PPCoin: Криптовалюта с подтверждением ставки (Proof-of-Stake)

Sunny King, Scott Nadal

19 August, 2012

Абстракция

Новый дизайн одноранговой криптовалюты, созданный на основе Биткойна от Сатоши Накамото: *Доказательство Ставки* (Proof-of-Stake) заменяет *Доказательство Работы* (Proof-of-Work), чтобы обеспечить большую безопасность сети. В соответствии с этим гибридным дизайном *Доказательство Работы* в основном обеспечивает первоначальное производство монет, а в долгосрочной перспективе в значительной степени не является необходимым. Уровень сетевой безопасности не зависит от долгосрочного потребления энергии, обеспечивая таким образом энергоэффективную и более экономичную и конкурентоспособную крипто валюту. *Доказательство Ставки* основано на возрасте монеты и генерируется каждым узлом с помощью схемы хеширования, которая похожа на Биткойн, но в ограниченном пространстве поиска. История блокчейна и расчет транзакций дополнительно защищены центральным механизмом, который распространяет контрольные точки.

Вступление

С момента создания Биткойна (Накамото, 2008) *Доказательство Работы* (PoW) был преобладающим дизайном в одноранговых криптовалютах. Концепция *Доказательства Работы* была основным стержнем и производственной моделью Накамото.

В октябре 2011 года мы поняли что концепция *Возраста Монет* поможет создать альтернативный дизайн, известный как *Доказательство Ставки* (PoS), на базе дизайна *Доказательство Работы* в Биткойне. Тогда мы оформили проект, в котором *Доказательство Ставки* используется для построения модели безопасности одноранговой криптовалюты и части ее производственного процесса, в то время как *Доказательство Работы* в основном облегчает начальную часть процесса, производство, и постепенно снижает свою значимость. Этот дизайн призван продемонстрировать жизнеспособность будущих криптовалют вне зависимости от энергопотребления. Я назвал проект ***ppcoin***.

Возраст монеты

Концепция Возраста Монет была известна Накамото по крайней мере с 2010 года и использовалась в Биткойне, например для определения приоритетов транзакций, хотя она не играла важную роль в модели безопасности Биткойна. Возраст Монеты просто определяется как количество сохраняющейся валюты. В простом примере, если Боб получил 10 монет от Алисы и хранил их в течение 90 дней, мы говорим, что Боб накопил 900 монет-дней в возрасте монеты. Когда Боб потратил эти 10 монет, которые он получил от Алисы, мы говорим, что монеты-дни, которые Боб накопил с этими 10 монетами, были израсходованы (*уничтожены*).

Чтобы упростить расчет возраста монет, мы ввели *временную метку* в каждую транзакцию. Временная *метка блока* и *метка транзакции* усилены для обеспечения расчета возраста валюты.

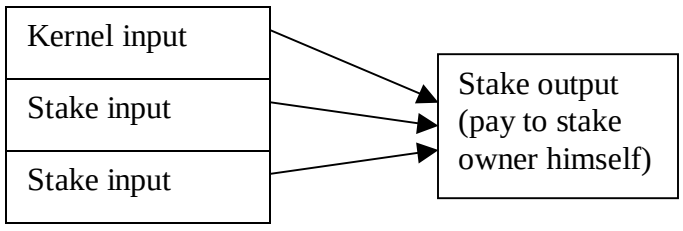
Доказательство Ставки (Proof-of-Stake)

Доказательство Работы внесла свой вклад в рождение большого прогресса Накамото, однако *Доказательство Работы* означает, что крипто валюта зависит от потребления энергии, что приводит к значительным расходам в работе этих сетей, которые несут пользователи за счет инфляций и комиссий за транзакции. Поскольку денежный курс в сети Биткойн замедляется, это может в конечном итоге оказать давление на увеличение комиссий за транзакции, чтобы поддержать предпочтительный уровень безопасности. Мы, естественно, задаемся вопросом, нужно ли нам поддерживать потребление энергии, чтобы иметь децентрализованную криптовалюту? Таким образом, мы решились на важный шаг как теоретически, так и технологически, чтобы продемонстрировать что безопасность одноранговой криптовалюты не должна зависеть от потребления энергии.

Концепция под названием *Доказательство Ставки* (Proof-of-Stake) обсуждалась в кругах Биткойн с 2011 года. В общем, *Доказательство Ставки* означает форму доказательства владения валютой. Возраст валюты, потребляемой транзакцией, можно рассматривать как одну из форм подтверждения ставки. Мы независимо друг от друга открыли концепцию *Доказательство Ставки* и концепцию *Возраст Монет* в октябре 2011 года, благодаря чему поняли, что *Доказательство Ставки* действительно может заменить большинство функций *Доказательства Работы*, с внимательной переработкой модели Биткойн. В основном это связано с тем что как и в *Доказательстве Работы, Доказательство Ставки* нельзя будет подделать. Конечно, это важнейшее требование денежных систем - исключить подделку. С философской точки зрения деньги - это форма доказательства прошлой работы, поэтому они должны быть в состоянии заменить доказательство работы сами по себе.

Генерация блоков с Доказательством Ставки

В нашем гибридном дизайне блоки разделены на два разных типа: блоки *Доказательства Работы,* и блоки *Доказательства Ставки*



Структура транзакции *Доказательство Ставки* и *Coinstake*

Доказательства Ставки в блоках нового типа, это специальная транзакция, называемая **coinstake** (*названная в честь специальной транзакции в Bitcoin Coinbase*). В блоке транзакции *coinstake,* владелец получает монеты потребляя срок

транзакции, одновременно получая привилегию создания сетевого блока путем выполнения *Доказательства Ставки*.

Первый вход монеты называется *kernel* и требуется для выполнения определенных целевых протоколов хеширования, что делает генерацию блока случайным процессом, аналогично блокам *Доказательства Работы*. Однако важным отличием является то, что операция хеширования выполняется в ограниченном пространстве поиска (*один хэш в секунду на выходе из неиспользуемого кошелька*) вместо неограниченного пространства поиска, как в *Доказательства Работы*, поэтому у нашей концепции нет значительного потребления энергии.

Цель хэша - достичь основу ставки, эта цель на единицу возраста монеты (*монеты-дни*), потребляемой в ядре (*в отличие от целевого значения в Доказательства Работы, которое является фиксированным целевым значением, применимым к каждому узлу*). Таким образом, чем больше израсходован возраст монет в ядре, тем больше вероятность того, что хеш будет выполнен.
Например, если у Боба есть кошелек, в котором накоплено 100 монет-дней, ожидается что он достигнет ядра за 2 дня, тогда как Алиса с ее выходом из 200 монет-дней может ожидать около одного дня.

В нашем проекте и хэш цель *Доказательства Работы*, и хэш цель *Доказательства Ставки* постоянно корректируются, это лучше чем двухнедельный интервал корректировки в Биткойне. Это сделано для того чтобы избежать резкого скачка в скорости генерации сети.

Чеканка на основе Доказательства Ставки (PoS)

Введен новый производственный процесс для блоков *Доказательства Ставки* в дополнение к майнингу с *Доказательством Работы* в Биткойне. Блок *Доказательства Ставки* делает монеты на основе потребленного возраста монеты в транзакции *Coinstake*. Скорость производства: 1 цент за потребленную монету-год выбрана для того чтобы вызвать низкую инфляцию в будущем.

Мы сохранили *Доказательство Работы* как часть процесса, чтобы облегчить первоначальное производство. Также возможно, что в системе *Чистого Доказательства Ставки* первоначальное производство может быть начато с блока генезиса (*первого блока*) посредством процесса аналогичного процессу на фондовом рынке. *Первоначальное Публичное Размещение акций (IPO).*

Основной протокол

Протокол определяет какой конкурирующий блокчейн выиграет чеканку с использованием возраста потребляемой валюты. Здесь каждая израсходованная транзакция в блоке, влияет на ценность блока. Блокчейн с наибольшим общим возрастом потребленных монет выбирается в качестве основного блокчейна.

Это контрастирует с блокчейном который использует *Доказательство Работы*, в протоколе Биткойн, где используется общая активность для определения основной цепочки.

Новый дизайн снимает беспокойство с *51% проблемой* в Биткойне, где система считается безопасной только тогда, когда хорошие узлы контролируют не менее 51% рабочей мощности сети. Стоимость контроля всегда должна быть выше, чем стоимость мощности майнинга, это бы увеличивало стоимость атаки для очень сильных организаций. Возраст монет злоумышленника расходуется во время атаки, что затрудняет продолжение атаки злоумышленником и предотвращает попадание сторонних транзакций в основную цепочку.

Контрольные точки (checkpoints): Защита истории

Одним из недостатков использования общего возраста потребленной монеты для определения основной цепочки является то, что это самая низкая стоимость атаки на цепочку блоков. Хотя Биткойн имеет относительно сильную защиту, Накамото также ввел контрольные точки в 2010 году в качестве механизма для усиления блокчейна, предотвращая любую возможную модификацию любой части блока перед контрольной точкой.

Еще одна проблема заключается в том, что стоимость двойной расходованной атаки можно было бы снизить, так как злоумышленнику может потребоваться только накопить определенный возраст для монеты и принудительно реорганизовать цепочку блоков. Чтобы сделать торговлю практичной в такой системе, мы решили ввести дополнительную форму контрольных точек, которые транслируются централизованно, с гораздо более короткими интервалами, несколько раз в день, чтобы заморозить блокчейн и завершить транзакции. Этот новый тип контрольной точки похож на систему предупреждений в Биткойн.

Laurie (2011) утверждал, что Биткойн не полностью решил проблему распределенного консенсуса, потому что механизм контрольных точек не распределен. Мы попытались разработать практичный протокол распределенных контрольных точек, но пришли к выводу, что защититься от сетевой атаки слишком сложно. Хотя механизм проверки вещания является формой централизации, мы считаем его приемлемым до того чтобы сделать доступным распределенное решение.

Другая техническая причина связана с использованием точек централизованного вещания. Чтобы защититься от типа атаки типа «отказ в обслуживании», ядро монеты должно быть проверено до того, как блок Доказательства Ставки может быть принят в локальную базу данных (*дерево блоков*) каждого узла. Из-за модели данных узла Биткойн (*спецификация индекса транзакции*) где требуется проверка чтобы обеспечить пропускную способность всех узлов, чтобы проверить соединение каждого ядра монеты перед принятием блока в дереве блоков. Из-за вышеупомянутых практических соображений мы решили не изменять модель данных узла, а вместо этого использовать центральные контрольные точки. Наше решение состоит в том, чтобы изменить расчет возраста монеты, чтобы он требовал минимального возраста, например одного месяца, ниже которого возраст монеты считается равным нулю. Затем используется центральная контрольная точка, чтобы

гарантировать что все узлы могут согласовать предыдущие транзакции старше одного месяца, что позволяет проверить соединение ядра монеты, так как ядро требует НЕнулевого возраста монет, поэтому должно использовать результат, полученный более месяца назад.

Подписи блоков и Дубликат Протокола Ставки

Каждый блок должен быть подписан его владельцем, чтобы злоумышленники не могли скопировать и использовать одно и то же *Доказательства Ставки*. Протокол *Дублированной Ставки* разработан для защиты от злоумышленника который с использованием одного *Доказательства Ставки* может генерировать множество блоков в качестве атаки с "отказом в обслуживании". Каждый узел собирает пару: (*kernel и временная метка*) всех транзакций, которые он видел. Если полученный блок содержит повторяющуюся пару, точно равной с ранее полученного блока, мы игнорируем такой блок (*повторяющаяся ставка*) до тех пор, пока не будет получен последующий блок (*orphan block*).

Энергетическая эффективность

Когда показатель *Доказательства Работы* приближается к нулю, все меньше и меньше стимулов для создания блоков. В этом долгосрочном сценарии энергопотребление сети может упасть до очень низкого уровня, поскольку незаинтересованные майнеры прекращают работу с блоками доказательств. Сеть Биткойн сталкивается с таким риском, и можно только увеличить комиссию транзакции до достаточно высоких уровней, чтобы поддерживать потребление энергии. Согласно нашему проекту, даже если потребление энергии приближается к нулю, сеть по-прежнему защищена *Доказательством Ставки*. Так мы называем это: долгосрочная, энергоэффективная криптовалюта даже при потреблении энергии в *Доказательстве Ставки* близкой к нулю

Прочие соображения

Мы изменили скорость генерации *Доказательства Ставки*, чтобы она определялась не высотой блока (*временем*), а сложностью. Когда сложность майнинга увеличивается, скорость создания *Доказательством Работы* снижается. Выбрана относительно плавная кривая, (*в отличие от ступенчатых функций Биткойна*), чтобы избежать искусственного шока рынка. Выбрана непрерывная кривая, чтобы каждое 16-кратное увеличение сложности вдвое уменьшало количество монет.

В долгосрочной перспективе кривая генерации с *Доказательством Работы* не будет слишком сильно отличаться от кривой биткойна с точки зрения инфляционного поведения, учитывая продолжение закона Мура. Мы считаем разумным последовать традиционному наблюдению, согласно которому рынок отдает предпочтение валюте с низкой инфляцией по сравнению с валютой с высокой инфляцией, несмотря на значительную критику Биткойн, некоторыми экономистами-идеологами.

Babaioff и его коллеги (2011) изучали влияние комиссии за транзакцию и утверждали, что комиссия за транзакцию является стимулом к отказу от сотрудничества между майнерами. В нашей системе эта атака еще больше, поэтому мы больше не взимаем комиссию за транзакцию чтобы заблокировать владельца.

Вместо этого мы решили полностью уничтожить комиссию за транзакцию. Это устраняет стимул не распознавать блоки других майнеров. Он также служит дефляционной силой, чтобы противостоять инфляционной силе что идет от чеканки с помощью *Доказательства Ставки*.

Мы также выбираем взимать комиссию за торговлю на уровне протокола, чтобы защититься от атаки вздутия.

В ходе нашего исследования мы обнаружили и третью возможность помимо *Доказательства Работы* и *Доказательства Ставки*, которую мы назвали *Proof of Excellence*. В соответствии с этой системой турниры проводится для чеканки монет на основе результатов участников турнира, имитируя призы реальных турниров. Хотя эта система имеет тенденцию потреблять энергию когда искусственный интеллект преуспеет в вовлеченной игре. Я все же нашел эту концепцию интересной даже в такой ситуации, потому что она предлагает все таки разумную форму потребления энергии.

Заключение

После проверки нашего дизайна на рынке мы ожидаем, что модели *Доказательства Ставки* станут потенциально более конкурентоспособной формой одноранговой криптовалюты, чем проекты с *Доказательством Работы*, благодаря устранению зависимости от энергопотребления, что позволит снизить инфляцию, налоги на более низкие уровни транзакций при сопоставимых уровнях сетевой безопасности.

Подтверждение

Большое спасибо Ричарду Смиту за помощь в тестировании в разных сетях и другой работой.
Мы хотели бы поблагодарить разработчиков Сатоши Накамото и Биткойн, чья блестящая новаторская работа открыла нам глаза и сделала возможным такой проект.

Справка

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): “Сделать децентрализованные валюты наверное, невозможно, но надо сделать их хотя бы энергоэффективными.” (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)