Prizm Whitepaper
Revision - March, 2017

В этом документе описывается первоначальная концепция PRIZM.

Предисловие

Биткойн - первая в мире децентрализованная цифровая валюта, позволяющая легко хранить и передавать криптографические монеты, используя P2P сеть для передачи информации, хеширование в качестве сигнала синхронизации для предотвращения двойного расходования средств, а также мощную систему сценариев для определения владельца монет. В этом есть растущая технология и бизнес-инфраструктура. По оригинальному дизайну биткойны взаимозаменяемы, выступая в качестве нейтрального средства обмена. Биткойны могут обладать спец свойствами, поддерживаемыми либо эмитентом, либо публичным соглашением, и имеют стоимость, независимую от номинальной стоимости, лежащей в его основе.Биткойн доказал, что p2p электронная платежная система может действительно работать и выполнять обработку платежей, без участия третьей стороны. Однако для того, чтобы вся электронная экономика была основана на полностью децентрализованном одноранговом решении, система должна уметь делать следующее:

1) Обрабатывать транзакции надежно, быстро и эффективно, в размере тысяч в час или более;
2) Стимулировать людей к участию в обеспечении безопасности сети;
3) Масштабировать на глобальном уровне с минимальным расходом ресурсов;
4) И быть в состоянии работать на широком спектре устройств, включая мобильные.

PZM (произносится “Призм”) удовлетворяет всем этим условиям. А также имеет дополнительный преимущества, уникальное преимущество названное Парамайнинг, которых нет ни в одной из существующих криптовалют. Но об этом позже.

Обзор

PRIZM - это 100%-ная пруф-оф-стейк криптовалюта, основанная на ядре NEXT, построенная на языке Java с открытым исходным кодом. Уникальный алгоритм PRIZM пруф-оф-стейк не зависит от какой-либо реализации концепции «возраст монеты», используемой другими криптовалютами пруф-оф-стейк, и устойчив к так называемым атакам «nothing (ничего) at stake». Общее количество доступных монет было распределено в блоке генезиса. Криптография Curve25519 используется для обеспечения баланса безопасности и требуемой вычислительной мощности наряду с более часто используемыми алгоритмами хэширования SHA256. Блоки генерируются каждые 60 секунд, в среднем, аккаунтами, которые не заблокированы на сетевых узлах. PZM перераспределяются посредством включения транзакционных сборов, которые присуждаются аккаунту, когда он успешно создает блок. Этот процесс известен как форжинг и сродни понятию «майнинг», используемому другими криптовалютами. Транзакции считаются безопасными после 10 подтверждений блока, а текущая архитектура и размер блока PZM позволяют обрабатывать до 367 200 транзакций в день. PZM 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.

Технологии ядра

Proof of Stake

В традиционной модели «Proof of Work», используемой большинством криптовалют, безопасность сети обеспечивается участниками, выполняющими «работу». Они применяют 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 PZM, 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 форму специализированного, запатентованного оборудования, 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 достиг 51% мощности майнинга биткойнов в прошлом, 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, 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.

Модель Proof of Stake в PRIZM

Призм использует систему, в которой каждая «монета» на счете может рассматриваться как миниатюрная майнинг риг. 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 транзакционных комиссий, расположенных внутри блока. PZM 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 Блокчейна всегда имеет значение в системе Пруф-оф-стейк.

Основные принципы применяются к алгоритму Prizm Proof of Stake:

- 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.
- Чтобы владельцы учетных записей не перемещали свои средства с одной учетной записи на другую как средство манипулирования 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.

Сопоставление с Peercoin Proof of Stake

Peercoin использует параметр возраста монеты как часть алгоритма вероятности майнинга. В этой системе, чем дольше ваши Peercoins были на вашем аккаунте (до 90 дней), тем с большей мощностью (возраст монеты) они должны создавать блок. Акт «Минтинг» блока требует потребления достоинства возраста монет, и сеть определяет консенсус, выбирая цепочку с наибольшим общим потребленным возрастом монет. Когда блоки Peercoin отделяются, потребленный возраст монеты возвращается обратно в исходный аккаунт блока. В результате затраты на атаки сети Peercoin низкие, так как злоумышленники могут продолжать пытаться генерировать блоки (называемые гриндинг стейк) до тех пор, пока они не будут успешными. Peercoin минимизирует эти и другие риски путем централизованной огласки контрольных точек блокчейна несколько раз в день, чтобы «заморозить» блокчейн и блокировать транзакции. Prizm не использует возраст монеты как часть алгоритма форжинга. «Шанс» создания блока каким-либо аккаунтом зависит только от его действующего баланса (который является достоинством каждой учетной записи), времени с момента последнего блока (который делится всех форжащих аккаунтов) и базового целевого значения (которое также общее для всех аккаунтов).

Монеты

Первоначальная эмиссия - 10 миллионов PZM, а финальное количество 600 триллионов PzM. Монеты были выпущены с созданием блока генезиса (первый блок в цепочке блоков). Премайнинг реализуется во всех странах мира, по номинальной стоимости, ограниченными партиями, для достижения стартовой децентрализации Prizm. Общий объем PZM составит 600 триллионов монет.
Аккаунт генезис генерирует анти-монеты по сигналам ПараМайнинга (сигнал отправить монеты на определенный кошелек) до предела минус 600 триллионов PZM

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

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

Достижение поставленных целей сообщества CWT (www.cwt.top) возможно при условии паритета PZM с основными фиатными валютами.

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 зашифрованными 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 PZM 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.

Блоки

Как и в других криптовалютах, Леджер (главная книга операций) операций PZM строится и хранится в связанном ряду блоков, известном как blockchain. Эта книга обеспечивает постоянный учет транзакций, которые имели место быть, а также устанавливает порядок, в котором были совершены транзакции. Копия Блокчейн 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 PZM, 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
• Базовое целевое значение и кумулятивная сложность для блока

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 = Tb x S x Be
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 определеннымм параметром аккаунта, является эффективный параметр баланса.

Совокупная сложность

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

Dcb = Dpb + 264 / Tb

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 на подделку блока. 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 форкс (неуполномоченные фрагменты цепи) и демонтируются путем изучения значений совокупной сложности цепей, хранящихся в каждом форке.

Парамайнинг

ПараМайнинг - ключевое преимущество PRIZM перед остальными криптовалютами.
В базовый механизм форжинга, разработчиками PRIZM был добавлен уникальный, линейно-ретроградный механизм определения награды за хранение средств, направленный на экономическую привлекательность и постепенное замещение массой PZM всех существующих финансовых инструментов мира. То есть, в дополнение к основному механизму форжинга, который не увеличивает количество средств в системе. В PZM существует дополнительный механизм ПараМайнинг, который создает новые монеты, согласно метрик стандартной математики развития нормализованной финансовой системы в срезе мировой экономики. По нашим просчетам - лишь такой формат роста массы монет может обеспечить постепенное и уверенное замещение всех, существующих на данный момент экономических инструментов.
Скорость добычи новых монет с помощью Парамайнига вычисляется из двух основных параметров, это количество монет на личном кошельке и количество монет на кошельках последователей до 888 уровней. По своим характеристикам Парамайнинг является системой MLM 2.0 исключающей из себя всё что отталкивает простого человека от сетевого бизнеса, но при этом вовлекает его в развитие сети для увеличения скорости добычи монет на личном кошельке.
Система ПараМайнинга при совершении любой транзакции в кошельке производит запись блокчейн содержащую в себе значение количества монет хозяина кошелька и количество монет в кошельках его последователей, в этот момент генерируются новые монеты на баланс кошелька.

Например: *Имея в кошельке 99PZM и 100000PZM 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. Таким образом мы получаем систему со сложным процентом которая для увеличения капитализации стимулирует пользователя совершать транзакции подключая новых держателей кошельков, увеличивая тем самым оборот своей структуры. По самым скромным расчетам ежемесячный прирост количества монет у такого пользователя составляет не менее 10%*

Система Парамайнинг является самым совершенным инструментом для продвижения и популяризации, так как она не имеет аналогов ни в одной современной криптовалюте. Основным преимуществом Парамайнинга 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. Прамайнинг работает на любом кошельке с балансом свыше 1PZM и автоматически останавливается при достижении баланса равного 1млн. PZM

Так же впервые применена система установления реферальных связей без использования каких либо ссылок. После создания нового кошелька система фиксирует в блокчейн от кого поступает первая транзакция и навсегда устанавливает реферальную цепочку, которую невозможно изменить, это позволяет с лёгкостью строить глобальные MLM сети и увеличивать скорость добычи новых монет.

Техническая реализация 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 приведет 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 PZM, достаточно всего одной монеты в электронном кошельке , который автоматически запускает Парамайниг. Это процесс, позволяющий без каких-либо затрат электроэнергии увеличить количество монет в кошельке. ПараМайнинг запускается с 1 монеты и останавливается автоматически при достижении 1 миллиона монет в кошельке. ПараМайнинг - это уникальный метод создания новых монет всеми пользователями одновременно, регулируемый двумя параметрами:

1. Количество монет в личном кошельке.

Скорость роста количества монет в %	**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

По предварительным расчетам, завершение ПараМайнинга может произойти спустя порядка 500 лет, с момента генерации первого блока.

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.

Аккаунты PRIZM

Prizm реализует 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 Кода-Соломона, 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 предваряются «PRIZM-», что делает адреса аккаунтов Prizm легко узнаваемыми и отличимыми от форматов адресов, используемых другими криптовалютами. Адрес учетной записи, закодированный Кодом-Соломона, связанный с секретной кодовой фразой, генерируется следующим образом:

1. Секретная кодовая фраза хэшируется с помощью SHA256 для получения личного ключа аккаунта.
2. Закрытый ключ зашифровывается 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 Кода-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 жетонов, 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 в клиентах Prizm. Он представляет текущий баланс счета, за вычетом монет, участвующих в неподтвержденных, отправленных транзакциях.
- Гарантированные балансы активов перечисляют (составляют список) гарантированные балансы всех активов, связанных с конкретным аккаунтом.
- Неподтвержденные балансы активов перечисляют неподтвержденные балансы всех активов, связанных с определенным аккаунтом.

Wallet.dat

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

Подтверждение транзакций

Все транзакции PZM считаются неподтвержденными до тех пор, пока они не будут включены в действительный блок сети. Новые созданные блоки распределяются в сеть 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 (блокчейн), 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 (дедлайн), 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 транзакции 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

Основы криптографии PRIZM

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. Реализации Next на Java были рассмотрены DoctorEvil в марте 2014 года. 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.

Основные особенности

Продвинутый JavaScript клиент

Удобное клиентское приложение, Второго поколения, встроенное в дистрибутив основного программного обеспечения Prizm, и 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.

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.

Портативные устройства

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.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ PRIZM

1. POS - тип форжинга
2. Смешение двух технологий paramining + forging одновременно

Paramining. Исходный коды закрыты (не выложены), до определенных времен, в качестве защиты против клонов, как гарантия что система будет ликвидной.

3. Партнерская программа 888 уровней в структуре
4. Ядро криптосистемы NEXT / Proof of stake
5. User-friendly interface для мобильных устройств,
6. пароль пользователей не передается на сервер

Проблемы

Ничего на кону.

В атаке «ничего не поставлено на карту», форжеры пытаются построить блоки поверх всех вилок, которые они видят, потому что это им обходится почти в ничто, и потому, что игнорирование любой вилки может означать потерю на блоке вознаграждений, которые будут заработаны, если бы эта вилка была предназначена чтобы стать цепочкой с наибольшей кумулятивной трудностью. Хотя эта атака теоретически возможна, в настоящее время она непрактична. Сеть Prizm не испытывает длинных вилок блокчейна, а награда за низкие блоки не дает веского стимула для прибыли; Кроме того, компрометируя

безопасность сети и доверие ради такой небольшой прибыли, можно было бы сделать любую победу пиррикой.

Атаки на историю

В «атаке на историю» кто-то приобретает большое количество монет, продает их, а затем пытается создать успешную вилку только перед тем, как их монеты были проданы или обменены. Если атака не удалась, попытка ничего не стоит, поскольку монеты уже проданы или переданы; Если атака прошла успешно, атакующий получает свои жетоны обратно. Экстремальные формы этой атаки включают получение закрытых ключей из старых учетных записей и их использование для построения успешной цепочки прямо из блока генезиса. В Призм основная атака истории обычно не срабатывает, потому что все ставки должны быть неподвижными на 1440 блоков, прежде чем их можно будет использовать для форжинга; Кроме того, эффективный баланс аккаунта, который генерирует каждый блок, проверяется как часть проверки блока. Крайняя форма этой атаки обычно не срабатывает, так как блокчейн PRIZM не может быть реорганизован более чем на 720 блоков позади текущей высоты блока. Это ограничивает временные рамки, в которых плохой актер мог установить эту форму атаки.

Приложение

Проблемы Биткойна, рассмотренные через Prizm.

Prizm был создан как криптовалюта 2.0 - ответ Биткоину. Prizm использует функции, которые хорошо зарекомендовали себя в Биткойне, и рассматривают аспекты, вызывающие озабоченность. В этом приложении рассматриваются проблемы с протоколом и сетью Bitcoin, которые сглаживаются технологией Prizm.

Размер Блокчейна

Биткойн Блокчейн представляет собой полный последовательный сбор сгенерированных блоков данных, содержащих электронную книгу регистров для всех транзакций Биткоин, происходящих с момента его запуска в январе 2009 года. Четыре года спустя в январе 2013 года размер блокчейна Биткойна составлял 4 гигабайта (ГБ) - примерное количество данных, необходимых для хранения двухчасового фильма на диске DVD. Восемнадцать месяцев спустя, в июле 2014 года, размер блокчейна Биткойна увеличился почти в пять -до19 гигабайт (ГБ) 37. Биткойн-блокчейн подвергается экспоненциальному росту, и модификации исходного протокола Биткойн потребуют решения этого.

Количество транзакций 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 клиентов, ограничивает максимальную пропускную способность существующей сети Bitcoin до около 7 ТПС. Сравните это с пропускной способности сети VISA для обработки 10000 ТПС, и вы увидите, что Bitcoin не может конкурировать, как она существует сегодня.

Ответ PRIZM

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 на подтверждение транзакций

Время подтверждения транзакций для Биткойн варьировалось от 5 до 10 минут большей части в течение 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 Биткойн требуются несколько проверок (обычно шесть предпочтительных подтверждений), один час может легко пройти до того, как будет завершена продажа активов, оплачиваемых Биткойном.

Ответ 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 централизации

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 Биткойном, привел к созданию крупных одноуровневых установок специализированного майнинг оборудования 44, а также опору на небольшой набор крупных майнинг пулов 45. Это привело к эффекту «централизации», где Большие объемы майнинга сосредоточены в контроле за уменьшающимся числом людей. Это не только создает такую структуру мощности, 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 46 и выполнить 51% -ную атаку. Также существуют атаки, требующие всего лишь 25% от общей мощности хеширования сети. 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.

Ответ PRIZM

Стимулы, предоставляемые алгоритмом Proof of Stake, используемом в Prizm, обеспечивают низкий возврат инвестиций примерно на 0,1%. Поскольку с каждым блоком не генерируются новые монеты, 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.

Proof of Work - расходы на содержание

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», 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, 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 биткойнов - 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 биткойны 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 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!» [6]. 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.

Решения Prizm

Анализ стоимости и энергоэффективности сети Prizm показывает, что вся экосистема PRIZM может поддерживаться примерно за 60 000 долларов США в год, что в настоящее время почти в 2200 раз дешевле затрат на эксплуатацию сети Биткойн.

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. На момент написания, это награда 25 BTC, что составляет 10% инфляции в общем объеме поставок Биткоинов только в этом году. За каждый биткойн в 1000 долларов тот, которому он принадлежит, этот человек платит по 100 долларов за биткойн в этом году, чтобы «заплатить» майнерам за безопасность сети.

Да пребудет с Вами сила PRIZM!