УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.13**

Н.А. ПОЛУЯНЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук

ЙМОВІРНІСТЬ УСПІШНОЇ АТАКИ ПОДВІЙНОЇ ВИТРАТИ НА БЛОКЧЕЙН-СИСТЕМИ ІЗ ЙМОВІРНІСНИМ ПРОТОКОЛОМ КОНСЕНСУСУ

Вступ

Як правило, всі «класичні» платіжні системи є централізованими, що мають адміністративну ланку, яка забезпечує контроль легітимності будь-якої операції. При цьому, підстава для прийняття рішень про легітимність платежу є інформація, яка надається адміністратором, а не інформація, яка представлена платником. Тому платник в змозі лише сформувати заявку на повторну витрату одних і тих же засобів, а адміністративна ланка підтвердить тільки першу заявку і відкине всі інші, що блокує можливість подвійної витрати одних і тих же цінностей. У блокчейн-системах передбачається відсутність адміністративного ресурсу, і отже, можливість проведення подвійної витрати одних і тих же цінностей стає можливим.

Атака подвійного витрачання буває в багатьох формах. Кожен з можливих методів, що реалізує ту чи іншу форму, повинен перевірятися і оброблятися програмним забезпеченням повного вузла. Наведемо різні методи, які можуть бути застосовані для проведення повторної витрати одних і тих же коштів:

- одна транзакція в mempool, що витрачає один і той же вхідні значення (UTXO – Unspent Transaction (TX) Output) кілька разів;
- кілька транзакцій в mempool, які витрачають кошти, посилаючись на одні і ті ж вхідні значення (UTXO);
- транзакція в одному блоці, яка проводить одні і ті ж вхідні значення (UTXO) кілька разів;
- кілька транзакцій в різних блоках витрачають одні і ті ж вхідні значення (UTXO);
- проведення атаки за допомогою вдалого розгалуження блокчейн-реєстру, при цьому кожна з гілок містить різні транзакції, що змінюють діючий стан блокчейн-системи.

Вразливостям, що засновані на перших чотирьох наведених методах, можна вдало запобігти за допомогою відповідної реалізації програмного забезпечення. Однак все одно залишається можливість її реалізації, наприклад у [1, 2] наведено опис виявлених вразливостей у Bitcoin Core, а також детальний аналіз причини їх появи [3].

Щоб максимально унеможливити маніпулювання блокчейн-системою на свою користь однієї особи, процес майнинга Bitcoin розроблений як дорога і ресурсномістка операція. Для формування нового блоку з транзакціями в блокчейн-систему майнери повинні надати дійсні докази виконаної роботи. Але не зважаючи на це, у зловмисника, який намагається виконати п'ятий спосіб, так само є не менш чотирьох варіантів його проведення (більш детально дивиться у [4]) серед яких є атака 51 %.

Сутність атаки 51 % полягає у наступному: зловмисник генерує платіжну транзакцію і випускає її в мережу; продавець очікує отримання відповідної кількості підтверджень, перш ніж прийняти платіж і здійснити операцію. Одночасно зловмисник таємно починає формувати блок, що містить шахрайську транзакцію, за якою слідують додаткові блоки для її підтвердження. Оскільки обчислювальна потужність атакуючого більше, ніж решта обчислювальної потужності всіх майнерів разом узятих, атакуючий може добувати блоки за менший час. Як тільки продавець приймає транзакцію, зловмисник розповсюджує таємно здобуті блоки, щоб створити розгалуження в блокчейн-реєстрі. Якщо шахрайське розгалуження, створене атакуючим, містить більшу кількість блоків, ніж початковий ланцюг, воно стає домінуючим, і всі майнери приймають дане розгалуження за основне і починають його поширювати, а також включати в ланцюжок блоків при формуванні наступних блоків. Таким чином, первісна платіжна транзакція більше не існує в блокчейн-реєстрі.

Ця атака є найбільшою загрозою для блокчейн-систем з консенсусами, які мають ймовірнісний характер завершеності, оскільки вона безпосередньо пов'язана з ресурсами, які може використовувати зловмисник. Ресурси виміряються з точки зору фінансової та обчислювальної потужності. Важливо відзначити, що навіть при обчислювальній потужності менше 50 % зловмисник все ще може маніпулювати системою.

Для захисту від атаки 51 % продавці можуть приймати різні заходи захисту, найбільш ефективним з них є очікування включення транзакції з оплатою в один з блоків блокчейн-реєстру. При цьому вузол, який формує блок, не допустить включення в блок транзакцій, які намагаються повторно витратити раніш витрачені кошти. І якщо навіть такий блок буде сформовано вузлом зловмисника, його відкинуть вузли чесної мережі і блок не буде додано до блокчейн-реєстру чесних користувачів.

Процес включення транзакції до складу нового блоку називається підтвердженням транзакції. Включення в один блок відповідає одному підтвердженню. Формування і додавання до реєстру блокчейн-ланцюжка ще з $(N-1)$ блоків, які посилаються на блок з транзакцією, відповідає N підтвердженням. Однак, якщо використовується алгоритм консенсусу Доказ виконаної роботи та зловмисник має досить великі ресурси (володіє високопродуктивним обладнанням, здатним забезпечити високий гешрейт (англ. – hashrate) зловмисника) у нього все ще залишається досить висока ймовірність успішно провести подвійну витрату шляхом формування альтернативного ланцюжка блокчейн реєстру.

Успіх атаки подвійних витрат безпосередньо залежить від ресурсів (гешрейта) атакуючого і кількості підтверджень. Ймовірність формування альтернативного ланцюжка експоненціально зменшується зі зростанням кількості підтверджень і зменшенням гешрейта атакуючого. Чим більше підтверджень має транзакція, тим менш імовірне скасування транзакції через заміну діючого ланцюжка альтернативним, що сформовано зловмисником. Однак, з іншого боку, чим більше продавець чекає підтверджень, тим довше затримується проведення самої угоди, що внаслідок веде до значних затримок, дискомфорту використання системи та збиткам взаємодіючих сторін.

Тому угоди з нульовим підтвердженням потенційно мають великий ризик стати жертвою атаки подвійних витрат, а угоди, які очікують велику кількість підтверджень, – зазнати збитків через затримки в їх укладанні. Тому, знаходження оптимальної кількості підтверджень, при яких ризик атаки подвійної витрати буде нижче деякого прийнятного рівня, а час очікування буде мінімально необхідним, є актуальним завданням.

Наприклад, існує думка [5 – 8], якщо використовується механізм консенсусу на основі Доказу виконаної роботи на основі геш-функції і у атакуючого знаходиться 10 % обчислювальної потужності (гешрейт) від загальної мережі і очікується шість підтверджень, – ймовірність успіху такої атаки складе 0,1 %. Наведена оцінка ґрунтується на моделі «розорення гравця» (см. [9]), яка не використовує незалежні події для чесної мережі і зловмисника та багато інших припущень.

Сукупність цих припущень та обмежень дає значну похибку між експериментальними моделюваннями методами Монте-Карло та відповідно ймовірностями проведення успішних атак на блокчейн-системи, які використовують механізм консенсусу на основі Доказу виконаної роботи [10]. Ця стаття є логічним продовженням роботи в цьому напрямку та дає аналітичний вираз ймовірності успішного розгалуження ланцюжка блоків при використанні алгоритму консенсусу Доказ виконаної роботи.

Моделі, що застосовується при оцінки вдалої реалізації атаки 51 %

Оцінку ймовірності вдалої реалізації атаки 51 % дано ще в роботі Сатоши Накамото [11], а також більш точні результати отримано Мені Розенфельдом [5], які на сьогоднішній день є одними з найпопулярніших і цитованих робіт в даній сфері. Існують також інші роботи, які уточнюють і доповнюють результати отримані Сатоши Накамото і Мені Розенфельдом, більш детально про це було описано в [10].

Згадані роботи формують свої виводи на підставі моделі «розорення гравця». На основі даної моделі отримується формула для розрахунку ймовірності успішного проведення атаки. В основу цієї моделі покладено факт, що у кожному випробуванні або виграє зловмисник (формуючи черговий блок), або зловмисник програє і при цьому вважається, що виграє чесна мережа (формуючи черговий блок). Однак в роботах не наводиться будь-якого обґрунтування обраної моделі. Автори припускають, що якщо блок не сформував зловмисник, то в такому випадку блок обов'язково формує чесна мережа, при цьому це припущення ніяк не обґрунтовується.

Ми пропонуємо використовувати модель «незалежних гравців». У даній моделі, на відміну від моделі «розорення гравця», формування чергового блоку у зловмисника і чесної мережі відбувається повністю незалежно один від одного. Нехай ймовірність сформувати блок зловмисником буде q, а чесною мережею – p, відмовившись від обов'язкового для моделі «розорення гравця» виконання умови $p=1-q$, ми отримаємо в результаті кожної спроби (або серії спроб протягом заданого інтервалу часу) простір елементарних подій, що містить наступні події:

- елементарна подія «блок сформований чесною мережею і атакуючий не сформував блок» з ймовірністю $p\cdot(1-q)$;
- елементарна подія «блок не сформований чесною мережею і атакуючий сформував блок» з ймовірністю $(1-p)\cdot q$;
- елементарна подія «блок не сформований чесною мережею і атакує не сформував блок» з ймовірністю $(1-p)\cdot(1-q)$;
- елементарна подія «блок сформований чесною мережею і атакуючий сформував блок» $p\cdot q$.

Безліч всіх елементарних подій становить повну групу подій:

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

Ця модель з чотирма елементарними подіями описує реальний ймовірнісний процес в блокчейн-системі при встановленні консенсусу на основі алгоритму «Proof of work».

З метою можливості порівняння з результатами, отриманими у роботах Сатоши Накамото і Мені Розенфельда, також будемо використовувати деякі спрощення:

- час поширення блоку у мережі дуже малий, тобто обмін інформацією між вузлами відбувається практично миттєво (час синхронізації дорівнює нулю);
- гешрейт зловмисника, гешрейт чесної мережі і складність майнінгу не змінюється з часом протягом всієї гонки;
- можливості зловмисника з підтримки стану гонки досить великі, але не безмежні;
- крім зловмисника всі інші користувачі мережі діють строго відповідно до правил протоколу блокчейн-мережі;
- перемогою зловмисника будемо вважати формування необхідної кількості блоків підтвердження раніше або одночасно (вважається, що один блок зловмисник сформував заздалегідь) або, в іншому випадку, – подальшого формування ланцюжка блоків рівною з чесною мережею довжини.

Зауважимо, що в умовах блокчейн-систем ймовірність p для кожного окремого суб'єкта не залежить від номера випробувань і від інших суб'єктів і визначається виключно потужністю, яку він має (справедливо для алгоритмів консенсусу Доказу виконаної роботи та його аналогів). Ймовірність p можна прив'язати до гешрейту (кількості протестованих геш-функцій в секунду), але в загальному випадку покладемо значення p – ймовірність сформувати блок за деяку умовну одиницю часу.

Зловмисник може перемогти в момент початку гонки. При цьому йому необхідно сформувати N або більше блоків до того моменту, коли чесна мережа сформує N блоків. Якщо йому це не вдасться, то у нього все ще є можливість наздогнати чесну мережу на

$N + j$ блоці, де j – кількість блоків сформованих чесною мережею на додаток до необхідних N блоків.

Отримаємо вираз, який характеризує ймовірність формування блоків в залежності від N, j і кількості невдалих спроб сформувати блок чесною мережею (k).

Ймовірність перемоги зловмисника

Ґрунтуючись на наведеній групі подій, отримаємо наступні можливі ймовірності і комбінації в яких зловмисник здобуває перемогу (для $N=1, j=0$):

1. При першій спробі (в даному випадку при $t = N + j + k = 1 + 0 + 0 = 1$). Комбінація може бути тільки одна – коли і чесна мережа, і зловмисник одночасно знаходять блоки. У цьому випадку ймовірність перемоги зловмисника буде визначатися як $PI_{N=1,\,j=0,k=0} = p \cdot q$;

2. При другій спробі ($t = N + 1 = 2$). При цьому, може бути дві різні ситуації

- чесна мережа знаходить блок при першому випробуванні, але не знаходить при другому (ймовірність чого дорівнює $p \cdot (1-p)$). У даному випадку, якщо зловмисник знайде блок при першому випробуванні, ми прийдемо до п.1, отже, він може знайти блок тільки за друге випробування (ймовірність $(1-q)\cdot q$);

- чесна мережа не знаходить блок при першому випробуванні, а знаходить тільки при другому (ймовірність чого дорівнює $(1-p)\cdot p$). При цьому зловмисник може знайти блок при першому випробуванні (з ймовірністю $q\cdot(1-q)$) або при другому випробуванні (з ймовірністю $(1-q)\cdot q$), і при обох випробуваннях (з ймовірністю $q \cdot q$).

Загальна ймовірність даної події:

$$PI_{N=1,\,j=0,k=1} = \left[p\cdot(1-p)\cdot(1-q)\cdot q \right] +$$
$$+\left[(1-p)\cdot p\cdot q\cdot(1-q) + (1-p)\cdot p\cdot(1-q)\cdot q + (1-p)\cdot p\cdot q\cdot q \right] =$$
$$= p\cdot(1-p)\cdot\left[(1-q)\cdot q \right] + (1-p)\cdot p\cdot\left[q\cdot(1-q) + (1-q)\cdot q + q\cdot q \right];$$

3. При третій спробі ($t = N + 2 = 3$). Тут також можна розглянути три ситуації: чесна мережа формує блок на першому, на другому або на третьому випробуванні і при цьому існують різні комбінації, коли може бути сформований блок (або блоки) зловмисником. Сумарна ймовірність настання подій буде обчислюватися аналогічно вищеописаним подіям, підсумкова ймовірність яких буде:

$$\begin{aligned} PI_{N=1,\,j=0,k=2} &= p\cdot(1-p)\cdot(1-p)\cdot\left[(1-q)\cdot(1-q)\cdot q \right] + \\ &+ (1-p)\cdot p\cdot(1-p)\cdot\left[(1-q)\cdot(1-q)\cdot q \right] + \\ &+ (1-p)\cdot(1-p)\cdot p\cdot\left[q\cdot(1-q)\cdot(1-q) + (1-q)\cdot q\cdot(1-q) + \right. \\ &+ (1-q)\cdot(1-q)\cdot q + q\cdot q\cdot(1-q) + q\cdot(1-q)\cdot q + (1-q)\cdot q\cdot q + \\ &\left. + q\cdot q\cdot q \right] = \\ &= p^1\cdot(1-p)^2\left[q^1\cdot(1-q)^2 \right] + p^1\cdot(1-p)^2\left[q^1\cdot(1-q)^2 \right] + \\ &+ p^1\cdot(1-p)^2\left[3\cdot q^1\cdot(1-q)^2 + 3\cdot q^2\cdot(1-q)^1 + q^3 \right] \end{aligned}$$

4. При t-й спробі ($t = N + k$). Ймовірність перемоги зловмисника буде визначатися:

$$PI_{N=1,\,j=0,k=k} = k \cdot p^1 \cdot (1-p)^k \cdot \left[q^1 \cdot (1-q)^k \right] + \\ + p^1 \cdot (1-p)^k \cdot \left[(k+1) \cdot q^1 \cdot (1-q)^k + \binom{k+1}{2} \cdot q^2 \cdot (1-q)^{k-1} + \right. \\ \left. + \binom{k+1}{3} \cdot q^3 \cdot (1-q)^{k-2} + \ldots + (k+1) \cdot q^k \cdot (1-q)^1 + q^{(k+1)} \right]$$

При цьому, розкладаючи вираз $(a+b)^n$ в степеневий ряд, отримуємо співвідношення з біноміальними коефіцієнтами:

$$(a+b)^n = a^n + n \cdot a^1 \cdot b^{(n-1)} + \binom{n}{2} \cdot a^2 \cdot b^{n-2} + \binom{n}{3} \cdot a^3 \cdot b^{n-3} + \ldots + n \cdot a^1 \cdot b^{n-1} + 1 \cdot a^n,$$

припускаючи $a = q$, $b = (1-q)$, а $n = k+1$, отримуємо вираз у других квадратних дужках з точністю до першого доданка, тобто:

$$((1-q)+q)^{k+1} = (1-q)^{k+1} + (k+1) \cdot (1-q)^k \cdot q^1 + \binom{k+1}{2} \cdot (1-q)^{k-1} \cdot q^2 + \\ + \binom{k+1}{3} \cdot (1-q)^{k-2} \cdot q^3 + \ldots + (k+1) \cdot (1-q)^1 \cdot q^k + q^{(k+1)}$$

Разом з тим $((1-q)+q)^{k+1} = 1^{k+1} = 1$. Таким чином, можна спростити вираз:

$$PI_{N=1,\,j=0,k=k} = k \cdot p^1 \cdot (1-p)^k \cdot \left[q^1 \cdot (1-q)^k \right] + p^1 \cdot (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right].$$

Підсумовуючи $k = 0, 1, 2, \ldots$, знайдемо ймовірність успішного проведення зловмисником атаки подвійної витрати за умови, що чесною мережею сформоване не більше $N = 1$ блоків:

$$PI_{N=1,\,j=0} = \sum_{k=0}^{\infty} \left\{ k \cdot p \cdot (1-p)^k \cdot \left[q \cdot (1-q)^k \right] + p \cdot (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right] \right\} = \\ = p \cdot q \cdot \sum_{k=0}^{\infty} \left\{ k \cdot (1-p)^k \cdot \left[(1-q)^k \right] \right\} + p \cdot \sum_{k=0}^{\infty} \left\{ (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right] \right\}$$

Проводячи аналогічні міркування і далі отримуємо ймовірність виграшу зловмисника у чесній мережі (PI):

$$PI = p^N \cdot \sum_{k=0}^{\infty} \left((1-p)^k \cdot \binom{t-1}{N-1} \cdot \left[\binom{t-1}{N} \cdot q^N \cdot (1-q)^k + \left\{ 1 - \sum_{i=0}^{N-1} \binom{t}{i} \cdot q^i \cdot (1-q)^{t-i} \right\} \right] \right) + \\ + \sum_{j=1}^{\infty} \left[p^{(N+j)} \cdot q^{(N+j)} \cdot \sum_{k=1}^{\infty} \left(sum_p \cdot (1-p)^k \cdot (1-q)^k \right) \right], \qquad (1)$$

де

$t = N + j + k$;

$$sum_p = \sum_{ip_{(N+j)}=1}^{k} \left(\sum_{ip_{(N+j-1)}=ip_{(N+j)}+1}^{k+1} \left(\ldots \sum_{ip_2=ip_3+1}^{N+j+k-2} \left(\sum_{ip_1=ip_2+1}^{N+j+k-1} \left(sum_q \right) \right) \right) \right);$$

$$sum_q = \sum_{iq_{(N+j)}=1}^{k+1} \left(\sum_{iq_{(N+j-1)}=iq_{(N+j)}+1}^{k+2} \left(\ldots \sum_{iq_{(N+1)}=iq_{(N+2)}+1}^{k+N-1} \left(\sum_{iq_N=\max(iq_{(N+1)}+1,\,ip_{(N-1)})}^{k+N} \left(\ldots \sum_{iq_3=\max(iq_4+1,\,ip_2)}^{N+j+k-2} \left(\sum_{iq_2=\max(iq_3+1,\,ip_1)}^{N+j+k-1} (1) \right) \right) \right) \right) \right).$$

Звертаємо увагу, якщо $N=1$, то зовнішнє підсумовування для sum_q починається с $iq_{(N+j)}=ip_{(N+j-1)}$, а якщо і $j=0$, то в цьому випадку $sum_q=1$.

Порівняння результатів з моделлю розорення гравця. Рекомендації щодо «безпечного» числа підтверджень

На основі отриманих виразів покажемо, яка необхідна кількість підтверджень для збереження ймовірності успіху зловмисника нижче заданого «безпечного» значення, при різних значеннях гешрейта. Під «безпечним» значенням будемо розуміти таке значення P_S, при якому верхня межа ймовірності проведення атаки подвійної витрати може вважатися прийнятним ризиком.

Конкретне «безпечне» значення ймовірності проведення атаки подвійної витрати кожен користувач визначає для себе сам в залежності від прийнятних для нього ризиків (величини угоди, ризиків репутації, необхідної оперативності проведення операції тощо). Нами розглянуто значення $P_S=0{,}1;0{,}01;0{,}001$ і проведено порівняння отриманих результатів з результатами, отриманими на підставі моделі розорення гравця, які детально досліджені в роботі Мені Розенфельда [5].

На рис. 1 – 3 наведено мінімальну кількість підтверджень, необхідну для підтримки ймовірності успішного проведення атаки подвійної витрати, в залежності від гешрейта атакуючого, що дорівнює або нижче значення P_S. Гешрейт чесної мережі як і раніше будемо вважати $p=1-q$.

При порівнянні отриманих результатів з результатами, розрахованими відповідно до моделі розорення гравця, що наведені в роботі Мені Розенфельда [5.], бачимо, що ймовірність успішного проведення атаки подвійної витрати нижче, ніж вважалося до цього. У зв'язку з чим можливо обмежитись меншою кількістю необхідних підтверджень в блокчейн-системі при тому ж рівні безпеки. Це на практиці дозволить значно знизити час очікування для укладання угоди і, як наслідок, значно підвищити швидкість проведення операцій з блокчейн-системами.

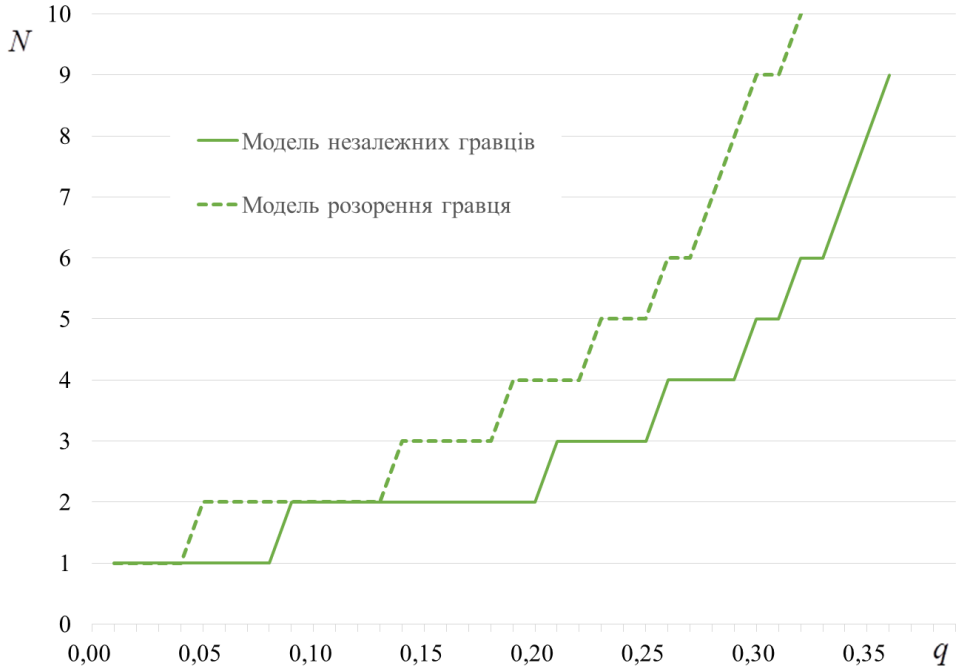

Рис. 1. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S=0{,}1$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця

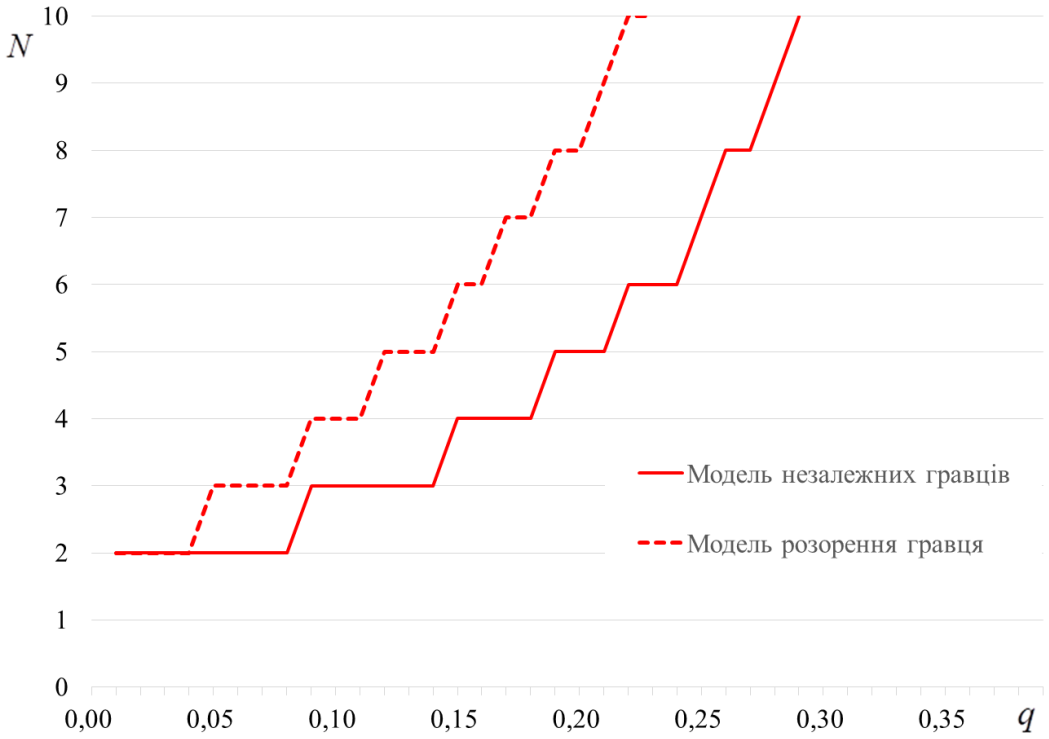

Рис. 2. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S = 0,01$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця.

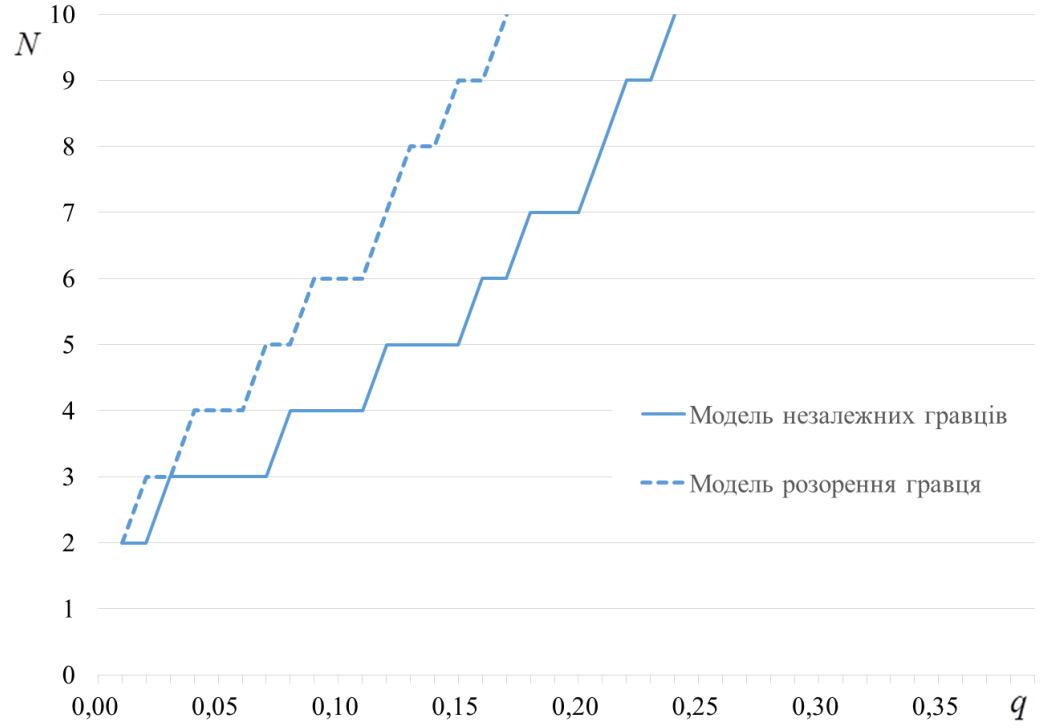

Рис. 3. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S = 0,001$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця

Так, якщо передбачається, що в розпорядженні зловмисника є 15 % від загальної потужності мережі, то необхідно два підтвердження, щоб зберегти ймовірність успіху зловмисника не вище 10 %, в той час, як для моделі розорення гравця необхідно очікувати три підтвердження. Якщо необхідна ймовірність успіху зловмисника не вище 1 % (при тих же умовах), необхідно очікувати чотири підтвердження, а для моделі розорення гравця – шість підтверджень. Якщо бажаємо забезпечити ймовірність успіху зловмисника не вище 0,1 %, необхідно очікувати п'ять підтверджень, а для моделі розорення гравця – дев'ять.

Таким чином, для вибраного прикладу необхідний середньостатистичний час, який витрачається на очікування підтвердження угод можна скоротити на $1/3$ (33 %) для $P_S = 10\%$; на $2/6$ (33 %) для $P_S = 1\%$ і на $4/9$ (44 %) для $P_S = 0{,}1\%$. В інших випадках з наведених результатів середньостатистичний час очікування може скоротитися і до двох разів (наприклад, при $P_S = 0{,}1$ и $q = 0{,}5 - 0{,}8; 0{,}19 - 2{,}0; 0{,}29$).

Висновки

На підставі моделі незалежних гравців отримано аналітичний вираз розрахунку ймовірності успішного проведення зловмисником атаки подвійної витрати на блокчейн-системи, що використовують алгоритм консенсусу Доказ виконаної роботи на основі геш-функції. Вираз отримано для випадку, коли передбачається, що зловмисник попередньо сформував один блок (для порівняння з раніш незалежно отриманими результатами). Отриманий вираз (1) характеризує ймовірність зловмисником провести успішну атаку подвійної витрати на блокчейн-систему у залежності від використовуваної кількості підтверджень, а також гешрейта чесною мережею і зловмисником. Наведено кількісні значення даної ймовірності.

На основі отриманих результатів наведено рекомендації щодо визначення «безпечної» кількості підтверджень для успішного протистояння атаки подвійної витрати на блокчейн-систему. Проведено порівняння з результатами, отриманими Мені Розенфельдом (які використовують модель розорення гравця). Показано, що можливо обмежитись меншою кількістю необхідних підтверджень в блокчейн-системі при тому ж рівні безпеки. Отримані результати на практиці дозволять значно (до двох разів) знизити час очікування для укладання угоди і, як наслідок, значно підвищити швидкість проведення операцій з блокчейн-системами при збереженні заданого рівня безпеки.

Список літератури:

1. Hackernoon: Two Ways to Double-Spend https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362.
2. BitcoinCore: CVE-2018-17144 Full Disclosure https://bitcoincore.org/en/2018/09/20/notice/.
3. Hackernoon: Two Ways to Double-Spend https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362.
4. Zaghloul, E., Li, T., Mutka, M.W., & Ren, J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435.
5. Rosenfeld M. Analysis of hashrate-based double-spending / Meni Rosenfeld, 2014. 13 c.
6. Gervais A., Ritzdorf H., Karame G. O., & Čapkun S. (2015). Tampering with the delivery of blocks and transactions in Bitcoin. In CCS 2015 – Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (Vol. 2015-October, pp. 692-705). Association for Computing Machinery. https://doi.org/10.1145/2810103.2813655.
7. Zaghloul E., Li T., Mutka M.W., & Ren J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435.

8. BitcoinWiki: Double-spending https://ru.bitcoinwiki.org/wiki/Double-spending
9. Ширяев А. Н. Вероятность : в 2-х кн. ; 4-е изд., перераб. и доп. Москва : МЦНМО, 2007.
10. Полуяненко Н.А., Кузнецов А.А. Моделирование атаки двойной траты на протокол консенсуса «proof of work» // Радиотехника. 2019. № 198. С. 146–161. DOI: 10.30837/rt.2019.3.198.11
11. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto, 2009. 9 с.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 07.02.2020