УДК 004.056.5 **DOI:10.30837/rt.2020.4.203.03**

Н.А. ПОЛУЯНЕНКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
В.Э. САФОНЕНКО, А.А. КУЗНЕЦОВ, д-р техн. наук

УТОЧНЕНИЕ ОЦЕНОК ВЕРОЯТНОСТИ УСПЕХА АТАКИ ДВОЙНОЙ ТРАТЫ НА БЛОКЧЕЙН СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ НЕЗАВИСИМЫХ ИГРОКОВ

Введение

Технология блокчейн исследуется во многих инновационных приложениях [1], таких как: криптовалюты [2 – 4]; умные контракты [5, 6]; системы связи [7 – 9]; здравоохранение [10 – 14]; Интернет вещей [15 – 19]; финансовые системы [20 – 23]; разработка программного обеспечения [24 – 26]; электронное голосование [27 – 31]; в [32 – 34] авторы предложили безопасную и легковесную архитектуру на основе блокчейна для умного дома; и многие другие. Институты исследования глобального рынка Gartner и Deloitte выбрали блокчейн в качестве одного из технологических трендов 2017 г. [35]. Построенная на основе блокчейн технологии криптовалюта Bitcoin была оценена как самая эффективная валюта в 2015 г. [36] и самый эффективный товар в 2016 г. [37], а также имела более 400 000 подтвержденных транзакций [38] ежедневно в декабре 2018 и мае 2019 г., что указывает на значительную вовлеченность в данную сферу.

Используя прозрачную и полностью распределенную одноранговую архитектуру блокчейн, приложения выигрывают от модели, в которой возможно только добавление данных, в которой «транзакции» принимаются в блокчейн реестр и при правильном функционировании системы не могут быть модифицированы или удалены. Прозрачность блокчейн систем позволяет хранить общедоступные и неопровержимые записи [39]. Одноранговая блокчейн система обеспечивает проверяемое ведение реестра без централизованного управления, что позволяет решать проблемы единой точки отказа и единой точки доверия [40].

Технология блокчейн позволяет изменить способ реализации всех типов транзакций и предоставляет широкий спектр возможностей в других областях, таких как децентрализованный протокол конфиденциального вычисления (Secure multi-party computation) [41], использование в децентрализованных автономных корпорациях (decentralized autonomous corporation) [42].

Со времени появления технологии блокчейн в 2009 г. (в качестве основного механизма работы сети Bitcoin) она показала многообещающие перспективы применения и привлекла большое внимание ученых и промышленности. Внедрение полнофункциональных языков программирования Turing, позволяют пользователям разрабатывать интеллектуальные контракты, работающие на блокчейне. Благодаря децентрализованному механизму блокчейна интеллектуальные контракты позволяют взаимно не доверяющим пользователям осуществлять обмен данными или транзакциями без необходимости получения каких-либо сторонних доверенных прав.

Однако, несмотря на все перечисленные достоинства, достижение единого состояния во всех распределенных узлах децентрализованной системы является сложной задачей. Согласованные алгоритмы должны быть устойчивы к сбоям узлов, разбиению сети, задержкам сообщений и сообщениям, которые приходят не в порядке очереди и повреждены. Им также приходится иметь дело с корыстными и намеренно вредоносными узлами, которые заинтересованы в некорректной работе сети. Для решения этой проблемы было предложено несколько алгоритмов, называемых консенсусами, каждый из которых реализует набор необходимых предположений, касающихся синхронизации, передачи сообщений, сбоев, вредоносных узлов, производительности и безопасности при обмене сообщениями. Для блокчейн сети достижение консенсуса гарантирует, что все узлы в сети согласовывают единообразное глобальное состояние блокчейн реестра.

Несмотря на функциональные особенности, которые блокчейн привносит в пространство разработки приложений, в последних отчетах подчеркиваются риски безопасности, связанные с этой технологией [15, 43 – 46]. Например, в июне 2016 г. неизвестному злоумышленнику удалось воспользоваться рекурсивной уязвимостью вызовов смарт-контрактов и вывести более 50 миллионов долларов США из «The DAO», децентрализованной автономной организации, которая работает на основе интеллектуальных контрактов, основанных на блокчейне, или заранее запрограммированных правил, управляющих организацией [47, 48]. В августе 2016 г. с биржи Bitfinex в Гонконге были похищены биткойны на сумму 72 миллиона долларов США [49]. В июне 2017 г. Bitfinex также испытал атаку распределенного отказа в обслуживании (DDoS), которая привела к её временной остановке.

Несколько бирж Bitcoin и Ethereum также часто страдают от DDoS-атак и DNS-атак, что затрудняет доступность сервиса для пользователей. Так, блокчейн Bitcoin является мишенью для пылевых или спам-операций, чтобы задержать обработку законных сделок. В мае, августе и ноябре 2017 г. пулы памяти Биткойна были заполнены пылевыми транзакциями, что привело к задержкам в проверке транзакций и увеличению платы за майнинг биткойнов [50]. Например, в результате приостановки транзакции в ноябре 2017 г. была задержана оплата биткойнов на сумму 700 миллионов долларов США [51]. Часто целью таких атак является мотивация пользователей Bitcoin переходить на другие криптовалюты с более быстрым временем обработки транзакций.

Из-за публично проверяемого характера криптовалюты, на основе блокчейна, они уязвимы для некоторых мошеннических действий. Так, MtGox, занимавшийся обменом валюты Bitcoin в Японии, в марте 2014 г. подвергся нападению двух злоумышленников, похитивших биткойны на сумму 460 миллионов долларов США [52, 53]. Злоумышленники собрали полезную информацию из блокчейна Bitcoin и создали фальшивую систему транзакций, чтобы повысить рыночную цену. Из-за такой деятельности, MtGox понес тяжелую потерю, что привело к его банкротству.

Одной из основных атак на блокчейн системы, в протоколах которых используются алгоритмы консенсуса на основе доказательств выполненной работы, является атаки связанные с возможностью проведения двойных расходов. Более того, данный тип атак является конструктивной особенностью таких систем, и от которых не существует абсолютной защиты.

Двойные расходы – это результат успешного расходования одних и тех же средств более одного раза. Предотвращение данной возможности является одной из наиболее важных задач любой цифровой учетной системы. Так, перефразируя фразу из вики биткойна [54], можно утверждать: в блокчейн системе Bitcoin всё (майнинг, доказательство работы, сложность и т.д.) существует для создания истории транзакций, которую невозможно изменить в вычислительном отношении, что делает существующие транзакции необратимыми. Сама возможность удвоения расходов резко ухудшает доверие к системе и ценность решений на её основе.

Двойные траты – это проблема, которая существует с момента появления блокчейн систем, и остается актуальной по сегодняшний день. Для понимания важности и масштабов убытков приведем некоторые инциденты, связанные с удачно реализованными атаками двойного расходования средств.

1. Примеры проведенных атак двойной траты

Печальным побочным эффектом для блокчейн-технологий стал рост числа злоумышленников, использующих публичные блокчейн системы в незаконных целях. Ниже приведены некоторые примеры успешного проведения атак двойных трат.

Один из форков Биткойна, Bitcoin Gold (BTG), дважды подвергся такой атаке в сети:

- с 16 по 18 мая 2018 г. (было похищено 388 000 BTG, убытки составили более 18,6 миллионов долларов США) [55 – 58];

- в 2020 г. (в ходе атаки 23 января проведена реорганизация 14 блоков и 24 января – 15 блоков, убыток составил 7 167 BTG (более 70 000 $ США) ориентировочная стоимость каждой атаки по реорганизации блокчейна составила около 1 700 долларов США) [59, 60].

Неоднократно на протяжении последних нескольких лет были проведены успешные атаки на Ethereum Classic (ETC):

- с 05.01.2019 по 07.01.2019 г., по информации биржи Coinbase [61], было осуществлено 15 реорганизаций цепочки блокчейна Ethereum Classic, 12 из которых содержали двойные траты на общую сумму 219 500 ETC (1,1 миллионов долларов США);

- по информации компании Bitfly, которая является оператором майнинг-пула Ethermine [62] 01.08.2020 г., начиная с блока 10 904 146, блокчейн Ethereum Classic подвергся реорганизации глубиной в 3 693 блоков, что соответствует примерно 12 часам майнинга [63]. Как говорится в сообщении, реорганизация проведена, вероятно, с помощью атаки 51 %. Для проведения атаки злоумышленник арендовал посторонние мощности на сумму 17,5 BTC (192 тысячи долларов США), при этом он вывел на несколько кошельков 807 260 ETC (5,6 миллионов долларов США) [64];

- с 05.08.2020 по 06.08.2020 г. на блоке 10 935 622 блокчейн Ethereum Classic подвергся реорганизации глубиной в 4 236 блоков [65, 66]. Злоумышленник успешно дважды потратил 238 306 ETC (1,68 миллиона долларов США), кроме того, злоумышленник также получил 14 234,30 ETC в качестве награды за найденные блоки [67];

- 30.10.2020 г. также по информации компании Bitfly [68] еще одна атака 51 % состоялась на сеть Ethereum Classic, что повлекло реорганизацию более 7 000 блоков, что соответствует примерно двум дням майнинга. Команда Ethereum Classic порекомендовала [69] майнерам, биржам и другим сервисам на некоторое время установить количество подтверждений транзакций не менее 7 000.

Ориентированная на конфиденциальность криптовалюта Verge (XVG) 22 мая 2018 г. позволила злоумышленнику скрыться с примерно 1,75 миллиона долларов США. Протокол Verge использует ротацию пяти алгоритмов майнинга. Предположительно злоумышленник получил контроль над двумя из них – scrypt и lyra2re (используя ложные временные метки), что позволило практически без труда сформировать блоки и тем самым заставить сеть принять их в основную цепь [70].

Несмотря на то, что на самую большую и популярную блокчейн сеть Bitcoin на сегодняшний день неизвестны удачные реализации атаки двойной траты, но повышение стоимости данной криптовалюты повысило популярность её майнинга, который определяется как использование вычислительной мощности (то есть мощности хеширования) для генерации новых блоков [71]. Увеличенное количество майнеров уменьшило вероятность того, что отдельный майнер сможет добыть новый блок и, следовательно, получить награду. Следовательно, мелкомасштабная добыча стала очень рискованной. Поэтому, как естественная защита от специфического риска, большинство майнеров присоединились к майнинговым пулам. Пулы приобрели такую популярность, что с 2015 г. от 95 до почти 100 процентов мощности хэша (обработки) в сети Bitcoin контролируется пулами. Ситуация аналогична во всех основных криптовалютах [71].

В подтверждение угроз потери децентрализации в наиболее крупных блокчейн системах приведем данные из [72]. В Bitcoin еженедельная мощность майнинга одним объектом никогда не превышала 21 % от общей мощности. В отличие от этого, главный майнер Ethereum никогда не имел менее 21 % мощности майнинга. Более того, четверка лучших майнеров Bitcoin имеет более 53 % средней мощности майнинга. В среднем 61 % еженедельной мощности было разделено только тремя майнерами Ethereum. Хотя майнеры меняют ранги в течение периода наблюдения, каждое место оспаривается лишь несколькими майнерами. В частности, только два майнера Bitcoin и три майнера Ethereum когда-либо занимали высшие позиции. Один и тот же майнинг пул находился на верхнем уровне в течение 29 % времени в Bitcoin и 14 % времени в Ethereum. Более 50 % майнинговых мощностей было распределено

исключительно между восьмью майнерами в Bitcoin и пятью майнерами в Ethereum в течение всего наблюдаемого периода. Даже 90 % майнинговых мощностей, похоже, контролируются только 16 майнерами в Bitcoin и только 11 майнерами в Эфириуме. Следовательно, для поддержки блокчейна обе платформы в значительной степени зависят от очень небольшого числа отдельных объектов майнинга.

Наиболее эффективной защитой от двойных расходов является проверка участниками учетных блокчейн систем включения платежа в блокчейн реестр и дополнительное ожидание нескольких подтверждений. Подтверждения происходят всякий раз, когда формируется новый блок, ссылающийся на цепочку блоков содержащую транзакцию с платежом. Для системы Bitcoin это происходит в среднем каждые 10 минут. До включения транзакции в блок (иногда называемым «нулевым подтверждением») нет никакой гарантии, что транзакция не будет израсходована дважды. Более того, могут быть веские легальные причины для изменения транзакции, главным образом для добавления дополнительных комиссий к «зависшей» транзакции, которая в противном случае могла бы оставаться не добавленной в реестр блокчейна в течение нескольких дней.

Пользователи учетных блокчейн систем могут значительно снизить вероятность проведения успешных атак двойной траты, максимально увеличивая необходимое число подтверждений и, следовательно, время проведения сделки. И хотя это решение просто по своей концепции, его часто чрезвычайно сложно реализовать на практике.

Интересная информация предоставлена в [73], где описываются случаи и механизмы контратак блокчейн сетей на попытку злоумышленников реорганизовать их блокчейн реестр. Так, в статье приходят к выводам, что растущая глубина рынков по аренде хешрейта может ставить под угрозу безопасность криптовалют на основе алгоритма доказательства выполненной работы. В то же время возможность контратак может остановить атакующих от каких-либо действий. Если этого баланса сил достаточно, чтобы защитить цепь, это ведет к вопросу о том, какое именно количество мощностей необходимо для предотвращения атак.

Но, несмотря на то, какую стратегию мы выбираем (увеличения времени подтверждения или возможность проведения контрмер), необходимо иметь четкое представление о мощностях, которые необходимо задействовать (как при потенциальной атаке, так и при проведении защиты) для оптимизации затрачиваемых ресурсов и сокращении потенциальных рисков.

Анализ работ, посвященных количественной оценке вероятности успешного проведения атаки двойной траты на блокчейн системы, подробно описан в [76, 83]. Наиболее известными и цитируемыми являются работы Сатоши Накамото [74] и более точные результаты получены Мени Розенфельдом [75].

В статье приведен сравнительный анализ упомянутых работ с предлагаемой моделью, которая, на наш взгляд, более адекватно описывает реальные процессы консенсуса на основе доказательства выполненной работы, происходящей в блокчейн системах.

2. Корректировка формул С. Накамото та М. Розенфельда на основе модели независимых игроков

2.1. Используемые модели

Упомянутые работы формируют свои выводы на основании модели «разорение игрока». На основе данной модели получается формула для расчета вероятности успешного проведения атаки. В основу этой модели положен факт, что в каждом испытании или выигрывает злоумышленник (формируя очередной блок) или злоумышленник проигрывает и при этом считается, что выигрывает честная сеть (формируя очередной блок). Авторы предполагают, что если блок не сформировал злоумышленник, то в таком случае блок обязательно формирует честная сеть, причем это предположение никак не обосновано.

Мы предлагаем использовать модель «независимых игроков». В данной модели, в отличие от модели «разорение игрока», формирование очередного блока у злоумышленника и

честной сети происходит полностью независимо друг от друга. Пусть вероятность сформировать блок злоумышленником будет q, а честной сетью – p, отказавшись от обязательного для модели «разорение игрока» выполнения условия $p = 1 - q$, мы получаем в результате каждой попытки (или серии попыток в течение заданного интервала времени) пространство элементарных событий, содержащих следующие события:

– элементарное событие «блок сформирован честной сетью и атакующий не сформировал блок» с вероятностью $p \cdot (1 - q)$;

– элементарное событие «блок не сформирован честной сетью и атакующий сформировал блок» с вероятностью $(1 - p) \cdot q$;

– элементарное событие «блок не сформирован честной сетью и атакующий не сформировал блок» с вероятностью $(1 - p) \cdot (1 - q)$;

– элементарное событие «блок сформирован честной сетью и атакующий сформировал блок» $p \cdot q$.

Множество всех элементарных событий составляет полную группу событий:

$$p \cdot (1 - q) + (1 - p) \cdot q + (1 - p) \cdot (1 - q) + p \cdot q = 1.$$

Рассмотрим трансформацию формул Сатоши Накамото [74] и Мени Розенфельда [75] при переходе от модели разорения игрока к модели независимых игроков.

Вероятность удачного проведения атаки двойной траты (обозначим ее как PI), согласно примерам, приведенным в упомянутых работах, можно представить следующим образом:

$$PI = PI_1 \cdot Q_v + PI_2 \cdot Q_2, \tag{1}$$

где PI_1 – вероятность злоумышленника сформировать z блоки позже честной сети. Символом z обозначим количество подтверждений (сформированных блоков), которые ожидает продавец перед тем, как признать транзакцию с переводом средств действительной; Q_v – вероятность восполнения злоумышленником честной сети с учетом отставания на v блоках (при неограниченном количестве попыток); PI_2 – вероятность злоумышленника сформировать z блоки одновременно или ранее честной сети; Q_2 – вероятность восполнения злоумышленником честной сети с учетом того, что злоумышленником уже сформировано необходимое количество блоков, то есть $Q_2 = 1$.

Заметим, что в данной работе рассматривается вероятность удачного проведения атаки двойной траты при условии неограниченного количества попыток злоумышленника догнать честную сеть. Случай, когда количество попыток ограничено, рассматривается в [76, 77].

Рассмотрим каждый из приведенных компонентов отдельно и сравним формулы для разных моделей.

2.2. Вычисление значения Q_v

Q_v – вероятности злоумышленника догнать честную сеть после того, как честная сеть сформировала необходимое количество блоков (z), и при этом злоумышленник отстает на $0 < v \le z$ блоков.

Для получения формулы определения Q_v воспользуемся материалами, приведенными в [78], и адаптируем их для случая формирования блоков в блокчейн системах.

Случайным блужданием называют случайный процесс специального вида, исторически связанный с моделью перемещения какой-либо частицы под действием некоторого случайного процесса в произвольном фазовом пространстве. При этом предполагается, что изменение на каждом шаге не зависит от предыдущих состояний и от времени.

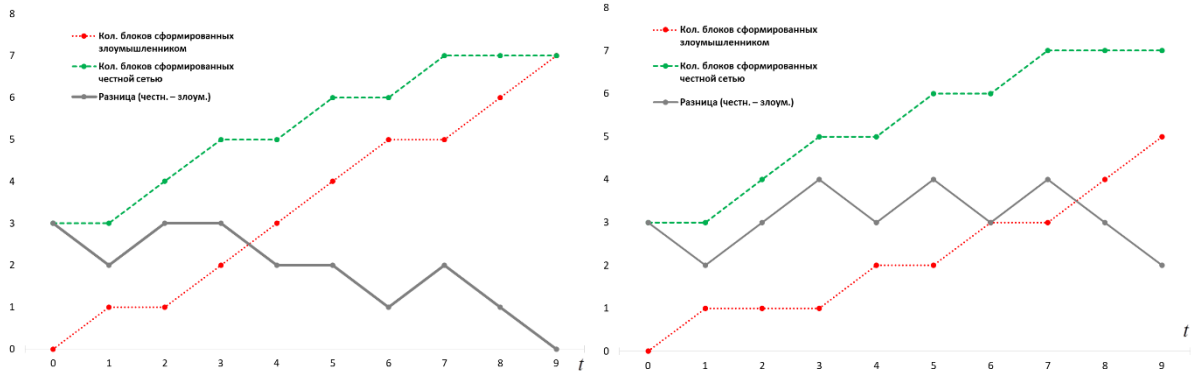
Основные черты общих случайных блужданий можно охарактеризовать на примере простейшего случайного блуждания, порождаемого схемой испытаний Бернулли. Подробно схема Бернули рассматривается во многих книгах по теории вероятностей, например в [79].

Пусть $\xi_0, \xi_1, \xi_2, \ldots$ – произвольная последовательность случайных величин, принимающих значения из множества $\{1, 2, \ldots, n\}$. Тогда последовательность $\xi_0, \ldots, \xi_n$ является последовательностью независимых случайных величин,

модель разорения игрока	*модель независимых игроков*
$\{\xi_i = 1\} = p,$	$\{\xi_i = 1\} = p',$
$\{\xi_i = 0\} = 0,$	$\{\xi_i = 0\} = r',$
$\{\xi_i = -1\} = q,$	$\{\xi_i = -1\} = q',$
$p + q = 1.$	$p' + r' + q' = 1.$

Положим $S_0 = x_0$, $S_t = x_0 + \xi_1 + \ldots + \xi_t = x_t$, $1 \le t \le n$. Последовательность $(S_t)_{t \le n}$ можно рассматривать как траекторию случайного блуждания некоторой «частицы», выходящей из нуля. При этом $S_{t+1} = S_t + \xi_{t+1}$. Данная траектория будет соответствовать разнице между количеством блоков, сформированных честной сетью и злоумышленником. Перемещение осуществляется скачками в дискретные моменты времени. В результате каждого перемещения (шага) частица, находящаяся в точке x_t в момент времени t, в следующий момент $t+1$ перемещается либо на единицу вверх (с вероятностью p для модели разорения игрока и с вероятностью p' для модели независимых игроков), либо на единицу вниз (с вероятностью q для модели разорения игрока и с вероятностью q' – для модели независимых игроков) или остается на месте (с нулевой вероятностью для модели разорения игрока и с вероятностью r' для модели независимых игроков), совершая таким образом случайное блуждание на полупрямой $[0; \infty)$.

При введенных условиях траектории случайного блуждания заметно отличаются для двух рассматриваемых моделей. Пример таких траекторий представлен на рис. 1. На рисунках показано одинаковое изменение сформированных блоков для честной сети (зеленая пунктирная линия). Для злоумышленника (красная линия точками), на рис. 1, *а* изменения происходят случайным образом, на рис. 1, *б* – в строгой зависимости от событий честной сети. В двух представленных случаях траектория разницы количества сформированных блоков (серая сплошная линия) значительно отличается для двух рассматриваемых моделей.



а *б*

Рис. 1. Пример траектории случайного блуждания: *а* – для модели независимых игроков; *б* – для модели разорения игрока

При этом вероятность траектории «частицы» достигнуть нуля будет соответствовать в моделях вероятности злоумышленником догнать честную сеть.

Для *модели разорения игрока* вероятность догнать злоумышленником честную сеть с учетом отставания на v блоков будет определяться (подробный вывод формулы можно найти, например, в [80, 81]) так:

$$Q_v = \begin{cases} \frac{1-\left(\frac{p}{q}\right)^v}{1-\left(\frac{p}{q}\right)^{N-v}}, \text{якщо } p \neq q \\ \frac{v}{N}, \text{якщо } p = q = 0{,}5 \end{cases}, \quad (2)$$

где q – вероятность злоумышленником создать блок; p – вероятность создать блок честной сетью (считаем, что $p+q=1$); N – позиция поглощающего экрана, в нашем случае достаточно большое число; $0 < v \leq N$.

В предельном случае, когда $N \to \infty$, получаем:

$$Q_v = \begin{cases} 1, & \text{якщо } p \leq q \\ \left(\frac{q}{p}\right)^v, & \text{якщо } p > q \end{cases}, \quad (3)$$

Для *модели независимых игроков* вероятность догнать злоумышленником честную сеть с учетом отставания на v блоков (подробный вывод формулы можно найти, например, в п. 3.3 [82]):

$$Q_v = \frac{\left(q'/p'\right)^v + \left(q'/p'\right)^{v+1} + \left(q'/p'\right)^{v+2} + \ldots + \left(q'/p'\right)^{N-1}}{1 + \left(q'/p'\right)^1 + \left(q'/p'\right)^2 + \left(q'/p'\right)^3 + \ldots + \left(q'/p'\right)^{N-1}}. \quad (4)$$

где q' – вероятность сократить отставание между злоумышленником и честной сетью (то есть вероятность того, что злоумышленник сформирует блок, а у честной сети сформировать блок не получится, определяется как $q' = q \cdot (1-p)$ и может принимать значения $0 \leq q' \leq 1$); p' – вероятность увеличить отставание (то есть вероятность того, что злоумышленник не сформирует блок, а у честной сети сформировать блок получится, определяется как $p' = p \cdot (1-q)$ и может принимать значения $0 \leq p' \leq 1$), при этом в общем случае $p' + q' \neq 1$; N – позиция поглощающего экрана, в нашем случае достаточно большое число; $0 < v \leq N$.

На рис. 2 представлены вероятности догнать злоумышленником честную сеть Q_v в зависимости от первоначального отставания v для двух рассматриваемых моделей (при q = 0,3; p = 0,7; N = 100).

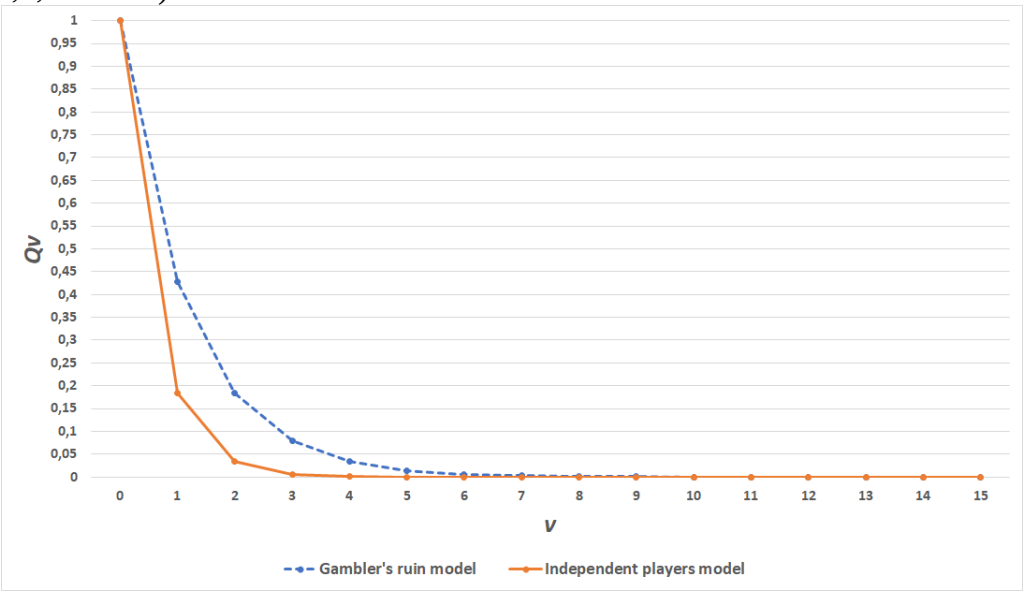


Рис. 2. Вероятность догнать злоумышленником честную сеть Q_v в зависимости от первоначального отставания v для модели разорения игрока (пунктирная линия) и модели независимых игроков

2.3. Вычисление значений PI_1 та PI_2 (модель независимых игроков)

В случае допущения, что функция распределения вероятности создать блок соответствует отрицательному биномиальному закону, как это делается в работе Мени Розенфельда [75], то вероятность честной сети сформировать z блоков ровно за $z+k_p$ попыток (где $k_p = 0,1,\ldots$):

$$P_p(p,z,k_p) = \binom{k_p+z-1}{k_p} p^z (1-p)^{k_p}, \tag{5}$$

где $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ – биномиальный коэффициент.

При этом вероятность злоумышленника сформировать v блоков ($v = 0,1,\ldots,z+k_p$) за такое же количество попыток (то есть ровно за $z+k_q$ попыток):

$$P_q(q,z,k_p,v) = \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}. \tag{6}$$

Таким образом, вероятность злоумышленника отстать от честной сети (то есть сформировать менее блоков)

$$P_q(q,z,k_p,0 \le v < z) = \sum_{v=0}^{z-1} \left\{ \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v} \right\}. \tag{7}$$

Чтобы подсчитать вероятность того, что злоумышленнику удалось догнать и опередить честную сеть (то есть сформировать z или более блоков) за количество попыток, которое не превышает значения $z+k_p$, необходимо суммировать все вероятности для $z \le v \le z+k_p$, т.е.

$$P_q(q,z,k_p,z \le v \le z+k_p) = \sum_{v=z}^{z+k_p} \left\{ \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v} \right\}. \tag{8}$$

Учитывая, что честная сеть способна сформировать z блоков за произвольное (от z и более) количество попыток, вероятность злоумышленника сформировать z блоков одновременно или ранее честной сети, возможно вычислить из выражения

$$PI_2 = \sum_{k_p=0}^{\infty} \left[P_p(p,z,k_p) \cdot \sum_{v=z}^{z+k_p} P_q(q,z,k_p,v) \right]. \tag{9}$$

Аналогичным образом будет подсчитываться вероятность злоумышленника сформировать z блоков позднее честной сети:

$$PI_1 = \sum_{k_p=0}^{\infty} \left[P_p(p,z,k_p) \cdot \sum_{v=0}^{z-1} P_q(q,z,k_p,v) \right]. \tag{10}$$

Подставляя выражения (PI_1), (PI_2) и (Q_v) в (1) и вынося общие составляющие, получаем

$$PI = \sum_{k_{p=0}}^{\infty} \left(P_p(p,z,k_p) \cdot \left[\sum_{v=0}^{z-1} \left\{ P_q(q,z,k_p,v) \cdot Q_{(z-v)} \right\} + \sum_{v=z}^{z+k_p} \left\{ P_q(q,z,k_p,v) \cdot 1 \right\} \right] \right) \tag{11}$$

или, подставляя (P_p) и (P_q),

$$PI = \sum_{k_p=0}^{\infty}\left(\binom{k_p+z-1}{k_p} p^z (1-p)^{k_p}\left[\sum_{v=0}^{z-1}\left\{\binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}\cdot Q_{(z-v)}\right\} + \sum_{v=z}^{z+k_p}\left\{\binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}\cdot 1\right\}\right]\right). \quad (12)$$

Напомним, что значение $Q_{(z-v)}$ вычисляется по формуле (4).

Согласно модели разорения игрока, приведенной в работе Мени Розенфельда [75], вероятность удачного проведения атаки двойной траты рассчитывается по выражению

$$PI = \begin{cases} 1 - \sum_{k=0}^{z-1}\binom{k+z-1}{k}\left(q^k p^z - p^k q^z\right), если\ p > q \\ 1, если\ p \le q \end{cases}. \quad (13)$$

На рис. 3 приведено сравнение результатов вероятности удачного проведения атаки двойной траты, рассчитанных согласно модели независимых игроков (для наглядности положено, что $p+q=1$) и модели разорения игрока.

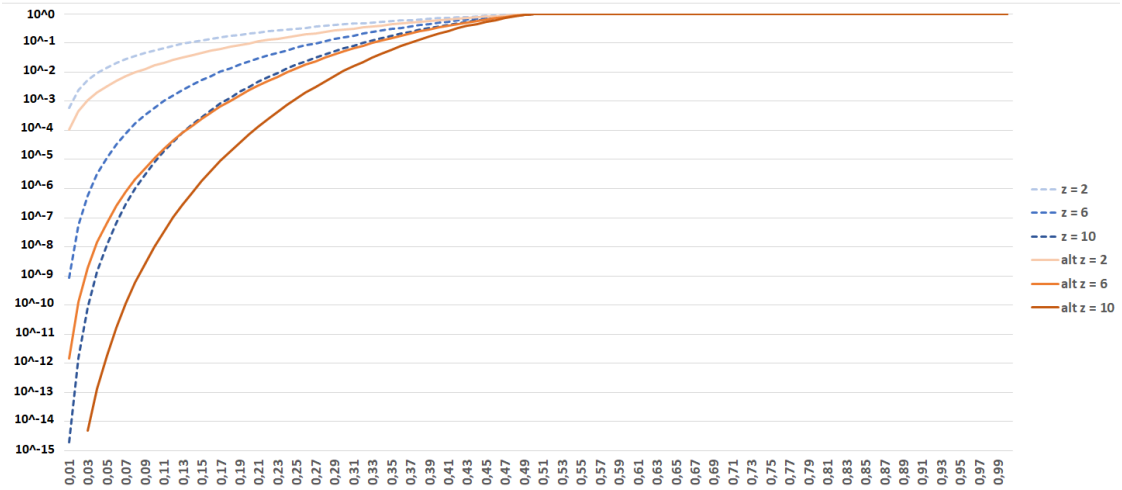


Рис. 3. Вероятности удачного проведения атаки двойной траты
рассчитанные согласно модели независимых игроков (по формуле (13))
и модели разорения игрока (формула 1 работы Розенфельда [39]) при различных значениях Z

Выводы

Рассмотрена вероятность успешного проведения атаки двойной траты на блокчейн системы, которые построены с помощью алгоритмов консенсуса по Доказательствам выполненной работы (PoW).

Показано, что проблема двойных трат в блокчейн системах не является чисто теоретической. Приведен ряд примеров проведения удачных атак на децентрализованные учетные системы с существенными (миллионными) убытками.

Проанализирована вероятность удачного проведения атак двойной траты с учетом скорректированной аналитической модели, основанной на «независимых игроках». Работа является логическим дополнением работ [76, 77, 83] и рассматривает корректировки аналитических выражений, приведенных в работах Сатоши Накамото [74] и Мени Розенфельда [75], основанных на моделях «разорения игрока».

Отмечено значительное отличие результатов, полученных по приведенным двум моделям. Получены аналитические оценки вероятностей успешной реализации атак двойной траты на блокчейн системы, которые существенно отличаются от результатов, полученных с использованием модели «разорения игрока».

Приведенные результаты свидетельствуют, что безопасность децентрализованных блокчейн систем, которые построены с консенсусами на основе доказательств выполненной работы, имеют более высокую надежность, чем считалось ранее. В качестве примера, при хэш-рейте злоумышленника $q = 0{,}1$ и $z = 6$ подтверждениях, вероятность удачного проведения атаки двойной траты будет составлять 0,00001 в соответствии с моделью «независимых игроков», против вероятности в 0,0006 полученного на основании модели «разорения игрока».

Полученные результаты могут быть полезными при обосновании конкретных показателей и параметров протокола консенсуса для блокчейн систем на основе доказательства проделанной работы, при применении его в качестве основного механизма установления консенсуса перспективных децентрализованных распределенных систем и сетей, построенных по технологии блокчейн.

Список литературы:

1. Saad M., Spaulding J., Njilla L., Kamhoua C.,Shetty S., Nyang D., Mohaisen A. Exploring the Attack Surface of Blockchain: A Systematic Overview. (2019) https://www.researchgate.net/publication/331806569_Overview_of_Attack_Surfaces_in_Blockchain

2. L. Mauri, S. Cimato, and E. Damiani. A comparative analysisof current cryptocurrencies // Proceedings of the 4th InternationalConference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira – Portugal, Jan. 2018, pp. 127–138. https://doi.org/10.5220/0006648801270138

3. G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies // Proceedings of the 2016 Annual Network and Distributed SystemSecurity Symposium (NDSS), San Diego, CA, Feb. 2016. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/centrally-banked-cryptocurrencies.pdf

4. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, andE. W. Felten. Research perspectives and challenges for bitcoin andcryptocurrencies // IACR Cryptology ePrint Archive, vol. 2015, p. 261, 2015. http://eprint.iacr.org/2015/261

5. A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou Hawk:The blockchain model of cryptography and privacy-preserving smartcontracts // Proceedings of the 37th IEEE Symposium on Securityand Privacy (Oakland), San Jose, CA, May 2016, pp. 839–858. https://doi.org/10.1109/SP.2016.55

6. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi,G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Z. Béguelin. Formal verificationof smart contracts: Short paper // Proceedings of the 23rdACM Conference on Computer and Communications Security(CCS), Vienna, Austria, Oct. 2016, pp. 91–96. http://doi.acm.org/10.1145/2993600.2993611

7. P. K. Sharma, S. Rathore, and J. H. Park. Distarch-scnet: Blockchain-based distributed architecture with li-fi communication for a scalable smart city network // IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 55–64, 2018. Available: https://doi.org/10.1109/MCE.2018.2816745

8. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g // IET Communications, vol. 12, no. 5, pp. 527–532, 2018. Available: https://doi.org/10.1049/iet-com.2017.0619

9. Sharma P.K., Singh S., Jeong Y.-S., Park J.H. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks // IEEE Communications Magazine, 2017, vol. 55 (9), pp. 78–85

10. R. Guo, H. Shi, Q. Zhao, and D. Zheng. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems // IEEE Access, vol. 6, pp. 11 676–11 686, 2018. Available: https://doi.org/10.1109/ACCESS.2018.2801266

11. D. Rakic. Blockchain technology in healthcare // Proceedings of the 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health, Funchal, Madeira, Portugal, March 2018., pp. 13–20. Available: https://doi.org/10.5220/0006531600130020

12. A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman. A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data (2016). URL https://www.media.mit.edu/publications/medrec-whitepaper/

13. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. Medrec: Using blockchain for medical data access and permission management // International Conference on Open and Big Data (OBD), 2016, pp. 25-30.

14. Yue, H. Wang, D. Jin, M. Li, W. Jiang. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control // Journal of medical systems, 2016, p. 218

15. E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha. A survey of how to use blockchain to secure internet of things and the stalker attack // Security and Communication Networks, vol. 2018, pp. 9. 675 050:1–9 675 050:27, 2018. Available: https://doi.org/10.1155/2018/9675050

16. P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park. Distblocknet: A distributed blockchains-based secure SDN architecture for iot networks // IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017. Available: https://goo.gl/UBv1Sf

17. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home // IEEE Percom workshop on security privacy and trust in the internet of thing, 2017

18. Y. Zhang, J. Wen. The iot electric business model: Using blockchain technology for the internet of things // Peer-to-Peer Networking and Applications, 2016, pp. 1-12.

19. J. Sun, J. Yan, K. Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities // Financial Innovation, 2016, p. 26.

20. H. Hyvärinen, M. Risius, and G. Friis. A blockchain-based approach towards overcoming financial fraud in public sector services // Business & Information Systems Engineering, vol. 59, no. 6, pp. 441–456, 2017. Available: https://doi.org/10.1007/s12599-017-0502-4

21. F. Holotiuk, F. Pisani, and J. Moormann. The impact of blockchain technology on business models in the payments industry // Towards Thought Leadership in Digital Transformation: 13. Internationale Tagung Wirtschaftsinformatik, St.Gallen, Switzerland, Feb, 2017. Available: http://aisel.aisnet.org/wi2017/track09/paper/6

22. S. Huckle, R. Bhattacharya, M. White, N. Beloff. Internet of things, blockchain and shared economy applications // Procedia Computer Science, Vol. 98, 2016, pp. 461-466.

23. P. Hurich, The virtual is real: An argument for characterizing bitcoins as private property // Banking & Finance Law Review, Vol. 31, Carswell Publishing, 2016, p. 573.

24. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, S. Chen. The blockchain as a software connector // The 13th Working IEEE/IFIP Conference on Software Architecture, 2016

25. E.Nordstr¨om., Personal clouds: Concedo, Masters thesis, Lulea University of Technology (2015).

26. J. S. Czepluch, N. Z. Lollike, S. O. Malone. The use of block chain technology in different application domains // The IT University of Copenhagen, Copenhagen, 2015.

27. G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, Broncovote: Secure voting system using ethereum's blockchain // Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira – Portugal, Jan 2018, pp. 96–107. Available: https://doi.org/10.5220/0006609700960107

28. F. S. Hardwick, R. N. Akram, and K. Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy // CoRR, vol. abs/1805.10258, 2018. Available: http://arxiv.org/abs/1805.10258

29. K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie. A review of contemporary e-voting: Requirements, technology, systems and usability // Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017

30. D. A. Gritzalis. Principles and requirements for a secure e-voting system // Computers & Security, vol. 21, no. 6, pp. 539–556, 2002

31. R. Anane, R. Freeland, and G. Theodoropoulos. E-voting requirements and implementation // The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392

32. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram.LSB: A lightweight scalable blockchain for IoT security and anonymity // J. Parallel Distrib. Comput., vol. 134, pp. 180–197, 2019

33. Arif S., Khan M.A., Rehman S.U., Kabir M.A. & Imran M. Investigating Smart Home Security: Is Blockchain the Answer? // IEEE Access, 2020, 8, 117802-117816

34. Younghun Lee, Shailendra Rathore, Jin Ho Park, Jong Hyuk Park. A blockchain-based smart home gateway architecture for preventing data forgery // Human-centric Computing and Information Sciences, 2020, Volume 10, Number 1, Page 1

35. PR Wire (2016) Gartner: blockchain and connected home are almost at the peak of the hype cycle. https://prwire.com.au/pr/62010/gartner-blockchain-andconnected-home-are-almost-at-the-peak-of-the-hype-cycle

36. J. DESJARDINS, Its official: Bitcoin was the top performing currency of 2015 (2016). URL http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/

37. J. Adinolfi, And 2016s best-performing commodity is ... bitcoin? (2016). URL http://www.marketwatch.com/story/and-2016s-best-performing-commodity-is-bitcoin-2016-12-22

38. Blockchain.info. Confirmed transactions per day (2020). URL https://blockchain.info/charts/n-transactions?timespan=all#

39. G. Zyskind, O. Nathan, and A. Pentland. Decentralizing privacy: Using blockchain to protect personal data // 2015 IEEE Symposium on Security and Privacy Workshops, SPW, San Jose, CA, USA, May 2015, pp. 180–184. Available: https://goo.gl/kTNim3

40. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. Enabling blockchain innovations with pegged sidechains. 2014

41. G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized Computation Platform with Guaranteed Privacy, 2015. https://arxiv.org/abs/1506.03471

42. M. Swan. Blockchain thinking: The brain as a dac (decentralized autonomous organization) // Proceedings of the Texas Bitcoin Conferenc, pp. 27–29, 2015.

43. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen. A survey on the security of blockchain systems // CoRR, vol. abs/1802.06993, 2018. Available: http://arxiv.org/abs/1802.06993

44. I.-C. Lin and T.-C. Liao. A survey of blockchain security issues and challenges // IJ Network Security, vol. 19, no. 5, pp. 653–659, 2017

45. N. Atzei, M. Bartoletti, T. Cimoli. A survey of attacks on Ethereum smart contracts sok // Proceedings of the 6th International Conference on Principles of Security and Trust -Volume 10204, 2017, pp. 164–186. Available: https://doi.org/10.1007/978-3-662-54455-6_8

46. M. C. K. Khalilov and A. Levi. A survey on anonymity and privacy in bitcoin-like digital cash systems // IEEE Communications Surveys and Tutorials, vol. 20, no. 3, pp. 2543–2585, 2018. Available: https://doi.org/10.1109/COMST.2018.2818623

47. D. Siegel. Understanding The DAO Attack. https://www.coindesk.com/understanding-dao-hack-journalists/

48. V. Buterin, Critical update re: Dao vulnerability (2016). URL https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

50. M. Saad, M. T. Thai, and A. Mohaisen. POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization // Proceedings of Asia Conference on Computer and Communications Security, ASIACCS, Incheon, Republic of Korea, Jun 2018, pp. 809–811. Available: https://goo.gl/4kgiCM

51. I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse. Bitcoin-ng: A scalable blockchain protocol // Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI), Santa Clara, CA, Mar. 2016, pp. 45–59. Available: https://goo.gl/VGN4yw

52. R. McMillan.The inside story of mt. gox, bitcoin's 460 million usd disaster. 2014. Available: https://www.wired.com/2014/03/bitcoin-exchange/

53. J. Adelstein, Behind the biggest Bitcoin heist in history: Inside the implosion of mt.gox (2016). URL http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html

54. Irreversible Transactions https://en.bitcoin.it/wiki/Irreversible_Transactions.

55. Partz H. Bittrex to Delist Bitcoin Gold by Mid-September, Following $18 Million Hack of BTG in May. 04.09.2018 https://cointelegraph.com/news/bittrex-to-delist-bitcoin-gold-by-mid-september-following-18-million-hack-of-btg-in-may

56. Cimpanu C. Hacker Makes Over $18 Million in Double-Spend Attack on Bitcoin Gold Network 24.05.2018 https://www.bleepingcomputer.com/news/security/hacker-makes-over-18-million-in-double-spend-attack-on-bitcoin-gold-network/

57. Iskra E. Responding to Attacks 24.05.2018 https://bitcoingold.org/responding-to-attacks/

58. Wilmoth J. Spend Attack, Exchanges Lose Millions https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/

59. Martin J. Bitcoin Gold Blockchain Hit by 51% Attack Leading to $70K Double Spend 27.01.2020 https://cointelegraph.com/news/bitcoin-gold-blockchain-hit-by-51-attack-leading-to-70k-double-spend

60. Lovejoy J. Bitcoin Gold (BTG) was 51% attacked. 25.01.2020 https://gist.github.com/metalicjames/71321570a105940529e709651d0a9765

61. Coinbase: Deep Chain Reorganization Detected on Ethereum Classic (ETC) https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

62. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1289489999004463111

63. HackMD: ETC Chain Split Diagnosis https://hackmd.io/@cUBb4hAvQciAEPoU2yfrzQ/Skd4X6MZw

64. Bitquery: Attacker Stole 807K ETC in Ethereum Classic 51% Attack https://blog.bitquery.io/attacker-stole-807k-etc-in-ethereum-classic-51-attack

65. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1291216063628226562

66. Binance (@binance) / Твиттер https://twitter.com/binance/status/1291225022866944000

67. Bitquery: Ethereum Classic Attack, 8 August: Catch me if you can https://blog.bitquery.io/ethereum-classic-attack-8-august-catch-me-if-you-can

68. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1299822510607917056

69. Ethereum Classic (@eth_classic) / Твиттер https://twitter.com/eth_classic/status/1299824170260340737

70. Wilmoth J. Privacy Coin Verge Succumbs to 51% Attack [Again] 22.05.2020 https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/

71. Ville Savolainen, Jorge Soria Ruiz-Ogarrio. Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies. 2019.
https://helda.helsinki.fi//bitstream/handle/10138/309233/SSRN_id3506748.pdf

72. Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., and Sirer, E. G. (2018). Decentralization in bitcoin and ethereum networks. https://arxiv.org/pdf/1801.03998.pdf

73.Lovejoy J. Reorgs on Bitcoin Gold: Counterattacks in the wild. 11.03.2020 https://medium.com/mit-media-lab-digital-currency-initiative/reorgs-on-bitcoin-gold-counterattacks-in-the-wild-da7e2b797c21

74. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p.

75. Rosenfeld M. Analysis of hashrate-based double-spending. 2014. 13 p. (arXiv preprint arXiv:1402.2009).

76. Poluyanenko N., Kuznetsov A., Lisickiy K., Datsenko S., Nakisko O., Rudenko S. (2021) The Problem of Double Costs in Blockchain Systems // Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, vol 1247. Springer,

Cham. PP 640-652. ISSN 2194-5357, ISSN 2194-5365 (electronic), ISBN 978-3-030-55505-4, ISBN 978-3-030-55506-1 (eBook) https://doi.org/10.1007/978-3-030-55506-1_57

77. Poluyanenko N, Kuznetsov A., Lazareva E., Marakushyn A. Extrapolation to calculate the probability of a double spending attack. CMIS 2020: 610-620.

78. Малахов Е.И. Случайные блуждания на полупрямой с поглощающим экраном с возможностью остановки http://math.isu.ru/ru/chairs/tpdm/docs/Platonovskie2017/Malahov.pdf

79. Гмурман В.Е. Теория вероятностей и математическая статистика. Москва : Высш. шк., 1997.

80. Ширяев А. Н. Вероятность : в 2-х кн. ; 4-е изд., переработ. и доп. Москва : МЦНМО, 2007.

81. K. Sigman. Gambler's ruin problem. www.columbia.edu/~ks20/FE-Notes/4700-07-Notes-GR.pdf , June 7 2016

82. Зубков А.М. Конспект лекций по теории случайных процессов. Москва : МГУ. Мех.-мат. факультет. 6-й семестр. 2008. – 90 с. https://epdf.pub/-6-88e2c451ff9dcbefcfbfacfb1bca654742391.html

83. Poluyanenko N., Pisarenko N., Safonenko V., Makushenko T., Pushko O., Zaburmekha Y., Kuznetsova K. Simulation of a double spending attack on the proof of work consensus protocol // CEUR Workshop Proceedings. Volume 2654, 2020, Pages 32-59. 2019 International Workshop on Cyber Hygiene, CybHyg 2019; Kyiv; Ukraine; 30 November 2019. ISSN: 16130073.

Поступила в редколлегию 12.10.2020

Сведения об авторах:

Полуяненко Николай Александрович – канд. техн. наук, доцент, доцент кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Горбенко Юрий Иванович – канд. техн. наук, первый заместитель главного конструктора, АТ «Институт информационных технологий», Украина; e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Сафоненко Владислав Едуардович – доцент кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: vladyslavsafonenko@gmail.com, ORCID: https://orcid.org/0000-0002-2983-8689

Кузнецов Александр Александрович – д-р техн. наук, профессор, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326