Теоретико-игровые модели рынка криптовалют

М. Замешина, Н. Осипов

Московский физико-технический институт (государственный университет)

Bitcoin - это первая децентрализованная глобальная валюта. В своей статье [1] Сатоши описал механизм её работы на технологии Blockchain .Как и у любой другой валюты, её основная цель - облегчить обмен товарами и услугами, но в отличие от остальных, Биткоин решает проблему в распределении отслеживания и проверки транзакций, что позволяет считать эту систему безопасной для проведения глобальных транзакций.

Из-за большой дисперсии выигрыша при соло-майнинге и экспоненциального~роста хэшрейта сети стали создаваться mining pools, популяции которых составляют сотни тысяч. В нашей работе мы расскажем, чем математически отличается работа в пуле от соло майнинга и каким образом может распределяться выигрыш среди майнеров. Мы покажем динамику прыжков майнеров между пулами, полученную с помощью математического моделирования сети, с учетом количества транзакций и без, а также используя различные типы подсчёта параметров.

Система Proof-Of-Work устроена таким образом, что сложность криптографической задачи меняется с течением времени в зависимости от динамики хэшрейта. После открытия каждых 2016 блоков она пересчитывается. Рассмотрим времена между открытиями блоков. Оказывается, что этот процесс оказывается Пуассоновским. Для доказательства воспользуемся QQ-plot и методами корреляционных коэффициентов.

С помощью различных методов разделений награды, описанных в [2], смоделируем работу майнеров в сети. Пусть изначально все они майнят индивидуально. В случайные моменты времени они могут переходить в пулы друг друга, максимизируя функционал. Рассмотрим модели “близоруких майнеров”, усреднения прошлого, дисконтирования прошлого, функционала устойчивости к риску и посмотрим на асимптотическое поведение пулов майнеров.

Основываясь на [3], опишем еще игры с различным числом включаемых транзакций и без. Для первого варианта пулы максимизируют награду по количеству транзакций s_i, которые пул включает в блок в зависимости от того, сколько транзакций включают в блок другие пулы. Считается, что τ_s -- фиксированное время, нужное для обработки **s** транзакций. Во втором же случае считаем, что майнеры разбиваются на рискующих и тех, кто предпочитает оставаться майнить на месте.

В результате работы были найдены функции распределения числа найденных блоков и времени между моментами выигрыша индивидуальным майнером и майнером в пуле, обоснована пуассоновость процесса открытия блока и получены асимптотические поведения пулов при моделировании игр.

Литература

1. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system. – 2008.
2. *Rosenfeld M.* Analysis of bitcoin pooled mining reward systems //arXiv preprint arXiv:1112.4980. – 2011.
3. *Houy N.* The Bitcoin mining game. – 2014. MLA