Вступ до технології Blockchain

Макар’ян Владислав
Запорізький національний університет
2023

Що таке Blockchain?

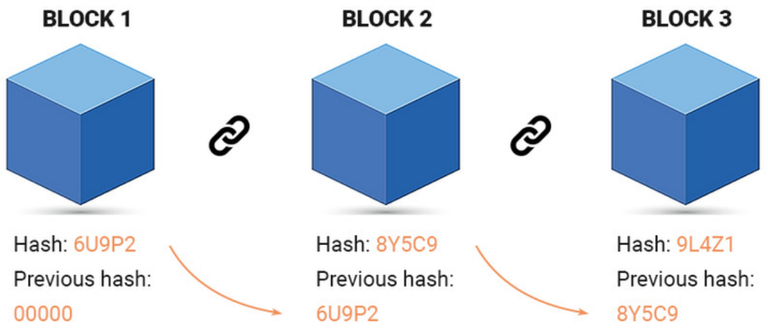
Блокчейн — це децентралізована, розподілена книга, яка записує транзакції через багато комп'ютерів таким чином, що запис не може бути змінений заднім числом без зміни всіх наступних блоків і згоди мережі.

Основні характеристики:

- **Розподілена книга (Distributed Ledger):** Книга ведеться одночасно через мережу багатьох вузлів (комп'ютерів)
- **Незмінні записи (Immutable Records):** Одного разу записані дані в будь-якому даному блоку не можуть бути змінені без впливу на всі наступні блоки, для чого потрібна згода мережі.
- **Децентралізація:** Жодна окрема особа не володіє книгою. Це колаборативний процес, який є прозорим для його учасників.
- **Безпека:** Використовує криптографічні техніки для забезпечення транзакцій і контролю створення нових одиниць.

Чому це важливо:

- Зменшує потребу у довірених третіх сторонах (наприклад, банках, клірингових палатах).
- Підвищує прозорість та відстежуваність транзакцій.
- Має потенціал для прориву в різних галузях, уможливлюючи нові бізнес-моделі.



Історія блокчейну

- Поняття "криптографічної ланцюга блоків" було вперше описане в 1991 році Стюартом Хабером та В. Скоттом Сторнеттом.
- Концепція розподіленої книги існувала до виникнення сучасних блокчейнів.

Bitcoin і Satoshi Nakamoto:

- **2008 рік:** Анонімний(і) особа(и) під іменем Сатоши Накамото публікує white paper, описуючи Bitcoin як "першу децентралізовану цифрову валюту".
- **2009 рік:** Запуск мережі Bitcoin і видобуток першого блоку, так званого "Genesis Block".

Еволюція технології:

- Після біткойна з'явилися інші криптовалюти та блокчейн-платформи, такі як Ethereum, що впроваджують смарт-контракти.

Останні події:

- Зростання секторів DeFi (децентралізовані фінанси) та NFT (не взаємозамінні токени).
- Впровадження блокчейну в різних галузях - від фінансів до логістики.

Основні концепції

Блоки:

- Базова структурна одиниця блокчейну, що містить пакет транзакцій.
- Кожен блок має унікальний хеш-код і посилання на попередній блок, створюючи ланцюг.

Майнінг:

- Процес додавання нових блоків до блокчейну через виконання складних математичних задач.
- Майнери отримують винагороду у формі криптовалюти за кожен успішно доданий блок.

Консенсусні механізми:

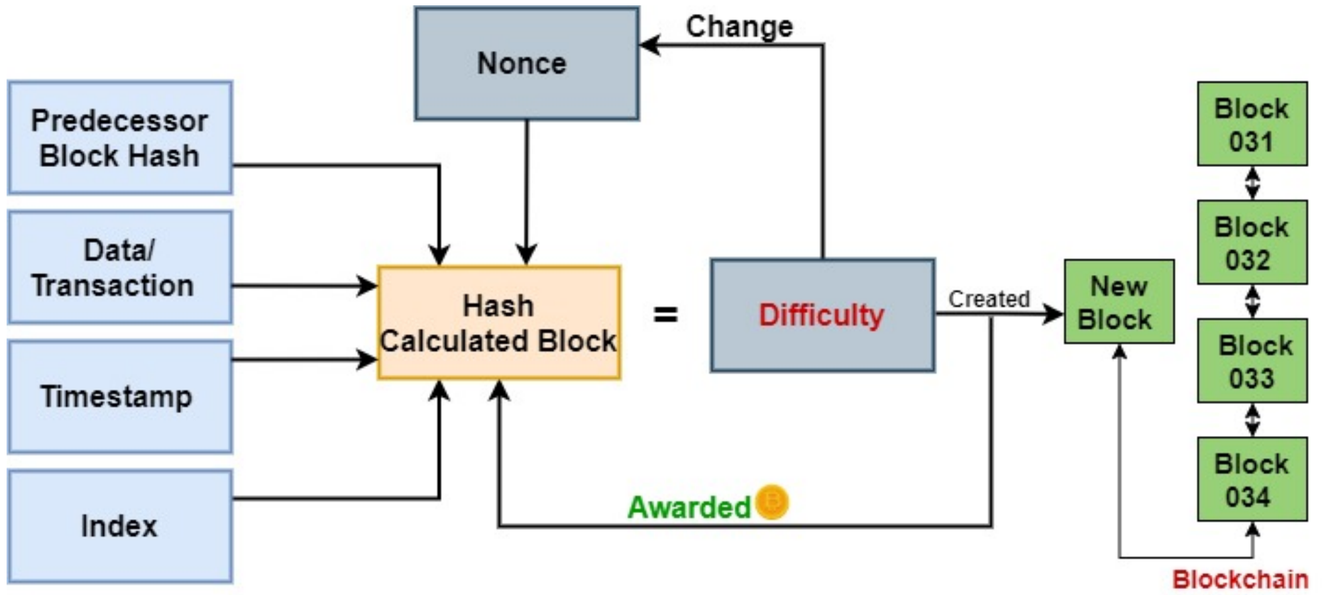
- Алгоритми, що забезпечують узгодження стану блокчейну серед всіх учасників мережі.
- Приклади включають **Proof of Work** (доказ роботи), **Proof of Stake** (доказ володіння) і декілька інших.

Транзакції:

- Записи про пересування активів, можуть бути криптовалютами, контрактами, записами або іншими даними.
- Підтверджуються учасниками мережі перед додаванням до блоку.

Distributed Ledger:

- Всі транзакції розподілені між багатьма комп'ютерами, забезпечуючи високий рівень безпеки і доступності.
- Записи в книзі є незмінними і прозорими для всіх учасників мережі.



Блокчейн і Криптовалюти

Основи криптовалют:

- Криптовалюта - це цифровий або віртуальний актив, що використовує криптографію для захисту транзакцій.
- Блокчейн служить як розподілена книга для всіх транзакцій криптовалюти.

Функціонування криптовалют:

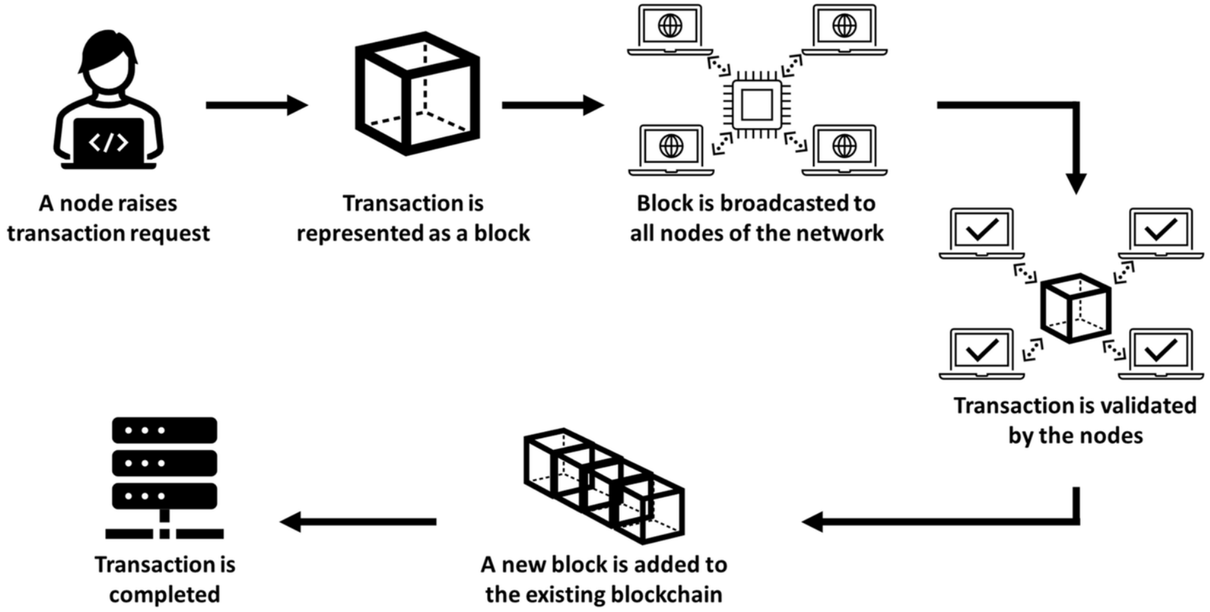
- Криптовалюти використовують блокчейн для створення децентралізованої середовища, де не потрібен центральний авторитет.
- Майнінг або інші консенсусні механізми забезпечують валідацію транзакцій і генерацію нових монет.

Безпека та прозорість:

- Блокчейн забезпечує високий рівень безпеки транзакцій завдяки криптографічним методам.
- Всі транзакції є прозорими і перевіреними, що зменшує можливість шахрайства.

Bitcoin і Ethereum:

- Bitcoin: Введений в 2009 році як перша децентралізована криптовалюта, яка використовує блокчейн.
- Ethereum: Розроблений для розширення використання блокчейну за допомогою розумних контрактів та DApps.



Смарт-контракти та Децентралізовані Додатки (DApps)

Смарт-контракти:

- Смарт-контракт - це самодостатня програма, яка зберігає умови контракту в блокчейні.
- Вони автоматично виконують, контролюють або документують юридично значущі події або дії відповідно до коду умови.

DApps:

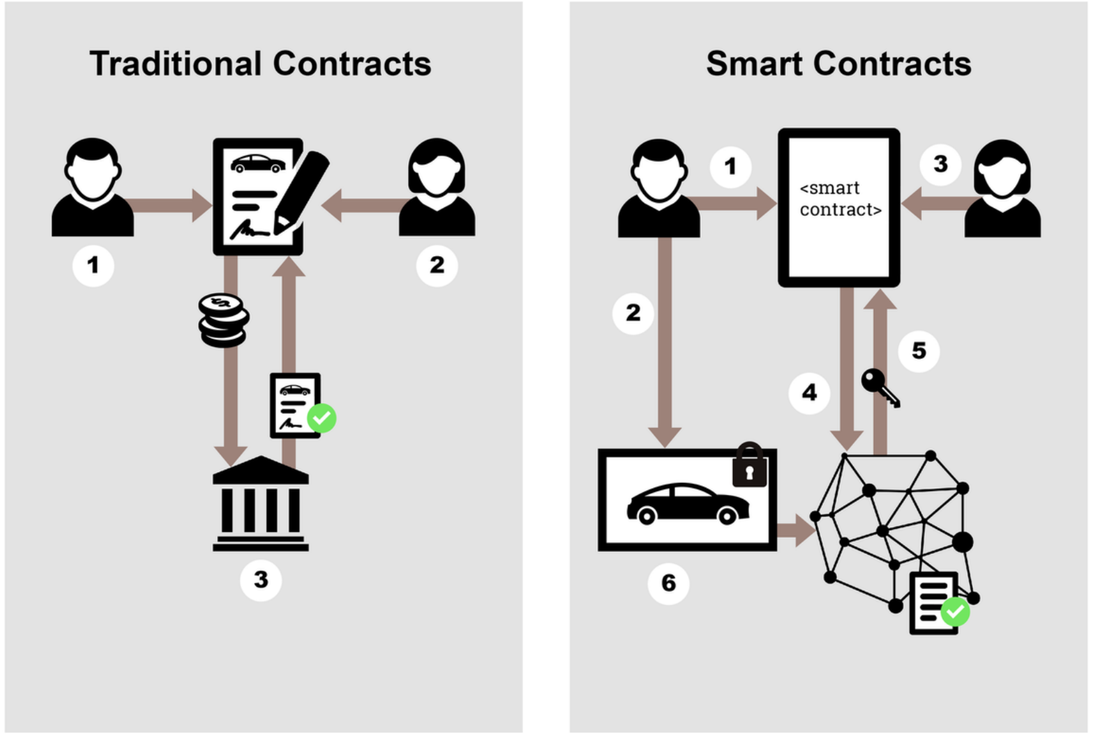
- Додатки, що функціонують на блокчейні і використовують смарт-контракти для автоматизації процесів.
- Можуть працювати на будь-якій блокчейн платформі, але популярні на Ethereum, EOS, Tron та інших.

Приклади DApps:

- Децентралізовані фінансові сервіси (DeFi), ігри, торгові платформи, соціальні мережі.
- CryptoKitties, Uniswap, Compound як приклади популярних DApps.

Значення DApps:

- Відкриття нових можливостей для безпечних та прозорих фінансових транзакцій.
- Революція в традиційних галузях завдяки децентралізації процесів.



Обмеження Блокчейну

Масштабованість:

- Виклики з обробкою великої кількості транзакцій одночасно.
- Проблеми із затримкою та високі комісії в мережах, таких як Bitcoin та Ethereum.

Енергоспоживання:

- Критика механізму консенсусу Proof of Work за його велике енергоспоживання.
- Пошуки альтернативних, більш екологічно чистих механізмів консенсусу.

Регулювання:

- Невизначеність у регулюванні блокчейну може стримувати його прийняття та інтеграцію.
- Виклики у відповідності до нормативних вимог у різних країнах.

Безпека та Конфіденційність:

- Хоча блокчейн вважається безпечним, існують ризики "51% атак", фішингу та інших видів махінацій.
- Проблеми з приватністю в публічних блокчейнах, де транзакції є прозорими.

Інтероперабельність:

- Взаємодія між різними блокчейнами залишається технічно складною.
- Відсутність стандартів для спілкування блокчейн платформ між собою.