```
Знайдений маршрут: [1, 5, 9, 10, 14, 15, 20]
Загальна вага маршруту: 13
```

Рис. 3. Приклад виконання, вивід у консолі

Отже, оптимізація військової логістики в умовах бойових дій є критично важливим завданням для забезпечення ефективного функціонування збройних сил. Використання алгоритму A* дає змогу значно покращити процес планування маршрутів транспортування боєприпасів, евакуації поранених та переміщення військової техніки, забезпечуючи швидкість, безпеку та гнучкість ухвалення рішень.

Дослідження показало, що алгоритм A* є ефективним методом пошуку оптимальних маршрутів у динамічному та небезпечному середовищі. Його здатність адаптуватися до мінливих бойових умов допомагає швидко перераховувати маршрути та знаходити оптимальне рішення в режимі реального часу. Навіть більше, використання цього алгоритму в автоматизованій системі управління військовою логістикою може значно підвищити ефективність бойових дій і зменшити ризик втрати особового складу та техніки [5].

Подальше вдосконалення алгоритму A* у військових умовах можливе за рахунок інтеграції методів машинного навчання, що дасть змогу прогнозувати потенційні загрози на маршрутах та ще краще адаптувати логістичні рішення до реальних умов бойових дій. Розвиток таких технологій сприятиме підвищенню рівня безпеки та ефективності військової логістики, що є одним із ключових факторів успішного ведення бойових операцій.

Abstract. The article considers the problem of optimizing military logistics in combat conditions using the A* algorithm. The work analyzes the basic principles of the A* algorithm, as well as the features of its application in the military sphere. The adaptation of the algorithm to the realities of combat operations is studied, taking into account the variability of the operational situation, obstacles and risks, such as destroyed infrastructure facilities, minefields and the possibility of enemy attacks. Particular attention is paid to the integration of the A* algorithm into modern automated military logistics management systems, which allows for a prompt response to changes in the combat zone and to ensure the safe and rapid movement of military columns. The possibilities of combined use of A* with other artificial intelligence and machine learning methods to increase the accuracy of forecasting optimal routes are considered.

Keywords: military logistics, A* algorithm, route optimization, automated control systems.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бондаренко О. В., Петров С. І. Алгоритми оптимізації маршрутів у військовій логістиці: теоретичні та прикладні аспекти. Київ: НУОУ, 2020. 256 с.

2. Черненко В. Ю. Використання алгоритмів штучного інтелекту для військової навігації та логістики. *Вісник НТУУ «КПІ». Серія: Інформаційні технології.* 2019. № 12. С. 45–53.

3. Military Logistics and Artificial Intelligence: A Review of Algorithmic Approaches / ed. J. Smith, A. Carter. Cambridge: MIT Press, 2021. 410 с.

4. Дачковський В. О., Сампір О. М. Алгоритм функціонування системи логістичного забезпечення. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 35(2). С. 87–92. URL: https://sit.nuou.org.ua/article/download/178529/178787/395594 (дата звернення: 11.03.2025).

5. Ramezani F., Rajabioun R., Ioannou P. Adaptive Route Guidance: A Model-Based Approach За допомогою Modified A * Algorithm. *IEEE Transactions on Intelligent Transportation Systems.* 2016. Vol. 17, № 3. P. 782–791.

УДК 004.056.53:004.738.1

ТЕХНОЛОГІЯ БЛОКЧЕЙН: ПЕРЕВАГИ, ВИКЛИКИ ТА ЗАГРОЗИ У СФЕРІ КІБЕРБЕЗПЕКИ

Д. М. Єрмак, Л. В. Загоруйко

Анотація. У статті досліджуються можливості та виклики використання технології блокчейн у контексті кібербезпеки. Описано ключові переваги блокчейну, зокрема його децентралізовану природу, прозорість, незмінність транзакцій та стійкість до маніпуляцій.

Ключові слова: блокчейн, кіберзахист, кібератаки.

Вступ. Жодна інформаційна система не може бути повністю захищеною. Те, що сьогодні вважається безпечним, завтра може перестати бути таким, враховуючи постійну винахідливість злочинців у пошуку нових способів атак. Технологія блокчейну постає як один із потенційних шляхів підвищення безпеки в цифровому світі. Блокчейн, з його розподіленою природою, забезпечує новий підхід до зберігання та передачі інформації, що ґрунтується на прозорості, незмінності та колективній верифікації даних. Однак попри свою архітектурну стійкість до маніпуляцій, блокчейн, як і будь-яка інша система, має свої вразливості та виклики.

Актуальність. Блокчейн можна описати як розподілену базу даних, до якої мають спільний доступ різні користувачі комп'ютерів. Дані в блокчейні структуровані в блоки, з'єднані між собою криптографічним ланцюжком. Коли транзакція або група транзакцій додається до блокчейну, блок перевіряється та узгоджується за допомогою механізму консенсусу. Механізм консенсусу передбачає колективну участь деяких учасників у розподіленій мережі. У біткоїні це відбувається за допомогою процесів «майнінгу» та «хешування», які потребують значних обчислювальних потужностей [1].

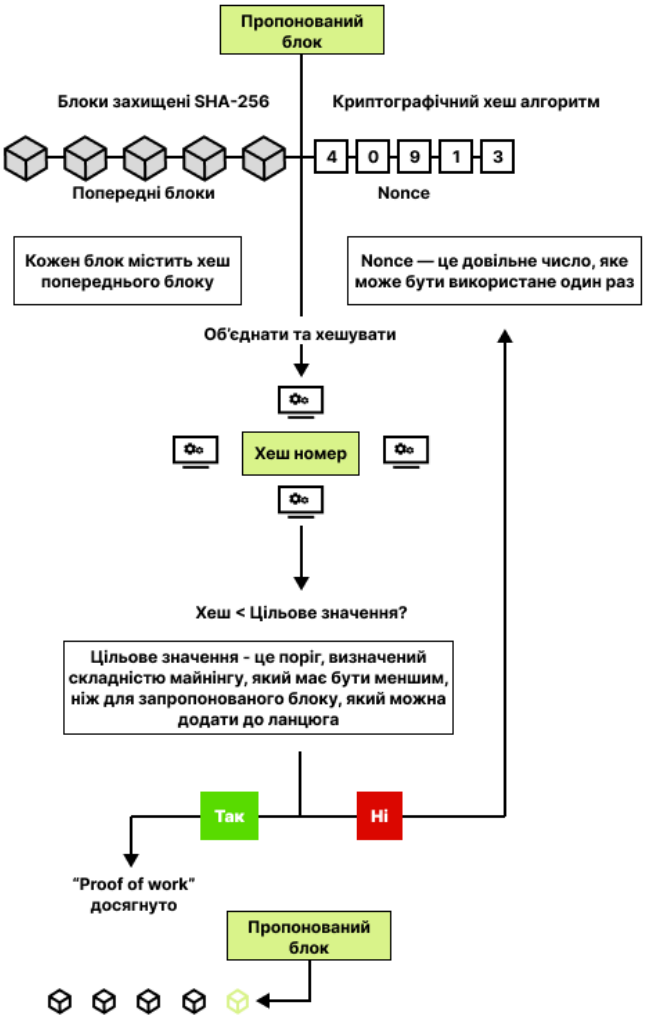

Рис. 1. Схема роботи механізму консенсусу Proof of Work

Цикл роботи блокчейн [2]:

1) користувач надає запит на транзакцію;
2) створюється блок, що представляє транзакцію;
3) блок транслюється до всіх вузлів мережі;
4) усі вузли перевіряють блок;
5) блок додається до ланцюга;
6) транзакція перевіряється та виконується.

Переваги блокчейн-технологій [3]:

1. Блокчейн забезпечує повні, послідовні та актуальні дані без похибок.

2. Однією з найбільших переваг блокчейну є поширення, яке дає змогу спільно використовувати базу даних без центрального органу чи установи. Завдяки децентралізованій природі блокчейну майже неможливо втручатися в дані, на відміну від традиційних баз даних.

3. Блокчейни забезпечують прозорість і незмінність транзакцій, оскільки всі транзакції не можуть бути змінені або видалені.

4. Користувачі можуть легко відстежувати історію будь-якої транзакції, оскільки всі транзакції в блокчейні мають цифрові штампи.

5. Кілька копій даних можуть зберігатися в блокчейні, що дає змогу користувачам уникати зберігання чутливих даних в одному місці.

Недоліки блокчейн-технологій:

1. Блокчейни є дорогими і ресурсомісткими, оскільки кожен вузол у блокчейні повторює завдання для досягнення консенсусу.

2. Транзакція в блокчейні вважається завершеною тільки тоді, коли всі вузли в блокчейні успішно перевіряють цю транзакцію. Це може бути дуже повільним процесом, оскільки вставлений блок потрібно перевірити, щоб усі вузли визнали транзакцію автентичною.

3. Розмір блокчейну зростає з додаванням нового блоку. Вузол повинен зберігати всю історію блокчейну, щоб брати участь у валідації транзакцій, що призводить до безперервного зростання блокчейну. Блокчейн буде рости швидше, якщо у нього будуть великі блоки, і це може розділити майнерів, що вплине на стабільність блокчейну, оскільки стабільність залежить від кількості вузлів у мережі.

4. У блокчейні користувачі перевіряють транзакцію на основі сертифікатної автентифікації, криптовалют тощо. Але немає способу скасувати транзакцію, навіть якщо обидві сторони, залучені до транзакції, готові це зробити, або якщо транзакція зривається з якоїсь причини.

5. Одним із недоліків блокчейну є його складність і заплутаність, що робить його важким для розуміння звичайною людиною. Блокчейн наповнений складними концепціями та процесами, які ще не відшліфовані так, щоб їх міг легко зрозуміти пересічний громадянин, і тому він ще не готовий до масового використання.

Існують три типи блокчейнів [4]:

1) публічний;

2) приватний;

3) консорціуму.

Публічна блокчейн-мережа має відкритий доступ, не встановлюючи обмежень для користувачів. Будь-хто може відправляти транзакції або стати валідатором у цій мережі. Зазвичай такі мережі пропонують економічні стимули для учасників, які забезпечують їхню безпеку, та використовують алгоритми «Proof of stake» або «Proof of work». Одними з найбільших і найвідоміших публічних блокчейнів є Біткоїн і Ефіріум [4].

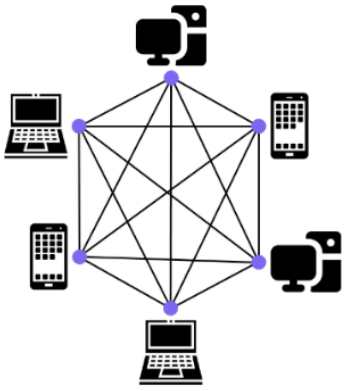

Рис. 2. Публічний блокчейн

Приватні блокчейни є спеціалізованою версією технології блокчейн, призначеною для використання всередині окремої організації або консорціуму. На відміну від публічних блокчейнів, які відкриті для всіх і забезпечують повну прозорість, приватні блокчейни працюють на основі дозволів, надаючи доступ і можливість підтверджувати транзакції лише авторизованим

учасникам. Така модель забезпечує вищий рівень безпеки, конфіденційності та контролю, що робить приватні блокчейни особливо привабливими для бізнесу, який прагне оптимізувати процеси та захистити конфіденційну інформацію [5].

Переваги приватного блокчейну:

– покращена безпека;
– покращена продуктивність;
– енергоефективність;
– масштабованість;
– гнучкість;
– відповідність нормативним вимогам.

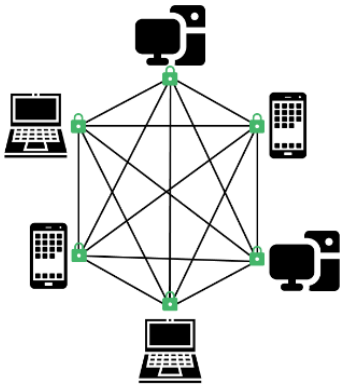

Рис. 3. Приватний блокчейн

Блокчейн консорціуму складається з попередньо вибраного набору вузлів або комп'ютерів, які відповідають для контролю доступу до ресурсів мережі блокчейн. Метою блокчейну консорціуму є усунути єдину автономію приватного блокчейну, маючи кілька суб'єктів або організацій, відповідальних за консенсус і прийняття рішень на користь усієї мережі. Оскільки допускаються лише попередньо відібрані організації для підтвердження транзакцій і консенсусу, в цій мережі стимули не потрібні [6].

Існують чотири основні типи кібератак, до яких вразливі блокчейн-мережі:

1. Атака 51 %. Ця кібератака стосується ситуації, коли група майнерів у мережі блокчейн може отримати контроль над понад 50 % хешрейту майнінгу в мережі. Цей контроль може дозволити їм маніпулювати мережею різними способами. Наприклад, вони можуть заважати новим транзакціям отримувати підтвердження, фактично зупиняючи платежі між користувачами. Вони також можуть скасовувати транзакції, які були завершені, коли вони контролювали, що потенційно може призвести до подвійного витрачання монет [8].

2. Sybil Attacks. Атака Sybil – це тип загрози безпеці, коли одна особа створює кілька шахрайських вузлів у спробі отримати контроль над мережею блокчейну [9].

3. Маршрутна атака. Подумайте про атаку маршруту як про те, що хтось змінює дорожні знаки, щоб неправильно спрямувати вас у небезпечну зону. У контексті блокчейну це описує кібератаку, яка використовує вразливі місця системи маршрутизації мережі блокчейн.

Система маршрутизації блокчейну обслуговує зв'язок між вузлами в ланцюзі та тими, що працюють поза ланцюгом. Зловмисний вузол може порушити цей зв'язок, запустивши атаки на розділення або затримку, що призведе до неефективного та менш безпечного обміну інформацією.

Під час атак із розділенням зловмисник потенційно може фрагментувати мережу на окремі ланцюжки. Технічно вони діють як міст між цими ланцюгами, тобто весь трафік проходить через них. Внаслідок цього виникають паралельні ланцюги. Ця атака може призвести до відмови в обслуговуванні, подвійних витрат (тобто можливості витратити ту саму криптовалюту двічі) і втрати доходу.

У разі атак із затримкою зловмисник затримує доставку нещодавно видобутого блоку до цільового вузла щонайменше на 20 хвилин. Протягом цього періоду часу вузол-жертва не знає про блокування та включені в нього транзакції, що робить атаку практично непомітною. Ця

затримка може спричинити різні проблеми, включно з подвійною витратою та втратою обчислювальних ресурсів майнерами [10].

4. Фішингові атаки – класична техніка онлайн-шахрайства.

Висновки. Технологія блокчейн пропонує інноваційний підхід до зберігання та передачі даних завдяки своїй децентралізованій структурі, прозорості та незмінності транзакцій. Однак незважаючи на свої переваги, вона має певні недоліки, зокрема високі ресурсові вимоги та складність у розумінні і впровадженні. До того ж існують кіберзагрози, як-от атака 51 %, атака Sybil та маршрутні атаки, що можуть порушити функціонування блокчейн-систем. Отже, блокчейн є перспективним інструментом для підвищення безпеки, але не є універсальним рішенням і потребує подальшого вдосконалення.

Abstract. The article explores the opportunities and challenges of using blockchain technology in the context of cybersecurity. The key advantages of the blockchain are described, including its decentralised nature, transparency, immutability of transactions and resistance to manipulation.

Keywords: blockchain, cyber defence, cyber attacks.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Blockchain Security? | Is Blockchain Safe? URL: https://www.kaspersky.com/resource-center/definitions/what-is-blockchain-security (дата звернення: 14.02.2025)

2. Cyber Security in the Blockchain. *UPU-WAPD: Philatelic Webinar December 14, 2021 Crypto & Hybrid Stamps, What future for philately?* URL: https://www.upu.int/UPU/media/upu/DL.PHIL/Presentations/2021%20WADP%20Webinar/1-Cybersecurite-dans-la-Blockchain.pdf (дата звернення: 17.02.2025)

3. Understanding Blockchain Technology. URL: https://www.researchgate.net/publication/336130918_Understanding_Blockchain_Technology (дата звернення: 17.02.2025).

4. Introduction to Blockchain. URL: https://www.researchgate.net/publication/343601688_Introduction_to_Blockchain (дата звернення: 15.02.2025)

5. An Introduction to Private Blockchain. URL: https://www.geeksforgeeks.org/private-blockchain/ (дата звернення: 18.02.2025)

6. Consortium blockchain for security and privacy-preserving in e-government systems / N. Elisa, L. Yang, H. Li, F. Chao, N. Naik. URL: https://iceb.johogo.com/proceedings/2019/ICEB_2019_paper_70_full.pdf (дата звернення: 19.02.2025)

7. Introduction to Blockchain Technology. URL: https://ntiprit.gov.in/pdf/blockchainanddistributed/Blockchain_Introduction_KR.pdf (дата звернення: 19.02.2025)

8. What is a 51 % attack and what are the risks? URL: https://www.coinbase.com/ru/learn/crypto-glossary/what-is-a-51-percent-attack-and-what-are-the-risks (дата звернення: 19.02.2025)

9. What is a sybil attack in crypto? URL: https://www.coinbase.com/ru/learn/crypto-glossary/what-is-a-sybil-attack-in-crypto (дата звернення: 19.02.2025)

10. Routing Attack Meaning. URL: https://www.ledger.com/academy/glossary/routing-attack#:~:text=What%20Is%20a%20Routing%20Attack,a%20blockchain%20network%27s%20routing%20system (дата звернення: 19.02.2025)

УДК: 004.001

СТАТИСТИЧНЕ ДОСЛІДЖЕННЯ ВАЛЮТНОЇ ПАРИ «ЄВРО – ДОЛАР» З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Б. О. Коба, Л. П. Половенко

Анотація. У роботі досліджуються можливості використання штучного інтелекту (ШІ) для аналізу та прогнозування валютних курсів, зокрема валютної пари «євро – долар США». Основна увага зосереджена на застосуванні сучасних методів обробки великих даних, машинного навчання та нейронних мереж. Визначено основні переваги інтеграції ШІ у процеси фінансового аналізу та алгоритмічної торгівлі, що сприяє підвищенню точності прогнозів та ефективному управлінню фінансовими ризиками. Розглянуто методи ARIMA, GARCH і сезонну декомпозицію Холта–Вінтерса, які дають змогу будувати надійні прогностичні моделі валютних курсів.

Ключові слова: штучний інтелект, валютні курси, алгоритмічна торгівля, ARIMA, GARCH, нейронні мережі, сезонна декомпозиція.

Вступ. У сучасних умовах глобалізації та динамічного розвитку фінансових ринків валютний ринок Форекс займає провідне місце за обсягами операцій та рівнем ліквідності. Прогно-