УДК 004.056
DOI: 10.31673/2409-7292.2022.025969

Павлюк А.В., Луценко М.М.

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ТЕХНОЛОГІЇ БЛОКЧЕЙН ВІД КІБЕРАТАК

В статті приведено основні відомості про мережу Блокчейн. Проаналізовано різні види загроз та наведено їх класифікацію. Досліджено методи та засоби використання мережі Блокчейн. Досліджено можливості мережі створеної на основі технології Блокчейн. На основі досліджень проведених в роботі розроблено рекомендації щодо забезпечення захисту інформації при використанні Блокчейну.

Ключові слова: Блокчейн, атака, кібербезпека, методи захисту мережі.

Вступ

Блокчейн – це неперервний ланцюг з блоків в яких записана інформація, ці блоки створюються постійно з деяким інтервалом [1]. А також в кожному блокові, орім самого першого, є інформація про попередній блок. Якщо це Блокчейн, наприклад, криптовалюти Bitcoin то інформація в блоках буде про транзакції та інші дії з цією криптовалютою. Зв'язок між блоками забезпечується не тільки нумерацією, але й тим, що кожен блок містить власну хеш-суму і хеш-суму попереднього блоку. Зміна будь-якої інформації в блоці змінить його хеш-суму. Щоб відповідати правилам побудови ланцюжка, зміни хеш-суми потрібно буде записати в наступний блок, що викличе зміни його власної хеш-суми. При цьому попередні блоки не торкаються. Якщо блок, що змінюється, останній у ланцюжку, то внесення змін може не вимагати істотних зусиль. Але якщо після блоку, що змінюється, вже сформовано продовження, то зміна може виявитися вкрай трудомістким процесом. Справа в тому, що зазвичай копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно одна від одної.

Різновиди атак на Блокчейн

Атак на Блокчейн є доволі багато, але в них всіх одна закономірність чим більше зловмисник бажає отримати, тим більше зусиль йому потрібно витратити. Тому один зловмисник мало на що буде спроможний, та і зусилля не оправдають витрачених сил. Мережа Блокчейн включає вузли, які створюють і запускають транзакції та надають інші послуги. Наприклад, мережа Bitcoin утворена вузлами, які надсилають та отримують транзакції, і майнерами, які додають схвалені транзакції до блоків. Кіберзлочинці шукають уразливості мережі та експлуатують їх за допомогою наступних типів атак.

Атака 51%

Атака 51% відбувається, коли зловмисник у мережі отримує контроль над можливостями майнінгу певного Блокчейну. Це означає, що зловмисники матимуть понад 50% потужності майнінгу і зможуть майнити швидше, ніж усі інші [2].

Зловмисники можуть зупинити підтвердження та замовлення нових транзакцій. Також вони можуть потім переписати частини Блокчейну та скасувати транзакції. Атака 51% зазвичай обходить протоколи безпеки Блокчейну. Вплив атаки може бути легким або серйозним, залежно від потужності зловмисника. Хеш-потужність більш критична в атаках. Якщо зловмисник має більший відсоток, ймовірність атаки на систему також висока. Збитки, завдані атакою, також залежать від того ж фактора. Також зловмисники які мають більше ніж 51 відсоток обчислювальних можливостей можуть створювати свої альтернативні блоки тайком від інших користувачів. Тобто ці альтернативні блоки будуть дійсними адже зловмисник має більшу половину обчислювальних можливостей. Ця атака дозволяє зловмисникам скасувати транзакцію ще до її підтвердження. Це призводить до подвійного витрачання монети. Більше того, справжні майнери заробляють менше за оновлення Блокчейну, оскільки зловмисники крадуть їхні акції.

Але так як всі майнери бажають збільшувати свої заробітки, вони збільшують потужність своєї обчислювальної системи, і тому деякі з них можуть не помітити як перейшли грань в 50% потужності всіх майнерів разом взятих. В такому випадку це не критично поки учасник діє відповідно до правил і не перешкоджає природній роботі

системи. Хоч це і несе шкоду іншим майнерам і робить видобуток невигідним, але якщо транзакції підтверджуються вірно, то користувач не завдає шкоди системі. Атака починається там, де учасник використовує свою перевагу для нечесного видобутку [3].

Атака Фінні

Атака Фінні є варіацією «подвійного витрачання», коли для здійснення угоди очікується не більше одного підтвердження транзакції. Атакуючий готує транзакцію з оплатою товару разом з нею готує блок, що містить транзакцію на переказ цих коштів на інший свій рахунок, але не публікує цей блок у мережі. Як тільки транзакція з оплатою підтверджується одним із майнерів і зловмисник отримує товар, він негайно публікує заздалегідь підготовлений блок у мережу [4].

У цьому випадку в мережі виявляється два ланцюжки блоків однакової довжини. І якщо решта майнерів розвиватиме другий ланцюжок, що містить транзакцію на переказ грошей на рахунок атакуючого, то транзакція переказу грошей продавцю буде відхилена, і, отже, продавець втратить гроші, тому що товар уже був відправлений. Захистом у разі є очікування продавцем деякого достатньої кількості підтверджень транзакцій, що зменшує ймовірність цієї атаки, але не усуває її повністю. Якщо атакуючий має контроль над n вузлами мережі, а продавець очікує менше підтвердження транзакцій, то використовуючи атаку Фінні атакуючий може створити більш довгий ланцюжок з транзакцією, що переводить кошти на контрольований ним рахунок. Після публікації ланцюжка в мережу, майнери продовжувати працювати над довшим ланцюжком, що містить блок з необхідною атакуючою транзакцією. Або ж якщо ланцюжки блоків однакові за довжиною то майнери мають обрати блок, в такому випадка шанс успіху буде рівний 50%.

Race Attack

Атака типу "перегони" (Race Attack). Атакуючий здійснює транзакцію «A», оплачуючи покупку. Одночасно він виконує транзакцію «B», яка переводить ці ж гроші на інший рахунок зловмисника. Якщо магазин не чекає грошей і відвантажує куплені товари, то йде на значний ризик: із ймовірністю 50% транзакція «B» може потрапити в ланцюжок блоків без будь-яких зусиль з боку зломщика. Що ще гірше, він може збільшити цю можливість, вибираючи вузли мережі для передачі тієї чи іншої транзакції. Розрахунки для таких операцій можна знайти у цьому документі [5]. Ця атака схожа з атакою Фінні за своїм принципом, та також є варіацією «подвійного витрачання».

DDoS

Розподілені атаки відмови в обслуговуванні (DDoS) важко виконати в мережі Блокчейн, але вони можливі. Під час атаки на мережу Блокчейн за допомогою DDoS хакери мають намір вивести з ладу сервер, споживаючи всі його ресурси обробки численними запитами. Зловмисники DDoS прагнуть відключити мережеві пули майнінгу, електронні гаманці, криптобіржі та інші фінансові послуги [6]. Блокчейн також можна зламати за допомогою DDoS на прикладному рівні за допомогою DDoS-ботнетів.

Timejacking

Timejacking використовує теоретичну вразливість в обробці часових позначок Біткойн. Під час атаки з використанням таймджакера хакер змінює лічильник часу мережі вузла і змушує вузол прийняти альтернативний Блокчейн. Цього можна досягти, коли зловмисник додає в мережу кілька підроблених однорангових пристроїв з неточними мітками часу. Однак атаці з використанням таймджаку можна запобігти, обмеживши діапазони часу прийняття або використовуючи системний час вузла. Значення часової мітки блоку верифікується не щодо системного часу вузла, а щодо медіанного часу його сусідів – часу мережі. Як визначається час мережі? При встановленні нового з'єднання вузли обмінюються своїм системним часом. Потім кожен вузол обчислює відхилення власного системного часу від системного часу кожного сусіда, а для обчислених відхилень вибирається медіане значення. Отже, власний системний час + медіанне відхилення = час мережі.

Таким чином, зловмисник може маніпулювати значенням часу мережі жертви, підключивши до неї достатню кількість сусідів, що анонсують системний час, який відстає.

Зменшується значення часу мережі жертви — зменшується і верхня межа діапазону допустимих значень тимчасової мітки блоку, що верифікується. Але якщо відхилення часу сусіда перевищує 70 хвилин, його час не буде враховуватися при обчисленні часу мережі. Тому максимальне значення, на яке можна зменшити для жертви, дорівнює 70 хвилин.

Атака маршутизації (Routing attacks)

Зловмисник BGP — це атака маршрутизації, під час якої провайдер перенаправляє інтернет-трафік, рекламуючи фальшиві оголошення в системі маршрутизації Інтернету. Зловмисник може використовувати атаки маршрутизації, щоб розділити мережу на два (або більше) компоненти які не перетинаються. Не дозволяючи вузлам всередині компонента спілкуватися з вузлами за його межами, зловмисник змушує створити паралельні Блокчейни. Після припинення атаки всі блоки, видобуті в меншому компоненті, будуть відкинуті разом з усіма включеними транзакціями та доходом майнерів [7].

Також ця атака може використовуватися, щоб затримати доставку блоку до вузла-жертви на 20 хвилин, залишаючись при цьому повністю непоміченим. Протягом цього періоду жертва не знає про останній здобутий блок і відповідні транзакції. Вплив цього нападу залежить від жертви. Якщо жертвою є торговець, вона схильна до атак подвійних витрат. Якщо це майнер, через атаку він втрачає свою обчислювальну потужність. Нарешті, якщо жертвою є звичайний вузол, він не може зробити внесок у мережу, поширюючи останню версію Блокчейну.

Атака eclipse

Ця атака вимагає, щоб хакер контролював велику кількість IP-адрес або мав розподілений ботнет. Потім зловмисник перезаписує адреси в «випробуваній» таблиці вузла-жертви і чекає, поки вузол-жертви не буде перезапущено. Після перезапуску всі вихідні з'єднання вузла-жертви будуть перенаправлені на IP-адреси, які контролюються зловмисником [8].

Через це жертва не може отримати транзакції, які її цікавлять. При поверхневому розгляді атака «*eclipse»* може здатися схожою атаку Sybil . Хоча в них і є певна схожість – зловмисник поширюватиме в мережі підроблені пули – кінцеві цілі різні. При атаці «*eclipse»* зловмисник прагне того, щоб усі з'єднання жертви виконувались за контрольованими зловмисниками вузлами. Він оточує мету підконтрольними IP-адресами, яких жертва з великою ймовірністю підключиться при перезапуску програмного забезпечення. Перезапуск може бути або примусовим (наприклад, за допомогою DDoS-атаки на ціль) або у зв'язку з іншими обставинами, тоді зловмисник буде лише очікувати доки ці обставини не стануться [9].

Атака Sybil

Sybil Атака є загрозою безпеці в онлайн системі, де одна людина намагається захопити мережу, створивши кілька облікових записів, вузлів або комп'ютерів. Це може бути також просто, як одна людина, яка створює кілька облікових записів у соціальній мережі. Але у світі криптовалют більш підходящим прикладом буде те, що хтось запускає відразу кілька вузлів у blockchain ланцюжку. Слово "Sybil" у своїй назві походить з тематичного дослідження про жінку на ім'я Sybil Dorsett, яка лікувалася від дисоціативного розладу особистості, також званого "множинного розладу особистості" [10].

Мережа Blockchain не має довірених вузлів, і кожен запит надсилається певній кількості вузлів. Тоді жертву оточують фальшиві вузли, які закривають усі їхні транзакції. Нарешті, жертва стає відкритою для атак подвійних витрат. На Рис. 1 зображені вузли мережі Блокчейн. Оранжевим кольором зображені вузли які контролює зловмисник, зеленим зображений вузол жертви на яку проводиться атака, сірими зображені чесні вузли які не підконтрольні зловмиснику [11].

Vector 76 Attack

Всі розроблені технології, включаючи Блокчейн , мають вектори атак, якими кіберзлочинці можуть скористатися для власної вигоди. У криптовалютному світі однією з найменш відомих атак є Vector 76 Attack або Vector Attack 76 . Це тип атаки з подвійними

витратами, яка використовує для виконання невелику помилку в системі консенсусу Біткойн. В результаті цього зловмисник може заволодіти коштами і завдати збитків своїм жертвам [12].

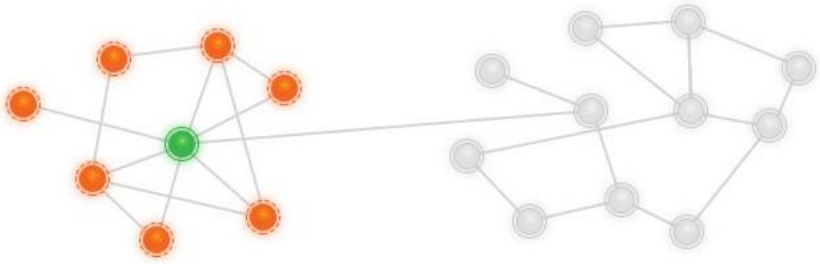

Рис. 1. Схема вузлів при атаці "Sybil"

Ця атака виконується, коли недобросовісний майнер, який контролює 2 повні мережі вузлів, підключає один з них (вузол А) безпосередньо до служби обміну. Потім другий повний вузол (вузол В) з'єднує його з іншими вузлами, які добре розташовані в мережі Блокчейн. Щоб знати, до яких вузлів підключатися, зловмисник повинен контролювати момент, коли вузли передають транзакції, і як вони потім поширюють їх на інші вузли в мережі. Таким чином, він зможе знати, які вузли першими передають операції, і зможе підключитися до цільової служби та з добре розташованими вузлами.

Вразливість подвійної витрати

Подвійні витрати — це поширений спосіб атаки на Блокчейн, який використовує механізм перевірки транзакцій. Усі транзакції в Блокчейні повинні бути перевірені користувачами, щоб бути визнаними дійсними, що вимагає часу. Зловмисники можуть використати цю затримку на свою користь і обманом змусити систему використовувати ті самі монети або токени в кількох транзакціях [13].

Також від цієї атаки пішли інші атаки які були названі вище. На відміну від фінансових установ, Блокчейни підтверджують транзакції лише після того, як усі вузли мережі узгоджені. Поки блок із транзакцією не перевірений, транзакція класифікується як неперевірена. Однак перевірка займає певну кількість часу, що створює ідеальний вектор для кібератак. Як і у випадку з підробленими грошима, такі подвійні витрати призводять до інфляції, створюючи нову кількість скопійованої валюти, якої раніше не було. Це девальвує валюту щодо інших грошових одиниць або товарів і зменшує довіру користувачів, а також обіг та збереження валюти.

Пилові атаки

Шахраї нещодавно усвідомили, що користувачі криптовалют не звертають особливої уваги на ці крихітні суми, що з'являються в їхніх гаманцях, тому вони почали створювати "пилові атаки" з великої кількості адрес, відправляючи їм кілька сатоші. Після атак декількох адрес, наступний крок включає в себе комбінований аналіз цих адрес у спробі визначити, які з них належать одному гаманцю. Мета полягає в тому, щоб в кінцевому підсумку мати можливість зв'язати атаковані адреси та гаманці з відповідними компаніями або приватними особами. У разі успіху зловмисники можуть використовувати ці знання для своїх цілей або для ретельно продуманих фішингових атак або кібер-вимагання [14].

Успішно проведені атаки на Блокчейн та вжиті заходи

Атака 51%

У дрібних мережах повести атаку може і майнер-одинак. Але у великих, де на майнінг кинуті величезні потужності, це під силу лише серйозним майнінг-пулам. Наприклад, у 2014 році відомий майнінг-пул GHash.IO заволодів 55% потужностями мережі Bitcoin . Біткоїн-

спільнота забило тривогу, коли обчислювальні потужності пулу досягли лише 30%. Але буквально за кілька тижнів показник подолав критичний поріг 51% [15].

Самі представники пулу заявили, що атаку здійснювати не збираються, оскільки зацікавлені у подальшому розвитку мережі. Крім того, пул оголосив про тимчасове припинення реєстрації нових учасників та добровільне зниження хешрейту до 40%. Щоправда, із невідомих причин до кінця року GHash.IO взагалі припинив своє існування. Але чому ж майнери, які вже заволоділи необхідними для атаки обчислювальними потужностями, не захотіли використати вразливість такої популярної мережі? Відповідь полягає у негативному впливі атаки 51% на ринкові показники криптовалюти. Також у 2016 році відразу дві криптовалюти, що функціонують на базі Ethereum, Krypton і Shift піддалися атаці від групи хакерів, які іменують себе «Команда 51». В результаті атаки зловмисникам вдалося здійснити подвійне списання коштів і вкрасти через біржу Bittrex 22000 монет. 07.01.2019 з'явилися повідомлення про те, що на блоці 10904146 мережа Ethereum Classic зазнала реорганізації. Її глибина становила 3693 блоків. Тоді розробники висунули припущення, що може йтися про атаку подвійної витрати . Для проведення атаки зловмисник орендував сторонні потужності у сумі 17,5 BTC ($192 000). Перед цим він вивів на кілька гаманців 807 260 ETC ($5,6 млн), ймовірно, з біржової адреси [16].

Далі він почав передавати криптовалюту між своїми гаманцями, включаючи її до здобутих ним самим блоків. На той момент відстежити дії хакера було неможливо, оскільки він зберігав транзакції лише у своїй версії ланцюга, а не публікував їх у Блокчейні. Перемістивши здобуті ETC на біржу, зловмисник конвертував їх у інші активи та опублікував свої транзакції у Блокчейні, що призвело до реорганізації ланцюга.

Атака Фінні

Наприклад, якщо ви збираєтеся прийняти менше 100 євро, з підтвердженням цього може бути достатньо, оскільки вартість атаки буде значно вищою. Атаку Фінні легко виправити на рівні коду, але, незважаючи на це, розробники не зробили цього через серйозну причину: вона вимагає змін, які різко змінюють спосіб обробки консенсусу в мережі і можуть мати небажані наслідки. З цієї причини, а також враховуючи, що децентралізація та збільшення потужності майнінгу роблять цю слабкість надзвичайно важкою для використання, розробники Біткойн не помітили помилку і залишили все як є. Адже «Якщо працює, не чіпай».

Race attack

У грудні 2019 року вірусне відео продемонструвало, що Біткойн витрачається подвійно в місцях, які приймають Біткойн. Ці атаки стали можливими за допомогою Replace-By-Fee (RBF), дещо суперечливе оновлення протоколу Bitcoin. Перша трансакція була надіслана продавцю, а потім друга трансакція з вищою платою. Ця транзакція RBF замінила першу трансакцію, оскільки вища комісія означала, що вона буде оброблятися переважно, що дозволяло витрачати її вдвічі. Ці атаки спрацювали, оскільки продавці приймали непідтверджені трансакції. У аналогічному інциденті раніше того ж року деякі канадські власники біткоїнів переводили в готівку свої Біткойни, фактично не перерахувавши їх.

Атака eclipse

Вони відомі від самого створення перших однорангових мереж. Наприклад, згідно з протоколом Kademlia, він був схильний до таких атак. Важливий момент, що дозволяє уникнути атак Eclipse – мати надійний процес вибору однорангового вузла для мережі. Наприклад, в Ethereum цей процес використовує протокол, заснований на Kademlia. Це дозволяє Ethereum зв'язувати кожен елемент з ключем і зберігатися тільки в тих парах, ідентифікатор вузла яких близький до пов'язаного з ним ключа. Ця «близькість» визначається як двійкова відстань Хеммінга між ключем та ідентифікатором вузла.

DDoS-атаки

У 2017 році Bitfinex постраждав від масової DDoS-атаки . Особливо незручно це було для IOTA Foundation, який запустив свій токен IOTA на платформі за день до того, як Bitfinex повідомив користувачів про атаку. Через три роки, у лютому 2020 року, Bitfinex

зазнав ще одну DDoS-атаку лише через день після того, як криптовалютна біржа помітила подібну атаку [17].

Sybil Attack

Щоб запобігти атакам Sybil, Блокчейни реалізують різні алгоритми консенсусу – наприклад, proof-of-work і proof-of-stake — що збільшує вартість таких атак і робить їх невигідними для потенційних зловмисників. Одним із правил є те, що можливість створення блоку має бути пропорційна загальній обробній потужності механізму Proof of Work. Це означає, що ви дійсно повинні володіти потужністю комп'ютера, необхідною для створення нового блоку, що робить це дуже складним і дорогим для зловмисника.

Способи захисту інформації при використанні Блокчейну

Захист інформації в мережі Блокчейн потрібний тому що при неправильних діях або навіть будівництву цієї Блокчейн мережі, все може піти не так як потрібно. Тому потрібно правильно підбирати модифікації та панелі керування, а також правильно налаштувати систему та точки опори. Все це потрібно налаштовувати під певну ціль, адже Блокчейн мережа яка використовується в криптовалюті не зможе підійти для внутрішніх політик якоїсь компанії. Технологія Блокчейн зі спеціальними протоколами, що допускають різну ступінь анонімності та конфіденційності, може забезпечити захист медичних, фінансових та інших персональних даних, допускаючи при цьому використання цих даних в додатках з штучним інтелектом.

Для початку розглянемо децентралізований Блокчейн. Такі мережі використовуються в криптовалютах, плюси таких мереж в тому що немає того хто може змінити політику створення блоків, або ж змінити інформацію в блоках які були створені. В цих мережах у всіх користувачів рівні права, вони можуть як записувати так і читати інформацію, але при цьому вони можуть змінювати інформацію лише з приводу себе. Також користувачі самі можуть обирати яку інформацію про них зможуть читати інші користувачі. Наприклад, користувач може використовувати Блокчейн з особистою інформацією про здоров'я і розкривати певні елементи цієї інформації виключно для певних цілей (наприклад, отримання рецепта у окуліста) постачальникам товарів або послуг (таких як виробники контактних лінз).

Такі мережі добре підходять для державних установ або ж для кількох компаній які склали між собою договори. Це допомагає зменшувати корупцію та збільшувати довіру людей до цих компаній чи установ, завдяки прозорості систем. В таких мережах, можливо переглянути лише інформацію про транзакції або про дії установ. Наприклад в установі по продажу землі буде видно хто купив собі ділянку та за яку ціну. Для таких мереж рекомендування мати багато вузлів які зможуть правильно функціонувати, також одним з важливих є те що користувачі мають бути обмежені тим яку кількість вузлів вони можуть створювати.

Для користувачів таких мереж рекомендовано спостерігати щоб ваша інформація про вас та ваш обліковий запис не була розповсюджена вами самими. Також не використовувати послуги провайдерів які присвоюють вам IP-адресу та спостерігають за всі вашими діями. Такі провайдери можуть прив'язувати інформацію про ваші дії до вашого облікового запису провайдера. Можливо сам провайдер і не буде використовувати інформацію яку він зібрав, але зловмисники можуть проникнути в бази даних провайдера, та використати інформацію що там зберігається для злочинів. Наприклад для компанії які бажають побудувати Блокчейн мережу в середині своєї компанії, наприклад для перегляду того хто в скільки прийшов на роботу та передачі інформації з приводу роботи та тому подібну інформацію, такий вид мереж не підходить. Для них для таких цілей більш підходить централізована мережа. В таких мережах працює ієрархія, є хтось один хто може робити всі дії з блоками мережі, та є звичайні користувачі, тобто працівники компанії які можуть лише читати інформацію в блоках. Можна наділити правом додавати блоки з інформацією деяких користувачів або ж механізми яким довіряє власник тобто керівник компанії.

Для зберігання інформації в таких мережах потрібно слідкувати за тим щоб користувачі не розповсюджували дані Блокчейну, та не піддавались на хитрощі зловмисників. Рекомендовано часто проводити тренінги та перевірку виконання всіх вимог. Для таких мереж не потрібно багато устаткування та приборів. Але при цьому потрібно слідкувати за цілісністю мережі та за тим щоб мережа була закрита на доступ користувачам з зовні.

Висновок

Захищеність мережі Блокчейну залежить від багатьох факторів, головний фактор – це кількість вузлів які знаходяться в мережі. Чим більше вузлів в мережі тим більша захищеність самої мережі. Користувачі отримують два види ключів, які мають різні функції, один використовується для шифрування, а інший для розшифрування. Тому їхні дані та передавання інформації добре захищені. Також мережа Блокчейн прозора, завдяки чому можна побачити підозрілі зміни, або підозрілі транзакції. Атаки є двох видів, орієнтовані на користувача, та орієнтовані на саму мережу. Користувач може бути атакований атаками типу фішинг, або попавши в ботнет зловмисника. Атакуючи мережу зловмисник має ціль змінити ланцюжок поставок блоків, переписавши блоки так щоб отримати вигоду. Такі атаки є доволі затратними, тому вони дуже рідкісні. Також були не одноразові випадки коли мережа атакувалася користувачами які цього навіть не підозрювали.

Кібербезпека також може використовувати Блокчейн для покращення цілісності даних. Якщо це буде децентралізована мережа Блокчейну то внесення змін до неї буде відбуватись лише після підтвердження правильності інформації іншими учасниками мереж. Технологія Блокчейн може змінити світ дуже сильно, адже ця технологія націлена на автоматизацію більшості процесів які на сьогоднішній день займають багато часу. Також завдяки цій технології є можливість змінити використання інформації про людей, та зменшити кількість не потрібно збираної інформації..

Перелік посилань

1. Загальне поняття Блокчейн: https://uk.wikipedia.org
2. Атака 51 % https://uk.wikipedia.org/wiki/%D0%90%D1%821%51%
3. Understanding 51% attack https://www.section.io/engineering-education/understanding-the-51-attack-on-blockchain/
4. Атака Фінні https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues
5. Атака типу "перегони" https://readli.net/chitat-online/?b=973663&pg=31
6. BLOCKCHAIN DDOS ATTACKS https://halborn.com/how-blockchain-ddos-attacks-work/
7. Routing attacks are pervasive and do divert Bitcoin traffic https://btc-hijack.ethz.ch/#:~:text=An
8. Eclipse https://bytwork.com/articles/eclipse-ataka
9. Атака затамнення https://cryptor.net/bezopasnost/ataki-v-mire-kriptovalyut
10. Слово "Sybil" https://academy.binance.com/ru/articles/sybil-attacks-explained
11. Blockchain Attack Vectors https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors
12. Vector 76 Attack https://academy.bit2me.com/en/which-is-vector-attack-76/#6s
13. Double-spending https://en.wikipedia.org/wiki/Double-spending
14. Новий вид шкідливої активності https://academy.binance.com/uk/articles/what-is-a-dusting-attack
15. Криптовалюти піддаються атаці https://web.archive.org/web/20190115182327/https://cryptonet.biz/ru/ataka-51-naskolko-opasna-i-kak-vliyaet-na-rynok-kriptovalyut/
16. Атака в 2019 https://freemanlaw.com/blockchain-attacks-is-no-one-safe-in-the-world-of-cryptocurrencies/
17. Атака в 2017 на Bitfinex https://bitnovosti.com/2017/11/29/poslednyaya-ddos-ataka-zastavila-ponervnichat-klientov-bitfinex/

Надійшла: 14.06.2022 Рецензент: д.т.н., професор Кожухівський А.Д.