

СИСТЕМИ ЗАХИСТУ У КРИПТОВАЛЮТАХ СВІТУ

На сьогодні фінансовий ринок має багато різних криптовалют. Найпопулярнішими криптовалютами є Bitcoin, Ethereum, Litecoin, Monero, Dash. До цього списку можна занести першу криптовату, що була створена в Україні, це – Карбованець (Електронний карбованець). Електронний карбованець (Karbowanec – KRB) – криптовалюта, орієнтована на українського користувача. Вона була започаткована 30 травня 2016 року, оголошення про запуск проекту і початок майнінгу було розміщене на форумі Bitcointalk. Публічної інформації про розробників немає. Працює на технології CryptoNote.

Однією з технологій, що використовується в криптовалютах, є блокчейн. Блокчейн (ланцюжок блоків) – розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Ці дані мають бути захищені від підробки та спотворення: кожен блок містить часову позначку, хеш попереднього блока та дані транзакцій, подані як хеш-дерево.

Існують різні механізми захисту криптовалют. Розглянемо деякі з них, що описані в [1-4].

Протокол доказу з нульовим розголошенням. Він дозволяє захистити інформацію про те, скільки грошей знаходиться на конкретному обліковому записі, блоці розподіленої бази даних. Щоб підтвердити, що транзакція обробляється правильно, необхідне лише повідомити про основні властивості записів, не називаючи конкретних цифр (протокол підтверджує наявність інформації, не розкриваючи її змісту). Так працює доказ з нульовим розголошенням. Використовується з 2014-2015 років.

Доказ виконання роботи. Доказ виконання роботи – Proof-of-work (PoW) є принципом захисту систем від зловживання послугами (наприклад, DoS-атак або розсилок спаму), заснованим на необхідності виконання стороною, яка робить запит (клієнтом), деякої досить складної тривалої роботи (POW-завдання, одностороння функція), результат якої легко і швидко перевіряється стороною, що обробляє запит (сервером). Головна особливість цих схем полягає в асиметрії витрат часу — тривалість для ініціатора запиту і висока швидкість для відповіді.

Підтвердження частки. Підтвердження частки – Proof-of-stake (PoS) є методом захисту в криптовалютах, заснованим на необхідності доказу зберігання певної кількості коштів на рахунку. При використанні цього

методу алгоритм криптовалюти з більшою ймовірністю вибере для підтвердження чергового блоку в ланцюжку обліковий запис з великою кількістю коштів на рахунку. Метод використовують як альтернативу методу Proof-of-work, в якому більшу ймовірність підтвердження блоку має обліковий запис з великими обчислювальними потужностями. Метод був запропонований в 2011.

Криптографічні цифрові підписи. Хоча криптовалютний фінансовий потік не передбачає контролю з боку центрального банку, транзакції теж потрібно підтверджувати цифровим підписом.

Криптографічні хеш-функції. Хеш-функція – це функція, що перетворює входні дані будь-якого (як правило великого) розміру в дані фіксованого розміру. У різних валютах використовуються різні хеш-функції (таблиці 1).

Таблиця 1 – Хеш-функції та методи захисту, що використовуються у криптовалютах

криптовалюта	хеш-функція	метод захисту
Bitcoin	SHA-256d	PoW
Litecoin	Scrypt	PoW
Monero	CryptoNight	PoW
Ethereum	Ethash	PoW

Гомоморфне шифрування. Для збереження анонімності можна застосовувати гомоморфне шифрування. Воно дозволяє виконувати з зашифрованими даними математичні операції, які відповідають результатам обчислень з оригінальними даними. Головне у всіх методах - забезпечити правильну синхронізацію інформації елементів системи. Інакше є ризик заплутатися: деякі комп'ютери будуть вважати, що у вас є певна сума криптовалюти, а інші не побачать грошей на рахунку.

Роботу технології розподілених реєстрів(блокчейну) підтримують майнери. Вони займаються підтвердженням транзакцій, генерацією нових блоків і додаванням їх в блокчейн. У мережах, заснованих на алгоритмі консенсусу PoW, для додавання нового блоку майнеру потрібно проводити складні обчислення, щоб довести виконання роботи.

Така важливість обчислювальних потужностей робить можливим проведення атаки 51%. [5].

Її суть полягає в тому, що кілька майнерів зі значними обчислювальними потужностями (хешрейтом), можуть отримати «контрольний пакет» в мережі, тобто в них у наявності більше всього хешрейту. В результаті вони можуть створювати блоки на свій розсуд,

маніпулювати двосторонніми операціями, не підтверджувати транзакції - це відкриває можливість для багаторазових витрат одних і тих же грошей («подвійні витрати»).

У 2018 році жертвами такої атаки стали шість відомих криптовалютних проєктів.

Проект Electroneum піддався атаці в квітні 2018 року. Цей альткоїн був запущений на базі алгоритму CryptoNight. Після атаки розробникам вдалося підвищити рівень безпеки проєкту.

Монета Bitcoin Gold була атакована двічі - в перший раз 16 травня 2018 року, а потім три дні потому. В результаті збиток перевищив \$ 18 млн, а криптовалютні біржі почали виключати Bitcoin Gold з лістингу.

В кінці травня 2018 року під атакою виявилася мережа монети Litecoin Cash. При цьому розробникам вдалося досить швидко впоратися з цим завданням, що запобігло масштабні втрати.

На початку червня 2018 року жертвою атаки «51 відсоток» стала мережа ZenCash. Зловмиснику вдалося захопити контроль над мережею на кілька годин. В результаті йому вдалося двічі витратити криптовалюту на суму \$ 30 000.

Зломщикам вдалося використати алгоритм Lyra2Re для атаки на мережу криптовалюти Verge. В результаті було викрадено близько \$ 1,4 млн.

Популярна в Японії криптовалюта Monacoin була атакована в травні 2017 року. На момент атаки проєкт використовував алгоритм Lyra2Rev2. Зловмисникам вдалося його зламати, збиток від їх дій був оцінений в \$ 90 000.

Хоча багато вдалих атак було проведено на різні криптовалюти, вони не втрачають свого попиту і залишаються популярними, як от біткойн.

Розглянемо безпеку цей найпопулярнішої криптовалюти світу [6].

Біткойн дозволяє досягти безпрецедентного рівня безпеки. Мережа захищає користувачів від найбільш поширених шахрайств, таких як повернення платежів або неавторизовані списання коштів, а біткойни неможливо підробити. Користувачі можуть створити резервну копію або зашифрувати свої гаманці, а пристрої для зберігання біткойнів можуть в майбутньому зробити крадіжку дуже малоімовірною.

Блокчейн (біткоіну) - це публічний запис всіх біткойн-транзакцій в хронологічному порядку. Ланцюжок блоків єдиний для всіх користувачів біткойнів. Блокчейн застосовує певний набір правил, для генерації нових блоків. Одне з правил полягає в тому, що здатність створювати блок, повинна бути пропорційна загальній обчислювальній потужності механізму PoW. Це означає, що вам фактично необхідно володіти своєю комп'ютерною потужністю, необхідною для створення нового блоку, що робить процес злому дуже складним і дорогим для зловмисника.

У квітні 2014 року Лабораторія Касперського повідомила про зростання вірусних атак, спрямованих на крадіжки біткойнів, в тому числі через крадіжку файлів з ключами (wallet.dat).

Для захисту від збоїв рекомендовано використовувати паперові та / або цифрові бекапи (з можливістю їх зашифрувати і / або зберігати кілька частин в різних місцях).

Для захисту від крадіжки рекомендовано «холодне зберігання» або апаратні засоби захисту. При цьому шифрування гаманця саме по собі не є надійним захистом від троянських програм, оскільки пароль може бути прочитаний через кейлоггер. Холодне зберігання полягає в зберіганні приватного ключа на комп'ютері, що не є підключеним до інтернету, і з можливістю здійснення операцій на комп'ютері, який має підключення до інтернету. Даний метод реалізований, наприклад в Bitcoin-клієнті *Armory*.

Отже, найпопулярнішою валютою вважається біткойн через постійну увагу та цікавість все більшої кількості людей. Система безпеки біткойн постійно оновлюється та вдосконалюється.

Однак гарантувати стовідсотковий захист навіть у біткойні не можливо, в нього як і в інших криптовалютах, атакуючі знаходять слабкі місця, які можуть бути використані для атаки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безопасность криптовалют [Електронний ресурс]. – Режим доступу: <https://postnauka.ru/talks/81984>
2. Доказ виконаної роботи [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Доказ_виконаної_роботи
3. Proof-of-stake [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Proof-of-stake>
4. Список криптовалют [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Список_криптовалют
5. Как взламывают блокчейн и криптовалюты: 6 успешных атак «51 процента» [Електронний ресурс]. – Режим доступу: <https://www.securitylab.ru/blog/company/pt/344915.php>
6. Биткойн#Безопасность [Електронний ресурс]. – Режим доступу: <https://ru.wikipedia.org/wiki/Биткойн#Безопасность>