УДК 004.056.5: 004.738 DOI: 10.26565/2519-2310-2019-3-05

КЛАСИФІКАЦІЯ АТАК ПОДВІЙНИХ ВИТРАТ В БЛОКЧЕЙН СИСТЕМАХ

Євгеній Деменко, Олександр Онікійчук, Микита Гончаров,
Сергій Даценко, Микола Полуяненко

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
demenjay@gmail.com, onik4524a@gmail.com, wdpgames@yandex.ru, sergdacenko@gmail.com
nlfsr01@gmail.com

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологічний університет Монтеррея, Монтеррей, 64849, Мексика.
kalash@itesm.mx

Надійшло: Листопад 2019.

***Анотація**: У статті наведено короткий огляд та проведено систематизацію інформації за проблематикою подвійних витрат в блокчейн системах з ймовірнісними методами консенсусу і можливими шляхами її вирішення. Описано процедури, за допомогою яких реалізуються атаки подвійних витрат. Розкрито сутність маніпуляцій за допомогою яких зловмисник може намагатися провести подвійні витрати у децентралізованих платіжних системах. Наведено детальних опис дій атакуючого та шляхи запобігання атаки. Розгляд починається від простих атак заснованих на створені дублюючих транзакцій та закінчується більш складними атаками, такими як: атака-гонка; атака Фіннеєм; атака Vector76; атака «51%». Ці атаки вимагають від атакуючого значних ресурсів та можливості розгалуження блокчейн реєстру. Остання група атак проаналізована більш детальніше, з наведенням варіантів її застосування. В якості найбільш небезпечної виділено атаку «51 %», що, на думку авторів, є найбільшою загрозою для безпеки блокчейн систем з ймовірнісними алгоритмами консенсусу.*

***Ключові слова:** комп'ютерні мережі; децентралізовані системи; блокчейн; атака на блокчейн мережі; подвійні витрати.*

1 Вступ

Як правило, всі «класичні» платіжні системи є централізованими, що мають адміністративну ланку, яка забезпечує контроль легітимності будь-якої операції [1]. 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 подвійний витрати одних і тих же цінностей стає можливим. Для захисту від атаки подвійної витрати 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 транзакції, які намагаються повторно витратити раніш витрачених коштів. І, якщо навіть такий блок буде сформовано вузлом зловмисника, його відкинуть вузли чесної мережі і блок не буде додано до блокчейн реєстр 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 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 подвійної витрати безпосередньо залежить від ресурсів (гешрейта) атакуючого і кількості підтверджень. Ймовірність формування альтернативного ланцюжка експоненціальна зменшується зі зростанням кількості підтверджень і зменшенням гешрейта атакую-

чого. 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 призводить до значних затримок, дискомфорту використання системи та збиткам взаємодіючих сторін.

Тому угоди, з нульовим підтвердженням, потенційно мають великий ризик стати жертвою атаки подвійної витрати, а угоди, які очікують велику кількість підтверджень – зазнати збитків через затримки в їх укладанні. Тому, питання знаходження оптимальної кількості підтверджень, при яких ризик атаки подвійний витрати буде нижче деякого прийнятного рівня, а час очікування буде мінімально необхідним, є актуальним завданням. Наприклад, існує думка ([2-5] та ін.), якщо використовується механізм консенсусу на основі Доказу виконаної роботи (*англ. PoW – Proof-of-work*) на основі геш-функції і у атакуючого знаходиться 10 % обчислювальної потужності (гешрейт) від загальної мережі, і очікується 6 підтверджень – ймовірність успіху такої атаки, приблизно, складе 0,1 %. Наведена оцінка ґрунтується на моделі «розорення гравця» [6].

2 Опис та типи атак подвійної витрати

Подвійні витрати (*англ. Double-spending*) – ситуація в децентралізованих платіжних системах (*криптовалютах*), коли користувач пробує повторно використовувати раніше передане [15]. Зазвичай мережа не прийме таку транзакцію як дійсну. Але в паралельних розгалуженнях ланцюга блоків можуть перебувати транзакції, які по-різному розпоряджаються одним і тим же.

Коли здійснюється угода за криптовалюту, то передбачається, що після перерахування монет відправник отримує у відповідь продукт або послугу, яку він оплатив. Враховуючи ці процедурні особливості, сутність атаки подвійної витрати полягає в тому, що спочатку зловмисник переконує продавця в тому, що транзакція на оплату вже була проведена, після чого продавець передає свій товар, а покупець (зловмисник) отримує його. Після отримання товару зловмисник робить все можливе щоб блокчейн мережа прийняла та зберегла іншу транзакцію. Таким чином, в разі успіху зловмисника у продавця не залишається а ні товару, а ні плати за нього.

Атака подвійної витрати існує в багатьох формах [11]. Кожен з можливих методів, що реалізує ту чи іншу форму, повинен перевірятися і оброблятися відповідним програмним забезпеченням (ПЗ) повного вузла. Наведемо методи, що можуть бути застосовані для проведення повторної витрати одних і тих же коштів:

- одна транзакція в мемпулі (*англ. Bitcoin Mempool* [7]), що витрачає одні й ті ж вхідні значення (*UTXO – Unspent Transaction (TX) Output*) кілька разів;
- кілька транзакцій в мемпулі (*англ. Bitcoin Mempool*), які витрачають кошти, посилаючись на одні й ті ж вхідні значення (*UTXO*);
- транзакція в одному блоці, яка проводить одні й ті ж вхідні значення (*UTXO*) кілька разів;
- кілька транзакцій в різних блоках витрачають одні й ті ж вхідні значення (*UTXO*);
- проведення атаки за допомогою вдалого розгалуження блокчейн реєстру, де кожна з гілок містить різні транзакції, що змінюють діючий стан блокчейн системи.

Якщо вразливостям, що засновані на перших чотирьох методах, можна запобігти за допомогою відповідної реалізації ПЗ, то останній метод, який засновано на самому принципі реалізації консенсусу (*використанні ймовірнісних механізмів консенсусу*), не виключає вдалої реалізації відповідної загрози.

Опис виявлених у Bitcoin Core вразливостей, що засновані на перших 4-х методах, а також детальний аналіз причини їх появи можна знайти у роботах [8-9]. Щоб максимально унеможливити маніпулювання блокчейн системою на користь тільки однієї особи, процес майнин-

га був розроблений, як дуже ресурсномістка операція. Так, для формування нового блоку з транзакціями в блокчейн системі, майнери повинні надати дійсні докази виконаної роботи. Але, не зважаючи на це, у зловмисника, який намагається використати п'ятий метод, так само є кілька варіантів його реалізації [4].

2.1 Атака-гонка

Атака-гонка [10] відноситься до випадку, коли торговець приймає непідтверджену транзакцію (*транзакція знаходиться в пулі транзакцій і очікує додавання в блок блокчейн реєстру*) і відразу ж надає платнику продукт/послугу, перш ніж ця транзакція буде підтверджена. Зловмисник з наміром ввести в оману продавця створює дві транзакції: - (I) транзакцію, яка платить продавцю необхідну суму в обмін на продукт/послугу; - (II) шахрайську транзакцію, яка платить ту ж суму на гаманець зловмисника. Обидві транзакції використовують одні і ті ж вхідні дані та намагаються витратити одну й ту ж криптовалюту. Зловмисник одночасно випускає обидві транзакції в блокчейн мережу. Майнер додає їх до мемпулу (*англ. Bitcoin Mempool*) та вважає обидві транзакції дійсними до тих пір, поки одна з них не буде додана до блокчейн реєстру. Транзакція, яка зберігається в блокчейн реєстрі, називається підтвердженою транзакцією. У цей момент входи збереженої транзакції не можуть бути використані в якості вхідних даних для інших транзакцій. Отже, шахрайська транзакція може бути перевірена першою і додана в ланцюжок блоків, що робить платіжну транзакцію недійсною. Неприпустима транзакція відхиляється системою та видаляється з mempool-ів транзакцій майнером.

Щоб уникнути атаки-гонки, торговці повинні дочекатися завершення процесу майнингу і появи транзакції в блокчейн реєстрі, перш ніж надавати платнику продукт або послугу.

2.2 Атака Фіннеєм

Атака Фіннеєм була вперше запропонована на форумі присвяченому біткойну [11]. Як і у випадку з атакою-перегонів, атакуючий, що виконує цю атаку, доб'ється успіху тільки в тому випадку, якщо торговець приймає непідтверджену транзакцію. Для цього атакуючий створює дві транзакції, схожі на ті, що беруть участь в гонці, і утримує їх обидві. Потім зловмисник починає формувати блок, що містить шахрайську транзакцію. Якщо зловмисник успішно сформує блок, він використовує іншу транзакцію, щоб негайно сплатити продавцю в обмін на продукт/послугу. Як тільки продавець здійснює операцію, зловмисник публікує видобутий блок в блокчейн мережу, який містить шахрайську транзакцію. Зважаючи на те, що блок вже сформовано, він буде негайно доданий до блокчейну. В результаті платіжна транзакція стане недійсною. На додаток до цього, зловмисник отримує винагороду за видобутий блок, який несе шахрайську транзакцію. Однак здатність самостійно добувати блок малоймовірна, враховуючи ресурси, які необхідні для виконання завдання.

2.4 Атака Vector76

В порівнянні з атаками-гонки і Фінні, атака Vector76 [12,13] вимагає, щоб продавець чекав створення одного блоку, та додав його в ланцюжок блоків в якості підтвердження. Щоб скасувати транзакцію, зловмисникам необхідно створити розгалуження в блокчейні. Спочатку зловмисник створює платіжну транзакцію продавця, но не передає її в мережу. Потім зловмисник намагається самостійно і таємно сформувати блок з цією транзакцією. У разі успіху атакуючий утримує блок, поки чесні майнери не сформують ще один блок. На наступному кроці, атакуючий публікує блок в мережу одночасно з тим, як чесні майнери публікують свій блок, що призводить до розгалуження блокчейн реєстру.

Перед тим, як розгалуження вирішиться, зловмисник створює шахрайську транзакцію, що повторно витрачає той же вхід транзакції, який використовувався в транзакції, оплачуваної продавцем. Потім зловмисник передає шахрайську транзакцію чесним майнерам, які не мають розгалуження з блоком, що містить транзакцію перераховуючи кошти продавцю. Ці майнери вважають шахрайську транзакцію дійсною і починають формувати з нею новий

блок. В результаті кожна гілка такого блокчейна зберігає одну з транзакцій. Якщо гілка, яка містить шахрайську транзакцію, збільшується в порівнянні з іншого гілкою, то спроба подвійного витрачання буде успішною.

2.5 Атака «51%»

Атака «51%» є найбільшою загрозою для блокчейн систем з консенсусами, які мають ймовірнісний характер завершеності [14]. Ця атака безпосередньо пов'язана з ресурсами, які може використовувати зловмисник [15]. Ресурси вимірюються з точки зору фінансової та обчислювальної потужності. Як правило великі організації мають кошти для контролю більшої частки наявної обчислювальної потужності, та в разі необхідності, можуть зруйнувати або підштовхнути систему до свого бажаного статусу. Важливо відзначити, що навіть при обчислювальній потужності менш 50%, зловмисник все ще може маніпулювати системою. Ця атака також згадується, як атака більшості, згідно якій зловмисник (*зазвичай група майнерів*) контролює більше половини всієї обчислювальної потужності системи. Таким чином контролюючі велику частину потужностей, зловмисник може втручатися в процес майнінгу блоків і скасовувати будь-який блок транзакцій. Під час атаки на «51%» система втрачає цілісність, оскільки у інших майнерів більше немає стимулу брати участь в процесі майнінгу.

Щоб краще зрозуміти особливості цієї атаки, розглянемо випадок, коли зловмисник генерує платіжну транзакцію та «випускає» її в мережу. Ланцюжок блоків можна уявити у вигляді дерева, що починається з початкового (генезис) блоку і йде послідовно. Гілки цього дерева представляють собою історії транзакцій. Гілка не може містити двох конфліктних транзакцій, однак може бути інша гілка, яка містить конфліктуючу транзакцію. Це відповідає ситуації, коли в один момент часу сформовано два різних блока і частина вузлів мережі додала до ланцюга перший блок, а інша частина - другий. Зазвичай, така розбіжність дозволяється, як тільки знаходиться наступний блок. Вірною гілкою цього дерева вважається та, яка включає в себе більш довгий ланцюг наступних блоків.

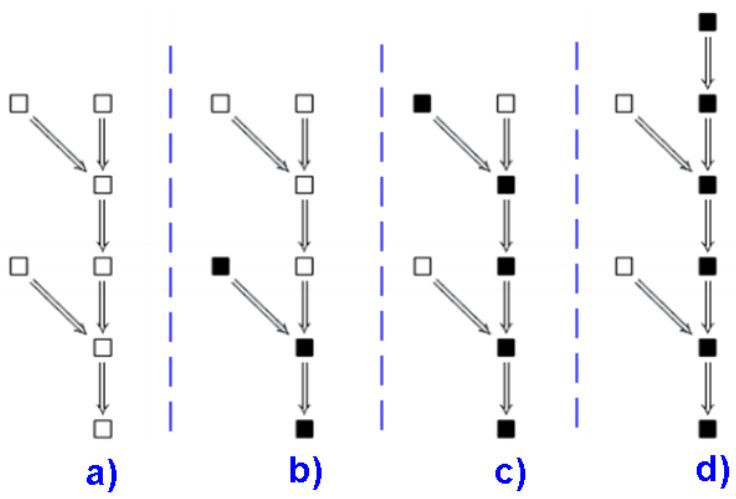

Рис. 1 – Приклади можливих ланцюжків блоків

Для прикладу розглянемо ланцюжок блоків, якій зображено на рис. 1 [16]. Дерево починається знизу, а стрілки вказують з якого блоку на який йде посилання в заголовку блоку. Використані на рис. 1 легенди мають наступне розшифрування: a) можливий варіант побудови дерева; b) позначена гілка недійсна, так як її довжина становить тільки три блоки, в той час як існує довша гілка за неї; c) темна гілка, що має, як і пряма, найбільшу довжину, з-за цього деякими вузлами вважається дійсною; d) випадок, коли знаходиться новий блок, що посилається тільки на один з попередніх блоків, то деяка гілка стає довшою і приймається усіма вузлами, як дійсна.

Узагальнюючи результати аналізу відомих форм реалізації атаки подвійної витрати можливо стверджувати, що для її успішного проведення потрібно виконати наступні кроки:

1. Провести транзакцію, яка атакує першу здійснену оплату.
2. Почати таємно майнити, використовуючи для цього той блок, який включає в себе цю останню транзакцію.
3. Дочекатися, поки транзакція, що відправляє гроші продавцеві, отримає достатню кількість підтверджуючих блоків, а продавець передасть свій товар, будучи впевненим, що гроші дійсно привласнені йому.

4. Продовжувати майнити таємну альтернативну гілку, поки вона не стане більшою, ніж публічна, після чого почати транслювати її в мережу. Оскільки нова гілка довша за всіх інших відомих, то вона буде хибно вважатися дійсною, а переказ одного біткоїна (*англ. BTC*) продавцеві буде замінений відправкою відповідних монет зловмиснику.

На рис. 2 приведено типовий алгоритм атаки подвійної витрати [16], де:

a) стан мережі до початку дій зловмисника;

b) створена гілка (*зліва*), яка включає в себе транзакцію відправки одного біткоїна продавця, що має два підтвердження. В результаті цього продавець передає свій товар. В цей час у зловмисника є згенерований блок, що включає атакуючу транзакцію;

c) якщо атакуючому вдасться створити більш довший ланцюжок, то він публікує його в мережу і біткоїни повертаються йому.

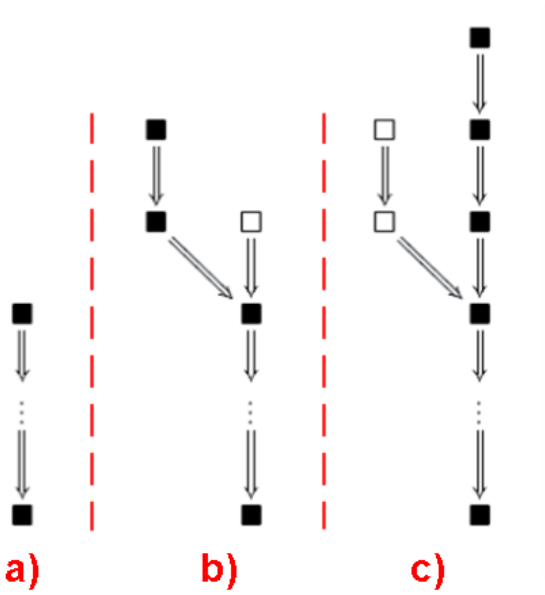

Рис. 2 – Здійснення атаки подвійної витрати

Технічно все це відбувається наступним чином. Зловмисник в блоці з номером, наприклад, 5, виконує деяку транзакцію, переказуючи гроші постачальнику послуг або товарів за покупку. Постачальник отримує ці гроші і, відповідно, поставляє покупцеві відповідну послугу/товар. Після отримання товару/послуги зловмисник швидко починає майнити інший блок з однаковим номером 5, тобто блок, який слідує за блоком номер 4, але в якому, або немає цієї фінансової транзакції, або він переводить ці гроші собі на інший гаманець. При цьому, для того щоб гарантувати прийняття чесними майнерами саме цього альтернативного ланцюжка, він на альтернативний блок з номером 5 намагається додати якомога більше блоків. Якщо у нього вийде зробити альтернативний ланцюжок більш довшим, то саме він, відповідно до протоколу консенсусу, буде вважатися вірним. Очевидно, що чим більше частка зловмисника (*не важливо, чи це обчислювальні потужності у разі Доказу виконаної роботи (англ. PoW – Proof-of-Work) або частка долі у разі підтвердження частки (англ. PoS – Proof-of-Stake*), тим більше у нього шансів успішно виконати цю атаку. Зокрема, якщо частка зловмисника більше половини, то ймовірність успіху цієї атаки прагне до 1.

4 Висновки

Надано огляд відомих схем проведення атак подвійної витрати. Розглянуті основні типи атак подвійної трати таки як: - атака-гонка; - атака Фіннеєм; - атака Vector76; - атака більшості. Визначені можливі методи захисту від наведених атак.

В якості найбільш значущої атаки, визначено атаку «51 %» (*атака більшості*). Підкреслено, що станом на сьогоднішній день, саме ця атака є найбільшою загрозою для безпеки блокчейн систем з ймовірнісними консенсусами. Це обумовлено тим, що вона базується на конструктивної особливості консенсусу, та не має гарантованого захисту від вдалого проведення.

За результатами аналізу доступних джерел за визначеною проблематикою, зроблено висновок, що успіх атаки подвійних витрат безпосередньо залежить від ресурсів (*гешрейта*) атакуючого і кількості підтверджень, тому ймовірність формування альтернативного (фіктивного) ланцюжка експоненціально зменшується зі зростанням кількості підтверджень та зменшенням гешрейту атакуючого. При цьому, зі збільшенням кількості підтверджень транзакції, зменшується ймовірність її скасування через заміну діючого ланцюжка альтернатив-

ним, який був сформований зловмисником. Однак, з іншого боку, чим більше продавець чекає підтверджень, тим більше затримується проведення самої угоди, що, в підсумку, призводить до певного дискомфорту від використання системи та збиткам взаємодіючих сторін.

В цілому, всі розглянуті атаки є дуже небезпечними саме для децентралізованих систем, тому вони потребують належної уваги зі сторони розробників блокчейн систем та фахівців з питань забезпечення інформаційної безпеки.

Незважаючи на те, що існує багато різних способів зменшення вірогідності успішного проведення відомих атак [16], питання щодо можливості їх повного запобігання все досі залишається відкритим, що обумовлює актуальність досліджень у даному напрямку.

Посилання

[1] Centralized, Decentralized, and Distributed Payment Mechanisms. [Online]. Available: https://www.aier.org/article/centralized-decentralized-and-distributed-payment-mechanisms/

[2] M. Rosenfeld, *Analysis of hashrate-based double-spending*, 2014. [Online]. Available: arXiv preprint arXiv:1402.2009

[3] A. Gervais, H. Ritzdorf, G. O. Karame, S. Čapkun, "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. [Online]. Available: https://doi.org/10.1145/2810103.2813655 https://eprint.iacr.org/2015/578.pdf

[4] E. Zaghloul, T. Li, M.W. Mutka, J. Ren, *Bitcoin and Blockchain: Security and Privacy*, 2019. [Online]. Available: ArXiv, abs/1904.11435

[5] BitcoinWiki: Double-spending. [Online]. Available: https://ru.bitcoinwiki.org/wiki/Double-spending

[6] А. Н. Ширяев, *Вероятность*: В 2-х кн. Кн. 1. Москва: МЦНМО, 2007.

[7] *The Bitcoin Mempool – A Beginner's Explanation*. [Online]. Available: https://99bitcoins.com/bitcoin/mempool/

[8] *Hackernoon: Two Ways to Double-Spend*. [Online]. Available: https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362

[9] *BitcoinCore: CVE-2018-17144 Full Disclosure*. [Online]. Available: https://bitcoincore.org/en/2018/ 09/20/notice/

[10] *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*. [Online]. Available: https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors

[11] H. Finney, *Best practice for fast transaction acceptance - how high is the risk?*. [Online]. Available: https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384, Feb. 2011

[12] *Bitcoin's Security Model Revisited*. [Online]. Available: https://arxiv.org/pdf/1605.09193.pdf

[13] Ch. Everett, *Blockchain Security*. [Online]. Available: https://www.simplexityanalysis.com/blog/2016/9/20/blockchain-security

[14] *The 51% Attack. What is it?* [Online]. Available: https://medium.com/swlh/the-51-attack-what-is-it-d295e70b9ac4

[15] *51% Attack Explained: The Attack on A Blockchain*. [Online]. Available: https://www.fxempire.com/education/article/51-attack-explained-the-attack-on-a-blockchain-513887

[16] П. Колесников, Ю. Бекетнова, Г. Крылов,*Технология Блокчейн. Анализ Атак, стратегии защиты*. [Online]. Available: https://www.mumcfm.ru/repository/7b9dcd8e4e51d467a0f8e1eff82157e504c569331681beb7e80117fd64e05d1a

Reviewer: Vyacheslav Kalashnikov, Dr. of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico.
E-mail: kalash@itesm.mx

Received on November 2019.

Authors:
Eugene Demenko, Computer Science Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: demenjay@gmail.com

Alexander Onikiychuk, Computer Science Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail:onik4524a@gmail.com

Nikita Goncharov, Computer Science Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: wdpgames@yandex.ru

Sergey Datsenko, Computer Science Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: sergdacenko@gmail.com

Nikolay Poluyanenko, Ph.D., Associate Professor, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: nlfsr01@gmail.com

Classification of double cost attack in blockchain system.

Abstract. The article provides a brief overview and systematization of information on the issue of double costs in blockchain systems with probabilistic consensus methods and possible ways to solve it. The procedures using which double-cost attacks are implemented are described. The essence of the manipulations with which an attacker can try to realize double costs in decentralized payment systems is disclosed. A detailed description of the attacker's actions and ways to prevent the attack is given. The review starts with simple attacks based on creating duplicate transactions and ends with more complex attacks such as: attack-Race; Phinea attack attack; Vector76 attack; «51 %» attack. These attacks require significant resources from the attacker and the possibility of branching

the registry blockchain. The last group of attacks is analyzed in more detail with an indication of their use cases. The most dangerous attack is highlighted. The attack «51 %» is highlighted as the most dangerous, which, according to the authors, poses the greatest threat to the safety of blockchain systems with probabilistic consensus algorithms.

Keywords: Computer Networks; Decentralization; Blockchain; Attack; Double Costs.

Рецензент: Вячеслав Калашников, д.ф.-м.н., проф., Технологический университет Монтеррея, Монтеррей, Мексика.
E-mail: kuznetsov@karazin.ua

Поступила: Ноябрь 2019.

Авторы:
Евгений Деменко, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: demenjay@gmail.com

Никита Гончаров, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: wdpgames@yandex.ru

Александр Оникийчук, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail:onik4524a@gmail.com

Сергей Даценко, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: sergdacenko@gmail.com

Николай Полуяненко, к.т.н., доцент кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: nlfsr01@gmail.com

Классификация атак двойных трат в блокчейн системах.

Аннотация. В статье представлен краткий обзор и проведена систематизация информации по проблематике двойных расходов в блокчейн системах с вероятностными методами консенсуса и возможными путями ее решения. Описаны процедуры, с помощью которых реализуются атаки двойных трат. Раскрыта сущность манипуляций, с помощью которых злоумышленник может попытаться провести двойные расходы в децентрализованных платежных системах. Приведено подробные описание действий атакующего и пути предотвращения атаки. Рассмотрение начинается от простых атак, основанных на создании дублирующих транзакций и заканчивается более сложными атаками, такими как: атака-гонка; атака Финеем; атака Vector76; атака «51%». Эти атаки требуют от атакующего значительных ресурсов и возможности разветвления блокчейн реестра. Последняя группа атак проанализирована более детально с указанием вариантов их применения. В качестве наиболее опасной выделена атака «51 %», которая, по мнению авторов, представляет наибольшую угрозу для безопасности блокчейн систем с вероятностными алгоритмами консенсуса.

Ключевые слова: компьютерные сети; децентрализованные системы; блокчейн; атака; двойные траты.