УДК 004.75

Н. С. Жмуцька

АНАЛІЗ ПРОБЛЕМИ НЕСАНКЦІОНОВАНОГО МАЙНІНГУ КРИПТОВАЛЮТИ

Вінницький національний технічний університет

Анотація

В роботі проаналізовано проблему несанкціонованого майнінгу криптовалюти. Розглянуто поняття блокчейну та криптовалюти, а також використання моделі PaaS для несанкціонованого майнінгу.

Ключові слова: блокчейн, майнінг, криптовалюта, сервер.

Abstract

The problem of unauthorized cryptocurrency mining was analyzed. The concept of blockchain, cryptocurrency, and use of PaaS model for unauthorized mining, were considered.

Keywords: blockchain, mining, cryptocurrency, server

Вступ

Зі зростанням популярності технології блокчейн та криптовалюти, з'являється багато бажаючих заробляти на цьому кошти. Проте хтось це робить використовуючи власні ресурси та кошти, а хтось шукає легкої наживи та використовує чужі ресурси.

Генерування (або майнінг) криптовалюти не можна назвати типовою загрозою інформаційній безпеці, оскільки це не завдає безпосередньої шкоди інформаційним ресурсам, також немає несанкціонованого доступу до інформації, копіювання чи модифікації. Також про цьому не порушується доступність інформації.

Проте несанкціоновані процеси генерування криптовалюти спричиняють надмірне навантаження системи, через що страждає продуктивність.

Основна частина

Криптовалюта - це цифрові гроші, фіатного аналога яким немає. Криптовалюта відрізняється від інших електронних валют тим, що захищена і зашифрована за допомогою спеціальних криптографічних алгоритмів. Головною особливістю криптовалюти вважається її децентралізованість, незалежність від єдиного центру управління.[1]

Всі ці особливості забезпечує технологія блокчейн, на принципах роботи якої і функціонує криптовалюта.

Блокчейн – це серія незмінних записів даних, яка управляється кластером комп'ютерів, які не належать будь-якої одиничної суті. Кожен з цих блоків даних (тобто блок) захищений і прив'язаний один до одного за допомогою криптографічних принципів (тобто ланцюжка).

Мережа блокчейн не має центральної влади - це самовизначення демократизованої системи. Оскільки це загальний і незмінний регістр, інформація в ньому відкрита для всіх і кожного. Отже, все, що побудовано на блокчейні, саме за своєю природою прозоро, і всі учасники несуть відповідальність за свої дії.

Блокчейн не несе транзакційних витрат (вартість інфраструктури - так, але немає витрат на транзакції). Блокчейн - це простий, але оригінальний спосіб передачі інформації від А до В повністю автоматизованим і безпечним способом.[2]

Одна сторона транзакції ініціює процес, створюючи блок. Цей блок перевірений тисячами, можливо, мільйонами комп'ютерів, розподілених по мережі.

Блок містить відомості про транзакції, дерево їхніх хешів, а також заголовок зі службовими даними, де зокрема наведено і хеш попереднього блока, тож кожен наступний блок є також підтвердженням попереднього.

Блок складається із заголовка та списку транзакцій. Заголовок блоку містить свій хеш, хеш попереднього блоку, хеші транзакцій та додаткову службову інформацію. Першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок.

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоці використовується деревисте хешування.

Інформація, що зберігається в блокчейні, існує у вигляді загальної бази даних, що постійно звіряється. Це спосіб використання мережі, який має очевидні переваги. База даних блокчейна не зберігається ні в одному місці, а це означає, що записи, які зберігаються в ній, дійсно є загальнодоступними і легко перевіряються. Ніякої централізованої версії цієї інформації для хакера не існує.

Характеристики криптовалюти:

– адаптивне масштабування. Для криптовалюти існує ряд правил, які забезпечують їх нормальне функціонування в різних масштабах.

Наприклад, алгоритм майнінгу біткоїна коригується залежно від числа здобутих за певний час блоків. Передбачається, що при деяких умовах обмежується час пропозиції, а також зменшується винагорода за майнінг (коли обсяги видобутку сильно збільшуються);

– криптографія. Для криптовалюти використовується особлива система шифрування даних, завдяки якій число створених монет можна тримати під контролем, а також здійснювати транзакції при обміні і розрахунках;

– децентралізованість. Фіатні гроші створюються певними органами, а системи таких валют контролюються з єдиного центру. Криптовалюта ж спирається на однорангові мережі, виключаючи можливість впливати на ланцюжок блоків з однієї точки;

– цифровий характер. Криптовалюта не існує у фізичному вигляді, вона виключно цифрова. Так, криптовалюту можна обміняти на товари або інші види грошей (долари, євро, вебмані), але сама цифрова валюта існує тільки в мережі;

– доказ виконання роботи. Основна маса криптовалюти діє по системі з доказом виконання роботи. Вона являє собою формулу, для підтвердження якої потрібні певні обчислювальні потужності;

– анонімність. Криптовалютні гаманці зашифровані, власники отримують до них доступ за спеціальними ідентифікаторами, ніяк не пов'язаним з особистістю і реальними даними людини. Інформація про транзакції знаходиться в загальному доступі, але дані знеособлені і не ведуть до власника криптовалюти;

– вартість. Ціну криптовалюти визначає кількість роботи, яку потрібно виконати для видобутку токенів, дефіцит і попит на монети можуть цю вартість змінювати.

Такий варіант визначення ціни називається системою з доказом роботи (proof-of-work). Також існує варіант підтвердження монет, заснований на доказі частки володіння (proof-of-stake).

Найпоширенішим способом видобутку криптовалюти вважається майнінг (від mining - добувати).

Головна мета майнінгу – пошук криптографічного підпису до блоку у вигляді хешу. Як тільки він підібраний – блок закривається. А майнер за це отримує винагороду у вигляді криптовалюти.

PaaS або платформа як послуга (англ. Platform as a service) – це один із способів надання клієнту готового програмного середовища. Одночасно надаються інструменти для тонкого налаштування такого середовища.[3]

Модель Platform as a service часто використовують для хмарного майнінгу. Проте багато великих хостинг-провайдерів забороняють майнінг криптовалюти на своїх платформах, оскільки майнінг витрачає багато ресурсів, що погіршує якість надання послуг іншим клієнтам.

Також існує тенденція створювати багато тимчасових безкоштовних облікових записів для майнінгу, що негативно відображається на продуктивності системи.

Тому виникає потреба створити інструмент, який буде своєчасно виявляти та знищувати несанкціоновані процеси генерування криптовалюти на серверах хостинг-провайдерів.

Висновки

В роботі було розглянуто поняття технології блокчейн, її особливості та переваги. Також було проаналізовано поняття криптовалюти та генерування (майнінгу) криптовалюти.

Далі розглянуто використання моделі Platform as a Service, а саме контейнерів, для генерування криптовалюти і зроблено висновок про необхідність створення засобу для виявлення несанкціонованих процесів генерування криптовалюти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бауэр В. П. Блокчейн как основа формирования дополненной реальности в цифровой экономике / В. П. Бауэр, С. Н. Сильвестров, П. Ю. Барышников // Информационное общество. – 2017. – № 3. – С. 30–40.
2. Агеев А. И. Криптовалюты, рынки и институты / А. И. Агеев, Е. Л. Логинов // Экономические стратегии. – 2018. – № 1. – С. 94–107.
3. Что такое PaaS? [Електронний ресурс] – Режим доступу до ресурсу: https://azure.microsoft.com/ru-ru/overview/what-is-paas/

Наталія Станіславівна Жмуцька – студентка групи УБ-18м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: nataliiazhm@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – кандидат технічнихних наук, доцент, Вінницький національний технічний університет, м. Вінниця.

Nataliia Zhmutska - student of UB-18m group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: nataliiazhm@gmail.com

Supervisor: ***Karpinets Vasyl V.*** – Ph.D., Docent, Vinnytsia National Technical University, Vinnytsia.