(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 в блокчейнах, основанных на доказательстве работы (далее - PoW-блокчейнов). Используя нашу структуру, мы зафиксировали параметры безопасности как существующих реализаций PoW (например, Bitcoin, Ethereum, Litecoin, Dogecoin), так и иных 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, которые поступают в нашу 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 конкурентных стратегиях, принимая во внимание мощность конкурентного майнинга, влияние атак затмения, награду за блоки, параметры реальной сети и консенсуса - эффективно отраженные в скорости устаревания блоков.

Учитывая текущие дискуссии в сообществе Биткоина о подходящем максимальном размере блока, обеспечивающем масштабируемость и рост системы, наша работа позволяет целостно сравнить безопасность и эффективность PoW-блокчейнов при различных параметрах - включая размер блока. Например, мы обнаружили, что увеличение размера блока от текущей загрузки транзакций Bitcoin (в среднем - 0.5 МБ) до 4 МБ не оказывает значительного влияния на эгоистичный майнинг и устойчивость блокчейна к двойной трате, при условии, что механизм распространения блоков обеспечивает низкую скорость устаревания блоков. Мы резюмируем наши выводы следующим образом.

Краткое изложение выводов:

- Мы показали, что эгоистичный майнинг не всегда является рациональной стратегией. Поэтому, чтобы зафиксировать рациональные альтернативы, мы подсчитываем устойчивость к двойной трате PoW-блокчейнов и объективно сравниваем безопасность различных PoW-блокчейнов по отношению к необходимому числу подтверждений транзакций. Делая так, мы снабжаем финансистов знаниями для принятия решения о числе подтверждений

предоставленного значения транзакции, необходимом для обеспечения безопасности против двойной траты.

- Наши результаты показывают, что по причине меньших наград за блоки и большей скорости устаревания блоков в Ethereum по сравнению с Bitcoin (от 0.41% до 6.8% в силу более короткого времени подтверждения), Ethereum (интервал между блоками в диапазоне 10-20 секунд) требует по крайней мере 37 подтверждений, чтобы достичь безопасности Bitcoin (интервал между блоками в среднем 10 минут) с 6 подтверждениями против конкурента с 30% всей майнинговой мощности. Аналогично, Litecoin потребует 28, а Dogecoin 47 подтверждений блоков соответственно, чтобы соответствовать безопасности Bitcoin.
- Мы показываем, что чем больше награда за блок в блокчейне (в, например, долларах США), тем он более устойчив против двойной траты.
- В заключение, мы анализируем влияние изменяющегося размера блока и/или межблочного интервала на эгоистичный майнинг и двойную трату. Наши результаты, к удивлению, показывают, что установка размера блока в среднем на 1 МБ и уменьшение межблочного интервала до 1 минуты не снижает безопасность значительно. Поэтому, наши результаты показывают, что PoW-блокчейны могут достичь эффективной пропускной способности более 60 транзакций в секунду (т/с) (что означает, что текущая пропускная способность Bitcoin в 7 т/с может быть существенно увеличена) без ущерба для безопасности системы.

Оставшаяся часть статьи организована следующим образом. В Разделе 2 мы обозреваем базовую концепцию, лежащую в основе PoW-блокчейна, в Разделе 3 мы представляем нашу модель Марковского процесса принятия решений для количественного анализа безопасности PoW-блокчейнов. В Разделе 4, мы представляем наш симулятор и оцениваем безопасность и производительность нескольких вариантов реализаций блокчейнов, основанных на PoW. В Разделе 5, мы обозреваем связанную работу и мы приходим к заключению статьи в Разделе 6.

2. Основа

В данном разделе мы кратко излагаем операции уровня консенсуса и сетевого уровня существующих PoW-блокчейнов.

2.1 Уровень консенсуса

Доказательство работы (PoW) - самый широко развитый механизм консенсуса в существующих блокчейнах. PoW был впервые представлен Bitcoin и предполагает, что каждый участник одноранговой сети голосует своей “вычислительной мощностью” решая задачу доказательства работы и конструируя приемлемые блоки. Bitcoin, например, использует механизм PoW, основанный на хеш-функциях, что подразумевает поиск такого значения параметра nonce, при котором он, хешированный с дополнительными параметрами блока (например, хеш-функцией Меркла, хешем-функцией предыдущего блока), даст значение хеш-функции меньшее, чем текущее целевое значение. Когда такой параметр nonce найден, майнер создает блок и передает его на уровень сети (см. Раздел 2.2) соседним участникам одноранговой сети. Другие участники одноранговой сети могут подтвердить PoW посчитав хеш-

функцию блока и проверить, меньше ли она, чем текущее целевое значение.