Prizm Whitepaper

Редакция - март, 2017

В этом документе описывается первоначальная концепция Prism.

Биткойн - первая в мире децентрализованная цифровая валюта, позволяющая легко хранить и передавать криптографические монеты, используя peer-to-peer (P2P) сеть для передачи информации, хеширование в качестве сигнала синхронизации для предотвращения двойного расходования средств, а также мощную систему сценариев для определения владельца монет. Биткоины взаимозаменяемы, выступая в качестве нейтрального средства обмена. Биткоины могут обладать специальными свойствами, поддерживаемыми либо эмитентом, либо публичным соглашением, и имеют стоимость, независимую от номинальной стоимости, лежащей в его основе. Prizm (PZM) - это криптографическая валюта нового поколения, полностью децентрализованная peer-to-peer электронная платежная система, реально работающая без участия третьей стороны.

Система способна обрабатывать транзакции надежно, быстро и эффективно, в размере тысяч в час или более, стимулировать людей к участию в обеспечении безопасности сети, масштабироваться на глобальном уровне с минимальным расходом ресурсов, с возможностью запуска на любом устройстве. Ключевым преимуществом Prizm, является уникальная технология ParaMining, которой нет больше ни в одной из существующих криптовалют. Но об этом позднее.

Содержание

1 Введение

Prizm - это 100% proof-of-stake (PoS) криптовалюта, построенная на ядре NXT, написанная на языке Java 1 NXT с открытым исходным кодом. Уникальный алгоритм NXT пруф-оф-стейк (proof-of-stake) не зависит от какой-либо реализации концепции «возраст монеты», используемой другими криптовалютами proof-of-stake, и устойчив к так называемым атакам «nothing (ничего) at stake». Общее количество, 10 миллионов доступных монет, было распределено в блоке генезиса. Криптография Curve25519 используется для обеспечения баланса безопасности и требуемой вычислительной мощности наряду с более часто используемыми алгоритмами хеширования SHA256.

Блоки генерируются, в среднем, каждые 60 секунд, аккаунтами, которые не заблокированы на сетевых узлах. PZM перераспределяются посредством включения комиссий за транзакции, которые зачисляются аккаунту, когда он успешно создает блок. Этот процесс известен как форжинг и схож с понятием «майнинг», используемому другими криптовалютами. Транзакции считаются безопасными после 10 подтверждений блока, а текущая архитектура и размер блока Prizm позволяют обрабатывать до 367 200 транзакций в день. Prizm включает в себя реализацию функции Transparent Forging, которая позволит увеличить производительность обработки транзакций на два порядка с помощью алгоритма генерации детерминированного блока, в сочетании с дополнительными механизмами безопасности сети.

2 Технологии ядра

2.1 Proof of Stake

В традиционной модели Proof of Work (PoW), используемой большинством криптовалют, безопасность сети обеспечивается участниками, выполняющими «работу (work)». Они вкладывают свои ресурсы (время вычисления / обработки), чтобы сверять транзакции с двойными расходами, и налагать внеочередные расходы на тех, кто попытается свернуть транзакции. За эту работу участники награждаются монетами, причем их частота и сумма варьируются в зависимости от рабочих параметров криптовалюты. Этот процесс известен под названием Майнинг. Частота генерации блоков, определяющая каждое доступное вознаграждение за майнинг криптовалюты, как правило, должна оставаться постоянной. В результате трудоемкость требуемой работы для получения вознаграждения должна увеличиваться по мере увеличения работоспособности сети.

По мере развития сети Proof of Work, у индивидуального пользователя становится меньше стимулов для поддержки сети, поскольку их потенциальная награда распределяется среди большего числа коллег.

В поисках рентабельности, майнеры продолжают вкладывать ресурсы в специализированное, запатентованное оборудование, которое требует значительных капиталовложений и высоких текущих энергетических затрат. С течением времени, сеть становится все более централизованной, так как более мелкие партнеры (те, кто может выполнять меньше работы) выпадают или объединяют свои ресурсы в «пулы».

Создатель биткоина Сатоши Накамото, предназначал чтоб сеть биткоина была полностью децентрализованной, Но никто не мог предугадать, что стимулы, обеспечиваемые системами Proof of Work, приведут к централизации процесса майнинга. Это приводит к возможности уязвимостей. GHash.io пул биткойна в прошлом достиг 51% мощности майнинга Биткоина, а верхние пять пулов майнинга биткоина составляют 70% мощности хэширования сети. Концепция децентрализации находится под угрозой полной потери.

В модели Proof of Stake, используемой Prizm, сетевая безопасность регулируется партнерами (peers), имеющими долю в сети. Стимулы, обеспечиваемые этим алгоритмом, не способствуют централизации, как алгоритмы Proof of Work, и данные показывают, что сеть Prizm остается высоко децентрализованной с момента ее создания: большое (и растущее) количество уникальных аккаунтов вносящих блоки в сеть, и пять топовых аккаунтов генерируют 35% от общего количества блоков.

2.1.1 Модель Proof of Stake в Prizm

Призм использует систему, в которой каждая «монета» на счете может использоваться как мини устройство для осуществления Майнинга (mining rig). Чем больше монет содержится в аккаунте, тем больше вероятность, что аккаунт получит право на создание блока.
Общая «награда», полученная в результате создания блока, представляет собой сумму комиссий за транзакции , расположенные внутри блока. Prizm не создает никаких новых монет в результате создания блоков. Перераспределение PZM происходит в результате того, что генераторы блока получают комиссионные за транзакции, поэтому термин «форжинг» (используется в данном контексте «создавать отношения или новые условия», вместо «майнинг»).

Последующие блоки генерируются на основе проверяемой, уникальной и почти непредсказуемой информации из предыдущего блока. Блоки связаны в силу этих связей, создавая цепочку блоков (и транзакций), которые можно проследить вплоть до блока генезиса.

Время генерации блока ориентировочно 59 секунд, но изменения вероятностей привели к тому, что среднее время генерации блока может составить 80 секунд, случаются и более длинные интервалы блоков.

Безопасность цепочки блоков (blockchain) всегда имеет значение в системе Proof of Stake.

Основные принципы алгоритма Proof of Stake в Prizm:

- Совокупное значение сложности сохраняется в качестве параметра в каждом блоке, и каждый последующий блок получает свою новую «сложность» от значения предыдущего блока. В случае двусмысленности, сеть достигает консенсуса, выбирая фрагмент блока или цепи с наивысшей кумулятивной сложностью. Это более подробно описано в разделе 2.4.1

- **Ч**тобы владельцы учетных записей не перемещали свои средства с одной учетной записи на другую, злоупотребляя, с целью получения возможности генерации блоков, монеты должны быть стационарными в пределах аккаунта для 1440 блоков, прежде чем они смогут внести свой вклад в процесс генерации блоков. Монеты, отвечающие этому критерию, способствуют эффективному балансу счета, и этот баланс используется для определения вероятности форжинга.

- Чтобы злоумышленник не мог создать новую цепочку на всем пути от блока генезиса, сеть позволяет только реструктуризацию цепи 720ти блоков, расположенных за текущим блоком. Любой блок, представленный на высоте ниже этого порога, отклоняется. Этот порог перемещения можно рассматривать как единственную фиксированную контрольную точку PZM.

- Из-за крайне низкой вероятности того, что какой-либо аккаунт возьмет на себя управление Блокчейн, создав собственную цепочку блоков,

транзакции считаются безопасными, если они закодированы в блок, который составляет 10 блоков, расположенных за текущим блоком.

2.2 Монеты

Первоначальная эмиссия - 10 миллионов PZM. Монеты были выпущены с созданием блока генезиса (первый блок в цепочке блоков PZM). Пре-майнинг реализуется во всех странах мира, по номинальной стоимости, ограниченными партиями, для достижения стартовой децентрализации Prizm.

Общий объем выпуска составит 6 миллиардов PZM.

Аккаунт генезис генерирует монеты по сигналам Paramining (сигнал отправить монеты на определенный кошелек) до предела минус 600 триллионов PZM.

Существование анти-токенов в генезисе имеет несколько интересных побочных эффектов:

- Все токены (монеты), отправленные на аккаунт-генезис, эффективно уничтожаются, так как отрицательный баланс аккаунта отменяет их.
- Основная функция Prizm - традиционная платежная система, но она была создана, чтобы сделать гораздо больше.

2.3 Сетевые узлы

Узлом сети Prizm является любое устройство, которое вносит транзакцию или данные блока в сеть. Любое устройство с программным обеспечением PZM рассматривается как узел.

Узлы могут быть подразделены на два типа: маркированные и обычные. Маркированный узел - это просто узел, который помечен зашифрованным токеном, полученным из личного ключа аккаунта; Этот токен может быть декодирован, чтобы показать конкретный адрес учетной записи PZM и баланс, которые связаны с узлом. Акт размещения маркировки на узле добавляет уровень подотчетности и доверия, поэтому узлы с маркировкой более надежны, чем узлы, не имеющие маркировки в сети. Чем больше баланс аккаунта привязан к маркированному узлу, тем больше доверия уделено этому узлу. В то время, как злоумышленник может захотеть маркировать узел, чтобы заслужить доверие в сети, а затем использовать это доверие в злонамеренных целях; Барьер для входа (стоимость PZM, необходимая для создания адекватного доверия) препятствует такому злоупотреблению. Каждый узел в сети Prizm имеет возможность обрабатывать и передавать и транзакции, и информацию блоков. Блоки проверяются по мере их получения от других узлов, а в случаях, когда проверка блока не выполняется, узлы могут быть «занесены в черный список» временно, чтобы предотвратить распространение недействительных данных блока.

Каждый узел имеет встроенные механизмы защиты DDOS (Distributed Denial of Services), которые ограничивают количество сетевых запросов от любого пользователя до 30 в секунду.

2.4 Блоки

Как и в других криптовалютах, Леджер (главная книга операций) транзакций PZM строится и хранится в связанной цепочке блоков, известной как blockchain. Эта книга обеспечивает постоянный учет транзакций, которые имели место быть, а также устанавливает порядок, в котором были совершены транзакции. Копия blockchain хранится на каждом узле в сети Prizm, и каждый аккаунт, который не заблокирован на узле (путем предоставления закрытого ключа этой учетной записи), имеет возможность генерировать блоки, при условии, что по меньшей мере одна входящая транзакция в аккаунте была подтверждена 1440 раз. Любой аккаунт, соответствующий этим критериям, называется активным аккаунтом.

В Prizm, каждый блок содержит до 255 транзакций, все они предваряются Хедером в 192 байта, который содержит идентифицирующие параметры. Каждая транзакция в блоке представлена максимум 160 байтами, а максимальный размер блока - 32 КБ.

Все блоки содержат следующие параметры:

- Версия блока, значение высоты блока и идентификатор блока
- Временная метка блока, выраженная в секундах от блока генезиса
- ID аккаунта, создавшего блок, а также открытый ключ аккаунта.
- Идентификатор и хэш предыдущего блока
- Количество транзакций, хранящихся в блоке
- Общая сумма PZM, представленная транзакциями и комиссиями в блоке
- Данные транзакции для всех транзакций, включенных в блок, включая их идентификаторы транзакций
- Длина полезной нагрузки блока и значение хэш-функции полезной нагрузки блока
- Сигнатура генерации блока
- Сигнатура для всего блока
- Базовое целевое значение и кумулятивная сложность для блока

2.4.1 Создание блоков (форжинг)

Три значения являются ключевыми, для определения, какой аккаунт имеет право генерировать блок, какой аккаунт получает право на создание блока, и какой блок считается авторитетным во время конфликта: *базовое целевое значение, целевое значение и совокупная сложность.*

Базовое целевое значение

Чтобы выиграть право форжить (генерировать) блок, все активные аккаунты Prizm «конкурируют», пытаясь создать хеш-значение, которое ниже заданного базового целевого значения. Это базовое целевое значение изменяется от блока к блоку и выводится из базового целевого значения предыдущего блока, умноженного на количество времени, которое потребовалось для генерации того блока.

Целевое значение

Каждый аккаунт рассчитывает свое собственное целевое значение на основе текущей эффективной ставки.

Это значение равно:

$$T = T_b \times S \times B_e$$

где:

T новое целевое значение

Tb базовое целевое значение

S время, прошедшее с момента последнего блока, в секундах

Be эффективный баланс аккаунта

Как видно из формулы, целевое значение растет с каждой секундой, прошедшей с момента времени предыдущего блока. Максимальное целевое значение составляет 1,53722867 x 1017, а минимальное целевое значение составляет половину базового целевого значения предыдущего блока.

Это целевое значение и базовое целевое значение одинаковы для всех учетных записей, пытающихся форжить на вершине какого-то определенного блока. Единственным определенным параметром аккаунта, является эффективный параметр баланса.

Совокупная сложность

Совокупное значение сложности получается из базового целевого значения, по формуле:

$$D_{cb} = D_{pb} + 2_{64} / T_b$$

где:

Dcb сложность текущего блока

Dpb сложность предыдущего блока

Tb базовое целевое значение текущего блока

Алгоритм Форжинга

Каждый блок в цепочке имеет параметр генерации подписи. Для участия в процессе форжинга блока, активный аккаунт криптографически подписывает предыдущий сгенерированный блок своим собственным публичным ключом. Это создает 64-байтовую подпись, которая затем хешируется с использованием SHA256. Первые 8 байт полученного хеша дают число, называемое хит аккаунта.

Хит сравнивается с текущим целевым значением. Если вычисленный Хит ниже целевого, то следующий блок может быть сгенерирован. Как отмечено в формуле целевого значения, целевое значение увеличивается с каждой секундой. Даже если в сети всего несколько активных аккаунтов, один из них в конечном итоге будет генерировать блок, потому что целевое значение станет очень большим. Следствием этого является то, что вы можете оценить время, которое потребуется для любого аккаунта, чтобы форжить блок, сравнив значение хита того аккаунта, с целевым значением.

Последний пункт имеет большое значение. Так как любой узел может запросить эффективный баланс для любого активного аккаунта, имеется возможность пройти через все активные аккаунты, чтобы определить их индивидуальное значение хита. Это означает, что с разумной точностью можно предсказать, какой следующий аккаунт выиграет право форжить блок.

Атака перетасовки может быть спровоцирована путем перемещения доли в аккаунт, который будет генерировать следующий блок, что является еще одной причиной, по которой ставка PZM должна быть стационарной для 1440 блоков, прежде чем она сможет внести свой вклад в форжинг (через эффективное значение баланса). Интересно, что новое базовое целевое значение для следующего блока не может быть разумно предсказано, поэтому практически детерминированный процесс определения, кто будет форжить следующий блок, становится все более и более стохастическим, поскольку предпринимаются попытки предсказать будущие блоки. Эта особенность алгоритма форжинга PZM помогает сформировать основу для разработки и реализации алгоритма Transparent Forging (прозрачный форжинг).

Когда активный аккаунт получает право на создание блока, он объединяет до 255 доступных неподтвержденных транзакций в новый блок и заполняет блок всеми его необходимыми параметрами. Этот блок затем транслируется в сеть в качестве кандидата в блокчейн.

Величина полезной нагрузки, генерирующий аккаунт и все подписи на каждом блоке могут быть проверены всеми сетевыми узлами, которые это получают. В ситуации, когда сгенерировано несколько блоков, узлы будут

выбирать блок с наивысшим накопленным значением сложности, как авторитетный блок. Поскольку блок-данные распределяются между участниками (одноранговыми узлами), обнаруживаются форки (неуполномоченные фрагменты цепи) и демонтируются путем изучения значений совокупной сложности цепей, хранящихся в каждом форке.

Лизинг баланс

Поскольку возможность какого-либо аккауна заниматься форжингом основана на параметре эффективного баланса, можно «ссужать» полномочия форжинга с одного аккаунта на другой, не отказываясь от контроля токенов, связанных с аккаунтом. Используя транзакцию типа «контроль учетных записей», владелец аккаунта может временно уменьшить фактический баланс счета до нуля, добавив его к эффективному балансу другого аккаунта. Влияние форжинга целевого аккаунта увеличивается до конца периода времени, указанного владельцем оригинального аккаунта, после чего фактический баланс возвращается в исходную учетную запись.

Аккаунты, использующие арендованные мощности для форжинга, чаще генерируют блоки и получают больше транзакционных сборов, но эти комиссии автоматически не возвращаются на арендные счета. Однако с небольшим количеством кодирования эта система позволяет создавать более менее надежные пулы форжинга, которые могут делать выплаты участникам.

2.4.2 Accounts

Prizm представляет умный кошелек, как часть своего дизайна: все аккаунты хранятся в сети с личными ключами для каждого возможного адреса учетной записи, непосредственно выводимого из кодовой фразы каждого аккаунта, с использованием комбинации операций SHA256 и Curve25519.

Каждая учетная запись представлена 64-битным числом, и это число выражается как адрес аккаунта, использующий запись коррекции ошибок Рида-Соломона (Reed-Solomon), которая позволяет обнаруживать до четырех ошибок в адресе учетной записи или исправлять до двух ошибок . Этот формат был реализован в ответ на опасения, что неверный адрес аккаунта может привести к тому, что монеты, псевдонимы или активы будут необратимо перенесены на ошибочные целевые аккаунты. Адреса аккаунтов всегда начинаются с префикса «PRIZM-», что делает адреса аккаунтов Prizm легко узнаваемыми и отличными от форматов адресов, используемых другими криптовалютами.

Адрес учетной записи, закодированный Ридом-Соломоном, связанный с секретной кодовой фразой, генерируется следующим образом:

1. Секретная кодовая фраза хэшируется с помощью SHA256 для получения личного ключа аккаунта.

2. Закрытый ключ зашифрован с помощью Curve25519, для получения открытого ключа учетной записи.

3. Публичный ключ хешируется с SHA256 для получения идентификатора учетной записи.

4. Первые 64 бита идентификатора аккаунта - это видимый номер аккаунта.

5. Кодирование Рида-Соломона, видимого номера счета с префиксом «PRIZM-» генерирует адрес аккаунта.

Когда аккаунт получает доступ, с помощью секретной кодовой фразы, в первый раз, он не защищен публичным ключом. Когда совершается первая исходящая транзакция из аккаунта, 256-битный публичный ключ, полученный из кодовой фразы, сохраняется в блокчейн, и это защищает аккаунт. Адресное пространство для публичных ключей (2256) больше, чем адресное пространство для номеров аккаунтов (264), поэтому нет однозначного сопоставления кодовых слов с номерами аккаунтов и возможных коллизий. Эти коллизии определяются и предотвращаются следующим образом: после того, как для доступа к аккаунту используется определенная кодовая фраза, и этот аккаунт защищен публичным 256-битным ключом, никакая другая пара публичного-приватного ключей не может получить доступ к этому номеру аккаунта.

Свойства баланса аккаунта

Для каждого аккаунта Prizm, доступны несколько различных уровней баланса. Каждый тип служит для разных целей, и многие из этих значений проверяются как часть проверки и обработки транзакций.

- Эффективный баланс аккаунта используется в качестве основы для расчетов форжинга аккаунта. Эффективный баланс аккаунта состоит из всех монет, которые были стационарными на этом аккаунте для 1440 блоков. Кроме того, функция «Лизинг аккаунта» позволяет устанавливать эффективный баланс на другом аккаунте на временный период.

- Гарантированный баланс счета состоит из всех монет, которые были стационарными на счете для 1440 блоков. В отличие от эффективного баланса, этот баланс не может быть присвоен какой-либо другой учетной записи.

- Базовый баланс счета учитывает все транзакции, которые имели, по крайней мере, одно подтверждение.

- Форжащий Баланс аккаунта показывает общее количество PZM, полученное в результате успешного форжинга блоков.

- Неподтвержденный баланс аккаунта - это тот, который отображается у клиентов Prizm. Он представляет текущий баланс счета, за вычетом монет, участвующих в неподтвержденных, отправленных транзакциях.

- Гарантированные балансы активов составляют гарантированные балансы всех активов, связанных с конкретным аккаунтом.

- Неподтвержденные балансы активов составляют неподтвержденные балансы всех активов, связанных с определенным аккаунтом.

Кошелек

Биткойн и родственные валюты часто используют зашифрованный файл, под названием кошелек, для хранения сгенерированных адресов для получения монет. Ядро Next, используемое в проекте Prizm не имитирует эту функциональность, но и не исключает этого. Возможно, для клиентов-девелоперов реализовать систему, в которой группа закрытых ключей для учетных записей Prizm хранится в зашифрованном автономном файле.

2.4.3 Транзакции

Транзакции - это единственное средство, благодаря которому аккаунты Prizm могут изменять свое состояние, или баланс. Каждая транзакция выполняет только одну функцию, запись которой постоянно сохраняется в сети после того, как транзакция была включена в блок.

Комиссия за транзакции

Плата за транзакции является основным механизмом, посредством которого PZM возвращаются обратно в сеть. Каждая транзакция требует минимальной платы, в размере 0,5 PZM.

Подтверждение транзакций

Все транзакции PZM считаются неподтвержденными до тех пор, пока они не будут включены в действительный блок сети. Новые созданные блоки распределяются в сети узлом (и связанной учетной записью), который их создает, и транзакция, которая включена в блок, считается полученной одним подтверждением. Поскольку последующие блоки добавляются к существующей цепочке блоков (blockchain), каждый дополнительный блок добавляет еще одно подтверждение количеству подтверждений транзакции.

Если транзакция не включена в блок до истечения его срока, она сгорает и удаляется из пула транзакций.

Сроки транзакций

Каждая транзакция содержит параметр крайнего срока (deadline), установленный на количество минут с момента отправки транзакции в сеть. По умолчанию, дедлайн составляет 1440 минут (24 часа). Транзакция, которая была передана в сеть, но не была включена в блок, называется неподтвержденной транзакцией.

Если транзакция не была включена в блок до истечения дедлайна транзакции, транзакция удаляется из сети.

Транзакции могут быть оставлены неподтвержденными, поскольку они недействительны или искажены, или потому, что блоки заполняются транзакциями, которые предлагают платить более высокую комиссию. В будущем такие функции, как транзакции с несколькими сигнатурами, могут использовать предельные сроки, в качестве средства обеспечения соблюдения срока действия.

Создание и обработка транзакций

Подробная информация о создании и обработке транзакций PZM выглядит следующим образом:

Отправитель указывает параметры транзакции. Типы транзакций меняются, и желаемый тип указывается при создании транзакции, но для всех транзакций необходимо указать несколько параметров:

- Личный ключ для отправляющего счета
- дедлайн транзакции
- необязательная транзакция с привязкой

2.5 Парамайнинг

Технология Парамайнинг (Paramining) - ключевое преимущество Prizm перед остальными криптовалютами.
Разработчиками Prizm был создан уникальный, линейно-ретроградный механизм начисления вознаграждения за хранение средств, направленный на экономическую привлекательность и постепенное замещение массой PZM всех существующих финансовых инструментов мира.
Парамайнинг создан в дополнение к основному механизму Форжингу, который не увеличивает количество средств в системе. Эта технология позволяет генерировать новые монеты, согласно метрик стандартной математики развития нормализованной финансовой системы в срезе мировой экономики. По нашим подсчетам - лишь такой формат роста массы монет может обеспечить постепенное и уверенное замещение всех, существующих на данный момент экономических инструментов.

Механизм работы

По своим характеристикам, Парамайнинг является системой MLM 2.0, исключающей из себя всё, что отталкивает простого человека от сетевого маркетинга, но при этом вовлекает его в развитие сети для увеличения скорости добычи монет в личном кошельке.

Скорость добычи новых монет с помощью механизма Парамайнинг зависит от двух основных параметров: количество монет в личном кошельке и количество монет на кошельках последователей до 888 уровней.

1. Количество монет в личном кошельке.

Скорость роста количества монет, %	Количество монет в кошельке
0,12%	от 1 до 99
0,14%	от 100 до 999
0,18%	от 1000 до 9999
0,21%	от 10000 до 49999
0,25%	от 50000 до 99999
0,28%	от 100000 до 499999
0,33%	от 500000 до 1000000

2. Количество монет в кошельках последователей на 888 уровней в глубину.

Множитель	Объем монет структуры последователей
2,18	от 1000 до 9999
2,36	от 10000 до 99999
2,77	от 100000 до 999999
3,05	от 1000000 до 9999999
3,36	от 10000000 до 99999999
3,88	от 100000000 до 999999999
4,37	от 1000000000

Принцип Парамайнинг базируется на фундаментальных законах физики, из раздела “Видимое излучение”. Подобно модели нашей Вселенной, система постоянно расширяется, набирая скорость.

0.12% * 2.18 = 0.26% за 24 часа.

ВСЕГО: Более чем 8% новых монет в месяц.

0.18% * 2.77 = 0.49% за 24 часа.

ВСЕГО: Более чем 15% новых монет в месяц.

Например: Имея в кошельке 99 PZM и 100000 PZM в 888 уровнях структуры, применяется процент роста количества монет 0,12% и множитель 2,77, что позволяет генерировать 3,3 новых монеты ежедневно. Для зачисления этих монет на баланс достаточно совершить любую транзакцию.

Система Парамайнинг, при совершении транзакций в кошельке, производит запись в Блокчейн, содержащую в себе информацию о количестве монет владельца кошелька и количество монет в кошельках его последователей, в этот момент генерируются новые монеты на баланс кошелька.

Таким образом, мы получаем систему со сложным процентом, которая стимулирует пользователей совершать транзакции, для увеличения капитализации их денежных средств, подключать новых держателей кошельков, увеличивая тем самым оборот своей структуры. По самым скромным расчетам, ежемесячный прирост количества монет у такого пользователя составляет не менее 10%.

Структура последователей

Впервые, в истории криптовалют применена, так называемая, структура последователей. После создания нового кошелька, система фиксирует в блокчейн от кого поступила первая транзакция и навсегда устанавливает реферальную связь, которую невозможно изменить. “Это позволяет с легкостью строить глобальные MLM сети и увеличивать скорость добычи новых монет.

Техническая реализация технологии Парамайнинг, в данный момент, не описывается детально, по причине того, что для всех нас, свободных людей, главное - это создать не 100 “мертвых” инструментов, а один - с хорошей поддержкой и хорошо работающий. Если же будет раскрыто наше ноу-хау, то кто-то обязательно попробует это повторить и это невольно приводит к рассеиванию внимания и использованию данной идеи не для благородных и значимых для нашей планеты целей, а для целей, нам не известным и не всегда отличающихся позитивной окраской намерения.

Для начала добычи новых монет PZM, достаточно всего одной монеты в электронном кошельке , которая автоматически запускает Парамайниг. Это процесс, позволяющий без каких-либо затрат электроэнергии увеличить количество монет в кошельке. Технология Парамайнинг работает на каждом кошельке Prizm и автоматически останавливается при достижении баланса в 1 миллион монет в кошельке .

Система Парамайнинг является самым совершенным инструментом для продвижения и популяризации, так как она не имеет аналогов ни в одной современной криптовалюте. Основным преимуществом технологии Парамайнинг является то, что ни один пользователь сети не может вмешаться в этот механизм и сфальсифицировать новые монеты, все пользователи могут в режиме реального времени отслеживать число выпущенных системой монет.

2.6 Основы криптографии

Обмен ключами в Prizm основан на алгоритме Curve25519, который генерирует общий секретный ключ с использованием быстрой эффективной эллиптической кривой Diffie-Hellman с высокой степенью защиты. Алгоритм был впервые продемонстрирован Даниэлем Дж. Бернштейном в 2006 году.

Подписание сообщений в Prizm осуществляется с использованием алгоритма электронной цифровой подписи Elliptic-Curve (EC-KCDSA), который был определен группой IEEE P1363a в 1998 году командой Целевой группы KCDSA.

Оба алгоритма были выбраны для баланса скорости и безопасности для размера ключа всего 32 байта.

2.6.1 Алгоритм шифрования

Когда Алиса отправляет Бобу зашифрованный текст, она:

1. Вычисляет общий секрет (shared secret):

- shared_secret = Curve25519(Alice_private_key, Bob_public_key)

2. Вычисляет N seeds:

- seedn = SHA256(seed n-1), где

seed 0 = SHA256 (shared_secret)

3. Вычисляет N keys:

- Keyn = SHA256 (Inv (seed)), где Inv (X) - инверсия всех битов X

4. Шифрует открытый текст:

- ciphertext[n] = plaintext[n] XOR keyn

После получения Боб расшифровывает зашифрованный текст:

1. Вычисляет a shared secret:

- shared_secret = Curve25519(Bob_private_key, Alice_public_key)

2. Вычисляет N семян (подобно шагу Алисы):

- seedn = SHA256(seed n-1), where seed0 = SHA256(shared_secret)

Seedn = SHA256 (семя n-1), где seed0 = SHA256 (shared_secret)

3. Вычисляет N ключей (идентично шагу Алисы):

- keyn = SHA256(Inv(seed n)), where Inv(X) is the inversion of all bits of X

Keyn = SHA256 (Inv (seed n)), где Inv (X) - инверсия всех битов X

4. Расшифровывает зашифрованный текст:

- plaintext[n] = ciphertext[n] XOR keyn

Примечание: Если кто-то угадывает часть открытого текста, он может расшифровать часть последующих сообщений между Алисой и Бобом, если

они используют одни и те же пары ключей. Поэтому, рекомендуется создавать новую пару частных / открытых ключей для каждого сообщения.

3 Основные особенности

3.1 Продвинутый клиент JavaScript

Удобное клиентское приложение, Второго поколения, встроенное в дистрибутив основного программного обеспечения Prizm, к которому можно получить доступ через локальный веб-браузер. Клиент обеспечивает полную поддержку всех основных функций Prizm, реализованных так, что личные ключи пользователей никогда не будут доступны в сети. Он также включает в себя расширенный административный интерфейс и встроенную документацию по Javadoc для низкоприоритетного прикладного программного интерфейса Prizm.

3.2 Базовые платежи

Наиболее фундаментальной особенностью любой криптовалюты является способность передавать монеты с одной учетной записи на другую. Это наиболее фундаментальный тип транзакций Prizm, и он позволяет использовать базовые платежные функции.

3.3 Портативность девайса

Благодаря своей кросс-платформе, основанной на Java roots, хешированию Proof of Stake и его будущей способности уменьшать размер цепочки блоков, Prizm чрезвычайно хорошо подходит для использования на небольших маломощных устройствах с низким ресурсом. Приложения для Android и iPhone и программное обеспечение были перенесены на маломощные устройства ARM, такие как платформы RaspberryPi и CubieTruck.

Возможность реализации Prizm на маломощных, всегда подключенных устройствах, таких как смартфоны, позволяет нам представить сценарий, в котором большинство сетей Prizm поддерживается на мобильных устройствах. Низкая стоимость и потребление ресурсов этих устройств значительно сокращают расходы на сеть по сравнению с традиционными криптовалютами Proof of Work.

4 Проблемы

4.1 Атаки Proof of Stake

4.1.1 Ничего на кону (nothing at Stake)

В атаке «ничего не поставлено на карту», форжеры (forgers) пытаются строить блоки поверх каждого форка (fork), который они видят, потому что это действие им почти ни во что не обходится, и потому, что игнорирование любого форка может означать потерю на вознаграждениях блока, которые могли быть заработаны, если бы этот форк был предназначен чтобы стать цепочкой с наибольшим кумулятивная сложность.

Хотя эта атака теоретически возможна, в настоящее время она не практикуется. В сети Prizm не случаются длинные форки блокчейна, а награда за низкие блоки не дает веского стимула для получения прибыли; Кроме того, компрометируя безопасность сети и доверие ради такой небольшой прибыли, можно было бы сделать любую победу пиррихой (pyrrhic).

4.1.2 История атак

В « атаке истории», кто-то приобретает большое количество монет, продает их, а затем пытается создать успешный форк перед тем, как его монеты были проданы или обменены. Если атака не удалась, попытка ничего не стоит, поскольку монеты уже проданы или обменены; Если атака прошла успешно, атакующий получает свои монеты обратно. Экстремальные формы этой атаки включают получение закрытых ключей из старых аккаунтов и их использование для построения успешной цепочки прямо из блока генезиса.

В Prizm основная атака истории вообще не срабатывает, потому что все ставки должны быть фиксированы на 1440 блоках, прежде чем их можно будет использовать для форжинга; Кроме того, эффективный баланс аккаунта, который генерирует каждый блок, проверяется как часть аттестации блока. Экстремальная форма этой атаки вообще не срабатывает, так как блокчейн в Prizm не может быть реорганизован более чем на 720 блоков, за текущей высотой блока. Это ограничивает временные рамки, в которых злоумышленник мог бы установить эту форму атаки.

Приложение: Решение некоторых проблем Биткоина, используемых в Prizm

Prizm использует функции, которые хорошо зарекомендовали себя в Биткойне, и исключает использование аспектов, вызывающих проблемы. В этом приложении рассматриваются некоторые проблемы с протоколом Bitcoin и сетью, которые решаются в Prizm с помощью найденных альтернатив.

Размер цепочки блоков (Blockchain Size)

Количество транзакций Bitcoin в день

В конце 2013 года количество транзакций, обрабатываемых в сети Биткойн, достигло максимума в 70 000 в день, что составляет около 0,8 транзакций в секунду (tps).

Нынешний стандартный размер блока Bitcoin в один мегабайт, генерируется (в среднем) каждые десять минут на "полный узел" (full node), ограничивает максимальную пропускную способность существующей сети Bitcoin до около 7 tps. Сравните это с пропускной способности сети VISA для обработки 10000 tps, и вы увидите, что Bitcoin не конкурентоспособен, в том виде как он существует сегодня. Увеличение общественного использования системы Биткойн приведет к тому, что биткойн скоро столкнется с лимитом транзакций в день и остановит дальнейший рост. Чтобы предотвратить это, разработчики программного обеспечения Bitcoin работают над созданием «тонких клиентов», использующих упрощенную проверку платежей (SPV). Чтобы обеспечивать большую пропускную способность в те же средние 10-минутные сроки, тонкие клиенты SPV не будут выполнять полную проверку безопасности на больших блоках, которые они обрабатывают. Вместо этого они будут исследовать несколько хэшированных блокчейнов от конкурирующих майнеров и предполагать, что версия блокчейнов, сгенерированная большинством майнеров, верна. По словам Майка Херна из биткойн, «вместо проверки всего содержимого, [SPV] просто полагает, что большинство майнеров честны.

Количество транзакций Prizm в день

В своем текущем состоянии сеть Prizm может обрабатывать до 367 200 транзакций в день - более, чем в девять раз превышающих текущие пиковые значения Биткойна. Реализация Transparent Forging позволяет практически мгновенно обрабатывать транзакции, значительно увеличивая этот предел.

Время подтверждения транзакций в Bitcoin

Время подтверждения транзакций в Биткоин варьировалось от 5 до 10 минут, в течение большей части 2013 года. После объявления в конце 2013 года, что китайские банки не будут допущены для обработки биткоинов, среднее время транзакций Биткойна значительно увеличилось, до 8-13 минут, с периодическими пиками в 19 Минут. С тех пор время подтверждения сместилось в диапазон от 8 до 10 минут.Тем не менее, поскольку для завершения транзакции Биткоин требуются несколько проверок (обычно шесть предпочтительных подтверждений), один час может легко пройти до того, как будет завершена продажа активов, оплачиваемых Биткоином.

Время подтверждения транзакций в Prizm

Среднее время генерации блока для PZM исторически было показано равным примерно 80 секундам, и среднее время обработки транзакции равнялось такому же значению. Сделки считаются безопасными после десяти подтверждений, что означает, что транзакции становятся постоянными менее чем за 14 минут.

Внедрение Transparent Forging (прозрачный форжинг) позволяет совершать практически мгновенные транзакции, что еще больше сократит это время.

Проблемы с централизацией

Увеличение сложности и в сочетании скорости хэш-сети для Bitcoin создало высокий барьер для выхода на рынок для новичков, и снижение прибыли для существующих майнинг-установок. Стимул поощрения блоков, используемый Биткоином, привел к созданию крупных одноуровневых установок специализированного майнинг оборудования, а также опору на небольшой набор крупных майнинг пулов. Это привело к эффекту «централизации», где большие объемы майнинга сосредоточены на контроле за уменьшающимся числом людей. Это не только создает такую мощную структуру, которую Биткойн разрабатывал для обхода, но также представляет реальную возможность того, что одна операция или пул майнинга может набрать 51% общей мощности майнинга в сети и выполнить 51% -ную атаку. Также существуют атаки, требующие всего лишь 25% от общей мощности хеширования сети.

Известно, что в начале января 2014 года GHash.io начал добровольно уменьшать мощность своего собственного майнинга, так как он приближался к уровню 51%. Через несколько дней мощность в пуле уменьшилась до 34% от общей мощности сети, но скорость сразу же начала увеличиваться, и в июне 2014 года снова достигли опасных уровней.

Решения Prizm

Стимулы, предоставляемые алгоритмом Next's Proof of Stake, используемом в проекте Prizm, обеспечивают низкий возврат инвестиций примерно на

0,1%. Поскольку с каждым блоком новые монеты не генерируются, нет дополнительного «вознаграждения за майнинг», которое стимулирует объединение усилий для создания блоков. Данные показывают, что сеть Prizm остается очень децентрализованной с момента ее создания: большое (и растущее) количество уникальных учетных записей вносит блоки в сеть, а пять крупнейших учетных записей генерируют 35% от общего числа блоков.

Ресурсные расходы Proof of Work

Подтверждение транзакций для существующих биткоинов и создание новых биткоинов, для ввода в обращение, требует огромной вычислительной мощности, которая должна постоянно работать. Эта вычислительная мощность обеспечивается так называемыми «майнинг ригс» (mining rigs), которыми управляют «майнеры». Майнеры биткоинов соревнуются между собой, чтобы добавить следующий блок транзакций в общую цепочку биткоинов. Это делается путем «хеширования» - объединения всех транзакций Биткоина, происходящих в течение последних десяти минут, и попыток зашифровать их в блок данных, который также по совпадению имеет определенное количество последовательных нулей в нем. Большинство пробных блоков, генерируемых при помощи хеширования майнеров, не имеют этого целевого количества нулей, поэтому они вносят небольшие изменения и пытаются снова. Миллиард попыток найти этот «выигрышный» блок называется гигахэш (gigahash), причем Mining rig оценивается тем, сколько гигахэшей он может выполнять за секунду, обозначается GH / сек. Победивший майнер, первым создавший криптографически правильный блок Биткоина, тут же получает вознаграждение в 25 новых биткоинов - вознаграждение на момент написания статьи составляло около 15 750 долларов США. Это соревнование среди майнеров, с присуждаемой им наградой, повторяется снова и снова, каждые десять минут, или около того. К началу 2014 года генерировалось более 3500 биткоинов в день, равное около 2,2 миллиона долларов США в день.

С таким большим количеством денег на ставке, майнеры поддержали стремительную гонку вооружений в технологии майнинг риг, чтобы улучшить свои шансы на победу. Первоначально, биткоины добывались с использованием центрального процессора (CPU), типичного настольного компьютера. Затем, для повышения скорости, использовались микросхемы специализированного графического процессора (GPU), в high-end видеокартах. Затем, были задействованы микропроцессоры с программируемой вентильной матрицей (FPGA), а затем микросхемы специализированных прикладных интегральных микросхем (ASIC). Технология ASIC является вершиной линейки для биткойн-майнеров, но гонка вооружений продолжается с появлением различных поколений микросхем ASIC. Текущее поколение микросхем ASIC - это так называемые 28 нм устройства, основанные на размере их микроскопических

транзисторов в нанометрах. Они должны были быть заменены на 20-нм ASIC-модули к концу 2014 года. Примером новой ультрасовременной майнинг риг могла бы стать 28-нм ASIC-карта «Monarch» от Butterfly Labs, которая должна обеспечить 600GH / sec для потребления электроэнергии 350 Вт и стоимостью 2200 долларов США.

Инфраструктура майнинг риг, которая в настоящее время используется для поддержки текущих операций Биткойн, поразительна. Биткоин ASIC подобен аутистам-ученым - они могут выполнять только расчет блока биткоинов и ничего более, но они могут делать это одним вычислением, на скоростях суперкомпьютера. В ноябре 2013 года журнал Forbes опубликовал статью под названием «Глобальная вычислительная мощность биткоинов в 256 раз быстрее, чем 500 объединенных суперкомпьютеров!». В середине января 2014 года, статистика, хранящаяся на сайте blockchain.info, показала, что для постоянной поддержки операций Биткойн требуется непрерывная хеш-скорость около 18 миллионов ГХ / сек. В течение одного дня, такая мощь хэширования произвела 1,5 трлн пробных блоков, которые были сгенерированы и отвергнуты майонерами Биткойна, в поисках одного - волшебных 144 блоков, которые покроют им 2,2 млн. долларов США. Почти все расчеты Биткойна не направлены на исправление бедствия путем моделирования DNA, или поиска радиосигналов от E.T .; Вместо этого они полностью расходуются впустую.

Мощность и затраты, связанные с этой расточительной фоновой поддержкой Биткоина, огромны. Если бы все майнинг риги Биткойна обладали уровнями «Монарха», как описано выше, - а они не будут, пока не модернизируются, - они будут представлять пул из 30 000 машин стоимостью более 63 млн. Долл. США и потребляющих более 10 мегаватт непрерывной мощности во время работы Счет за электричество более 3,5 млн. Долларов США в день.

Реальные цифры значительно выше для текущего, менее эффективного майнинг риг пула машин, фактически поддерживающих сегодня Биткойн. И эти цифры в настоящее время идут вверх по кривой экспоненциального роста, поскольку биткойн марширует от своей текущей одной транзакции в секунду до ее текущего максимума из семи транзакций в секунду.

Расходы на содержание POW, относящиеся к держателям монет

В дополнение к огромным расходам на электроэнергию существует скрытая плата за простое хранение биткоинов. Для каждого найденного блока тот, кто генерирует блок, получает вознаграждение. Это составляет, приблизительно, 10% инфляции, в общем объеме поставок Биткоина в год. За каждые имеющиеся биткоины, на сумму 1000 долларов , владелец платит по 100 долларов за Биткоин в год, чтобы «заплатить» майнерам за безопасность сети