

АНАЛІТИЧНИЙ ВЕБСЕРВІС ДЛЯ ВИЯВЛЕННЯ РИЗИКОВИХ ТРАНЗАКЦІЙ ЦИФРОВИХ АКТИВІВ НА ОСНОВІ AML ТА KYC

Розвиток цифрових активів і глобальна популяризація криптовалютних технологій сприяли зростанню обсягу транзакцій, що відбуваються поза межами традиційної фінансової системи. Децентралізована сутність блокчейнів забезпечує високу швидкість і доступність операцій, водночас створює серйозні виклики у сфері фінансового контролю та дотримання міжнародних норм боротьби з відмиванням коштів (AML) і політик ідентифікації клієнтів (KYC) [1, 2]. Анонімність та відсутність централізованого управління цифровими активами ускладнюють відстеження транзакцій, що може сприяти їхньому використанню в незаконних схемах, включаючи фінансування тероризму, шахрайства та відмивання грошей.

Попри наявність комерційних інструментів для моніторингу криптовалютних транзакцій, більшість із них мають низку обмежень: недостатня інтеграція із різними блокчейнами, високий поріг входу через значну вартість послуг, а також обмеженість аналітичних алгоритмів для виявлення складних схем фінансових махінацій. Це створює необхідність розробки інноваційного інтегрованого вебсервісу, який дозволить здійснювати поглиблений аналіз транзакцій цифрових активів, автоматизувати процеси ідентифікації ризикованих операцій та відповідати вимогам міжнародного фінансового регулювання.

Вебсервіс автоматизує аналіз транзакцій цифрових активів для виявлення фінансових ризиків, допомагаючи мінімізувати незаконні операції й підвищити безпеку та прозорість крипторинку.

Зі зростанням популярності криптовалют та збільшенням обсягу транзакцій з'явилась потреба у спеціалізованих інструментах для їхнього аналізу та моніторингу. Існує достатня кількість аналогів запропонованого програмного продукту на ринку.

Серед найбільш відомих платформ можна виділити Elliptic, Crystal Blockchain та Check Crypto Address. Elliptic (<https://www.elliptic.co/>) використовує алгоритми машинного навчання для виявлення складних схем відмивання грошей, однак підтримує обмежену кількість блокчейнів і орієнтований переважно на корпоративних клієнтів. Crystal Blockchain (<https://crystalintelligence.com/>) пропонує потужні інструменти візуалізації, що спрощують аналіз транзакцій, але також має обмежену підтримку блокчейнів. Check Crypto Address (<https://checkcryptoaddress.com/>), навпаки, підтримує широкий спектр криптовалют, проте має обмежені аналітичні можливості.

Завдяки проведеному порівнянню, важливими аспектами стали: висока точність аналізу, широка підтримка блокчейнів, зручний інтерфейс, розширені можливості візуалізації, а також застосування методів штучного інтелекту для виявлення ризикових транзакцій.

Дана розробка базується на аналізі транзакцій цифрових активів. Головна його мета – виявити ризикові транзакції, визначити джерела та кінцеві точки руху активів, оцінити «репутацію» гаманців. Основними підходами при цьому стали графовий аналіз та методи машинного навчання. Графовий аналіз дозволяє будувати моделі взаємозв'язків між криптовалютними адресами, що допомагає виявляти підозрілі кластери, циклічні перекази та ключових посередників у транзакційних мережах [3]. Методи машинного навчання застосовуються для автоматизованого виявлення шахрайських схем та нелегальних операцій. Вони ефективні при обробці великих обсягів даних, адже дозволяють аналізувати багатовимірні параметри транзакцій, адаптуючись до нових схем шахрайства. Комбінування методів машинного навчання та графового аналізу забезпечило комплексний підхід до аналізу даних.

Вибір засобів реалізації вебсервісу базується на критеріях продуктивності, безпеки, гнучкості та масштабованості. Серверна частина створена на PHP (Symfony) з API Platform для роботи з запитами. Python разом із бібліотеками використовується для аналізу даних. React забезпечує інтерактивний інтерфейс, MySQL – надійне зберігання даних, Docker – стабільність і гнучкість розгортання, а Nginx виконує роль вебсервера. Така комбінація дозволила досягти балансу між швидкістю розробки, масштабованістю та надійністю вебсервісу.

Список використаних джерел:

1. What Is Anti-Money Laundering (AML)? [Електронний ресурс] - Режим доступу до ресурсу: <https://blog.whitebit.com/en/what-is-anti-money-laundering/>.
2. What Is KYC or Identity Verification, and How Is It Increasingly Important for Crypto? [Електронний ресурс] - Режим доступу до ресурсу: <https://www.binance.com/en/blog/ecosystem/%E2%80%8Bwhat-is-kyc-or-identity-verification-and-how-is-it-increasingly-important-for-crypto-421499824684902130>.
3. Graph Algorithms: Practical Examples in Apache Spark and Neo4j / Mark Needham, Amy E. Hodler, – O'Reilly, 2019. 268 с.