УДК 004.056.5

Миронець І.В.
Черкаський державний технологічний університет

Шкребтій А.В.
Черкаський державний технологічний університет

Борисенко В.А.
Черкаський національний університет імені Богдана Хмельницького

ТЕХНОЛОГІЯ БЛОКЧЕЙН: АНАЛІЗ ЗАГРОЗ ДЛЯ БЛОКЧЕЙН-СИСТЕМ ІЗ МЕХАНІЗМОМ ДОСЯГНЕННЯ КОНСЕНСУСУ

У статті аналізуються та досліджуються поняття криптовалюти та технології, на якій вона будується. Обґрунтовано важливість існування цієї валюти та описано можливості й переваги розглянутих технологій для подальших розвідок у цій галузі. Проаналізовано та висвітлено основні загрози для систем, побудованих на механізмі досягнення консенсусу. Отримано результати, покладені в основу розроблення методу покращення захисту криптовалютних транзакцій на основі вдосконалених блокчейнів.

Ключові слова: *блокчейн, біткоін, криптовалюта, транзакції, майнінг, атака 51%, атака Сібілли, «double-spending» (подвійні витрати).*

Постановка проблеми. 2017 рік став переломним для технологій блокчейн і біткоін. Спираючись на суху статистику, можна сказати, що динаміка зростання ціни на валюту за рік зросла у понад 10 разів. Ґрунтуючись на даних сайту *Coinspot*, можна побачити, що світова спільнота готова до переходу на нову сходинку валютних операцій в Інтернеті.

Проте за умов широкого використання новітніх технологій, основною проблемою пересічних користувачів Інтернету залишається неосвіченість у цьому питанні, а також недовіра до технології.

Блокчейн впроваджується не лише в економічному руслі, а й може стати плацдармом для формування «розумних» контрактів у будь-якій сфері діяльності. Як і всі технології, блокчейн не є досконалою на 100%, тому на неї можуть здійснюватися атаки, про які повинні знати користувачі.

Аналіз публікацій і досліджень. Щоб розібратися в поставленому питанні, потрібно визначити поняття, що стоїть за словом «блокчейн», «біткоін» і «криптовалюта» загалом. У цих термінах легко заплутатися, тому що слова «біткоін» і «блокчейн» можуть позначати будь-яку з трьох частин концепції: базову блокчейн-технологію, протокол і клієнта. Крім того, ці терміни можуть застосовуватися для позначення концепції криптовалюти.

Біткоін – це цифрова готівка. Це одночасно і цифрова валюта, і онлайн платіжна система, у якій технології шифрування забезпечують управління генерацією грошових одиниць і підтвердження переказу коштів, яка працює незалежно від державних центробанків [1, с.20].

Криптовалюта – це цифрова валюта, захищена за допомогою криптографічних технологій. Фізичного аналога у цих грошових одиниць немає, вони існують тільки у віртуальному просторі [2, с.4].

Блокчейн – це технологія надійного розподіленого зберігання записів про всі зроблені біткоін-транзакції. Блокчейн є ланцюжком блоків даних, обсяг якого постійно зростає в міру додавання майнерами нових блоків із записами найостанніших транзакцій, які відбуваються кожні 10 хвилин.

Блоки записуються в блокчейн у лінійному послідовно-хронологічному порядку. На кожному повному вузлі (комп’ютері), підключеному до мережі біткоінів за допомогою клієнта, який виконує перевірку і передання транзакцій, зберігається

копія блокчейна, яка автоматично завантажується, коли майнер приєднується до біткоін-мережі.

У реєстрі зберігається повна інформація про всі адреси і баланси, починаючи з генезис-блоку, тобто найпершого блоку транзакцій, до останнього [3, с.33].

На рис. 1 можна побачити схему транзакції за участю технології блокчейн.

Блокчейн-технологія вважається головною інновацією біткоіну, тому що саме нею послуговуються тим, «що не вимагає довіри» (*trustless*) механізмом верифікації всіх транзакцій у мережі. Принципове нововведення блокчейна полягає в його архітектурі, що забезпечує можливості децентралізованих транзакцій, які не потребують довіри. Замість того, щоб встановлювати і підтримувати відносини довіри з партнером по транзакції (іншою людиною) або стороннім учасником-посередником (наприклад, банком), користувачі покладаються на загальнодоступну розподілену базу даних, яка зберігається на багатьох децентралізованих вузлах і підтримується «майнерами-бухгалтерами».

Блокчейн дозволяє позбутися від «довірених посередників» і повністю децентралізувати транзакції довільних типів між будь-якими учасниками в глобальному масштабі.

Технічно блокчейн-технологія є ще одним прикладним рівнем, вона постачає в Інтернет абсолютно нову ланку підтримки економічних транзакцій: як моментальних грошових платежів в універсальній криптовалюті, так і більш складних і довготривалих фінансових контрактів.

У системі, схожій на блокчейн, можуть відбуватися транзакції з будь-якими валютами, фінансовими контрактами, матеріальними і нематеріальними активами. Більш того, блокчейн може застосовуватися не тільки для транзакцій, а й для фіксації, відстеження, моніторингу та здійснення операцій із будь-якими активами. Це величезна електронна таблиця для реєстрації всіх активів обліковою системою для виконання операцій із ними в глобальному масштабі без обмежень за формою активів, типом учасників або географічним положенням.

Постановка завдання. Основним завданням для проведення цього дослідження є аналіз технології блокчейнів і можливих атак на системи, побудовані на її основі.

Виклад основного матеріалу. ***Атака 51%.*** Щоб закріпити блок у ланцюжку, майнери вирішують обчислювально складне завдання. Той, хто знаходить відповідь першим, отримує право додати інформацію про транзакції користувачів у блокчейн. Розв'язувана обчислювальна задача не просто складна, а її відповідь повинна задовольняти певні умови. Тому малоймовірним є те, що два майнери знайдуть рішення блоку

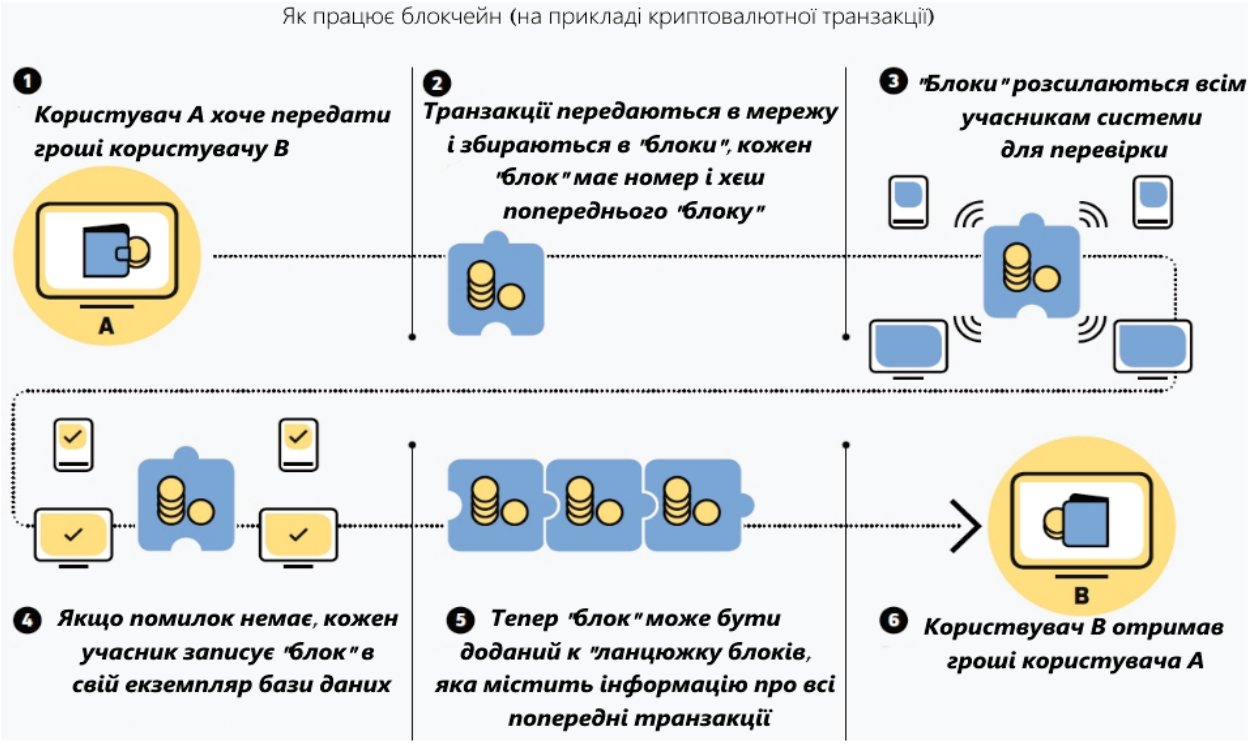

Рис. 1. Схема транзакції за участю технології блокчейн

одночасно. Але така ситуація можлива. У цьому випадку обидва учасники мережі засилають свої блоки в блокчейн, ланцюжок роздвоюється і тому виникає форк. Далі, товариство продовжує майнити і додавати нову інформацію до блокчейну. Кожен наступний майнер пов'язує блок із тим ланцюжком, який, на його думку, буде вважатися основним. Згодом стає зрозуміло, який ланцюг співтовариство визнало валідним – він обирається консенсусом.

Надалі дрібні форки забуваються й ігноруються, а будь-яка інформація, що додається до них підлягає повторному обробленню. Якщо один (або декілька) учасників мережі отримає більшу частину «голосів», то він зможе контролювати консенсус і вносити в блокчейн тільки свої дані. Проте навіть при отриманні переваги в один відсоток над іншою половиною спільноти, дуже складно змінити вже записану інформацію.

Зловмисник може лише добудовувати блоки до потрібних йому гілок. Зазначимо, що реалізувати атаку можна і за менших потужностей (<50%), хоча ймовірність успіху за цих умов різко знижується.

Але ж є ще більш неприємний сценарій: атакуючий може передумати і переписати всю історію генерації блоків, починаючи з деякого моменту в минулому. Як тільки зломщик заволодіє більшою частиною потужностей мережі, то це лише питання часу, коли він наздожене і пережене наступний ланцюжок. У результаті «хороша» транзакція може стати «поганою» і навпаки. Гроші, які ви отримали місяць тому, зникнуть із вашого гаманця і повернуться до їх власника. Таким чином, атакуючий може: «забороняти» включення окремих (або всіх) транзакцій у ланцюжок блоків, скасовувати старі транзакції (повертати гроші) і робити скасовані транзакції дійсними; атакуючий не може контролювати обіг грошей інших людей (перенаправляти або перехоплювати транзакції) і перешкоджати обміну даними між вузлами мережі.

Атака Сібілли. Атака отримала свою назву на честь клінічного випадку, що описує жінку з дисоціативним розладом особистості. За аналогією з цим кейсом, атака Сібілли має на увазі ситуацію, коли один вузол у мережі набуває кілька сутностей. Такий тип атаки найбільш поширений у *p2p*-мережах [4].

Атакуючий намагається «оточити» вузол жертви, заволодіти сусідніми вузлами мережі. Отримавши доступ до вузлів, він контролює всі вхідні і вихідні дані, може передавати «жертві» неправдиву інформацію або не давати їй передавати що-небудь у мережі. Крім того, атакуючий може ідентифікувати транзакції, відправлені вузлом жертви. Як правило, зробити це дуже складно: коди біткоіна й інших криптовалют написані так, що вузол обирає з'єднання з іншими вузлами практично випадково. Навіть у тому разі, коли зломщик контролює 80% усіх вузлів у мережі й нам потрібно встановити 8 випадкових вихідних з'єднань, імовірність опинитися повністю оточеним становить всього $0{,}8^8 = 17\%$.

І все ж це можливо, якщо знати те, як працює алгоритм встановлення з'єднань, використовувати його слабкі місця. Вразливість полягає в тому, що при підключенні до мережі вузол не знає IP-адресу довірених вузлів і не має іншого вибору, окрім як запросити їх у довірених вузлів. Крім того, навіть якщо список довірених вузлів відомий заздалегідь, неможливо підтримувати з'єднання тільки з ними, адже це порушує принципи децентралізованої організації мережі. Якщо блокувати з'єднання з новими вузлами і заборонити їх додавання в список довірених вузлів, мережа буде працювати дуже неефективно (з топологічної точки зору).

Із технічної точки зору кожен вузол зберігає список усіх відомих IP-адрес інших вузлів. Із ними пов'язані такі дані: коли востаннє вузол був у мережі, скільки успішних з'єднань було встановлено з ним і т.д. За необхідності вузли діляться частинами цього списку зі своїми мережами, тим самим оновлюючи інформацію. На початку клієнт намагається розширити своє коло контактів, підключаючись як до відомих вузлів, так і до тих, з якими ще не було з'єднань. Незважаючи на те, що процес носить випадковий характер, зломщик може зробити так, щоб журнал «жертви» містив майже лише адреси атакуючого.

Double-spending. Атака «double-spending» (подвійні витрати) – це атака, яка полягає в тому, що спочатку продавець переконується в тому, що транзакція на оплату була проведена, після чого він передає свій товар, а після отримання товару покупцем створюється нова транзакція, яка і приймається мережею *bitcoin*. У продавця не залишиться ні товару, ні грошей, тому що все буде у зловмисника. Проблема полягає в синхронізації: потрібний певний універсальний сигнал, який указує, що деяка транзакція є кінцевою і жодних інших конфліктуючих транзакцій прийнято не буде.

Розробники *bitcoin* захищають систему, стверджуючи, що подібна атака вимагає дуже високих

обчислювальних ресурсів. Якщо зловмисник все ж має істотні обчислювальні ресурси, то атака можлива. Транзакція має *n* підтверджень, якщо вона включена в блок, який є частиною діючого ланцюжка, і існує *n* блоків, включаючи цей і всі наступні, що йдуть від нього. Уважається, що захистити транзакцію від double-spending може достатнє число таких підтверджень [5].

Атака типу «гонки» (Race Attack). Атакуючий здійснює транзакцію *A*, проводячи фінансову операцію. Одночасно він виконує транзакцію *B*, що переводить ці ж гроші на інший рахунок зловмисника. Якщо магазин не чекає грошей і відвантажує куплені товари, то йде на значний ризик: із імовірністю 50% транзакція *B* може потрапити в ланцюжок блоків без будь-яких зусиль із боку зломщика. Що ще гірше, він може збільшити цю ймовірність, вибираючи вузли мережі для передання тієї чи іншої транзакції.

Егоїстичний майнінг. Ця атака є розвитком попередніх сценаріїв подвійних витрат. У цьому разі метою є не просте шахрайство з фінансовими операціями, а й контроль над мережею за наявності менш ніж 50% потужностей. Усе починається з того, що пул, яким володіє зловмисник, заявляє, що «тут майнінг вигідніше, ніж в інших пулах». Майнери входять у пул і починають майнити, в результаті чого пул отримує 51% потужностей. Звичайно, кожен майнер розуміє, що, приєднуючись до великого пулу, він наражає на небезпеку систему, з якої отримує прибуток. Пул здійснює майнінг таємно і завжди прагне продовжити свій приватний ланцюжок. У певний момент часу останні блоки приватного і публічного ланцюжків можуть виявитися аналогічними, але таке трапляється дуже рідко.

Коли пул знаходить новий блок, який збільшує його приватний ланцюжок, то:

1) у разі, коли ланцюжок блоків на той момент розгалузився, то пул публікує свій власний блок і виграє гонку. Блок, знайдений чесним майнером, стає ізольованим, і їх робота виявляється марною.

2) якщо розгалуження немає, то пул залишає цей блок таємним і продовжує нарощувати свій ланцюжок (тим самим збільшуючи відрив).

Головною метою цієї атаки є порожня витрата ресурсів мережі. Таке трапляється щоразу, коли присутній хоча б один приватний блок: звичайна мережа не знає, що вона відстає, і майн-блоки, з великою ймовірністю, будуть ізольовані. Природно, що пул час від часу буде втрачати гроші, коли він не опублікує власний блок, який ізолюється після програшу.

Висновки. Під час проведення цього дослідження було розглянуто поняття «криптовалюта», «біткоін» та «блокчейн». Проаналізовано та описано основні типи загроз для блокчейн-систем із механізмом досягнення консенсусу. Основними видами загроз або атак на такі системи є: атаки на обчислювальні потужності «Атака 51%» та «Егоїстичний майнінг», «Атака Сибілли», заснована на розгалуженні й підміні достовірної інформації, атака «double-spending», пов'язана з подвійними витратами фінансів користувача, а також «Атака типу «гонки».

Усі вищеперераховані атаки є суттєвими недоліками системи блокчейн, що лежить в основі багатьох криптовалютних транзакцій. Детальний аналіз таких вразливостей покладено в основу розроблення методу захисту криптовалютних операцій на основі вдосконалених блокчейнів, що є метою подальших досліджень.

Список літератури:

1. Блокчейн: Схема новой экономики. Мелани Свои: (перевод с английского). Москва: Издательство «Олимп-Бизнес», 2017. 240 с.

2. Феномен биткоина или все что нужно знать о цифровом золоте. Sirius crypto, 2017. 32 с.

3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Draft. Feb 9, 2016, published by Princeton University Press.

4. Атаки в мире криптовалют. URL: https://cryptor.net/bezopasnost/ataki-v-mire-kriptovalyut. (дата звернення: 28.02.2018).

5. Атаки в мире криптовалют. URL: pingblockchain.com/ataki-v-sviti-kriptovaljut. (дата звернення: 06.03.2018).

ТЕХНОЛОГИЯ БЛОКЧЕЙН: АНАЛИЗ УГРОЗ ДЛЯ БЛОКЧЕЙН-СИСТЕМ С МЕХАНИЗМОМ ДОСТИЖЕНИЯ КОНСЕНСУСА

В статье анализируются и исследуются понятия криптовалюты и технологий, на которой она строится. Обоснована важность ее существования и описаны возможности и преимущества рассмотренных технологий для дальнейших разработок в данной области. Проанализированы и освещены основные угрозы для систем, построенных на механизме достижения консенсуса. Полученные результаты положены в основу разработки метода улучшения защиты криптовалютных транзакций на основе усовершенствованных блокчейнов.

Ключевые слова: *блокчейн, биткоин, криптовалюта, транзакции, майнинг, атака 51%, атака Сибиллы, «double-spending» (двойные расходы).*

BLOCKCHAIN TECHNOLOGY: THREAT ANALYSIS FOR BLOCKCHAIN-SYSTEM WITH CONSENSUS-BUILDING MECHANISM

The article analyzes and explores the concepts of crypto currency and technologies, on which it is built. The importance of its existence is substantiated and the possibilities and advantages of the considered technologies for further developments in this field are described. The main threats for systems built on the consensus mechanism are analyzed and highlighted. The obtained results are the basis for the development of a method for improving the protection of crypto-currency transactions based on advanced block systems.

Key words: *blockchain, bitcoin, crypto currency, transactions, mining, 51% attack, Sybil attack, double-spending.*