Компания Bison Trails сообщает о запуске протокола Support for the Keep

Support for the Keep – протокол на платформе Bison Trails, который позволит владельцам Эфира (ETH) принимать участие в Stake Drop от протокола Keep. Stake Drop – это механизм, с помощью которого владельцы ETH могут участвовать в сети Keep и получать вознаграждение – рабочие KEEP-токены. Такое решение позволит ускорить процесс внутреннего (он-чейн) использования BTC в приложениях DeFi (децентрализованных финансов). Раздача наград начинается 13 мая (примечание: статья опубликована 26 апреля 2020 года, обновлена 8 июня 2020 года).

Основные моменты

- Keep – слой конфиденциальности для платформы Эфириум (Ethereum), который выполняет сложную задачу по обеспечению безопасных и конфиденциальных данных, использующихся в публичном блокчейне.
- Первое применение протокола Keep на практике – создание системы TBTC, в рамках которой происходит выпуск обеспеченных биткоином токенов стандарта ERC-20. Эта система позволяет владельцам BTC безопасно хранить их приватные ключи за пределами блокчейна (off-chain), в то же время используя BTC на платформе Ethereum в приложениях DeFi.
- Владельцы ETH и KEEP могут запускать ноды на основе протокола Keep, который распределит 20% от общего обеспечения KEEP в качестве субсидий для операторов нод (узлов) после 24 месяцев действия механизма Stake Drop.
- Stake Drop начинается 8 июня для стейкеров KEEP+ETH (майнеров, которые используют криптовалюты с алгоритмом консенсуса PoS – подтверждения ставки), с распределением максимального вознаграждения в течение 2-6 месяцев.
- Начиная с 8 июля, участникам нужно будет только стейкать ETH без обязанности иметь KEEP. Тем не менее, стейкинг KEEP в течение этого периода существенно повышает для участника вероятность быть выбранным для выполнения работы. Это, соответственно, позволит ему заработать вознаграждение. Длительность этого периода – 6 месяцев. После истечения указанного срока сторонам для дальнейшего участия нужно будет также стейкать заработанный KEEP.

Цель протокола Keep

Публичная основа блокчейна создана намеренно; выступая в роли «гроссбуха», блокчейн создает условия для того, чтобы все транзакции регистрировались именно в его пределах. По умолчанию каждая транзакция видна для каждого, включая «конкурирующие интересы». Протокол Keep был создан для того, чтобы создать своеобразный мост между сферами личных данных, находящихся в безопасности, и публичными блокчейнами.

Нововведения в протоколе Keep

При использовании Keep небольшие объемы конфиденциальных данных (например, личные ключи) могут храниться офф-чейн (за пределами цепи). Тем не менее, они все равно используются в смарт-контрактах он-чейн бездоверительно. Бездоверительный компонент возможен из-за развития случайного маяка в протоколе Keep. Случайный маяк – это источник надежной случайности, который делает практически невозможной вероятность сговора.

Другое важное новшество, внедренное в Keep, - это способность протокола разрешать использование в публичном блокчейне приватной информации, которая удерживается вне цепи, но хранится в нодах. Хранилища, в которых содержится эта информация, могут быть созданы для множества функций – например, для повторного шифрования прокси. Протокол Keep имеет

хорошие ресурсы для решения проблемы потребности в конфиденциальности, что сделает возможным более широкое принятие публичными блокчейнами конфиденциальных данных.

Keep преодолевает разрыв между блокчейнами путем разрешения перемещений токенов между протоколами. Так, поскольку разработчики хотят, чтобы блокчейн Биткоина оставался простым и безопасным, людям сложно использовать Биткоин при выполнении финансовых транзакций в качестве обеспечения займа или взаимодействовать с DeFi как с Эфириумом. Чтобы решить этот вопрос, разработчики протокола Keep разработали способ безопасного использования биткоина на других блокчейнах (на начальном этапе это Эфириум) без утраты особенностей биткоина как криптовалюты.

Команда разработчиков KEEP

Принцип работы протокола Keep

Keep – это конфиденциальный слой для платформы Эфириум. Он принимает фрагменты информации, делит их на отдельные части, хранит эти части с помощью различных операторов нод, а также позволяет владельцам информации собирать эти части воедино по мере надобности.

Например, приватный (то есть открытый) ключ может быть разбит на части и храниться в виде отдельных фрагментов, при этом эти части могут быть соединены только тогда, когда это понадобится владельцу представленной информации. Это актуально для совершения таких действий, как отправка транзакции или подписание сообщения. Случайное физическое лицо не имеет доступа к информации, если только оно не вступило в сговор с другими для совершения мошеннических действий в сети. Но даже для таких случаев сеть установила правила, которые предусматривают наказание для мошенников. Оно выражается в том, что мошенники, действуя подобным образом, потеряют гораздо больше в криптовалюте ETH, чем они могли бы получить в BTC.

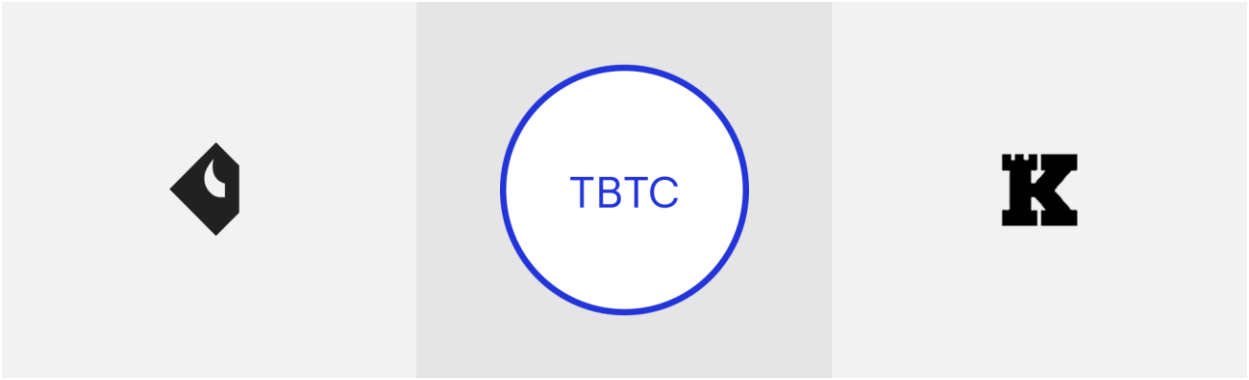
Ниже представлены основные понятия, которые помогут понять особенности и принципы работы протокола Keep:

- keeps. Это «небольшие офф-чейн хранилища информации конфиденциального характера, которые также пригодны для вычислительных работ. Они могут открываться, закрываться и управляться смарт-контрактами в автономном режиме». Есть много разновидностей таких keep-хранилищ. Keep-хранилища поддерживаются операторами нод (узлов). За это операторы получают вознаграждение. Каждый тип такого мини-хранилища требует разного количества нод для его обслуживания. Они выбираются случайным образом из крупного фонда доступных нод.
- KEEP-токен. Это нативный рабочий токен, необходимый для объекта, который хочет стать членом сети Keep и иметь право зарабатывать вознаграждение за выполнение работы на платформе. «Работа» определяется как вычисление и полезность, требуемые со стороны

ноды для выбора и объединения keep-хранилищ, а также для возможности прочесть связанную с этим информацию.

- Распределенная генерация ключа (DKG). Это криптографический процесс, в котором множественные стороны способствуют вычислению общего публичного (открытого) и приватного (закрытого) ключа. Этот процесс делает невозможным доступ конкретных участников к закрытому ключу.
- Случайный маяк. Это надежный источник случайности, который используется в процессе выбора бездоверенной группы в Keep. Маяк выбирает провайдеров для каждого нового keep-хранилища информации.
- Группа подписантов. Группа, состоящая из нод в системе Keep, необходимая для подписания контрактов по деятельности, которая происходит он-чейн (внутри цепи). Ноды никогда не оставляют единичных подписей. Например, случайный маяк (Random Beacon) требует создания группы из 64 подписантов.

Первое децентрализованное приложение на основе Keep: TBTC



TBTC – обеспеченный биткоином по принципу «1 к 1» токен стандарта ERC-20. Это первый токен, который будет выпущен в обращение через децентрализованный протокол. 1 TBTC может быть погашен 1 BTC. Поскольку в данном случае на платформе Эфириум находится именно биткоин, а не его стоимость, указанный токен позволяет использовать биткоин в системе DeFi (децентрализованные финансы). Существование TBTC стало возможным благодаря нововведениям в Keep. Они позволили приватным (закрытым) ключам оставаться секретными и в то же время – принимать участие в публичном блокчейне.

Аарон Хэншоу, технический директор и соучредитель BISON TRAILS: *«Безопасное хранение конфиденциальной информации, применяемое в смарт-контрактах, - заслуживающее внимания нововведение, реализованное командой Keep. TBTC, будучи бездоверительным децентрализованным активом, имеет огромный потенциал наконец-то разблокировать приложения DeFi для BTC путем его перемещения на платформу Ethereum. Мы в восторге от того, что поддерживаем Keep на своей платформе инфраструктур, и с нетерпением ожидаем участия в Stake Drop от Keep».*

Как работает TBTC

Чтобы выпустить токен TBTC с BTC, система должна выполнить процесс, состоящий из нескольких шагов.

Вначале сеть Keep создает адрес для депозитора, на который будет отправлен BTC:

- Случайный маяк выбирает 64 ноды, которые используют хранилища типа «Random Beacon», для получения случайного числа.
- Это случайное число используется, в свою очередь, для выбора трех Keep-нод, которые управляют как хранилищами типа «Random Beacon», так и хранилищами TBTC (это

называется BondedECDSAKeep). Выбор указанных трех нод происходит с учетом того, какое количество Keep-токенов на них производится путем стейкинга. Количество всех стейканых KEEP-токенов, которые присутствуют на одной ноде, примерно соответствует количеству времени, в течение которого нода будет выполнять работу (например, если у вас есть 1% от общего KEEP-токена, стейкинг которого происходил на вашей ноде, то вы выполните около 1% работ в сети).

- Помимо токена KEEP, ноды также должны иметь залоговый ETH. Это необходимо для создания TBTC. В настоящее время нода должна иметь как минимум 50% от стоимости биткоина в ETH, создавая таким образом общее залоговое обеспечение в размере 150% для всех трех нод. Такое сверхобеспечение необходимо для того, чтобы предотвратить вероятность сговора между нодами, направленного на кражу Биткоина. В представленных условиях они потеряют больше, чем Биткоин, который они надеялись украсть.
- После того, как три ноды выбраны, они начинают работать вместе для выполнения распределенной генерации ключа, чтобы создать открытую и закрытую пару ключей для биткоина. Этот процесс выполняется при условии, что каждая нода видит только свою собственную часть закрытого ключа, в то же время создавая единый, совместно используемый открытый ключ.
- Каждая нода принимает свою часть закрытого биткоин-ключа и помещает его в свое TBTC-хранилище.

Далее депозитор вносит свой BTC:

- Биткоин-адрес предоставляется пользователю, который хочет внести биткоин на депозит.
- После того, как депозит создан, ноды (подписанты), участвующие в процессе создания ключей, получают небольшое вознаграждение за подписание в качестве депонированного дохода за оказанные услуги.
- Пользователь обеспечивается доказательством SVP (упрощенная верификация платежей), которое исходит из цепи BTC и используется в качестве подтверждения в цепи Эфириума. Оно указывает на то, что депозит был совершен правильно.
- Депозитор использует это подтверждение в dApp для того, чтобы доказать, что он имеет право на свой TBTC, который он теперь может получить и использовать в блокчейне Эфириума в протоколах DeFi.

Чтобы вернуть BTC:

- Пользователь сжигает свой TBTC путем смарт-контракта, который уведомляет подписантов, владеющих закрытым ключом к его депозиту, о том, что необходимо собрать ключ из частей и отправить депозит на адрес, определенный депозитором.
- Пользователь, погашающий депозит, оплачивает вознаграждение подписантам, в то время как это вознаграждение, бывшее изначально депонированным, возвращается к первоначальному депозитору. Любой участник может закрыть любой TBTC-депозит в любое время, включая и тех, кто не принимал участия в его открытии. Это не окажет никакого влияния на первоначального депозитора.
- Группа подписантов создает и выпускает подпись для биткоин-транзакций на блокчейне биткоина. В дальнейшем группа генерирует SPV-доказательство транзакции и выпускает его на блокчейне Эфириума.
- В этом случае подписанты получают их залоговые ETH обратно вместе с вознаграждением за подпись. Теперь они могут использовать ETH в целях продолжения создания TBTC либо полностью изъять его.

За первые 4 месяца, начиная с июня 2020 года, будет создана система покрытия в tBTC (первый месяц – 100 tBTC, второй – 250 tBTC, третий – 750 tBTC, четвертый – 1000 tBTC). Пятый месяц не подразумевает покрытия.

Stake Drop

TBTC действует в рамках двустороннего рынка. Как и в случаях с большинством финансовых продуктов, TBTC требует полезного использования и ликвидности. В первую очередь, здесь должны быть BTC-депозиты и ETH-стейкеры.

Чтобы облегчить достижение критической массы, команда Keep планирует существенно стимулировать участие в Stake Drop в течение первых 12-18 месяцев. Stake Drop – механизм, посредством которого пользователи с ETH, но не имеющие KEEP, могут стейкать и принимать участие в сети Keep, а также получать вознаграждение в виде токенов KEEP и комиссии подписантов.

В первые 2 месяца после запуска Stake Drop будет наблюдаться максимальное распределение вознаграждений. В данном случае поддержка будет оказана участникам, которые готовы начать зарабатывать вознаграждения с 13 мая.

В первые 6 месяцев участникам нужно будет только стейкать ETH. В этот период им необязательно иметь KEEP, хотя стейкинг KEEP существенно повышает вероятность для них быть выбранными для выполнения работ, благодаря чему можно заработать вознаграждение. После 6 месяцев сторонам также нужно будет стейкать KEEP для того, чтобы продолжить участие, но, скорее всего, к этому моменту они заработают достаточно много вознаграждений, чтобы сделать это. (Если вас интересует участие в Stake Drop и вы хотите обсудить это с нашими экспертами по протоколу, пожалуйста, напишите нам.

Вознаграждение за ликвидность

Команда Keep размещает 5% токенов KEEP (50 миллионов KEEP // $6 миллионов USD) в качестве вознаграждения за ликвидность, для того, чтобы стимулировать владельцев tBTC добавить tBTC в DeFi-торговлю и протоколы ликвидности (например, Uniswap). Это вознаграждение способствует принятию tBTC и упрощает обслуживание ликвидаций депозита для стороны, выполняющей ликвидацию. Дальнейшие подробности от команды Keep будут известны уже совсем скоро.

Экономические вопросы в Keep

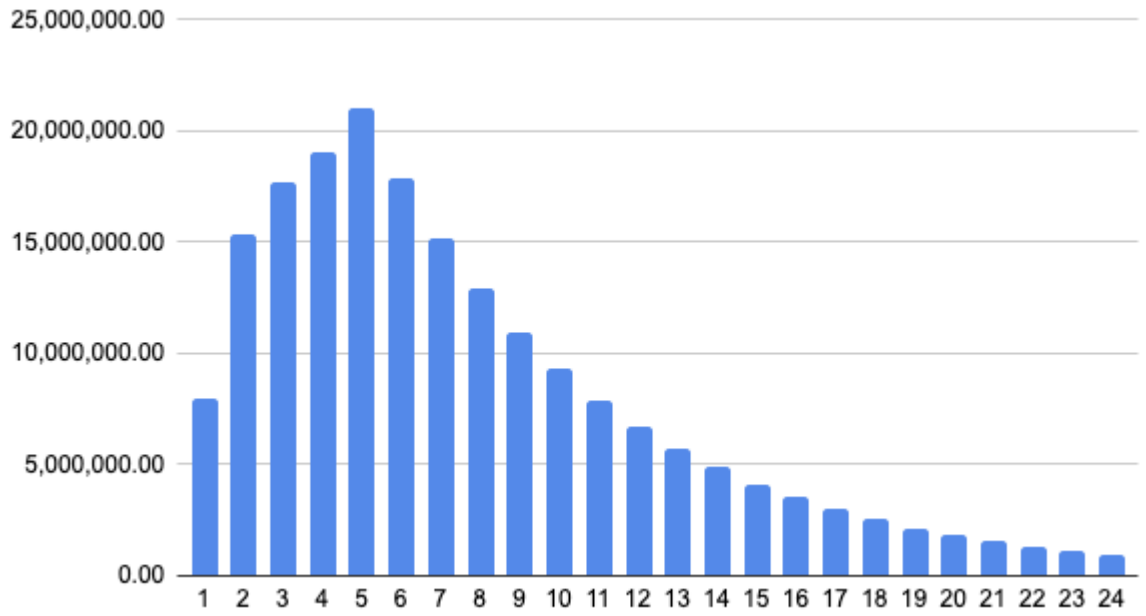
Типы токенов	KEEP – нативный рабочий токен ETH – используется в качестве залогового обеспечения для создания TBTC и оплаты вознаграждения на платформе Ethereum BTC – используется как начальный депозит в процессе выпуска в обращение TBTC TBTC – токен стандарта ERC-20, который представляет Биткоин на платформе Ethereum
Общее начальное обеспечение	1 000 000 000 (миллиард)
Общее число запланированных субсидий	25% или 250 миллионов от 1 миллиарда будут распределены в качестве субсидии в первые 24 месяца (200 миллионов в Stake Drop и 50 миллионов в качестве вознаграждения за ликвидацию
Максимальное обеспечение токенов	1 000 000 000
Стоимость токена при продаже	$.12
Уровень инфляции	Инфляции нет
Максимальный размер в стейкинге	Максимума нет

Минимальный размер в стейкинге	100,000 KEEP ($12 000 USD). Опишем со временем на предсказуемом графике. Еще не выпущен
Период блокировки	Выплаты вознаграждения подписантов в ETH или TBTC не блокируются
Период прекращения залоговых обязательств и делегирования	60 дней для токенов KEEP 0 дней для ETH (если TBTC, в создании которого вы принимали участие, погашен)

Поскольку KEEP является рабочим токеном, а общее обеспечение токена существует на момент запуска, в сети отсутствует размер инфляции. Keep планирует стимулировать массовое участие с самого начала, а не спустя несколько первых лет, используя Stake Drop для распределения KEEP.

Благодаря Stake Drop, 20% от токенов KEEP (200 000 000) будут распределены в качестве субсидии участникам, управляющим TBTC-хранилищем и хранилищем типа «случайный маяк». Это гарантирует, что в сети стейкается достаточное количество ETH, а также обеспечивает выплату вознаграждений пользователям нод, которые управляют хранилищем TBTC в большей мере, чем те, кто управляет только хранилищем типа «случайный маяк». Больше деталей о субсидиях можно найти здесь – в документе, любезно предоставленном командой Keep.

Распределение STAKEDROP от KEEP



Источник – команда Keep

Стейкинг Keep

Стейкинг Keep и ETH как подписант TBTC

- Операторы нод, которые управляют хранилищем TBTC, должны стейкать ETH вместе с KEEP для участия и получения вознаграждения. На протяжении Stake Drop вам понадобится только стейкать ETH. Вознаграждение поступает в виде KEEP от Stake Drop, а вознаграждение подписантов оплачивается в токенах TBTC.
- Стейкинг ETH и KEEP повысит вознаграждение до 11% сверх ETH. Этого можно достичь только на протяжении Stake Drop. Кроме того, стейкинг одновременно ETH и KEEP увеличит шансы ноды быть выбранной для создания TBTC до 20-30%. Это, в свою очередь, ускорит увеличение доли их участия по сравнению с нодами, управляющими только ETH.

- 18% от общего обеспечения KEEP (180 000 000) будет выплачено в качестве вознаграждения подписантам TBTC через Stake Drop. Сумма, которую может получить конкретная нода, зависит от количества ETH, участвовавшего в стейкинге ноды. Поскольку количество работы (часть от общего показателя), которое просят выполнить ноду, эквивалентно проценту от общей суммы ETH, которую получила нода методом стейкинга, вознаграждения будут существенно зависеть от результатов как индивидуального, так и общего стейкинга.
- На этапе запуска размер вознаграждения составит 5 bps (0,05%) для каждого BTC на депозите (bps – базисный пункт, единица, равная 1/100 от 1% и используемая для обозначения изменений в стоимости финансового инструмента). Этот уровень повысится, так как сеть TBTC масштабируется; ожидается, что он будет в общем повышаться до 2-4% каждый год в рыночной системе TBTC в среднесрочной и долгосрочной перспективе. Единственным вознаграждением, за которое ответственна система TBTC, является комиссия вознаграждение подписантам. Последняя депонируется, когда подписант выпускает в оборот TBTC, и выплачивается ему после погашения депозита.

STAKING KEEP в качестве подписанта «случайного маяка»

- Из 20% токенов, распределяемых с помощью Stake Drop, 2% пойдет на выплату владельцам KEEP, которые управляют нодами с хранилищем случайного маяка.
- К концу первого года это отразится на размере выплат в виде 4-5%.
- Ноды также получают вознаграждение подписантов за их участие в «случайном маяке», но их сумма, вероятнее всего, будет минимальной до тех пор, пока использование Keep не достигнет критической массы.

Зачем управлять нодой?

- Если вы являетесь текущим владельцем KEEP через инвестиционный контракт для будущих токенов (SAFT), то по этому контракту от вас будет требоваться стейкинг вашего KEEP на протяжении 6-24 месяцев.
- Даже без указанного требования Stake Drop обеспечивает крайне привлекательную возможность участия в Keep, особенно, если вы заинтересованы в стейкинге ETH.
- KEEP в размере двух миллионов (около 24 миллионов USD) распределяется в качестве вознаграждения для указанных управляющих нод в течение первых 24 месяцев.
- В настоящее время Keep не поддерживает более, чем одного пользователя, делегированного в одну ноду, хотя договоры об объединении пулов могут быть введены позднее. На этапе запуска единственным способом участвовать является управление нодой.

Зачем управлять нодой Keep с Bison Trails?

Bison Trails был одним из первых сторонних поставщиков, которые продвигали ноды на платформе Keep. Мы начали эту деятельность в июне 2019 года. С тех пор мы обеспечили основу, которая позволила изменить параметры протокола для удовлетворения требований по продуктивной эксплуатации инфраструктуры, а также создали первое особое приложение без участия команды Keep для того, чтобы улучшить настройки их инфраструктуры. Наш запрос на выполнение данных усилий объединен здесь.

Мэтт Луонго, генеральный директор, основатель проекта KEEP: «Команда Bison Trails феноменальна. Они глубоко привержены сети Keep и оказали неоценимую помощь в разработке проекта нашего протокола, а также его продвижении. Сеть Keep требует множества надежных, распределенных и безопасных нод, делая Bison Trails сильным партнером, а также хорошим выбором для тех, кто владеет токеном Keep, и вообще для всех, кто присоединяется к нашему Stake Drop 8 июня».

Наша платформа специально разработана для безопасного и надежного управления множественными нодами. Поэтому она идеальна для сети рабочего токена, которая требует разнообразия нод и высокого уровня доступности. Кроме того, есть 3 роли с соответствующими адресами, которые используются для установления и управления нодой Keep:

- Владелец/доверитель, который предоставляет в ноду KEEP или ETH без попечительства.
- Оператор, управляющий нодой и поддерживающий ее.
- Бенефициарий, который получает коллегиальные вознаграждения и вознаграждения подписантов.

Такой план позволяет, привлекая инфраструктурных провайдеров без попечительства для управления вашей нодой, делать этот процесс простым и честным. К таким провайдерам относится Bison Trails. Свяжитесь с нами, если у вас есть вопросы о протоколе Keep, а также если вы хотите начать управление нодой Keep.

Bison Trails: поставщик инфраструктурных решений в блокчейн

Bison Trails – компания, предоставляющая инфраструктурные решения, основанная в Нью-Йорке. Ее основная сфера интереса – участие в блокчейне. Мы создали платформу для всех, кто желает без приложения особых усилий участвовать в новых цепочках (например, путем использования децентрализованной сети Cosmos Validators, открытой платформы Tezos Bakers и глобальной системы платежей Libra Validators). Вам не нужно затрачивать много времени и вкладывать ресурсы в развитие любых инженерных изысканий, протоколов, разработчиков или обеспечение безопасности внутри сети. Наша цель – создать условия для процветания целой блокчейн-экосистемы путем обеспечения надежной инфраструктуры для новаторов, создающих будущее.