(Introduction - 3 абзац)

В этой статье мы решаем данную проблему и предоставляем новую количественную структуру для анализа связи безопасности и производительности с различными алгоритмами консенсуса и параметрами сети блокчейнов, основанных на доказательстве работы (далее - PoW-блокчейнов). Используя нашу структуру, мы зафиксировали параметры безопасности как существующих реализаций PoW(например, Bitcoin, Etherium, Litecoin, Dogecoin), так и возможных реализаций с различными консенсусами и параметрами сети.

Наша структура (см. Рисунок 1) состоит из двух ключевых элементов: (I) экземпляр блокчейна и (II) модель безопасности блокчейна. Реализация блокчейна - это PoW-блокчейн в совокупности с предоставленным набором параметров консенсуса и сети, таких как задержка сети, время генерации блока, размер блока, механизм распространения информации и т.д. Например, Bitcoin, Litecoin и Etherium соответствуют 3 различным реализациям блокчейна. Для того, чтобы реалистично воссоздать любую другую реализацию блокчейна, мы разработали симулятор, который эмитирует консенсус и сетевой слой, реализуя, среди прочего, рекламо-подобный механизм распространения информации, незапрошенное выдвижение блоков, ретрансляционную сеть, механизм распространения заголовков.

Основной выходной параметр реализации блокчейна(измеренный или симулированный) - скорость устаревания(утери) блоков, которая поступает в модель безопасности. С другой стороны, наша модель безопасности основана на Марковском процессе принятия решений для двойной траты и эгоистичного майнинга и позволяет нам рассуждать об оптимальных состязательных стратегиях принимая во внимание мощность состязательного майнинга, влияние атак затмения, награду за блоки, параметры реальной сети и консенсуса - эффективно зафиксированные за счет скорости устаревания блоков.