

Abstract. This article provides a comparative analysis of two main types of databases: relational SQL and non-relational NoSQL. It explores their nature, characteristics, and applications. The article highlights the differences in data structure, query languages, schemas, scalability, and other aspects. The comparison helps determine which type of database best suits specific data processing and storage needs.

Keywords: Relational, Non-relational, SQL, NoSQL, Data structure, Scalability.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sem V. Альтернативна наука: SQL чи NoSQL – ось в чому питання. URL: <https://alternativescience.net/programming/242-sql-chy-nosql-os-v-chomu-pytannya/> (дата звернення 06.10.2023 р.).
2. Dou: Типи баз даних: особливості, відмінності та приклади. URL: <https://dou.ua/lenta/articles/types-of-databases/> (дата звернення 06.10.2023 р.).
3. Що таке SQL. URL: https://uk.myservername.com/sql-vs-nosql-exact-differences#What_is_SQL (дата звернення 06.10.2023 р.).
4. Lauren Schaefer. MongoDB: NoSQL vs SQL Database. URL: <https://www.mongodb.com/nosql-explained/nosql-vs-sql> (дата звернення 06.10.2023 р.).
5. Різниця між SQL vs MySQL vs SQL Server. URL: <https://uk.myservername.com/difference-between-sql-vs-mysql-vs-sql-server> (дата звернення 06.10.2023 р.).
6. Огороднік М. О., Зелінська О. В. Переваги та недоліки реляційних та нереляційних баз даних. Прикладні аспекти сучасних міждисциплінарних досліджень: матеріали I Всеукраїнської науково-практичної конференції (м. Вінниця, 26 листопада 2021 р.). Вінниця: ДонНУ імені Василя Стуса. 2021. С. 106–109. URL: <https://jpasmd.donnu.edu.ua/issue/view/403> (дата звернення 06.10.2023 р.).

УДК 004.031.43:336.743-028.63]-047.44

РОЗРОБКА МЕТОДИКИ КОНТРОЛЮ ЗА ОБІГОМ ЦИФРОВИХ ФІНАНСОВИХ АКТИВІВ НА ОСНОВІ АНАЛІЗУ КРИПТОВАЛЮТНИХ ТРАНЗАКЦІЙ

Ю. О. Мазур, Л. В. Загоруйко

Анотація. У статті викладені методики контролю за обігом цифрових фінансових активів на основі аналізу криптовалютних транзакцій з використанням методів машинного навчання. Криптовалюти стали невід’ємною частиною сучасної фінансової системи, і їх обіг постійно зростає. Щоправда, відсутність ефективних засобів контролю та моніторингу може створити ризики для фінансової стабільності та безпеки. У статті пропонується новий підхід до контролю за обігом криптовалют, який використовує алгоритми машинного навчання для аналізу транзакцій та виявлення потенційних порушень.

Ключові слова: криптовалюта, транзакція, машинне навчання, ризики безпеки.

За останні роки цифрові фінансові активи, відомі також як криптовалюти, стали невід’ємною частиною сучасного фінансового середовища. Їх продажі та визнання з боку світової спільноти зростає, і це вже впливає на різні аспекти світових фінансів. Щоправда, зі зростанням популярності цифрових валют також зростає потенційна небезпека їх використання для незаконних операцій, включно з відмиванням грошей, фінансуванням тероризму та іншою злочинною діяльністю. Для забезпечення фінансової стабільності та безпеки необхідно розробити ефективні інструменти для контролю та моніторингу обігу цих цифрових активів. Однією з перспективних стратегій є використання аналізу криптовалютних транзакцій на основі методів машинного навчання. Це дає змогу автоматизувати процес виявлення потенційних порушень і незвичайних дій у світі криптовалют. Аналіз криптовалютних транзакцій може бути важливим інструментом для отримання інформації, яка сприяє виявленню транзакцій, які порушують закони або суперечать офіційній політиці держави в галузі криптовалют [1]. Цей вид аналізу може бути корисним для урядів і відповідних державних органів для виявлення зв’язків між підозрілими транзакціями та конкретними особами, а також для розкриття незаконних схем обігу та використання цифрових фінансових активів та криптовалют. Офіційні особи використовують різні методи та технології для виявлення осіб, які здійснюють незаконні криптовалютні транзакції.

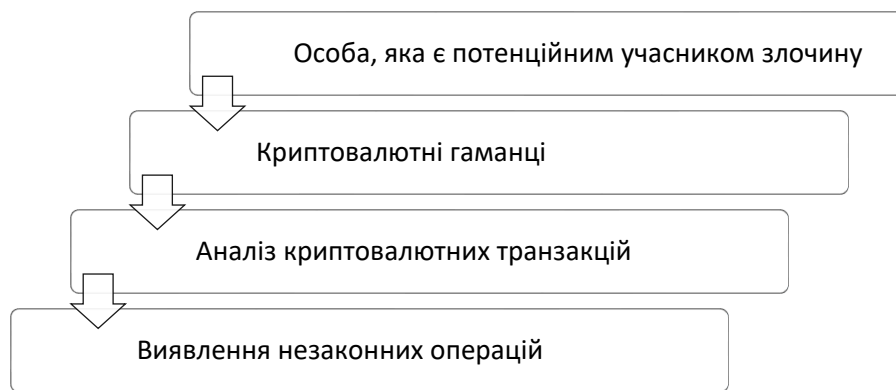


Рис. 1. Схема вияву незаконних операцій [1]

Одним зі способів зниження ризиків є розробка ефективної методики контролю за їх обігом. Така методика повинна дозволити відстежувати транзакції з цифрових фінансових активів та виявляти підозрілі операції. Одним із підходів до розробки методики контролю за обігом активів є використання аналізу криптовалютних транзакцій [2].

- По-перше, криптовалютні транзакції є повністю прозорими та доступними для всіх. Це означає, що їх можна легко відстежувати та аналізувати.

- По-друге, криптовалютні транзакції мають унікальний ідентифікатор, який дає змогу їх легко відстежувати.

- По-третє, криптовалютні транзакції можуть бути легко пов'язані між собою, що дає змогу відстежувати історію коштів.

Аналіз криптовалютних транзакцій може бути використаний для виявлення підозрілих операцій, як-от [3]:

- Транзакції на великі суми грошей, які здійснюються в короткий проміжок часу.
- Транзакції, які здійснюються між пов'язаними сторонами.
- Транзакції, які здійснюються до або після підозрілих подій, як-от теракт або злочин.

Розробка методики контролю за обігом цифрових фінансових активів на основі аналізу криптовалютних транзакцій є складним завданням. Однак це завдання є важливим для забезпечення безпеки фінансових ринків та захисту від злочинності. Основні етапи розробки методики контролю за обігом активів на основі аналізу криптовалютних транзакцій [3]:

1. Вибір методів аналізу криптовалютних транзакцій. На цьому етапі необхідно вибрати методи, які будуть використовуватися для виявлення підозрілих операцій. До таких методів належать:

- Аналіз транзакційних даних. Цей метод полягає в аналізі даних, як-от сума транзакції, відправник, одержувач, час і місце транзакції.

- Аналіз мережевих зв'язків. Цей метод полягає в аналізі зв'язків між різними криптовалютними адресами.

- Аналіз штучного інтелекту. Цей метод полягає в використанні алгоритмів машинного навчання для виявлення підозрілих операцій.

2. Розробка алгоритму виявлення підозрілих операцій. На цьому етапі необхідно розробити алгоритм, який буде використовуватися для виявлення підозрілих операцій на основі обраних методів аналізу.

3. Впровадження методики. На цьому етапі необхідно впровадити розроблену методику в реальну систему контролю за обігом цифрових фінансових активів.

Переваги методики контролю за обігом цифрових фінансових активів на основі аналізу криптовалютних транзакцій:

- високий рівень точності виявлення підозрілих операцій;
- можливість відстежувати історію коштів;
- можливість автоматизувати процес виявлення підозрілих операцій.

Недоліки методики контролю за обігом цифрових фінансових активів на основі аналізу криптовалютних транзакцій:

- висока вартість реалізації;
- можливість обходу системи контролю.

Алгоритми машинного навчання можуть бути використані для виявлення підозрілих криптовалютних транзакцій. Ці алгоритми навчаються на наборі даних, який містить як підозрілі, так і непідозрілі транзакції. На основі цього навчання алгоритми можуть навчитися виявляти ознаки підозрілих транзакцій.

Існує низка різних типів алгоритмів машинного навчання, які можуть бути використані для виявлення підозрілих криптовалютних транзакцій. До таких алгоритмів належать [4]:

- навчання на опорних векторах (*SVM*);
- деревні рішення;
- навчання з ансамблів;
- глибоке навчання.

Алгоритми машинного навчання мають низку переваг перед традиційними методами виявлення підозрілих операцій. До таких переваг належать [5]:

- висока точність виявлення підозрілих операцій;
- можливість адаптації до нових даних;
- автоматизація процесу виявлення підозрілих операцій.

Алгоритми машинного навчання також мають низку недоліків. До таких недоліків належать:

- висока вартість реалізації;
- необхідність великої кількості даних для навчання;
- відсутність прозорості.

Крім виявлення підозрілих операцій, алгоритми машинного навчання можуть бути використані для інших цілей, пов'язаних з контролем за обігом цифрових фінансових активів. До таких цілей можуть належати:

- ідентифікація нових криптовалютних адрес, які можуть бути пов'язані з незаконними операціями;
- виявлення зв'язків між криптовалютними адресами, які можуть бути використані для відмивання грошей;
- профілювання криптовалютних користувачів для виявлення потенційних загроз.

Розробка ефективних алгоритмів машинного навчання для вирішення цих завдань є актуальним напрямом досліджень.

Деякі компанії вже використовують алгоритми машинного навчання для виявлення підозрілих криптовалютних транзакцій [6]. Наприклад, компанія Chainalysis використовує алгоритми машинного навчання для виявлення трафіку, пов'язаного з відмиванням грошей. Компанія Elliptic використовує алгоритми машинного навчання для виявлення зв'язків між криптовалютними адресами, які можуть бути використані для фінансування тероризму.

Розвиток алгоритмів машинного навчання для виявлення підозрілих криптовалютних транзакцій є перспективним напрямом досліджень. Ці алгоритми мають потенціал для підвищення ефективності контролю за обігом цифрових фінансових активів та захисту від злочинності.

Abstract. This research aims to develop a methodology for monitoring the circulation of digital financial assets based on the analysis of cryptocurrency transactions using machine learning methods. Cryptocurrencies have become an integral part of the modern financial system, and their circulation continues to grow. However, the lack of effective means of control and monitoring can pose risks to financial stability and security. In this study, we propose a novel approach to monitoring the circulation of cryptocurrencies by utilizing machine learning algorithms for transaction analysis and the detection of potential violations.

Keywords: cryptocurrency, transaction, machine learning, security risk.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A survey on blockchain security / A. Dorri, M. Steger, P. Tascia, N. Christin. *IEEE Communications Surveys & Tutorials*. 2017. P. 2084–2122.
2. Ferretti A., Gragnani G., Merlo A. Detecting money laundering in cryptocurrencies: A machine learning approach. *In 2017 IEEE 31st International Conference on Data Engineering (ICDE)*. 2017. P. 1433–1444.

3. Hu Z., Luo L., Chen S. A novel deep learning model for detecting fraudulent cryptocurrency transactions. *IEEE Transactions on Information Forensics and Security*. 2020. Vol. 15(11). P. 3200–3212.
4. Li Y., Zhang Y., Yu Y. A hybrid machine learning approach for detecting cryptocurrency money laundering. *IEEE Transactions on Information Forensics and Security*. 2019. Vol. 14(12). P. 2882–2895.
5. Mukherjee S., Sharma S. K. A survey on machine learning techniques for cryptocurrency fraud detection. *In 2021 International Conference on Information Systems Security and Privacy*. 2021. Vol. 16(13). P. 1–9.
6. Okamoto T., Ohta S. Detecting money laundering in bitcoin transactions using machine learning. *In 2017 IEEE Symposium on Security and Privacy (SP)*. 2017. P. 119–134.

УДК 004.6

ЕВОЛЮЦІЯ БАЗ ДАНИХ ІЗ ПОЯВОЮ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

Я. В. Мишківська, В. М. Гончар

Анотація. Ця стаття розглядає вплив технології блокчейн на бази даних, пояснює принципи її функціонування та аналізує, як вона змінює підхід до зберігання та обробки інформації. Зазначаються переваги та недоліки використання блокчейну в цьому контексті, а також надається огляд майбутніх перспектив використання цієї технології в базах даних.

Ключові слова: блокчейн, база даних, децентралізація.

Останніми роками технології блокчейн привертають увагу як наукової, так і практичної спільноти, починаючи від фінансового сектору і закінчуючи сферою медицини та громадської безпеки. Вони суттєво вплинули на еволюцію баз даних, створивши нові можливості та виклики. Стаття має на меті розглянути цей важливий розвиток у контексті баз даних та дослідити вплив технології блокчейн на розробку баз даних.

Бази даних є невід’ємним інструментом сучасного цифрового суспільства і відіграють важливу роль у зберіганні, обробці та доступі до великих обсягів інформації. Їх використовують у багатьох сферах, включно з бізнесом, наукою, медициною та навіть урядовою сферою. Лише вони дають змогу використовувати великий обсяг даних, здійснювати ефективний доступ до даних. Створення баз даних є досить цікавою та важливою частиною розвитку новітніх технологій, тому їх історія не менш цікава. Вона включає в себе численні етапи та відкриття, що створили ті бази даних, які ми маємо сьогодні. Нижче описана коротка історія баз даних:

1. Початок і поява реляційних баз даних (1960–1980-ті роки): перші спроби створення баз даних належать до середини 20 століття, коли комп’ютери тільки починали використовуватися для оптимізації бізнес-процесів та обробки даних. У той час інформація зазвичай зберігалася у формі текстових файлів або карток. Потім у 1960 році Едгар Кодд розробив реляційну модель даних, яка представляла дані у вигляді таблиць і визначала зв’язки між таблицями. Ця модель стала основою для побудови реляційних баз даних.

2. Поява SQL (1980-ті): структурована мова запитів SQL стала стандартом для доступу та управління реляційними базами даних. Це полегшує роботу з даними та робить їх більш доступними.

3. Комерційні СУБД (1980–1990-ті): з появою комерційних систем управління реляційними базами даних (СУБД), як-от Oracle, IBM DB2 та Microsoft SQL Server, надійність та ефективність обробки даних зросли.

4. Розподілені та об’єктно-орієнтовані бази даних (1990–2000-ті роки): з розвитком мережних технологій з’явилися розподілені бази даних, які можуть зберігати та обробляти дані на різних серверах. Поява об’єктно-орієнтованих баз даних пов’язана з потребою в більш гнучкій обробці складних структур даних.

5. «Big Data» та поява NoSQL (2010 – теперішній час): у 21 столітті збільшення обсягів даних і поява «великих даних» привели до розвитку баз даних NoSQL. Ці системи дають змогу ефективно зберігати та обробляти неструктуровані дані, як-от текст, зображення та відео; технології, як-от Hadoop, Mongo DB та Cassandra набули популярності в цьому контексті.

6. Від технології великих даних до блокчейну (сучасність): сучасна історія баз даних також пов’язана з розвитком технології блокчейн. Розпочавшись як розподілений реєстр для крипто-