УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, e-mail: *lusi.kovalchuk@gmail.com*.

Н.В. КУЧИНСЬКА
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, e-mail: *n.kuchinska@gmail.com*.

М.С. КОНДРАТЕНКО
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, e-mail: *nikolay.ns95@gmail.com*.

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-of-PROOF ЗА РІЗНИХ ТИПІВ КОНСЕНСУСУ У МЕЙНЧЕЙНІ/САЙДЧЕЙНІ ДЛЯ ЗАПОБІГАННЯ АТАЦІ ПОДВІЙНОЇ ВИТРАТИ. I. PoS У МЕЙНЧЕЙНІ ТА PoW У САЙДЧЕЙНІ

Анотація. Розглянуто питання безпечного функціонування дворівневого блокчейну зі складним змішаним протоколом консенсусу Proof-of-Stake в основному блокчейні (мейнчейні) та протоколом Proof-of-Work у другорядному блокчейні (сайдчейні). Дворівневий блокчейн побудовано за принципом протоколу Proof-of-Proof, коли стійкість сайдчейну забезпечена стійкістю мейнчейну через посилання блоків мейнчейну на блоки сайдчейну з використанням спеціальних транзакцій. Ця структура дає змогу швидше створювати блоки у сайдчейні і відповідно швидше обробляти транзакції, не знижуючи стійкості та не збільшуючи обсягу блоку. Такий дворівневий блокчейн є найбільш зручним для створення каскадної системи державних реєстрів, гарантовано захищаючи від підміни та підробки документів. Основний результат роботи — отримання явних аналітичних виразів для оцінки ймовірності атаки подвійної витрати, направленої на сайдчейн у дворівневому блокчейні за умови наявності зловмисника як у сайдчейні, так і у мейнчейні.

Ключові слова: блокчейн, мейнчейн, сайдчейн, криптовалюти, майнінг, протокол консенсусу Proof-of-Proof, атака подвійної витрати.

ВСТУП

Поняття протоколу консенсусу в блокчейні з'явилось у роботі [1], де Сатоші Накамото вперше ввів означення блокчейну. У цій роботі розглянуто лише протокол консенсусу Proof-of-Work (PoW) [2] і при цьому взагалі не визначено можливості використання інших протоколів консенсусу. Цей протокол і наразі залишається найбільш поширеним, однак його численні недоліки спонукали дослідників іншим шляхом досягати консенсусів. Детальніші огляди основних сучасних протоколів консенсусу можна знайти в роботах [3–7].

Протокол консенсусу є базовим для коректного функціонування блокчейну, його властивості визначають стійкість блокчейну до атак [8]. Тому багато наукових робіт, дотичних до теми блокчейну, присвячено саме порівняльному аналізу протоколів консенсусу та, насамперед аналізу їхньої стійкості до основних типів атак [8, 9]. Зазначимо, що в усіх наведених вище роботах аналізували класичний однорівневий блокчейн, для якого на цей час отримано багато результатів.

Ця робота суттєво відрізняється від зазначених вище, оскільки досліджує проблему безпечного функціонування дворівневого блокчейну [10] зі складним

змішаним протоколом консенсусу Proof-of-Stake (PoS) [11] в основному блокчейні (тут і далі мейнчейн) та Proof-of-Work у другорядному блокчейні (тут і далі сайдчейн). Такий дворівневий блокчейн побудовано за принципом протоколу Proof-of-Proof [12], коли стійкість сайдчейну забезпечується стійкістю мейнчейну через посилання блоків мейнчейну на блоки сайдчейну з використанням спеціальних транзакцій. Ця структура дає змогу швидше створювати блоки у сайдчейні і відповідно швидше обробляти транзакції, не знижуючи стійкості блокчейну до різних типів атак та не збільшуючи обсягу блоку.

Такі дворівневі (каскадні) блокчейни можна використовувати, наприклад, для побудови каскадних державних реєстрів. Детальніше спосіб побудови каскадних реєстрів, а також переваги такого способу ведення реєстрів описано в роботі [13].

Зазначимо, що ця стаття є третьою серед серії робіт, в яких здійснюється оцінювання стійкості протоколу Proof-of-Proof до атаки подвійної витрати та за явними формули обчислено ймовірність такої атаки. Отримані формули також уможливлюють обчислення найменшої потрібної кількості блоків підтвердження (у сайдчейні), за якої імовірність атаки подвійної витрати буде меншою за задану величину ε (наприклад, як референтне значення зазвичай вибирають $\varepsilon = 0.001$). У працях, в яких було отримано аналогічні результати, розглянуто випадки однакових типів консенсусу в мейнчейні та в сайдчейні:

— протоколи консенсусу Proof-of-Work (з урахуванням часу синхронізації) в обох блокчейнах [14];

— протокол консенсусу Proof-of-Stake в обох блокчейнах [15].

Зазначимо, що зазвичай час синхронізації є важливим параметром блокчейну, але в нашій моделі ми можемо нехтувати цим параметром. Вибір математичної моделі обґрунтовано такими аргументами:

1) вважатимемо, що час до створення блоку (тобто довжина таймслоту) у мейнчейні є суттєво більшим за час синхронізації, до того ж чесні слотлідери створюють блок на початку свого таймслоту;

2) збільшення часу синхронізації у сайдчейні лише збільшить стійкість сайдчейну до атаки подвійної витрати, оскільки тоді час створення певної кількості блоків буде більшим, ніж очікуваний і відповідно за цей час у мейнчейні буде створено більшу кількість блоків.

1. ПОЗНАЧЕННЯ ТА ДОПОМІЖНІ ТВЕРДЖЕННЯ

Насамперед наведемо формалізований опис моделі, в якій проведемо дослідження, сформулюємо задачу досліджень, а також уведемо основні позначення. Далі сформулюємо та доведемо основні твердження, потрібні для розв'язання поставленої задачі.

Формалізація моделі дослідження та її основних властивостей. Розглядувану модель визначимо так.

У мейнчейні, який забезпечує стійкість до атак (зокрема, до атаки подвійної витрати), використовується протокол консенсусу Proof-of-Stake (як основний блокчейн вибрано мережу Ethereum). Це означає, що процес створення блоків поділяється на епохи, кожна з яких складається з певної кількості відрізків часу — так званих таймслотів (для протоколу PoS таймслоти можуть тривати від кількох секунд до кількох хвилин).

Позначимо N кількість блоків у одній епосі, а τ — тривалість одного таймслоту. Тоді час, відведений на одну епоху, дорівнюватиме $N \cdot \tau$. Для спрощення моделі (не зменшуючи загальності) будемо вважати, що в кожному таймслоті є тільки один слотлідер — учасник мережі, який у цьому таймслоті відповідає за випуск блоку. При цьому у кожному таймслоті слотлідер вибирається випадково згідно з певною процедурою вибору незалежно від інших таймслотів серед великої кількості так званих стейкхолдерів. Стейкхолдер — це учасник блокчейну, який має певний достатньо великий (інколи від кількох десятків тисяч у доларовому еквіваленті) капітал у визначеному криптоактиві (наприклад, що функціонує у цій мережі). Для того щоб долучитись до створення блоків, тобто отримати можливість стати слотлідером, учасник повинен покласти певну кількість свого капіталу на депозит — створити стейк. Стейк (депозит) потрібен для страхування на випадок порушення правил функціонування мережі. У разі доведеного порушення правил функціонування мережі учасник може бути оштрафований на певну суму, значення якої навіть може збігатися з його депозитом. Поки учасник має ненульовий депозит і при цьому не заявляв про його відкликання, він з ненульовою ймовірністю може стати слотлідером. У разі подання заяви на відкликання він вже не може стати слотлідером. З моменту подання заяви на відкликання до отримання свого капіталу має минути декілька епох, щоб стейкхолдер не мав можливості забрати свій депозит одразу після порушення правил.

За кожен створений блок слотлідер отримує значну винагороду. Наприклад, в мережі Ethereum нагорода за створення блоку складає 5 ETH, що приблизно дорівнює 16000 дол. США. Тому стейкхолдер має подвійну зацікавленість у коректному функціонуванні мережі — і стосовно винагороди за створення блоку, і стосовно підвищення курсу криптоактиву, що збільшить доларовий еквівалент його депозиту. Крім того, слотлідер отримує оплату (відсоток від суми транзакції) за кожну транзакцію, яку він додає у свій блок. Така система винагород і штрафів мотивує коректне функціонування мережі.

Проте за різних обставин у мережі можуть з'явитись зловмисники, які порушують правила функціонування блокчейну з метою отримання неправомірної вигоди. Таким інструментом отримання неправомірної вигоди може бути так звана атака подвійної витрати [1].

Процедура вибору слотлідера зазвичай базується на перевірних випадкових функціях (verifiable random functions) [16] і детально описана в [17].

Позначимо $S_1, \dots, S_n$ множину всіх (активних) стейкхолдерів мережі, а $\alpha_1, \dots, \alpha_n$ — величини їхніх депозитів. Тоді частку депозиту i-го слотлідера можна визначити як $p_i = \dfrac{\alpha_i}{\alpha}$, де $\alpha = \sum_{j=1}^{n} \alpha_j$. У цих позначеннях ключову властивість створення блоків (властивість процедури вибору слотлідерів) у дещо спрощеному вигляді для основного блокчейну сформулюємо так. ймовірність стейкхолдера S_i стати слотлідером у будь-якому окремому таймслоті дорівнює p_i.

Перейдемо до опису сайдчейну, тобто блокчейну, який успадковує стійкість. Вважатимемо, що в цій мережі використовують протокол консенсусу Proof-of-Work. У цьому разі взагалі немає ні таймслотів, ні епох, а наступний блок створить той майнер, якому пощастить швидше за інших підібрати таку величину *nonce*, що значення геш-функції від створюваного блоку буде меншим, ніж деяка цільова величина. Потенційно майнером (або створювачем блоку) у цій мережі може бути кожен, хто володіє певними обчислювальними потужностями.

Позначимо $P_1, \ldots, P_m$ множину всіх майнерів сайдчейну, а величини їхніх обчислювальних потужностей позначимо $\beta_1, \ldots, \beta_m$, де β_i — кількість гешувань, які *i*-й майнер може виконувати за фіксовану одиницю часу. Тоді частка обчислювальних потужностей *i*-го майнера дорівнює $q_i = \beta_i / \beta$, де $\beta = \sum_{i=1}^{n} \beta_i$. У цих позначеннях за аналогією до властивості основного блокчейну можемо сформулювати властивість процедури створення блоків для сайдчейну.

Властивість сайдчейну: якщо час синхронізації мережі $\Delta = 0$, то ймовірність того, що наступний блок буде створено майнером P_i, дорівнює q_i.

Зазначимо, що для протоколу консенсусу PoW ця властивість не випливає автоматично із означення протоколу, і вперше це було доведено (для блокчейну з нульовим часом синхронізації) у роботі [18]. Для більш складних випадків аналог цієї властивості було доведено у роботах [19, 20]. Далі для отримання результатів використовуватимемо результати робіт [18, 21].

Оскільки основною темою дослідження є стійкість блокчейну до атаки подвійної витрати, опишемо алгоритм, за яким ця атака відбувається. Зазначимо, що наведений далі опис атаки стосується найпростішого випадку — однорівневого блокчейну. Розглянутий у цій статті випадок стосується дворівневого блокчейну. Описана далі атака може відбуватись на обидва рівні — на основний блокчейн, який забезпечує стійкість, та на сайдчейн, який цю стійкість успадковує від основного.

Атаку подвійної витрати для різних моделей досліджено у багатьох публікаціях [1, 16 , 18–21], у популярних статтях та блогах, а також у різних навчальних програмах. (Наприклад, у навчальному курсі Принстонського університету під назвою «Bitcoin and Cryptocurrency»; в англомовних джерелах під назвою «Double Spending Attack» (атака подвійної витрати). Сутність атаки полягає в тому, що зловмисник намагається двічі скористатись однією своєю монетою, виконавши нею два платежі.

Це відбувається так. Зловмисник створює транзакцію, в якій переводить якусь свою монету вендору (постачальнику) як оплату за постачання товарів чи послуг та викладає цю транзакцію в майнінговий пул. Майнери включають цю транзакцію у визначений блок блокчейну, наприклад блок з номером 5. Одночасно з цим зловмисник формує іншу транзакцію, в якій цією ж самою монетою виконує платіж на іншу адресу (наприклад, на свою). Цю транзакцію він не викладає в майнінговий пул, а включає її в блок альтернативної гілки блокчейну. Цю альтернативну гілку він генерує сам, не розсилаючи створені в ній блоки іншим майнерам — інакше постачальник виявить, що зловмисник намагається виконати атаку. Після отримання своєї оплати постачальник надсилає відповідний товар. У цей час зловмисник намагається створити якомога більше блоків на альтернативній гілці. Якщо після надсилання товару йому вдається створити альтернативну гілку, довшу за «справжню», то він її надсилає до мережі. Тоді за основним правилом блокчейна — правилом довшої гілки всі майнери мають переключитись на його гілку, а блоки з іншої гілки і всі транзакції, які в них були, вважаються недійсними. Очевидно, що чим більшою є частка ресурсу зловмисника (обчислювальних потужностей для протоколу PoW або депозиту для протоколу PoS), тим він має більше шансів виконати цю атаку. Зокрема, якщо в зловмисника є не менше, ніж половина ресурсів, то ймовірність такої атаки (на нескінченному проміжку часу) дорівнює одиниці.

Для захисту від такої атаки С. Накамото в [1] запропонував не постачати товар відразу після включення транзакції в блок, а зачекати створення певної кількості нових блоків — блоків підтвердження і лише потім постачати товар. У цьому випадку зловмисник не може створити альтернативної гілки відразу після оплати, тому що її побачить постачальник і товар не надішле. Тому зловмисник може створювати цю альтернативну гілку лише своїми ресурсами.

Перший етап атаки відбувається до того моменту, коли постачальник, дочекавшись певної кількості блоків підтвердження, доставляє товар. Якщо на цьому етапі зловмиснику вдається створити довшу гілку, він відразу надсилає її до мережі і, таким чином, постачальник залишається без оплати. Якщо на цьому етапі зловмисник не зміг створити довшої гілки, то він продовжує її нарощувати (не генеруючи блоків для «правильної» гілки), сподіваючись, що з часом йому пощастить наздогнати іншу гілку. Якщо це станеться, він відразу викладе свою альтернативну гілку, і за правилами майнінгу її вважатимуть справжньою. Це другий етап атаки, який може бути нескінченно довгим.

Зазначимо, що ймовірність атаки спадає експоненційно із зростанням кількості блоків підтвердження [14, 18–21]. У роботі [1] С. Накамото також навів вирази для обчислення ймовірності атаки подвійної витрати, але, як було показано в [18, 19], в обчисленні було допущено багато суттєвих помилок (з детальнішим поясненням з цього питання можна ознайомитись в [19]).

Вперше коректні результати стосовно ймовірності атаки подвійної витрати, а також необхідної кількості блоків підтвердження було опубліковано в роботі [18] для протоколу PoW і у роботі [21] — протоколу PoS. У цих статтях розглянуто однорівневі блокчейни з одним протоколом консенсусу.

2. ПОСТАНОВКА ЗАДАЧІ

Розглянемо дворівневий блокчейн з протоколом консенсусу Proof-of-Proof [10], у мейнчейні якого використано протокол PoS, а в сайдчейні — протокол PoW. Нехай деяка транзакція, що перераховує кошти постачальнику, включена в блок B_0 сайдчейну. Через деякий час після цього у мейнчейні з'являється посилання на блок B_0, тобто з'являється блок B^*, до заголовку якого входить або геш-значення від блоку B_0, або геш-значення одного з наступних блоків сайдчейну, який безпосередньо або опосередковано посилається на блок B_0. У такому разі атака подвійної витрати на сайдчейн стає можливою лише за умови, що вона відбулась у мейнчейні після створення блоку B^*.

Сформулюємо задачу. Визначити таку найменшу кількість z блоків підтвердження у сайдчейні (після першого посилання на блок B_0 у мейнчейні, тобто після виходу блоку B^*), що ймовірність атаки подвійної витрати на блок B_0 не перевищувала би заданого $\varepsilon \in (0,1)$.

Аналогічну задачу було повністю розв'язано для дворівневого протоколу консенсусу Proof-of-Proof за таких умов, коли:

— в обох блокчейнах (у мейнчейні і в сайдчейні) використано той самий протокол консенсусу PoW [14];

— в обох блокчейнах (у мейнчейні і в сайдчейні) використано той самий протокол консенсусу PoS [15].

Ми розв'язуємо цю задачу за умови, що в мейнчейні використано протокол консенсусу PoS, а в сайдчейні — протокол консенсусу PoW.

Сформулюємо та доведемо допоміжні твердження.

Опишемо поведінку зловмисника, який потенційно може бути присутнім в обох блокчейнах. Вважатимемо слотлідерів (у мейнчейні) та майнерів (у сайдчейні) чесними, якщо всі їхні дії не суперечать правилам створення блоків у блокчейні, до яких, зокрема, належить правило довшого ланцюжка. Також вважатимемо, що чесні слотлідери завжди створюють новий блок у своєму таймслоті, посилаються у ньому на останній блок найдовшого ланцюжка та миттєво поширюють його для всіх вузлів мережі. Так само, чесні майнери завжди присутні в мережі, створюючи новий блок, посилаються у ньому на останній блок найдовшого ланцюжка та миттєво поширюють його для всіх вузлів мережі. Нечесні майнери (або зловмисники) можуть порушувати будь-які правила створення блоків. Ми робимо припущення на користь зловмисника і надалі вважаємо, що:

— всі зловмисники консолідовані, можуть миттєво обмінюватись повідомленнями;

— в основному блокчейні частка зловмисника (сума депозитів всіх нечесних стейкхолдерів) дорівнює p_m (від англійського слова malicious), частка чесних слотлідерів дорівнює p_h (від англійського слова honest), причому $p_m + p_h = 1$ і $p_m < p_h$;

— у сайдчейні частка зловмисника (сума обчислювальних потужностей всіх нечесних стейкхолдерів) дорівнює q_m, частка чесних майнерів дорівнює q_h, причому $q_m + q_h = 1$ і $q_m < q_h$.

Зазначимо, що відповідно до процедури вибору слотлідерів розподіл блоків у протоколі PoS між чесними слотлідерами та зловмисником підпорядковується біноміальному закону, а саме: ймовірність $P_{n,k}$ того, що у довільно вибраному відрізку з n послідовних таймслотів буде рівно k таймслотів, у яких слотлідером є зловмисник, обчислюється так:

$$P_{n,k} = C_n^k \cdot p_m^k \cdot p_h^{n-k}. \tag{1}$$

Згідно з (1) отримаємо таке твердження, доведення якого є очевидним.

Лема 1. Нехай l, $n \in \mathrm{N}$, $l < n$. Тоді ймовірність $P_{n,\geq l}^{(h)}$ того, що у ланцюжку з n послідовних таймслотів не менше, ніж l таймслотів належать чесним стейкхолдерам, дорівнює

$$P_{n,\geq l}^{(h)} = \sum_{j=l}^{n} C_n^j \cdot p_m^{n-j} \cdot p_h^j. \tag{2}$$

Зазначимо, що одним з видів зловмисної діяльності слотлідерів може бути відмова від створення блоків у призначені таймслоти. Унаслідок цього протягом відрізку з n послідовних таймслотів може бути створено не n блоків, як очікується, а менша їхня кількість, яка в найгіршому випадку дорівнює кількості чесних слотлідерів на цьому відрізку. Це потрібно враховувати, щоб мати впевненість, що за визначений час в основному блокчейні було створено кількість блоків, не меншу за деяке визначене число.

Виберемо деяке достатньо мале значення $\varepsilon_{SP} \in (0,1)$ та визначимо $z_{SP}(\varepsilon_{SP})$ як таке найменше натуральне число, що після $z_{SP}(\varepsilon_{SP})$ блоків підтвердження в основному блокчейні ймовірність атаки подвійної витрати буде меншою за задане ε_{SP} (формули для обчислення $z_{SP}(\varepsilon_{SP})$ отримано у роботі [21]). Визначимо тепер кількість таймслотів $n_{SP,TS}(\varepsilon_{SP})$, які потрібно чекати в мейнчейні, щоб імовірність атаки подвійної витрати була меншою за задане ε_{SP}. Відповідно до леми 1 і формули (2) отримуємо таке твердження.

Лема 2. Нехай $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$. Тоді якщо після створення блоку B^* у мейнчейні минуло $n_{SP,TS}$ таймслотів до відправлення товару, де

$$n_{SP,TS}(\varepsilon_{SP}) = \arg\min_{n} \{1 - P^{(h)}_{n,\geq z_{SP}(\varepsilon_{SP}^{(II)})} < \varepsilon_{SP}^{(I)}\}, \tag{3}$$

то ймовірність $P_{SP,DS}(n_{SP,TS}(\varepsilon_{SP}))$ атаки подвійної витрати, яка скасовує цей блок, не перевищує ε_{SP}.

Доведення. Визначимо подію $E_1 = E_1(n_{SP,TS}(\varepsilon_{SP}))$ як таку, що атака подвійної витрати у мейнчейні відбулась за умови, що пройшло $n_{SP,TS}(\varepsilon_{SP})$ таймслотів після створення блоку з транзакцією. Також визначимо подію $E_2 = E_2(n_{SP,TS}(\varepsilon_{SP}))$ як таку, що за $n_{SP,TS}(\varepsilon_{SP})$ таймслотів, які минули після створення блоку з транзакцією, було згенеровано не менше, ніж $z_{SP}(\varepsilon_{SP}^{(II)})$ блоків. Тоді ймовірність атаки подвійної витрати $P_{SP,DS}(n_{SP,TS}(\varepsilon_{SP}))$ можна записати як

$$P_{SP,DS}(n_{SP,TS}(\varepsilon_{SP})) = P(E_1) = P(E_1 / E_2)\cdot P(E_2) + P(E_1 / \overline{E_2})\cdot P(\overline{E_2}) \leq$$

$$\leq P(E_1 / E_2) + P(\overline{E_2}) \leq \varepsilon_{SP}^{(II)} + \varepsilon_{SP}^{(I)} = \varepsilon_{SP}.$$

Лему доведено.

На підставі лем 1 і 2 для заданого значення ε_{SP} можна визначити, яка кількість таймслотів після створення блоку з транзакцією гарантує, що ймовірність атаки подвійної витрати у мейнчейні не перевищує ε_{SP}. Ця кількість таймслотів може набувати різних значень залежно від вибору доданків у виразі $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$ (зокрема, далі у розд. 5 наведено результати для випадків, коли $\varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$ задано як 0.0002 + 0.0003, 0.0003 + 0.0002 та 0.01 + 0.01).

Для заданого достатньо малого $\varepsilon_{SI} \in (0,1)$ позначимо $z_{SI} = z_{SI}(n_{SP,TS}; \varepsilon_{SI})$ таку найменшу кількість блоків у сайдчейні, що за час їхнього створення у мейнчейні з ймовірністю, не меншою за $1 - \varepsilon_{SI}$, пройшло не менше, ніж $n_{SP,TS}$ таймслотів. Далі потрібно визначити $z_{SI} = z_{SI}(n_{SP,TS}; \varepsilon_{SI})$ залежно від заданих $n_{SP,TS}$ та ε_{SI}.

Позначимо ν середню інтенсивність створення блоків у сайдчейні, тобто кількість створених блоків за одиницю часу (для визначеності за одиницю часу вважаємо 1 с). Ця величина є оберненою до середнього часу виходу блоку (наприклад, для BTC $\nu = \frac{1}{600}$) та залежить від сукупних обчислювальних потужностей майнерів у мережі та цільової величини (порогового геш-значення). Зазвичай у протоколі PoW цільова величина періодично переобчислюється і при цьому регулюється так, щоб середній час до створення блоку несуттєво відхилявся від встановленого в цьому блокчейні.

Якщо записати величину ν як суму: $\nu = \nu_h + \nu_m$, де ν_h та ν_m є інтенсивностями створення блоків чесними майнерами та зловмисником відповідно, то справджуватимуться рівності [19]

$$q_h = \frac{\nu_h}{\nu},\ q_m = \frac{\nu_m}{\nu}. \tag{4}$$

Також позначимо τ тривалість таймслоту у мейнчейні.

Для цих позначень справедливе таке твердження.

Лема 3. Визначимо подію $E_{SI} = E_{SI}(z_{SI}, n)$ як таку, що за той час, як у сайдчейні створено z_{SI} блоків, у мейнчейні минуло менше, ніж n таймслотів. Тоді

$$P(E_{SI}) \le 1 - e^{-\nu \cdot \tau \cdot n} \cdot \sum_{k=0}^{z_{SI}-1} \frac{(\nu \cdot \tau \cdot n)^k}{k!}. \tag{5}$$

Доведення. Визначимо подію $E_{SP} = E_{SP}(z_{SI}, n)$ як таку, що за той час, коли у мейнчейні минуло n таймслотів, у сайдчейні створено не менше, ніж z_{SI} блоків. Тоді $E_{SI} \subset E_{SP}$, отже $P(E_{SI}) \le P(E_{SP})$.

Оскільки τ — тривалість таймслоту у мейнчейні, то подію E_{SP} можна визначити як таку, що за час $\tau \cdot n$ у сайдчейні створено не менше, ніж z_{SI} блоків, або час до створення z_{SI} блоків не перевищує величини $\tau \cdot n$. Обчислимо верхню оцінку ймовірності цієї події, яка буде також і верхньою оцінкою події E_{SI}. Також припускатимемо, що час синхронізації блоків у сайдчейні дорівнює нулю, оскільки зі збільшенням часу синхронізації ймовірність події E_{SP} буде зменшуватись, а нам потрібно обчислити верхню оцінку цієї імовірності. Тоді випадкова величина t_ν, яка є часом, що минув до створення наступного блоку у сайдчейні, має (у випадку нульового часу поширення блоку) експоненційний розподіл [18]:

$$F_{t_\nu}(x) = P(t_\nu \le x) = 1 - e^{-\nu \cdot x}, \tag{6}$$

а відповідно час $t_{\nu,b}$, що минув до створення b блоків, — розподіл Ерланга [18]:

$$F_{t_{\nu,b}}(x) = P(t_{\nu,b} \le x) = 1 - e^{-\nu \cdot x} \cdot \sum_{k=0}^{b-1} \frac{(\nu \cdot x)^k}{k!}. \tag{7}$$

Тому ми можемо оцінити ймовірність події E_{SP} за формулою

$$P(E_{SP}) = P(t_{\nu, z_{SI}} \le \tau \cdot n) = 1 - e^{-\nu \cdot \tau \cdot n} \cdot \sum_{k=0}^{z_{SI}-1} \frac{(\nu \cdot \tau \cdot n)^k}{k!}. \tag{8}$$

Лему доведено.

У наступному розділі леми 1–3 використаємо для побудови алгоритму визначення кількості блоків підтвердження у сайдчейні, які захищають від атаки подвійної витрати, успадковуючи стійкість мейнчейну до цієї атаки.

3. АЛГОРИТМ ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ ЗАЛЕЖНО ВІД ЗАДАНОЇ ДОПУСТИМОЇ ЙМОВІРНОСТІ ТА ПАРАМЕТРІВ МЕРЕЖІ

Відповідно до лем 1–3 запропонуємо алгоритм визначення кількості блоків підтвердження у сайдчейні, використовуючи уведені раніше позначення для параметрів мейнчейну та сайдчейну для вхідних даних алгоритму.

Алгоритм 1

Вхід алгоритму: параметри мейнчейну τ, p_m, p_h; параметр сайдчейну ν; допустиме значення ймовірності атаки ε.

1. Записати параметр ε як суму двох параметрів: $\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$. (Зауважимо, що в цих позначеннях ε_{SP} є верхньою оцінкою ймовірності атаки подвійної витрати у мейнчейні за умови того, що після транзакції пройшло $n_{SP,TS}(\varepsilon_{SP})$ таймслотів, а ε_{SI} є верхньою оцінкою ймовірності того, що за той час, коли у сайдчейні створено $z_{SI} = z_{SI}(n_{SP,TS}; \varepsilon_{SI})$ блоків, у мейнчейні пройшло менше, ніж $n_{SP,TS}$ таймслотів.)

2. Записати параметр ε_{SP} як суму двох параметрів:

$$\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}.$$

(Зауважимо, що в цих позначеннях $\varepsilon_{SP}^{(I)}$ є верхньою оцінкою ймовірності атаки подвійної витрати в мейнчейні за умови створення $z_{SP}(\varepsilon_{SP}^{(II)})$ блоків підтвердження, а $\varepsilon_{SP}^{(II)}$ — верхня оцінка ймовірності того, що в мейнчейні створено менше, ніж $z_{SP}(\varepsilon_{SP}^{(II)})$ блоків протягом $n_{SP,TS}(\varepsilon_{SP})$ таймслотів.)

3. З використанням параметрів мейнчейну за формулою (5) для ймовірності атаки, описаної в роботі [21], за заданим $\varepsilon_{SP}^{(II)}$ визначити таку (найменшу) кількість $z_{SP}(\varepsilon_{SP}^{(II)})$ блоків підтвердження для мейнчейну, після створення яких імовірність атаки подвійної витрати у мейнчейні не перевищуватиме заданого $\varepsilon_{SP}^{(II)}$.

4. З використанням лем 1 і 2 та формул (2), (3) визначити кількість таймслотів $n_{SP,TS}(\varepsilon_{SP})$ за заданими значеннями $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$ та за значенням $z_{SP}(\varepsilon_{SP}^{(II)})$, отриманим у п. 3 цього алгоритму.

5. За формулою (5) леми 3 визначити таку найменшу кількість блоків z_{SI} у сайдчейні, що величина $P(E_{SI}) < \varepsilon_{SI}$, тобто

$$z_{SI} = \arg\min_{z} \left\{ 1 - e^{-\nu \cdot \tau \cdot n_{SP,TS}(\varepsilon_{SP})} \cdot \sum_{k=0}^{z-1} \frac{(\nu \cdot \tau \cdot n_{SP,TS}(\varepsilon_{SP}))^k}{k!} < \varepsilon_{SI} \right\} \qquad (9)$$

(значення $n_{SP,TS}(\varepsilon_{SP})$ обчислено у п. 4 цього алгоритму).

Результат роботи алгоритму: z_{SI}.

4. ОЦІНКА ЙМОВІРНОСТІ АТАКИ ПОДВІЙНОЇ ВИТРАТИ

Сформулюємо і доведемо теорему про ймовірність атаки, якщо величину z_{SI} отримано за алгоритмом 1.

Теорема 1. Нехай величину z_{SI} отримано за алгоритмом 1 для заданих вхідних параметрів дворівневої мережі τ, p_m, p_h, ν та заданої величини ε. Тоді ймовірність $P(\tau, p_m, p_h, \nu)$ атаки подвійної витрати на блок B_0 не перевищує ε за умови, що після створення у мейнчейні відповідного блоку B^* у сайдчейні створено не менше, ніж z_{SI} блоків.

Доведення. Визначимо подію E як таку, що атака подвійної витрати на блок B_0 за умови створення не менше, ніж z_{SI} блоків, була успішною. Також скористаємось подією $E_{SI} = E_{SI}(z_{SI}, n)$, визначеною у доведенні леми 3, і подамо ймовірність події E як

$$P(E) = P(E / E_{SI}) \cdot P(E_{SI}) + P(E_1 / \overline{E_{SI}}) \cdot P(\overline{E_{SI}}) \le$$

$$\le P(E_{SI}) + P(E_1 / \overline{E_{SI}}).$$

Згідно з вибором z_{SI} у п. 5 алгоритму 1 $P(E_{SI}) < \varepsilon_{SI}$. Умовна ймовірність $P(E_1 / \overline{E_{SI}}) \le \varepsilon_{SP}$ згідно з лемою 2 і п. 4 алгоритму 1. Звідси отримуємо

$$P(E) \le \varepsilon_{SI} + \varepsilon_{SP} = \varepsilon.$$

Теорему доведено.

5. АНАЛІЗ ЧИСЕЛЬНИХ РЕЗУЛЬТАТІВ

Наведемо чисельні результати для необхідної кількості блоків підтвердження z_{SI} залежно від параметра τ (тривалість таймслоту в секундах) для мейнчейну та параметра ν (кількість створених блоків за секунду) для сайдчейну (табл. 1–3). У таблицях також наведено варіанти розбиття ймовірності атаки ε на доданки $\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$ та $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$ відповідно до пп. 1 та 2 алгоритму 1. Зазначимо, що це розбиття може бути довільним і від нього буде залежати результат z_{SI} роботи алгоритму 1. Але за будь-якого розбиття зазначених імовірностей на доданки отримане значення кількості блоків підтвердження буде забезпечувати вимогу, щоб значення ймовірності атаки подвійної витрати не перевищувало заданої величини ε.

У табл. 1–3 наведено значення величини z_{SI}, для якого ймовірність атаки подвійної витрати не перевищує $\varepsilon = 0.001$, для заданої частки стейку зловмисника p_m та заданих параметрів мейнчейну τ та сайдчейну ν.

Зазначимо, що співвідношення наведених у таблицях чисельних результатів є очікуваним:

— чим більшою є частка депозиту зловмисника, тим більшою має бути потрібна кількість блоків підтвердження;

— чим швидше створюються блоки у сайдчейні порівняно з мейнчейном (тобто чим меншою є величина $\dfrac{1}{\nu \cdot \tau}$), тим більшою має бути потрібна кількість блоків підтвердження у сайдчейні.

Така особливість чисельних результатів ще раз опосередковано підтверджує коректність отриманих у роботі аналітичних результатів.

Таблиця 1. Значення величини z_{SI} для $\tau = 10$ та $\nu = 1/600$

p_m	0.15	0.25	0.4
$\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$	0.0005 + 0.0005	0.0005 + 0.0005	0.02 + 0.02
$\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$	0.0002 + 0.0003	0.0003 + 0.0002	0.01 + 0.01
$z_{SP}(\varepsilon_{SP}^{(II)})$	10	25	35
$n_{SP,\,TS}(\varepsilon_{SP})$	19	48	75
z_{SI}	4	6	5

Таблиця 2. Значення величини z_{SI} для $\tau = 15$ та $\nu = 1/20$

p_m	0.15	0.25	0.4
$\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$	0.0005 + 0.0005	0.0005 + 0.0005	0.02 + 0.02
$\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$	0.0002 + 0.0003	0.0003 + 0.0002	0.01 + 0.01
$z_{SP}(\varepsilon_{SP}^{(II)})$	10	25	35
$n_{SP,\,TS}(\varepsilon_{SP})$	24	48	75
z_{SI}	34	58	73

Таблиця 3. Значення величини z_{SI} для $\tau = 20$ та $\nu = 1/15$

p_m	0.15	0.25	0.4
$\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$	0.0005 + 0.0005	0.0005 + 0.0005	0.02 + 0.02
$\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$	0.0002 + 0.0003	0.0003 + 0.0002	0.01 + 0.01
$z_{SP}(\varepsilon_{SP}^{(II)})$	10	25	35
$n_{SP,\,TS}(\varepsilon_{SP})$	24	48	75
z_{SI}	53	93	122

ВИСНОВКИ

Отримано результати, які є необхідними для безпечного використання дворівневого блокчейну з протоколом консенсусу Proof-of-Proof. Такий дворівневий блокчейн найбільш придатний для створення каскадної системи державних реєстрів, яка буде гарантовано захищена від підміни та підроблення документів, а її користувачі — від рейдерства. Дворівневий блокчейн можна також використовувати як середовище для смарт-контрактів, що має підвищену безпеку та спрощує юридичне обґрунтування статусу смарт-контракту.

Ми розглянули одну з чотирьох можливий комбінацій протоколів консенсусу, а саме — протокол консенсусу Proof-of-Stake в мейнчейні та протокол Proof-of-Work у сайдчейні. Оскільки дві інші комбінації, коли в обох блокчейнах однакові протоколи консенсусу, було досліджено у роботах [14, 15], то для подальшого дослідження залишається одна комбінація — Proof-of-Work в мейнчейні та Proof-of-Stake в сайдчейні.

Також актуальним є питання стосовно розбиття допустимої ймовірності атаки ε на відповідні доданки: $\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$ та $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$. Використовуючи таке розбиття, можна отримати різні значення для кількості блоків підтвердження z_{SI}, тобто чисельні результати, наведені в табл. 1–3, є лише одними з можливих варіантів. Вірогідно, що для якогось іншого розбиття ймовірностей на відповідні доданки необхідна кількість блоків підтвердження виявиться меншою. Наразі ми не можемо дати рекомендацій стосовно цього розбиття на доданки, і найпростішим (але не обов'язково оптимальним з погляду мінімізації кількості блоків підтвердження) можна вважати варіант розбиття на однакові доданки або на такі, для яких простіше обчислювати величини $z_{SP}(\varepsilon_{SP}^{(II)})$, $n_{SP,TS}(\varepsilon_{SP})$ та z_{SI}. Це питання також є актуальним для подальших досліджень.

СПИСОК ЛІТЕРАТУРИ

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. URL: https://bitcoin.org/bitcoin.pdf.
2. Quigley J.L., Gilbert J. What is Proof-of-Work (PoW)? All you need to know. URL: https://blockworks.co/news/what-is-proof-of-work.
3. Chirag. A guide to understand blockchain consensus algorithms. 2021. URL: https://appinventiv.com/blog/blockchain-consensus-algorithms-guide/.
4. Akunne P. A guide to blockchain consensus protocols. 2021. URL: https://blog.logrocket.com/guide-blockchain-consensus-protocols/.
5. Fáwolé J., Malanii O., Ciattaglia L. Consensus mechanisms in blockchain: A deep dive into the different types. 2023. URL: https://hacken.io/discover/consensus-mechanisms/.
6. Xiao Y., Zhang N., Lou W. Hou Y.T. A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22, N 2. P. 1432–1465. https://doi.org/10.1109/COMST.2020.2969706.
7. Sankar L.S., Sindhu M., Sethumadhavan M. Survey of consensus protocols on blockchain applications. *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Coimbatore, India, 2017. P. 1–5. https://doi.org/10.1109/ICACCS.2017.8014672.
8. Guru A., Mohanta B.K., Mohapatra H., Al-Turjman F., Altrjman C., Yadav A. A survey on consensus protocols and attacks on blockchain technology. *Appl. Sci.* 2023. Vol. 13, N 4. 2604. https://doi.org/10.3390/app13042604.
9. Zhang S., Lee, J.-H., Analysis of the main consensus protocols of blockchain. *ICT Express*. 2020. Vol. 6, Iss. 2. P. 93–97. https://doi.org/10.1016/j.icte.2019.08.001.
10. Proof-of-Proof and veriblock blockchain protocol consensus algorithm and economic incentivization specifications. VeriBlock, Inc. URL: https://mirror1.veriblock.org/Proof-of-Proof_and_VeriBlock_Blockchain_Protocol_Consensus_Algorithm_and_Economic_Incentivization_ v1.0.pdf.
11. Saleh F., Blockchain without waste: Proof-of-Stake. *The Review of Financial Studies*. 2021. Vol. 34, Iss. 3. P. 1156–1190, https://doi.org/10.1093/rfs/hhaa075

12. Sanchez M., Fisher J. Proof-of-Proof: A decentralized, trustless, transparent, and scalable means of inheriting Proof-of-Work security. VeriBlock, Inc. https://raw.githubusercontent.com/cedricwalter/blockchain-consensus/master/whitepaper/PoP-Whitepaper.pdf.
13. М.С. Кондратенко. Використання технології блокчейну при побудові ієрархічної структури на множині державних реєстрів для захисту від підробки інформації. *Електрон. моделювання.* 2023. Т. 45, № 3. С. 43–56. https://doi.org/10.15407/emodel.45.03.043.
14. Kovalchuk L., Kostanda V., Marukhnenko O., Pozhylenkov O. Achieving security in Proof-of-Proof protocol with non-zero synchronization time. *Mathematics*. 2022. Vol. 10, Iss. 14. 2422. https://doi.org/10.3390/math10142422.
15. Кондратенко М.С. Визначення кількості блоків підтвердження у блокчейні, в якому розміщено реєстр другого рівня у випадку, коли в обох блокчейнах використовується протокол консенсусу POS. *Зб. матеріалів XLI Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* (м. Київ, 17 травня 2023), Київ: ІПМЕ ім. Г.Є. Пухова НАН України, 2023. С. 188–190. URL: https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf.
16. Buser M., Dowsley R., Esgin M.F. et al. Post-quantum verifiable random function from symmetric primitives in PoS blockchain. In: Atluri V., Di Pietro R., Jensen C.D., Meng W. (Eds.). Computer Security — ESORICS 2022. ESORICS 2022. *Lecture Notes in Computer Science.* Vol. 13554. Cham: Springer, 2022. P. 25–45. https://doi.org/10.1007/978-3-031-17140-6_2.
17. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure Proof-of-Stake blockchain protocol. In: Katz J., Shacham H. (Eds.) Advances in Cryptology — CRYPTO 2017. CRYPTO 2017. *Lecture Notes in Computer Science*. Vol 10401. Cham: Springer, 2017. P. 357–388. https://doi.org/10.1007/978-3-319-63688-7_12.
18. Grunspan C., Pérez-Marco R., Double spend races. arXiv:1702.02867v3 [cs.CR], 6 May 2020. https://doi.org/10.48550/arXiv.1702.02867
19. Kovalchuk L., Kaidalov D., Nastenko A., Rodinko M., Shevtsov O., Oliynykov R. Decreasing security threshold against double spend attack in networks with slow synchronization. *Computer Communications.* 2020. Vol. 154. P. 75–81. https://doi.org/10.1016/j.comcom.2020.01.079.
20. Kovalchuk L., Rodinko M., Oliynykov R., Kaidalov D., Nastenko A. Probability of double spend attack for network with non-zero time delay. *Publ. Math. Debrecen*. 2022. Suppl. 100. P. 597–615. https://doi.org/10.5486/pmd.2022.suppl.4.
21. Karpinski M., Kovalchuk L., Kochan R., Oliynykov R., Rodinko M., Wieclaw L. Blockchain technologies: Probability of double-spend attack on a Proof-of-Stake consensus. *Sensors*. 2021. Vol 21, Iss. 19. 6408. https://doi.org/10.3390/s21196408.

L.V. Kovalchuk, N.V. Kuchynska, M.S. Kondratenko

DETERMINING THE NUMBER OF CONFIRMATION BLOCKS IN A TWO-LEVEL BLOCKCHAIN WITH PROOF-OF-PROOF CONSENSUS PROTOCOL FOR DIFFERENT CONSENSUS TYPES IN MAINCHAIN/SIDECHAIN TO PREVENT DOUBLE-SPEND ATTACK. I. PoS IN MAINCHAIN AND PoW IN SIDECHAIN

Abstract. The paper investigates the issues of the safe operation of a two-level blockchain with a complex mixed consensus protocol — Proof-of-Stake in the main blockchain (mainchain) and Proof-of-Work in the secondary (sidechain). This two-level blockchain is built on the principle of the Proof-of-Proof protocol, where the safety of the sidechain is ensured by the stability of the mainchain, by referring the mainchain blocks to the sidechain blocks using special transactions. Such a structure allows faster issuance of blocks in the sidechain and, accordingly, faster processing of transactions without loss of security and without increasing the volume of the block. In turn, such a two-level blockchain is of the greatest interest for the creation of a cascade system of state registers, which will be guaranteed to be protected against the substitution and forgery of documents. The main results of the work are explicit analytical expressions for estimates of probability of double spend attack on such two-level blockchain, under the condition of adversary in sidechain and in mainchain.

Keywords: blockchain, mainchain, sidechain, cryptocurrencies, mining, Proof-of-Proof consensus protocol, double spend attack.

Надійшла до редакції 23.01.2024