ESPERS

Проект команды CryptoCoderz

Технический документ

Создано командой CryptoCoderz
20 Февраля 2018 года (версия 1.0)

ESPERS

СОДЕРЖАНИЕ

Вступление

Появление технологии блокчейн в начале 2000-х годов взволновало мир, всем было интересно увидеть, что же из этого получится. В первую очередь биткойн привлек внимание как валюта, которая работала в блокчейне и в других видах связи, которые появились после него. Потребность в усовершенствовании технологии блокчейн для повседневного пользования, в котором и провайдер, и пользователь выиграют от обеспечения и децентрализации, пока что была не полностью реализована.

Espers - это гибридная блок-цепь Proof-Of-Work / Proof-Of-Stake (PoW / PoS), которая была создана для решения проблемы разделения и отсутствия удобства использования, которое в настоящее время приписывается технологии блокчейн, как для унификации, так и для расширения возможностей. Реализованные функции, такие как защищенный обмен сообщениями, межсетевое взаимодействие, модульные боковые цепи, веб-сайты в цепочке, хранение файлов в цепочке, объединяются через универсальный интерфейс, который может участвовать в проекте любой монеты. Использование ESP (Espers) монеты как «топливо» или катализатор, который управляет услугами, что задействованы в цепочке, стимулирует интерес к участию в блоках обработки для интернета. Майнерам / инвесторам рекомендуется участвовать в создании последовательной генерации блоков и обеспечении максимальной молниеносной сети в целом. Этот документ призван подробно описать различные системы, которые использует проект Espers, и как они работают в унисон, чтобы предоставить конечному пользователю любого сообщества беспрепятственный и наглядный опыт.

ESPERS

ТЕХНОЛОГИЯ БЛОКЧЕЙН

***Текущие недостатки**

Сегодня большая часть того, что приписывается блокчейну, - это просто единая функциональная система с очень специфической целью, предназначенной для получения дохода. Создатель биткоина надеялся предложить по-настоящему уникальную технологию, не фокусирующуюся на доходах, но это видение затмилось, когда сотни блокчейн-цепей начали функционировать. Хотя новости и средства массовой информации хотели бы, чтобы вы считали, что технология блокчейн не должна быть монофункциональной. К сожалению, средства массовой информации сосредотачиваются только на потерях и выгодах. Так среднестатистический человек опасается любой системы блокчейн, которая занимается исключительно предоставлением токенов или монет. Хотя индивидуально технологические достижения мало способны связать биткоины на основе блокчейнов, даже альтернативы, такие, как Ethereum, не обеспечивают простое решение.

***Текущая реализация и преимущества**

Блокчейн можно охарактеризовать как «цифровой регистр, в котором транзакции, выполненные в биткоине или другой криптовалюте, записываются хронологически и публично» (Google). Хотя это более или менее верно, заявляя, что цифровой журнал блокчейна используется для записи истории транзакций, что мысленно заставляет ограничить то, что, по их мнению, может быть сделано с ним. В первую очередь блокчейн, действительно, используется для широкого распространения децентрализованного цифрового регистратора, который хранит записанные данные транзакций для всей системы, позволяя любому иметь возможность безопасно получать доступ к своим учетным записям и информации. Без центральной точки отказа, будучи децентрализованной, блокчейны, такие, как биткойн, очень устойчивы к любой форме снятия или атаки системы.

Распределенные регистры также обеспечивают прозрачность, позволяющую видеть общую информацию всем, сохраняя при этом более частные значения и информацию под блокировкой закрытого ключа, который является индивидуальным для каждого пользователя. Информация транзакций хранится в информационных блоках, которые обычно известны как «блоки». Блоки генерируются «майнерами», людьми, которые занимаются добычей, либо размещением форм, предоставляющих ресурсы для шифрования блока информации и передачи его в сеть.

Поскольку блокчейн генерирует блоки, он также может управлять их размером, что облегчает возможность хранения разных типов данных в больших объемах, которые затем предоставляются конечным пользователям. Это отрицает необходимость наращивать блокчейны, если это не требуется по параметрам цепи. При сборке блокчейн является очень способной системой с точки зрения "монет", но ее универсальность на этом не заканчивается.

***Будущие возможности**

Блокчейн может использоваться для решений множества проблем с программным обеспечением в отношении дополнительной безопасности и надежности, предлагаемой системой децентрализации. Ограничением является только ваше воображение и креативность. Сообщества говорят об операционных системах, системах обмена сообщениями, системах хранения данных, которые все работают на блок-цепи, что значительно придает смысл нашим текущим заявлениям.

Когда сообщества и проекты начнут уходить от монетарной направленности и больше ориентироваться на развитие самих технологических возможностей, это создаст реальную упорядоченность, как в плане безопасности, так и в надежности наших повседневных задач.

МЕХАНИЗМ ОПЛАТЫ И СОГЛАСОВАННОСТИ

Espers использует гибридную блок-цепочку Proof-Of-Work / Proof-Of-Stake (PoW / PoS), которая непосредственно влияет на то, как система обрабатывает производство блоков и стимулирует интерес к этому.

Proof-Of-Work или (PoW), как это часто называют, является самым заметным используемым методом, так как он также является наиболее распространенным среди проектов блокчейн с момента его использования в биткойне.

PoW функционирует благодаря тому, что участники предоставляют вычислительную мощность в форме, известной как «хэш» или «хеширование», в отношении хеширования блока блокчейн. Участники награждаются за правильно поданные блоки, которые принимаются блокчейном/ сетью, а затем подтверждены как возрастные блоки, обеспечивающие последующее генерирование (майнинг) будущих блоков, заставляя участников заинтересоваться. Кроме того, несколько участников, как правило, объединяют свои ресурсы с помощью «интеллектуального анализа», который обычно конкурирует друг с другом, что позволяет даже тем, у кого мало вычислительной мощности, получать компенсацию за то, что они предоставляют, а не пытаться победить со значительно большей мощностью хэширования. Этот метод распространения не соответствует совершенству, хотя можно атаковать блокчейн, контролируя, какая информация находится в блоках, которые сейчас в процессе майнинга. Они называются «плохими блоками», которые представляют собой блоки с недействительной информацией, которые обычно не принимаются даже, возможно, разделяя блокчейн на две версии (разветвление). Данные версии затем конкурируют за действительность и принятие в сеть, когда объект имеет возможность вычислять с помощью огромного количества власти, к которой большинство не имеют доступа.

Proof-Of-Stake или (PoS) связано с тем, что PoS использует монеты, которыми владеет участник, и удерживает их для создания блока, тем самым, владея большим количеством монет и ставя их в аренду, что дает участнику более высокую возможность генерации следующего блока. Стекин - это действие, позволяющее одному кошельку / клиенту оставаться в сети, чтобы поддерживать сеть, когда случайно выбранные монеты становятся временно недоступными, в то время как кошелек / клиент подделывает блок, а затем компенсирует участникам заработанные проценты по используемым монетам.

Чем дольше они владели своими монетами, тем больший «вес» они накапливают, и тем выше их шансы на подделку следующего блока, как только обнаружен блок, вес монеты сбрасывается, чтобы другие участники могли также добывать блок. Этот метод считается более безопасным, как если бы он был правильно распределен, участники аннулировали бы большинство любых видов атак, которые злоупотребляют мощностью хэширования, чтобы получить контроль над блочной цепочкой. Однако сначала нужно получить монеты, чтобы сделать ставку, которая, в зависимости от их стоимости, может быть дорогостоящей и в целом сдерживающим фактором для проекта, если это единственный доступный метод.

PoW / PoS Hybrid, известный обычно как «гибридный» метод распределения, перемешивает как PoW, так и PoS вместе с сингулярной блочной цепью. Гибридные системы по-прежнему относительно новы, так как в нескольких блочных цепях используется достаточно сложный алгоритм сложности, который регулирует временной интервал между сгенерированными блоками для PoW или PoS и в этом случае как в унисон. Для Espers был создан специальный алгоритм переназначения сложности, известный как «VRX», чтобы обеспечить правильную перетасовку сгенерированных типов блоков в полной гибридной блок-цепочке. Таким образом, безопасность Espers существенно возрастает, поскольку PoW и PoS восполняют недостатки друг друга, позволяя существенному фронту блокчейна работать исключительно по одному определенному методу.

Структура согласования и вознаграждения на момент написания данной статьи для проекта ESPERS описана ниже:

Время блокировки (после применения алгоритма VRX)

- Минимальное соблюдение интервала: 3,5 минуты на блок
- Расстояние между объектами: 5 минут на блок
- Максимальное (мягкий предел): 7 минут на блок

Proof-of-Work/ PoW

- Блок 0-10: 0 ESP на блок (начальные блоки *)
- Блок 11-365: 50 000 000 ESP на блок (зарезервированные блоки *)
- Блок 366+: 5000 ESP на блок + тарифы сети (стандартные блоки)

Proof-of-Stake / PoS

- Блок 2125-20 000: годовая процентная ставка 250% (2-дневный просчет *)
- Блок 20,001-2,000,800: 25% годовых (Стандартный этап)
- Блок 2,000,801-3,000,300: 5% годовых (масштаб 1-й фазы)
- Блок 3,000,300+: годовой процент 1% (Масштабирование 2-йфазы *)

- **Максимальное количество монет Espers**: 50 000 000 000 ESP (50 миллиардов ESP *)

Начальные блоки *: Относится к установке вознаграждения блока «0», так что первые несколько блоков цепочки могут анализироваться при их добыче без получения вознаграждения для майнера.

Зарезервированные блоки *: Изначально проект Эсперс отдал 20% со всего блокчейна в так называемый «Air-Drop» всем, кто хотел участвовать бесплатно, при этом, резервируя 5%, которые были распределены поровну между шестью членами команды, чтобы финансировать текущее развитие. Это было сделано в апреле 2016 года при запуске и перенесено в смену блочной цепи, которая была проведена вскоре после этого.

2-дневная ошибка в расчёте*: При запуске системы PoS в Espers первоначально было введено ошибочное значение для годового процентного уравнения, которое вычисляет вознаграждения за участие пользователя. Это привело к 2-дневной (48 часов) компенсации вознаграждений созданных PoS, но никоим образом не оказало существенного влияния на общее предложение / функцию, и эта ошибка была быстро решена. Было обработано 20 тысяч блоков, так как это было

первоочередным действием для того, чтобы запустить алгоритм VRX, и за это время цепь работала в ускоренном режиме по отношению к генерации блоков.

Масштабирование фазы №1 *: стандартная фаза вознаграждения PoS заканчивается после создания примерно 48 миллиардов ESP.

Масштабирование фазы №2 *: позже окончательный масштаб до 1% проводится достаточно близко к достижению максимального объема поставки монет.

50-Billion ESP *: максимальное количество монет ожидается примерно через 30 лет после запуска (2016-2046)

ПРЕДЕЛЬНАЯ СКОРОСТЬ УРОВНЯ X (VRX)

VRX или предельная скорость уровня X - это система перенаправления проблемных блокчейн - цепочек, которая, используя сканирование глубины в несколько блоков, быстро адаптирует реализованные уровни сложности «блокчейн / альткоин» или уровни сложности, чтобы обеспечить узкое окно вокруг желаемого времени блока. Разумеется, для некоторых проблем в блочном промежутке из-за значительного увеличения или уменьшения хэшрейтов /финансирования в зависимости от того, является ли блокчейн, основанный на Proof-Of-Work, Proof-Of-Stake или Hybrid, системе VRX гарантирует, что блоки генерируют последовательно даже в темпе. Кроме того, для гибридных блокчейн - цепей блоки должны перетасовываться в соотношении 50/50, что позволяет использовать оба типа согласования.

Просто поставьте индексы VRX на предыдущее заданное количество блоков (типичные эталонные реализации установлены на предыдущие шесть блоков), а затем сравните каждый из них друг с другом по отношению к их временным блокам, таким образом определяется заданное расстояние между этими блоками. Затем система принимает заданное расстояние между блоками и сравнивает его с желаемым интервалом между блоками в так называемом «Check Round». Этот Check Round похож на другие доступные системы перенацеливания, но настраивается по другой кривой, которая быстро адаптируется к большим изменениям в хэшировании блокчейна, а также не требует слишком многого, чтобы не «останавливать» работу блокчейна. Существует один Check Round для каждой пары индексированных блоков, поэтому с использованием глубины индекса на 6 блоков VRX будет выдано пять Check Round.

После того, как VRX выполнит свои проверки, он затем определит, должно ли оно изменить сложность либо вверх, либо вниз, в зависимости от того, было ли превышено требуемое время блокировки, серьезность которого ограничена максимальным удвоением предыдущей сложности блока или ее уменьшением вдвое. Наконец, среднее значение вычисляется между различными парами изменений сложности, так что происходит наиболее логичное изменение в сложности, которое наилучшим образом соответствует блочной цепочке и затем регистрируется системой Espers. **(См. Функциональную схему на следующей странице, на которой изображена фактическая функция).**

В поздних версиях VRX-систем (например, такая, как используется сейчас) существует уникальное колебание сложности PoW / PoS, в котором гибридные системы искажают трудности на кривой в пользу менее часто встречающегося типа блока. Это гарантирует, что ни один тип блока не сможет выиграть над другим, и оба (майнер и стейкер) могут принести пользу блочной

цепи одинаково. VRX был разработан для непосредственного взаимодействия с системой ограничений блоков Velocity Espers, которая более подробно обсуждается в следующем разделе. Это связано с тем, что никакой другой метод перенастройки трудности не был совместим с ним, поскольку сложность блоков играет важную роль в самой системе Velocity.

ESPERS

(Диаграма примера функции)

[Получение предыдущего блока - 1] → [Время блока прим. 07:00]

- 7 – минутный промежуток между блоками (mbs1)

[Получение предыдущего блока - 2] → [Время блока прим. 07:07]

- 9 – минутный промежуток между блоками (mbs2)

[Получение предыдущего блока - 3] → [Время блока прим. 07:16]

- 8 – минутный промежуток между блоками (mbs3)

[Получение предыдущего блока - 4] → [Время блока прим. 07:24]

- 5 – минутный промежуток между блоками (mbs4)

[Получение предыдущего блока - 5] → [Время блока прим. 07:29]

- 5 – минутный промежуток между блоками (mbs5)

[Получение предыдущего блока - 6] → [Время блока прим. 07:34]

Целевой промежуток = 5 минутный промежуток между блоками (mbsT)

[Проверочный круг 1] → [mbs1 > mbsT] → [Понижение]

[Проверочный круг 2] → [mbs2 > mbsT] → [Понижение]

[Проверочный круг 3] → [mbs3 > mbsT] → [Понижение]

[Проверочный круг 4] → [mbs4 = mbsT] → [Выравнивание]

[Проверочный круг 5] → [mbs5 = mbsT] → [Выравнивание]

Сравните действия, затем выберите наиболее подходящее действие

Понижение = 3

Выравнивание = 2

Понижение > Выравнивание

VRX понижает сложность майнинга/генерации блокчейна, чтобы соответствовать целевому промежутку

СИСТЕМА ОГРАНИЧЕНИЯ СКОРОСТИ БЛОКЧЕЙНА

Общая функциональность

Velocity - это переписанная функция, первоначально найденная в Frycoin (теперь старый биткоин основан на альткоине). Случайно наткнувшись на эту функцию, стало очевидно, что, хотя существенные разделы кода необходимо будет переделать, сама функция имела хорошую общую предпосылку как в аспектах безопасности, так и в стабильности цепи, что делает ее очень востребованной. Эта функция была успешно переписана, несмотря на несколько небольших неудач и ошибок в более ранних версиях, которые фактически не влияют на стабильность цепи или работу с монетами, как ожидалось в начале. Позже в разработке были созданы дополнительные системы, которые ранее не были частью оригинальной функции для правильной общей работы блокчейн.

Ключевая роль Velocity заключается в том, чтобы ограничить цепочку с параметрами, уже определенными внутри кода, вместо того, чтобы иметь межблочное расстояние и другие свойства, которые проявляются как реакция на работу цепочки. Другие реализации технологии блокчейн - внезапное увеличение хешрейта, которые могут определять возможную атаку, по-прежнему являются уязвимыми, несмотря на то, что системы перенацеливания с наилучшей сложностью реализуются для управления интервалом между блоками. Сетевые оплаты, возможные недопустимые проблемы с балансом при осуществлении транзакций и другие действия блокчейна выполняются с двойной проверкой, но все еще подвержены атаке, будь то временные или двойные траты. Всё это вызывает негодование у пользователей из-за потерь, которые являются неприемлемыми.

Проблема возможного использования параметров разрешается системой Velocity, являющейся «тройной проверкой». Даже после того, как блок во время генерации, по-видимому, подходит всем требованиям и затем генерируется, теперь он уже не просто принят. Вместо этого он проверяется еще раз на несоответствия и возможные другие баги. В первую очередь пользователи будут видеть отклоненные блоки во время майнинга или стекинга (или оба в зависимости от свойств монет). Несмотря на тенденцию предполагать, что что-то не так с цепочкой, поскольку оно отвергает блоки, это на самом деле абсолютно нормальная и приветствуемая операция.

Рассуждение заключается в том, что быстрые блокировки, неправильные оплаты, недостаточный баланс и другие проблемы могут управляться талантливым программистом со злым умыслом. Чтобы защититься от таких ситуаций, Velocity проверяет сгенерированный блок на параметры цепи. Сначала он проверяет блок на правильное расстояние, если блок был сгенерирован слишком быстро и из-за этого не выполнил один из основных параметров для цепочки, тогда он незамедлительно отклоняется, что предотвращает возможные атаки и любое внезапное увеличение хэшрейта.

Следующий шаг проверяет, что ранее клиент, осуществивший транзакцию (если она была сделана в предыдущем блоке), осуществил действительную транзакцию, сравнив предыдущий баланс с текущим балансом вместе с уплаченными комиссиями за минимальную плату, требуемую для оплаты блока, ожидающего принятия транзакции. Если какой-либо из этих параметров не выполняется (помните, что это стандартные параметры цепи и ничего необычного), тогда блок отклоняется, несмотря на то, что он успешно сгенерирован. Таким образом, эта система защищает

цепочку, делая ее более стабильной, предсказуемой и с общей надежностью, внушая уверенность в том, что принятые блоки действительно являются блоками, которые действительно защищают систему.

Эта функция все еще является прототипом системы. Его внедрение в блокчейн Espers (которая является полностью гибридной системой, использующей как PoW, так и PoS одновременно) вызвала небольшие сбои с исходной системой перенацеливания, которые были устранены путем перехода к ранее упомянутой системе перехвата VRX. Эти глюки состояли в том, что они затрудняли работу до тех пор, пока не будет использована надлежащая система перенацеливания. При этом принимаемые блоки теперь разнесены последовательно, как минимум, на 3,5 минуты, позволяя цепочке двигаться вперед плавно. Затем проверка транзакции и предыдущие проверки баланса в настоящее время отключены до тех пор, пока проверки не станут безупречными. Реализация этих конкретных проверок все еще разрабатывается для правильного определения этих разделов параметров цепи.

Анализ безопасности

Майнеры также могут создавать автоматические отсечки для системы, чтобы не тратить энергию, тогда как блоки просто не принимаются цепью, создавая два возможных эксплойта. Во-первых, пользователи с усовершенствованными системами интеллектуального анализа данных могут эффективно препроводить блок за время, когда цепочка не принимает блоки и не удерживает ее от представления до истечения минимального времени. Если затем система должна была использовать проверку безопасности, которая проверяет временную метку блока, чтобы узнать, удерживал ли майнер блок для представления другого эксплойта, то надо было установить удерживаемый блок, который должен быть создан с действительной меткой времени, чтобы майнер знал каждое допустимое время окна. Эти два эксплойта разрешаются сначала, если ранее установленный метод системы гарантирует, что временная метка блока не поступает из-за окна разрешенного блока. Это препятствует атакам, создавая дополнительные стадии сложности, которые должен пройти атакующий хакер, прежде чем иметь шанс на успех. Затем реализация VRX штрафует минимальное время блокировки, в результате чего мощность, необходимая для поддержания возможной атаки (даже при вводе правильной временной метки), увеличивается экспоненциально, пока только после нескольких генерируемых блоков сложность настолько велика, что минимальное время больше не может быть достигнуто, а другое майнер / стакер может просто найти следующий блок. Это быстро отрицает любой возможный прогресс в атаке. Конечно, система Velocity требует, чтобы удовлетворялись все параметры, а не просто соблюдались правила время блокировки для того, чтобы принять правильно сгенерированный блок.

Система может быть расширена, чтобы включать в себя больше проверочных функций и еще более строгую реализацию, которая может адаптироваться к любым добавленным или удаленным функциям. Это делает систему Espers очень адаптируемой и менее трудной для работы, поскольку она может расти вместе с монетой и по мере того, как она становится более совершенной и зрелой. Поэтому новая функция безопасности называется Velocity (англ. Скорость).

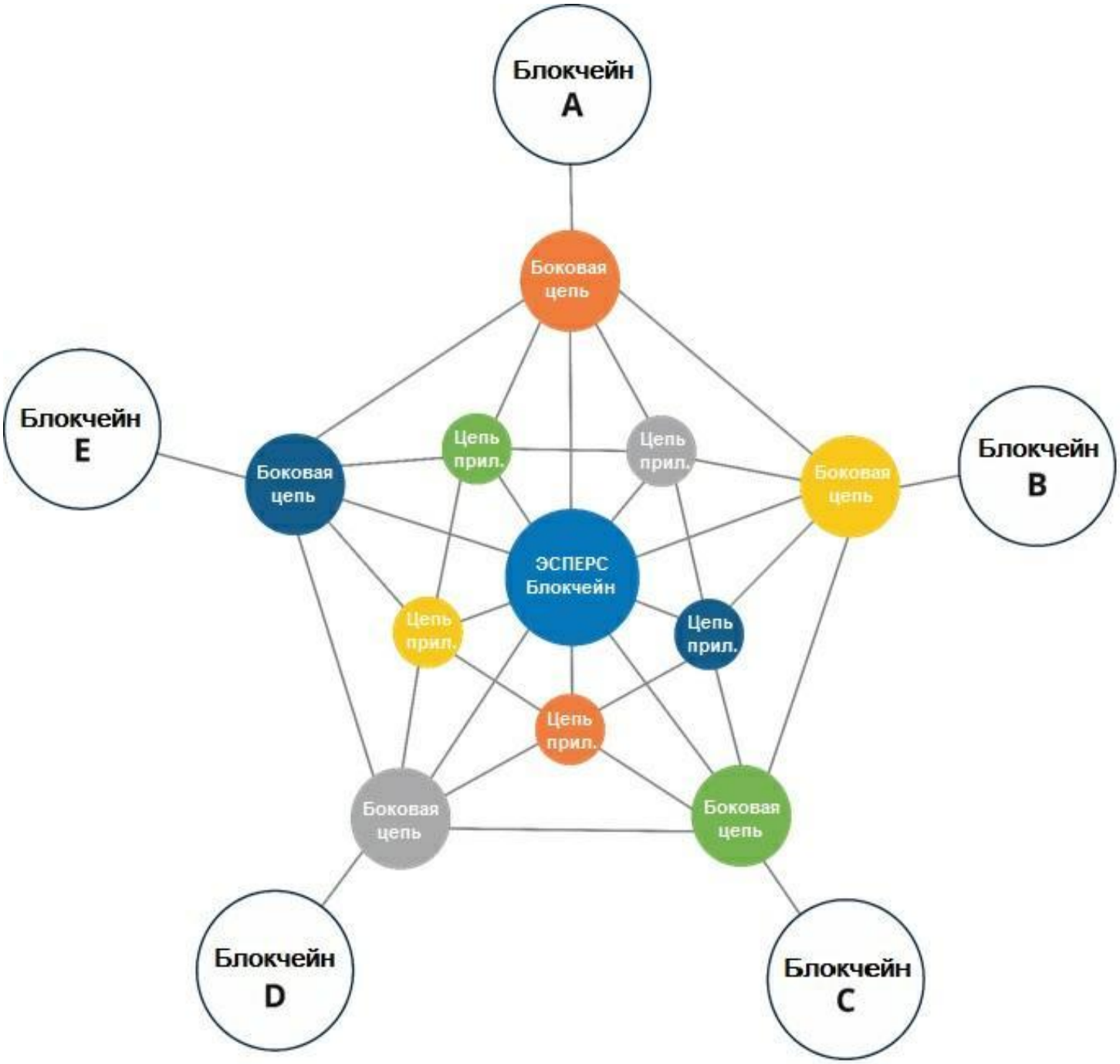
ИНТЕРФЕЙСЫ SIDECHAIN & CROSS-CHAIN

В то время как один блокчейн вполне способен обрабатывать большие объемы информации, возникли новые методы, когда система блокчейн будет использовать более мелкие блок-цепи, которые зависят от первоначальной цепочки, которая ее создала, называемой связующими звеньями, чтобы одновременно обрабатывать больше данных, одновременно уменьшая нагрузки на сеть в любой конкретной цепи. Это создано для того, чтобы основная цепь взаимодействовала с боковыми цепями напрямую, имея боковую цепь, полностью зависящую от основной цепи. Подход Espers заключается в том, чтобы боковые цепи оставались способными функционировать совершенно независимо. Эти боковые цепи, которые когда-то были созданы, продолжают функционировать без требования существования сети Espers. Использование межсетевого интерфейса для передачи данных от одной блок-цепи к другой позволит каждой цепочке иметь возможность совместно использовать рабочие нагрузки, оставаясь полностью независимыми. Эта независимость означает, что не смотря на какие-либо сбои или проблемы с данной цепочкой, остальная часть сети останется неповрежденной и работоспособной, а не потерпит полный крах. Использование этой системы даже позволяет полностью взаимодействовать с другими проектами и сообществами, позволяя нескольким проектам объединяться и приносить пользу друг другу, если сообщества захотят это сделать.

Например, если проект, способный шифровать сообщения и распределение монеты, обрабатывает только транзакционные данные для монеты с блочной цепочкой «A» при обработке только текстовых данных сообщения с блочной цепочкой «B», каждая блок-цепочка должна обрабатывать свои соответствующие службы. Затем, используя межцепочечное взаимодействие, продукты могут обмениваться данными друг с другом, предоставляя конечным пользователям текущую и интуитивно понятную систему, которая быстра, надежна и безопасна. Чтобы уточнить этот пример - если блок-цепь «A» была гипотетически поставлена под угрозу, блок-цепь «B» остается функциональной, и ее службы также будут продолжать правильно функционировать, предоставляя пользователям возможности использовать службы, которые им нужны, даже если один или несколько элементов больше не доступны. Этот тип системы также помогает проекту блокчейн освободиться от стереотипа предлагать только один тип сервиса.

Обратитесь к рисунку A для визуальной иллюстрации предлагаемой системы.

ESPERS


Блокчейн
A
Боковая
цепь
Блокчейн
E
Боковая
цепь
Цепь
прил.
Цепь
прил.
Боковая
цепь
Блокчейн
B
ЭСПЕРС
Блокчейн
Цепь
прил.
Цепь
прил.
Цепь
прил.
Боковая
цепь
Боковая
цепь
Блокчейн
D
Блокчейн
C

БЕЗОПАСНЫЙ ОБМЕН СООБЩЕНИЯМИ

Фактически было несколько различных попыток реализовать -Secure Messaging- в проектах блокчейн. К сожалению, мало кто из них использует алгоритм цепочки для шифрования сообщений. Чтобы обеспечить быструю доставку, сообщение фактически не привязывается к блокчейну, а, скорее, к закрытому ключу, в котором отправляется содержимое сообщения, и из которого они могут быть прочитаны. Учет очень быстрых ретрансляций сообщений без необходимости добавлять нагрузку к сети блокчейн - умное решение. Тем не менее, правильная реализация безопасного обмена сообщениями должна будет транслировать сообщения через узлы, используя саму блок-цепочку, как это обычно сделал бы майнинговый блок.

Сохраняя исходный текст в блоке, подобно тому, как блок генезиса биткоинов содержит заголовок статьи новостей, сообщения могут быть более безопасными, чем просто быть зашифрованными и отправляться получателю. Это связано не только с тем, чтобы шифровать сообщение через алгоритм шифрования, но также и с возможностью подтвердить, что отправленное / принятое сообщение действительно успешно отправилось. Разрешение сообщения подтвердить его достоверность работает таким же образом, как и транзакция, подтверждает ее достоверность в блочной цепочке, гарантируя, что сообщения, полученные и отправленные, содержат только то, что они должны были содержать. В некоторых случаях фальсифицированные или даже спам-сообщения значительно сокращаются или даже полностью аннулируются.

Хотя содержимое сообщений остается конфиденциальным, по соображениям прозрачности, блок-цепочка все еще сообщает, когда отправляется сообщение и какой у него ключ открытия. Тем не менее, получатель и отправитель являются единственными, кто связан с контентом, так как публично видно только заметку, сделанную в цепочке о том, что было отправлено сообщение вместе с открытыми ключами, которые уже обычно доступны. Прозрачность требуется для любого рода переноса данных, независимо от того, используется ли она для монет или для другого типа обслуживания. Это связано с тем, что без прозрачности он становится очень запутанным, чтобы убедиться, что получатель действительно получил предполагаемый метод обслуживания, поскольку цепочка не может правильно зафиксировать предпринятые действия.

Продолжая, помимо включения текста в качестве содержимого сообщения, система обмена сообщениями Espers также предназначена для обработки и распространения всего - от базовых изображений до сжатых файлов и документов, что позволяет его пользователям выйти за рамки стандартного ограничения только текста. Для достижения вышеупомянутой системы боковой цепи и межцепочечного взаимодействия используется интерфейс. Когда Espers является катализатором обработки текстовых данных своими другими боковыми цепями, он непосредственно взаимодействует с блочной цепью Espers, а также с другими отдельными боковыми цепями, чтобы одновременно обрабатывать другие данные, одновременно сохраняя свет сетевой нагрузки. Это делается для того, чтобы удалить центральную точку отказа из системы, обеспечивая при этом большую гибкость служб. Например, если пользователь «A» отправляет сообщение пользователю «B» в блок-цепочке Espers, которое содержит стилизованные текстовые

данные, а также несколько изображений, сообщение будет фактически разделяться и обрабатываться одновременно в разделах.

Выйдя за цепь Espers, используя сетевое взаимодействие, система также может напрямую взаимодействовать с другими проектами и их сообществами, объединяя их, позволяя пользователям из одного сообщества напрямую взаимодействовать с другим. Если два пользователя участвующих блочных цепей хотят отправлять сообщение от своего локального кошелька / клиента на кошелек / клиента другого пользователя, независимо от того, является ли он той же цепочкой, сообществом или проектом, они это могут с легкостью делать. Это разрушает разделение между сообществами и позволяет получить более высокую возможность реального использования от систем, которые в настоящее время существуют и которые все еще создаются. Каждая цепочка обрабатывает сообщения с оплатой, выплачиваемой каждой из их сетей, и их сообщества заинтересованы в обработке блоков.

Ключевым преимуществом является то, как это влияет на цель системы Espers. Отдельные организации, например, компании, могут удобно и эффективно запускать автономные блок-цепи для собственных нужд, таких, как межсетевые обмены сообщениями и обработка данных, которым требуется безопасность/ зашифрованность объекта. Эта межсетевая связь позволяет взаимодействовать с другим отделом или совершенно другим объектом, сохраняя при этом конфиденциальность и индивидуальную безопасность.

SITE-ON-CHAIN

Существующие интернет-протоколы, включая SSL и TLS, все еще оставляют желать лучшего. Веб-сайты, серверы и даже персональные компьютеры скомпрометированы почти бесчисленное количество раз в день, даже при использовании лучших практик и протокола безопасности. Это связано с тем, что большая часть трафика, который проходит через всемирную сеть, не шифруется и не защищается. Более авторитетные веб-сайты и компании обязательно используют какое-то шифрование для трафика со своими веб-сайтами, но даже тогда скомпрометированный сервер или сеть могут привести к сбою всей системы, что может поставить под угрозу информацию о клиенте, информацию о бизнесе и другие конфиденциальные данные.

В ответ на это затруднительное положение проект Espers предполагает, что веб-сайты и другие интернет-сервисы будут управляться / храниться / размещаться через блок-цепочку, тем самым почти отрицая любую возможную атаку на веб-сайты и другие интернет-сервисы, даже не влияя на удобство использования. При использовании блок-цепи в качестве интернет-протокола вы фактически добавляете почти непроницаемый уровень защиты для любого вида обслуживаемых сервисов, особенно веб-сайтов. Идя дальше, просто добавляя уровень безопасности, веб-сайт с блочной цепью не имеет возможности страдать от DDOS-атаки, так как нет никаких серверов или центров обработки данных для компрометации, нет файлов для «взлома», без хостинга, чтобы беспокоиться, никаких головных болей домена, нет проблем с хранением данных для перехвата и т. д. Чтобы достичь этой высокой цели, ранее обсуждавшиеся функции все используются в унисон, чтобы создать правильно отображаемый веб-сайт для любого пользователя через любой участвующий блокчейн проект.

Сначала принимающая сторона загружает свой веб-сайт через клиента Espers, который быстро преобразует файлы в исходный код и сохраняет его в индексированных блоках на блок-цепочке. Отдельные боковые цепи используются для хранения каждого типа информации, чтобы типы кода, изображения, видео и другие данные не насыщали какую-либо данную цепочку. Когда хостинг-сторона отправляет свой сайт на блок-цепочку, они также платят небольшую плату за сеть, чтобы обрабатывать данные с помощью блок-цепи, как и при оплате транзакционной комиссии за отправку транзакции. Эта плата имеет номинальную сумму и существует просто, чтобы заплатить достойную компенсацию любому майнеру или стейкеру, который мог бы обработать блок. После того, как данные, которые были обработаны на блоке, и блок был подтвержден, он становится доступным для всего сообщества, используя систему Espers и любые другие участвующие системы.

При просмотре веб-сайтов клиент Espers запрашивает каждую цепочку для своего заданного типа данных и визуализирует ее на стороне клиента для взаимодействия с пользователем. Это означает, что любой вид веб-браузера всегда основан на сеансе и не отображается другим лицом или сторонним пользователем. Любая информация, обрабатываемая между веб-сайтом и пользователем, также защищена вместе со всей информацией, просматриваемой пользователем, с доступом к цепочке отчетов и другими переменными использования, которые должны храниться в аналитических целях. Таким образом, служба просмотра веб-страниц, такая как Google, может отправить свой собственный браузер, который затем просканирует цепочку для сайтов, размещенных на ней, в некотором смысле, не предлагая никакой временной разницы между нашей нынешней интернет-системой и тем, что можно фактически назвать " интернет 3.0 ", сохраняя при этом безопасный и наглядный опыт.

Используя систему межсетевых интерфейсов, Espers может быть соединена с будущими проектами единомышленников, чтобы, вместо создания подразделения, пользователь мог просматривать веб-сайты, хранящиеся в системе другого проекта, целиком из системы клиентов Espers и блок-цепи, в то время как, фактически оставаясь полностью независимым, чтобы не допустить риска сбоя цепи взаимосвязанного проекта, влияющего на используемую в настоящее время систему пользователя. Это поощряет единство, позволяя стандартизировать, исходя из необходимости создания собственной системы.

СЕТЕВОЙ / МОБИЛЬНЫЙ BLOCKCHAIN

По мере роста блокчейна, он становится «более тяжелым» в том смысле, что он постоянно хранит информацию без учета возможных ограничений аппаратного обеспечения или обслуживания для конечного пользователя. Чтобы обойти такую озабоченность для возможных мобильных пользователей или пользователей, которые просто не могут хранить всю цепочку либо в этот момент / на неопределенный срок, важно предложить альтернативу тому, что известно как «полный» клиент. Стандартные или «полные» клиенты хранятся в общедоступных хранилищах и проверяют всю блок-цепочку, которая позволяет значительно уменьшить количество резервирования и поддержки, поскольку члены сообщества / пользователи используют систему, в то время как «Легкий» или «Мобильный блок-код» действует как портал доступа, запрашивая блок-цепочку и вытаскивая данные из него. Это больше похоже на блок-браузер, а не на фактическое хранение системы локально.

Не сохраняя большинство файлов локально, систему Espers можно удобнее использовать в полной мере на мобильном устройстве или пользователем с ограниченными возможностями сети / хранилища. Хотя большая часть того, что делает эту систему легким, просто сканирует блок-цепочку, она также, конечно, имеет возможность отправлять данные в блок-цепочку, которая будет обрабатываться в предстоящем блоке с или без синхронизации блок-цепи. Каждая система должна позволять быть настроенной пользователем, который ее использует, и, таким образом, Сетевой / Мобильный Блокчейн также может синхронизировать либо частично, либо целиком. Если опция выбрана, система будет синхронизироваться с последней контрольной точки и «предполагать», что предыдущие транзакции, о которых сообщают цепочки, размещенные узлами, действительны. Другой вариант - иметь «тихую» полную синхронизацию для запуска, где после завершения полусинхронизации с последней контрольной точки клиент начинает синхронизировать остальную блокировку в фоновом режиме, позволяя пользователю полностью поддерживать сеть на свое усмотрение.

CHAIN ПРИЛОЖЕНИЯ

Поскольку система блокировки Espers предназначена для использования боковых цепей и модульных функций, «Chain Apps» относится к способности проекта подключать любое приложение с привязкой к блочным цепям в себя и наращивать возможности. Некоторые из этих цепных приложений исходят из проголосовавших функций X-Node (об этом далее в следующем разделе), а другие - от сторонних сторон, проверенных до внедрения в систему. Созданные пользователем сетевые приложения могут быть отправлены в любое время через системного клиента и затем будут быстро обработаны для назначения уникальной боковой цепи для ее использования.

УЗЛЫ-X

X-Nodes не следует путать с Masternodes, которая является централизованной системой, в которой пользователи блокируют определенный баланс, чтобы участвовать в дополнительных сетевых функциях и поддерживать их, а затем, вознаграждая участника некоторыми из

сгенерированных монет из следующего блока, если они имеют на это право. Вместо этого X-Nodes полностью исключают, что любой член сообщества может участвовать в системе независимо от их текущего баланса или предыдущего опыта. Это гарантирует, что аспект децентрализации проекта Espers и блок - схемы в целом не утрачиваются, еще раз усиливая общую сеть.

Способ работы X-Node заключается в том, что участник регистрируется в сети в качестве дополнительного процессора данных, позволяя им хранить дополнительные боковые цепи, которые используются для обеспечения дополнительных функций цепочки. Как и в Masternode, X-Node требует постоянного подключения к Интернету и наказывает любого участника, который последовательно отключается, чтобы избежать несовместимых подключений или любых возможных зависаний в сервисе, предоставляемом конечным пользователям. Чем дольше пользователь находится в системе, тем выше вероятность того, что они станут частью компенсированных X-узлов, которые автоматически проголосовали за сеть в зависимости от надежности и обработки данных. Участвующий пользователь может также блокировать любую желаемую сумму своего баланса, которая будет эффективно замораживаться, поскольку участник больше не сможет делать ставку до тех пор, пока они не будут разблокированы с X-узла, и при этом баланс будет действовать как множитель для предусмотренного коэффициента компенсации. Разумеется, множитель находится на кривой и реализует несколько систем борьбы с поломками, например, требуя периода охлаждения для недавно заблокированных монет. Пока не остынет, участник не увидит эффект множения. Чем меньше блокировка, тем дольше пользователь должен ждать, пока блокировка остынет с экспоненциальной скоростью. Большие балансы требуют от пользователей ждать меньше времени, чтобы остыть, имея множитель на экспоненциальной кривой. Это отрицает полезность значительно больших балансов, гарантируя, что пользователям предлагается блокировать большие суммы, которые будут вознаграждены раньше, при этом наказывая возможную блокировку «пыли» до такой степени, что это становится непрактичным.

Заблокированный баланс по-прежнему сможет найти следующий блок в цепочке, однако любые созданные монеты переадресовываются (после блокировки охлаждения) на голосование выбранного участника. Голосование в сети, таким образом, имеет решающее значение для быстрого создания функциональных возможностей проектной группой и повышает поддержку сообщества. Участники могут также выбрать просто «не голосовать», однако аспект множителя снова наказывается, поскольку это создает снижение поддержки новых сетевых функций. Любой участник может подать запрошенную функцию, за которую можно будет проголосовать в сети для будущего развития, однако, когда раунд голосования заканчивается, любое голосование по объектам, которые не были выбраны, объединяется вместе и разбивается на два раздела, которые затем используются независимо. Первая половина разделена на секции, которые затем перетекают обратно в сеть, поскольку сборы выплачиваются, позволяя майнерам и стакерам получить небольшой «бонус» до тех пор, пока баланс не закончится, а вторая половина будет выставлена на выигрыш, проголосовавший за функции. Пользователи могут разблокировать свой баланс в любое время, участвуя в системе X-Node, даже если баланс не завершил период охлаждения, дающий пользователям полный контроль над своим опытом. Аналогично, если участник отказывается в любой отрезок предоставленного ему времени, как и если бы он не отказывался, участник повлечет за собой еще одно охлаждение между деактивацией и разрешенным временем реактивации. Кроме того, система X-Node является наглядно понятной и позволяет одним щелчком мыши удалять возможную ошибку пользователя, которая часто встречается со схожими функциями, такими, как Masternodes, и заменяя ее интересами

пользователя / иммерсией. Это также требует значительной нагрузки от потребностей в поддержке, несоответствий в сети и общей сложности работы или участия в системе.

ЭСПЕРС

ТРАЕКТОРИЯ ДВИЖЕНИЯ

Q4 2017

- Обновление сайта
- Проверка блок-цепей PoW&PoS
- Обновление кошелька
- Маркетинговая компания (активная)

Q1 2018

- Техническая документация
- Мобильный кошелек
- Легкий клиент

Q2 2018

- Узлы X
- Боковые цепи
- Система оповещения

Q3 2018

- Цепь приложений
- Поперечная цепь
- Размещение цепей

ESPERS

Встречайте нашу команду

Идеальное сочетание креативности и волшебства разработки

CRYPTOCODERZ

Jonathan Zaretsky

Главный проект-менеджер
Разработчик

ARSONIC

Guillaume Huot

Главный Web-разработчик
Графический дизайнер

MONOXIDE

Ассистент проект-менеджера
Связь с общественностью

BBOBB

Проектная логистика

CTGIANT

Помощник разработчика

ARCADE

Justin Cappellini

Связь с общественностью

BATYSTA

Antonio Batista

Проектная логистика

ESPERS

ЗАКЛЮЧЕНИЕ

Этот технический документ (документ) предназначен только для информационных целей, а не для обязательного исполнения. Не полагайтесь на эту информацию при взаимодействии с монетами Espers, так как в конечном счете разработка и выбор времени остаются по собственному усмотрению команды Espers / CryptoCoderz.

Мы, команда Espers / CryptoCoderz, ни в коем случае не намерены наносить вред никому в любой форме. Никогда не было целью массовой продажи монет, предпродажи или любого другого метода финансирования широких масс, используемого для проекта Espers / CryptoCoderz или его разработчиков. Пожалуйста, поймите, какие риски связаны с криптографической технологией блокчейн и их соответствующими монетами. Команда Espers / CryptoCoderz не может нести ответственность за любые потерянные, украденные или иным образом отсутствующие средства любого вида. Если вы не уверены или имеете какие-либо сомнения в отношении этого проекта, мы настоятельно призываем вас НЕ инвестировать или участвовать в этом, поскольку это прототип технологической системы, как указано во многих областях, и может использоваться на свой страх и риск.

У нас нет связи с продуктом Yobit под названием «Espers». Это отдельный продукт, исключительно управляемый Yobit.

БЛАГОДАРНОСТЬ

Большое спасибо всем, кто помог воплотить этот проект в реальность, особая благодарность предоставляется следующим членам сообщества (юзернеймы), которые внесли вклад в создание и редакцию этого документа:

CafeConTiki

IPandamonium

Kevinboerland

Bit010

CryptoCarrot

cXplexus

Eugen

Gandalf86

IK

Tekna

Vin

Wolf