ЗАСТОСУВАННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ДЛЯ ПОКРАЩЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ БЛОКЧЕЙН-СИСТЕМ

А.О. Попова, студентка ОП « Інженерія програмного забезпечення»
О.М. Любименко, к.ф.-м.н., доцент, доцент кафедри «ПМІ»
Н.О. Маслова, к.т.н., доцент, доцент кафедри «ПМІ»
Донецький національний технічний університет, Луцьк, Україна

Анотація. Блокчейн є розподіленою базою даних, яка зберігає перелік записів, називаних блоками, що пов'язані між собою та захищені від несанкціонованих змін криптографічними методами. Безпека та надійність блокчейн-систем є критично важливою для забезпечення цілісності даних, конфіденційності та захисту від зловмисних атак. Застосування математичних моделей може допомогти покращити безпеку та надійність цих систем.
Ключові слова: блокчейн, безпека, надійність, математична модель, криптографія.

Блокчейн, як надійний механізм для зберігання інформації про різноманітні транзакції, угоди та контракти, відіграє важливу роль в сучасному цифровому світі. Ця технологія, що базується на принципах математики, вже давно перестала асоціюватися виключно з біткоїном і стала основою для створення нових додатків і систем. Вважається, що блокчейн є логічним продовженням традиційних інструментів обліку. Якщо раніше блокчейн розглядали переважно як сховище даних, то тепер його можливості значно розширилися, оскільки він також може виконувати програми. Деякі блокчейни навіть дозволяють кожному запису містити міні-програму. Ця властивість не обмежує сферу застосування блокчейну, а навпаки, розширює його можливості. В основі блокчейну – математика, але це не обмежує сферу його реалізації [1].

Використання математичних моделей може значно покращити безпеку та надійність блокчейн-систем. Ці моделі можуть враховувати різні аспекти, включаючи криптографічні алгоритми, розподіл обчислювальних ресурсів, механізми консенсусу, управління ризиками та масштабованість. Вони базуються на використанні різних математичних інструментів та методів, до яких входять теорія ймовірностей, теорія ігор, теорія графів, криптографічні протоколи та інші.

Одним із головних викликів для блокчейн-систем є їх обмежена пропускна здатність, що стає особливо критичним зі зростанням кількості користувачів та транзакцій. Використовуючи теорію графів, теорію кодування та інші галузі математики, можна розробляти нові способи компактного зберігання даних у блокчейні, а також ефективні механізми для паралельної обробки транзакцій.

Математичні моделі можуть бути використані для аналізу та прогнозування поведінки учасників блокчейн-мережі, що є важливим для забезпечення її стабільності та безпеки. Наприклад, за допомогою теорії ігор можна досліджувати стратегії учасників, їх мотивацію та стимули для чесної або нечесної поведінки. Це може бути використано для розробки більш стійких протоколів консенсусу.

Використання надійних криптографічних алгоритмів, таких як алгоритми з доведеною стійкістю до атак, є ключовим для забезпечення безпеки блокчейн-

систем. Математичні моделі можуть бути використані для аналізу стійкості цих алгоритмів та оцінки ризиків.

Блокчейн-системи покладаються на розподілені обчислювальні потужності для забезпечення консенсусу та валідації транзакцій. Математична модель може допомогти оптимізувати розподіл цих потужностей для підвищення надійності та зменшення ризику відмови.

Різні механізми консенсусу, такі як Proof-of-Work (PoW) або Proof-of-Stake (PoS), використовуються в блокчейн-системах для досягнення узгодженості даних. Математична модель може бути використана для аналізу ефективності та безпеки цих механізмів, а також для розробки нових, більш надійних підходів.

Блокчейн-системи можуть бути вразливими до різних видів атак, таких як атаки подвійної витрати, атаки з використанням квантових обчислень тощо. Математична модель може допомогти оцінити ризики та розробити стратегії для їх мінімізації.

Із зростанням кількості користувачів та транзакцій у блокчейн-системах виникає потреба у масштабованості. Математична модель може бути використана для оптимізації пропускної здатності, часу підтвердження транзакцій та інших показників продуктивності.

Математичні моделі можуть бути використані як для аналізу існуючих систем, так і для розробки нових, більш безпечних та надійних рішень. Одним з прикладів застосування математичної моделі для захисту блокчейн-систем може бути аналіз потенційних загроз, таких як, наприклад, «атака 51%».

Математична модель дозволяє розрахувати імовірність того, що атакуючий зможе надолужити різницю в блоках і навіть набути перевагу над чесними вузлами. Для цього використовується наступна модель:

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases},$$

де p – імовірність чесного вузла знайти наступний блок,

q – імовірність атакуючого знайти наступний блок,

q_z – імовірність того, що атакуючий зможе надолужити різницю в z блоків.

Враховуючи припущення, що $p > q$, то з ростом числа блоків, на яке відстає атакуючий, імовірність експоненційно зменшується. Отже, без вдалого відриву з самого початку, шанси атакуючого на успіх мізерно малі [2].

Цей приклад демонструє, як математичні моделі можуть бути використані для аналізу потенційних загроз і покращення безпеки блокчейн-систем, тому застосування таких моделей може допомогти в розробці нових, більш безпечних та надійних рішень.

Перелік посилань

1. Накамото С. Bitcoin: A Peer-to-Peer Electronic Cash System / С. Накамото. - 2008.
2. Миронець І.В., Шкребтій А.В. Криптографічні алгоритми та особливості їх використання в блокчейн-системах // Український науковий журнал Інформаційна безпека. - 2019. - Том 25, №2. - С. 104-109.