленных веб-браузеров было бы идеальным решением с точки зрения пользователя, у них существует слишком много проблем с логистикой в работе с такими защищенными и конфиденциальными сетевыми сервисами, которым мы хотим предоставить наши услуги.
   - DNS-протоколы: использование существующей веб-структуры заставляет сеть соблюдать и подвергаться ограничениям, налагаемым существующими веб-протоколами, включая DNS. DNS исторически был первым пунктом атаки для цензурирования контента. Некоторые решения, такие как цепи DNS, пытаются решить эту проблему, но не могут сделать это полностью зашифрованным способом, который позволяет скрыть конечный IP адрес. Кроме того, несмотря на то, что в случае необходимости он позволяет сайтам сохранять свой существующий домен, он также делает возможным риск централизации и не соответствует нашим критериям автономной и устойчивой к цензуре сети.
   - Шифрование SSL. Использование обычных веб-браузеров означает, что единственной доступной схемой шифрования является SSL. Это требует модификация браузера для импорта пользовательских сертификатов SSL и не позволяет внедрить гораздо более мощную схему мульти-шифрования Force.
   - Используя существующие веб-браузеры, нет возможности скрыть IP адрес клиента и хоста. Это является важным условием для поддержания Force Network, как конфиденциальной и устойчивой к цензуре сети.

Для того, чтобы сделать сеть по-настоящему конфиденциальной, Force предлагает разработать собственный браузер, находящийся в кошельке. Это позволяет Force Network использовать собственные разрешения имен и протоколы шифрования, гарантируя, что анонимный трафик в сети остается секретным и устойчивым к цензуре.

С учетом вышеизложенного, незашифрованные общедоступные страницы будут доступны для просмотра с помощью обычных веб-браузеров. Эта услуга позволит всем пользователям с максимальной легкостью просмотреть общедоступную информацию (например, услуги, цены и адреса кошельков платежных узлов). Незашифрованные общедоступные страницы также предоставляют знакомые точки доступа к контрактным услугам в сети Force Network.

3. Force - это мультипротокольная сеть, предоставляющая широкий набор децентрализованных и масштабируемых сетевых сервисов. Помимо функций конфиденциальности, Force Network стремится быть гораздо большим, чем просто веб-решением. Мы планируем создать целый ряд конфиденциальных сетевых сервисов и протоколов на основе базового протокола Force Network, как описано в разделе III.

   Это тот пункт, который отличает Force Network от схожих технологий. Становясь чем-то большим, чем просто ограниченным, нерасширяемым решением только для Интернета, Force стремится стать протоколагностической и расширяемой структурой. Force Network может поддерживать множество услуг различной природы, эффективно являясь полной заменой существующим крупномасштабным традиционным сетям.

4. Гранулированная модель оплаты конкретных сервисов. Force Network в полной мере использует экономический профицит используя механизм разумного ценообразования (DSP) и информацию из базы данных о здоровье узлов. Сеть постоянно следит за теми областями обслуживания (DSH), которые или недостаточно обслуживаются, или наоборот чрезмерно, и соответственно этому, корректирует цены в масштабе всей сети, чтобы участники постоянно стремились к равновесию качества и доступности по всему спектру услуг, предоставляемых сетью.

   Это является принципиально иным подходом к традиционным механизмам балансировки нагрузки, которые существуют в услугах с одной задачей. Нагрузка больше не рассматривается в качестве сетевого ресурса, который не используется оптимальным образом для предоставления услуги, а скорее, как экономическая ценность, которая остается неиспользованной, в то время, как целая область обслуживания является сбалансированной для достижения гармонии между предложением и спросом.

5. Force Network использует динамическую модель предоставления услуг Plug-and-Play, похожую на модель Uber. Являясь контрапунктом к выше описанному пункту № 4, а также для обеспечения разумного ценообразования, узлы могут динамически отсоединяться и присоединяться к любому DSH, основываясь на свои предпочтения, без необходимости установки дополнительного оборудования. Это плавный переход, который позволяет сети в целом обеспечить мизерное время простоя, превосходное качество обслуживания и пользовательский опыт, в то же время полностью компенсируя поставщиков услуг в этом процессе. Выход из сети в качестве поставщика услуг будет вести к расходам, однако они будет значительно ниже, чем те расходы, которые обычно сопровождают данный процесс. Это будет применимо только во время доставки активной услуги и будет бесплатным, если узел не будет работать.

   Данная модель распределения затрат помогает выровнять игровое поле и повышает подотчетность для всех участников. В настоящее время, расходы, связанные с переключением услуг, в основном, обременяют потребителей, в то время, как с поставщиков услуг взимается минимальная плата за отмену (например, плата за отмену в случае любого повторного прекращения обслуживания).

   Force Network также предполагает, что будут разработаны более совершенные средства управления сетевыми узлами с целью оказания разумной помощи провайдерам сетевых узлов в достижении максимального использования их узлов (и таким образом, доходов), таких как внутренние службы, которые автоматически контролируют рынок и выполняют мягкие (с меньшими сборами) переходы

от услуг с низким спросом к услугам с высоким спросом.

III Обзор Сетевой Инфраструктуры

III. A Сетевое расслоение

Мы предлагаем трехслойную сетевую модель для предоставления Force Network услуг. Эти три слоя взаимодействуют друг с другом таким образом, чтобы гарантировать, что услуга Force Network работоспособна.

- **1-ый Слой** будет базовым протоколом консенсуса proof-of-stake, с приложенным конфиденциальным блокчейном. Это то место, где будут происходить транзакции Force Network и будет утилизироваться валидация proof-of-stake. Также, с помощью 1 Слоя, будут переданы ключи шифрования и IP адреса точек входа.
- **Во 2-ом Слое** будут отображаться мастерноды, которые будут выступать в качестве первой точки подключения к Force Network. Мастерноды будут размещать такой контент, как страницы индекса сетевой услуги, информацию о работоспособности узла и шифрованные маршруты узлов перехода.

  Страницы индекса будут включать такую информацию, как описание сетевых услуг, цены и адреса кошельков платежных узлов. Эти страницы также будут доступны для просмотра с использованием традиционного Интернета. Страницы индексов сетевых услуг могут обновляться только с помощью правильного конфиденциального ключа, генерируемого платежным узлом при создании данной услуги.

  Мастерноды также будут накапливать и сохранять информацию о состоянии сети (NHI) для мониторинга производимого узлами оплаты. В то время, как вся идентифицируемая информация в реальном мире будет зашифрована для предотвращения нарушения конфиденциальности, NHI будет общедоступен в качестве средства предоставления столь необходимой прозрачности потребителям с целью оказания помощи в процессе выбора ими будущих поставщиков услуг. Мастернода не будет знать прямого IP адреса какого-либо из узлов. Вместо этого, платежный узел будет генерировать уникальные маршруты после завершения оплаты услуг (см. Раздел III D.). Мастерноды периодически хешируют свои базы данных и синхронизируются с остальной сетью мастерноды.
- **3-ий Слой** будет уровнем обслуживания и доставки, состоящим из множества различных узлов. Это те узлы, которые предоставляют все низкоуровневые услуги сетевого протокола. (См. список примеров поддерживаемых сетевых протоколов в разделе “Введение”). Каждый узел, в любой момент времени, может добровольно и динамично входить или выходить из распределенной услуги Hive (DSH). DSH представляет собой набор сетевых узлов, одновременно выполняющих протокол определенный услуги с целью формирования распределенной сети, которая размещает и передает эту услугу. Например, услуга DVPN будет представлять собой собственный DSH, где любое количество узлов может одновременно присоединиться или отсоединиться от определенного Hive, и каждый Hive будет предоставлять свою услугу, используя собственные составляющие узлы. Узел может также работать как узел оплаты, известный как Service Escrow Oracles (SEO). Функциями SEO являются:
  - служить посредником между провайдерами услуг и потребителями;
  - обеспечивать безопасную доставку услуги после получения платежа;
  - заключать контракты с сетевыми узлами;
  - генерировать цепи узлов перехода (см. Раздел III. Г);
  - шифровать IP цепей узлов перехода;
  - передавать клиенту ключи шифрования для каждого шага цепи узла перехода;

  SEO будут называться “платежными узлами”. Более подробная информация о функции платежных узлов будет описана ниже.

III. B Специальная Маршрутизация Цепи (Ad-Hoc Chain Routing) и Крупномасштабная Туннельная Сетевая Архитектура

Force Network использует механизм Ad-Hoc Chain Routing (AHCR), который означает, что запросы не передаются по всей сети. Вместо этого, запросы перемещаются только по цепи узла перехода, причем каждый узел перехода знает только IP адрес того узла, который был до него, а также последующего узла, к которому переходит транзакция в соответствии с типом запроса услуги. Ответы возвращаются по той же цепи, пока они не дойдут до запрашивающего лица. Даже тот узел, который находится непосредственно после исходного запроса не знает, кем является исходное запрашивающее лицо, поскольку оно выглядит как еще один узел

перехода.

В рамках Force Network, для идентификации узлов используются уникальные хешированные общедоступные адреса (UHPA). UHPA хранятся с помощью мастернод наряду с другими жизненно важными сервисными данными для создания динамической базы данных, которую могут использовать платежные узлы, с целью определения оптимальных узлов для включения в Ad-Hoc цепи для каждого запроса на услугу. UHPA используются для корреляции общей информации с узлами, тогда как традиционные IP адреса используются только платежными узлами во время процесса генерации узла перехода и самими узлами перехода (подробнее см. Раздел III D). IP адреса используются только тогда, когда это необходимо для обеспечения базовой связи TCP / IP между узлами.

В дополнение к механизму AHCR и формированию достаточно глубинного решения с полным подключением по картографии и маршрутизации, Force Network будет использовать крупномасштабную туннельную сетевую (LSTN) архитектуру, где каждому участвующему узлу будет автоматически присвоена UHPA, которая известна множеству мастернод. Использование LSTN способствует полному скрытию всех IP адресов от общедоступной сети мастерноды. IP каждого контрактного узла отправляется на платежный узел только после оплаты контракта.

Узел может выбрать одновременное предоставление нескольких услуг и затем одновременно присоединиться к более чем одному DSH. Прежде чем узел присоединяется к новому DSH, он генерирует новый UHPA и загружает ее в мастерноды. Это уменьшает векторы атак, поскольку корреляция идентификаторов услуг становится более трудной. Сами DSH не будут содержать никакой информации о маршрутизации и будут из себя представлять простые и эффективные конструкции группировки для участвующих узлов.

III. C Связь с сетью

Первоначальное создание служб требует деликатной двусторонней связи для поддержания конфиденциальности и устойчивости к цензуре. В этом разделе мы описываем процесс, который Force Network будет использовать с целью задействования услуги с того момента, когда клиент подключается к мастерноде и до момента, когда клиент получит запрошенные данные.

1. Клиент запрашивает список услуг, размещенных ближайшей мастернодой и выбирает услугу. В списке указаны минимальная требуемая цена, адрес кошелька и вид предоставляемой услуги.

2. Клиент отправляет сумму FOR по указанному адресу со следующей информацией, прикрепленной к транзакции:

   – Публичный ключ уникальной пары ключей, которую он генерирует для дешифрования данных.

   – Примерное расположение клиента для оптимизации маршрута (необязательно)

   – Любую другую информацию, необходимую для предлагаемого типа услуги

3. Платежный узел, связанный с адресом кошелька, инициируется оплатой и генерирует цепь узлов перехода. Этот процесс устанавливает зашифрованное анонимное соединение между клиентом и поставщиком услуг. (Эти шаги описаны ниже, в разделе “Как создается цепь узлов перехода”).

4. Платежный узел шифрует IP адрес точки доступа с помощью открытого ключа клиента и отправляет микрооперацию с прикрепленными данными обратно клиенту.

5. Клиент расшифровывает IP адрес входящего узла перехода с использованием закрытого ключа, сгенерированного во 2-ом шаге, и теперь он имеет точку входа в Force Network и все ключи шифрования, необходимые для многократного шифрования запроса данных для каждого перехода. (Подробнее см. в разделе “Шифрование IP адреса узла перехода”).

6. Теперь клиент может многократно зашифровывать и отправлять / получать данные для услуги в / из IP точки входа цепи перехода. Вход узла перехода будет перенаправлять данные на IP адрес следующего узла перехода, установленного платежным узлом, а данные будут продолжат этот путь до тех, пока не достигнут конечного узла хостинга.

III. D Как создаются цепи узлов перехода (процесс генерации цепей узлов перехода)

После того как клиент отправит платеж на адрес кошелька платежных узлов, платежный узел сгенерирует цепь узлов перехода для подключения клиента к узлу запрашиваемой услуги. Чтобы сеть работала быстро и плавно, платежные

узлы должны быть очень экономичными в том, как именно они генерируют цепи узлов перехода. Каждая цепь может генерироваться динамически и уникально для клиента, запрашивающего ее. Цепи также должны быть упругими и обеспечивать долговечность. Поэтому процесс генерации цепей происходит как можно реже.

Мастерноды предоставляют список каждого узла перехода UHPA, который включает в себя адрес кошелька, общедоступный ключ шифрования, приблизительную геолокацию, коэффициент времени работы и стоимость этих услуг. Один узел, на котором запущен один кошелек, может иметь несколько UHPA для различных предоставляемых услуг. Платежные узлы используют этот список для динамического задействования наилучших узлов для предоставления услуги клиенту. В случае нашего первоначального интернет-сервиса, лучшими считаются те узлы, которые расположены рядом с клиентом, чтобы свести латентность к минимуму.

Когда узел платежей обнаруживает подходящие узлы перехода, он отправляет туда платеж с прикрепленным пакетом контрактов и зашифрованным при помощи открытого ключа узлов. Пакет контракта включает:

- идентификатор услуги для идентификации этого договора;
- ключ кодовой фразы для идентификации и аутентификации конечного пользователя;
- закрытый ключ для дешифрования многократно зашифрованных данных одним этапом и тем самым делая отслеживание данных по узлам невозможным;
- IP следующего узла в цепи для пересылки данных;
- дополнительные IP адреса узла перехода, если основной узел не работает (дополнительная услуга).

Если в случае сбоя, услуга хочет свести к минимуму создание дополнительных узлов перехода, то во время первоначального генерирования цепи могут быть предоставлены альтернативные IP адреса следующего перехода. Если первичная точка выходит из строя, то альтернативный вариант можно попробовать без необходимости создания новой переходной цепи.

Если узел перехода не сможет передать данные, то информация о невыполнении возвращается по цепи обратно клиенту и с возвратом денег за вычетом комиссионных сборов.

Тогда клиент отправляет другую транзакцию в кошелек платежных узлов, чтобы создать новую цепь. Эти транзакции могут быть микроплатежами за наименее дорогостоящее решение или включать в себя более крупный платеж за услуги, приобретенные заблаговременно.

Этот механизм загрузки / извлечения для цепи перехода имеет множество преимуществ:

- IP адрес узлов хостинга оплаты и контента никогда не раскрывается клиенту.
- IP адрес клиента никогда не отображается на узлах хостинга оплаты или контента.
- У платежных узлов есть возможность предварительно контролировать статус узла и при необходимости отправлять новые IP адреса узла перехода.
- Узлы перехода знают только предыдущий IP адрес и следующий IP адрес в цепи. Они не знают, на какой стадии они находятся в цепи, поэтому они не могут знать, является ли предыдущий IP адрес клиентом, или следующий IP адрес конечным пунктом назначения.

Вся связь, проводимая через Force Network, будет зашифрована используя алгоритмов шифрования аппаратных средств. Это контрастирует с традиционными сертификатами SSL, которые требуют известных, центрально присвоенных доменных имен в качестве доверенного бенефициара. Поскольку традиционные браузеры, такие как Chrome, Firefox и Safari, спроектированы именно таким образом, чтобы требовать такую сертификацию SSL для достоверного информирования пользователя о том, что их связь зашифрована, то Force Network будет использовать специально созданный, встроенный в кошелек браузер на основе Chromium, сохраняя при этом тот же уровень удобства и легкости использования, к которым привыкли конечные пользователи. Браузер и кошелек будут открытыми для обеспечения независимого аудита безопасности.

После того, как вышеупомянутый набор технологий будет полностью разработан и защищен, следующей вехой станет перенос некоторых сервисов на традиционные настольные и мобильные браузеры с использованием пользовательского расширения и / или мобильного приложения в качестве моста между требованиями к дизайну браузера и архитектурой Force Network. Это позволит Force

Network расширить свои сервисные предложения.

Каждый DSH установит количество необходимых переходов для своей службы. Эта автономия позволит некоторым службам быть более конфиденциальными, чем другие и по более высокой цене. Некоторые данные, такие как индексные страницы, могут быть зачислены, как не конфиденциальные и могут быть поданы непосредственно из мастернод с использованием традиционного Интернета.

Цепи узлов перехода создаются платежным узлом, после того, как платеж получен от клиента. Узел оплаты может учитывать множество факторов при проектировании запрошенной цепи узлов перехода на основе услуги, требований к пропускной способности, приблизительного местоположения и т. д..

III. E Как платежный узел генерирует обратную цепь для ограниченного знания IP

IP адреса очень мощные. IP адрес - это метод, с помощью которого хосты контента могут быть идентифицированы и контент может быть удален. Поскольку мы создаем сеть страниц, устойчивых к удалению, мы должны быть очень осторожны в протоколе управления безопасностью для IP адресов, особенно IP конечного узла хостинга. Чтобы сохранить эту конфиденциальную информацию, мы будем использовать схему ограниченной информации, чтобы только предыдущий узел в цепочке знал следующий IP адрес в цепи, и ни один из сервисных узлов не знал о конечном пункте назначения.

1. Платежный узел получает IP адрес узла хоста, либо заключая контракт с одним из них, либо используя тот, который устанавливают поставщики услуги.

2. Платёжный узел заключает контракт с конечным узлом перехода в цепи и отправляет ему IP хостингового узла в качестве следующего перехода. Этот узел перехода отправляет свой IP адрес платежному узлу (с другой микро транзакцией).

3. В конечном итоге, платежный узел попадает на первый узел перехода в цепи и отправляет этот IP адрес клиенту в качестве точки входа.

IV Расширенные функции поддержки сети

IV. A A Информация о состоянии сети и подтверждение работоспособности узла на основе хэш (HNUV)

Если узел хочет прекратить свои услуги (постоянно или временно, и независимо от причины), он должен пройти надлежащую процедуру выхода. Это влечет за собой отправку уведомления о выходе на мастерноду, которая может обновлять базу данных узлов. Указанная база данных периодически проверяется узлами оплаты для определения доступности узлов для генерации цепей перехода, а также для штрафов за простой.

Если узел отказывает, не следуя процедурам выхода, то в цепь узлов перехода будет встроен механизм повтора. Узел, который расположен до отказавшего узла, отправит IP адрес отказавшего узла платежному узлу с микро транзакцией. Затем платежный узел, либо отправит новый следующий IP адрес на этот узел перехода, либо создаст совершенно новую цепь и отправит ее клиенту. На основе схемы платежей по контракту, платежный узел примет к сведению отказавший узел, оштрафует его и отправит отчет в базу данных информации о состоянии мастерноды.

Для совершения данной операции, каждому узлу необходимо будет открыть и запустить кошелек Force. Кошелек будет периодически отправлять зашифрованные данные в сеть главного узла, включая UHPA, типы предлагаемых услуг, приблизительное местоположение для эффективной маршрутизации, время безотказной работы и статус. Это позволит новым платежным узлам выбирать лучший маршрут для каждого отправителя. С достаточным количеством сообщений об отказавшем узле, мастернода будет обновлять информацию о состоянии узлов и соотношении времени безотказной работы в базе данных, а затем распространять обновление на другие мастерноды. Когда узел снова подключится к сети, он должен повторно отправить свою служебную запись в мастерноду, чтобы заново зарегистрироваться. Поскольку узлы перехода не обладают возможностью отправлять данные на платежные узлы без осуществления транзакции, вместо этого они периодически передают информацию о работоспособности в сеть мастерноды, чтобы с ними могли связаться новые платежные узлы.

С целью еще большей защиты сети от злона-

меренных участников и для обеспечения качества услуг QoS, будет внедрен механизм HNUV. Подобно тому, как консенсус блокчейна может выбирать - принять ему или отклонить узел из сети на основе целостности передаваемых им данных, просто проверив хэш заголовка, то любая злонамеренная попытка узла удержать свой активный статус для оплаты, изменяя своего клиент с тем, чтобы отправить ложные данные о безотказной работе без выполнения услуги, предлагаемой DSH, членом которой он является, приведет к отказу от сети, за которым последует штраф за соединение в виде периода заморозки. Это будет сделано путем проверки хэша кода клиентов, а также ключевых параметров, которые он периодически транслирует с использованием уникального алгоритма хэширования и верификации - HNUV.

IV. B Настраиваемые уровни конфиденциальности

Различные типы контента могут иметь разные уровни безопасности, основанные на том, как установлен платежный узел для данной услуги. В этом техническом документе мы описываем самые высокие уровни безопасности, так как они являются наиболее сложными для выполнения. Все, что находится уровнем ниже, (меньшее количество переходов, отсутствие переходов, меньшее шифрование и т. д.) будет доступно для служб, которые предпочитают скорость абсолютной конфиденциальности или устойчивости контента.

IV. C Хостинг контента и / или услуг в Force Network

У поставщиков контента и услуг есть множество способов размещения контента на Force Network. Для простого примера предположим, что Вы хотите разместить устойчивую к цензуре веб-страницу в Force Network.

1. Настройте платежный узел (или заключите с ним контракт) и определите цену для своего контента. Бесплатный контент легко распространяется через существующую сеть, но должен быть доступен для всех. Контент / услуги, использующие систему разрешений для ограничения доступа, должны взимать плату.

2. Настройте сеть узлов переходов (или заключите с ней контракт) для дальнейшего использования. Узел оплаты также может быть разработан для использования базы данных главного узла для динамического заключения контракта узлов переходов для каждого пользователя с узлами, которые соответствуют списку его критериев.

3. Настройте сетевой узел (или заключите с ним контракт), который подключается к веб DSH для хранения и размещения Вашего контента.

4. Загрузите страницу индекса услуги в сеть главного узла и задействуйте Ваш платежный узел для принятия платежа от клиентов. Теперь для доставки контента он может генерировать для клиентов цепи узлов переходов до сетевого узла.

Разработчики создадут службы, которые будут автоматизировать общие задачи в Force Network и предоставлять шаблоны. Они также будут создавать полные комплекты управления контентом, которые располагаются поверх Force Network. Одна служебная сеть или сетевой узел могут заключать контракт с другим, чтобы для удобства пользователя агрегировать контент в одном месте.

IV. D Модель управления доступом к сети

Безопасность и конфиденциальность лежат в основе Force Network. В соответствии с нашим упором на безопасность и конфиденциальность, на уровне сети мы разработаем обширный механизм контроля доступа, основанного на разрешении. У злонамеренных участников не будет возможности напрямую подключиться к узлам сети, ответственным за доставки услуг. Даже для просмотра IP адреса первого узла перехода, они должны будут пройти полную схему авторизации, настроенную узлами оплаты. Они также должны будут владеть правильным служебным ключом, прежде чем узел входа сможет должным образом маршрутизировать их запрос.

Чтобы проиллюстрировать эту мощность доступа к защищенной сети, давайте сравним ее с существующей моделью. В существующем интернете нет встроенных ограничений на доступ к контенту. Каждая веб-страница должна иметь собственные функции управления учетными записями для защиты своего контента от общественности. Любой пользователь имеет доступ к полям имени пользователя и пароля. Без существующих ограничений традиционный интернет постоянно уязвим для инъекционных взломов и грубой силы. Кроме того, IP адрес сервера напрямую доступен злоумышленникам, что делает сайт уязвимым для DDOS атак и других серверных атак.

Напротив, Force Network требует, чтобы потенциальный пользователь переходил по нескольким уровням безопасности. Если не предоставлен явный доступ, то узел платежа не выдаст Вам IP адрес первого узла перехода. Даже если у Вас он есть, без правильного служебного ключа, узлы обслуживания не будут распространять Ваш запрос или предоставлять какие-либо другие услуги. На основе служебного ключа запросы могут даже маршрутизироваться на разные сетевые узлы в зависимости от уровня доступа. Этот доступ, контролируемый на сетевом уровне, значительно уменьшает векторы атак хакеров.

Каждая страница, файл или служба могут иметь свой собственный список разрешений с такими параметрами, как: разрешать всем ограниченный доступ для чтения, ограниченный доступ для письма и т. д. Поскольку узлы распределены, нет необходимости размещать ограниченную информацию на том же узле, что и публичная информация. Это означает, что веб-сайт может иметь индексную страницу общественного пользования, доступную всем и размещенную в сети бесплатных узлов. Публичная индексная страница может разъяснять, что предлагает сайт, а также указывать цены и адрес кошелька платежного узла. Остальная часть сайта / услуги будет доступна только после удовлетворения требований платежного узла для этого сайта.

V Утилиты и экономика токенов

V. A Случаи использования токенов FOR

1. **Для платы за услуги.** Они пересылаются непосредственно потребителями на узлы оплаты по условному депонированию, которые, в свою очередь, ретранслируют их на узлы предоставления услуг, за вычетом комиссии. Платежный узел может группировать платежи на основе схемы оплаты узлов, с целью уменьшения нагрузки на сеть и снижения платы за перечисление.

2. **Для управления обмена аутентификационными ключами.** Клиенты оплачивают адрес кошелька, связанный с услугой, указанной в базе данных мастерноды. Платежный узел управляет кошельком и отправляет ключи доступа клиенту после создания сетевой цепи.

3. **Чтобы заниматься стекингом монет для создания узла (основного, платежного, перехода, сетевого и т. д.) с целью обеспечения благоприятного поведения.**

4. **Для вознаграждения мастернод и стекеров монет за предоставление консенсуса, расширенных услуг и обеспечения безопасности Force Network.**

V. B Стекинг токенов FOR

Любой человек может превратить свое устройство в любой тип необходимого им узла Force, в зависимости от ресурсов, которыми он владеет и которые он хочет разместить в сети. Тип узла может быть задействован только в том случае, если удовлетворяются требования к конкретным ресурсам узла (например, залоговое обеспечение токена и требования к оборудованию).

Чем более важен тип узла для сети, тем выше залог, который требуется от пользователя для его работы. В результате этого, чем более критичный становится узел, тем менее вероятно, что пользователи будут следовать векторам вредоносных атак в сети, используя указанный узел, поскольку они будут рисковать еще большей долей своих инвестиций. Это самая основополагающая предпосылка, обеспечивающая консенсусную защиту proof-of-stake, применяемую к сети Force Network.

V. C Оплата за услуги

Force Network работает, скрывая как можно больше информации о соединениях. В этом разделе описывается, как оплачиваются услуги с использованием криптовалюты FOR.

Сервисный узел отслеживает использование на основе сервисного ключа, созданного при создании сетевой цепи. При отправке данных он может уведомить клиента, что необходимы дополнительные средства, и при необходимости может закрыть доступ к контенту. После этого клиент может отправить дополнительные средства на платежный узел, который затем обновляет статус оплаты в сервисном узле. Платежный узел будет использовать эти средства для оплаты узлов перехода с использованием согласованной схемы обслуживания.

Узлы перехода могут отслеживать данные об использовании на основе служебного ключа. Различные узлы будут иметь разные требования к платежам, которые основаны на предпочтениях операторов узлов. К примеру, некоторые узлы перехода могут ограничивать общее количество использования служебного ключа, или же пропускную способность, используемую этим ключом. Ес-

ли платеж не соответствует ожидаемому объему, узел перехода может сообщать о нарушениях платежных узлов в сеть мастерноды. Вредоносные узлы будут оштрафованы на монеты, с помощью которых они занимаются стекингом.

V. D Динамичное Ценообразование Услуг (DSP)

Поскольку сеть будет распределена, а участие провайдера услуг будет добровольным, архитектура должна быть в состоянии обеспечить высокие стандарты доступности услуг для удовлетворения спроса. Относительно простым способом обеспечения беспрецедентной доступности услуг будет стимулирование поставщиков услуг путем создания справедливого и динамично развивающегося механизма умного ценообразования для предлагаемых ими услуг. Для этого мы предлагаем механизм динамичного ценообразования услуг (DSP). DSP - это функция, рассчитанная и проверенная сетью, целью которой является определение наиболее экономичной ценовой точки для поставщиков услуг, которая как можно ближе к реальному времени на основе сочетания следующих факторов:

1. **Оценка требований к совокупной сервисной сети (CSNRS):** сеть будет оценивать общий уровень ресурсов необходимых для каждой услуги с целью обеспечения достаточного качества обслуживания, создавать составной балл, который будет служить множителем, а при прочих равных условиях, чем выше будут требования услуги, тем выше будет цена для обеспечения адекватной компенсации.
2. Отношение количества активных пользователей потребляющих каждую услугу (потребность в услугах) N_u к числу сетевых пользователей, активно участвующих в DHS (предоставление услуги) N_{node}.
3. (Не обязательно) Стоимость токена FOR в фиате, основанного на объемно-взвешенном среднем показателе, полученном из данных обмена.

Специализированные DSP будут вычислять и нормализовать свои данные с целью создания рейтинга цен на услуги. Каждый нормализованный балл DSP будет умножен на индекс сетевых цен (NPI), который будет получен путем обзора номера 2 (вышеупомянутого), как соотношение, так и как абсолютное число.

Каждый узел также получит базовый ранг, определяемый его производительностью в сети и надежностью обслуживания. Это создаст элемент конкуренции между узлами, для того, чтобы стать самым надежным узлом для каждой услуги. Узел, который продолжает перескакивать между службами и впоследствии создает прерывания, получит значительно более низкий ранг, чем узел, который сохраняется, даже если цены на услугу в целом снижаются.

Информация о ценах будет распространяться по сети и будет доступна для всех участников. Основываясь на данных DSP, клиенты смогут принимать разумные решения по потреблению услуг, а поставщики услуг смогут определить, к каким hive должны подключаться их узлы в любой данный момент времени. Это также будет способствовать корректировке спроса. Слишком большое количество узлов не будет поддерживать услуги с недостаточным спросом, и наоборот, слишком малое количество узлов не будет поддерживать услуги с чрезмерно большим спросом.

VI Заключение

В этом документе мы представили подробный обзор новой децентрализованной сетевой инфраструктуры, которая обеспечивает децентрализованные масштабируемые сетевые услуги (DSNS). В рамках этой новой парадигмы клиенты смогут потреблять ad-hoc сетевые услуги, предоставляемые провайдерами услуг, с очень небольшими предварительными знаниями или требованиями к ресурсам. Это будет выполняться с помощью агностического, беспристрастного, автономного и надежного механизма сопоставления положения клиент-провайдера, полностью исключая при этом идентификацию участника. Протокол содержит две новые архитектуры: Ad-Hoc маршрутизацию цепи (AHCR) и крупномасштабную туннелированную сеть (LSTN). Они разработаны таким образом, чтобы была гарантия, что связь и контент, обрабатываемые сетью, будут защищены от цензуры при помощи сквозного шифрования.

Поставщики услуг могут беспрепятственно присоединяться и / или перемещаться между службами или вообще выходить из сети. Поощряется также ведение постоянной записи качества обслуживания для предотвращения ухудшения услуги, используя алгоритмы ранжирования и ценообразования в реальном времени, которые поддерживаются межсетевым консенсусом. Участники, ответственные за безопасность и устойчивость базовой инфраструктуры, регулярно получают компенсацию сетью за свои услуги, используя ее базовый экономический токен, Force Coin

(FOR), тогда как поставщики сетевых услуг конкурируют напрямую за качество услуг и опыт за вознаграждение, выплачиваемое непосредственно конечными пользователями в виде указанного токена.

Традиционные сетевые услуги, по своей сути, находятся в невыгодном положении из-за их централизованного характера; они требуют доверия на многих уровнях, чтобы поддерживать целостность услуги. Например, глобальные инициативы, направленные на подрыв нейтралитета сети для честных участников, набирают обороты и могут быть легко внедрены центральными органами и поставщиками услуг в условиях, когда консенсус сконцентрирован в руках нескольких. Поскольку Force Network опирается на надежный консенсус сети с использованием механизма Proof-of-Stake, попытка нарушить любой аспект его работы становится экономически неосуществимой.

Force Network стремится не только защищать свободу информации от нежелательной цензуры в глобальном масштабе, но и нарушить сложившийся коммерческий ландшафт благодаря своей крепкой и гибкой архитектуре. С очень широкими рыночными приложениями, такими как зашифрованная связь, доставка контента, медиа стриминг, услуги с оплатой за просмотр и услуги по облачным вычислениям и хранению, а также в то время, когда предприятия демонстрируют все возрастающую потребность полностью управляемых услуг, автоматизации задач, аутсорсинга оборудования, быстрого развертывание служб и большого хранилища данных, ландшафт возможностей для Force Network куда более обширен с его недорогим, и с низким требованием обслуживания, и плавным и надежным коммерческим профилем.

Вместе с целым набором интернет-протоколов эта сетевая архитектура проложит путь для нового вида Интернета. Этот документ будет служить справочным материалом для разработок и будет постепенно улучшаться путем устранения потенциальных недостатков и векторов атак и подробного описания реализации более низкого уровня по мере их развертывания.

Особая благодарность

Авторы хотели бы выразить особую благодарность johndis, bumbr, ihackcoinz и pdq за их понимание и вклад в подготовку этой статьи.