

Визначення поняття блокчейн (blockchain), його види, сфери застосування, позитивні та негативні сторони.

Ілля Кореновський, студент¹ (ORCID:0009-0001-0375-6722)

¹ Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна

АНОТАЦІЯ

У роботі досліджується роль та значення технології блокчейн у сучасному світі, а також її широке застосування в різних сферах. Починаючи з визначення базових принципів блокчейну як децентралізованої технології зберігання даних розглянуто структуру блокчейну, його складові частини. Технологія розглянута через практичне застосування в таких галузях, як логістика, медицина, енергетика та електронне голосування, проведений аналіз переваг блокчейну, зокрема його безпеки, прозорості та стійкості до підробок, а також недоліків, таких як складність технології та значні витрати енергії під час перевірки транзакцій.

Ключові слова: блокчейн, блоки, вузли (ноди), хеш-функції, децентралізація.

1. ВСТУП

У сучасному світі технології відіграють ключову роль у формуванні нових парадигм у різних сферах діяльності. Однією з найбільш інноваційних технологій останніх років є блокчейн. Ця технологія виникла на основі криптографії і швидко набула популярності завдяки своїм унікальним можливостям забезпечення прозорості та безпеки інформації.

2. ВИЗНАЧЕННЯ

Блокчейн - це децентралізована технологія зберігання інформації, яка використовується в управлінні даними, в розробці смарт-контрактів, інформаційних сферах та інших онлайн-додатках. Блокчейн, що походить від англійських слів «block» (блок) та «chain» (ланцюг), представляє собою розподілений реєстр, який зберігає записи у формі послідовно з'єднаних блоків. Кожен блок містить набір транзакцій і інформацію про попередній блок, утворюючи таким чином незмінний ланцюг даних. Цей механізм забезпечує високу стійкість до змін і підробок, що робить технологію блокчейн особливо цінною для фінансових транзакцій, управління ланцюгами постачання, створення смарт-контрактів та багато іншого.

3. СТРУКТУРА БЛОКЧЕЙНУ

Блокчейн - розподілена база даних, що зберігає впорядкований ланцюжок записів, який постійно довшас. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій.

3.1. Блоки

Кожен блок складається з:

- Заголовок Блоку:

*Версія: Ідентифікатор версії блоку.

*Часова позначка: Час, коли блок був створений.

*Кореневий хеш: Хеш всіх транзакцій у блоці.

*Хеш попереднього блоку: Хеш заголовка попереднього блоку, що забезпечують зв'язок між ними.

*Нонси: Значення, яке змінюється під час процесу майнінгу для досягнення правильного хешу.

-Транзакції:

*Вхідні дані: Інформація про джерело коштів, які використовуються в транзакції.

*Вихідні дані: Інформація про нові адреси та суми коштів, які передаються.

*Кількість транзакцій: Кількість транзакцій, що містяться в блоці.

3.2. Ланцюг блоків

*Послідовність блоків: Блоки з'єднані в хронологічному порядку через хеші попередніх блоків, утворюючи ланцюг.

*Незмінність: Зміна будь-якого блоку в ланцюзі вплине на всі наступні блоки.

3.3. Розподілений реєстр

*Вузли: Комп'ютери або пристрої, що зберігають копії блокчейн-реєстру.

*Консенсусний механізм: Процес, який забезпечує єдину версію реєстру серед усіх вузлів.

3.4. Аудит та перевірка.

*Валідація транзакцій: Процес перевірки правильності транзакцій перед їх включенням у блок.

*Перевірка блоків: Процес перевірки правильності нових блоків перед їх додаванням до ланцюга.

4. ВИДИ БЛОКЧЕЙНІВ

4.1. Публічний блокчейн

Публічний блокчейн - це розподілена база даних, що зберігає записи транзакцій або інших даних у вигляді послідовності блоків, які з'єднані в незмінний ланцюг. Доступ до публічного блокчейну відкритий для всіх учасників мережі, і його можна переглядати, перевіряти та додавати нові транзакції. Його основні особливості включають: вільний доступ; прозорість; не має контролюючого центру, тобто функціонує без централізованого органу управління; розподілені вузли; безпека та довіра; захист від змін; автоматизація угод; розподілені додатки.

4.2. Приватний блокчейн.

Приватний блокчейн — це тип блокчейн-мережі, який є обмеженим і контрольованим, на відміну від публічного

блокчейну. У приватному блокчейні доступ до мережі та можливість взаємодії з нею регулюються централізованими або обмеженими правилами. Приватний блокчейн — це блокчейн-мережа, що управляється і контролюється певною організацією або групою організацій, де доступ до мережі та можливість участі обмежені заздалегідь визначеними правилами. Його основні властивості включають: обмежений доступ; контроль та адміністрування; керовані процеси; часто використовують менш ресурсомні алгоритми ніж в публічних блокчейнах; можливість оновлення; безпека та конфіденційність (аналогічно публічним блокчейнам, тільки доступ більш обмежений до даних).

4.3. Гібридний блокчейн.

Гібридні блокчейни є різновидом мережі, яка має елементи як приватних, так і публічних блокчейнів. Вони поєднують у собі безпеку та прозорість загальнодоступних блокчейнів з контролем та конфіденційністю приватних блокчейнів. У гібридному ланцюжку блоків деякі частини мережі можуть бути відкриті для громадськості для перевірки транзакцій, тоді як інші блоки можуть мати обмежений доступ. Гібридні блокчейни забезпечують вищий рівень масштабованості та ефективності порівняно з публічними блокчейнами та дають можливість налаштувати мережу відповідно до конкретних бізнес-вимог.

5. ЯК ПРАЦЮЄ БЛОКЧЕЙН

Блокчейн діє як децентралізована книга даних, яка забезпечує прозорість, безпеку та незмінність за допомогою криптографічних методів, децентралізованих мереж і механізмів консенсусу. Ці властивості роблять блокчейн потужним інструментом для забезпечення довіри та автоматизації в різних сферах.

Спочатку йде ініціація транзакцій. Це коли користувач ініціює транзакцію, наприклад, записує дані або виконує переказ коштів, вона спочатку передається до мережі. Потім транзакція поширюється серед учасників мереж, які перевіряють її на відповідання правилам. Далі йде формування блоку: після перевірки транзакцій, їх групують в новий блок. У публічних блокчейнах новому блоку треба пройти процес консенсусу. У приватних блокчейнах процес може бути спрощеним. Після проходження всіх попередніх процесів, новий блок перевіряється всіма учасниками мережі на відповідність правилам і додається до ланцюга. Після додавання блоку до ланцюга, дані з нього стають частиною незмінного реєстру.

Також обов'язковим пунктом є криптографічний захист. Кожен блок має свій унікальний хеш, який включає інформацію про транзакції та хеш попереднього блоку. Транзакції підписуються цифровими підписами, для того щоб підтвердити їх справжність та авторство. Важлива частина всього ланцюжка-децентралізація. Блокчейн-мережа, яка складається з численних незалежних вузлів, які зберігають копії всього блокчейну, що забезпечує стійкість до збоїв та атак, оскільки дані не зберігаються в одному місці. Наявність нового блоку перевіряється на відповідність всім вимогам перед додаванням його до ланцюга.

6. СФЕРИ ЗАСТОСУВАННЯ БЛОКЧЕЙНУ

6.1. Логістика

Блокчейн можна використовувати для створення захищеного від несанкціонованого втручання запису кожної транзакції, що відбувається в ланцюжку поставок, підвищуючи ефективність, підзвітність і прозорість.

6.2. Медицина

Технологію блокчейн можна використовувати для безпечного зберігання електронних медичних записів і керування ними, а також для відстеження розповсюдження ліків для забезпечення їх автентичності та безпеки.

6.3. Енергетика

Завдяки блокчейну можна розподіляти енергію, управляти та відстежувати розподіл та її споживання, а також створювати смарт-контракти для автоматичного виконання угод про постачання енергії.

6.4. Голосування та демократія

Також блокчейн можна використовувати для електронних голосувань: безпечні та прозорі системи для проведення виборів, а також зменшення ризику фальсифікацій і підробок.

7. ПЛЮСИ Й МІНУСИ БЛОКЧЕЙНУ

7.1. Плюси

Цілісність даних. Технологія блокчейн розроблена таким чином, що блоки та навіть транзакції, додані до ланцюжка, неможливо редагувати, що в кінцевому підсумку забезпечує високий рівень безпеки. Технологія блокчейн використовується для децентралізованого зберігання інформації, що дозволяє будь-кому перевірити точність інформації.

7.2. Мінуси

Базова технологія блокчейн є складною для людей, які не мають технічних знань. Це може перешкодити масовому впровадженню. Також процес перевірки транзакцій в блокчейні споживає велику кількість електроенергії.

Список літератури

- [1] WhiteBIT. Що таке блокчейн? Пояснюємо простими словами. WBblog. 2023. URL: <https://blog.whitebit.com/uk/what-is-blockchain-technology/#heading-28>
- [2] What Is Blockchain? IBM. URL: <https://www.ibm.com/topics/blockchain#:~:text=IBM-,What%20is%20blockchain%3F,patents%2C%20copyrights%2C%20branding>
- [3] Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins. Що таке блокчейн і як він працює? URL: <https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work>.

¹ Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали