УДК 004.056.5

ОЦЕНКА ВЕРОЯТНОСТИ ВЫИГРЫША ПРИ ПРОВЕДЕНИИ МАЙНИНГА НЕБОЛЬШОЙ ГРУППОЙ УЧАСТНИКОВ

А. В. Черемушкин

НИИ «Квант», г. Москва, Россия

В работах Ittay Eyal и Emin Gün Sirer показано, что протокол майнинга, реализованный в биткоине, является уязвимым к атаке со стороны группы участников, составляющей относительно небольшую часть от общего числа майнеров, позволяющей ей получить вознаграждение, превышающее размер доли имеющихся у них вычислительных ресурсов, и описана стратегия проведения т. н. корыстного майнинга. В данной работе описана уточнённая вероятностно-автоматная марковская модель корыстного майнинга, основанная на предположении о независимости обеих групп участников. Пусть доля вычислительных ресурсов у корыстной группы пропорциональна p, $0 < p < 1/2$, а у второй группы — $(1 - p)$. Рассматривается также ситуация, когда в случае разветвления цепочки блоков во второй группе часть участников, пропорциональная $\gamma(1-p)$, будет строить продолжение для цепочки, сформированной первой группой, а остальные (относительная доля $(1 - \gamma)(1 - p)$) — для второй цепочки. Основной результат состоит в обосновании уточнённого интервала $0 < p \leqslant 0{,}429$, соответствующего значениям параметра p, при котором корыстная группа получает относительное вознаграждение, превышающее вознаграждение при честном майнинге. Левая граница соответствует значению $\gamma = 1$, а правая — 0. Аналогично, при $0{,}358 \leqslant p \leqslant 0{,}454$ и подходящих значениях γ корыстная группа получает относительное вознаграждение, превышающее вознаграждение остальных участников.

Ключевые слова: *блокчейн, майнинг, марковская модель, вероятностный автомат.*

DOI 10.17223/20710410/49/5

SELFISH MINING STRATEGY ELABORATION

A. V. Cheremushkin

"Research Institute Kvant", Moscow, Russia

E-mail: avc238@mail.ru

As it was shown by Ittay Eyal and Emin Gün Sirer, the Bitcoin mining protocol is not incentive-compatible, because there exists an attack in which colluding miners obtain a revenue larger than their fair share. We describe an elaboration of Selfish-Mine Strategy and present an extended model of selfish mining based on independency hypothesis: both groups are made their work independently from each other. We describe a new state machine modelling selfish pool strategy. Let the selfish pool has mining power of p, $0 < p < 1/2$, and the others of $(1 - p)$. We also consider the situation in which the others mine a block on the previously private branch (frequency $\gamma(1-p)$), and the others mine a block on the public branch (frequency $(1-\gamma)(1-p)$). Main result is an elaboration of an interval in which selfish miners will earn more than their relative mining power: 1) for a given p, a pool of size p obtains a revenue larger

than than its relative size for p in the following range: $0 < p \leqslant 0.429$ (the left bound corresponds to $\gamma = 1$, and the right one — to $\gamma = 0$); 2) for a given p, a pool of size p obtains a revenue larger than a revenue of other group in the following range: $0.358 \leqslant p \leqslant 0.449$.

Keywords: *blockchain, mining, Markov model, state machine.*

Введение

В работе [1] анонсирована, а позднее в [2, 3] опубликована стратегия поведения выделенной (корыстной) группы участников майнинга, у которой суммарная вычислительная мощность принадлежащих им ресурсов не превосходит половины от общей вычислительной мощности, используемой для майнинга. Стратегия, названная авторами *стратегией корыстного майнинга*, позволяет получать данной группе вознаграждение, превышающее размер доли имеющихся у них вычислительных ресурсов. В её основе лежит утаивание части успешно подобранных блоков, с помощью которых можно уменьшить выигрыш остальной группы участников. Для обоснования предложенной стратегии авторы описали модель поведения всей системы, в рамках которой можно показать, что стратегия даёт выигрыш даже в случае, когда доля вычислительных ресурсов этой группы может составлять всего $1/3$ от общей суммарной вычислительной мощности всех участников майнинга.

В настоящей работе приводится уточнение данной модели, основанное на модели независимого поведения обеих групп.

1. Модель протокола формирования блокчейна

Напомним основные моменты способа формирования цепочки блоков (блокчейна) на основе поиска решения трудоемкой задачи. В криптовалюте Биткоин в качестве такой задачи выбрана задача подбора случайного вектора, который на входе хеш-функции вместе с хеш-свёрткой данных о транзакциях, входящих в данный блок, и свёрткой предыдущего блока даёт значение, имеющее в старших разрядах в двоичной записи n нулей, где n — большое число, определяющее сложность решения задачи. Средняя трудоёмкость M решения задачи подбора такого случайного вектора составляет 2^n операций хеширования, поскольку при случайном выборе аргумента вероятность появления на выходе хеш-функции такого значения составляет 2^{-n}. Поиск такого случайного вектора называется майнингом, которым занимается большое число майнеров, объединяющихся в группы (пулы) для увеличения вероятности успешного подбора. Разные пулы могут формировать различные наборы транзакций для очередного блока. Это является одной из причин появления разветвлений в блокчейне, когда появляется несколько продолжений для уже имеющейся цепочки блоков.

Параметры майнинга в биткоине обычно рассчитываются таким образом, чтобы один блок генерировался в среднем каждые 10 м. При фиксированной суммарной вычислительной мощности этот временной интервал t рассчитывается как математическое ожидание геометрического распределения $t = 1/P$. Здесь вероятность успешного подбора за секунду определяется равенством $P = V/M$, где V — производительность, т. е. число операций хеширования в секунду. Если суммарная вычислительная мощность V возрастает, то для сохранения этого интервала увеличивается трудоёмкость M подбора соответствующего значения хеш-свертки, т. е. параметр n.

В результате можно считать, что вероятность успешного формирования блока в этом временном интервале равна единице.

В случае, когда нескольким пулам удается успешно сфомировать продолжение для последнего блока, публикуется разветвление. Далее осуществляется поиск продолжения для каждого из вариантов и в конечном счёте оставляется то, которое имеет наибольшую длину. В этом случае вознаграждение получают те пулы, которые участвовали в формировании наиболее длинной цепочки. Чтобы ограничить время принятия, решения обычно ограничивают длину цепочек в разветвлении (например, шестью блоками). Будем рассматривать наиболее простую модель, когда длины цепочек в разветвлении не ограничены, а решение об оставлении принимается при простом превышении длин на 1; при этом пренебрегаем временем на пересылку данных и временем принятия решения.

2. Описание модели из [1]

Предложенный в [1] оригинальный метод основан на использовании теоретико-автоматной марковской модели поведения системы, представляющей собой вероятностный автомат со счётным множеством состояний $s = 0, 1, \ldots$, в котором к состоянию $s = i$ относятся все ситуации, в которых корыстная группа имеет преимущество в числе правильно сформированных блоков, сохраняемых в тайне и образующих цепочку из i блоков. При этом рассматриваются только те состояния, когда $i \geqslant 0$, поскольку в случае, когда группа остальных участников получает преимущество в числе правильно сформированных блоков, корыстная группа прекращает формирование своей цепочки, присоединяется к остальным участникам и начинает подбирать продолжение для цепочки, сформированной остальными участниками (тем самым осуществляется переход в состояние $s = 0$). В автомате введено ещё одно дополнительное состояние $0'$, соответствующее разветвлению на две цепочки одинаковой длины равной 1.

Пусть α, $0 < \alpha < 1/2$, — доля в суммарной производительности вычислительных ресурсов V, которой обладает группа корыстных участников майнинга. Тогда вероятность успешного формирования блока корыстной группой в течение временного интервала t равна $p = \alpha$, а для группы остальных участников соответственно $q = 1 - \alpha$. Для вычисления вероятностей нахождения автомата в каждом из состояний авторы [1] определяют вероятности перехода, исходя из предположения, что каждый раз успеха достигает либо одна, либо другая группа участников.

Идея состоит в том, что в случае успешного подбора очередного блока корыстная группа не обнародует результат, а держит его в тайне от остальных до тех пор, пока остальные участники сами не подберут очередной блок. В этом случае она поступает одним из следующих вариантов:

— если $s = 1$, то они обнародуют свой блок, создавая разветвление длины 1 и откладывая вопрос о том, какая из групп получит вознаграждение;
— если $s = 2$, то корыстная группа раскрывает оба своих блока, тем самым получая вознаграждение за два блока и лишая вознаграждения остальных участников;
— если $s \geqslant 3$, то они обнародуют блок, стоящий в начале своей сохраняемой в тайне цепочки, создавая разветвление из двух цепочек длины 1 либо увеличивая на 1 длину цепочки в существующем разветвлении, тем самым лишая группу остальных участников выигрыша.

Авторы [1] рассмотрели также случай, когда при наличии разветвления среди остальных участников найдется подгруппа, составляющая (по мощности) долю, равную γ, $0 \leqslant \gamma \leqslant 1$, которая будет пытаться продолжить ветку, созданную выделенной группой, тем самым повышая вероятность получения вознаграждения корыстной группой за блоки, подобранные ею ранее. Граф переходов вероятностного автомата,

моделирующего поведение участников, приведён на рис. 1. В алгоритме 1 [1] приняты следующие обозначения: L_{priv} — длина приватной цепочки, сохраняемой в тайне корыстной группой; L_{publ} — длина общедоступной цепочки в разветвлении.

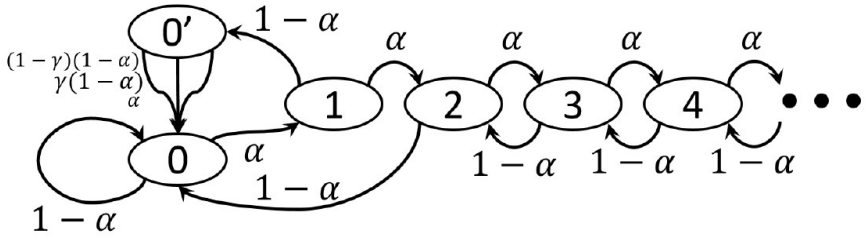

Рис. 1. Автоматная модель из [1]

Алгоритм 1. [1]

Инициализация
Общедоступная цепочка ← общеизвестные блоки.
Приватная цепочка ← общеизвестные блоки.
$L_{\text{priv}} := 0$.
Майнинг нового блока приватной цепочки.
Корыстная группа нашла блок
$\Delta_{\text{prev}} := L_{\text{priv}} - L_{\text{publ}}$.
Добавление нового блока к приватной цепочке.
$L_{\text{priv}} := L_{\text{priv}} + 1$.
Если $\Delta_{\text{prev}} = 0$ и $L_{\text{priv}} = 2$, **то**
    публикация всей приватной цепочки. *// Корыстная группа выигрывает благодаря большей длине на 1*
    $L_{\text{priv}} := 0$.
Майнинг нового блока приватной цепочки.
Другие нашли блок
$\Delta_{\text{prev}} := L_{\text{priv}} - L_{\text{publ}}$.
Добавление нового блока к общедоступной цепочке.
Если $\Delta_{\text{prev}} = 0$, **то**
    приватная цепочка ← общеизвестная цепочка. *// Вторая группа выиграла*
    $L_{\text{priv}} := 0$.
иначе
    Если $\Delta_{\text{prev}} = 1$, **то**
        публикация последнего блока приватной цепочки. *// Цепочки имеют одинаковую длину, разветвление длины 1*
    иначе
        Если $\Delta_{\text{prev}} = 2$, **то**
            публикация всей приватной цепочки. *// Корыстная группа выигрывает благодаря большей длине цепочки на 1*
            $L_{\text{priv}} := 0$,
            иначе $(\Delta_{\text{prev}} > 2)$
            Публикация первого неопубликованного блока приватной цепочки.
Майнинг нового блока приватной цепочки.

Рассмотренная в [1] модель позволяет успешно рассчитать вероятность получения вознаграждения, превышающего размер вознаграждения при честном майнинге: корыстная группа получает преимущество при выполнении неравенства

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2}.$$

3. Особенности предложенной в [1] модели

В [1] строится вероятностно-автоматная модель для случая, когда все майнеры разделены на две параллельно работающие группы, причём каждый раз успеха достигает либо одна, либо другая группа. Поэтому можно считать, что при переходе автоматной модели из одного состояния в другое производится бросание одной монеты с вероятностями выпадания сторон $p = \alpha$ и $q = 1 - \alpha$, а функционирование вероятностного автомата определяется последовательностью независимых испытаний с двумя исходами. Поскольку вероятности p и q определены для временного интервала t, для которого $p + q = 1$, то в рамках данной модели необходимо, чтобы выполнялось условие: после того как одна из групп достигает успеха, обе группы должны останавливать свои вычислительные устройства и начинать майнинг заново.

Обратим внимание на две особенности рассматриваемого подхода.

Во-первых, если бы обе группы придерживались стратегии честного майнинга и сразу объявляли об успешно сформированном блоке, то они бы одновременно начинали новый поиск очередного блока. Поэтому такую ситуацию можно было бы моделировать пуассоновским процессом с непрерывным временем с интенсивностью P, а моменты перехода автомата из одного состояния в другое совпадали бы с моментами останова компьютеров при успехе одной из групп. При этом выигрыш каждой из групп был бы пропорционален имеющимся вычислительным мощностям.

При использовании стратегии корыстного майнинга малая группа начинает утаивать результаты и синхронизацию времени по моментам подбора блоков нельзя произвести. Дело в том, что хотя бóльшая группа сразу объявляет о построенном блоке, малая группа может придерживать найденные блоки до тех пор, пока бóльшая группа не достигнет успеха, а затем раскрывать их, чтобы нейтрализовать выигрыш большой группы. Поэтому возможна ситуация, когда бóльшая группа ещё не смогла подобрать нужного хеш-значения и продолжает майнинг, а первая подобрала и утаила. С другой стороны, если бóльшая группа построила блок, но у меньшей группы есть несколько блоков в запасе, то она раскрывает первый блок своей цепочки для нейтрализации выигрыша другой стороны, но сама продолжает майнинг для поиска продолжения для последнего блока в своей цепочке. Поэтому моменты начала майнинга нового блока у разных групп разные.

Но граф переходов на рис. 1 строится исходя из условия, что при переходе в каждое состояние обе группы начинают подбор соответствующего блока заново, останавливая предыдущий поиск. Это делает данную модель моделью с дискретным временем. Поэтому в исходной работе, фактически, применяется более простая модель с дискретным временем, в которой синхронизация производится по фиксированным временным интервалам, в каждом из которых обязательно должен быть найден блок, причём числа p и q обозначают вероятности успешного подбора блока для корыстной группы и группы остальных участников в течение этого временного интервала.

Дискретная модель является, безусловно, огрублением реальной ситуации, когда время до следующего успешного формирования блока является случайной величиной.

Однако с её помощью можно просто оценивать вероятности успеха. Модель с дискретным временем часто используется для предварительной оценки ситуации. Главная идея авторов состоит в построении компактной вероятностно-автоматной модели, состояниями которой являются такие ситуации, когда первая группа имеет преимущество в некотором фиксированном числе сформированных блоков, сохраняемых в тайне от большей группы.

Вторая особенность заключается в следующем. На самом деле, две группы майнеров используют разные стратегии и решают разные задачи, действуя независимо. Это объясняется следующими соображениями. Поскольку группы используют разные стратегии и при этом одна из групп может скрывать результаты, то происходит параллельное решение двух задач двумя группами, обладающими разными вычислительными мощностями. Так как мощность у каждой из групп меньше общей суммарной, то теперь возможна ситуация, когда обе группы не успеют в течение заданного временного интервала подобрать нужного хеш-значения, что соответствует реальной ситуации, когда очередные блоки подбираются не в текущем, а в следующих временных интервалах. Также возможна ситуация, когда обе группы найдут искомые значения, одно из которых может быть скрыто корыстной группой. Если к концу временного интервала объявляется о нахождении двух разных продолжений цепочки блоков, причём одно из них оказывается длиннее, то для включения в блокчейн выбирается более длинная ветвь в разветвлении.

Поэтому более естественно эту ситуацию моделировать последовательностью независимых одинаково распределённых пар случайных величин (ξ_1, ξ_2) с вероятностями успеха $\mathsf{P}[\xi_1 = 1] = p$ (для первой группы) и $\mathsf{P}[\xi_2 = 1] = q$ (для второй группы).

Учтём это замечание и исследуем, как изменится модель для случая двух активных участников.

4. Уточнённый подход

Пусть, как и раньше, p — вероятность успеха в подборе нужного значения хеш-функции для корыстной группы, $0 < p < 1/2$, и $q = 1 - p$ — для группы остальных участников. Предполагаем, что обе группы являются однородными и моделируются двумя вычислителями с суммарными мощностями, пропорциональными данным вероятностям. Будем полагать, что обе группы действуют независимо, при этом попрежнему используется модель с дискретным временем. Рассмотрим автономный вероятностный автомат без выхода, множество состояний которого состоит из трёх групп. Первую группу составляют состояния s_i, $i = 0, 1, 2, \ldots$, в которых у корыстной группы участников имеется преимущество в числе подобранных хеш-значений для блоков, равное номеру состояния. Отрицательные значения, как и в предыдущей модели, не рассматриваются, так как они соответствуют нулевому состоянию. Вторую группу составляют состояния $s_{i,0}$, $i \geqslant 2$, в которых блокчейн допускает разветвление с двумя продолжениями и длина цепочки, сформированной корыстной группой, содержит на i блоков больше, чем цепочка, сформированная группой остальных участников майнинга. Случай $i = 1$ также не рассматривается, так как в этом случае первая группа раскрывает свою цепочку и система переходит в нулевое состояние. Третью группу образуют состояния $s_{i,i}$ при $i \geqslant 1$, которые соответствуют случаю разветвлений с двумя одинаковыми длинами продолжений исходной цепочки.

Стратегию поведения выделенной группы участников определим аналогично описанному в работе [1] алгоритму (алгоритм 2).

Алгоритм 2. Новый алгоритм

Инициализация
Общедоступная цепочка ← общеизвестные блоки.
Приватная цепочка ← общеизвестные блоки.
$L_{\text{priv}} := 0$.
Майнинг с головного блока приватной цепочки.
Корыстная группа нашла блок
$\Delta_{\text{prev}} := L_{\text{priv}} - L_{\text{publ}}$.
Добавление нового блока к приватной цепочке.
$L_{\text{priv}} := L_{\text{priv}} + 1$.
Если $\Delta_{\text{prev}} = 0$ и $L_{\text{priv}} \geqslant 2$, **то**
  публикация всей приватной цепочки, *// Корыстная группа выигрывает благодаря большей длине цепочки на 1*
  $L_{\text{priv}} := 0$.
Майнинг нового блока приватной цепочки.
Другие нашли блок
$\Delta_{\text{prev}} := L_{\text{priv}} - L_{\text{publ}}$.
Добавление нового блока к общедоступной цепочке.
Если $\Delta_{\text{prev}} = 0$, **то**
  приватная цепочка ← общеизвестная цепочка, *// Они выиграли*
  $L_{\text{priv}} := 0$;
иначе
  Если $\Delta_{\text{prev}} = 1$, **то**
    публикация последнего блока приватной цепочки, *// Цепочки имеют одинаковую длину, разветвление длины 1*
  иначе
    Если $\Delta_{\text{prev}} = 2$, **то**
      публикация всей приватной цепочки, *// Корыстная группа выигрывает благодаря большей длине цепочки на 1*
      $L_{\text{priv}} := 0$;
      иначе $(\Delta_{\text{prev}} > 2)$
      публикация первого неопубликованного блока приватной цепочки.
Корыстная группа нашла блок и другие нашли блок
$\Delta_{\text{prev}} := L_{\text{priv}} - L_{\text{publ}}$.
Добавление нового блока к приватной цепочке.
Добавление нового блока к общедоступной цепочке.
Если $\Delta_{\text{prev}} = 0$, **то**
  публикация новых блоков для обеих цепочек,
  $L_{\text{priv}} := L_{\text{priv}} + 1$; $L_{\text{publ}} := L_{\text{publ}} + 1$, *// Цепочки имеют одинаковую длину*
иначе
  Если $\Delta_{\text{prev}} = 1$ $(L_{\text{priv}} = 2)$, **то**
    публикация всей приватной цепочки, *// Корыстная группа выигрывает благодаря большей длине цепочки на 1*
    $L_{\text{priv}} := 0$;
    иначе $(\Delta_{\text{prev}} > 1)$
    публикация последнего блока приватной цепочки. *// Корыстная группа получает отложенный выигрыш за один блок*
Майнинг нового блока приватной цепочки.

Рассмотрим граф переходов вероятностного автомата, моделирующего поведение двух групп участников (рис. 2). В нём вершины помечены индексами соответствующих состояний, а переходы — парами ab, соответствующими значениям случайных величин $\xi_1 = a$ и $\xi_2 = b$ $(a, b \in \{0, 1\})$. Метки переходов приведены в табл. 1.

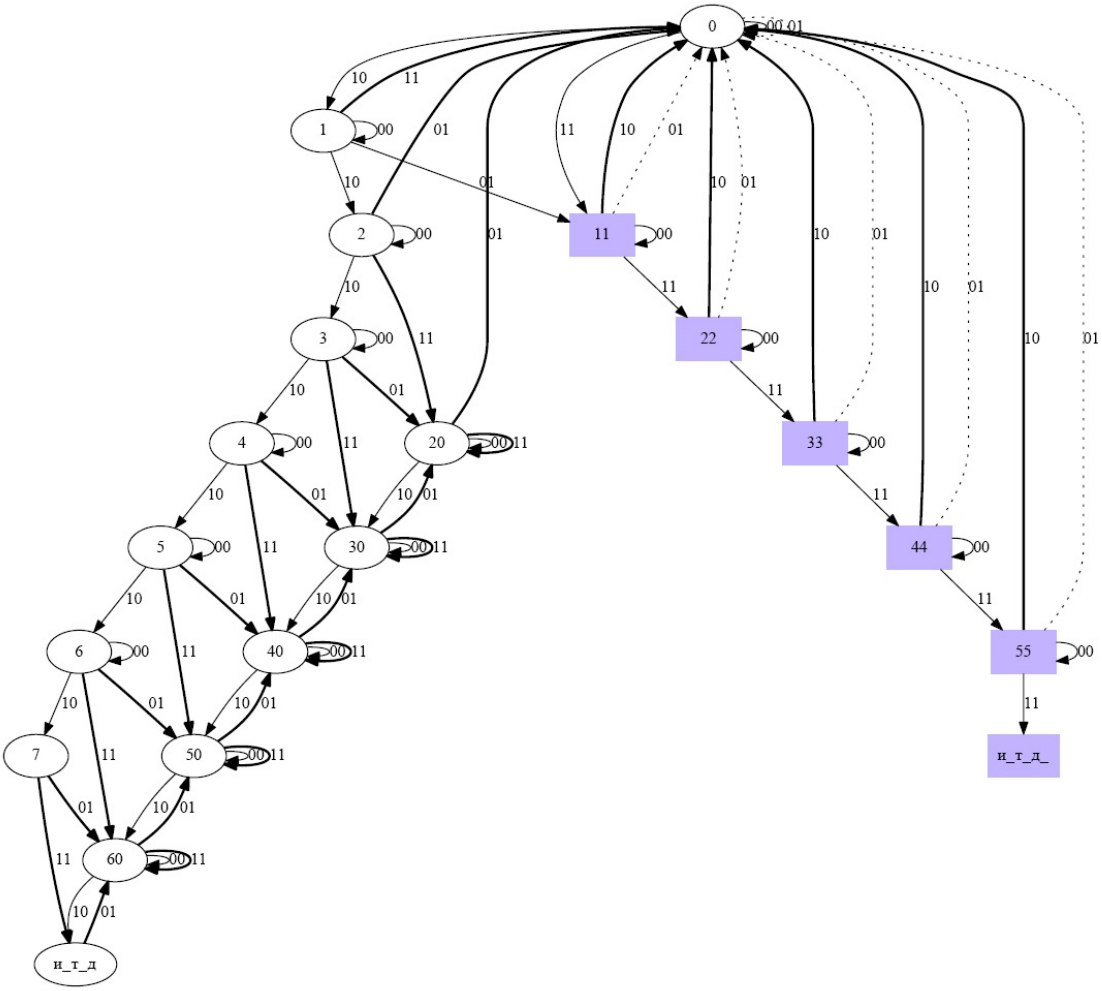

Рис. 2. Граф переходов состояний для уточнённой модели

Таблица 1

Метки переходов в уточнённой модели

Метка	Вероятность перехода	Событие
00	qp	Ни одна группа не нашла продолжения
01	q^2	Вторая группа нашла продолжение второй цепочки
10	p^2	Корыстная группа нашла продолжение своей цепочки
11	pq	Обе группы нашли продолжение для своих цепочек

Основное отличие в графах переходов на рис. 1 и 2, помимо увеличения до четырёх числа исходящих рёбер из каждой вершины, заключается в том, что состояние $0'$ в первом графе, соответствующее разветвлению на две цепочки одинаковой длины, заменено на цепочку состояний $s_{11}, s_{22}, \ldots$, соответствующих разветвлениям с двумя

одинаковыми цепочками длин $1, 2, \ldots$ соответственно. В первой модели такое разветвление может иметь только длину равную 1, а ситуаций с большими длинами цепочек не возникает, поскольку каждый раз выигрывает либо одна, либо другая сторона, но не обе вместе. Кроме того, добавлены состояния s_{i0} при $i \geqslant 2$, соответствующие разветвлению на две цепочки разных длин, в котором корыстная группа имеет преимущество, равное i блокам. На рис. 2 для изображения рёбер используются линии трёх типов: жирной линией нарисованы рёбра, соответствующие событиям, в которых корыстная группа гарантирует для себя вознаграждение; пунктиром — в которых вознаграждение получает группа остальных участников, а тонкие линии указывают, что ни одна из групп ничего не получает.

На самом деле участники обеих групп получают вознаграждение только при переходе в нулевое состояние, когда соответствующие цепочки окончательно включаются в блокчейн. Поэтому здесь, как и в работе [1], производится приписывание соответствующего вознаграждения переходам графа в тех случаях, когда участники гарантировали себе определённую часть вознаграждения, независимо от дальнейшей траектории поведения.

Поведение автомата моделируется цепью Маркова, для которой переходные вероятности задаются следующим образом. Из каждого состояния возможен переход в четыре состояния в зависимости от того, достигают или нет успеха указанные группы участников. Для удобства варианты переходов для всех состояний собраны в одну таблицу (табл. 2).

Таблица 2

Переходы графа для уточнённой модели

Исходное состояние	Метка ребра	Вероятность перехода	Следующее состояние	Выигрыш обеих групп
s_i $(i \geqslant 0)$	00	qp	s_i	$(0,0)$
s_0	01	q^2	s_0	$(0,1)$
s_1	01	q^2	$s_{1,1}$	$(0,0)$
s_2	01	q^2	s_0	$(2,0)$
s_i $(i \geqslant 3)$	01	q^2	$s_{i-1,0}$	$(1,0)$
s_i $(i \geqslant 0)$	10	p^2	s_{i+1}	$(0,0)$
s_0	11	pq	$s_{1,1}$	$(0,0)$
s_1	11	pq	s_0	$(2,0)$
s_i $(i \geqslant 2)$	11	pq	$s_{i,0}$	$(1,0)$
$s_{i,i}$ $(i \geqslant 1)$	00	qp	$s_{i,i}$	$(0,0)$
$s_{i,i}$ $(i \geqslant 1)$	01	q^2	s_0	$(0,i+1)$
$s_{i,i}$ $(i \geqslant 1)$	10	p^2	s_0	$(i+1,0)$
$s_{i,i}$ $(i \geqslant 1)$	11	pq	$s_{i+1,i+1}$	$(0,0)$
$s_{i,0}$ $(i \geqslant 2)$	00	qp	$s_{i,0}$	$(0,0)$
$s_{i,0}$ $(i \geqslant 3)$	01	q^2	$s_{i-1,0}$	$(1,0)$
$s_{i,0}$ $(i = 2)$	01	q^2	s_0	$(2,0)$
$s_{i,0}$ $(i \geqslant 2)$	10	p^2	$s_{i+1,0}$	$(0,0)$
$s_{i,0}$ $(i \geqslant 2)$	11	pq	$s_{i,0}$	$(1,0)$

4.1. Система уравнений для вероятностей состояний

Для оценки вероятностей выигрыша каждой из групп необходимо сначала вычислить вероятности p_i $(i = 0, 1, \ldots)$, $p_{i,0}$ $(j = 2, 3, \ldots)$ и $p_{i,i}$ $(i = 1, 2, \ldots)$ нахождения системы в каждом из состояний. Будем исходить из предположения, что соответствующая цепь Маркова является стационарной, т. е. эти вероятности не зависят от момента времени.

Вероятности нахождения системы в каждом из состояний должны удовлетворять следующим уравнениям:

$$p_0 = (p^2+q^2)\sum_{i\geqslant 1} p_{i,i} + qp_0 + pqp_1 + q^2(p_2+p_{2,0}); \tag{1}$$

$$p_i = pq\,p_i + p^2 p_{i-1}, \quad i \geqslant 1; \tag{2}$$

$$\begin{cases} p_{1,1} = qp\,p_{1,1} + pq\,p_0 + q^2 p_1, \\ p_{i,i} = qp\,p_{i,i} + pq\,p_{i-1,i-1} \quad (i \geqslant 2); \end{cases} \tag{3}$$

$$\begin{cases} p_{2,0} = qp\,p_{2,0} + q^2 p_{3,0} + pq\,p_{2,0} + pq\,p_2 + q^2 p_3, \\ p_{i,0} = qp\,p_{i,0} + p^2 p_{i-1,0} + q^2 p_{i+1,0} + pq\,p_{i,0} + pq\,p_i + q^2 p_{i+1} \quad (i \geqslant 3). \end{cases} \tag{4}$$

Наконец, общая сумма вероятностей всех состояний равна единице:

$$\sum_{i\geqslant 0} p_i + \sum_{i\geqslant 1} p_{i,i} + \sum_{i\geqslant 2} p_{i,0} = 1. \tag{5}$$

В дальнейшем найдём выражения для всех вероятностей через вероятность p_1 и значения p, q, $p < q$.

4.2. Вычисление вероятностей p_i

Лемма 1. Вероятности p_i при $i \geqslant 0$ удовлетворяют соотношениям

$$p_{i+1} = \frac{p^2}{1-pq} p_i. \tag{6}$$

Для любого $k \geqslant 0$ имеем

$$\sum_{i\geqslant k} p_i = p_k \tfrac{1-pq}{q}. \tag{7}$$

Доказательство. Первое соотношение равносильно уравнениям (2). Второе вытекает из первого и цепочки равенств $\sum\limits_{i\geqslant k} p_i = p_k \sum\limits_{i\geqslant 0} \left(\dfrac{p^2}{1-pq}\right)^i = p_k \dfrac{1-pq}{q}$. ■

В частности,

$$\sum_{i\geqslant 0} p_i = p_0 \frac{1-pq}{q} = p_1 \frac{(1-pq)^2}{p^2 q}. \tag{8}$$

Следствие 1. Имеют место следующие соотношения:

$$\begin{gathered} pq\,p_0 + q^2 p_1 = p_1 q/p, \\ pq\,p_i + q^2 p_{i+1} = p_1 \frac{p^{2i-1} q}{(1-pq)^i}, \quad i \geqslant 1. \end{gathered} \tag{9}$$

Оба соотношения вытекают из равенств (6).

4.3. Вычисление вероятностей $p_{i,i}$

Лемма 2. Вероятности $p_{i,i}$ при $i = 1, 2, \ldots$ удовлетворяют следующим соотношениям:

$$p_{1,1} = p_1 \frac{q}{p(1-pq)}, \qquad p_{i+1,i+1} = \frac{pq}{1-pq} p_{i,i}. \tag{10}$$

В частности,

$$\sum_{i\geqslant 1} p_{i,i} = p_1 \frac{q}{p(p^2+q^2)}. \tag{11}$$

Доказательство. Уравнения подсистемы (3) можно переписать в более удобном виде:

$$\begin{cases} (1-pq)p_{1,1} = pq\,p_0 + q^2 p_1, \\ (1-pq)p_{i,i} = pq\,p_{i-1,i-1}, \quad i \geqslant 2. \end{cases} \tag{12}$$

Выражение для $p_{1,1}$ вытекает из первого уравнения этой системы и равенства (9). Второе соотношение вытекает из оставшихся уравнений системы (12). Третье соотношение является следствием первых двух и равенства $1 - 2pq = p^2 + q^2$:

$$\sum_{i\geqslant 1} p_{i,i} = p_{1,1} \sum_{i\geqslant 0} \left(\frac{pq}{1-pq}\right)^i = p_{1,1}\frac{1-pq}{1-2pq} = \frac{p_1 q}{p(p^2+q^2)}.$$

Лемма 2 доказана. ■

Для удобства обозначим через Σ_0 значение, определяемое выражением

$$p_1\Sigma_0 = \sum_{i\geqslant 1} p_{i,i} = p_{1,1} + p_{2,2} + \ldots$$

Далее нам потребуются также значения Σ_1 и Σ_2, определяемые равенствами

$$p_1\Sigma_1 = \sum_{i\geqslant 1}(i+1)p_{i,i} = 2p_{1,1} + 3p_{2,2} + \ldots,$$
$$p_1\Sigma_2 = \sum_{i\geqslant 1} i p_{i,i} = p_{1,1} + 2p_{2,2} + \ldots$$

Лемма 3. Значения Σ_1 и Σ_2 вычисляются по формулам

$$\Sigma_1 = \frac{q(2-3pq)}{p(1-2pq)^2}, \qquad \Sigma_2 = \frac{q(1-pq)}{p(1-2pq)^2}. \tag{13}$$

Доказательство. Вычислим значение Σ_1. С учётом (10) имеем

$$p_1\Sigma_1 = p_{1,1}(2 + 3\frac{pq}{1-pq} + \ldots) = p_{1,1}\sum_{i\geqslant 1}(i+1)\left(\frac{pq}{1-pq}\right)^{i-1} =$$
$$= \frac{p_1}{p^2}\frac{pq}{1-pq}\sum_{i\geqslant 1}(i+1)\left(\frac{pq}{1-pq}\right)^{i-1} = \frac{p_1}{p^2}\sum_{i\geqslant 1}(i+1)\left(\frac{pq}{1-pq}\right)^{i} = \frac{p_1}{p^2}\left(\left(\frac{1-pq}{1-2pq}\right)^2 - 1\right).$$

Здесь использовано известное тождество

$$\sum_{i\geqslant 1} i x^{i-1} = \frac{1}{(1-x)^2}, \tag{14}$$

справедливое при $0 \leqslant x < 1$. Значит,

$$\Sigma_1 = \frac{1}{p^2}\left(\left(\frac{1-pq}{1-2pq}\right)^2 - 1\right) = \frac{1}{p^2}\left(\frac{2pq - 3p^2q^2}{(1-2pq)^2}\right) = \frac{q(2-3pq)}{p(1-2pq)^2}.$$

Аналогично с учётом (14) получаем

$$p_1\Sigma_2 = p_{1,1}(1 + 2\frac{pq}{1-pq} + \ldots) = p_{1,1}\sum_{i\geqslant 1} i\left(\frac{pq}{1-pq}\right)^{i-1} =$$
$$= \frac{p_1}{p^2}\frac{pq}{1-pq}\sum_{i\geqslant 1} i\left(\frac{pq}{1-pq}\right)^{i-1} = \frac{p_1}{p^2}\frac{pq}{1-pq}\left(\frac{1-pq}{1-2pq}\right)^2 = p_1\frac{q(1-pq)}{p(1-2pq)^2}.$$

Лемма 3 доказана. ■

4.4. Вычисление вероятностей $p_{i,0}$

Утверждение 1. Величины $p_{i,0}$, $i \geqslant 2$, вычисляются по следующим формулам:

$$p_{2,0} = p_1 \frac{p^3}{q^2(1-pq)}; \tag{15}$$

$$p_{i+1,0} = p_1 \left(\frac{p^2}{q^2}\right)^i \left(\frac{p+q^2}{1-pq} - \left(\frac{q^2}{1-pq}\right)^i\right), \quad i \geqslant 2. \tag{16}$$

Доказательство. Из равенств (1), (7) и (11) получаем

$$p_2 + p_{2,0} = \frac{1}{q}\sum_{i\geqslant 2} p_i = p_1 \tfrac{p^2}{q^2}.$$

Поэтому

$$p_{2,0} = (p_2 + p_{2,0}) - p_2 = p_1\left(\frac{p^2}{q^2} - \frac{p^2}{1-pq}\right) = p_1 \frac{p^3}{q^2(1-pq)}. \tag{17}$$

Уравнения системы (4) можно переписать в более удобном виде:

$$\begin{cases} (1-2pq)p_{2,0} = q^2 p_{3,0} + pq\, p_2 + q^2 p_3, \\ (1-2pq)p_{i,0} = p^2 p_{i-1,0} + q^2 p_{i+1,0} + pq\, p_i + q^2 p_{i+1}, \quad i > 2, \end{cases}$$

или иначе

$$\begin{cases} (p^2+q^2)p_{2,0} = q^2 p_{3,0} + p_1 \dfrac{p^3 q}{(1-pq)^2}, \\ (p^2+q^2)p_{i,0} = p^2 p_{i-1,0} + q^2 p_{i+1,0} + p_1 \dfrac{p^{2i-1} q}{(1-pq)^i}, \quad i > 2. \end{cases}$$

Отсюда

$$\begin{cases} p_{2,0} - p_{3,0} = -\dfrac{p^2}{q^2} p_{2,0} + p_1 \dfrac{p^3}{q(1-pq)^2}, \\ p_{i,0} - p_{i+1,0} = \dfrac{p^2}{q^2}(p_{i-1,0} - p_{i,0}) + p_1 \dfrac{p^{2i-1}}{q(1-pq)^i}, \quad i > 2. \end{cases}$$

Обозначив через $y(i) = p_{i,0} - p_{i+1,0}$, получаем

$$\begin{cases} y(2) = -\dfrac{p^2}{q^2} p_{2,0} + p_1 \dfrac{p^3}{q(1-pq)^2}, \\ y(i) = \dfrac{p^2}{q^2} y(i-1) + p_1 \dfrac{p^{2i-1}}{q(1-pq)^i}, \quad i > 2. \end{cases}$$

Значит, при $i \geqslant 2$

$$y(i) = \frac{p^2}{q^2}\left(\dots \frac{p^2}{q^2}\left(-\frac{p^2}{q^2}p_{2,0} + p_1\frac{p^3}{q(1-pq)^2}\right) + p_1\frac{p^5}{q(1-pq)^3}\dots\right) + p_1\frac{p^{2i-1}}{q(1-pq)^i} =$$

$$= p_1 \sum_{j=2}^{i}\left(\frac{p^2}{q^2}\right)^{i-j} \frac{p^{2j-1}}{q(1-pq)^j} - \left(\frac{p^2}{q^2}\right)^{i-1} p_{2,0} = p_1 \sum_{j=2}^{i} \frac{p^{2i-1}}{q^{2i-2j+1}(1-pq)^j} - \left(\frac{p^2}{q^2}\right)^{i-1} p_{2,0} =$$

$$= p_1\left(\frac{p^{2i-1}}{q^{2i+1}} \sum_{j\geqslant 2}^{i}\left(\frac{q^2}{1-pq}\right)^j - \left(\frac{p^2}{q^2}\right)^{i-1} p_{2,0}/p_1\right) =$$

$$= p_1 \left(\frac{p^{2i-1}}{q^{2i+1}} \left(\frac{q^2}{1-pq} \right)^2 \sum_{j \geqslant 0}^{i-2} \left(\frac{q^2}{1-pq} \right)^j - \left(\frac{p^2}{q^2} \right)^{i-1} p_{2,0}/p_1 \right) =$$

$$= p_1 \left(\frac{p^{2i-1}}{q^{2i+1}} \left(\frac{q^2}{1-pq} \right)^2 \frac{1-pq}{p} \left(1 - \left(\frac{q^2}{1-pq} \right)^{i-1} \right) - \left(\frac{p^2}{q^2} \right)^{i-1} p_{2,0}/p_1 \right) =$$

$$= p_1 \left(\left(\frac{p^2}{q^2} \right)^{i-1} \frac{q}{1-pq} \left(1 - \left(\frac{q^2}{1-pq} \right)^{i-1} \right) - \left(\frac{p^2}{q^2} \right)^{i-1} p_{2,0}/p_1 \right) =$$

$$= p_1 \left(\left(\frac{q}{1-pq} - p_{2,0}/p_1 \right) \left(\frac{p^2}{q^2} \right)^{i-1} - \frac{q}{1-pq} \left(\frac{q^2}{1-pq} \right)^{i-1} \right) =$$

$$= p_1 \left(\frac{q^3-p^3}{q^2(1-pq)} \left(\frac{p^2}{q^2} \right)^{i-1} - \frac{q}{(1-pq)} \left(\frac{p^2}{1-pq} \right)^{i-1} \right).$$

Таким образом,

$$p_{i+1,0} = p_{i,0} - p_1 \left(\frac{q^3-p^3}{q^2(1-pq)} \left(\frac{p^2}{q^2} \right)^{i-1} - \frac{q}{(1-pq)} \left(\frac{p^2}{1-pq} \right)^{i-1} \right) =$$

$$= p_{2,0} - p_1 \sum_{j=2}^{i} \left(\frac{q^3-p^3}{q^2(1-pq)} \left(\frac{p^2}{q^2} \right)^{j-1} - \frac{q}{(1-pq)} \left(\frac{p^2}{1-pq} \right)^{j-1} \right) =$$

$$= p_1 \frac{p^3}{q^2(1-pq)} - p_1 \left(\frac{q^3-p^3}{q^2(1-pq)} \sum_{j=2}^{i} \left(\frac{p^2}{q^2} \right)^{j-1} - \frac{q}{(1-pq)} \sum_{j=2}^{i} \left(\frac{p^2}{1-pq} \right)^{j-1} \right) =$$

$$= p_1 \frac{p^3}{q^2(1-pq)} - p_1 \left(\frac{q^3-p^3}{q^2(1-pq)} \frac{p^2}{q-p} \left(1 - \left(\frac{p^2}{q^2} \right)^{i-1} \right) - \frac{q}{(1-pq)} \frac{p^2}{q} \left(1 - \left(\frac{p^2}{1-pq} \right)^{i-1} \right) \right) =$$

$$= p_1 \left(\frac{q^3-p^3}{(1-pq)} \frac{1}{q-p} \left(\frac{p^2}{q^2} \right)^i - \left(\frac{p^2}{1-pq} \right)^i \right) = p_1 \left(\frac{p^2}{q^2} \right)^i \left(\frac{p+q^2}{1-pq} - \left(\frac{q^2}{1-pq} \right)^i \right).$$

Утверждение 1 доказано. ■

Следствие 2. Значение Σ_3, определяемое выражением

$$\sum_{i \geqslant 2} p_{i,0} = p_1 \Sigma_3,$$

вычисляется по формуле

$$\Sigma_3 = \frac{p^3}{q(q-p)}. \tag{18}$$

Доказательство. Действительно, из (16) имеем

$$\sum_{i \geqslant 3} p_{i,0} = \sum_{i \geqslant 2} p_{i+1,0} = p_1 \sum_{i \geqslant 2} \left(\frac{p^2}{q^2} \right)^i \left(\frac{p+q^2}{1-pq} - \left(\frac{q^2}{1-pq} \right)^i \right) =$$

$$= p_1 \left(\frac{p+q^2}{1-pq} \sum_{i \geqslant 2} \left(\frac{p^2}{q^2} \right)^i - \sum_{i \geqslant 2} \left(\frac{p^2}{1-pq} \right)^i \right) = p_1 \left(\frac{p+q^2}{1-pq} \left(\frac{p^2}{q^2} \right)^2 \frac{q^2}{q-p} - \left(\frac{p^2}{1-pq} \right)^2 \frac{1-pq}{q} \right) =$$

$$= p_1 \frac{p^4}{q^4(1-pq)} \left(\frac{q^2(p+q^2)}{(q-p)} - q^3 \right) = p_1 \frac{p^5(1+q)}{q^2(1-pq)(q-p)}.$$

Отсюда с учётом (15) получаем

$$\sum_{i\geqslant 2} p_{i,0} = p_{2,0} + \sum_{i\geqslant 3} p_{i,0} = p_1 \frac{p^3}{q^2(1-pq)} \left(1 + \frac{p^2(1+q)}{q-p}\right) = p_1 \frac{p^3}{q(q-p)}.$$

Следствие 2 доказано. ■

4.5. Вычисление вероятности p_1

Из равенства (5) с учётом (7), (11) и (18) получаем выражение для вычисления вероятности p_1:

$$p_1 \left(\frac{(1-pq)^2}{p^2 q} + \frac{q}{p(p^2+q^2)} + \frac{p^3}{q(q-p)}\right) = 1.$$

4.6. Вычисление R

Оценим выигрыш, получаемый выделенной группой участников. Вознаграждение первой группы с учётом (9), (7), (17), (18) и (13) равно

$$r_0 = 2pq\,p_1 + q^2\,p_2 + (pq+q^2)\sum_{i\geqslant 2} p_i + q^2 p_{2,0} + (qp+q^2)\sum_{i\geqslant 2} p_{i,0} + p^2 \sum_{i\geqslant 1}(i+1)p_{i,i} =$$

$$= p_1 \left(2pq + \frac{p^2q^2}{1-pq} + p^2 + \frac{p^3}{1-pq} + q\Sigma_3 + p^2\Sigma_1\right).$$

Для второй группы вознаграждение равно

$$r_1 = q^2 \left(p_0 + \sum_{i\geqslant 1}(i+1)p_{i,i}\right) = p_1 q^2 \left(\frac{1-pq}{p^2} + \Sigma_1\right).$$

Доля первой группы в общей сумме вознаграждения по результатам майнинга оценивается выражением $R = r_0/(r_0+r_1)$; заметим, что оно не зависит от p_1. На рис. 3 приведены результаты вычислений величины выигрыша R при честном и корыстном майнинге в зависимости от вероятности p. Из графика видно, что корыстная группа получает преимущество по сравнению с честным майнингом при $p > 0{,}429$, причём её вознаграждение превышает вознаграждение остальной группы при $p > 0{,}454$.

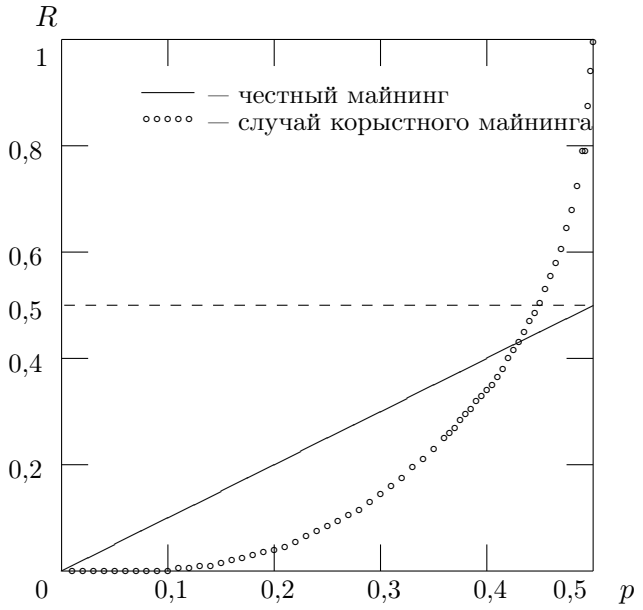

Рис. 3. График зависимости величины выигрыша R при честном и корыстном майнинге от величины вероятности p

5. Использование предположения о подключении части участников из второй группы

Теперь по аналогии с [1] рассмотрим ситуацию, когда в случае разветвления блокчейна на две цепочки часть майнеров, не входящих в выделенную группу, подключится к поиску продолжения цепочки, найденной выделенной группой участников. Пусть доля таких участников в общей вычислительной мощности второй группы участников оценивается величиной γ, $0 \leqslant \gamma \leqslant 1$.

Для анализа этой ситуации будем, как и раньше, рассматривать вероятностную модель, включающую две группы участников, осуществляющих майнинг с вероятностями успеха p и q. В тех случаях, когда для группы остальных участников имеется выбор того, для какой из цепочек строить продолжение, будем предполагать, что вероятность успешного подбора продолжения для цепочки, содержащей блоки, найденные группой корыстных участников, равна γq, а для второй цепочки в разветвлении блокчейна она равна $(1-\gamma)q$.

Заметим, что модель с независимым поведением каждой из подгрупп оказывается слишком сложной для исследования, так как при этом появляется возможность таких переходов в новое состояние, когда все три участника добиваются успеха. Это приводит к необходимости рассмотрения тройных, четверных и т. д. разветвлений блокчейна, что приводит к дополнительному увеличению числа участников и значительно усложняет вид графа переходов и всей марковской модели.

С другой стороны, в данном случае обе подгруппы используют честную стратегию, решая свои задачи в открытую. Для простоты предположим, что они так же, как и корыстная группа, находятся в одном пуле, управляющем распределением работ и сбором результатов. Поэтому естественно считать, что все члены группы прекращают перебор в момент успешного подбора блока одной из подгрупп. Следовательно, здесь возможно использование одной случайной величины с тремя исходами: ни одна из подгрупп не нашла варианта (этот вариант остаётся, так как $q < 1$), успешна первая или вторая подгруппа.

Таким образом, для тех состояний, которые соответствуют разветвлению блокчейна, должно быть не четыре, а шесть вариантов перехода в другие состояния: (два варианта для корыстной группы)$\times$(три варианта для группы остальных участников). Такому порядку проведения майнинга соответствует модель с двумя группами: одна — это корыстная группа, работающая в соответствии с алгоритмом корыстного майнинга, вторая — группа остальных майнеров, выдающая результатом подбора продолжение либо первой, либо второй цепочки. Её работа моделируется случайной величиной, принимающей три значения 0, 1, 2 с вероятностями p, $q\gamma$, $q(1-\gamma)$ соответственно.

Соберём в одну таблицу варианты перехода для всех состояний (табл. 3). Первая часть таблицы такая же, как и в табл. 2, так как она соответствует состояниям, в которых корыстная группа скрывает свою часть цепочки, и поэтому вторая группа целиком работает на продолжение опубликованной части цепочки. Отличие имеется только для состояний, в которых имеется разветвление. Из табл. 3 видно, что при $0 < \gamma < 1$ вероятность выигрыша корыстной группы должна увеличиться, так как в графе появляются дополнительные переходы, приносящие успех первой группе. Модифицированный граф переходов, моделирующий этот случай, приведён на рис. 4.

Таблица 3

Переходы модифицированного графа

Исходное состояние	Метка ребра	Верояность перехода	Следующее состояние	Выигрыш обеих групп
s_i $(i \geqslant 0)$	00	qp	s_i	$(0,0)$
s_0	01	q^2	s_0	$(0,1)$
s_1	01	q^2	$s_{1,1}$	$(0,0)$
s_2	01	q^2	s_0	$(2,0)$
s_i $(i \geqslant 3)$	01	q^2	$s_{i-1,0}$	$(1,0)$
s_i $(i \geqslant 0)$	10	p^2	s_{i+1}	$(0,0)$
s_0	11	pq	$s_{1,1}$	$(0,0)$
s_1	11	pq	s_0	$(2,0)$
s_i $(i \geqslant 2)$	11	pq	$s_{i,0}$	$(1,0)$
$s_{i,i}$	00	qp	$s_{i,i}$	$(0,0)$
$s_{i,i}$	01	$q^2\gamma$	s_0	$(i,1)$
$s_{i,i}$	02	$q^2(1-\gamma)$	s_0	$(0,i+1)$
$s_{i,i}$	10	p^2	s_0	$(i+1,0)$
$s_{i,i}$	11	$pq\gamma$	$s_{1,1}$	$(i,0)$
$s_{i,i}$	12	$pq(1-\gamma)$	$s_{i+1,i+1}$	$(0,0)$
$s_{i,0}$	00	qp	$s_{i,0}$	$(0,0)$
$s_{2,0}$	01	$q^2\gamma$	s_0	$(2,0)$
$s_{i,0}$ $(i>2)$	01	$q^2\gamma$	$s_{i-1,0}$	$(1,0)$
$s_{2,0}$	02	$q^2(1-\gamma)$	s_0	$(2,0)$
$s_{i,0}$ $(i>2)$	02	$q^2(1-\gamma)$	$s_{i-1,0}$	$(1,0)$
$s_{i,0}$	10	p^2	$s_{i+1,0}$	$(0,0)$
$s_{i,0}$	11	$pq\gamma$	$s_{i,0}$	$(1,0)$
$s_{i,0}$	12	$pq(1-\gamma)$	$s_{i,0}$	$(1,0)$

Система уравнений для вероятностей состояний теперь имеет следующий вид:

$$p_0 = (p^2+q^2)\sum_{i\geqslant 1} p_{i,i} + qp_0 + pqp_1 + q^2\left(p_2 + p_{2,0}\right); \tag{19}$$

$$p_i = pq\,p_i + p^2 p_{i-1}, \quad i \geqslant 1; \tag{20}$$

$$\begin{cases} p_{1,1} = qp\,p_{1,1} + pq\,p_0 + q^2 p_1 + pq\gamma \sum\limits_{j\geqslant 1} p_{j,j}, \\ p_{i,i} = pq\,p_{i,i} + pq(1-\gamma)\,p_{i-1,i-1}, \quad i \geqslant 2; \end{cases} \tag{21}$$

$$\begin{cases} p_{2,0} = qp\,p_{2,0} + q^2 p_{3,0} + pq\,p_{2,0} + pq\,p_2 + q^2 p_3, \\ p_{i,0} = qp\,p_{i,0} + p^2 p_{i-1,0} + q^2 p_{i+1,0} + pq\,p_{i,0} + pq\,p_i + q^2 p_{i+1}, \quad i \geqslant 3. \end{cases} \tag{22}$$

В дальнейшем поступим аналогично предыдущему случаю и найдём выражения для всех вероятностей через вероятность p_1 и значения параметров p, q и γ.

Заметим, что уравнения (19), (20) и (22) совпадают с (1), (2) и (4) соответственно. Поэтому для вероятностей p_i, $i \geqslant 0$, справедливы формулы (6), (7) и (8). Отличие имеется только в первом уравнении для вероятности p_{11} в подсистемах (3) и (21).

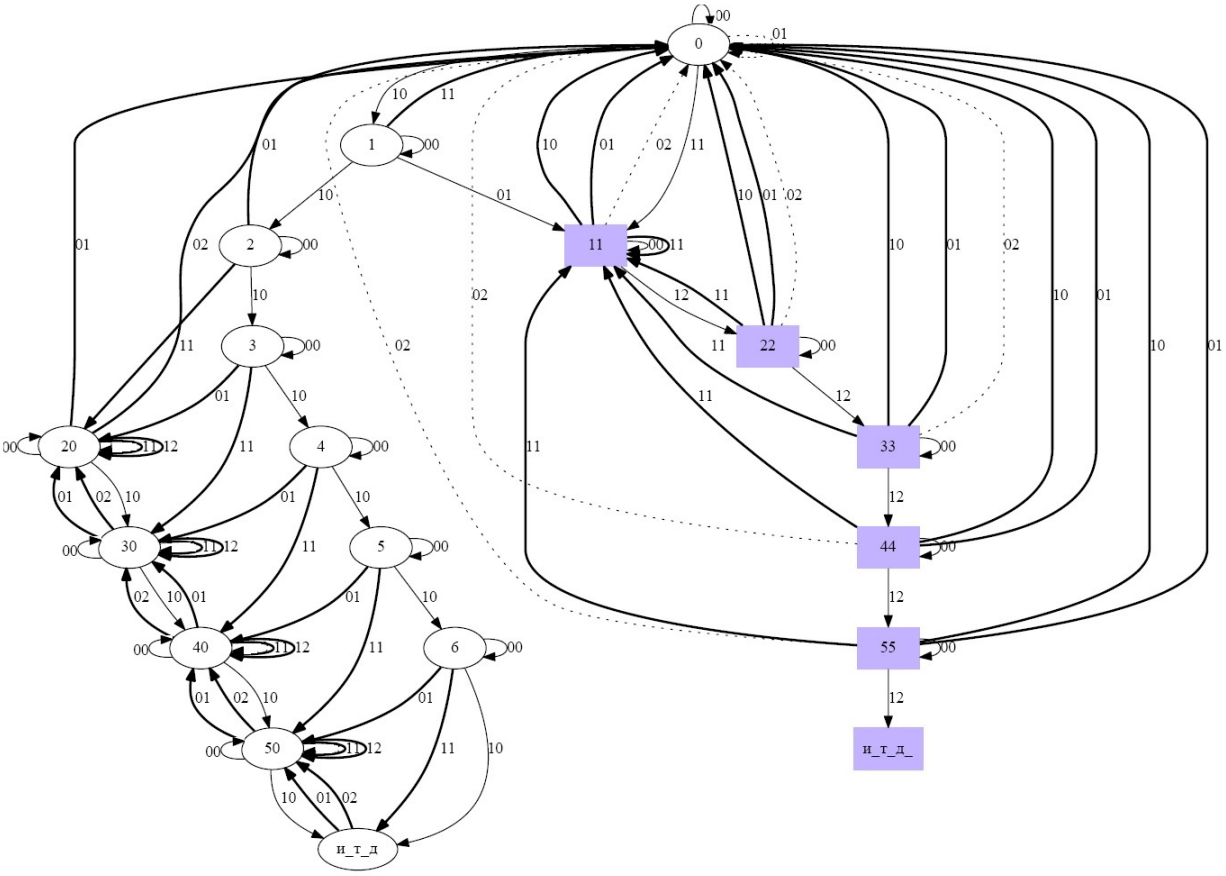

Рис. 4. Автоматная модель при $0 \leqslant \gamma \leqslant 1$

5.1. Вычисление вероятностей $p_{i,i}$

Лемма 4. Справедливы следующие равенства:

$$p_{i+1,i+1} = \frac{pq(1-\gamma)}{1-pq} p_{i,i}, \qquad i = 1, 2, \ldots; \tag{23}$$

$$p_{1,1} = p_1 \frac{q(1-pq(2-\gamma))}{p(1-pq)(1-2pq)}; \tag{24}$$

$$\sum_{i \geqslant 1} p_{i,i} = p_{1,1} \frac{1-pq}{1-pq(2-\gamma)} = p_1 \frac{q}{p(1-2pq)}. \tag{25}$$

Доказательство. Преобразуем выражения (21):

$$\begin{cases} (1-pq)p_{1,1} = pq\, p_0 + q^2 p_1 + pq\gamma \sum\limits_{j \geqslant 1} p_{j,j}, \\ (1-pq)p_{i,i} = pq(1-\gamma)\, p_{i-1,i-1}, \quad i \geqslant 2. \end{cases} \tag{26}$$

Равенства (23) получаются из второго уравнения системы (26), поэтому

$$\sum_{i \geqslant 1} p_{i,i} = p_{1,1} \sum_{i \geqslant 0} \left(\frac{pq(1-\gamma)}{1-pq} \right)^i = p_{1,1} \frac{1-pq}{1-pq(2-\gamma)}. \tag{27}$$

Для нахождения выражения для вероятности $p_{1,1}$ необходимо вычислить правую сумму в правой части первого уравнения системы (26). Используя равенство (9), имеем

$$p_{1,1} = p_1 \frac{q}{p(1-pq)} + \frac{pq\gamma \sum\limits_{j\geqslant 1} p_{j,j}}{1-pq}. \tag{28}$$

Из (27) и (28) получаем равенство

$$p_{1,1}\left(1 - \frac{pq\gamma}{1-pq(2-\gamma)}\right) = p_1 \frac{q}{p(1-pq)},$$

что равносильно (24). Подставляя выражение (24) в (27), получаем требуемое выражение (25) для суммы. ■

Рассмотрим теперь, как изменятся значения сумм Σ_0, Σ_1 и Σ_2. Выражение (25) совпадает с (11), поэтому значение Σ_0 остается неизменным.

Лемма 5. Значения Σ_1 и Σ_2 вычисляются по формулам

$$\Sigma_1 = \frac{q(2-pq(3-\gamma))}{p(1-2pq)(1-pq(2-\gamma))}, \qquad \Sigma_2 = \frac{q(1-pq)}{p(1-2pq)(1-pq(2-\gamma))}. \tag{29}$$

Доказательство. В силу тождества (14) с учётом (24) справедливы формулы

$$p_1\Sigma_2 = \sum_{i\geqslant 1} i p_{i,i} = p_{1,1} \sum_{i\geqslant 1} i \left(\frac{pq(1-\gamma)}{1-pq}\right)^{i-1} = p_{1,1} \frac{1}{\left(1 - \dfrac{pq(1-\gamma)}{1-pq}\right)^2} =$$

$$= p_{1,1}\left(\frac{1-pq}{(1-pq(2-\gamma)}\right)^2 = p_1 \frac{q(1-pq)}{p(1-2pq)(1-pq(2-\gamma))}.$$

Отсюда

$$p_1\Sigma_1 = p_1(\Sigma_2 + \Sigma_0) = p_{1,1}\frac{(1-pq)(2-pq(3-\gamma))}{(1-pq(2-\gamma))^2} = p_1 \frac{q(2-pq(3-\gamma))}{p(1-2pq)(1-pq(2-\gamma))}.$$

Лемма доказана. ■

5.2. Вычисление вероятностей $p_{i,0}$

Поскольку выражение (25) не зависит от γ, значение вероятности $p_{2,0}$, вычисляемое с помощью уравнения (19), остаётся неизменным и определяется выражением (15). Поэтому значения вероятностей $p_{i,0}$, $i \geqslant 3$, также не меняются и определяются выражениями (16).

5.3. Вычисление вознаграждения для обеих групп

Перейдём к оценке величины $R = r_0/(r_0 + r_1)$ доли вознаграждения корыстной группы в общей сумме вознаграждения, полученной при применении описанной стратегии майнинга. Вознаграждение первой группы в этом случае определяется как

$$r_0 = 2pq\,p_1 + q^2\,p_2 + (pq+q^2)\sum_{i\geqslant 2} p_i + q^2 p_{2,0} + (qp+q^2)\sum_{i\geqslant 2} p_{i,0} + p^2 \sum_{i\geqslant 1}(i+1)p_{ii} +$$

$$+ (q^2+pq)\gamma \sum_{i\geqslant 1} i p_{ii} = p_1\left(2pq + \frac{p^2q^2}{1-pq} + p^2 + \frac{p^3}{1-pq} + q\Sigma_3 + p^2\Sigma_1 + q\gamma\Sigma_2\right).$$

Для второй группы вознаграждение равно

$$r_1 = p_1 q^2 \left(\frac{1 - pq}{p^2} + (1 - \gamma)\Sigma_1 + \gamma\Sigma_0 \right).$$

Значения сумм Σ_0, Σ_1 и Σ_2 вычисляются с помощью тождеств (11) и (29).

Приведённые формулы позволяют вычислить значение доли R при произвольных значениях параметров $0 \leqslant p < 1/2$ и $0 \leqslant \gamma \leqslant 1$. Результаты вычислений приведены на рис. 5–7. На рис. 5 показан график зависимости от параметра γ минимального значения вероятности p, при котором впервые выполняется условие $R > 1/2$. Вычисления показывают, что выигрыш корыстной группы при соответствующем значении γ превышает выигрыш остальной группы при значениях вероятности p в пределах

$$0{,}358 \leqslant p \leqslant 0{,}449.$$

Наибольшее значение достигается при $\gamma = 0$, а наименьшее — при $\gamma = 1$. На рис. 6 показан аналогичный график зависимости от параметра γ минимального значения вероятности p, при котором впервые выполняется условие $R > p$. В данном случае получаем, что выигрыш корыстной группы превышает при соответствующем значении γ выигрыш, полученный ими при честном выполнении блокчейн протокола, для значений вероятности p в пределах

$$0 < p \leqslant 0{,}429.$$

В работе [1] этот интервал имеет вид $0 < p \leqslant 0{,}333$.

На рис. 7 приведён график величины доли вознаграждения R при честном и корыстном майнинге в зависимости от величины вероятности p для трёх значений параметра γ (0, 0,5 и 1).

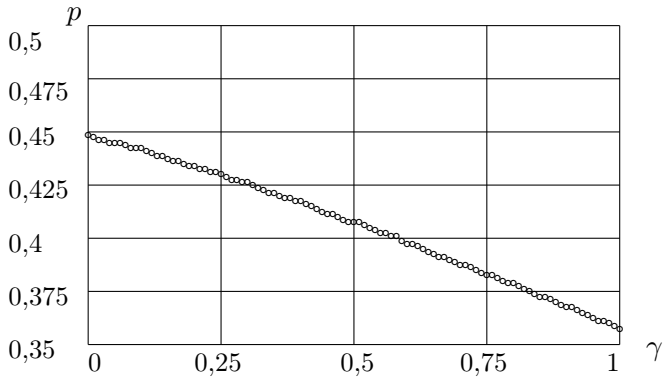

Рис. 5. График зависимости значения вероятности p, при котором впервые выполняется условие $R > 1/2$, от параметра γ

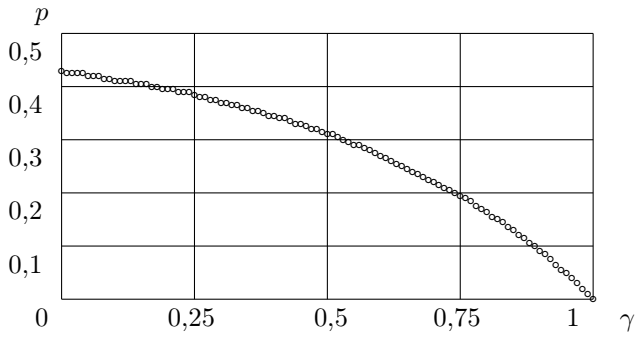

Рис. 6. График зависимости значения вероятности p, при котором впервые выполняется условие $R > p$, от параметра γ

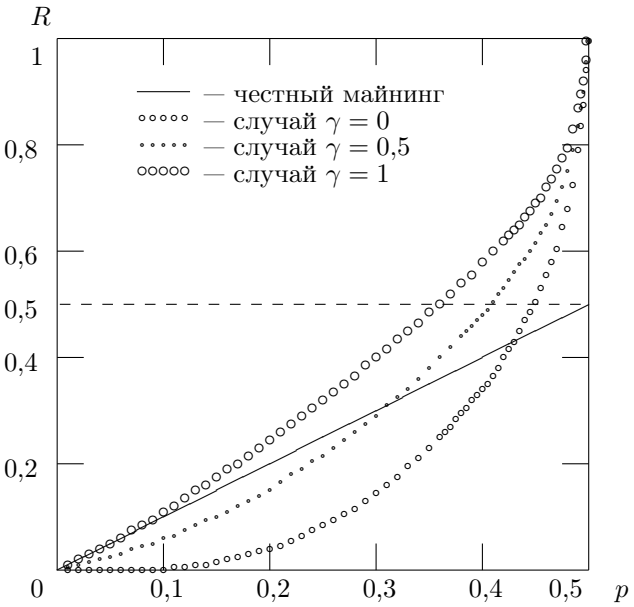

Рис. 7. Графики зависимости величины выигрыша R при корыстном майнинге в зависимости от величины вероятности p и параметра γ

Автор выражает благодарность рецензенту за внимательное прочтение рукописи и многочисленные полезные замечания.

ЛИТЕРАТУРА

1. *Ittay E. and Emin G. S.* Majority is Not Enough: Bitcoin Mining is Vulnerable. arXiv:1311.0243. 2013. http://arxiv.org/abs/1311.0243.
2. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable // Financial Cryptography and Data Security: 18th Intern. Conf. Christ Church, Barbados, March 3–7, 2014. P. 436–454.
3. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable // Commun. ACM. 2018. V. 61. No. 7. P. 95–102. https://doi.org/10.1145/3212998.

REFERENCES

1. *Ittay E. and Emin G. S.* Majority is Not Enough: Bitcoin Mining is Vulnerable. arXiv:1311.0243. 2013. `http://arxiv.org/abs/1311.0243`.
2. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable. Financial Cryptography and Data Security: 18th Intern. Conf. Christ Church, Barbados, March 3–7, 2014, pp. 436–454.
3. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable. Commun. ACM, 2018, vol. 61, no. 7, pp. 95–102. `https://doi.org/10.1145/3212998`.