SENTINEL

A Blockchain Framework for Building Decentralized VPN Applications

Блокчейн-фреймворк для создания децентрализованных VPN-приложений.

Оглавление

01.
Введение: Видение Стража

Цель экосистемы Sentinel — обеспечить универсальный доступ к Интернету надежным и доказуемым образом. Это будет достигнуто за счет предоставления организациям и частным лицам по всему миру возможности создавать экономически эффективные, масштабируемые, распределенные и децентрализованные сетевые решения на основе блокчейна Sentinel Cosmos, используя следующие преимущества:

01	02	03
Децентрализованный консенсус	Сетевые интеграции с открытым исходным кодом	Распределенная сеть узлов на базе сообщества

Интернет создал форму переплетенного глобального сознания, способного оказывать чрезвычайно положительное воздействие. Однако значимость и мощь возможностей Интернета по распространению информации находятся под угрозой. Наблюдается быстрый рост глобальной интернет-цензуры и массового сбора данных, и с постоянно растущей зависимостью людей от Интернета в настоящее время эта тенденция цензуры и сбора данных нарушает основные права человека на доступ к информации и неприкосновенность частной жизни.

Первоначальная цель экосистемы Sentinel — предоставить основу для построения децентрализованных виртуальных частных сетей или dVPN. VPN-приложения используются людьми по всему миру с целью доступа к контенту с географическим ограничением путем подключения к серверам, расположенным в регионах, где их желаемый контент не ограничен, и в то же время обеспечивает конфиденциальность их взаимодействия посредством установления зашифрованного соединения. . Независимо от того, является ли целью доступ к контенту с ограниченным доступом или повышение безопасности передачи данных через Интернет, люди во всем мире требуют безопасных, дешевых и надежных услуг VPN.

С выпуском Cosmos IBC, обеспечивающего межсетевое взаимодействие, Sentinel сможет выполнять роль поставщика частной сети или уровня dVPN в инфраструктурном стеке Web 3.0. В ближайшем будущем можно будет создать полностью децентрализованное приложение DeFi, которое:

- Размещение в TLD сети рукопожатия
- Данные хранятся в IPFS (Filecoin) • Используются вычислительные ресурсы сети Akash.
- Интегрируется с dVPN, построенными в сети Sentinel, чтобы предоставить как приложению, так и его пользователям конфиденциальность и безопасность на сетевом уровне.

На момент создания технология VPN была в основном ориентирована на создание безопасных туннелей между серверами организации и ее участниками для обеспечения зашифрованной передачи данных. За последнее десятилетие современные потребители начали ассоциировать VPN не только с традиционным нарративом, ориентированным на предприятия, но и с совершенно новым нарративом, связанным с их проблемами, связанными с конфиденциальностью, интернет-безопасностью и глобальным доступом к данным. В результате этих опасений мы наблюдаем расцвет индустрии VPN, которая растет со скоростью 15% в год, при этом прогнозируется, что к 2030 году мировая рыночная капитализация отрасли достигнет 75 миллиардов долларов.

Текущие приложения VPN, доступные потребителям в пространстве VPN, не могут доказать подлинность своих заявлений и сдержать свои обещания пользователю, гарантируя пользователям «конфиденциальность» и «надежность», что создает серьезное противоречие. В последние годы это противоречие выявляется почти ежеквартально, поскольку ведущие VPN-сети постоянно подвергаются риску преднамеренного хранения и сбора пользовательских данных, в то же время допуская серьезные уязвимости в системе безопасности. Индустрия VPN в настоящее время работает как картель, и подавляющее большинство ведущих брендов имеют одних и тех же владельцев. Эти похожие продукты имеют одинаковую степень неизвестности, в то время как потребители не доверяют их внутренней функциональности.

В отличие от этих популярных «клиентских» VPN-приложений, надежная и целостная сеть «dVPN» (термин, первоначально придуманный Sentinel в 2017 году) обладает следующими достоинствами:

1. оказуемое шифрование — доказуемость установления сквозного шифрования между пользователем и сервером, с которого пользователь намеревается получить доступ к данным, посредством систем прозрачности с открытым исходным кодом и проверки целостности приложений.

2. одтверждение пропускной способности — Наличие системы доказуемости пропускной способности, которая позволяет предоставлять пропускную способность поставщиком серверов в обмен на согласованную компенсацию от пользователя ненадежным и доказуемым образом.

3. оказательство отсутствия журналов — возможность предоставить доказательства отсутствия журналов, относящихся к просмотру пользователем или истории данных. централизованно хранятся разработчиками приложений

4. аспределенные узлы выхода — наличие сети «узлов выхода» (серверов dVPN), право собственности на которые распределено между многими участниками, которые не знают личность пользователя.

5. аспределенная ретрансляционная сеть . Наличие надежной ретрансляционной сети с надежным управлением и участием для снижения риска злоумышленников, при этом гарантируя, что узлы выходного узла не будут знать личность пользователя.

Заинтересованные стороны, участвующие в сети Sentinel, включают:

Валидаторы — участники консенсуса в грядущем Sentinel — Cosmos Hub, которые отвечают за безопасность сети и участвуют в управлении экосистемой Sentinel.

Пользователь — конечный пользователь, который хочет получить доступ к сети dVPN, построенной на платформе Sentinel, для безопасного Интернет доказуемым образом

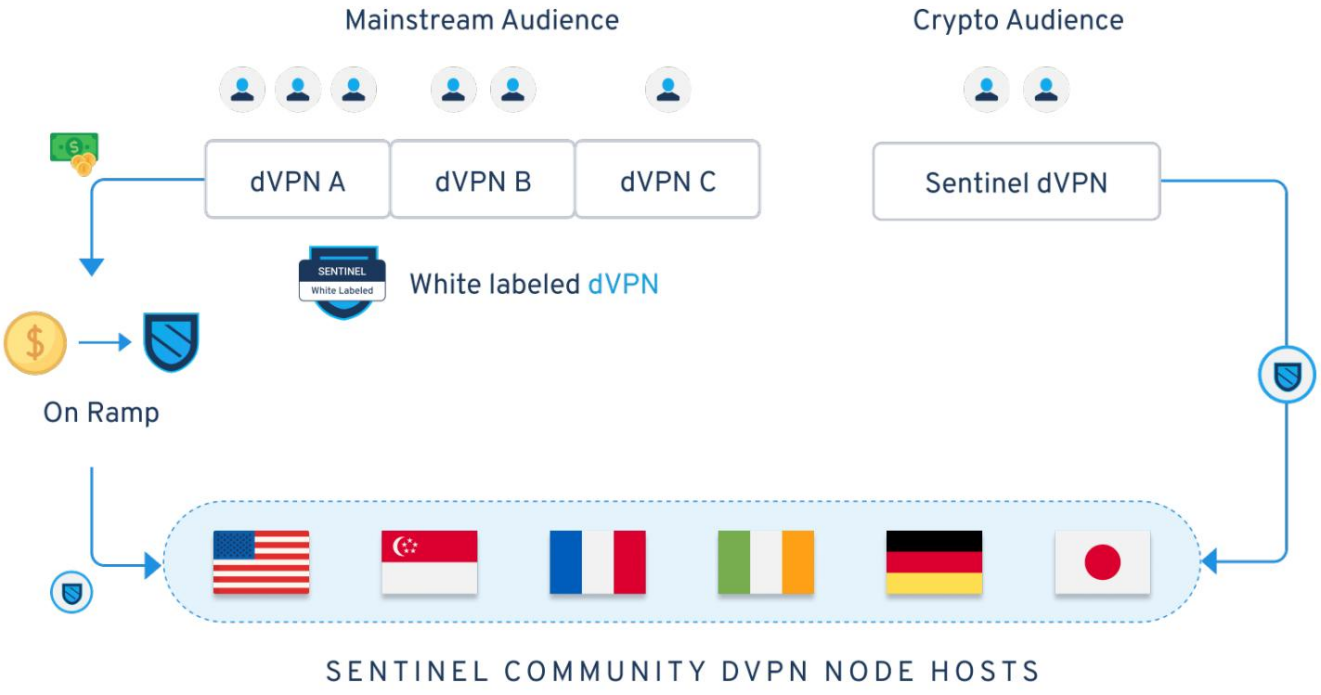
Хосты узла dVPN — члены сообщества, намеревающиеся монетизировать предоставление неиспользуемой полосы пропускания для dVPN, построенных в сети Sentinel, путем размещения выходного узла или узла ретрансляции (соответствующих определенным требуемым пороговым значениям уровня обслуживания).

Создатель приложения dVPN — создатель dVPN, построенный на платформе Sentinel, с использованием зоны Sentinel dVPN в качестве уровня инфраструктуры. Создатель приложения отвечает за привлечение пользователей и маркетинг для получения дохода, чтобы иметь возможность оплачивать хосты узлов dVPN.

02.
Децентрализация индустрии VPN

> Sentinel — это не отдельное приложение dVPN, а сеть независимых приложений dVPN, построенная на базе протокола Sentinel dVPN.

Целью экосистемы Sentinel является децентрализация индустрии VPN и представление dVPN массовому потребителю. Однако эта цель будет достигнута не за счет запуска и поддержки одного приложения, ориентированного на потребителя (Sentinel dVPN), а за счет сначала создания, а затем разработки структуры, которую можно использовать для создания сети независимо управляемых децентрализованных VPN.



dVPN, построенные на платформе Sentinel, могут эксплуатироваться как юридическими лицами, так и отдельными лицами. Sentinel также стремится сотрудничать с существующими поставщиками централизованных VPN, помогая им преобразовать их внутреннюю архитектуру в децентрализованную структуру; позволяя этим компаниям еще больше укрепить доверие со своей существующей клиентской базой, а также позволяя им еще больше расширить свои предложения услуг.

Вы можете задаться вопросом, почему предприниматель или существующая организация хотят работать с Sentinel, создавая dVPN?

Три ключевые проблемы, которые создают барьеры для входа на рынок новых и существующих VPN-компаний, облегчаются экосистемой Sentinel:

1 тоимость и процесс разработки приложений dVPN — сетевые протоколы, такие как OpenVPN и Wireguard, хотя и полностью с открытым исходным кодом, должен быть упакован в масштабируемый и безопасный «кросс-платформенный» набор приложений. Между тем, интеграция систем на основе подписки и платежных шлюзов представляет собой утомительный пример некоторых из более простых реализаций, необходимых при разработке сети dVPN. Требования к ресурсам, необходимые для разработки высококачественного приложения VPN/dVPN с нуля, большинство считают исчерпывающими.

Sentinel предлагает кроссплатформенные клиенты dVPN с открытым исходным кодом, которые отличаются отказоустойчивостью, безопасностью и масштабируемостью. Это связано с тем, что Sentinel использует архитектуру на основе Cosmos, которая предлагает систему «управления учетными записями» с открытым и закрытым ключом в дополнение к запросам узлов в цепочке (подробнее в будущих публикациях). Мы позаботились о том, чтобы построение на основе платформы Sentinel и настройка архитектуры были удобными для разработчиков. Общий процесс будет чрезвычайно конкурентоспособным по стоимости по сравнению с разработкой собственного приложения VPN/dVPN.

2 правление узлами и обработка запросов DMCA. Ведущие поставщики облачных услуг неизбежно ограничат доступ к серверам для хостов выходных узлов из-за потоковой передачи или загрузки пиратского контента с узла, что, несомненно, привлечет запросы DMCA. Централизованным VPN-организациям, как правило, приходится полагаться на «офшорные услуги хостинга», которые могут не обеспечивать такую же степень надежности с точки зрения бесперебойной работы и поддержки клиентов в режиме реального времени, которую предлагают более хорошо зарекомендовавшие себя провайдеры.

Экосистема Sentinel снимает ответственность за управление выходными узлами с организаций, создающих приложения на платформе Sentinel, благодаря интеграции хостов узлов Sentinel, основанных на сообществах.

Владельцы VPN-приложений смогут заключать контракты на обслуживание и устанавливать определенные стандарты качества с узлами в экосистеме Sentinel, при этом им не придется самим управлять владением этими серверами.

3 отенциальные угрозы безопасности и риски, связанные с хакерами — закрытый и централизованный VPN решения не подлежат рецензированию и, следовательно, не могут быть оценены беспристрастными экспертами по безопасности. Это может привести к потенциальным уязвимостям или угрозам безопасности, которые могут нанести ущерб или серьезно подорвать репутацию компании, предоставляющей услугу.

Возникновение уязвимости в системе безопасности не только подвергает пользователей риску из-за возможного использования их данных, но также создает огромное отсутствие доверия к самой организации VPN, что может резко повлиять на доход и устойчивость организации.

Эта структура с открытым исходным кодом, предоставляемая Sentinel, значительно снижает вероятность возникновения уязвимости системы безопасности. Примером сильных сторон программного обеспечения с открытым исходным кодом могут быть военные организации мира, использующие Linux в качестве предпочтительной операционной системы в большинстве своих систем. Linux имеет полностью открытый исходный код и постоянно проверяется третьими сторонами; в отличие от программного пакета, такого как Windows, который имеет закрытый исходный код и печально известен своими проблемами безопасности.

В то время как платформа Sentinel предлагает инструменты, а также инфраструктуру для создания и эксплуатации надежного сервиса dVPN, владелец приложения несет ответственность за привлечение клиентов и понимание их конкретного целевого рынка для развертывания эффективных маркетинговых стратегий. Важно отметить, что разработка и реализация продукта — это только часть уравнения. Другая часть связана с фактической адаптацией пользователей и созданием продукта, пользующегося спросом на рынке.

4 ключевых принципа успеха эффективного приложения DVPN включают в себя:

1 ильный пользовательский интерфейс/UX . Приложения, построенные на платформе Sentinel, должны быть неотличимы от ведущих VPN-сервисов, уже предоставляемых в отрасли, с точки зрения уровня удобства для пользователя и простоты доступа. Пользователи могут не захотеть переходить на более децентрализованное решение, если процесс их адаптации не будет плавным, даже с учетом растущей тенденции спроса на безопасные и прозрачные VPN-сервисы. Кривая обучения использованию приложения dVPN должна быть сведена к минимуму за счет использования интеллектуального дизайна. Необходимо уделять особое внимание эстетике приложения, чтобы продемонстрировать сильный имидж бренда.

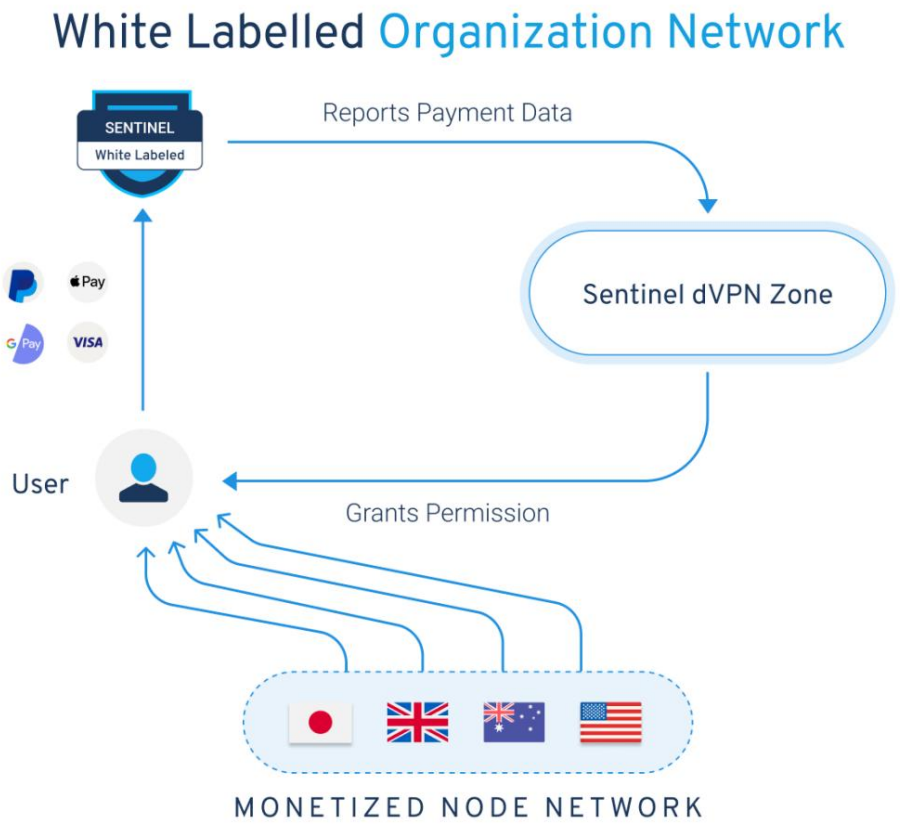
2 тратегия эффективного ценообразования . Внедрение модели ценообразования, которая не только экономически эффективна, но и Прибыльность играет решающую роль при попытке создать успешное приложение dVPN. Для приложений важно иметь возможность генерировать доход, который затем передается узлам. Это позволяет им монетизировать предоставление ресурсов полосы пропускания; создание здоровой и устойчивой децентрализованной экономики. Используемая модель ценообразования полностью зависит от целевой демографической группы и типа услуг, предлагаемых приложением. В будущем создатели приложений dVPN в рамках экосистемы Sentinel смогут предлагать расширенные услуги в своих приложениях. Эти расширенные услуги включают в себя

предстоящая сеть ретрансляции наряду с другими усовершенствованными реализациями, связанными с конфиденциальностью. Дополнительные услуги могут быть включены в существующие подписки пользователей или могут быть монетизированы в зависимости от точного объема потребляемых данных. Независимо от стратегии ценообразования или модели получения дохода, используемой владельцем/оператором DVPN, создатель приложения обязан провести надлежащую проверку и анализ, чтобы прийти к наилучшей модели ценообразования.

3 нтеграция основных платежных шлюзов . Крайне важно, чтобы приложения, построенные на платформе Sentinel, предлагали пользователям возможность совершать покупки с помощью таких способов оплаты, основанных на фиатных деньгах, как:

Виза/Мастеркард | Apple Pay | Google Play магазин | Электронные кошельки (например, Paypal, Skrill и т. д.)

Наличие только варианта оплаты, связанного с криптовалютой, создало бы огромный барьер для входа; предотвращение простого перехода среднего потребителя от централизованного поставщика услуг VPN. В то время как узлы, размещенные в экосистеме Sentinel, должны оплачиваться с помощью цифровых активов на основе блокчейна, владельцы приложений DVPN имеют возможность монетизировать свои приложения с помощью каналов оплаты фиатных денег. Собранные фиатные валюты затем могут использовать услугу «на рампе» для конвертации фиатной валюты в цифровой актив, который затем используется для оплаты хостов узлов.



4 азнообразие протоколов маршрутизации. В разных географических регионах требуются определенные протоколы маршрутизации для беспрепятственного доступа к данным из Интернета без вмешательства потенциальных препятствий. Необходимо полностью понимать тонкости и особенности различных географических регионов для правильного развертывания оптимальных протоколов маршрутизации, ориентированных на пользователя, в приложении DVPN. Сетевая конфигурация, которая безупречно работает в одном регионе, может быть полностью избыточной в другом, что требует индивидуального подхода при выборе подходящих протоколов маршрутизации для приложения DVPN. Например, протокол OpenVPN не может обойти брандмауэры нескольких разных стран, в то время как он беспрепятственно работает в других странах.

03.
Обзор архитектуры блокчейна Sentinel Cosmos

Cosmos: будущее децентрализованных криптовалютных экосистем

Решения по функциональной совместимости, которые облегчают обмен активами и данными между различными децентрализованными сетями, основанными на криптовалюте, могут уменьшить трайбализм в отрасли. В этом контексте «трайбализм» относится к агрессивной тенденции, которую демонстрируют децентрализованные сети, пытаясь установить или продемонстрировать свое превосходство над своими аналогами.

Факты таковы, что некоторые сети предлагают уникальные услуги, обеспечиваемые их индивидуальной архитектурой и уникальным направлением развития. Функциональная совместимость позволяет участникам экосистемы одновременно использовать преимущества каждой из этих сетей без необходимости проводить сравнение, что обеспечивает горизонтальную масштабируемость/специализацию.

Cosmos стремится уменьшить этот «трайбализм» в экосистеме, соединяя эти конкурирующие цепи вместе, эффективно уменьшая серьезное разобщающее влияние, которое обычно разделяет их. Модуль Cosmos IBC позволит этим сетевым приложениям расширить свою общую демографическую целевую аудиторию за счет обслуживания гораздо более широкой пользовательской базы, помогая облегчить привлечение новых клиентов, позволяя им принимать динамические межсетевые платежи.

В настоящее время наиболее значимые инициативы по обеспечению совместимости между Cosmos и другими очень ценными и уважаемыми сетями включают интероперабельные «мосты», строящиеся между Cosmos и ZCash, и Polkadot.

Экосистема Cosmos позволяет Sentinel создавать и управлять своей собственной сетью на уровне «концентратора». В то время как приложения dVPN, созданные в сети Sentinel, находятся либо в общих зонах, либо в собственных собственных зонах, в зависимости от требований к пропускной способности каждого отдельного приложения.

Цепи, построенные с использованием Cosmos, могут поддерживать автономию, связанную с управлением, а также обеспечивать взаимодействие между другими концентраторами и зонами в сети Cosmos.
В отличие от модели токенов ERC20, сети, построенные на Cosmos, не должны будут платить комиссию собственным токеном Cosmos «ATOM», вместо этого они могут платить собственным токеном сети.

Структура концентратора и зоны

Sentinel использует архитектуру Cosmos Hub/Zone для повышения масштабируемости, связанной с dVPN dApp, за счет обмена всеми специфическими транзакциями и данными приложения в «зоне Sentinel dVPN» (или боковой цепи), при этом абстрагируя транзакции и управление, связанные с токенами, в «Sentinel Hub». (или основная цепь). Зоны будут связываться с основной цепочкой (хабом) Sentinel через межблочную коммуникацию Cosmos (IBC).
Протокол. Зону можно условно сравнить с типом «канала состояния», который развертывается для эффективного масштабирования.

Зона приложения dVPN будет иметь собственное управление консенсусом, которое, скорее всего, будет подмножеством участников валидатора консенсуса Hub. Несмотря на то, что на уровне зоны не будет обмениваться денежными средствами, стимулирование и дестимулирование валидаторов будет происходить на уровне Sentinel Hub.

Используя IBC, концентратор Sentinel Network взаимодействует с концентратором Cosmos и другими концентраторами как часть сети Cosmos. Это не только позволит службам в сети Sentinel взаимодействовать друг с другом и принимать либо собственный токен SENT, либо другие токены из белого списка, но также поможет им подключаться к другим сетям в сети Cosmos.

Блокчейн Sentinel — Tendermint может размещать dApps и/или сервисы, которые работают в своих собственных независимых зонах, имея специальное управление, построенное на основе консенсуса Tendermint, что позволяет их собственному набору валидаторов проверять транзакции.

пропускная способность

Tendermint использует систему консенсуса bPOS, в которой блокчейны могут устанавливать конечное количество валидаторов для достижения более быстрого консенсуса, в то же время защищая сеть от «византийских атак».

В сети Sentinel будут построены различные решения для P2P-коммуникаций и обеспечения конфиденциальности, основанные на моделях получения дохода на основе микротранзакций в больших объемах. Это делает блокчейн Tendermint идеальным для поддержки сети Sentinel благодаря способности достигать высокого TPS (транзакций в секунду), особенно по сравнению со значительно более низкими «15 транзакциями в секунду» Ethereum.

Количество транзакций в секунду (TPS) для блокчейнов, использующих консенсус Proof-of-Work (POW), было относительно

медленный, и многие решения масштабирования для таких согласованных сетей требуют больших капиталовложений в специализированное оборудование.

Cosmos использует уникальный связанный консенсус Proof-of-Stake, при котором голоса от фиксированного числа валидаторов с определенной степенью энтропии принимаются сетью в указанный момент времени. Это увеличивает общую пропускную способность транзакций в сети из-за конечного числа валидаторов, обрабатывающих транзакции.

Консенсусная система Tendermint BFT позволяет сети Sentinel достигать более высоких скоростей транзакций, чем любая существующая в настоящее время сеть PoW; Сети PoW обременены отсутствием определенной завершенности. В системах на основе bPOS, таких как Tendermint, почти мгновенная окончательность достигается за счет использования системы голосования на основе кругового перебора с использованием конечного числа валидаторов, позволяя держателям токенов «привязывать» токены к валидаторам, которые считаются заслуживающими доверия.

Интероперабельный

Характер функциональной совместимости протокола Cosmos IBC позволяет создавать зону привязки (обеспеченную стабильной монетой). Эта функция может быть разработана для сетей, не входящих в экосистему Tendermint или Cosmos.
Полезность этих зон будет в первую очередь для межсетевых платежей. С помощью этой технологии узлы, размещенные в сообществе, работающие в сети Sentinel dVPN, могут принимать криптовалюты, такие как Ethereum, BTC, PIVX, DASH, NEO, Dfinity, Cardano и т. д., в обмен на пропускную способность.

Любая криптовалюта может быть интегрирована, независимо от того, построена ли она на Cosmos SDK. Это стало возможным благодаря использованию «мостов», которые требуют установления интероперабельного соединения между двумя сетями.
Sentinel Hub будет подключен к Cosmos IBC, что позволит пользователям DVPN совершать платежи в разных валютах или стейблкоинах, поддерживаемых Cosmos IBC.

В связи с тем, что протокол IBC можно эффективно использовать для связи между различными сетями, которые имеют разные механизмы консенсуса и структурные схемы (например, ZCash/Cosmos), Sentinel считает, что протокол IBC чрезвычайно эффективен для масштабируемости транзакций и эффективности, связанной с dAPP, благодаря введение модели Hub/Zone.

Технология, предоставляемая Cosmos Network и Tendermint, позволяет нам представить себе настоящую свободную рыночную экономику, основанную на «безупречной межсетевой платежной интеграции», которая до сих пор была невозможна ни с одной другой платформой/сетью. Это первый шаг на долгом пути создания блокчейн-приложений, которые будут приняты в реальном мире.

Управление

В основной сети Sentinel на основе Cosmos управление сетью будет в руках валидаторов. Эти валидаторы будут демократически определены в основной сети Sentinel на базе Cosmos посредством делегирования токенов держателями. «Сила голоса» или вес валидаторов определяется не только историческими показателями, но и количеством токенов, делегированных им сторонниками Sentinel.

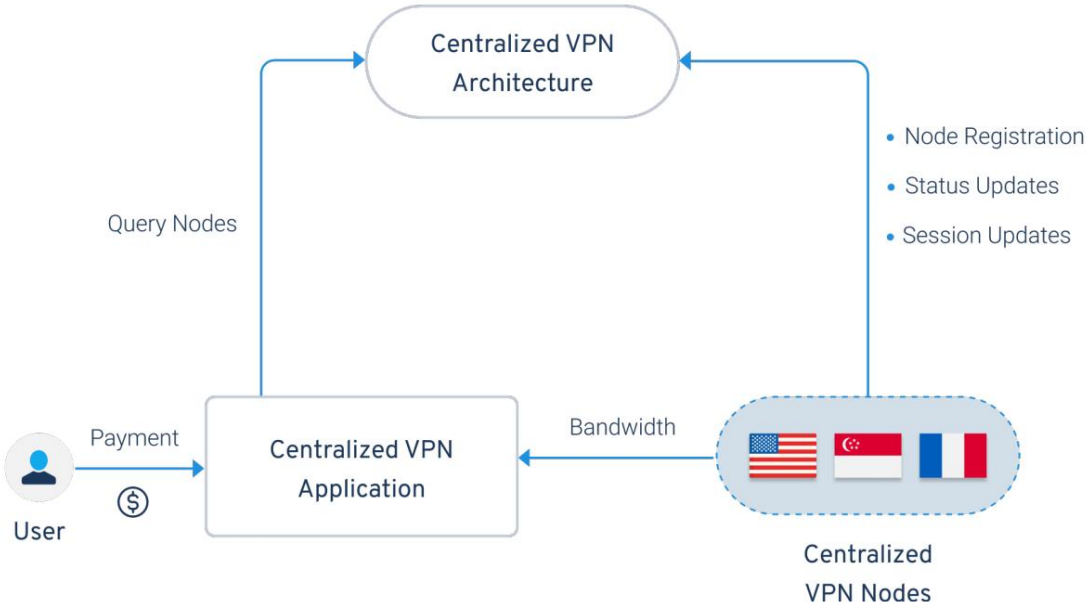
Предложения по управлению сетью обрабатываются набором демократичных валидаторов, что позволяет обойти требование разветвления на «новую цепочку». Эти предложения могут включать:

- Принятие новых валидаторов или отклонение существующих вредоносных валидаторов.
- Принятие новых зон и мостов или отказ от существующих
- Изменения в поставке или блокировка вредоносной/взломанной учетной записи.

04.
Обзор архитектуры Sentinel dVPN

Централизованная архитектура VPN состоит из нескольких промежуточных серверов, которые необходимы для управления разрешениями пользователя, а также для установления подключения пользователя к узлу VPN. Эта централизованная архитектура требует высокой степени зависимости от этих промежуточных серверов, которые представляют риск для отказоустойчивости сети из-за множества точек отказа, а также множества точек атаки. Время простоя централизованных сетей VPN может быть связано с неправильным функционированием одного или нескольких из этих компонентов и может привести к снижению качества обслуживания и удовлетворенности пользователей.

Платформа Sentinel dVPN обеспечивает невероятную степень отказоустойчивости и безопасности по сравнению с любой VPN потребительского уровня. Архитектура Sentinels сводит к минимуму количество промежуточных серверов и зависимостей. Помимо системы управления и создания учетных записей, которая происходит полностью в сети, процесс запроса доступных серверов происходит в сети. Поскольку блокчейн, на котором размещено приложение, будет работать 24 часа в сутки, 7 дней в неделю, без сбоев, поскольку инфраструктура сообщества валидаторов глобально децентрализована (на нее не влияют перебои в работе 1, 2 или 3 центров обработки данных), такое приложение будет намного превосходить предложения централизованных соревнований.



Основным фактором устойчивости архитектуры Sentinel является децентрализованное распределение вычислительной мощности, которая потребуется для работы Sentinel Hub и Sentinel Zone. Вычислительная мощность, необходимая для функционирования экосистемы Sentinel dVPN, не предоставляется и не зависит от какой-либо централизованной организации. Вместо этого она предоставляется экспертными организациями по «проверке», распределенными по всему миру и имеющими системы с высокой степенью резервирования со значительной пропускной способностью и временем безотказной работы.

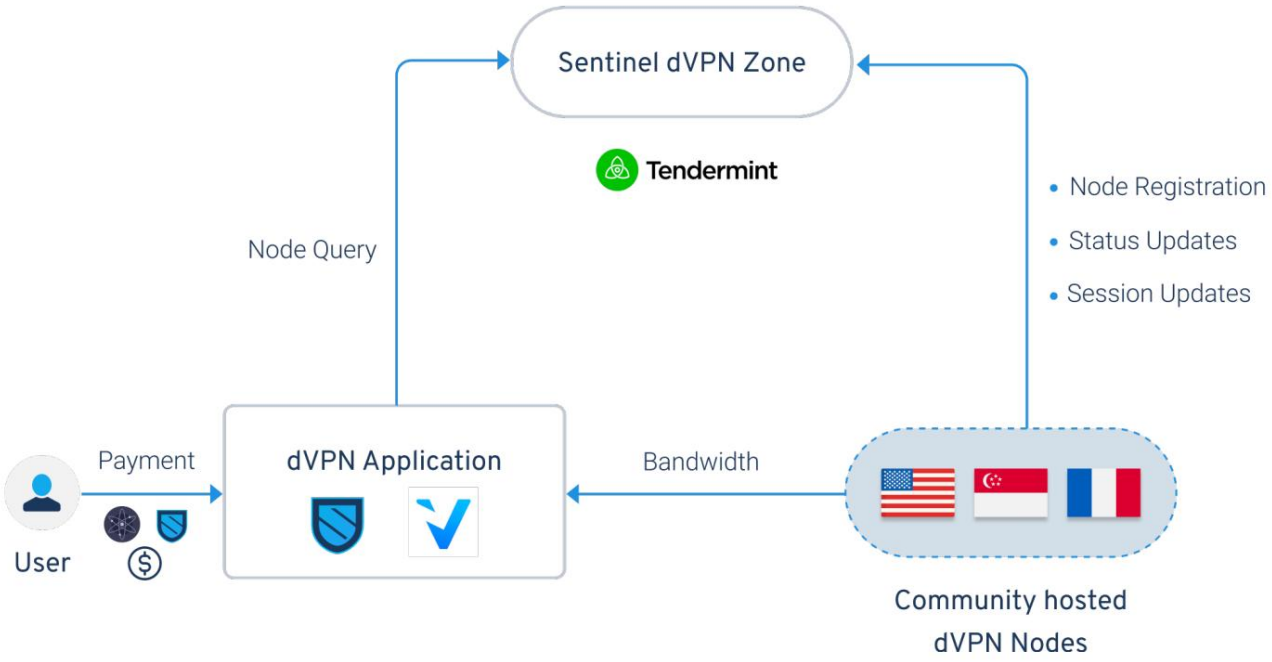
В то время как архитектура Sentinel гарантирует, что анонимность пользователя не будет скомпрометирована самим приложением, использование будущей сети ретрансляции Sentinel необходимо для обеспечения полной анонимности пользователя с точки зрения выходного узла. Сеть ретрансляции Sentinel позволит пользователям туннелировать свое соединение через ряд «узлов ретрансляции», которые гарантируют, что пользователь не взаимодействует напрямую с выходным узлом.

Собственный собственный протокол Sentinel «доказательство полосы пропускания» обеспечивает надежное и прозрачное измерение предоставления полосы пропускания от поставщика услуг (узлы сообщества) до конечного пользователя. Протокол «доказуемости пропускной способности» интегрируется с блокчейном Sentinel, обеспечивая четкую историю качества предоставляемой услуги пропускной способности и устанавливает уровень доверия между всеми вовлеченными участниками. Эти данные позже используются для определения того, соответствует ли узел требуемому соглашению об уровне обслуживания, чтобы избежать штрафных санкций.

Запрос в цепочке

Реализация Sentinel системы запросов «по цепочке» является одним из наиболее важных технических достижений Sentinel и обеспечивает высокую отказоустойчивость и децентрализованную архитектуру.

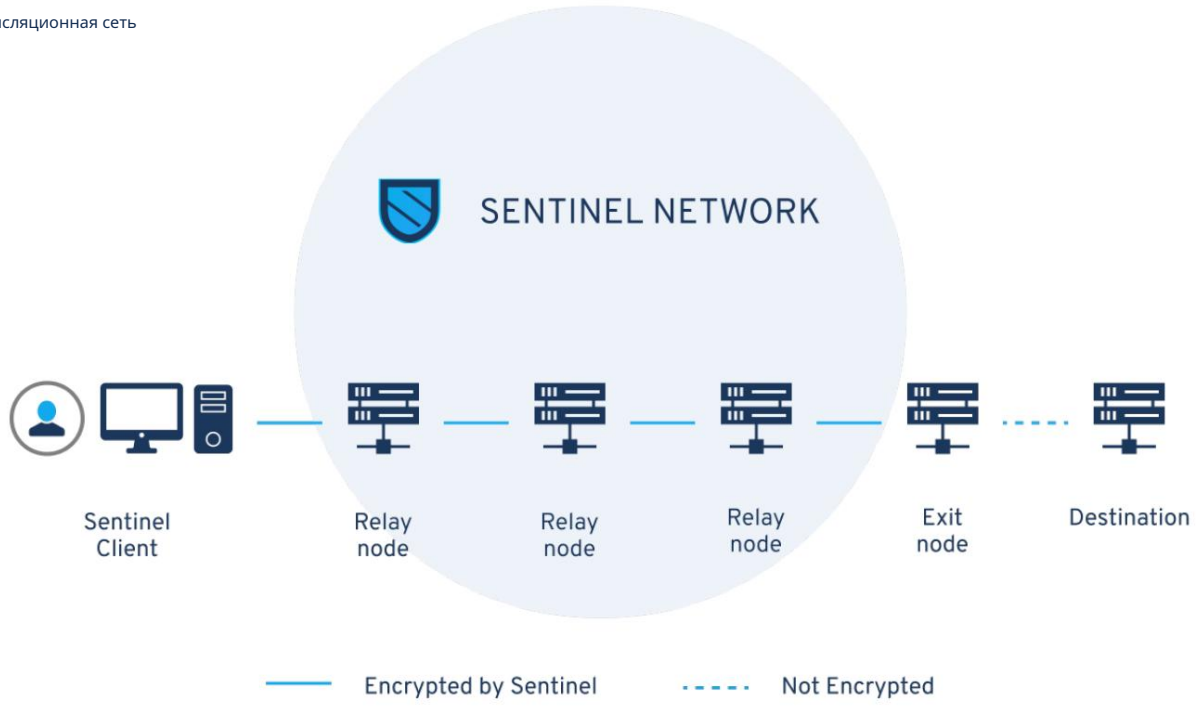
Благодаря архитектуре Sentinel dVPN соединение между пользователем и выходным узлом может быть установлено напрямую без необходимости подключения к промежуточному серверу (например, мастерноде для обнаружения узлов), которым может управлять разработчик приложения или третья сторона. Это достигается за счет использования блокчейна в качестве регистра для «запросов узлов», при этом узлы имеют возможность взаимодействовать и хранить информацию, относящуюся к свойствам узла и инструкциям по подключению. Пользовательское приложение dVPN на основе Sentinel будет просто запрашивать все доступные узлы dVPN, считывая данные транзакций в выделенной зоне dVPN Sentinel, заполняя список доступных серверов. Поскольку аутентификация и управление идентификацией уже происходят в цепочке, теоретически единственной точкой отказа структуры Sentinel dVPN dApp (кроме сетевой атаки Сивиллы) становится потенциальный сбой безопасности консенсуса на уровне цепочки. Единственный способ скомпрометировать приложение Sentinel dVPN — это скомпрометировать консенсус, основанный на валидаторе.



Основные приложения VPN обычно контролируют выходной узел, а также контролируют и используют промежуточные серверы запросов, которые существуют между выходным узлом и пользователем, что делает назначение сети ретрансляции избыточным, поскольку IP-адрес исходного пользователя легко увидеть.

Однако архитектура «запроса в цепочке» означает, что пользователю нужно напрямую общаться только с цепочкой, а не с какими-либо другими потенциально централизованными серверами, которые могут регистрировать их взаимодействия.

Ретрансляционная сеть



Надежная сеть ретрансляции является важным аспектом любого сквозного решения dVPN, которое полностью поддерживает право пользователя на конфиденциальность. Хотя ни создатель приложения dVPN, построенного на Sentinel, ни кто-либо из участников блокчейна Sentinel не имеет доступа к какой-либо личной информации, относящейся к пользователям (например, IP-адресу), выходной узел, размещенный в экосистеме Sentinel, будет иметь доступ к IP-адрес пользователя при отсутствии ретрансляционной сети. Хотя приложение DVPN может предоставить доказательства того, что никакие журналы, связанные с просмотром пользователей, и метаданные не собираются/хранятся централизованно разработчиками приложения, в настоящее время невозможно доказать, что журналы не собираются или не хранятся хостом выходного узла. на их локальном устройстве.

Проводя аналогию для описания ретрансляционной сети в более простых терминах, соединение между пользователем и выходным узлом можно сравнить с пользователем, совершающим сотовый вызов третьей стороне. Если намерение пользователя состоит в том, чтобы третья сторона не могла видеть номер пользователя в идентификаторе вызывающего абонента, пользователю вместо этого придется использовать устройство своего друга в качестве ретранслятора для маскировки номера телефона пользователя. Затем пользователь должен будет позвонить другу, который поставит пользователя на удержание и позвонит на сторонний номер, прежде чем объединить оба телефонных звонка и тем самым соединить пользователя с третьим абонентом. сторона без раскрытия данных пользователя.

Как и в примере с промежуточным сотовым абонентом, сеть ретрансляции состоит из «узлов ретрансляции». Узлы ретрансляции отличаются от узлов выхода в работе, поскольку узлы выхода напрямую общаются с пользователями (при отсутствии сети ретрансляции), а также взаимодействуют с веб-серверами в Интернете. В то время как узлы ретрансляции взаимодействуют только с пользователем, другими узлами ретрансляции или выходным узлом.

Сильная ретрансляционная сеть состоит из:

- Большое количество участников
- Сильное управление •

Интеграция с несколькими сетями

Использование системы ретрансляции, построенной на Sentinel, будет в первую очередь предназначено для пользователей, более заботящихся о конфиденциальности, которые готовы пожертвовать скоростью Интернета для повышения конфиденциальности.

Преимущества ретрансляционной сети реализуются только тогда, когда большое количество уникальных участников начинает размещать ретрансляционные или выходные узлы в сети. Если в какой-либо момент организация берет на себя управление значительной долей сети, она может деанонимизировать пользователя с помощью простого, но эффективного «Человека посередине» (MITM). Атака. Одной из основных целей ретрансляционной сети является обеспечение того, чтобы узлы ретрансляции не могли определить, туннелируют ли они к пользователю или к другому узлу ретрансляции. Если пользователь направит свой трафик как через узлы ретрансляции злоумышленника, так и через выходной узел, злоумышленник сможет сопоставить IP-адрес пользователя и, в свою очередь, определить, что пользователь инициирует запрос на трафик, а не просто другой. участник эстафеты.

Важность наличия распределенной сети для предотвращения атаки MITM в сети ретрансляции разделяет экосистема Биткойн, где целью майнинга является предотвращение атаки 51%. Если одна организация возьмет под свой контроль 51% общего хэшрейта майнинга сети Биткойн, эта организация сможет нанести ущерб сети.

целостности путем проведения атаки с двойной тратой. Биткойн пытается бороться с этими рисками монополизации в экосистеме майнинга с помощью своего механизма стимулирования. Этот механизм поощрения предоставляет майнерам вознаграждение в зависимости от их участия в поиске и проверке новых блоков в сети. Если бы Биткойн был добровольческой сетью без экономического дизайна, его безопасность, скорее всего, была бы скомпрометирована. Мощная организация, имеющая доступ к значительной аппаратной инфраструктуре, может легко взять на себя контроль над майнинговой сетью. Примером сети, управляемой добровольцами, является сеть TOR. В сети TOR ретрансляционные и выходные узлы не поощряются за их участие. Вместо этого их поощряют предоставлять свои услуги просто из общего уважения к духу децентрализации. Отраслевые эксперты обеспокоены тем, что сеть TOR была скомпрометирована организациями, которые контролируют значительное количество релейных и выходных узлов TOR. На данный момент в сети насчитывается около 6000 узлов ретрансляции TOR со средним числом активных пользователей 6 миллионов в день. Это ясно показывает ограничения и/или риски сети, основанной на волонтерах.

Успех ретрансляционной сети Sentinel полностью зависит от количества уникальных участников. Привлечение этих участников требует определенного уровня стимулирования через механизмы в сети.

Доказательство пропускной способности

Распределение пропускной способности в действительно децентрализованной сети имеет общую проблему с генерацией хэшей майнерами в сети Proof of Work (PoW). Эта проблема связана со способностью поставщика услуг (или майнера в случае PoW) неправомерно присваивать или фальсифицировать фактический объем выполненной работы. Одной из ключевых обязанностей майнеров в блокчейне Биткойн является подтверждение реальной работы (или количества сгенерированных хэшей) другими майнерами и обеспечение того, чтобы никто не использовал систему, чтобы заблокировать вознаграждение. Аналогичным образом, существует потребность в надежной архитектуре в случае распределения полосы пропускания в децентрализованной P2P-сети, чтобы предотвратить злоумышленника, который намеревается «подделать» объем предоставленной полосы пропускания.

Аналогия, которую можно провести, чтобы продемонстрировать требование доказуемости решений для сетей распределения полосы пропускания, - это разочаровывающий опыт, который многие пользователи мобильных телефонов заявляют со своим сетевым оператором в отношении их платы за международный роуминг. Большинство планов роуминга, предлагаемых сетевыми операторами, имеют ограничение на объем пропускной способности, которая может быть использована, или иногда даже выставляется счет с точки зрения совокупного объема пропускной способности, потребляемой пользователем. Нередко можно услышать отчеты от людей, которые полностью не доверяют своим операторам после опыта, когда они считают, что с них была завышена плата, и не понимают, как было рассчитано потребление полосы пропускания для счета за роуминг.

Доказуемость распределения пропускной способности важна не только для сценариев использования, ориентированных на работу с сетью, но также имеет первостепенное значение для сценариев использования, связанных с хранением и вычислениями, которые также предполагают огромное использование полосы пропускания. Одной из ключевых целей экосистемы Sentinel является разработка и внедрение первого протокола проверки пропускной способности, или «Proof of Bandwidth», чтобы обеспечить ненадежное совместное использование пропускной способности. То

Объем этого протокола выходит за рамки децентрализованных приложений VPN, построенных на Sentinel, имеет возможность интеграции с другими распределенными сетями совместного использования ресурсов p2p и даже с основными приложениями.

Первая реализация прототипа протокола Sentinel Proof of Bandwidth произошла в цепочке Ethereum при поддержке внешней сети распределенных мастернод. Эти мастерноды будут наблюдать и измерять распределение пропускной способности между поставщиком услуг и пользователем, а затем записывать определенные свойства сеанса, такие как продолжительность и потребляемая пропускная способность, в блокчейн Ethereum. Затем механизм выставления счетов приложения dVPN будет извлекать эти данные для создания счета, который должен быть оплачен пользователем. Этот прототип архитектуры функционировал, как и планировалось, однако его нельзя было назвать действительно децентрализованным из-за потребности в дополнительной сети мастернод.

Текущая реализация протокола доказуемости пропускной способности, которая разрабатывается в сети Sentinel Cosmos/ Tendermint, включает генерацию «подписей пропускной способности» как от поставщика услуг, так и от пользователя. Эти сигнатуры пропускной способности представляют собой, по сути, сообщения, состоящие из пропускной способности, передаваемой в P2P-соединении в течение предварительно настроенного периода времени. Поставщик услуг и пользователь генерируют свои собственные подписи, каждая из которых подписывается своим соответствующим закрытым ключом, и эти подписи затем сохраняются в цепочке для проверки происхождения. В случае расхождения между заявками на обмен пропускной способностью от пользователя и поставщика услуг (в течение предварительно настроенного периода времени) соединение будет разорвано из-за присутствия в обмене как минимум 1 злоумышленника.

Переменные подписи полосы пропускания, определенные разработчиком приложения dVPN:

- Период времени для создания каждой подписи полосы пропускания.
- Процентный порог несоответствия между подписями пользователя и поставщика услуг.

Пример: протокол Sentinel «Proof of Bandwidth» интегрирован с dVPN «XYZ», построенным на платформе Sentinel. Период времени для генерации подписи установлен в 10 минут, а порог несоответствия установлен в 10%. В первые 10 минут использования dVPN поставщик услуг вводит внутрисетевую подпись, соответствующую 1,05 ГБ предоставленной полосы пропускания, а пользователь вводит подпись, представляющую 1 ГБ потребляемой полосы пропускания. Расхождение между обеими подписями находится в пределах порогового значения 10%, что позволяет установленному соединению продолжаться без прерывания.

В следующем сеансе подпись поставщика услуг представляет собой предоставленные 2 ГБ, в то время как подпись пользователя представляет собой 1,5 ГБ, израсходованные с основным расхождением между двумя подписями, превышающим пороговое значение, что приводит к разрыву соединения.

Модели оплаты и условного депонирования:

Монетизация одноранговой системы распределения пропускной способности позволяет использовать более динамичные модели оплаты, чем обычно используется в традиционной индустрии VPN. В дополнение к общей «предоплаченной» системе, когда пользователь приобретает подписку на фиксированный период времени, поставщики пропускной способности (узлы) также имеют возможность устанавливать свои собственные цены за единицу (ГБ) потребляемой пропускной способности.

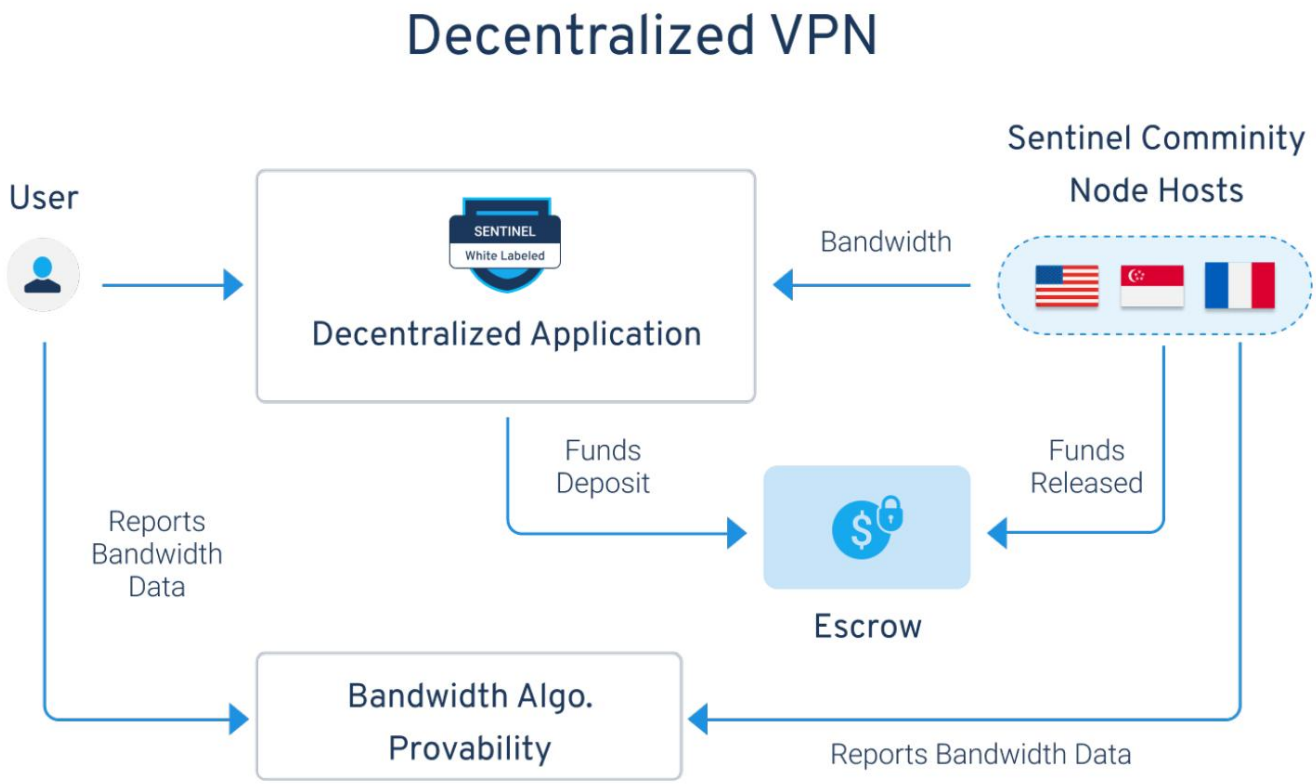
Плата за использование dVPN, работающих в экосистеме Sentinel, будет возможна как с помощью традиционных вариантов на основе фиата (например, кредитной карты), так и с помощью большого количества криптовалют, которые будут поддерживаться Cosmos IBC. Тем не менее, стоимость полосы пропускания по любой из моделей будет в основном деноминирована в фиатных деньгах.

Важно отметить, что, хотя оплата пропускной способности может производиться с помощью криптовалюты или фиата, платеж, который поставщик пропускной способности (узлы узла) будет производить за инфраструктуру для размещения узла, почти всегда будет деноминирован в фиате. Эти затраты, связанные с инфраструктурой, включают затраты на облачные вычисления, а также затраты на электроэнергию, стоимость оборудования, если хост-узел использует самостоятельную физическую установку.

В экосистеме Sentinel пользователям dVPN доступны две основные формы оплаты:

В режиме реального времени — модель оплаты в режиме реального времени используется хостами узлов dVPN на Sentinel, которые намереваются позволить пользователям платить за каждый «ГБ» потребленной полосы пропускания. В этой модели оплаты узлы узлов также имеют возможность устанавливать собственную цену за свои услуги.
Pre-Paid — модель с предоплатой — это более традиционная модель оплаты, похожая на ту, что обычно наблюдается в основной индустрии VPN, где пользователи приобретают доступ на определенный период времени. В модели с предоплатой нет ограничений на потребление полосы пропускания, и использование, как правило, не ограничено.

Система условного депонирования Sentinel dVPN. Система условного депонирования используется в модели оплаты в режиме реального времени между пользователем и поставщиком услуг, чтобы гарантировать, что ни одна из вовлеченных сторон не сможет мошенническим образом повлиять на транзакцию. Пользователь должен заблокировать определенное количество токенов на условном депонировании, прежде чем сможет установить соединение, и токены периодически вычитаются из этой заблокированной суммы в соответствии с пропускной способностью, потребляемой пользователем. Точное измерение пропускной способности, предоставляемой пользователю, происходит с помощью протокола Sentinel «Proof of Bandwidth», который связывается с депонированием, чтобы установить полностью децентрализованный подход к выпуску токенов из условного депонирования.



05.
Токен Утилита

Основная полезность токена Sentinel вращается вокруг его функций как:

• Токен управления и ставок • Средство платежа для подписок dVPN • Средство платежа для расширенных услуг dVPN • Рабочий токен

Токен управления и стейкинга:

- Токен Sentinel необходим для безопасности сети, поскольку он Хаб на основе космоса. Токен Sentinel будет использоваться для участия в принятии решений, связанных с управлением, в качестве формы «права голоса», где величина права голоса пользователя напрямую связана с количеством токенов, которыми он владеет.
- Пользователи могут получать вознаграждение в обмен на «делегирование» своего токена Sentinel валидатору и нахождение в стороне от управление.
- Пользователи могут размещать валидаторы и получать комиссионные от токенов, делегированных их валидаторам. Это возможно либо путем подачи заявки на делегирование, либо путем накопления достаточного количества токенов, чтобы считаться подходящим для активного набора валидаторов.

Концентратор Sentinel построен на основе Cosmos SDK и использует тот же протокол и структуру управления на основе dPOS, что и Cosmos Hub. Максимальное количество валидаторов при генезисе будет установлено на уровне 50. Не будет минимального требования для самостоятельного делегирования от валидаторов в хабе Sentinel.

Хотя от валидаторов не требуется минимальная сумма «самопривязки», валидаторы будут иметь право войти в активный набор валидаторов только в том случае, если у них есть больше токенов, делегированных их собственному валидатору (либо от них самих, либо от внешних держателей), чем у валидатора с наименьшее количество общего делегирования в активном наборе (последний валидатор, например, 50 -й валидатор). Этот критерий, определяющий право валидатора, также применяется по умолчанию в Cosmos и других сетях на основе Cosmos.

Владельцы токенов могут получать вознаграждение, защищая сеть.

Hub установлен на уровне 5%, чтобы обеспечить честное участие и отсутствие немедленной максимальной ставки комиссии.

Заинтересованные стороны токена Sentinel также будут иметь возможность создавать предложения по управлению или голосовать за предложения, выпущенные другими членами сообщества. Эти предложения по управлению обеспечивают возможность редактирования различных элементов или переменных цепочки без необходимости «хардфорка» или ручного отключения цепи на основе технического обслуживания.

Средство оплаты для подписок dVPN:

- Токен Sentinel можно использовать для оплаты подписки dVPN, однако оплата этих подписок не ограничивается токеном Sentinel

Подписка на услугу dVPN будет аналогична системе подписки для значительного большинства популярных реальных услуг VPN. Довольно редко можно увидеть биллинг на основе измерения пропускной способности в традиционной индустрии VPN, а службы VPN, которые предлагают измерение, обычно предлагают расширенные услуги безопасности и более эзотерические протоколы маршрутизации. Подписка на услуги dVPN, построенные на платформе Sentinel dVPN, потребует предоплаты за неограниченное использование dVPN через 1 или более устройств.

Токен Sentinel будет предложен в качестве опции для оплаты подписки. Однако пользователи не будут ограничены только токеном Sentinel, поскольку приложения dVPN, построенные на платформе Sentinel, будут иметь возможность добавлять реальные платежные шлюзы на основе фиата или платежные шлюзы, поддерживающие другие типы децентрализованных валют.

Благодаря функциональной совместимости платежей dVPN, построенные на Sentinel, смогут охватить более широкую аудиторию, способствуя транзакциям на основном рынке (например, Google Pay, Apple Pay). Если бы оплата подписки была ограничена токеном Sentinel, процесс привлечения клиентов было бы непросто масштабировать, а целевой рынок был бы очень ограниченным.

Средство оплаты расширенных услуг dVPN:

- Расширенные услуги потребуют от пользователей размещения токенов в системе условного депонирования, которая будет использоваться для оплаты в режиме реального времени и будет регулироваться протоколом проверки пропускной способности Sentinel. Эта структура является неотъемлемой частью экосистемы Sentinel Hub, поэтому транзакции будут ограничены собственным токеном.

Более продвинутые услуги, основанные на Sentinel, предложат пользователям повышенную конфиденциальность и большую степень недоверия за счет использования услуг условного депонирования, а также сетевых интеграций, ориентированных на безопасность. Эти услуги состоят из приложений, таких как ретрансляционные сети, для очень уникальных и демографически специфичных сетевых протоколов. Оказание услуг

поставщики расширенных услуг (не владельцы приложений DVPN) могут либо предлагать услуги по подписке, либо предлагать возможность выставления счетов за пропускную способность в реальном времени (оплата за ГБ).

Эти расширенные услуги будут использовать «протокол проверки пропускной способности» Sentinel для децентрализованной системы управления, ориентированной на измерение обмена пропускной способностью p2p в реальном времени. Этот протокол доказуемости гарантирует отсутствие искажений в отношении предоставления или потребления пропускной способности без необходимости использования сторонней системы мастернод, которая следит за соединением.

Как для подписки, так и для выставления счетов за эти расширенные услуги в режиме реального времени пользователям придется размещать свои токены Sentinel в системе условного депонирования. При использовании услуги на основе подписки оплата за весь срок подписки вычитается из заблокированной суммы токена в рассрочку. Например: для ежемесячной подписки на расширенную услугу может потребоваться 1/30 от общего платежа за подписку, вычитаемого из размещенных токенов Sentinel на условном депонировании в день. Для выставления счетов в режиме реального времени оплата будет периодически вычитаться из условного депонирования в прямой зависимости от объема пропускной способности, потребляемой пользователем, что обеспечивает ненадежную и безопасную транзакционную среду.

Рабочий токен:

- Токен на основе Sentinel Cosmos действует как рабочий токен, что позволяет держателям токенов, размещающим токены, получать вознаграждение. Эти вознаграждения генерируются хостами узлов, которые предоставляют пропускную способность для приложений dVPN, построенных на платформе Sentinel.

Сила децентрализации консенсуса блокчейна Sentinel в первую очередь зависит от участия в стейкинге в управлении валидатором хаба Sentinel. Владельцы токенов передают свои токены надежным валидаторам, чтобы получать вознаграждение за стейкинг, одновременно повышая безопасность сети за счет эффективного увеличения «стоимости атаки» для злоумышленника. Поскольку транзакция для услуг dVPN в обмен на цифровые активы (криптовалюты и стейблкоины) происходит в хабе Sentinel, держатели токена Sentinel будут получать вознаграждение от дохода, генерируемого хостами узлов в сети Sentinel, в обмен на вклад в безопасность транзакций в сети Sentinel. экосистема.

Процент от доходов, генерируемых хостами узлов, будет накапливаться в пуле, а затем периодически выплачиваться держателям токенов. Сумма, получаемая участниками токенов от распределения доходов, будет находиться в прямой зависимости от совокупного спроса на услуги dVPN из приложений, построенных на платформе Sentinel. Увеличение общего числа пользователей и доходов от подписки, полученных от приложений dVPN, созданных на основе Sentinel, приведет к увеличению количества необходимых узлов dVPN для обслуживания растущих требований пользователей к полосе пропускания.

06. Интеграция аппаратного маршрутизатора

Интеграция протокола Sentinel dVPN с сетевыми маршрутизаторами на основе Open-WRT (популярная прошивка маршрутизатора с открытым исходным кодом) позволит владельцам маршрутизаторов стать хостами узлов, легко монетизируя свою пропускную способность. Кроме того, Sentinel стремится поддерживать и интегрироваться с любым маршрутизатором с открытым исходным кодом, который может применять соединение dVPN по сети Wi-Fi в целом. dVPN на основе маршрутизатора позволит пользователям избежать установки приложения VPN на каждое из своих устройств, и пользователь потенциально может создать дополнительную домашнюю сеть, предназначенную только для доступа через dVPN.

Простота монетизации

Преимуществом экосистем, ориентированных на «монетизацию пропускной способности», таких как Sentinel, является низкий «стоимостной» барьер для входа для участников, поскольку почти все жители развитых стран имеют постоянное и надежное подключение к Интернету. Этот низкий «стоимостной» входной барьер для «монетизации пропускной способности» можно сравнить с высоким «стоимостным» входным барьером для майнинга биткойнов, который требует от пользователей покупать специальное оборудование для майнинга и заработка биткойнов.

Sentinel позволяет любому человеку во всем мире получать пассивный доход, предоставляя свой ресурс полосы пропускания приложениям DVPN, построенным на Sentinel. Размещение узла DVPN Sentinel на виртуальной машине требует определенного технического опыта. Этот «технический» барьер для входа снижает потенциал хост-сообщества узла Sentinel, поскольку отговаривает менее технически подкованных пользователей от участия. Чтобы преодолеть технический барьер на пути к управлению узлом, среднестатистическому пользователю должно быть не только чрезвычайно легко использовать Sentinel dVPN, но и должно быть максимально просто разместить узел и заработать токены в обмен на предоставление пропускной способности.

Пользователи, которые обеспокоены раскрытием своего резидентного IP-адреса при размещении выходных узлов, будут иметь возможность размещать ретрансляционные узлы. Размещая ретрансляционные узлы, владельцы маршрутизаторов Sentinel с поддержкой dVPN смогут оставаться анонимными от интернет-провайдеров, а также получать прибыль от пользователей, платящих за эту расширенную услугу.

Что такое маршрутизатор и зачем они нужны?

Маршрутизаторы — это устройства, которые чрезвычайно важны для нашей зависимости от Интернета, поскольку маршрутизаторы создают шлюз для соединения двух или более сетей друг с другом. Кроме того, маршрутизатор позволяет сети использовать несколько устройств, поскольку маршрутизатор обеспечивает надлежащую балансировку нагрузки и распределение пропускной способности.

Общие характеристики роутера:

1. Возможность установить беспроводную сеть. 2.
Возможность применять стандарты шифрования к данным, маршрутизируемым через беспроводную сеть.
3. Возможность разрешить беспроводной сети обрабатывать несколько устройств с балансировкой нагрузки.
4. Увеличение покрытия/диапазона сети
5. Возможность работы в двух диапазонах для предотвращения задержек

Каковы проблемы со стандартными маршрутизаторами?

1. Стандарты полностью закрыты и не предлагают публике возможность вести непредвзятый код.
обзоры
2. Стандартные маршрутизаторы не дают пользователям возможности туннелировать свою полосу пропускания через доказуемую сеть dVPN.
который предлагает гарантию безопасности и шифрования
3. Стандартные маршрутизаторы не предлагают пользователям возможность монетизировать избыточную неиспользуемую полосу пропускания.

Что это значит?

1. Стандартные маршрутизаторы можно взломать и ими можно манипулировать, а на обнаружение и исправление уязвимостей могут уйти месяцы или даже больше, поскольку кодовая база закрыта для общественности (пример Linux против Microsoft).
2. Стандартные маршрутизаторы в настоящее время не предоставляют пользователям возможности безопасного использования децентрализованного и распределенного VPN-приложения, которое может прозрачно подтвердить целостность своих внутренних операций.
3. Стандартные маршрутизаторы не позволяют пользователям монетизировать избыточную неиспользуемую полосу пропускания, что приводит к пустой трате платные ресурсы

07. Организационная структура

Организационная структура Sentinel в основном состоит из Фонда «Безопасные сетевые технологии» (или SNT) и коммерческой организации Exidio, занимающейся внедрением и развитием dVPN. На момент написания статьи фонд SNT и Exidio были полностью зарегистрированы и структурированы.

В то время как фонд SNT занимается методологической организацией и управлением децентрализованной экосистемой Sentinel, Exidio отвечает за техническую разработку инфраструктуры Sentinel dVPN, а также за привлечение создателей приложений dVPN.

Фонд «Безопасные сетевые технологии»

1 редоставление финансовой и нефинансовой поддержки проектам экосистемы Sentinel – Ответственность предоставление нефинансовой и финансовой поддержки проектам и организациям, существующим в экосистеме Sentinel, целью которых является развитие Sentinel и повышение ценности экосистемы Sentinel.

2 беспечение принятия — Миссия по стимулированию внедрения токена Sentinel посредством разработки и поддержки интеллектуальных вариантов использования и механизмов полезности.

3 беспечение экономической жизнеспособности токенов — Миссия по обеспечению сильной экономической структуры токенов в экосистеме Sentinel. Необходимо следить за инфляцией и другими параметрами сети, уделяя особое внимание тому, чтобы стоимость токена не снижалась значительно в долгосрочной перспективе.

4 беспечение экономического здоровья — Миссия по созданию здоровой и плодотворной среды для валидаторов/узлов/ другие поставщики услуг в экосистеме. Разработка и поддержание надежных экономических структур, которые могут гарантировать, что поставщики услуг смогут покрыть свои затраты безубыточности, а также получить разумную премию за свое время и усилия.

5 обавление партнеров по экосистеме — содействие партнерским отношениям между экосистемой Sentinel и организациями, которые повысят ценность экосистемы Sentinel и стимулируют использование протокола, а также внедрение токена.

6 асширение глобального сообщества — расширение глобального сообщества Sentinel за счет обслуживания и поддержки различных региональных групп и соответствующего управления представителями региональных групп. Фонд SNT отвечает за то, чтобы структура экосистемы была совместима с различными регионами и чтобы дизайн экосистемы не препятствовал какой-либо конкретной географии.

EXIDIO

Экосистема Sentinel быстро превращается из малоизвестной и анонимной сети в прозрачную экосистему реального мира, которая нацелена на удовлетворение требований основного потребителя. Exidio — это коммерческая организация, ориентированная на внедрение, перед которой стоит задача «Обеспечить безопасный доступ к Интернету 3.0», внося вклад и внедряя Sentinel dVPN и блокчейн-инфраструктуру Sentinel Cosmos.
Exidio будет работать с предпринимателями, а также с существующими компаниями в области VPN, чтобы либо создать новое приложение dVPN, либо перевести существующую сеть VPN на сеть dVPN.

В то время как Sentinel фокусируется на предоставлении среды, в которой размещаются различные компоненты целостной сети DVPN, Exidio сосредоточится на внедрении приложений dVPN с белой маркировкой и выполнении необходимых настроек.

Прогнозируется, что к 2027 году индустрия VPN станет рынком с оборотом более 90 миллиардов долларов, и VPN-предприниматели во всем мире пользуются растущим потребительским спросом на услуги VPN, внедряя решения с белой маркировкой. Решения с белой маркировкой предлагают преимущество снижения затрат на выход на рынок и требуют меньше технических знаний и ресурсов для управления.

Сосредоточенность Exidio на вкладе в Cosmos в первую очередь связана с:

1 азработка утилит — разработка значимых и творческих утилит, которые могут быть реализованы другими разработчиками в экосистеме космоса (например, развертывание Exidio с несколькими подписями / совместными учетными записями)

2 азработка dApps — разработка полезных и эффективных децентрализованных и распределенных приложений на основе блокчейна в экосистеме Cosmos (таких как Sentinel dVPN), которые способны обеспечить реальную полезность даже для основного пользователя.

3 клад в разработку ядра Cosmos SDK и Tendermint — участие в предложенной дорожной карте, а также работа над оптимизацией и повышением эффективности текущих кодовых баз Tendermint и Cosmos SDK.