УДК 004.056.5 DOI: 10.26565/2519-2310-2019-4-02

РОЗРАХУНОК ЙМОВІРНОСТІ УСПІХУ АТАКИ РОЗГАЛУЖЕННЯ БЛОКЧЕЙН РЕЄСТРУ

Владислав Сафоненко, Микита Гончаров, Сергій Даценко, Єлизавета Лазарєва, Микола Полуяненко

Харківський національний університет імені В.Н. Каразіна, Харків, Україна
vladyslavsafonenko@gmail.com, wdpgames@yandex.ru, sergdacenko@gmail.com, lazareva15elizaveta@gmail.com, nlfsr01@gmail.com,

Рецензент: Володимир Хома, д.т.н., проф., Опольський політехнічний Університет, Ополе, Польща
xoma@wp.pl

Поступила: Декабрь 2019.

Анотація: *У роботі систематизовано відомості за тематикою питань атаки розгалуження блокчейн реєстру. Запропоновано огляд та узагальнення інформації, яка представлена в найбільш авторитетних роботах за даним напрямом. Здійснено аналіз відповідних робіт стосовно оцінки ймовірностей подвійної витрати в протоколі консенсусу "Доказу виконаної роботи". Розглянуто проблематику розорення гравця та проведено аналогію з атакою подвійної витрати на блокчейн. Розглянуто експеримент Пуассона для загального випадку. Проаналізовано моделі на підставі яких, С. Накамото та М. Розенфельдом були зроблені спроби отримати кількісну оцінку ймовірності успішної атаки подвійної витрати на деякі алгоритми консенсусу, що мають ймовірнісну завершеність. Наведено спрощення і допущення, що мають місце у відповідних моделях, за допомогою яких отримано кінцевий вираз.*

Ключевые слова: *комп'ютерні мережі; децентралізовані системи; блокчейн технології; атака на блокчейн мережі; атака розгалуження, атака подвійної витрати, експеримент Пуассона.*

1 Вступ

Незважаючи на постійно зростаючу популярність блокчейн систем, кількість організацій, що впровадили його, все ще залишається відносно невеликим. Багато хто стурбований погрозами блокчейн технологій з точки зору безпеки, інші вважають, що технологія має повільний спосіб підтвердження транзакцій (*в тому числі здійснення платежів*). Ті, хто приймає його, повинні спробувати прийняти всі запобіжні заходи, перш ніж приймати транзакцію, щоб запобігти атакам з подвійною витратою.

Один з важливих запобіжних заходів полягає в тому, щоб вирішити, коли приймати транзакцію, перш ніж здійснювати операцію. Суб'єкти, що застосовують блокчейн технології, вважають за краще отримувати певну ступінь впевненості в якості гарантії того, щодо неможливості скасування прийнятої транзакції. Ті, хто може дозволити собі почекати тривалий період часу, перш ніж приймати транзакцію (*наприклад, онлайн-платформи*), вимагають, як мінімум шість підтверджень, перш ніж приймати транзакцію і вважати її необоротною. Однак інші, які не можуть дозволити собі цей час очікування (*наприклад, торгові автомати та системи, що працюють в онлайн режимі*), приймають транзакції з ризиком втрати платежу в результаті вдалої атаки подвійної витрати. Ймовірності успішної проведення атаки, що реалізує даний спосіб, присвячена досить велика кількість робіт. Далі ми проаналізуємо найбільш авторитетні та популярні роботи даного напрямку, які аналізують ймовірність успіху зловмисника на основі частки обчислювальної потужності, яку він контролює.

2 Ймовірність, що запропонована Сатоши Накамото

2.1 Припущення, викладені в роботі

Перша спроба зробити оцінку даної ймовірності наводиться в розділ 11 відповідної роботи Сатоши Накамото [1]. Стисло наведемо цей розділ з деякими нашими коментарями.

«Розглянемо сценарій, в якому зловмисник намагається генерувати більш довгий ланцюг блоків, ніж чесні учасники. Навіть, якщо він досягне успіху, це не призведе до того, що можна буде створювати «гроші з повітря», привласнювати собі чужі монети, або вносити інші довільні зміни. Вузли ніколи не приймуть некоректну транзакцію, навіть якщо блок її

містить. Атакуючий може лише намагатися змінити одну зі своїх транзакцій, щоб повернути собі гроші». Відносно даного твердження слід зауважити, що вузли не приймуть некоректну транзакцію тільки, якщо мають коректну програмну реалізацію всіх можливих перевірок (*приклад існуючої некоректної реалізації в мережі Bitcoin описаний в* [2, 3]), а також, якщо вузол не є вузлом зловмисника або не входить з ним у змову.

«Гонку між чесними учасниками і нападаючим можна уявити як біноміальне випадкове блукання. Успішна подія, коли «чесний» ланцюг подовжується на один блок, призводить до збільшення відриву на одиницю, збільшуючи свою перевагу на +1 , а неуспішне, коли черговий блок формує зловмисник, – до його скорочення на один блок, зменшуючи розрив на -1. Ймовірність атакуючого наздогнати різницю в кілька блоків така ж, як і в задачі про «розорення гравця». Уявімо, що гравець має необмежений кредит, починає з деяким дефіцитом і у нього є нескінченно багато спроб, щоб відіграться».

Таким чином, у цьому абзаці, моделювання здійснюється за допомогою наступних припущень:

Припущення С. Накамото № 1 – гонку між чесними учасниками і нападаючим можна уявити, як біноміальне випадкове блукання.

Припущення С. Накамото № 2 – ймовірність перемоги зловмисника еквівалентна задачі про «розорення гравця».

Припущення С. Накамото № 3 – зловмисник має можливість (бажання) нескінченно довго проводити атаку на мережу формуючи альтернативний ланцюжок. Це припущення детально розглядається в роботі [4].

«Ймовірність того, що він досягне успіху, як і ймовірність зловмисника наздогнати чесних учасників, обчислюється таким чином [5]:

$p =$ ймовірність появи блоку у чесному ланцюжку;

$q =$ ймовірність того, що блок створить атакуючий;

$q_z =$ ймовірність того, що атакуючий надолужить різницю в z блоках:

$$q_z = \begin{cases} 1 & якщо, p \le q \\ (q/p)^z & якщо, p > q \end{cases}. \quad (1)$$

В разі $p > q$ ймовірність зменшується експоненційно з ростом числа блоків, на яке відстає зловмисник. Оскільки всі ставки проти нього, без вдалого ривка на початку його шанси на успіх стають мізерно малі».

Припущення С. Накамото № 4 – ймовірності формування блоку чесною мережею або зловмисником вважаються константами, що не змінюються у часі. Однак, як зазначено у роботах [4, 6] чесна мережа або зловмисник можуть додати обчислювальних потужностей, або навпаки, з плином часу вони можуть зменшитися. Пінзон та Роча пропонують для рівняння, що керує цими моделями, використовувати розподіл ймовірностей Ерланга (*на відміну від Накамото, що використовує розподіл ймовірностей Пуассона та Розенфельда, котрий використовує від'ємний біноміальний розподіл ймовірностей*).

«Розглянемо тепер, як довго одержувачу платежу варто чекати, перш ніж він буде повністю впевнений, що колишній власник не зможе скасувати транзакцію. Ми припускаємо, що зловмисник-відправник дозволяє адресату деякий час вірити, що платіж був проведений, після чого повертає гроші собі. Одержувач дізнається про це, але шахрай сподівається, що буде вже занадто пізно.

Адресат створює нову пару ключів і повідомляє свій публічний ключ відправнику прямо перед підписанням транзакції. Це не дозволить відправнику заздалегідь почати працювати над ланцюжком і провести транзакцію в той момент, коли він буде досить вдалим, щоб зробити ривок вперед. Після відправки платежу шахрай починає потай працювати над паралельною версією ланцюжка, що містить альтернативну транзакцію».

Припущення С. Накамото № 5 – одержувач створює новий гаманець (*пару ключів*) безпосередньо перед підписанням транзакції. Як показує практика, багато інтернет магазинів або

користувачів мають фіксовані біткойн-адреси, що є добре відомими і загальнодоступними протягом досить тривалого (*у порівнянні з часом, необхідним на проведення атаки подвійний витрати*) часу.

«Одержувач чекає, поки транзакція не буде додана в блок і поки той не буде продовжений ще блоками. Йому невідомий прогрес зловмисника, але якщо середня швидкість генерації чесних блоків – відома величина, то число блоків нападника підпорядковується розподілу Пуассона з математичним очікуванням: $\lambda = z\frac{q}{p}$».

Припущення С. Накамото № 6 – функція прогресу зловмисника відповідає розподілу Пуассона. У роботі [7] показано помилковість даного припущення С. Накамото та і наводиться більш влучний вираз, відповідно до негативного біноміального розподілу.

«Щоб отримати можливість того, що атакуючий обжене чесних учасників мережі у кількості створених блоків, ми множимо значення випадкової величини (*число створених ним блоків*) на ймовірність того, що він зможе надолужити різницю, що залишилася (2):

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(q/p)^{(z-k)} & \text{если } k \le z\\ 1 & \text{если } k > z\end{cases}. \qquad (2)$$

Перегрупувавши складові і позбавляючись від нескінченної низки, отримуємо (3):

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right). \qquad (3)$$

Склавши відповідну програму (*для розрахунку ймовірності того, що атакуючий зможе надолужити різницю (p)*), та проаналізувавши отримані результати, можливо побачити, що ця ймовірність експоненційно падає з ростом z (див. рис. 1-2).

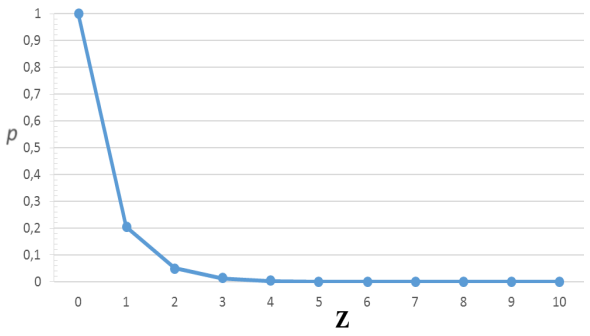

Рис. 1 – Розподіл ймовірності *p* при *q=0,1**

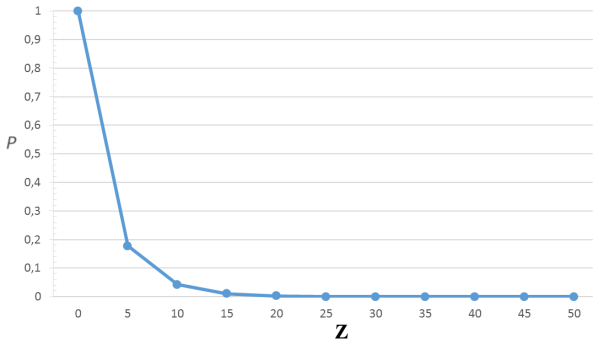

Рис. 2 – Розподіл ймовірності *p* при *q=0,3**

** q - ймовірність того, що блок створить атакуючий.*

2.2 Аналіз результатів щодо інших обмежень

Для того, щоб продемонструвати, які ще спрощення та допущення були зроблені в роботі С. Накамото, необхідно більш детально розглянути виведення математичних виразів, на які саме спирався С. Накамото при створенні моделі атаки. Більшість з наведеного в цьому підрозділі взято з [8, 9]. Відповідно до припущень С. Накамото № 1, гонку між чесними учасниками та нападаючим можна уявити, як біноміальне випадкове блукання.

Випадкове блукання – це математичний процес, який відбувається уздовж ряду станів, що з'єднані лінією (Рис. 3). Кожний стан нумерується, а процес починається зі стану «0». Таким чином, підкидаючи монету, ми просуваємося вперед по «орлам» і назад по «решкам» уздовж ряду станів.

Біткойн налаштовується так, що блоки виявляються приблизно кожні десять хвилин. При спробі реалізації атаки подвійної витрати, атакуючий буде генерувати блок в середньому кожні $10/q$ хвилин, а чесні майнери – генерувати блок в середньому кожні $10/p$ хвилин. Але, це тільки в середньому. Через випадковості, що притаманні майнінгу, зловмисник в будь-який момент може згенерувати на кілька блоків більше або менше, ніж чесні майнери. «Наше» випадкове блукання буде відслідковувати відмінність між їхніми підрахунками.

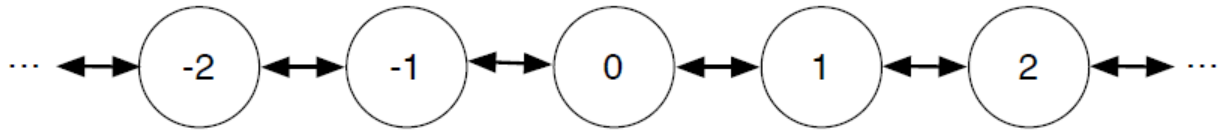

Рис. 3 – Схема процесу підрахунку

Щоб зрозуміти сутність походження наведеного вище рівняння (1), для якого Накамото цитує підручник Феллера 1968 року [5], ми повинні декілька заглибитися в проблему «завдання про розорення гравця» та її «невелику зміну». Для цього трохи змінимо позначення, які використовує Накамото, щоб зробити вираження більш простішим і послідовнішим. Те, що Накамото (і Феллер) позначили як «q_z» у формулі (1) в оригінальній статті, ми позначаємо як «Q_z».

2.3 Задача «розорення гравця»

Ця «знаменита» задача вперше була досліджена Блезом Паскалем (Blaise Pascal) і П'єром де Ферма (Pierre de Fermat) в 1656 році [10]. Вона моделює гравця, який входить в казино, щоб зіграти в просту азартну гру. Задача стартує з початкового стану з i монет та робить серію ставок. Кожна ставка приводить або до виграшу 1 монети з ймовірністю q, або програшу 1 монети з ймовірністю $p = q - 1$. Виграш або програш при кожній ставці не залежить від всіх інших ставок. Мета гравця полягає в тому, щоб виграти N монет, перш ніж розоритися (*тобто зменшити свій капітал до 0 монет*). Якщо гравець розорився, він більше не зможе грати, тому що у нього нема грошей, щоб виплатити 1 монету в разі наступного програшу. Таким чином, досягнення N або 0 завершує гру.

Припущення С. Накамото № 7 – $p + q = 1$. Тут і далі використовуються умови взаємозв'язку ймовірності формування блоку зловмисником та чесною мережею, в загальному ж випадку ймовірності q та p є незалежними значеннями. Наведені вирази не дають відповіді яким саме буде результат при незалежних величинах цих ймовірностей, що було зазначено у [11].

Дійсно, у визначенні завдання про розорення гравця використовується ймовірнісний простір з двома елементарними подіями: - «виграв перший гравець» та «виграв другий гравець». При моделюванні атаки подвійної витрати С. Накамото (*і, як буде показано далі, М. Розенфельд*) інтерпретують елементарні результати цього завдання як «блок, сформований чесною мережею» (*з ймовірністю такого результату* p) та «блок, сформований атакуючим» (*з ймовірністю* q), при чому $p = 1 - q$.

Однак в реальних блокчейн-системах ймовірність формування блоку (*знаходження прообразу функції гешування*) визначається виключно гешрейтом (*обчислювальними можливостями*) кожного учасника, тобто умова $p = 1 - q$ не повинна завжди виконуватися.

2.4 Невелика варіація розорення гравця

Щоб повернутися до С. Накамото, нам потрібно змінити гру. Накамото стверджує про ймовірність того, що зловмисник «коли-небудь наздожене», що є досить рішучою заявою. При цьому Накамото не аналізує, чи вдасться вирішити економіку: - можливо, зловмисник витрачає більше на майнінг, ніж вийде повернути після успішного проведення їм атаки подвійної витрати, або можливо, винагорода у вигляді монет за анонсування величезної кількості нових блоків більш прибуткова, ніж подвійна витрачена транзакція.

Метою Накамото є *виключно аналіз найгіршого сценарію*, коли зловмисник не шкодує витрат на використання своїх існуючих потужностей майнингу, щоб виграти в грі «розорення гравця». В контексті цього Накамото, можливо, намагався визначити найгірший випадок для кожного значення q, але в дійсності, найгіршим випадком є просто будь-яке значення $q > 0{,}5$.

Щоб досягти анонсованої мети Накамото, ми спочатку дозволимо атакуючому втратити до «y» монет, перш ніж виграти (*і потім ми подивимося, що станеться, коли y перейде в нескінченність*). Таким чином, ця невелика зміна перетворюється у початкове розорення гравця в такий спосіб: – гравець починає з $i = y$ монет, а гра закінчується або при 0 монетах, що є поразкою, або при $N = y + z$ монетах, які представляють собою виграш

$$q_y = \begin{cases} \dfrac{1-(p/q)^y}{1-(p/q)^{y+z}}, & \text{якщо } p \neq q; \\ \dfrac{y}{(y+z)}, & \text{якщо } p = q = 0{,}5. \end{cases} \tag{4}$$

Розглянемо випадок, коли гравець хоче втратити нескінченну суму грошей та, отже, має при цьому всі необмежені ресурси. Іншими словами, коли «y» йде у нескінченність. У разі, коли, $p < q$, то $(p/q)^y \to 0$, так як $y \to \infty$:

$$\lim_{y\to\infty} \frac{1-(p/q)^y}{1-(p/q)^{y+z}} = 1, \text{ коли } p < q. \tag{5}$$

У разі, коли $p > q$, для розрахунку границь беремо співвідношення $(p/q)^y$, як коефіцієнт з чисельника і знаменника:

$$\frac{1-(p/q)^y}{1-(p/q)^{y+z}} = \frac{(p/q)^y\left((p/q)^{-y}-1\right)}{(p/q)^y\left((p/q)^{-y}-(p/q)^z\right)} = \frac{(p/q)^{-y}-1}{(p/q)^{-y}-(p/q)^z}. \tag{6}$$

Відповідно, коли $p > q$, то $\left(\frac{p}{q}\right)^{-y} = \left(\frac{q}{p}\right)^y \to 0$, так як $y \to \infty$:

$$\lim_{y\to\infty} \frac{(p/q)^{-y}-1}{(p/q)^{-y}-(p/q)^z} = \frac{-1}{-(p/q)^z} = \left(\frac{q}{p}\right)^z, \text{ коли } p > q. \tag{7}$$

Оскільки в рівнянні (7) передбачається, що зловмисник має необмежені ресурси, то ми не можемо використовувати наш існуючий запис («q_∞» насправді не має сенсу), тому ми змінимо запис, та дозволимо «Q_z» позначати ймовірність надолуження з урахуванням z при необмежених ресурсах:

$$Q_z = \begin{cases} 1, & \text{якщо } p \le q; \\ \left(\dfrac{q}{p}\right)^z, & \text{якщо } p > q. \end{cases} \tag{8}$$

Слід зазначити, що вираз (8) справедливий тільки, якщо зловмисник має необмежені ресурси (*тобто, $N = y + z = [y \to \infty] = \infty$*), що вже обмовлялося вище (*див. Припущення Сатоши Накамото № 3*).

Рівняння для цього розділу було адаптовано з відповідних заміток Л. Рей-Беллі [12].

2.5 Аналогія з атакою подвійної витрати на блокчейн

Аналогію з нашим сценарієм блокчейну слід провести наступним чином. Нехай p – потужність майнингу та ймовірність того, що чесні майнери знайдуть наступний блок, а q – це

потужність майнінгу атакуючого. Ми визначаємо $q + p = 1$, так як припускаємо, що тільки атакуючий або чесний майнер може сформувати блок в кожному раунді. Якщо у атакуючого для здійснення майнінгу є необмежені апаратні ресурси та він зупиняється, коли досягає z, то ми можемо використовувати рівняння (8).

Припущення С. Накамото № 8 – тут варто відзначити, що «Q_z» це ймовірність того, що зловмисник просто наздожене чесну мережу. Замість цього Накамото мав би вирахувати «Q_{z+1}», тобто ймовірність того, що атакуючий випередить чесних майнерів.

Таким чином, у виразі (4) необхідно визначити виграш, як $N = y + z + 1$ [9]. Це припущення змінює гру так, щоб вона враховувала ймовірність атакуючого перевершити блоки, zrs сформовані чесними майнерами (9):

$$q_y = \begin{cases} \dfrac{1-(p/q)^y}{1-(p/q)^{y+z+1}}, & \text{якщо } p \neq q; \\ \dfrac{y}{(y+z+1)}, & \text{якщо } p = q = 0{,}5. \end{cases} \tag{9}$$

При цьому, якщо $q > p$, то це не призведе до змін, бо:

$$\lim_{y\to\infty} \frac{1-(p/q)^y}{1-(p/q)^{y+z+1}} = 1, \tag{10}$$

але для $p > q$, розділивши чисельник та знаменник на $(p/q)^y$, а потім обчислюючи границю отримуємо, що:

$$\frac{1-(p/q)^y}{1-(p/q)^{y+z+1}} = \frac{(p/q)^y\left((p/q)^{-y}-1\right)}{(p/q)^y\left((p/q)^{-y}-(p/q)^{z+1}\right)} = \frac{(p/q)^{-y}-1}{(p/q)^{-y}-(p/q)^{z+1}} \tag{11}$$

$$\lim_{y\to\infty} \frac{(p/q)^{-y}-1}{(p/q)^{-y}-(p/q)^{z+1}} = \frac{-1}{-(p/q)^{z+1}} = \left(\frac{q}{p}\right)^{z+1}, \quad (\text{коли } p > q).$$

Все це призведе до зміни виразу (8) до наступного виду:

$$Q_z = \begin{cases} 1, & \text{якщо } p \leq q; \\ \left(\dfrac{q}{p}\right)^{z+1}, & \text{якщо } p > q. \end{cases} \tag{12}$$

2.6 Експеримент Пуассона

Сатоши Накамото продовжує наступний аналіз.

«Одержувач чекає, поки транзакція не буде додана в блок та поки той не буде продовжений ще «z» блоками. Йому невідомий прогрес зловмисника, але якщо середня швидкість генерації чесних блоків – відома величина, то число блоків нападника підпорядковується розподілу Пуассона з математичним очікуванням:

$$\lambda = z\frac{q}{p}». \tag{13}$$

Щоб знайти це очікуване значення, Накамото використовує математичну модель, яка має назву «експеримент Пуассона» (*Припущення С. Накамото № 6*). В експерименті Пуассона ми моделюємо реальну ситуацію, що пов'язана з ймовірністю, підраховуючи кількість успіхів в серії інтервалів, виміряних в часі.

Щоб використовувати таку модель, ми повинні припустити наступне [13]:

1. *Кількість успіхів протягом кожного часового інтервалу не залежить від будь-якого іншого інтервалу.*
2. *Ймовірність того, що один успіх відбудеться протягом дуже короткого інтервалу часу, пропорційна тривалості інтервалу часу.*
3. *Ймовірність більш ніж одного успіху за такий короткий проміжок часу незначна.*
4. *Ймовірність успіху не змінюється під час експерименту, хоча в дійсності майнер може збільшувати або зменшувати свої ресурси (Припущення С. Накамото № 4).*

Щоб використовувати добре відомі результати для пуассонівських експериментів, наша перша задача – визначити значення «λ», яке є середнім числом успіхів, які ми очікуємо протягом кожного інтервалу. Це показник: – «*успіхи / інтервал*».

Для нас успіх – це кількість блоків, які, ми припускаємо, знайде зловмисник. А інтервал – це час, витрачений торговцем на очікування формування «*z*» блоків чесними майнерами.

Мережа біткоін налаштована таким чином, що кожні $T = 10$ хвилин виявляється 1 блок з 100% поточної потужності майнінгу. Для чесних вузлів кожні «*T*» хвилин виявляється «*p*» блоків. Щоб отримати «*z*» блоків, їм знадобиться наступний інтервал:

$$z \text{ блоків} \cdot \frac{T \text{ хвилин}}{p \text{ хвилин}} = \frac{zT}{p} \text{ хвилин}. \tag{14}$$

Для атакуючого q блоків виявляються кожні T хвилин, тому протягом цього інтервалу зловмисник буде формувати блоки зі швидкістю (15):

$$\lambda = \left(\frac{zT}{p} \text{хвилин/интервал} \right) \cdot \frac{q \text{ блоків}}{T \text{ хвилин}} = \frac{zq}{p} \text{ блоків/интервал}, \tag{15}$$

де $\lambda = \frac{zq}{p}$, просто середнє. Це означає, що випадкова величина була замінена на її математичне сподівання.

Припущення С. Накамото № 9 – (*як було зазначено в роботі* [14]) випадкову величину кількості сформованих було замінено на математичне очікування цієї величини.

У випробуванні пуассонівського експерименту ми будемо отримувати дані з розподілу Пуассона (*тобто ми будемо кидати кубик з розподілом Пуассона*), щоб побачити, скільки вдалих випробувань насправді сталося. Припустимо, сталося «*X*» вдач у конкретному випробуванні. Ймовірність того, що $X = k$ успіхів відбулося протягом нашого інтервалу, де $k \geq 0$, успіхів, які відбулися протягом нашого інтервалу, де:

$$P(X = k; \lambda) = \frac{\lambda^k e^{-\lambda}}{k!}. \tag{16}$$

Рівняння (16) називається «функцією щільності ймовірності Пуассона» [13].

2.7 Загальний випадок

Ми хочемо знати відповідь на більш загальне питання: - враховуючи, що продавець буде чекати *«z»* блоків, перш ніж фізично передати товари, замовлені зловмисником, наскільки ймовірним є те, що зловмисник з потужністю майнінгу q може виробити більше блоків, ніж чесні майнери до цього моменту або після?

Відповідь Накамото полягає в наступному. Нехай *«X»* буде випадковою величиною, що представляє кількість блоків, які зловмисник знайде за час, коли чесні майнери сформували *«z»* блоків. Ми вже визначили $P(X; \lambda)$, як ймовірність того, що атакуючий сформує *«X»* блоків. Також ми знаємо, що ймовірність надолуження від різниці, що залишилася $z - k$ дорів-

нює q_{z-k}. Тому, щоб знайти загальну ймовірність надолуження, ми підсумовуємо всі можливості X:

$$P\left(X=0;\lambda\right)Q_z+P\left(X=1;\lambda\right)Q_{z-1}+\ldots=\sum_{k=0}^{\infty}P\left(X=k;\lambda\right)Q_{z-k}=$$

$$=\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}Q_{z-k}\cdot \tag{17}$$

Фактично, коли $k>z$, ймовірність того, що зловмисник наздожене, дорівнює 1.

І так, як стверджує Сатоши Накамото: – «Щоб отримати можливість того, що атакуючий обжене чесних учасників, ми множимо значення випадкової величини (*число створених ним блоків*) на ймовірність того, що він зможе надолужити різницю, що залишилася(19):

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{Bmatrix}\left(q/p\right)^{(z-k)} & \text{якщо } k\le z\\ 1 & \text{якщо } k>z\end{Bmatrix}\text{».} \tag{18}$$

Нарешті, оскільки ймовірність того, що щось трапиться, дорівнює 1 мінус ймовірність того, що це не так, Накамото перебудовує наш (*майже*) кінцевий результат. Тут віднімаємо з 1 ймовірність того, що атакуючий видобуває k блоків і не наздожене (19)

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{Bmatrix}\left(q/p\right)^{(z-k)} & ,\text{якщо } k\le z\\ 1 & ,\text{якщо } k>z\end{Bmatrix}=1-\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{Bmatrix}1-\left(q/p\right)^{(z-k)} & ,\text{якщо } k\le z\\ 1-1 & ,\text{якщо } k>z\end{Bmatrix}=$$

$$=1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left(1-\left(\frac{q}{p}\right)^{(z-k)}\right)-\sum_{k=z+1}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left(0\right)=1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left(1-\left(\frac{q}{p}\right)^{(z-k)}\right). \tag{19}$$

Або, як Накамото говорить лаконічніше: «Перестановка, щоб уникнути підсумовування в нескінченному ряду розподілу

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-\left(q/p\right)^{(z-k)}\right)\text{».} \tag{20}$$

Знову ж таки, з огляду на *«Припущення С. Накамото № 8»* ми зацікавлені в тому, щоб зловмисник випередив чесних майнерів (21)

$$1-\sum_{k=0}^{z+1}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-\left(q/p\right)^{(z+1-k)}\right). \tag{21}$$

2.8 Ймовірність, що запропонована Мені Розенфельдом

Наведемо, з деякими нашими коментарями, витяг з розділу 4 роботи Розенфельда [15]. В авторському тексті ми зминемо оригінальні позначення, що введені Мені Розенфельдом на позначення, які ми вже використовували раніше в даній роботі.

«Стандартною практикою для продавця є очікування z підтверджень платіжної транзакції, а потім надання продукту. Поки мережа формує ці підтверджуючі блоки, зловмисник будує свою власну гілку, яка суперечить загальнодоступному ланцюгу. Яка ймовірність, що він вдало проведе атаку подвійної витрати?

До отримання z підтверджень зловмисник не може опублікувати своє альтернативне розгалуження, навіть якщо воно довше, оскільки він відрадить продавця від виконання замовлення. Він повинен дочекатися z підтверджень, а вже потім, або опублікувати свою гілку,

якщо у нього є перевага, або продовжити роботу над нею, сподіваючись, що він отримає необхідну перевагу.

Шанси на успіх у вирішальній мірі залежать від відставання зловмисника в момент досягнення z підтверджень чесною мережею. У своїй статті Сатоши Накамото робиться спрощене припущення (*згадане нами, як Припущення С. Накамото № 9*), що чесна мережа за середній час знаходить z блоків, $\frac{zT}{p}$ та, відповідно, k – число блоків знайдених атакуючим за цей час, слідує розподілу Пуассона (*Припущення С. Накамото № 6*) із середнім $z\frac{q}{p}$. Ми не будемо використовувати це припущення, а будемо більш точно моделювати k, як від'ємну біноміальну змінну; це кількість успіхів (*блоків, які виявив атакуючий*) до z невдач (*блоків, виявлених чесною мережею*) з ймовірністю q успіху. Ймовірність для даного значення k дорівнює

$$P(k)=\binom{k+z-1}{k}p^z q^k, \tag{22}$$

де $\binom{n}{k}=\frac{n!}{(n-k)!k!}$ – біноміальний коефіцієнт.

Як тільки в чесній мережі буде знайдено z блоків, протягом періоду часу, в ході якого атакуючий сформує $k+1$ блоків (*ми припускаємо, що один блок був попередньо здобутий атакуючим до початку атаки*), гонка починається з відставанням в $z-k-1$ блоків. Звідси випливає, що ймовірність подвійної витрати, коли продавець очікує z підтверджень, дорівнює (23)

$$r=\sum_{k=0}^{\infty}P(k)a_{z-k-1}=\sum_{k=0}^{z-1}\binom{k+z-1}{k}p^z q^k\left(\min\left(q/p,1\right)\right)^{z-k}+$$

$$+\sum_{k=z}^{\infty}\binom{k+z-1}{k}p^z q^k=\begin{cases}1-\sum_{k=0}^{z}\binom{k+z-1}{k}\left(p^z q^k-p^k q^z\right), & \text{якщо } q<p;\\ 1, & \text{якщо } q\geq p.\end{cases} \tag{23}$$

».

Зауважимо, що тут М. Розенфельд робить деякі припущення, що і С. Накамото (*Припущення С. Накамото №№ 1, 2, 3, 4, 5, 8*), але виправляє помилку, що пов'язана з *Припущеннями С. Накамото № 6 та № 9*.

У ряді робіт [16,17] їх авторами звернено увагу на те, що потрібно враховувати час синхронізації у мережі. У цих роботах представлений перший аналіз вразливості системи Біткойн з мережевої точки зору, крім того, ґрунтуючись на експериментальних даних, стверджується, що Біткойн є сильно централізований. Так, як наведено в [18], функція розподілу суми однаково розподілених експоненціальних величин є розподіл Ерланга.

Таким чином, можливо додатково виділити *Припущення № 10* (*яке присутнє у розглянутих розрахунках С. Накамото та М. Розенфельд*), сутність якого полягає в наступному: – результати отримані в припущенні про те, що час поширення блоку в мережі дорівнює нулю.

5 Висновки

В представленій роботі запропоновано критичний аналіз відомих публікацій щодо оцінці ймовірностей подвійний витрати в протоколі консенсусу *«Доказу виконаної роботи»*. Продемонстровано наявність невідповідності та необґрунтованих припущень у декількох відомих роботах, наприклад, таких як роботи Сатоши Накамото [1] та Мені Розенфельда [15].

Виконано аналіз моделей на підставі яких С. Накамото та М. Розенфельдом (*а також іншими авторами, що проводили уточнення отриманих виразів*) були зроблені спроби отримати кількісну оцінку ймовірності успішної атаки подвійний витрати на деякі алгоритми консенсусу, що мають ймовірнісну завершеність. Наведені припущення (*спрощення та допущення*), що мають місце у моделях, та за допомогою яких було отримано кінцевий вираз.

До основних припущень, які були зроблені в роботах, що розглядаються, слід віднести:

Припущення № 1 (С. Накамото, М. Розенфельд) – гонку між чесними учасниками і нападаючим можна уявити, як біноміальне випадкове блукання;

Припущення № 2 (С. Накамото, М. Розенфельд) – ймовірність перемоги зловмисника еквівалентна задачі про «розорення гравця»;

Припущення № 3 (С. Накамото, М. Розенфельд) – зловмисник має можливість (бажання) нескінченно довго проводити атаку на мережу, формуючи альтернативний ланцюг, тобто зловмисник має необмежені для цього ресурси;

Припущення № 4 (С. Накамото, М. Розенфельд) – ймовірності формування блоку чесною мережею або зловмисником вважаються константами, що не змінюються у часі;

Припущення № 5 (С. Накамото, М. Розенфельд) – одержувач замовлених товарів створює новий гаманець (*пару ключів*) безпосередньо перед підписанням транзакції.

Припущення № 6 (С. Накамото) – функція прогресу зловмисника відповідає розподілу Пуассона;

Припущення № 7 (С. Накамото, М. Розенфельд) – група подій в гонці між чесною мережею та зловмисником складається тільки з двох подій, ймовірності яких однозначно пов'язаним між собою співвідношенням $p + q = 1$;

Припущення № 8 (С. Накамото, М. Розенфельд) – вираз, щодо ймовірності успішного формування зловмисником свого альтернативного ланцюжка, отримано для випадку, коли зловмисник лише наздожене, а не випередить, чесну мережу.

Припущення № 9 (С. Накамото) – випадкову величину кількості сформованих блоків було замінено на математичне очікування цієї величини.

Припущення № 10 – результати були отримані в припущенні, що час поширення блоку в мережі дорівнює нулю.

В наведеної роботі авторським колективом розглянута задача розорення гравця та її невелика варіація, сутність якої описано в п. 2.4. Підкреслено існування аналогії з атакою «подвійної витрати на блокчейн» та проведено «Експеримент Пуассона». Розглянуто вірогідність випередження зловмисником чесної мережі в кількості сформованих блоків у загальному випадку.

Посилання

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto., 2009. – 9 с.

[2] Hackernoon: Two Ways to Double-Spend https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362 (дата звернення 28.12.19)

[3] BitcoinCore: CVE-2018-17144 Full Disclosure https://web.archive.org/web/20191005023317/https://bitcoincore.org/en/2018/09/20/notice/ (дата звернення 28.12.19)

[4] A. Pinar Ozisik., Brian Neil Levine. An Explanation of Nakamoto's Analysis of Double-spend Attacks https://arxiv.org/pdf/1701.03977.pdf (дата звернення 28.12.19)

[5] W. Feller. An Introduction to Probability Theory and its Applications: Volume I, Volume 3. John Wiley & Sons London-New York-Sydney-Toronto, 1968.

[6] Pinzón C., Rocha C. Double-spend Attack Models with Time Advantange for Bitcoin. Electronic Notes in Theoretical Computer Science. Volume 329, 9 December 2016, Pages 79-103 https://doi.org/10.1016/j.entcs.2016.12.006 (дата звернення 28.12.19)

[7] Rosenfeld M. Analysis of hashrate-based double-spending / Meni Rosenfeld., 2014. – 13 с (arXiv preprint arXiv:1402.2009)

[8] Ozisik A. P. and Levine B. N., “An explanation of Nakamoto’s analysis of double-spend attacks,” arXiv preprint arXiv:1701.03977, 2017 https://arxiv.org/pdf/1701.03977.pdf (дата звернення 30.12.19)

[9] Zaghloul, E., Li, T., Mutka, M.W., & Ren, J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435

[10] A.W.F. Edwards. Pascal's problem: The «gambler's ruin». Revue Internationale de Statistique, 51(1):73-79 (http://www.jstor.org/stable/1402732), Apr 1983

[11] Ковальчук Л.В. Основні визначення у галузі блокчейну та детальний аналіз результатів Накамото-Розенфельда-Грунспана про ймовірність атаки подвійної витрати. Звіт про НДР (проміжний), Харків, АТ ІІТ, 36 с.

[12] L. Rey-Bellet. Gambler's ruin and bold play. http://people.math.umass.edu/~lr7q/ps_files/teaching/math456/Week4.pdf, June 7 201651% Attack Explained: The Attack on a Blockchain https://www.fxempire.com/education/article/51-attack-explained-the-attack-on-a-blockchain-513887 (дата звернення 30.12.19)

[13] Walpole R. E., Myers R. H., Myers S. L., Ye K. Probability & Statistics for Engineers & Scientists. Prentice Hall, (See pg. 161 for a discussion of Poisson experiments), 9-th edition, 2012.
[14] Grunspan C., Pérez-Marco R. Double spend races. 2017. hal-01456773 https://hal.archives-ouvertes.fr/hal-01456773 (дата звернення 11.01.20)
[15] Rosenfeld M. Analysis of hashrate-based double-spending / Meni Rosenfeld., 2014. – 13 c (arXiv preprint arXiv:1402.2009)
[16] Apostolaki M. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies / M. Apostolaki, A. Zohar, L. Vanbever. – San Jose, CA, USA, 2017. – 18 p. https://btc-hijack.ethz.ch/files/btc_hijack.pdf
[17] Apostolaki M., Marti G., Müller J., Vanbever L. SABRE: Protecting Bitcoin against Routing Attacks. –San Diego, CA, USA, 2019. pp. 1-15 https://dx.doi.org/10.14722/ndss.2019.23252
[18] Kaidalov D.S., Kovalchuk L.V., Nastenko A.O., Rodinko M.Yu., Shevtsov O.V., Oliynykov R.V. Comparison of block expectation time for various consensus algorithms. Radio Electronics, Computer Science, Control. 2018. № 4. pp. 159-171 DOI 10.15588/1607-3274-2018-4-15

Рецензент: Владимир Хома, д.т.н., проф., Опольский Политехнический Университет, Ополе, Польша.
E-mail: kalash@itesm.mx

Поступила: Декабрь 2019.

Авторы:
Владислав Сафоненко, студент ФКН, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail:vladyslavsafonenko@gmail.com
Никита Гончаров, студент ФКН, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: wdpgames@yandex.ru
Сергей Даценко, студент ФКН, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: sergdacenko@gmail.com
Елизавета Лазарева, студентка ФКН, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail:lazareva15elizaveta@gmail.com
Николай Полуяненко, к.т.н., доцент кафедры, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: nlfsr01@gmail.com

Расчет вероятности атаки разветвления блокчейн реестра.

Аннотация. В работе систематизированы сведения по тематике вопроса атаки разветвления блокчейн реестра. Предложен обзор и обобщение информации, представленной в наиболее авторитетных работах в данном направлении. Осуществлен анализ соответствующих работ по оценке вероятности двойной траты в протоколе консенсуса "Доказательства выполненной работы". Рассмотрена проблематика разорения игрока и проведена аналогия с атакой двойной траты на блокчейн. Рассмотрен эксперимент Пуассона для общего случая. Проанализированы модели, на основании которых, С. Накамото и М. Розенфельдом были предприняты попытки получить количественную оценку вероятности успешной атаки двойной траты на некоторые алгоритмы консенсуса, имеющие вероятностную завершенность. Приведены упрощения и допущения, имеющие место в соответствующих моделях, с помощью которых получено конечное выражение.

Ключевые слова: компьютерные сети; децентрализованные системы; блокчейн технологии; атака на блокчейн; атака разветвления; атака двойной траты; эксперимент Пуассона.

Reviewer: Volodymyr Khoma, Dr. of Sciences (Eng.), Full Prof., The Opole University of Technology, Opole, Poland.
E-mail: kalash@itesm.mx

Received: December 2019.

Authors:
Vladyslav Safonenko, CSD Student, V.N. Karazin Kharkiv National University, Ukraine. E-mail: vladyslavsafonenko@gmail.com
Nikita Goncharov, CSD Student, V.N. Karazin Kharkiv National University, Ukraine. E-mail: wdpgames@yandex.ru
Sergey Datsenko, CSD Student, V.N. Karazin Kharkiv National University, Ukraine. E-mail: sergdacenko@gmail.com
Elizaveta Lazareva, CSD Student, V.N. Karazin Kharkiv National University, Ukraine. E-mail: lazareva15elizaveta@gmail.com
Nikolay Poluyanenko, Ph.D., Associate Prof., V.N. Karazin Kharkiv National University, Ukraine. E-mail: nlfsr01@gmail.com

Alternative history attack success probability calculation in blockchain system.

Annotation. This article systemizes the information on the subject of the alternative history attack of the blockchain registry. The review and generalization of the information presented in the most respected works in this direction is offered. The analysis of corresponding works on estimation of probability of double spending in the "Proof of Work" consensus protocol is carried out. The problems of the player's ruin are considered and an analogy with the attack of double spending on the blockchain is made. Poisson's experiment for the general case is considered. The models on the basis of which S. Nakamoto and M. Rosenfeld made attempts to get a quantitative estimation of probability of successful double spending attack on some algorithms of consensus having probability completeness are analyzed. Simplifications and assumptions that take place in the respective models with the help of which the final expression is obtained are given.

Keywords: Computer networks; Decentralized systems; Blockchain technology; Alternative history attack; Double spending attack; Poisson's experiment.