# Тема 16. Технологія блокчейн на прикладі біткоїн

## 5.1. Основи блокчейну

Технологію блокчейн описано в статті Сатоши Накамото «[Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf)». Там на восьми сторінках автор описав основи криптовалюти Біткоїн, в основі якої покладено алгоритм Блокчейна.

***Блокчейн з'явився разом з Біткоїном, але може використовуватися незалежно від нього і навіть модифікуватися. Будь-хто може зробити свій блокчейн в себе на ноутбуці.***

Блокчейн – це ланцюжок блоків або [зв’язний список](https://ru.wikipedia.org/wiki/Связный_список). В такому списку кожний наступний запис посилається на один попередній і так за ланцюжком до найпершого. Як вагони потягу, кожен тягне за собою наступний. З приводу списків є [стаття](https://tjournal.ru/41306-samoe-ponyatnoe-obyasnenie-principa-raboty-blokcheyna), де є пояснення для початківців. Аналогії частково взяті звідти.

#### Пояснення на прикладі

Друзі Олега постійно позичають в нього гроші. Олег добрий, але вкрай забудькуватий. За тиждень він вже не пам'ятає хто не повернув йому борг, але соромиться про це питати. Тому, одного разу він вирішив покласти цьому край, і сформував список друзів, яким позичав гроші.

1. ПОЗИЧИВ МАКСУ 100 ГРИВЕНЬ
2. ПОЗИЧИВ ІВАНУ 500 ГРИВЕНЬ
3. МАКС ВІДДАВ 50 ГРИВЕНЬ
4. ПОЗИЧИВ ІВАНУ 200 ГРИВЕНЬ
5. МАКС ВІДДАВ 50 ГРИВЕНЬ

Тепер Олег завжди може за списком переконатися, що Макс все повернув, а Іван не віддає вже 700 гривень. Одного разу Іван приходить до Олега і потайки затирає запис «Позичив Іванові 200 гривень» і вписує замість неї «Іван віддав 500 рублів».

Довіряючи своєму списку Олег забуває про борг і втрачає 700 рублів. Він вирішує якось з цим боротися.

У минулому році Олег ходив на курси з програмування, де йому розповіли про [хешування](https://ru.wikipedia.org/wiki/Хеширование). Він пам'ятає, що будь-який рядок можна перетворити в однозначний набір символів - хеш, і зміна будь-якого символу рядка повністю його змінить.

Хешування (англ. hashing) — перетворення масиву вхідних даних довільної довжини у (вихідний) бітовий рядок встановленої довжини, що виконується за певним алгоритмом. Функція, що реалізує алгоритм і виконує перетворення, називається «хеш-функцією» або «функцією згортання». Початкові дані називаються вхідним масивом, «ключем» або «повідомленням». Результат перетворення (вихідні дані) називається «хешем», «хеш-кодом», «хеш-сумою», «згорткою повідомлення».

Наприклад, на вхід 128-битної хеш-функції можна подати як багатосторінковий документ так і один символ. На виході в обох випадках утворюються різні набори псевдовипадкових шіснадцяткових цифр виду: «c4ca4238a0b923820dcc509a6f75849b».

Наприклад, додавання точки в кінці змінило підсумковий хеш до невпізнання - цим можна скористатися.

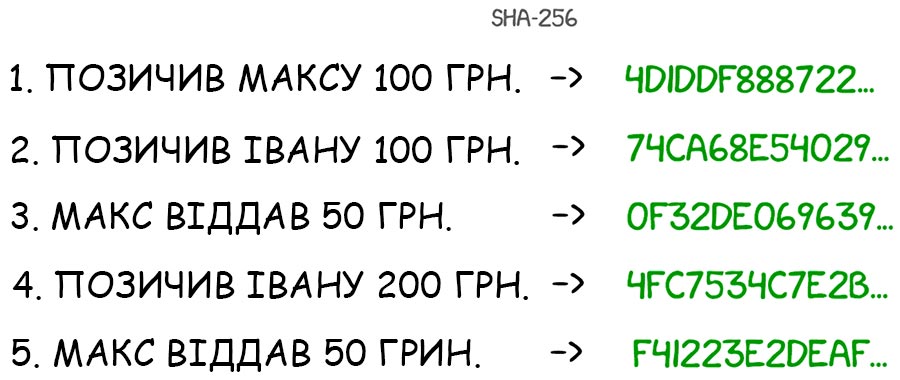
Рядок: Олег

Хеш: f3b6151d5a0734ab2af432d46071ec73dccb06175609fbeab19de8ceafbafd31

Рядок: Олег.

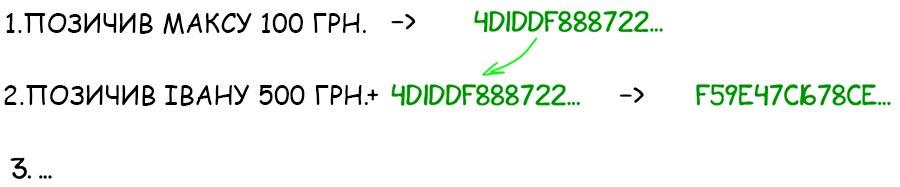
Хеш: 046ad15c460e409aa340b0e67a05a1ec75f6cb44430053c3c46192a3bb8cdf55

Олег бере загальновідомий хеш [SHA-256](https://ru.wikipedia.org/wiki/SHA-2#SHA-256) і хешує ним кожен запис, дописуючи результат в кінці. Тепер, Олег може упевнитися, що його записи ніхто не змінював, якщо захешувати ще раз і порівняти з попередніми результатами.



Але Іван теж знає про SHA-256 і легко може змінити запис разом з її хешем. Особливо, якщо хеш написаний прямо у списку.

Тому, для більшої безпеки Олег вирішує хешувати не лише сам запис, а складати його разом з хешем від минулого запису. Тепер, все записи залежать від попередніх. Якщо змінити хоча б один рядок, то доведеться перерахувати хеши всіх інших записів, що є нижче за списком.



Так в Олега з'являється особистий зв'язний список.

Але одного разу Іван прокрадається вночі, змінює потрібний йому запис і оновлює хеші для всього списку до кінця. В нього це займає кілька годин, але Олег все одно міцно спить і не чує. Ранком Олег виявляє абсолютно вірний список - все хеши збігаються. Але Іван все одно його обдурив, хоч і витратив на це безсонну ніч. Як ще можна захиститися?

Олег вирішує якось ускладнити йому життя. Тепер для додавання нового запису в список, Олег вирішуватиме пов'язане з ним складне завдання, наприклад математичне рівняння. Відповідь буде додаватися до підсумкового хешу.

Олег сильний в математиці, але навіть в нього на додавання запису йде по десять хвилин. Незважаючи на це, витрачений час того вартий, адже якщо Іван знову захоче щось змінити, йому доведеться заново вирішувати рівняння для кожного рядка, а їх можуть бути десятки. На це піде багато часу, адже рівняння кожен раз унікальні і пов'язані з конкретним записом.

Зате перевірити список все так же просто: спочатку потрібно як раніше порівняти хеші, а потім перевірити рішення рівнянь простою підстановкою. Якщо все збігається - список не змінений.

В реальності ж з рівняннями не все так добре: комп'ютери занадто добре їх вирішують, та й де зберігати стільки унікальних рівнянь. Тому, автори блокчейну придумали більш красиве завдання: потрібно знайти таке число (**nonce**), щоб підсумковий хеш всього запису починався на певну кількість нулів. Такий nonce складно знайти, зате результат завжди можна перевірити просто очима.

Таким чином, для підтвердження виконаної роботи з майнінгу, хеш блоку повинен задовольняти поточним умовам мережі - містити певну кількість початкових нулів, що змінюється з часом.

<https://hashes.com/ru/generate/hash>

Тепер Олег звіряє все хеши і додатково переконується, щоб кожен починався на обумовлену кількість нулів. Іван, навіть озброївшись потужним ноутбуком, не встигне за ніч перерахувати всі хеші так, щоб вони задовольняли умові - забракне часу.

Такий список по суті і є домашнім блокчейном. Його безпека гарантована математиками, які довели, що ці хеши не можна обчислити швидше, крім як перебором. Такий перебір хешів до кожного запису і є Майнінгом.

### Централізація довіри

Ідея вести захищений список «хто кому позичав» сподобалася друзям Олега. Вони теж не хочуть запам'ятовувати, хто за кого заплатив в барі і скільки ще залишився винен - ​​все записано на стіні. Вони обговорили ідею і вирішили, що їм потрібен єдиний список на всіх.

Але кому довірити вести таку важливу бухгалтерію? Адже коли справа стосується грошей - довіра виходить на перший план, для цього існують банки, яким згодом стали довіряти, оскільки вони підкріплені ліцензією, законами і страхівкою Центрального Банку (рис.16.1).

У колі друзів всі довіряють один одному і можна просто вибрати на цю роль самого відповідального (рис.16.1). Але якщо питання стосується незнайомих людей? Цілого міста, країни, або всього світу, як у випадку з Біткоїном? Там взагалі ніхто нікому не може довіряти.

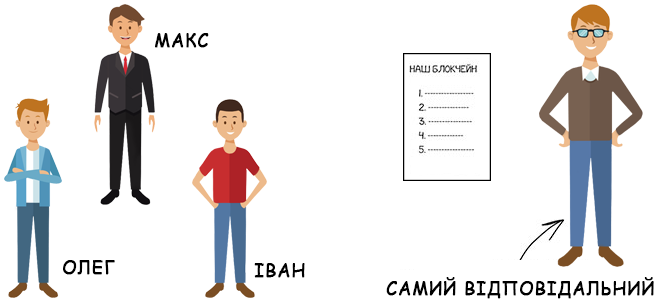


Рис.16.1. Вибір відповідальної особи для зберігання захищеного списку

### Децентралізація: ніхто не довіряє нікому

Так придумали альтернативний підхід: зберігати копію списку в кожного. Таким чином зловмиснику доведеться не просто переписати один список, але і проникнути в кожен будинок і переписати списки там. А потім з'ясується, що хтось зберігав в себе вдома аж кілька списків, про що ніхто не здогадувався. Це і є децентралізація (рис.16.2).

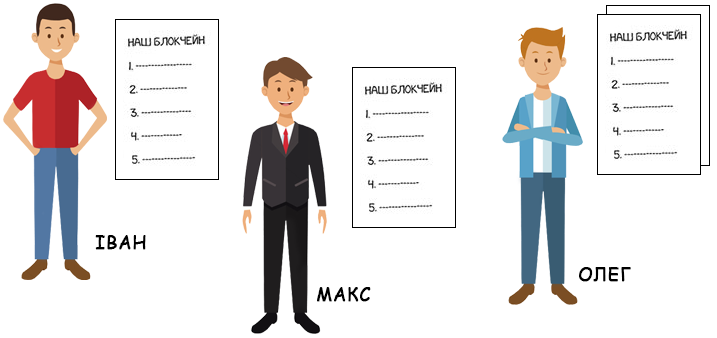


Рис.16.2. Принцип децентралізації у збереженні захищеного списку

Мінусом такого підходу є те, що для внесення нових записів доведеться обдзвонювати всіх інших учасників і повідомляти кожному з них свіжі зміни. Але якщо ці учасники - бездушні машини, це перестає бути проблемою.

В такій системі не існує єдиної точки довіри, а значить і можливості підкупу і шахрайства. Всі учасники системи діють згідно єдиного правила: ніхто не довіряє нікому. Кожен вірить тільки тій інформації, яка є у нього. Це головний закон будь-якої децентралізованої мережі.

## 16.2Транзакції

Купуючи товар в магазині, покупець вводить пін-код від своєї карти, дозволяючи магазину запитати в банку чи є на рахунку потрібна кількість грошей. Іншими словами, покупець підписує своїм пін-кодом транзакцію на потрібну суму, яку банк прийме або відхилить.

Записи типу «Позичив Івану 500 гривень» - теж транзакції. Але в цьому товаристві немає банку, що може авторизувати автора транзакцій. Як перевірити, що Іван потайки не додав запис «Макс заборгував Олегу 100500 гривень»?

У блокчейні для цього використовується механізм публічних і приватних ключів, ІТ-фахівці давно використовують їх для авторизації в SSH.

Коротко про те, як працює ця складна математика: ви в себе на комп'ютері генеруєте пару довгих простих чисел - публічний і приватний ключ. Приватний ключ вважається супер-секретним, оскільки може розшифрувати те, що зашифровано публічним. Але навпаки теж працює. Якщо роздати публічний ключ друзям, вони зможуть зашифрувати ним будь-яке повідомлення так, що прочитати його зможете тільки ви, оскільки володієте приватним. Але крім цього у публічного ключа є корисний ефект - за допомогою нього можна перевірити, що дані були зашифровані саме вашим приватним ключем, не розшифровуючи при цьому самі дані (рис. 16.3). Про всі ці властивості добре розказано [в «Книга шифров: тайная история шифров»](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjigpGa-8veAhUE3CwKHVY9BycQFjADegQIDhAB&url=http%3A%2F%2Fpadabum.com%2Fd.php%3Fid%3D50920&usg=AOvVaw0JpR274xVO4pgRExu_eu42).

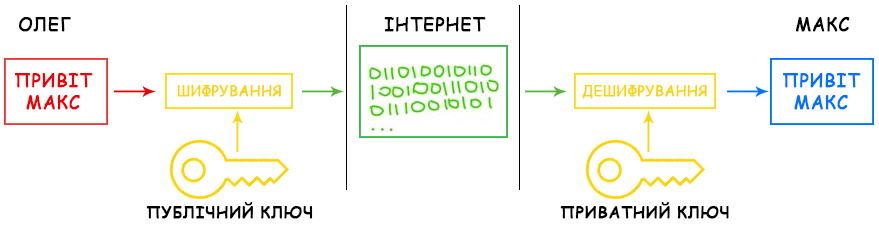


Рис.16.3. Механізм публічних і приватних ключів

Ми знаходимося в децентралізованому Інтернеті, де нікому не можна довіряти. Транзакція підписується приватним ключем і разом з публічним ключем надсилається до спеціального сховища - пул непідтверджених транзакцій. Так будь-який учасник мережі може перевірити, що саме ви були ініціатором транзакції, а не хтось хоче розплатитися вашими грошима.

Цим досягається відкритість і безпека мережі. Якщо раніше за це відповідали банки, то в блокчейні за це відповідає математика.

***Публічний ключ і є номером крипто-гаманця. Тобто, можна завести гаманець будь-якої криптовалюти взагалі не виходячи в мережу.***

Простим користувачам, які не бажають розбиратися як випускати і зберігати приватні ключі, допоможуть сервіси онлайн-гаманців. Щоб копіювати довгі публічні ключі, там роблять зручні QR-коди. Наприклад, [Blockchain Wallet](http://blockchain.info/wallet/) має зручний мобільний додаток і підтримує дві головні криптовалюти - BTC і ETH.

### Відсутність поняття «балансу»

Як і список, блокчейн по суті складається тільки з історії транзакцій. Він не зберігає баланс кожного гаманця, інакше б довелося винаходити додаткові способи захисту.

Володіння гаманцем підтверджує тільки приватний ключ. Але як інші учасники мережі переконаються, що у власника є достатньо грошей для покупки?

Оскільки немає балансу - це повинні доводити самі власники. Тому, в транзакцію блокчейна входить не тільки підпис учасника і скільки він хочете витратити, але і посилання на попередні транзакції, в яких отримано потрібну кількість грошей. Тобто, якщо хочеться витратити 400 гривень, потрібно пройтися по всій історії доходів і витрат, і прикріпити до своєї транзакції ті доходи, де надійшло 100 + 250 + 50 гривень, тим самим доводячи, що ці 400 гривень існують (рис.16.4).

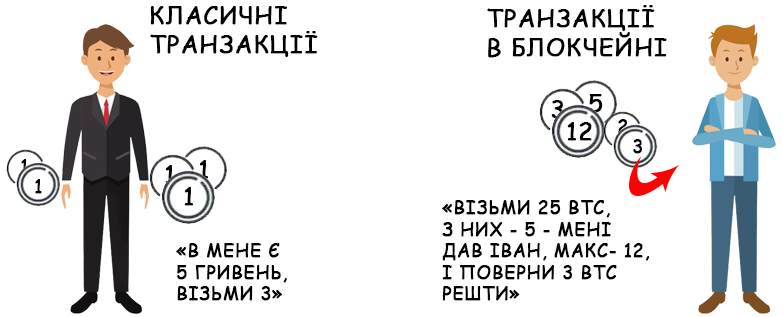


Рис.16.4. Відмінності між класичними транзакціями і транзакціями в блокчейні

Кожен учасник мережі ще раз обов'язково перевірить, що доходи не прикріплювали двічі. Що ті 300 гривень, що дав Макс минулого тижня, дійсно ще не витрачено.

Такі прикріплені до транзакції доходи в блокчейні називаються **інпут (input)**, а всі отримувачі грошей - **аутпут (output)**. Сума всіх інпутів рідко буває рівно такою, скільки потрібно перевести за раз – тому, одним з аутпутів найчастіше будете сам власник. Транзакція в блокчейні виглядає як «мені дали 3 і 2 BTC, я хочу з них перевести 4 BTC і решту 1 BTC повернути собі назад» (рис.16.5). Додатково з цієї «решти» ще можна вказати комісію за транзакцію, щоб Майнери активніше її додавали в блоки. Тоді, майнер отримає винагороду, а учасник дещо менше решти.

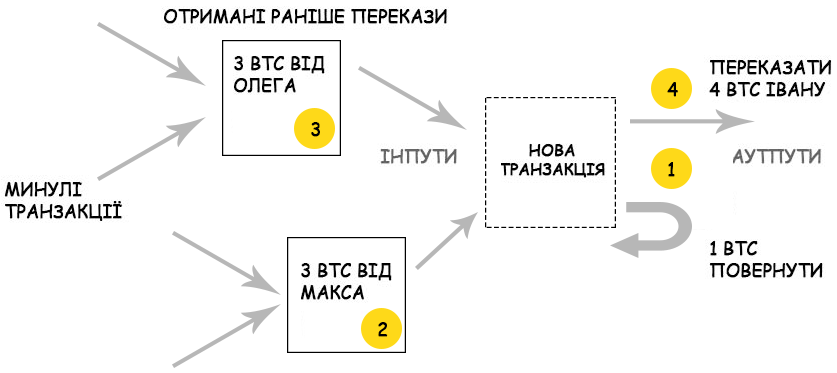


Рис.16.5. Вхідні та вихідні транзакції в блокчейні

Зручність блокчейну ще і в тому, що інпути не обов'язково мають бути з одного гаманця. Оскільки, перевіряється тільки ключ. Якщо знати приватні ключи всіх інпутів, то без проблем можна прикріпити їх до своєї транзакції і розплатитися цими грошима. Подібно, як в супермаркеті здійснити оплату з кількох карт, від яких знати пін-код.

Однак якщо втратити свій приватний ключ, наприклад, зламався твердий диск або вкрадено ноутбук, Біткоїни будуть втрачені назавжди. Ніхто не зможе використовувати їх в якості інпутів для нових транзакцій. Ця сума буде недоступною для всього світу назавжди – ці гроші пропадають. Тут немає єдиного банку, куди можна написати заяву з копією паспорта, і доступ буде відновлено. Для цього потрібен ще додатковий випуск нових Біткоїнів «з повітря».

### Проблема подвійної витрати

Вище згадувалося, що транзакції додаються до спеціального «пулу непідтверджених транзакцій». Навіщо потрібні проміжні етапи, якщо вже є готові підписані транзакції? Чому відразу їх не можна надіслати до обробки в блокчейн?

Тому, що сигнали з пункту А в пункт Б завжди йдуть із затримкою. Дві транзакції можуть піти абсолютно різними шляхами. І транзакція, яка ініційована першою, може дійти до одержувача пізніше, оскільки йшла більш довгим шляхом (рис.16.6). Так виходить [подвійне витрачання](https://ru.wikipedia.org/wiki/Двойное_расходование), коли одні і ті ж гроші відправлено відразу до двох адресатів, про що вони навіть не здогадаються.

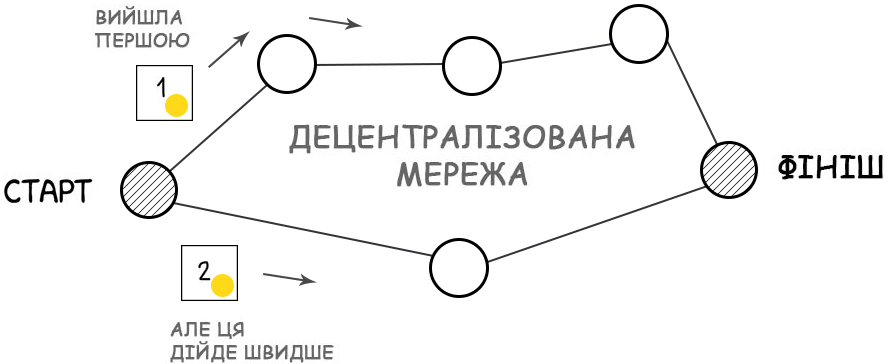


Рис.16.6. Шляхи проходження транзакцій і в блокчейні

Для децентралізованої мережі, в якій нікому не можна довіряти, ця проблема є особливо гострою. Як можна переконатися, що одна транзакція точно була раніше за іншу? Примушувати відправника вшивати в неї час відправки, чи не так? Але згадайте - нікому не можна довіряти, навіть відправнику. Час на всіх комп'ютерах обов'язково буде відрізнятися і немає способу їх гарантовано синхронізувати. Копія блокчейну зберігається на кожному комп'ютері мережі і кожен учасник довіряє тільки їй.

Як же переконатися, що одна транзакція була раніше за іншу? Відповідь проста: це неможливо. Немає способу підтвердити час транзакції в децентралізованої мережі. І ось в рішенні цієї проблеми і полягає третя важлива ідея блокчейна, яку придумав Сатоши і яка прописана в його назві – блоки (рис.16.7).

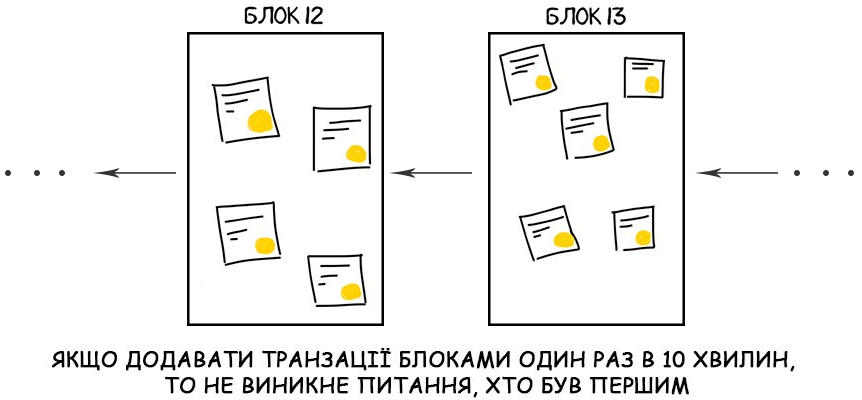


Рис.16.7. Формування блоків в блокчейні

## Блоки - основа блокчейну

Кожен працюючий комп'ютер в мережі вибирає із загального пулу будь-які транзакції, які йому подобаються. Зазвичай, просто за найвищою комісією, яку можна на ній заробити. Так він набирає собі транзакції, поки їх сумарний розмір не досягне обговорённого ліміту. У Біткоїні цей ліміт на розмір блоку дорівнює 1 Мб (після SegWit2x буде 2 Мб), а в Біткоїн Кеші - 8 Мб.

Весь блокчейн по суті є списоком таких блоків, де кожен посилається на попередній. По ньому можна відстежити будь-яку транзакцію за всю історію, розгортаючи блокчейн хоч до самого першого запису. Саме цей список і важить зараз сотні гігабайт і повинен бути повністю завантажений на всі комп'ютери, які хочуть брати участь в роботі мережі (але щоб просто створювати транзакції і переводити гроші, це не обов'язково) (рис.16.8). Завантажується він так само зі всіх найближчих комп'ютерів мережі, подібно до завантаження серіалів з торрентів, тільки нові серії в ньому виходять кожні 10 хвилин.

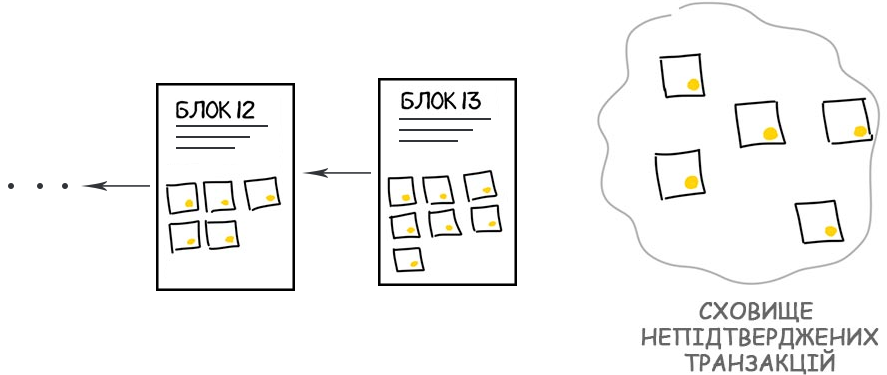


Рис.16.8. Сховище непідтверджених транзакцій

Після того як комп'ютер набрав собі транзакцій з пулу, він починає складати з них непорушний список у вигляді дерева - хешує записи попарно, потім результат ще раз попарно і так поки не залишиться лише один хеш - корінь дерева, який і додається до блоку (рис.16.9). Детальніше є на вікі: [Дерево Меркла](https://ru.wikipedia.org/wiki/TTH).



Рис.16.9. Дерево хешів

Чому саме деревом? Тому що з'являється можливість видаляти непотрібні (скасовані) транзакції з блоку. Тобто, наприклад є дві транзакції, що об'єднані хешом, одна або обидві вже не потрібні, оскільки це вже все давно віддано до інших транзакцій - так ось ці старі можна видалити, а хеш залишити, в результаті нічого не порушується. Це описано в пункті "7. Reclaiming Disk Space" в оригінальній статті Сатоші.

Оскільки актуальний блокчейн вже викачаний, комп'ютер точно знає який в ньому зараз останній блок. Йому залишається тільки додати посилання на нього в заголовок блоку, захешувати все це і повідомити всім іншим комп'ютерам мережі, що зроблено новий блок, і запропонувати додати його до ланцюжка блокчейна.

Решта повинні перевірити, що блок побудований за всіма правилами і що туда не додано зайвих транзакцій, а потім додати до себе в ланцюжки. Тепер всі транзакції в ньому підтверджені, блокчейн збільшений на один блок і все йде добре, чи не так?

А ось і ні. У мережі одночасно працюють тисячі комп'ютерів, і як тільки вони зберуть новий блок, вони майже одночасно повідомляють всіх, що їх блок створено першим. А в децентралізованої мережі неможливо довести хто дійсно був першим (рис.16.10).

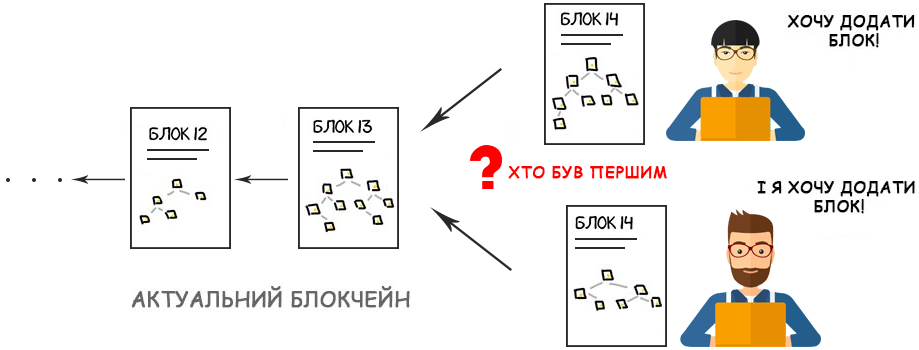


Рис.16.10. Визначення черговості додавання блоків

Тому, для додавання блоку до ланцюжка комп'ютери повинні вирішити певну складну задачу, яка забере у них певний час. Для комп'ютера - це додати в кінець блоку таке число (nonce), щоб в результаті хеш SHA-256 для всього блоку починався на певну кількість нулів (рис.16.11). Чим більше початкових нулів потрібно, тим складніше підібрати рішення.Це і є те завдання, яке треба вирішити, щоб додати блок до мережі Bitcoin. Для інших мереж завдання можуть відрізнятися.

Кількість цих "нульових біт" автоматично коригується в мережі приблизно раз на 2 тижні, щоб підтримувати постійну швидкість генерації нових блоків за будь-якої обчислювальної потужності майнерів в мережі.

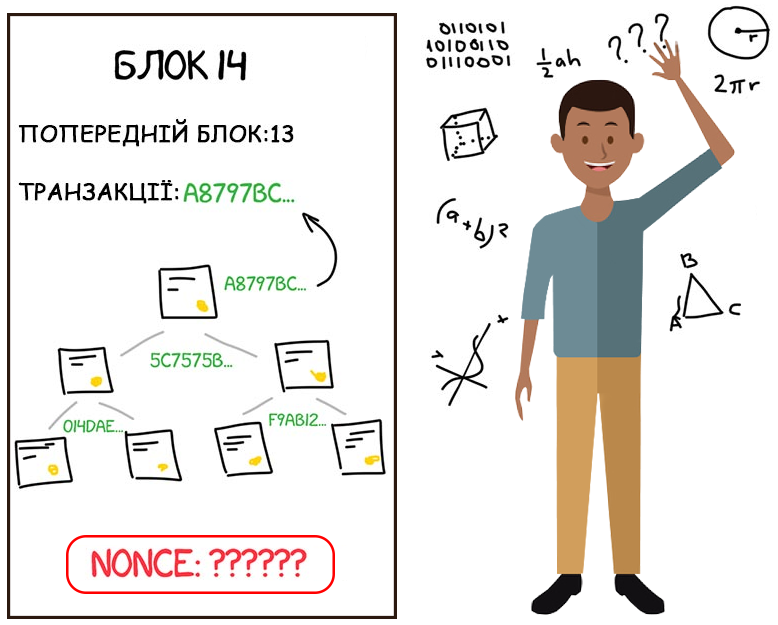


Рис.16.11. Додавання числа (nonce) до блоку

## 16.3. Майнінг

Майнінг Біткоїна – це не є священне таїнство. Майнінг не пов'язаний з пошуком нових Біткоїнів десь в глибинах Інтернету. Майнінг - це коли тисячі комп'ютерів по всьому світу гудуть по підвалах, перебираючи мільйони чисел в секунду, намагаючись підібрати хеш, що починається на 10 нулів (рис.16.12). Їм навіть не обов'язково для цього перебувати в мережі.

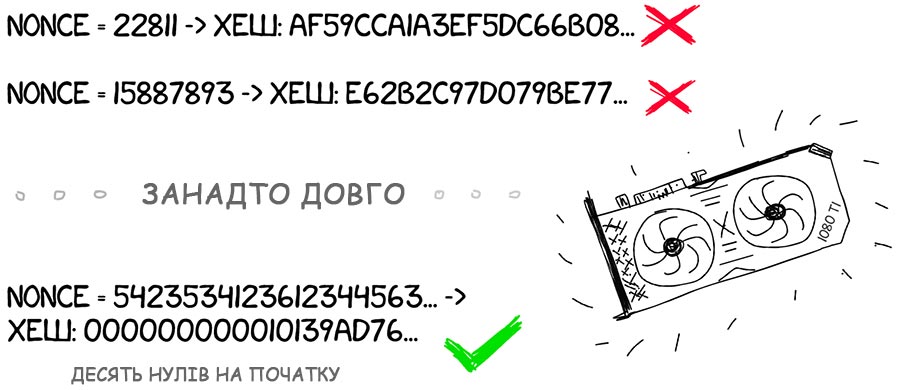


Рис. 16.12. Визначення правильності знайденого числа (nonce)

Відеокарти з сотнями паралельних ядер, вирішують цю задачу швидше за любий CPU.

Чому саме на 10 нулів? А просто так, в цьому немає жодного сенсу. Так придумав Сатоши. Оскільки, це одне з тих завдань, на яке точно завжди є рішення, але воно точно не може бути знайдено швидше, ніж довгим монотонним перебором варіантів.

Складність Майнінгу безпосередньо залежить від розміру мережі, тобто її сумарної потужності. Якщо створити власний блокчейн і запустити його вдома на двох ноутбуках, то задача повинна бути простішою. Наприклад, щоб хеш починався тільки з одного нуля, або щоб сума парних розрядів дорівнювала сумі непарних.

Щоб знайти хеш, що починається на 10 нулів, в одного комп'ютера піде кілька десятків років. Але якщо об'єднати тисячі комп'ютерів в єдину мережу і шукати паралельно, то за теорією ймовірностей це завдання вирішується в середньому за 10 хвилин. Це і є час появи нового блоку в блокчейні Біткоїна. Кожні 8-12 хвилин хтось на землі знаходить такий хеш і отримує привілей анонсувати свою знахідку до всіх, уникнувши тим самим проблеми хто був першим (рис.16.13).

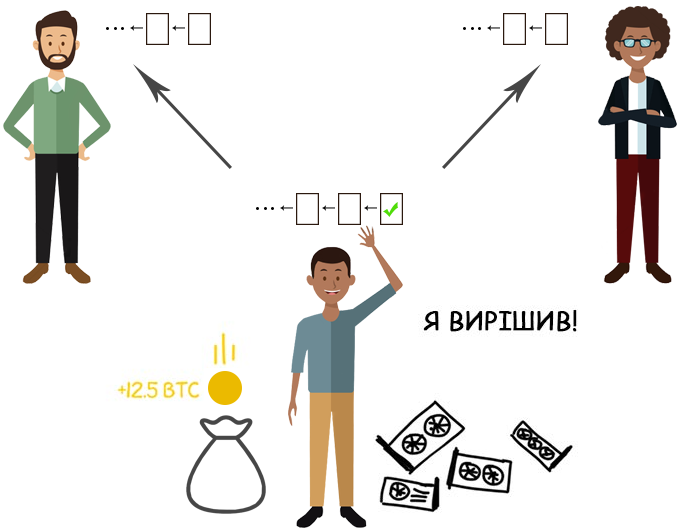


Рис.16.13. Визначення майнера, що підібрав вірний хеш

За знаходження відповіді комп'ютер отримує 6.25 ВТС (травень 2020 року) - це сума винагороди, яка генерується системою Біткоїна «з повітря» і зменшується кожні чотири роки. У травні 2017 року сума складала 12.5 BTC. Технічно це означає, що кожен майнер завжди додає в свій блок ще одну транзакцію - «створити 6.25 BTC і надіслати їх на мій гаманець». Коли ви чуєте «кількість Біткоїни в світі обмежена 21 млн, зараз наймайнілі вже 16 млн» - це і є такі винагороди, що генеруються мережею.

На справжній живий блок Біткоїна [можна подивитися](https://live.blockcypher.com/btc/block/000000000000000000c23ad8a3a1a5faa6e51e03ea7546eb86996dbbf5aaad26/) на одному зі спеціальних сайтів. Там є і транзакції з інпутами і аутпутами, і 18 нулів на початку і всі описані вище хеші.

***Любий блокчейн існує поки існують його майнери.***

Саме майнери обробляють транзакції, що з'являються до блокчейну. Так що якщо хтось розповідає вам, що він «зробить блокчейн для \*\*\*», перше питання, на який він повинен відповісти - хто і навіщо буде майнити на ньому. Найчастіше правильну відповідь - «будуть всі, тому що за майнінг ми даємо наші коіни, які будуть зростати і майнерам це вигідно». Але це може бути застосовано не для всіх проектів. Наприклад, якщо завтра міністерство охорони здоров’я створить свій закритий блокчейн для лікарів (а вони хочуть), хто його буде майнити? Терапевти у вихідні?

Але яка вигода майнерам буде потім, коли винагороди зникнуть або стануть мізерними?

За задумом Автора, на той час люди повинні будуть повірити в реальність Біткоїна і майнінг почне окупатися сумою комісій, що включені в кожну транзакцію. До цього все і йде: ще в 2012 році всі комісії були нульовими, майнер майнив тільки за винагороди від блоків. Сьогодні ж транзакція з нульовою комісією може знаходитися в пулі кілька годин, оскільки з'явилася і конкуренція, і люди готові платити за швидкість.

Тобто суть майнінгу - вирішити будь-яку обчислювальну задачу. Це завдання має бути досить простим, щоб в учасників мережі була стабільна ймовірність знайти відповідь - інакше транзакції будуть підтверджуватися вічність. Наприклад, на касі в магазині потрібно кожен раз чекати по пів години, поки банк підтвердить транзакцію. Ніхто не буде користуватися таким банком.

Але завдання повинне бути одночасно і складним, щоб відповідь не знайшли відразу всі майнери мережі. Оскільки в такому випадку вони нададуть в мережу багато блоків з однаковими транзакціями і буде ймовірність «подвійної розтрати». Або ще гірше - поділу єдиного блокчейна на кілька гілок, в яких вже ніхто не зможе розібратися, яка транзакція підтверджена, а яка ні.

Якщо нагорода в 6.25 BTC вручається лише раз в 10 хвилин і тільки для одного майнера, що знайшов блок, виходить решті потрібно даремно палити відеокарти кілька років в надії, що одного разу впаде $ …0000 (за поточним курсом)?

Для Біткоїна саме так, але так було не завжди. Раніше мережа була меншою, складність нижчою, а значить і вищою ймовірність одноосібно знайти хеш для нового блоку. Але і Біткоїн тоді коштував не так дорого.

Зараз Біткоїни поодинці вже ніхто не майнить. Тепер учасники об'єднуються в спеціальні групи - майнінг пули, де все разом намагаються знайти правильний хеш. Якщо хоч один з групи знаходить, то вся винагорода поділяється між учасниками залежно від їх внеску в загальну роботу.

Але одиночний майнінг цілком можливий в інших мережах. Ще недавно було легко майнити Ethereum, де блоки знаходяться кожні 10 секунд. Винагорода за блок там набагато нижче, але ймовірність заробити гроші виходить вище.

Значить майнери будуть спалювати тисячі відеокарт даремно і жодного виходу немає?

Так, але є ідеї. Описаний вище Майнінг є класичним і називається Proof-of-Work (доведення роботи). Тобто, кожна машина доводить, що вона працювала на благо мережі тим, що вирішує складні завдання із заданою вірогідністю.

Але деякі розробники починають робити блокчейни з іншими видами майнінгу. Зараз друга за популярністю концепція - це Proof-of-Stake ([доведення частки володіння](https://ru.wikipedia.org/wiki/Доказательство_доли_владения)). В такому виді майнінгу, чим більше «коїнів» на рахунку в учасника мережі, тим більше його ймовірність вставити до блокчейну свій блок. Можна придумати і інші види майнінгу.

## 16.4. Блокчейн

Уявімо ситуацію, в якій не дивлячись на всю теорію ймовірностей, два майнера все одно примудрилися одночасно знайти правильну відповідь. Вони починають розсилати два абсолютно вірних блоки по мережі. Ці блоки гарантовано відрізняються, але навіть якщо вони дивом вибрали однакові транзакції з пулу, склали абсолютно ідентичні дерева і вгадали однакове рандомне число (nonce), їх хеши все одно будуть різними, оскільки кожен пропише в блок свій номер гаманця для винагороди.

Тепер у нас є два валідних блоки і знов виникає проблема кого вважати першим. Як поведе себе мережа в такому випадку?

В алгоритмі блокчейна прописано, що учасники мережі просто беруть першу правильну відповідь, яка до них дійшла. Обидва майнери отримають свою винагороду, а всі інші починають майнити, спираючись на останній ними особисто отриманий блок, відкидаючи всі інші повторно-вірні. В мережі з'являються дві версії правильного блокчейну (рис.16.14). Такий парадокс.

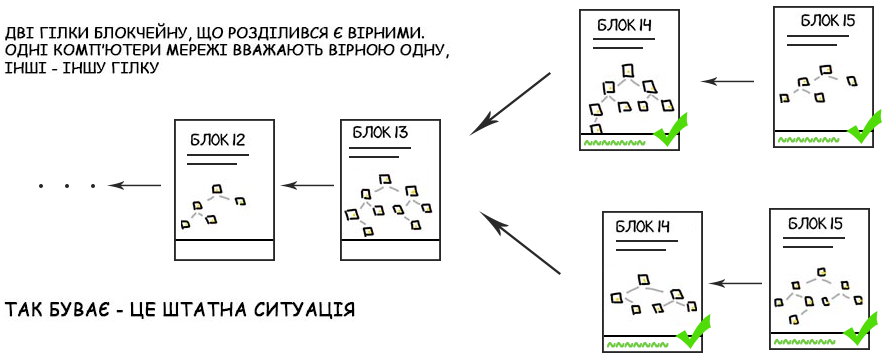


Рис. 16.14. Формування гілок з правильними хешами

Це штатна ситуація, в якій знову допомагає теорія ймовірностей. Мережа функціонує в такому роздвоєному стані, поки хтось із майнерів не знаходить наступний блок до одного з цих ланцюжків. Як тільки такий блок знаходиться і вставляється в ланцюжок, він стає довшим і виконується одна з угод мережі блокчейн: **за будь-яких умов, найдовший ланцюжок блоків приймається як єдино вірний для всієї мережі**.

Короткий ланцюжок, незважаючи на всю свою правильність, відкидається всіма учасникам мережі. Транзакції з нього повертаються до пулу (якщо вони не були підтверджені в іншому), а їх обробка починається заново. У майнера пропадає його винагорода, оскільки його блоку більше не існує (рис.16.15).

З ростом мережі такі збіги частішають, бували випадки, коли відкидався ланцюжок відразу з чотирьох блоків.

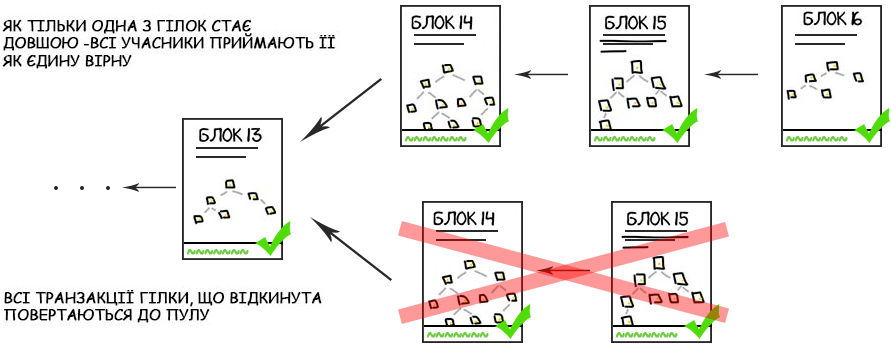


Рис.16.15. Вилучення коротшої гілки

Через це застосовуються три правила безпеки хвоста блокчейна (end of chain insecurity):

1. Винагородами за майнінг, можна користуватися лише через ще 20 підтверджених блоків після отримання. Для Біткоїна це близько трьох годин.
2. Якщо вам переслали Біткоїни, використовувати їх в якості інпутів в нових транзакціях можна тільки через 1-5 блоків.
3. Правила 1 і 2 лише прописані в налаштуваннях кожного клієнта. Ніхто не стежить за їх дотриманням. Але закон про самий довгший ланцюжок все одно знищить всі ваші транзакції, якщо спробувати обдурити систему, не дотримуючись правил.

### Намагаємося обдурити блокчейн

Тепер, коли відомо про Майнінг, влаштування блокчейну і правило найдовшого ланцюжка, може виникнути питання: а чи можна якось спеціально обійти блокчейн, скласти найдовший ланцюжок самому і тим самим підтвердити свої фейкові транзакції.

Припустимо, у вас є найпотужніший комп'ютер на Землі. Датацентри Google і Amazon разом взяті в вашому розпорядженні і ви намагаєтеся прорахувати такий ланцюжок, який стане найдовшим в мережі блокчейн (рис. 16.16).

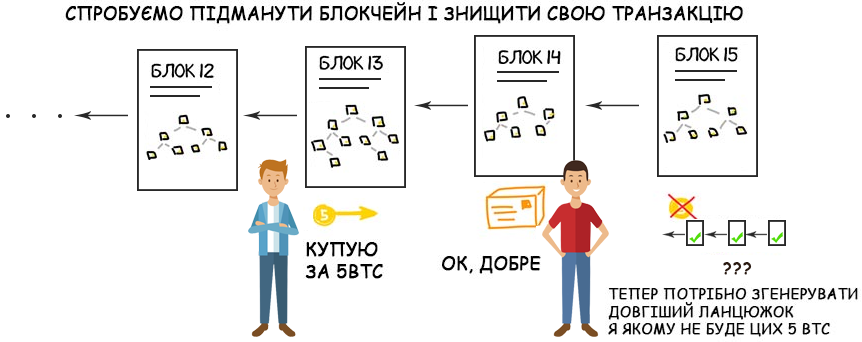


Рис.16.16. Спроби згенерувати підробний ланцюжок блокчейну

Ви не можете взяти і відразу прорахувати кілька блоків ланцюжка, адже кожен наступний блок залежить від попереднього. Тоді ви вирішуєте якомога швидше рахувати кожен блок на своїх величезних датацентрах паралельно з тим, як всі інші учасники продовжують збільшувати основний блокчейн. Чи можливо їх обігнати? Ймовірно, так.

Якщо ваша обчислювальна потужність буде складати більше 50% від потужності всіх учасників мережі, то з імовірністю 50% ви зможете побудувати більш довгий ланцюжок швидше за всіх інших разом взятих. Це теоретично можливий спосіб обдурити блокчейн, прорахувавши більш довгий ланцюжок транзакцій. Тоді всі транзакції справжньої мережі будуть вважатися неправильними, а ви зберете всі винагороди і почнете нову віху в історії криптовалюти, яка називається «розділення блокчейну». Одного разу через баг в коді так було з Ethereum.

Але в реальності жоден датацентр не зрівняється за потужністю зі всіма комп'ютерами в світі. Півтора мільярда китайців + півтора мільярда індусів з фермами для майнінгу і дешевою електрикою - це величезна обчислювальна потужність. Ніхто в світі поки не може скласти їм конкуренцію в поодинці, навіть Google.

Це приблизно як вийти на вулицю і намагатися переконати кожну людину в світі, що долар тепер коштує 1 гривню і встигнути до того, як в ЗМІ вас викриють. І ось якщо ви примудрилися переконати всіх, то зможете обвалити світову економіку. В теорії це можливо, але на практиці чомусь ні в кого не виходило (рис.16.17).

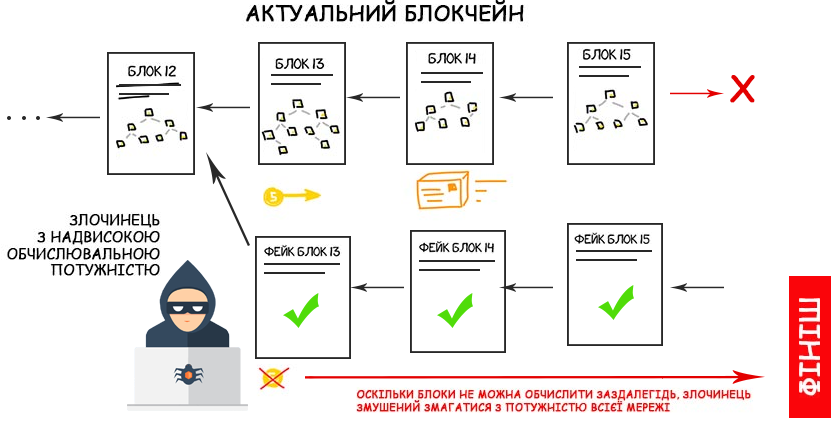


Рис. 16.17. Спроби злочинців зламати блокчейн біткоїна

На цій ймовірності тримається і блокчейн. Чим більше учасників-майнерів - тим більше безпеки і довіри до мережі. Тому, коли в Китаї накривають чергову велику майнінг-ферму, курс і обвалюється. Всі бояться, що десь у світі зібрано пул майнерів на ~ 49% потужності.

За фактом таке було кілька разів в 2014 році, коли один з пулів для майнінгу тимчасово став потужнішим за іншу мережу. Але маніпуляцій тоді помічено не було.

## 16.5. Унікальність технології Blockchain.

#### Децентралізація системи.

Інформація про блоки зберігається на всіх вузлах в мережі, немає єдиного централізованого управління транзакціями. Інформацію про транзакції може перевірити будь-хто: жодної комерційної таємниці, всі операції видно всім, перевірка надсилання коштів не становить проблем.

#### Анонімність транзакції.

Справжність транзакції та її виконання можна побачити завжди, а самого відправника ні. Можна бачити лише адресу, з якої здійснюється транзакція або адресу, для кого вона призначена. Для Блокчейну цього достатньо.

#### Неможливість підробки блоку.

За рахунок самого принципу роботи мережі це неймовірно складно зробити. Для того щоб блок вважався справжнім з ним повинні погодитися 51% всіх існуючих вузлів.

#### Виключається подвійна витрата коштів.

При надсиланні коштів відразу можна побачити, що вони відіслані, але ці кошти не будуть зараховані на рахунок, доки транзакція не потрапить у блок і не буде підтверджена. Приблизно в цей час зловмисник може ще раз надіслати ці ж кошти до іншої людині, але Блокчейн не дозволить цього зробити. В нього присутній такий запобіжник, як мітки часу і транзакція, яка була надіслана ​​раніше потрапить до блоку, а всі наступні, маючи інформацію про те, що переказ вже підтверджений будуть відкинуті мережею.

#### Комісія.

Комісія - справа добровільна. Її беруть для підтримки мережі вузлів. Вона додається до нагороди за формування блоку. В принципі, і це великий плюс, комісію можна не платити, майнер і так отримає нагороду за блок, але з нею транзакція обробляється швидше. В блокчейні комісія є справедливою, оскільки її отримує той, хто реально заслужив, витратив час і власні потужності на знаходження блоку.

## Сфери застосування блокчейну

Впровадження блокчейну збільшує швидкість обміну, зменшує витрати, покращує якість, надійність та доступність послуг. При цьому збільшується прозорість та надійність, зменшуються ризики.

Головна сфера застосування блокчейну - криптоіндустрія. Але крім цього проекти на блокчейні використовуються в банківському секторі, сфері фінансових послуг, платіжних сервісах, держсекторі (держпослуги, реєстри нерухомості, нотаріат, електронне голосування та ін.), транспорті та логістиці, IoT, охороні здоров'я, управлінні інтелектуальною власністю, енергетиці тощо.

### Криптоіндустрія

Криптоіндустрія - це широкий термін, який охоплює всі аспекти, пов'язані з криптовалютами та іншими цифровими активами.

* Криптовалюти - це цифрові валюти, які не випускаються центральними банками. Вони забезпечуються математичними алгоритмами і не піддаються інфляції. Найбільш відомі криптовалюти – це Біткойн, Ethereum, Tether та Binance Coin.
* Криптобіржі - це платформи, на яких можна купувати, продавати та обмінювати криптовалюти.
* Криптовалютні гаманці – це програмне забезпечення або апаратне забезпечення, яке використовується для зберігання криптовалют.
* NFT (невзаємозамінні токени) - це цифрові сертифікати на володіння цифровими активами, такими як витвори мистецтва, предмети колекціонування або ігрові предмети.

Криптоіндустрія є галуззю, що швидко розвивається, з великим потенціалом. Вона має потенціал змінити різні галузі та сфери життя.

### Державні послуги

Блокчейн-технологія може використовуватись у державних послугах для підвищення ефективності, прозорості та безпеки процесів.

* Посвідчення особи. Блокчейн може бути основою створення децентралізованих систем посвідчення личности. Замість того, щоб мати декілька окремих ідентифікаційних документів та систем, громадянин може мати унікальний ідентифікатор на блокчейні, пов'язаний із його особистими даними. Це може спростити процес ідентифікації та надання державних послуг.
* Управління реєстрами та документами. Блокчейн може використовуватися для зберігання та управління державними реєстрами та документами, такими як документи, що встановлюють право, свідоцтва про народження, свідоцтва про шлюб та інші. Записи в блокчейні неможливо змінити без згоди більшості учасників мережі, що забезпечує надійність та цілісність даних.
* Цифрова ідентифікація та авторизація. Блокчейн може використовуватися для створення безпечних ідентифікаційних рішень та цифрових підписів. Користувачі можуть мати унікальні ідентифікатори на блокчейні, які підтверджують їхню особу та дозволяють їм взаємодіяти з державними послугами без необхідності повторної аутентифікації в кожному конкретному випадку.
* Розподілені реєстри нерухомості. Блокчейн може бути використаний для створення розподілених реєстрів нерухомості, які забезпечують прозорість та незаперечність угод із нерухомістю. Усі транзакції та власні права можуть бути записані в блокчейні, що спрощує процедури переходу прав власності і запобігає можливим фальсифікаціям.
* Голосування. Блокчейн може використовуватись для забезпечення безпечного та прозорого голосування. Кожен голос може бути записаний у блокчейн, що дозволяє забезпечити незаперечність результатів та запобігти можливим маніпуляціям. Завдяки децентралізованій природі блокчейну, голосування може стати більш надійним та довірчим.

Впровадження блокчейну в державні послуги потребує ретельного розгляду правових, регуляторних та безпечних аспектів. Необхідно враховувати конкретні потреби та вимоги кожної держави, а також забезпечувати захист особистих даних громадян та запобігати можливим атакам на систему блокчейну.

### Бізнес

Блокчейн-технологія має широкий спектр застосувань у бізнесі та може принести багато переваг.

* Фінансові транзакції та платежі. Блокчейн може бути використаний для забезпечення безпечних та прозорих фінансових транзакцій та платежів. Він може значно знизити витрати та час, пов'язані з проведенням транзакцій, та усунути необхідність посередників. Смарт-контракти, що працюють на блокчейні, можуть автоматизувати виконання умов угод та забезпечити їхню надійність.
* Смарт-контракти - це комп'ютерні програми, які виконуються автоматично під час виконання певних умов. Вони можуть бути використані для автоматизації різних транзакцій, таких як укладання договорів або проведення платежів.
* Управління цифровими активами. Блокчейн може бути використаний для керування цифровими активами, такими як криптовалюти, токени та смарт-контракти. Він забезпечує надійну реєстрацію та передачу прав власності без необхідності довіряти центральним установам. Блокчейн може бути використаний для створення децентралізованих платформ для торгівлі цифровими активами.
* Децентралізовані програми (DApps) - це програми, які працюють на блокчейні. DApps не контролюються центральними органами влади та можуть використовуватися для різних цілей, таких як децентралізовані фінансові послуги, ігри та соціальні мережі.
* Управління та обмін даними. Блокчейн може бути використаний для безпечного та ефективного обміну даними між різними учасниками, такими як компанії, клієнти, постачальники та партнери. Він може допомогти усунути проблеми централізованого зберігання даних, запобігти їх підробці та забезпечити контроль за доступом до інформації.
* Постачання та ланцюжок поставок. Блокчейн може використовуватися для відстеження та керування ланцюжками поставок. Він може забезпечити прозорість і незаперечність даних про походження, якість, логістику та інші аспекти товарів. Завдяки цьому компанії можуть підвищити довіру споживачів, скоротити витрати на перевірку та аудит процесів поставок, а також ефективно реагувати на проблеми, такі як відгуки та повернення товарів.

Однак при впровадженні блокчейну в бізнесі важливо враховувати конкретні потреби та цілі компанії, а також оцінювати переваги та обмеження технології.

### Освіта та наука

Блокчейн-технологія має потенціал для застосування в освіті та науці, пропонуючи низку переваг.

* Підтвердження академічних досягнень. Блокчейн може використовуватись для створення надійної та прозорої системи підтвердження академічних досягнень, таких як дипломи, сертифікати та академічні рекорди. Це дозволяє учням та студентам мати повний контроль над своїми досягненнями, а також забезпечує роботодавцям достовірність поданих документів.
* Інтелектуальна власність та авторські права. Блокчейн може використовуватись для реєстрації та захисту інтелектуальної власності та авторських прав у наукових дослідженнях. Він дозволяє зберігати незалежне джерело підтвердження авторства та датування дослідницьких робіт, а також сприяє більш справедливому розподілу винагород та цитувань. Він може бути незалежним джерелом підтвердження авторства та датування створення контенту, такого як музика, фотографії, тексти та інші творчі твори.
* Спільні дослідження. Блокчейн може бути використаний для організації дослідницьких проектів та обміну науковими даними між вченими та дослідницькими установами. Він забезпечує безпечний та прозорий обмін інформацією, а також сприяє відстеженню джерел даних та результатів досліджень.
* Підтвердження фактів та достовірності джерел. Блокчейн може використовуватися для створення системи підтвердження фактів та достовірності джерел інформації. Він може допомогти боротися з проблемою фальсифікації даних та надати користувачеві прозорий доступ до інформації про джерело, час створення та зміни даних.
* Захист персональних даних. Блокчейн може бути використаний для управління персональними даними студентів та дослідників. Він може забезпечити захист даних, надавши користувачам контроль над своїми особистими даними та рішення, кому та коли надавати доступ до них.

Впровадження блокчейну в освіту та науку потребує подальших досліджень, розробки стандартів та співробітництва між учасниками. Однак блокчейн має потенціал підвищити прозорість, ефективність та надійність у цих галузях.

### Соціальна сфера

Блокчейн-технологія також має потенціал для використання у соціальній сфері.

* Управління особистими даними. Блокчейн може бути використаний для управління особистими даними громадян. Він дозволяє громадянам мати контроль над своїми даними та вирішувати, кому і коли надавати доступ до них. Завдяки блокчейну можна підвищити приватність даних та запобігти їх незаконному використанню.
* Управління охороною здоров'я. Блокчейн може бути використаний для покращення системи управління охороною здоров'я. Він дозволяє створити надійну та безпечну платформу для обміну медичними даними між різними учасниками, такими як лікарі, лікарні, страхові компанії та пацієнти. Завдяки цьому можна покращити координацію медичного догляду, запобігти дублюванню процедур, а також забезпечити захист конфіденційності пацієнтів.
* Облік та розподіл соціальних допомог. Блокчейн може використовуватися для обліку та розподілу соціальних допомог, таких як виплати по безробіттю, виплати для нужденних та інші види допомоги. Завдяки використанню блокчейну можна підвищити прозорість та незаперечність даних про одержувачів допомоги, запобігти шахрайству та забезпечити більш справедливий розподіл ресурсів.
* Благодійність та пожертвування. Блокчейн може використовуватися для покращення прозорості та ефективності процесів благодійності та пожертвувань. Він дозволяє відстежувати потоки коштів та переконатися, що пожертвування досягають призначених цілей. Завдяки блокчейну можна покращити довіру між донорами та отримувачами, а також спростити аудит та звітність про витрати коштів.

Важливо відзначити, що впровадження блокчейну у соціальну сферу потребує врахування правових, етичних та безпекових аспектів, а також співпраці між різними зацікавленими сторонами.

### Типи блокчейнів

У різних сферах можуть використовуватись як загальнодоступні, так і приватні блокчейни, залежно від конкретних проектів, ступеня децентралізації, вимог безпеки, масштабованості та контролю, необхідності конфіденційності даних та інших факторів.

* Загальнодоступні блокчейни. Загальнодоступні блокчейн-платформи, такі як Ethereum, Hyperledger Fabric, Corda та інші, надають гнучку інфраструктуру для розробки та розгортання різних додатків, включаючи криптовалюти, смарт-контракти, системи ідентифікації та інші рішення, які можуть застосовуватись у різних галузях.
* Приватні блокчейни. У деяких випадках, особливо у сферах, що потребують високої пропускної спроможності та масштабованості, компанії чи організації можуть розробляти власні приватні блокчейн-рішення, які адаптовані до їх конкретних потреб. Ці блокчейни обмежені доступом та контролюються конкретними учасниками, що може забезпечувати більшу приватність та керування мережею. Це може бути корисним, наприклад, для створення приватних ланцюгів поставок або систем керування даними, де потрібний більш суворий контроль та конфіденційність.
* Консорціальні блокчейни. Це блокчейни, керовані групою організацій, зазвичай, у рамках консорціуму. Тут кілька сторін співпрацюють для управління блокчейном. Прикладом може бути Hyperledger, створений Linux Foundation.
* Гібридні рішення. У деяких випадках використовується комбінація загальнодоступних та приватних блокчейнів. Наприклад, може бути приватний блокчейн, а інформація про ключові події може записуватися в загальнодоступний блокчейн для додаткової прозорості.
* Специфічні галузеві блокчейни. Деякі галузі розробляють власні блокчейни, адаптовані до своїх конкретних потреб і стандартів. Наприклад, блокчейни, орієнтовані на медичну галузь чи логістику.

Не обов'язково, щоб кожна сфера використовувала свій власний блокчейн. У деяких випадках може бути розроблено та використано спеціалізований блокчейн під конкретні потреби, частіше використовують універсальні публічні блокчейн-платформи з відкритим вихідним кодом.

## Контрольні питання

1. Поясніть поняття «хешування», «хеш-функція», «хеш-код». Що вони позначають?
2. Яка відмінність лежить між централізацією та децентралізацією довіри?
3. У рамках блокчейну, що називають публічним та приватним ключем?
4. Чим відрізняються транзакції в блокчейні від класичних фінансових транзакцій?
5. Пояснити особливості блоку в блокчейні. Яким чином він формується і забезпечує свою непорушність?
6. Що таке майнінг, хто і для чого ним займається?
7. Завдяки чому майнери отримують оплату за звою роботу?
8. Назвати причини, що запобігають шахрайству в блокчейні.
9. Перелічити популярні криптовалюти.
10. Для яких цілей, окрім фінансових можна використати блокчейн?

## Використані матеріали

* Блокчейн зсередини: як влаштовано біткоїн <https://vas3k.ru/blog/blockchain/>
* Сатоші Накамото. Bitcoin: A Peer-to-Peer Electronic Cash System <https://bitcoin.org/bitcoin.pdf>
* How Bitcoin Works Under the Hood <https://youtu.be/Lx9zgZCMqXE>
* Просте пояснення принципу роботи блокчейну <https://tjournal.ru/news/41306-samoe-ponyatnoe-obyasnenie-principa-raboty-blokcheyna>
* Пули для майнінгу <https://bits.media/pool-mining/>
* Біткойн - інноваційна платіжна система та новий вид грошей <https://bitcoin.org/uk/>
* Глобальная платформа Ethereum <https://ethereum.org/ru/>