Taproot: первое масштабное обновление биткоина за 4 года

Началось величайшее обновление биткоина за прошедшие 4 года. Случилось это благодаря тому, что все заинтересованные стороны наконец-то пришли к общему соглашению, которое было так необходимо для главной цифровой криптовалюты.

Taproot – это увеличение приватности и эффективности каждой транзакции. Обновление позволяет раскрыть возможности смарт-контрактов, все операции смогут проводиться без посредников.

Одной из главных частей обновления является усовершенствование цифровых подписей. Их можно сравнить с отпечатками пальцев, которые пользователи оставляют при транзакциях. Прежде был использован «алгоритм цифровой подписи с эллиптической кривой», который гарантировал надежность законным владельца, создавая подпись из закрытого ключа биткоин-кошелька. С обновлением будет доступна схема подписей Шнорра, которая при необходимости комбинирует несколько подписей в одну, а также делает простые и сложные транзакцию неотличимыми друг от друга. Это позволяет сэкономить место в блоках и повысить уровень конфиденциальности.

Благодаря усилению подписей появляются новые правила игры для смарт-контрактов. Если рассматривать смарт-контракты с теоретической точки зрения, они могут быть использованы в повседневной жизни, начиная от регистрации жилья и заканчивая оплатой коммунальных услуг. С обновлением Taproot смарт-контракты становятся дешевле, так как они проводятся одной транзакцией, а со снижением комиссии увеличивается масштабируемость сети. До Taproot для этих целей была чаще использована сеть Ethereum, но теперь биткоин становится достойным игроком в сфере децентрализованных финансов.

Первым концепцию Taproot описал Грегори Максвелл, разработчик Bitcoin Core в начале 2018 года. Запуск обновления подтвердили в июне 2021 года, а в октябре вышел клиент Bitcoin Core 22.0 с его поддержкой. Taproot стартовал 14 ноября 2021 года в 08:15, когда был добыт блок 709 632.

Taproot – обновление с обратной совместимостью. Хотя старые ноды и не прекратят работу в сети, пользоваться новыми возможностями они не смогут.