RUS

A. Вступление

Каждая страна за длительный период своего существования накопила большой опыт в различных областях науки, техники, культуры и повседневной жизни. В мире много умных и талантливых людей, которые передают свои знания из поколения в поколение, но многое потеряно или недоступно другим по разным причинам. Есть много людей, которые хотят не только передать своим детям, но и рассказать о чем-то всему миру. Так же, как в мире исчезают редкие животные, и будущее поколение их даже не вспомнит и не сможет увидеть, как они выглядели (например, мамонты и динозавры). В истории мы постоянно пытаемся восстановить информацию, но давайте подумаем о ее сохранении.

Думаю, каждый из вас задумывался о том, что будет в будущем, возможно, вы хотели перенести в будущее хотя бы частичку себя. Это как послать сообщение будущим поколениям, передать свои мысли, свое творчество и, в целом, себя. (например, музыканты, художники, мыслители и изобретатели). Мы знаем о них только потому, что бережно их хранили.

Во все времена были разные народы и страны. Между этими странами всегда были границы и контроль. С появлением Интернета границы и контроль постепенно стираются. В настоящее время почти каждый использует Интернет для получения новой информации и знаний со всего мира. Информация становится доступнее для всех.

Люди всегда общались друг с другом, где бы они ни находились. Использовал почту, телеграф и электронную почту для общения с близкими и для делового общения. Важность доставки и вопрос конфиденциальности был и остается важным вопросом для всех.

Для решения этих вопросов создан проект «Infinium».

B. Цель

Основная цель - хранить информацию и передавать сообщения с использованием передовых технологий криптографии и блокчейна. Наш проект сможет хранить информацию в зашифрованной базе данных, которая будет контролировать целостность хранимых данных. При сохранении информации высота блока будет фиксированной для отслеживания времени поступления информации. Безопасная передача сообщений от пользователя к пользователю. Используя современные технологии (узлы) «Infinium» будет доступен в любом уголке мира.

C. Проблема - бесконечного количества монет и объем базы данных

Это не проблема, а преимущество. Точнее, бесконечность - это наша жизнь. Жизнь человечества бесконечна, пока живы люди.

Золото всегда добывали и продолжают добывать по сей день для обмена на другие ценности. Золото тоже можно считать бесконечным, но получить его становится сложнее. Чем больше рабочих добывают золото, тем больше рабочим нужно платить. В нашем проекте для вознаграждения рабочих (майнеров) используется формула ($\log_2$(сложность)*2^40)/2. Чем больше работников, тем больше вознаграждение за блок.

Количество монет будет расти бесконечно, но медленно. Общий объем монет будет постоянно уменьшаться из-за платы за хранение. Например: я музыкант и хочу сохранить свою музыку и тексты, поэтому мне нужно потратить несколько монет на хранение. Эти монеты не переходят в общий объем монет, а удаляются из доступных монет. Таким образом уменьшит количество монет в обращении. В то же время в базу данных добавляется нематериальная ценность.

В настоящее время объем дисков огромен и в будущем размер будет увеличиваться, поэтому вы можете не беспокоиться о том, что монета бесконечна. Объем будет расти медленнее, чем скорость развития технологий (размер жесткого диска).

Поскольку монета бесконечна, у людей в будущем всегда будет возможность добавить информацию в хранилище.

D. Виды информации для сохранения

Основные виды информации для человека которые доступны с нашими технологиями это текст, фото и музыка. Поэтому в базе данных будут сохраняться именно они.

1. текст
2. фото
3. музыка

Также будет выделено место в блокчен для записи текстовой информации. О специфике данной информации будет рассказано ниже.

E. Область применения

Информация в базе данных

1. Текст — Произведения искусства, технические описания, стихи, тексты собственного сочинения, высказывания мудрых людей, послания для будущих поколений и все, что можно описать в текстовой форме.

2. Фото — логотипы компаний, фотографии знаменитостей и обычных людей, картины художников и все, что можно сфотографировать.

3. Музыка — Произведения ваших любимых композиторов, музыка вашего собственного сочинения, для диджея / музыкантов и все, что можно записать на аудио.

При загрузке данных дата (высота блока) будет фиксированной. Это необходимо для того, чтобы можно было видеть, когда была сделана запись. Например: музыкант написал музыку и хочет защитить свои права как первоисточник.

Информация в блокчейн

1. Учет количества монет
2. Контроль передачи монет другому лицу или оплата хранения информации
3. Шифрование и дешифрование данных.

Выделено дополнительное место для людей, которые хотят записывать какие-либо данные. Например: я хочу контролировать целостность базы данных или любой другой информации. Я могу сохранить хеш-функцию своих данных непосредственно в блокчейне, чтобы дополнительно проверить целостность моих личных данных.

Передача сообщений

1. Передача сообщений — актуально для всех

F. Варианты доступа к информации

1. Информация доступна каждому без ограничений.
2. Информация доступна каждому без ограничений, но после определенной даты (высоты блока). Например: я записал текст и хочу, чтобы все могли видеть текст только после блока № 5 000 000.
3. Информация доступна человеку или группе людей, владеющих кошельком. Кошелек будет как ключ к открытию скрытой от всех информации. (зашифровано закрытым ключом кошелька)

Например: человек / группа людей могут использовать его как хранилище конфиденциальной информации. Если человек / группа хочет открыть его для всех, они могут опубликовать свой кошелек для всех или создать новое сообщение для всех. Пункт 1. (Для чтения конфиденциальной информации достаточно иметь кошелек / ключ даже при нулевом балансе)

4. Информация, записанная в блокчейн, доступна каждому, поскольку она открыта. Истинную цель знает только создатель этой записи.
5. Сообщение может быть прочитано только пользователем, которому оно предназначено. Шифрование и дешифрование происходит с использованием ключа пользователя.

G. Отличие от других видов блокчейн/монет

Например Биткойн - 21000000 штук. Монеты ограниченного количества. Многие монеты биткоин были потеряны по разным причинам. Это означает, что реальная сумма будет намного меньше. Цена в будущем вырастет. Кто-то (группа людей / страна) в конечном итоге сможет получить большую часть монет и контролировать весь мир, если все будут использовать только биткоин в качестве стандарта. Кроме того, каждая транзакция отслеживается, и можно вычислить человека с монетами. Биткойн хранит только данные транзакций и не приносит пользы всем.

Другие монеты содержат большое / бесконечное количество монет, но их трудно использовать обычным людям. Использование контрактов и других технологий, которыми обладают только специалисты в этой области.

В отличие от таких видов. Наш вариант более безопасен от отслеживания и обеспечивает большую конфиденциальность. Легко использовать людям даже без специального образования. Бесконечное число позволяет будущим поколениям использовать технологии так же, как сегодня. Мы не ограничиваем наших детей, внуков, правнуков количеством монет или узкой специализацией ... мы передаем свои знания и опыт ...

Ценность нашей монеты заключается в самой информации, которую человек может записать в базу данных / блокчейн. Владение монетами позволит человеку сделать «бессмертное» послание для всех в настоящем и для будущих поколений.

В настоящее время владение любой информацией / технологиями может стоить 1000 биткойнов. Иногда бывает, что человек знает очень важную информацию и хочет поделиться ею со всем миром, но не знает, кому ее передать, чтобы все знали или хранили ее долгие годы. Наш проект «Infinium» поможет в этом. Способ письма и чтения будет простым для всех. Со временем такой информации будет больше. Каждый захочет что-то написать или прочитать в нашей базе данных и блокчейн. Ценность информации и способность записывать ее со временем только возрастут.

H. Сообщение будущим поколениям

Будьте четными с собой и окружающими, так вы оградите себя от лжи. Вы быстро сможете отличать истину от лжи. 0-ложь 1-истина — не будьте нулем в жизни. Даже одна единица может все изменить. Стремитесь к знаниям и делитесь ими. 313

I. О сети и исходном коде

1. Основное объяснение

Infinium - это криптовалюта, ориентированная на конфиденциальность, с возможностью хранения данных. Он основан на протоколе Cryptonote. Cryptonote - это протокол для построения децентрализованных сетей блокчейнов с абсолютной анонимностью, никто не может видеть детали транзакции, только отправитель и получатель. Анонимность осуществляется с помощью кольцевых подписей, кольцевые подписи представляют собой сложную схему, в которой для проверки требуется больше открытых ключей. В случае кольцевой подписи у нас есть группа лиц, каждый со своим секретным и открытым ключом. Утверждение, подтвержденное кольцевыми подписями, состоит в том, что подписавший данное сообщение является членом группы. Основное отличие от обычных схем цифровой подписи заключается в том, что подписывающей стороне требуется один секретный ключ, но проверяющий не может установить точную личность подписывающей стороны. Следовательно, если вы столкнетесь с кольцевой подписью с открытыми ключами Алисы, Боба и Кэрол, вы можете только заявить, что подписавшим был один из этих лиц, но вы не сможете точно определить его или ее. Эта концепция может использоваться для того, чтобы сделать цифровые транзакции, отправленные в сеть, не отслеживаемыми, используя открытые ключи других участников в кольцевой подписи, которая будет применяться к транзакции. Такой подход доказывает, что создатель транзакции имеет право потратить сумму, указанную в транзакции, но его личность будет неотличима от пользователей, чьи открытые ключи он использовал в своих кольцевых подписях. Следует отметить, что внешние транзакции не ограничивают вас от тратить собственные деньги. Ваш открытый ключ может присутствовать в десятках кольцевых подписей других людей, но только как фактор путаницы (даже если вы уже использовали соответствующий секретный ключ для подписания собственной транзакции). Более

того, если два пользователя создают кольцевые подписи с одним и тем же набором открытых ключей, подписи будут разными (если они не используют один и тот же закрытый ключ).

2. Доказательство двойной траты.

Многие из вас могут подумать, что при полностью анонимных платежах могут возникнуть проблемы, когда пользователь сможет потратить одни и те же монеты несколько раз, что, конечно, несовместимо с принципами какой-либо платежной системы. Но протокол cryptonote для этого готов. Кольцевая подпись - это класс криптоалгоритмов с различными функциями. Cryptonote использует модифицированную версию «отслеживаемой кольцевой подписи» и преобразовывает отслеживаемость в возможность связывания. Это свойство ограничивает анонимность подписывающего следующим образом: если он создает более одной кольцевой подписи с использованием одного и того же закрытого ключа (набор внешних открытых ключей не имеет значения), эти подписи будут связаны вместе, что указывает на попытку двойного расходования. Когда-то он использовался в протоколе cryptonote, поэтому пользователи могли совершать двойные траты, поскольку в ключевом изображении в cryptonote используется эллиптическая кривая ed25519, и его можно изменить особым образом, что позволило удвоить траты. Эта ошибка была исправлена в Infinium в версии v2.0.0.

3. Сеть.

Infinium использует сеть P2P для синхронизации блоков между узлами. Блоки являются частью цепочки блоков, в которой хранятся транзакции и данные. Все блоки содержат транзакцию coinbase, которая представляет собой эмиссию новых монет для валидаторов PoW (в современную эпоху в основном пулы майнинга) и другую транзакцию, не связанную с монетой, которая может быть транзакцией передачи монет или транзакцией хранилища данных. Сеть Infinium нацелена на разблокировку блоков примерно за 90 секунд, поэтому, если к сети присоединится больше валидаторов PoW, сложность разблокировки блока возрастет. Сеть рассчитана на сложность из 720 среднего времени разблокировки блока. Каждый узел сохраняет p2pstate, в котором записываются все соединения с другими узлами, которые этот узел имел во время своего существования. Когда узел запускается, он будет пытаться подключиться к узлам из своего p2pstate. Но когда вы полностью новый узел, вы будете использовать жестко запрограммированные начальные узлы. Это узлы, которыми управляет команда разработчиков Infinium, которые предназначены для первоначального подключения к сети Infinium.

4. Хардфорк Infinium 2.0.0+.

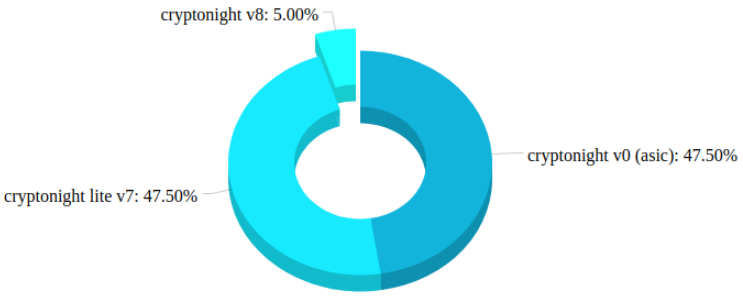
Это хардфорк от 4 ноября 2020 года, который изменил все в истории Infinium. Все старые транзакции были сохранены, и старые пользователи смогли восстановить свои кошельки с помощью экспортера старых ключей, который может экспортировать ключи из вашего старого кошелька и использовать его с более новыми версиями Infinium. Вам нужен этот экспортер, потому что новая версия Infinium использует алгоритм ChaCha8 для шифрования закрытого и открытого ключей в кошельке. Еще одним изменением в хардфорке было уменьшение вдвое вознаграждения за блок, поскольку вознаграждение за блок Infinium контролируется хешрейтом сети, вы можете найти формулу в C. Но сегодня есть гораздо более мощные устройства, чем тогда, когда Infinium был запущен в 2014 году. можно было майнить Infinium с помощью CPU, например, в то время самый топовый CPU в линейке - Intel Core i7 5820k имел около 190 H / s вычислительной мощности при майнинге Infinium. Но времена изменились, и теперь мы используем ASIC-майнеры, которые представляют собой устройства с чипами, предназначенные для майнинга этого одного конкретного алгоритма и делают это очень быстро. Например - antminer X3 имеет около 240 000 H / s, так что это было необходимо. Следующие улучшения касались скорости синхронизации и расчета общего предложения Infinium, потому что старая кодовая база была плохо написана, а переменная с общим предложением была переполнена. Кроме того, в новый Infinium добавлена поддержка семени BIP39, чтобы ваш кошелек легко запоминался. Новый хардфорк основан на протоколе cryptonote от bytecoin v3.4.2, спасибо команде Bytecoin.

5. **Хардфорк Infinium 3.0.0+.**

Этот хардфорк распределил равенство между майнерами и помог защитить сеть на будущее.

1. (Multiple PoW) Множественное доказательство работы.

С этого времени в сети Infinium активны различные алгоритмы майнинга. Мы хотим использовать все группы майнеров (CPU, GPU, FPGA, ASIC) для максимальной децентрализации сети Infinium. Проценты для каждого заполненного алгоритма указаны на диаграмме справа.



1.1) Как мы выбрали эти алгоритмы ?

Как я уже писал ранее, мы хотим равенства между всеми группами майнеров, поэтому мы сохранили оригинальный cryptonight v0 в качестве алгоритма для майнинга ASIC. Этот алгоритм проверен временем и, как известно, работает без каких-либо нежелательных ошибок. В качестве второго алгоритма мы выбрали cryptonight v8 для майнинга FPGA, этот алгоритм также проверен временем, и известно, что он работает без проблем, он был реализован в крупнейшем проекте Cryptonote (Monero), поэтому его безопасность гарантирована. Вы можете сказать, почему мы устанавливаем только 5% блока для майнинга с помощью этого алгоритма. Отличный вопрос, большую часть времени на других монетах хешрейт майнинга переходит на несколько ферм FPGA, которые могут писать битовый поток, потому что это не очень весело, потому что только некоторые объекты получают новые сгенерированные монеты, а остальные майнеры не имеют шансов на рентабельность. Поэтому мы установили его только на 5%, потому что мы не хотим упустить большой хешрейт от ферм FPGA, но не хотим разрушать прибыльность для других майнеров. И последний cryptonight lite v7, мы используем этот алгоритм для майнинга CPU и GPU, этот алгоритм никогда не майнился на FPGA, поэтому вероятность того, что битовый поток для него будет существовать, мала. С помощью этого алгоритма мы приносим добычу Infinium мелким майнерам дома, чтобы они могли зарабатывать вновь созданные монеты и защищать сеть.

1.2) Как мы установили проценты для каждого алгоритма?

Мы разработали простой метод, как установить проценты добытых блоков для конкретного алгоритма. В обычном режиме PoW сложность добычи монет была автоматически перенаправлена, чтобы попытаться добыть блоки в определенное время. INF (90 секунд), BTC (600 секунд). В большинстве случаев он рассчитывается исходя из того, сколько времени требуется для добычи блока в среднем, а затем сложность увеличивается или уменьшается, чтобы поразить цель. Мы создали 3 независимых сложности майнинга на infinium для каждого алгоритма, чтобы рассчитать проценты конкретного блока из каждого алгоритма в последних 720 блоках, а затем мы нацелены на определенное время для каждого алгоритма, чтобы приблизиться к процентам cn v0 - 189 секунд, cn v8 - 1878 секунд, cn lite v7 - 189 секунд.

1.3) Как рассчитывается вознаграждение за блок после этого изменения?

Награда за блок рассчитывается исходя из средней сложности по всем сложностям.

2. (Merged mining) Объединенный майнинг с этого хардфорка разрешен и Infinium функционирует как родительская монета в объединенном майнинге. Он здесь, чтобы привлечь других майнеров с других монет с помощью того же алгоритма, чтобы добыть их любимую монету + инфиниум и защитить обе сети. Это помогает стабилизировать хешрейт Infinium за счет большего количества майнеров, поэтому вышеупомянутые различные сложности алгоритмов будут более стабильными из-за этого в долгосрочной перспективе.

Оригинальные ссылки:

Сайт: https://infinium.space
Discord: https://discord.gg/jRQZMr9u84
Telegram: https://t.me/Infinium8
Github: https://github.com/Infinium-dev

Наша благодарность: разработчикам CryptoNote, разработчикам Bytecoin за поддержку протокола cryptonote до прихода команды Infinium.

технический документ, написанный Jacob и 313
Вдохновленный оригинальным техническим документом cryptonote:
https://infinium.space/cryptonote_v2/cryptonote_v2_whitepaper.pdf