Novacoin community.

Описание механизма эмиссии криптовалютной единицы novacoin.

Кривая эмиссии криптовалютной единицы novacoin уникальна - она неопределённая, т.е невозможно абсолютно точно предсказать, сколько монет будет существовать в конкретный момент времени, но эмиссия подчинена определенным правилам, которые преследуют следующие цели:

1) защитить децентрализованную систему от централизации на раннем этапе;

2) создать гибкий алгоритм эмиссии, в зависимости от числа транзакций в сети;

Кроме эмиссии, в novacoin есть и деэмиссия (уничтожение монет, потраченных на комиссию), которая сейчас не оказывает заметного влияния из-за малого числа переводов.

Эмиссия монет состоит из PoW- и PoS-эмиссии.

Описание отличительных особенностей PoW эмиссии

Идея PoW, в общем случае, берет свое начало от Bitcoin, с введением следующих, прошедших проверку временем улучшений.

PoW эмиссия за сутки определяется количеством блоков и величиной их награды.

Количество PoW блоков приводится к целевому интервалу времени между ними, через увеличение или уменьшение сложности создания каждого последующего PoW блока. Делается это динамически, а не порогово как в Bitcoin, то есть сложность изменяется после каждого нового блока (более плавное сглаживание изменений, призванных быть дополнительной защитой от прихода/ухода вычислительных мощностей в сеть).

Целевой интервал - промежуток времени между блоками, который задан крайними значениями от 10-ти до 30-ти минут, и стремится к 20 минутам в течение длительного времени в текущих, сбалансированных условиях работы сети, но временно сдвигается в сторону плавного увеличения или уменьшения к границам, описанным выше, при большом и длительном недостатке или избытке PoS блоков относительно их целевого интервала (количество PoS блоков также динамически подстраивается к их целевому интервалу при помощи изменения PoS-сложности).

Размер награды за PoW блок зависит от текущей PoW сложности и уменьшается пропорционально корню 6-й степени от сложности.

Награда за блок вычисляется по формуле:

nBlockReward = 100 / (difficulty / 0,000244) ^ (1/6)

Неопределенность эмиссии в PoW базируется на зависимости награды от общей сложности сети. (для справки: в bitcoin жестко прописаны скачки награды, так называемое уполовинивание награды в зависимости от времени существования сети).

На практике сложность в значительной мере зависит от рентабельности майнинга новакоина - следовательно, награда за PoW также зависит и от текущего биржевого курса криптовалюты. Однако использование корня 6-й степени очень сильно сглаживает это влияние. В данный момент награду можно принять равной 7.5 и нет каких-либо предпосылок для ее значительного увеличения, так как это потребовало бы значительного снижения сложности. Снижение сложности в два раза относительно текущей (сейчас она дает награду в 7.5 монет) увеличило бы награду лишь до 8.4 монет. Снижение сложности в 10 раз относительно текущей дало бы награду 11.0 монет. Таким образом даже снижение сложности в 10 раз, вызванное, например, снижением курса, увеличит награду за PoW блок лишь в 1.5 раза. То есть даже такое значительное изменение мало увеличит эмиссию. Таким образом, снизившаяся сложность майнинга оставит его столь же прибыльным, но уже для меньшего числа майнеров и их оборудования.

И наоборот, медленный, но уверенный рост производительности и удешевление оборудования для добычи так же медленно, но уверенно снижает эмиссию, даже без учета влияния курса.

Итого суточная эмиссия PoW составляет 360-1080 монет (со стремлением к средней величине в 540 монет при интервале в 20 минут между PoW блоками и текущей награде в 7.5 монет за блок).

Описание PoS эмиссии

Целевой интервал между блоками - 10 минут.
Награда за блок вычисляется:

nProofReward = min(10, CoinAge / 365 / (difficulty / 0.03125) ^ (1/3))

Неопределенность эмиссии в PoS - зависимость награды от сложности и веса в монето-днях выхода, генерирующего блок.

Определить точную величину PoS эмиссии значительно сложнее, чем сделать это для PoW эмиссии. Верхним её ограничением является 10 монет за блок, что при достаточно чётко поддерживаемом количестве 144 блока в сутки дает максимальную PoS эмиссию в 1440 монет в сутки. Реально же она гораздо меньше. Так как весьма проблематично заранее оценить среднее число монето-дней, использованных при генерации PoS блока, можно исходить именно из этого максимального ограничения, но учитывать, что на практике PoS эмиссия за сутки может быть меньше в несколько раз.

Также не стоит забывать о других факторах снижения эмиссии PoS:

- ограничение максимальной награды, превышающей лимит в 10 NVC (сейчас достаточно часты случаи обрезки, и даже иногда значимой обрезки, порядка сотен NVC);
- забытые и потеряные кошельки, которые уже никогда не сделают новых монет (включая уничтоженные 110к монет);
- обнуляющие накопленные монето-дни переводы монет при необходимости их траты (срочная трата, а также очень частое явление интенсивных переводов на биржу при сильных изменениях курса);
- другие варианты вынужденных переводов (например, отдельные входящие транзакции оказались настолько малого размера, что держатель был не в силах дождаться генерации ими блоков на фоне растущей PoS сложности и уменьшения награды);
- от желания снижения времени ожидания генерации PoS блока люди объединяют вновь полученые монеты и теряют при этом около 3-х дней хранения этих монет (такие случаи весьма часты, так как клиент чаще всего уменьшает транзакции разбивая их на две части при создании блока).

Влияние величины ROI PoS в этих обстоятельствах можно считать малозначимым. Тем не менее, оно создает дополнительное ограничение сверху на суточную PoS эмиссию - ее величина в долгосрочной перспективе не может превысить значение ROI (сейчас 34%) умноженное на величину всей денежной массы (сейчас это примерно 900 тысяч монет) и деленное на 365 (суток в году). Т.е. в данный момент это ограничение составляет около 840 монет в сутки.

Само значение ROI зависит от PoS сложности (динамика ее изменения малопредсказуема) и обратно пропорционально кубическому корню этой сложности. Верхнее его ограничение 100%, нижнее 1%:

ROI = (0.03125 / difficulty) ^ (1/3) * 100

Поскольку при 100% ROI ограничение на PoS в сутки выходит равным 2465 монет (и это число будет только увеличиваться при росте денежной массы), а это превышает вышеупомянутый достаточно жесткий лимит в 1440 - то возможность заметного влияния больших значений ROI на величину эмиссии можно не рассматривать.

Количество блоков и общая эмиссия в 2014 году по месяцам:

	PoW	**PoS**	**эмиссия**
январь	2190	4781	38372
февраль	1993	4369	30035
март	2376	4796	33700
апрель	2202	4386	30228
май	2298	4522	30759
июнь	2198	4276	29690

июль	2792	4544	35444
август	2800	4545	37707
сентябрь	2566	4213	34409
октябрь	2373	4321	29803
ноябрь	2166	4337	27601

Подсчёты показывают, что в первом полугодии соотношение PoW и PoS эмиссии составляло примерно 64/36%. К концу года оно немного изменилось (в основном это было вызвано ростом PoW сложности - и как следствие, уменьшением награды за PoW блок), и в октябре-ноябре составило 59/41%.

Деэмиссия

Как и в большинстве криптовалют, в novacoin присутствует необходимость уплачивать комиссию за совершение транзакций. Но в отличие, например, от Bitcoin, эти комиссии не включаются в награду нашедшему блок, а уничтожаются. Тем самым регулируется количество монет в обращении, и при дальнейшем развитии novacoin (росте числа транзакций и росте PoW и PoS сложности) может наступить момент, когда уничтожаемая комиссиями сумма станет равна или даже превысит эмиссию, что вызовет сокращение общего числа монет.

Обычная комиссия в novacoin составляет 0.001 NVC за транзакцию, точнее, за 1000 байт данных, включенных в цепочку блоков. Также берётся дополнительная комиссия (0.001 NVC) за каждый выход меньше 0.01 NVC.

Однако, если транзакция удовлетворяет некоторым условиям, она может быть отправлена без комиссии. Для этого необходимо, чтобы одновременно выполнялись следующие условия:

1) размер транзакции должен быть меньше 1000 байт;
2) размер выходов должен быть больше либо равен 0.01 NVC;
3) dPriority > 1 000 000 * 144 / 250,
   где
   dPriority = sum (размер входа в сатоши * количество подтверждений) / размер транзакции в байтах.

Нужно учитывать, что комиссия может взиматься и при генерации PoS блока. Это возможно в двух случаях:

-- блок был сгенерирован очень мелким выходом, и размер выхода (выходов) транзакции оказался меньше 0.01 NVC, либо dPriority оказался меньше 576 000;

-- при склейке нескольких мелких выходов размер транзакции превысил 1000 байт.

Конечно, эти правила комиссии действуют только для официального клиента. Если человек изменит базовый клиент, создаст транзакцию без комиссии (формально для которой требуется комиссия), и самостоятельно найдёт блок (неважно, PoS или PoW), в который включит эту нестандартную транзакцию, то такой блок будет принят сетью.

Терминология

CoinAge - связан с возрастом входов транзакций. CoinAge равен произведению количества монет и их возраста, измеряется в монето-днях. Возраст обнуляется при отправке монет, когда происходит подпись транзакции. CoinAge может использоваться для расчета обязательной комиссии, награды за блок или целевого значения.

Novacoin использует потребленный CoinAge для расчета награды за Proof-of-Stake блок.

CoinDayWeight - аналогично CoinAge, но возраст вычисляется с 30-дневным смещением до предела в 90 дней.

CoinDayWeight является параметром целевого значения в системе Proof-of-Stake.

nBlockTarget = CoinDayWeight * nNetworkTarget

Хеш доказательства должен удовлетворять nBlockTarget, так что более высокое значение CoinDayWeight означает более высокую вероятность создания блока Proof-of-Stake.

Графики для эмпирического анализа данных показателей на основе работающей сети с момента старта в марте 2013 года.

http://cryptometer.org/novacoin_104_week_charts.html

https://charts.novaco.in/#difficulty

https://charts.novaco.in/#totalcoins

Novacoin wiki: https://wiki.novaco.in/