

SegWit близко и что ждёт Bitcoin в ближайшее время

@DeCenter • July 13, 2017



Сегодня, 14 июля – первая из важных дат связанных с активацией SegWit.

SegWit (*Segregated Witness*) — это обновленный протокол с обратной совместимостью, первоначально предложенный командой разработчиков Bitcoin Core.

С момента появления, в декабре 2015 года, он стал краеугольным камнем их проекта по масштабированию сети Bitcoin и сейчас используется многими активными узлами биткоина.

SegWit также является частью Нью-Йоркского соглашения, подписанного в мае: альтернативного проекта масштабирования, который поддерживали 56 компаний и майнеры. И активируемый пользователями софтфорк (UASF) – **ВІР148** (предложение по улучшению Bitcoin 148), назначенное на 1 августа, которое тоже собирается активировать SegWit.

Различия заключаются в том, как именно должна произойти активация.

Первоначальное предложение было сделано командой разработчиков Bitcoin Core. В соответствии с требованиями **ВІР141** их код SegWit активируется, если за определенный период (примерно две недели) будет достигнуто согласие 95% майнеров. С учетом того, что майнеры, дающие свое согласие, действительно готовы поддержать это обновление, риск раскола блокчейна и криптовалюты биткоин будет минимальным.

Однако на данный момент свое согласие на **ВІР141** дали только 40–45% майнеров.

Поэтому часть пользователей Bitcoin выступает за активацию SegWit в рамках другого софтфорка **ВІР148**. С 1 августа их узлы будут отвергать блоки, не сигнализовавшие о поддержке **ВІР141**. Если это предложение будет поддержано большинством майнеров, они всегда будут претендовать на самую длинную активную цепочку блоков, что приведет к активации SegWit на всех согласившихся биткоин-клиентах и позволит избежать раскола.

Нью-Йоркское соглашение, также известное как **SegWit2x**, предполагает активировать SegWit согласно **ВІР91**. Как и в случае с **ВІР148**, все узлы **ВІР91** будут отвергать блоки, не давшие согласия на **ВІР141**. Однако в отличие от **ВІР148**, **ВІР91** нуждается в одобрении 80% майнеров, которое они должны подтвердить в течение двух дней. В этом случае вероятность раскола тоже будет минимальной.

Судя по голосованию, на данный момент основная часть пользователей поддерживает грядущее обновление, но даже этого в итоге может оказаться недостаточно.

Segwit



Что будет ждёт Bitcoin в случае хардфорка

Сценарий развития событий в Биткоине не будет сильно отличаться от того, что произошло с Эфириумом. Учитывая, что оба потенциальных блокчейна имеют достаточное количество сторонников, велика вероятность того, что оба они выживут после разделения.

Пользователи смогут хранить токены в обеих сетях, что будет рассматриваться как «безопасная игра» и распоряжаться своими средствами в обеих цепочках, пользуясь тем, что блокчейны будут бороться за пользователей при помощи хэшрейта и объема торговли.

«Если у вас есть биткоины и происходит хардфорк, то теперь у вас появляются биткоины в обеих сетях. Вам ничего не нужно делать». – *Андреас Антонопулос, эксперт в области Bitcoin*

При этом, майнерам либо придется выбрать одну из двух сетей, либо распределить свои мощности на два блокчейна. Блокчейн, получивший больше мощностей майнеров, будет более надежным. Так, хэшрейт сети Ethereum сейчас почти в 20 раз превосходит хэшрейт майнеров Ethereum Classic.

Как подготовиться к возможному хардфорку

Рекомендуется хранить свои биткоины в личном кошельке, который вы контролируете при помощи частных ключей. Это гарантирует, что ваши биткоины будут доступны в обоих блокчейнах.

«Средства, хранящиеся на бирже – не ваши. Именно такой статус они будут иметь в случае хардфорка», - *отмечает Антонопулос.*

Однако, даже если вы будете хранить свои биткоины на бирже, то возможно она позволит вам использовать средства в обеих сетях. Но стоит понимать, что это решение остается целиком и полностью прерогативой биржи и повлиять на него у вас не получится. Чтобы максимально обезопасить себя, имеет смысл хранить свои биткоины как в кошельке, так и оффлайн.

«Я рекомендую всем участникам сообщества разделять свои средства. Храните оффлайн часть своих BTC и никогда не продавайте их. Используйте для продажи другие запасы». – *Винни Лингэм, генеральный директор Civic*

Список важных дат



INSIDER PRO

14 июля – внедрение BTC1

BTC1 — это созданная по итогам Нью-Йоркского соглашения клиентская программа, ответвление кодовой базы Bitcoin Core. Бета-версия BTC1 была выпущена еще 30 июня. Однако, согласно предложению SegWit2x, именно 14 июля все майнеры, подписавшие Нью-Йоркское соглашение, должны установить бета-версию BTC1 и протестировать ее.

Это не окажет большого влияния на работу обычных пользователей или майнеров.

21 июля – подтверждение готовности майнеров к BIP91

В этот день узлы BTC1 будут отлажены и готовы к работе, но что еще более важно, это день, когда майнеры начнут сигнализировать о своей поддержке BIP91.

Это тоже не коснется обычных пользователей. Однако если вы майнер, то можете помочь активировать SegWit, отдав сигнал о своей поддержке BIP91. Для этого надо добывать блоки, сигнализирующие bit 4, используя BTC1 или любой другой биткоин-клиент с прошивкой BIP91.

23 июля – фиксация BIP91

Для активации BIP91 необходимо, чтобы из 336 последних блоков предложение поддержали 269, то есть 80%. Это займёт около 2 дней.

Опять-таки, это не коснется обычных пользователей. Однако если вы майнер и BIP91 будет активирован, то у вас будет еще пара дней на то, чтобы присоединиться к этому софтфорку.

25 июля – активация BIP91

25 июля, еще через 336 блоков после «фиксации» результатов, BIP91 может быть полностью активирован. Все блоки, не сигнализировавшие о своем согласии с протоколом Segregated Witness (в рамках BIP141), теперь будут отвергаться.

Обычных пользователей это по-прежнему не коснется. Но если вы майнер, то теперь вы сможете добывать только блоки, которые сигнализировали о своей поддержке SegWit (BIP141). Иначе есть риск, что большинство майнеров будет отвергать ваши блоки.

29 июля – дедлайн по BIP91

Если майнеры не хотят раскола биткоина, то 29 июля станет для них первым дедлайном.

Для того, чтобы BIP91 при активации был совместим с BIP148, все должно быть зафиксировано в этот день не позднее 11:00 МСК. Но чем раньше это случится, тем лучше. Чем ближе к дедлайну, тем выше риск того, что активация не произойдет вовремя.

Если BIP148 не успеют активировать до этого дедлайна, может произойти раскол.

Если вы майнер и BIP91 не был активирован 29 июля, то у вас есть два дня на то, чтобы выбрать, в каком блокчейне продолжать майнинг с 1 августа: в BIP148 или в исходной цепочке блоков (Legacy).

31 июля – дедлайн по BIP141

Технически, 31 июля у майнеров будет еще один шанс избежать раскола.

Не позднее этой даты произойдет либо активация BIP91, либо фиксация результатов по BIP141. Иначе говоря, если по BIP91 не было вовремя достигнуто согласия, то остается двухнедельный срок, в течение которого требовалось согласие 95% майнеров на активацию SegWit.

В реальности шансов на то, что последний день этого срока придется именно на 31 июля, очень немного. И даже если так случится, то, скорее всего, о том, будет ли достигнут порог согласия в 95%, станет известно заранее.

Поэтому, как объяснялось выше, готовиться к возможному расколу пользователям и майнерам следует уже с 29 июля. 31 июля — это последняя возможность что-то сделать.

1 августа – активация BIP148

В этот день произойдет активация BIP148, и для майнеров настанет третий и последний дедлайн для того, чтобы избежать раскола.

1 августа в 03:00 МСК (обратите внимание, что в США еще будет продолжаться 31 июля) все узлы BIP148 начнут отвергать блоки, не сигнализировавшие о своей поддержке протокола Segregated Witness (по условиям BIP141). Если предложения BIP141 от команды Bitcoin Core или BIP91 от BTC1 будут вовремя одобрены и/или активированы, то раскола блокчейна не произойдет.

Если же ни одно предложение не пройдет, у майнеров останется последний шанс избежать раскола, самостоятельно поддержав BIP148 большинство голосов. Это будет означать, что они всегда будут выбирать самую длинную цепочку, принятую существующими узлами Bitcoin, и активируют SegWit через BIP141.

Если ни BIP141, ни BIP91 и BIP148 не привлекут достаточную мощность хеша к 1 августа, а BIP148 действительно получит некоторую поддержку, цепь может разделиться. Если это произойдет, возникнут два типа биткоинов, которые мы будем называть 148 Bitcoin (или 148BTC) и Legacy Bitcoin (или LegacyBTC).

Если на момент раскола у вас будут биткоины (читай: личные ключи), вы автоматически станете владельцем как 148BTC, так и LegacyBTC. Вероятно, для доступа к обоим типам валюты понадобится новое программное обеспечение.

Тем не менее, если вы обычный пользователь, разумным решением будет приостановить любые транзакции, по крайней мере, до тех пор, пока ситуация не прояснится. В ином случае вы можете потерять деньги.

Если раскол случится, майнерам придется решить, какую цепь использовать (конечно, вы все равно сможете переключиться в любой момент — например, если захотите работать с самой прибыльной цепью).

4 августа – возможный запуск Bitcoin ABC

Хотя точная дата еще не установлена, 4 августа может стать днем появления нового типа биткоина — ABC.

Bitmain, один из крупных производителей устройств для майнинга, недавно объявил, что на случай, если BIP91 не активируется до 1 августа, а BIP148 покажет признаки жизни после этого срока, компания запустит «план на случай непредвиденных обстоятельств». О реализации этого плана действий, названного Bitcoin ABC, было объявлено на конференции Future of Bitcoin.

До 1 августа Bitcoin ABC будет делить общую историю с биткоином, но после в течение первых нескольких дней, вероятно, будет приватизирован Bitmain. Он также будет включать в себя несколько изменений протокола, в том числе несовместимых с прежним. Одно из самых важных изменений — увеличение лимита на размер блока.

Если на момент раскола — 03:00 МСК 1 августа — у вас уже были биткоины, то вы автоматически получите Bitcoin ABC. В этом случае вам может понадобиться дополнительное программное обеспечение, чтобы отправлять (и получать) валюту.

Майнеры смогут начать добычу Bitcoin ABC с 4 августа, если не раньше.

15 августа – потенциальные изменения в работе ВР148

Форк ВР148, который появится 1 августа, изначально активируется пользователями, а не майнерами. Пользователи будут отклонять любые блоки, которые не выглядят совместимыми с Segregated Witness (за ВР141). Это должно побудить майнеров придерживаться цепи ВР148 (в идеале, до тех пор, пока она не останется единственной). Но действительно ли это произойдет, пока неясно. До сих пор мало кто из майнеров публично заявил о поддержке UASF.

Если майнеры не поддержат Bitcoin 148, некоторые пользователи валюты могут выбрать хардфорк для изменения алгоритма проверки работоспособности. Это приведет к «увольнению» существующей группы майнеров, поскольку их оборудование ASIC с точки зрения ВР148 будет устаревшим, и открыты возможности для новых майнеров. Домашние фермы на процессорах CPU или GPU могут вернуть прежние позиции в добыче — по крайней мере, временно.

Открытая рабочая группа ВР148 на подканале Slack, которая называется Bitcoin-Core Community, в настоящее время разрабатывает детали предложения. Но судя по всему, если к 15 августа Bitcoin-148 покажет менее 15% от общей мощности хэширования, произойдет размещение хардфорка. Это будет означать окончательный раскол с Legacy Bitcoin.

Также это может привести к другому расколу на стороне Bitcoin 148, если некоторые из его пользователей откажутся присоединиться к хардфорку, который изменит алгоритм доказательства работы.

Если вы постоянный пользователь, владели биткоином во время раскола 1 августа, и не тратили биткоины до 15 августа, то станете обладателем NewPoWBTC. Если вы купили или заработали 148BTC с 1 августа по 15 августа, то после этого периода вы тоже станете обладателем NewPoWBTC.

Но если вы решили потратить биткоины, чтобы поддержать ту или иную сторону, все не так просто. Опять же, если вы хотите обезопасить себя, воздержитесь от любых сделок, пока ситуация не прояснится.

Если вы принадлежите к немногочисленной категории людей, которые занимались майнингом Bitcoin 148 на оборудовании ASIC, возможно, вы захотите от него отказаться.

И, конечно же, любой человек сможет работать с NewPoWBTC без специализированного оборудования ASIC.

Вторая половина августа – закрепление SegWit

Если бы майнеры избежали раскола цепи ВР141, ВР91 или ВР148, Segregated Witness должен был вступить в стадию закрепления в второй половине августа. Это событие ничего бы не значило, если бы прошло по протоколу ВР91 или ВР148, как ожидалось, и ничего бы не изменило.

Но «закрепление» означает, что все клиенты, поддерживающие SegWit, начнут применять новые правила в следующий период сложности: через две недели.

Поэтому, если вы обычный пользователь и хотите получить доступ к новым функциям или обеспечить первоклассную безопасность, у вас теперь есть две недели, чтобы приобрести программное обеспечение для SegWit.

Если раскола цепи не избежать, ситуация серьезно усложняется. К середине августа может появиться один, два, три или даже четыре «биткоина»: Bitcoin 148, NewPoW Bitcoin, Bitcoin ABC, а также Legacy Bitcoin.

В данный момент трудно сказать, как лучше справиться с этой ситуацией. *Обычному пользователю всегда лучше держаться за свои личные ключи, и, вероятно, вообще не совершать транзакции, пока ситуация не решится так или иначе.*

Майнеру всего лишь нужно продолжать добычу на самой выгодной цепи.

Конец августа – активация SegWit

Если раскола цепи не произойдет, активация SegWit ожидается примерно в это время.

Если вы используете совместимый клиент, то сможете начать пользоваться новыми функциями, сохраняя при этом первоклассную безопасность.

Если раскола цепи не избежать, скорее всего, прогнозы в такой ситуации невозможны.

Конец октября – Хардфорк SegWit2x

В конце этого года или в начале 2018-го ожидается активация хардфорка SegWit2x. Точнее, хардфорк активируется на клиентах BTC1 через три месяца после закрепления SegWit. Эта активация означает, что для майнинга необходим «базовый блок» размером более 1 Мб, а это делает клиенты BTC1 несовместимыми со всеми биткоин-клиентами, в которых отсутствует код хардфорка.

На данный момент очевидно, что не все будут менять свое программное обеспечение для поддержки хардфорка. Сообщество разработчиков биткоина почти единогласно отклонило это предложение, в то время как несколько компаний-производителей заявили о том, что не намерены поддерживать изменения. Да и не все пользователи на это согласны. Таким образом, это может привести к новому расколу цепи.

Майнеры, которые используют только клиент BTC1, чтобы активировать SegWit, и не намереваются поддерживать хардфорк, к этому моменту должны перейти на другой клиент.

[Источник 1](#) (Оригинал)

[Источник 2](#) (Перевод)

[Наш канал в Telegram](#)

[Канал про ICO](#)

[Мы ВКонтакте](#)

[Наш YouTube](#)

[Мы в Facebook](#)

Наши чаты в Telegram:

[Общий](#)

[Майнинг](#)

[Про ICO](#)

[Торговля](#)

[Разработчики](#)

