Отже, для захисту радіозв'язку у бойових умовах необхідно враховувати широкий спектр факторів, від апаратних обмежень до криптографічних загроз. Легковагові шифри, динамічне управління ключами та адаптивність до параметрів середовища є основними компонентами сучасних алгоритмів, які забезпечують швидку, надійну та захищену передачу інформації.

Список використаних джерел

1. Шолудько В. Г., Єсаулов М. Ю. Організація військового зв'язку: навч. посіб. Київ: 2017. 112 с.
2. Кутень Р. Б., Синявський О. Ю. Методи і засоби забезпечення стабільності та захисту радіозв'язку в умовах складної електромагнітної обстановки: наукова стаття. Львів: 2024.
3. Головін Ю. О. Основи радіозв'язку з рухомими об'єктами: навч. посіб. Київ: 2016. 14 с.

УДК 004.75:004.021

Ярошенко Б. М., здобувач вищої освіти,
Хмелівський Ю. С., асистент кафедри
інформаційних технологій

РОЛЬ АЛГОРИТМІВ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Блокчейн-технології є ключовим елементом сучасної цифрової економіки, забезпечуючи децентралізацію, прозорість і безпеку. Ці технології стали основою для інновацій, як-от криптовалюти, смарт-контракти та децентралізовані додатки (DApps). Алгоритми відіграють вирішальну роль у функціонуванні блокчейнів, забезпечуючи узгодженість даних, безпеку і масштабованість системи. Основні типи алгоритмів у блокчейні можна розділити на такі категорії:

1. Алгоритми консенсусу – це механізм, за допомогою якого блокчейн досягає узгодженості даних серед усіх учасників мережі без необхідності централізованих регуляторів. Оскільки мережа є одноранговою, процес перевірки транзакцій має бути автоматизованим. Алгоритми консенсусу забезпечують, щоб усі учасники мережі дотримувалися правил і здійснювали транзакції в належний спосіб. Вони також запобігають спробам подвійного витрачання цифрових валют, що є важливим для забезпечення безпеки. Серед найбільш відомих алгоритмів консенсусу – Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) [1].

2. Алгоритми хешування – це математична операція, яка приймає вхідні дані будь-якого розміру, обробляє їх і створює вихідні дані фіксованого розміру, відомі як хеш. У блокчейн-технологіях основними функціями цього алгоритму є підвищення безпеки, оскільки будь-яка зміна даних змінює хеш блоку, роблячи втручання очевидним. Це забезпечує цілісність даних, оскільки наступний блок містить хеш попереднього, і зміна даних у попередньому блоці робить ланцюг недійсним. Хешування також допомагає перевіряти дані – порівнюючи хеш блоку з хешем, на який посилається наступний блок, можна підтвердити, що дані не були змінені [2].

3. Структури даних є важливою частиною ефективної роботи блокчейн-технологій, оскільки правильна організація даних впливає на швидкість і надійність системи. Однією з основних структур є дерево Меркля (Merkle Tree), яке використовується для ефективної перевірки транзакцій у блоці. Завдяки цій структурі зменшується обсяг інформації, яку необхідно зберігати, що забезпечує високу швидкість перевірки. Дерево Меркля дає змогу перевіряти транзакції з мінімальними витратами ресурсів завдяки зменшенню кількості необхідних для перевірки даних. Також важливими є зв'язаний список (Linked List), який можна використовувати для представлення блоків у блокчейн-системі, де кожен блок містить хеш попереднього блоку, що утворює ланцюг [3].

4. Алгоритми пошуку та сортування сприяють ефективному управлінню транзакціями і доступу до даних. Наприклад, сортування транзакцій за розміром комісії дає змогу майнерам обробляти транзакції з найвищим пріоритетом, що оптимізує використання мережевих ресурсів. Для пошуку та доступу до даних використовуються структури, як-от хеш-таблиці, які забезпечують швидкий доступ до таких даних, наприклад, транзакції або баланси рахунків [4].

Алгоритми є основою ефективного функціонування блокчейн-технологій, забезпечуючи безпеку, децентралізацію та прозорість мереж. Основними типами алгоритмів є алгоритми консенсусу (PoW, PoS, PBFT тощо), хешування, а також структури даних, як-от дерево Меркля, що дають змогу ефективно перевіряти транзакції та зберігати цілісність даних. Правильне розуміння і застосування цих алгоритмів критичне для забезпечення стабільності та безпеки блокчейн-систем.

Список використаних джерел

1. Exbase. Алгоритм консенсусу. URL: https://exbase.io/uk/wiki/algoritm-konsensusu (дата звернення 02.12.2024).

2. Plisio. Як працює хешування в блокчейні? 2024. URL: https://plisio.net/uk/blog/how-does-hashing-in-blockchain-work (дата звернення 02.12.2024).

3. Merkle Tree: A Fundamental Component of Blockchains / H. Liu, X. Luo, H. Liu, X. Xia. 2021. URL: https://ieeexplore.ieee.org/document/9588047 (дата звернення 02.12.2024).

УДК 004.414.23:641.5

Кузьміна М. О., здобувачка вищої освіти,
Якубич К. О., асистент кафедри
інформаційних технологій

РОЗРОБКА ПРОГРАМИ ДЛЯ КУХАРІВ НА PYTHON

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. Сучасна кухня все частіше стає місцем впровадження новітніх технологій. Програми для кухарів дають змогу зручно управляти рецептами, формувати списки продуктів, планувати раціон та оптимізувати час. Python, як одна з найпопулярніших мов програмування, пропонує широкий спектр інструментів для створення інтуїтивних та ефективних рішень у цій сфері.