Хардфорк: отцы и дети криптовалют

Криптовалюты наглядный пример того как открытость может составить серьезную конкуренцию замкнутому корпоративному миру. Программный код доступный всем дал возможность быстрого создания новых цифровых монет с новыми функциями и лучшей безопасностью. Но по мере роста блокчейнов вносить «косметические» изменения все труднее и лучше сделать полностью независимый клон или хардфорк криптовалюты.

Цели создания новой монеты могут быть разными, но можно выделить три основных направления:

- решение проблем «родительской» валюты, такие как перегрузка сети bitcoin. Хардфорк Bitcoin Cash за счет увеличенного размера блока должен был уменьшить время подтверждения транзакций;

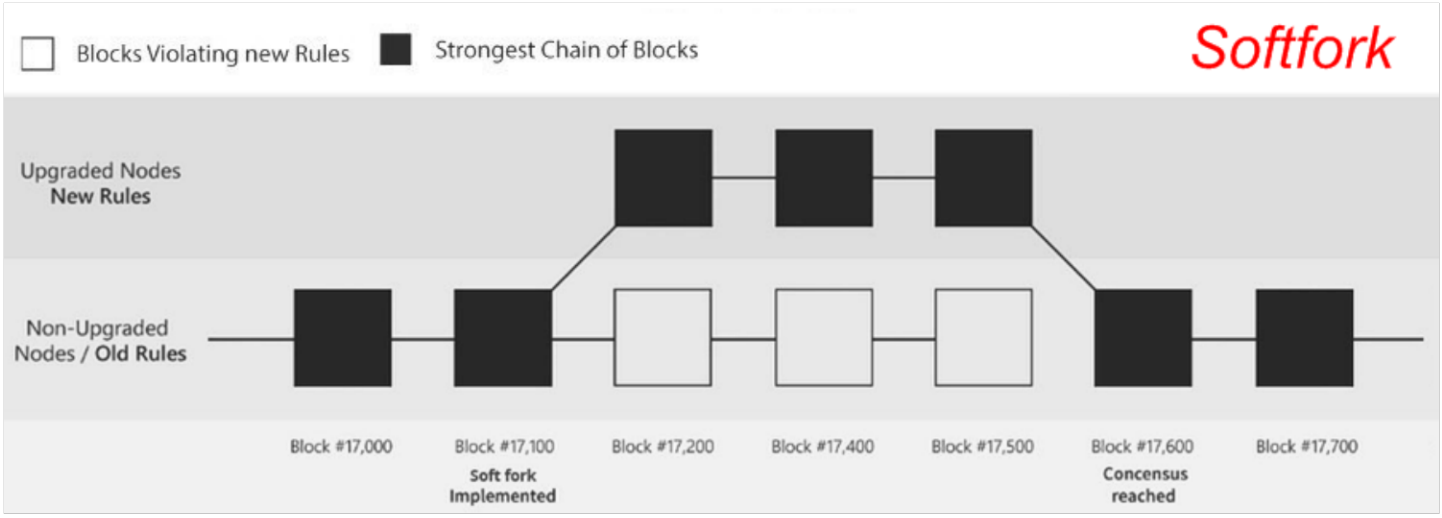
- маркетинговое. Хардфорк масштаба Ethereum сразу привлекает внимание и дает возможность выделиться, но важно соблюдать баланс между «пусканием пыли в глаза» криптосообществу и действительной пользой. Причины могут быть более серьезным, например, сохранение доли рынка в борьбе с ASIC-устройствами;

- мошенничество (скам). Сбор денег с последующим исчезновением. ICO также «грешат» подобным поведением, но законодательные ограничения делают подобный вариант все более рискованным. Проще и быстрее анонсировать несуществующий хардфорк.

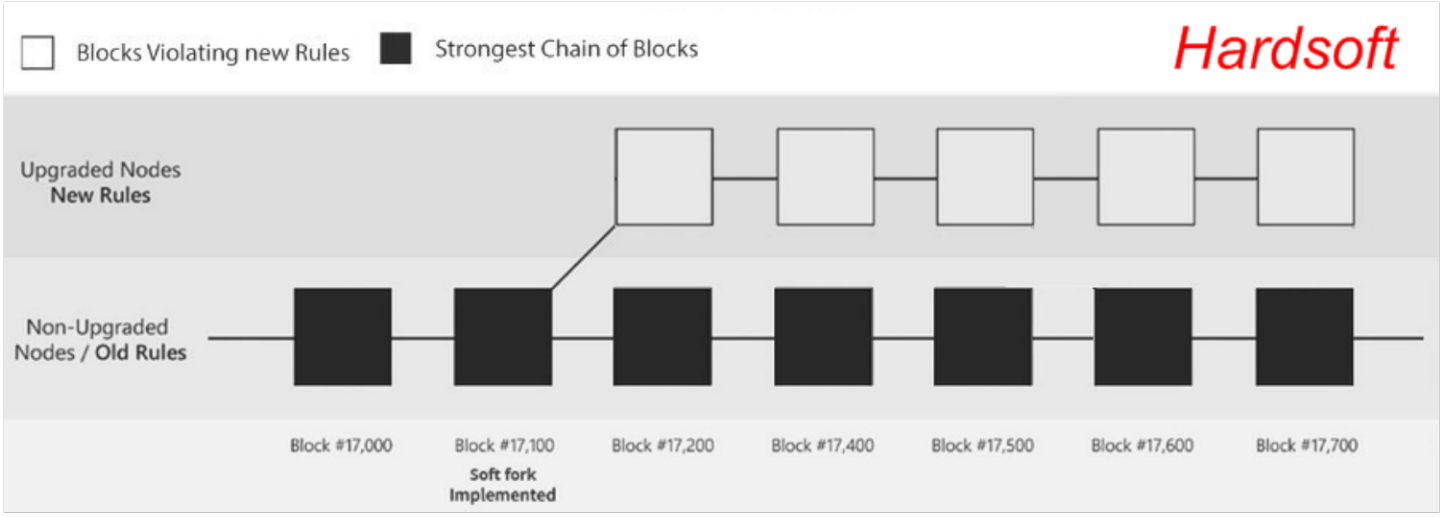
Как это работает

Для того чтобы понять, что такое hardfork напомним основной принцип блокчейна: каждый следующий блок подтверждающий транзакцию имеет ссылку на предыдущий. Таким образом, формируются непрерывные цепочки блоков, которые делают невозможным подделку информации в децентрализованном хранилище.

Логично предположить, что новая валюта должна иметь собственные блоки, отличающиеся от «родителя». Самый простой способ это использовать общий блокчейн и кошельки – Softfork.



Но если планируются изменения базового алгоритма, совместимость с базовым блокчейном становится невозможной, и, начиная с определенного номера блока, цепочки становятся полностью независимыми и происходит хардфорк.



Также потребуется отдельный кошелек для работы с новыми монетами.

Примеры удачных hardfork'ов…

Bitcoin
Первый хардфорк биткоина, долгое время занимавший второе место по стоимости и капитализации был Litecoin (Лайткоин). Ему удалось создать собственную экосистему и занять прочные позиции в финансовом секторе. По мнению аналитиков Лайткоин недооценен, и может резко вырасти в ближайшие 1-2 года.

Среди новых, безусловным лидером является Bitcoin Cash как по цене, так и по перспективам развития. Он имеет и собственный клон – Candy, который набирает популярность на волне интереса к «родителю».

Ethereum
Платформа больше ориентирована на softfork'и с общей базой смарт-контрактов Ethereum Network. Но проблемы перегрузки сети и уязвимости программного обеспечения потребовали кардинальных изменений и в августе 2017 г. был анонсирован двухэтапный хардфорк Ethereum Metropolis.

Первым этапом стал запуск в тестовом режиме новой сети для обработки контрактов ***Byzantium***, на втором этапе ***Constantinople*** планируется кардинальное изменение программного обеспечения и алгоритма майнинга. Точные сроки когда завершится хардфорк эфира неизвестны, впрочем, такая политика типична для Ethereum.

MONERO

Срочный хардфорк монеро 6 апреля 2018 г. был вызван анонсом Antminer X3 – первого ASIC-устройства для майнинга данной валюты. Разработчики остались верны своей приверженности CPU/GPU, чего нельзя сказать о пользователях. Часть из них решила остаться на старом блокчейн, как это произошло с Эфириумом. на старой платформе продолжается.

Хардфорк monero на старой платформе продолжается. Только за первую половину 2018 г. появились версии Zero, Classic, Original и MONERO 0. Оценить перспективность данных монет пока сложно, скорее они относятся к категории маркетинговых проектов.

BitShares

Платформа, ориентированная на децентрализованный обмен криптоактивами, построенная по принципу фондовых бирж. Позиционируется как аналог Эфириума для финансового сектора, имея собственный механизм смарт-контрактов.

Высокая скорость обработки транзакции стала одной из причин появления Ethereum Metropolis, но хардфорк BitShares в сентябре 2017 года еще больше увеличил отрыв от конкурента.

Как правильно пережить хардфорк

Разделение крупных валют кроме одобрения сообщества получают поддержку криптобирж и крупных майнеров поэтому хардфорк сети проходит без участия пользователей. Когда процесс завешен успешно в кошельках появляется дополнительный баланс с новыми монетами. Именно так поступил Bitcoin Cash – все владельцы получили количество BCH равное основному балансу Биткоин.

Когда небольшие криптовалюты делают hardfork, это всегда требует предварительного подтверждения, что на момент совершения на балансе кошелька имеются монеты базовой валюты. Сканированные копии не принимаются, так как легко подделываются, нужны закрытые ключи и после подтверждения получаете нужное количество на новый кошелек.

К чему приводит бездумная раздача ключей третьим лицам, показал хардфорк биткоин cash, когда поддельные (фишинговые) сайты получили количество ключей достаточное для кражи 33 миллионов долларов с Bitcoin и мультивалютных кошельков.

Правило №1. Старайтесь избегать проектов, в которых передаются закрытые ключи. Если все-таки решено поучаствовать переместите основную сумму на другой кошелек, а новые монеты выведите в надежное место, например, на криптобиржу. И больше не пользуйтесь hardfork кошельком!

Следующая проблема – у валюты нет собственного кошелька, и предлагается использовать сторонние приложения неизвестных разработчиков. Подобная ситуация была когда проводился хардфорк биткоин Diamond, где даже личности разработчиков остаются неизвестными. После перевода Биткоин на рекомендованные кошельки и предоставления ключей в момент разделения средства ушли в неизвестном направлении.

Правило №2. Не доверяем малоизвестным кошелькам и валютам без них. В открытом доступе, достаточно исходных кодов, чтобы создать кошелек, перед тем как начать хардфорк. Такое пренебрежение базовыми составляющими сразу говорит о ненадежности проекта.

Но, несмотря на проблемы это неплохой способ дополнительного заработка, если удачно выбрать, скажем, очередной хардфорк Биткоина. Свежие новости о предстоящих разделениях появляются каждый день, но лучше выбрать 2-3 валюты из группы лидеров для более тщательного анализа. Это будет страховкой от потери средств и нервов.