## 3 Модель безопасности PoW

В этом разделе мы представляем нашу модель безопасности блокчейна для количественной оценки оптимальных стратегий противостояния двойной трате и эгоистичному майнингу. Затем мы используем эти стратегии для сравнения показателей безопасности основанных на PoW блокчейнов, созданных с различными параметрами.

### 3.1. Модель безопасности

Наша модель расширяет Марковский процесс принятия решений (MDP), чтобы определить оптимальные состязательные стратегии и параметры:

*Частота устаревания блоков:* частота устаревания блоков $r_a$ позволяет нам учитывать различные размеры блоков, межблочных интервалов, задержек сети, механизмы распространения и конфигурацию сети (например, количество узлов).

*Мощность майнинга:* $\alpha$ - это доля общей мощности майнинга злоумышленника (остальная часть контролируется честной сетью).

*Стоимость майнинга:* затраты на состязательный майнинг $c_m \in [0, \alpha]$ соответствуют ожидаемой стоимости майнинга злоумышленника (т.е., общей стоимости майнинга, складывающейся из аппаратного обеспечения, электричества и человеческого труда) и выражается в виде награды за блоки. Например, если $c_m = \alpha$, стоимость майнинга злоумышленника эквивалентна его мощности майнинга, умноженной на награду за блок, т.е., стоимость майнинга покрывется ровно за счет заработанной честным майнингом награды за блок.

*Число подтверждений блока k:* Это число соответствует числу блоков, которое необходимо для подтверждения транзакции, чтобы финансист принял транзакцию.

*Возможность распространения:* Параметр распространения $\gamma$ отражает качество связи злоумышленника в сети (т.е., отражает долю сети, которая получает блоки злоумышленника, в случае когда злоумышленник и честные майнеры отправляют блоки в сеть одновременно).

*Влияние атак затмения.* Наша модель считает атаки затмения. Здесь мы предполагаем, что майнеры в честной сети оказываются под влиянием скорости устаревания блоков, когда злоумышленник и жертвы сговора не производят устаревших блоков. Это связано с тем, что злоумышленник может использовать любые добытые блоки для атаки и имеет только малый шанс добычи устаревшего блока после принятия честной цепи. Поэтому, на практике, показатели реальной скорости устаревания блоков злоумышленника значительно ниже, чем в честной сети. Особенности распространения и валидации в честной сети - причина, по которой она будет иметь большую частоту устаревания блоков. Заметим, что блоки, обнаруженный жертвой атаки затмения также могут продвигать частную сеть злоумышленника.

*Мы сравниваем это с существующими моделями, такими как модель Сапиршейна и других [31], которые сосредоточены только на эгоистичном майнинге и не могут отразить другие параметры блокчейна (с различной частотой устаревания блоков и подтверждений) и реальные параметры, такие как задержки сети.*

Чтобы проанализировать оптимальные стратегии двойной траты, мы определили сумму двойной траты как $u_d$, которая отвечает за минимальное значение транзакции, совершающей двойную трату, более выгодную, чем честный майнинг. Мы утверждаем, что $u_d$ является надежной метрикой для количественной оценки безопасности по отношению к атакам двойной траты. А именно, если вознаграждение за честный майнинг выше, чем выгода от нечестного поведения, финансисты могут безопасно принимать платежную транзакцию размером $u_d$ (так как такое значени считает безопасным, например, на основании данного числа подтверждений). Если, однако, поведение злоумышленника более выгодно, финансист должен избегать связанных с этим рисков двойной траты и связанных с этим намерений майнеров.

Мы фиксируем модель блокчейна, используя однопользовательское решение проблемы M := <S, A, P, R>, где все участники придерживаются стандартного протокола и S соответствует множеству состояний, A - множеству действий, P - матрице стохастического перехода, и R - матрице наград. Мы создаем экземпляры M как процесс принятия решений Маркова, описанный в разделах 3.2 и 3.3.

В нашей модели следующие действия доступны злоумышленнику:

*Принятие:* Злоумышленник принимает цепочку честной сети, что фактически соответствует перезапуску атаки. Это действие уместно, если злоумышленник считает, что вероятность победы над честной цепочкой мала.

*Переопределение:* Злоумышленник публикует на один блок больше, чем честная цепь и, следовательно, переопределяет конфликтующие блоки. Это случается, когда частная цепочка злоумышленника длиннее, чем текущая известная публичная цепочка (т.е. $l_a > l_h$) и для злоумышленника оптимально опубликовать $l_n+1$ из своих блоков, чтобы заменить уепочку честной сети своей собственной. Если злоумышленник использует майнинговые мощности жертвы, злоумышленник сможет использовать $b_{en}$ блоков от жертвы для переопределения.

*Соответствие:* Злоумышленник публикует столько блоков, сколько есть в честной сети и запускает гонку принятия между двумя цепочками, вместо переопределения честной цепочки.

*Ожидание:* Злоумышленник продолжает добычу в скрытой сети, пока блок не будет найден.

*Выход:* Это действие актуально только при изучении атаки двойной траты, так как оно соответствует успешной двойной трате с $k$ подтверждениями и осуществимо только когда $l_a > l_h$ и $l_a > k$.