БЛОКЧЕЙН, лекція 2

ПЛАН

1. Використання хеш-функції.
2. Дерево Меркла.
3. Спеціальні транзакції.
4. Hard & Soft fork
5. Обмеження блокчейну.
6. Приватний та публічний блокчейн.
7. Цифровий підпис до блокчейну: підпис транзакцій, підтвердження роботи.

Блокчейн — це децентралізований цифровий реєстр транзакцій (безперервно зростаючий список електронних записів), що зберігається протягом тривалого часу і захищений засобами шифрування (своєрідним алгоритмічним кодом).
Дані реєстру блокчейна розподіляються через мережу комп'ютерів. Його користувачі можуть безпосередньо взаємодіяти зі збереженими даними в режимі реального часу, не потребуючи посередника (дистриб'ютора) для підтвердження справжності транзакцій.
Ця технологія забезпечує незалежну, захищену від зовнішнього втручання та прозору платформу для учасників блокчейну, що дозволяє безпечно зберігати, передавати та обробляти конфіденційну інформацію.

Узагальнені відомості про блокчейн

- Децентралізований
- Одноранговий
- Захищений від зовнішнього втручання
- Синхронізований за погодженням
- Усуває необхідність перевірки третьою стороною
- Усі транзакції видно всім учасникам відповідного блокчейну

МОДЕЛІ МЕРЕЖІ

Централізована

Децентралізована

Розподілена

ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЇ

Хеш - це функція, яка реорганізує введення літер і цифр у зашифроване виведення фіксованої довжини. Хеш створюється з використанням алгоритму та необхідний для управління ланцюжком блоків у криптовалюті.

Основою будь-якої криптовалюти є блокчейн, який є глобальною бухгалтерською книгою, утвореною об'єднанням окремих блоків даних транзакцій.

Відео для перегляду : https://www.youtube.com/watch?v=Bul0XYMa8Jg
Відео російською, тому перегляд за бажанням
Англійською: http://surl.li/etwqx,

ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЇ

Блокчейн містить тільки надійні, перевірені транзакції і тим самим запобігає шахрайським операціям і подвійним витратам.

Зашифроване значення є послідовністю цифр і літер, які зовсім не схожі на вихідні дані - це і називається хеш. Майнінг критовалюти працює з цим хешем.

особливості:

- Хеш - це функція, що відповідає зашифрованим вимогам, необхідним для обчислення блокчейну.
- Хеші мають фіксовану довжину, проте практично неможливо вгадати довжину даних, якщо зловмисник намагається зламати блокчейн.
- Хеш розробляється з урахуванням інформації, що міститься в заголовку блоку.

Хешування вимагає обробку даних з блоку через математичну функцію, що призводить до виведення фіксованої довжини. Використання фіксованої довжини підвищує безпеку, тому що будь-хто, хто намагається зламати хеш, не зможе визначити довжину, побачивши довжину виведення.

Відео для перегляду: http://surl.li/etwrk

ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЇ

Візьмемо для прикладу алгоритм SHA-256 , і за допомогою сайту https://passwordsgenerator.net/sha256-hash-generator/ розглянемо як працює хеш-функція і деякі з її особливостей.

Lorem ipsum

Результат хеш функції для такого рядка буде наступний хеш:

A9A66978F378456C818FB8A3E7C6AD3D2C83E62724C CBDEA7B36253FB8DF5EDD

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras dapibus neque justo in condimentum metus tempus et. Mauris cursus, mauris et pellentesque tempor, lacus eros interdum orci, porta faucibus metus lacus id purus.

Результатом такого рядка буде хеш :

69733A6656C125D7B4F99E5485B149B29979AC1EF4D A9D171A503752F99C35C6

Візьмемо текст із попереднього прикладу, і заберемо крапку наприкінці:

7C9B07DB826C7E97647E220210E091FFC9555C35CC2 CAB810DA4DD4C772AF414

ВЛАСТИВОСТІ **ХЕШ-ФУНКЦІЇ:**

1.Швидкість. Швидкість обчислення хешу для будь-яких вхідних даних має бути максимально високою;
2.Односпрямованість . Не повинно бути способу обчислити вхідні дані з хеша;
3.Наявність лавинного ефекту. Найменша зміна у вхідних даних повинна кардинально змінювати хеш, без будь-яких посилань до попереднього хешу;
4.Стійкість до **колізій** ;
5.Стійкість до **атак.**

Криптографічна хеш-функція дає гарантію безпеки використання замість швидкості роботи, в той час як звичайна хеш-функція може бути швидше криптографічної, але значно програвати в безпеці.

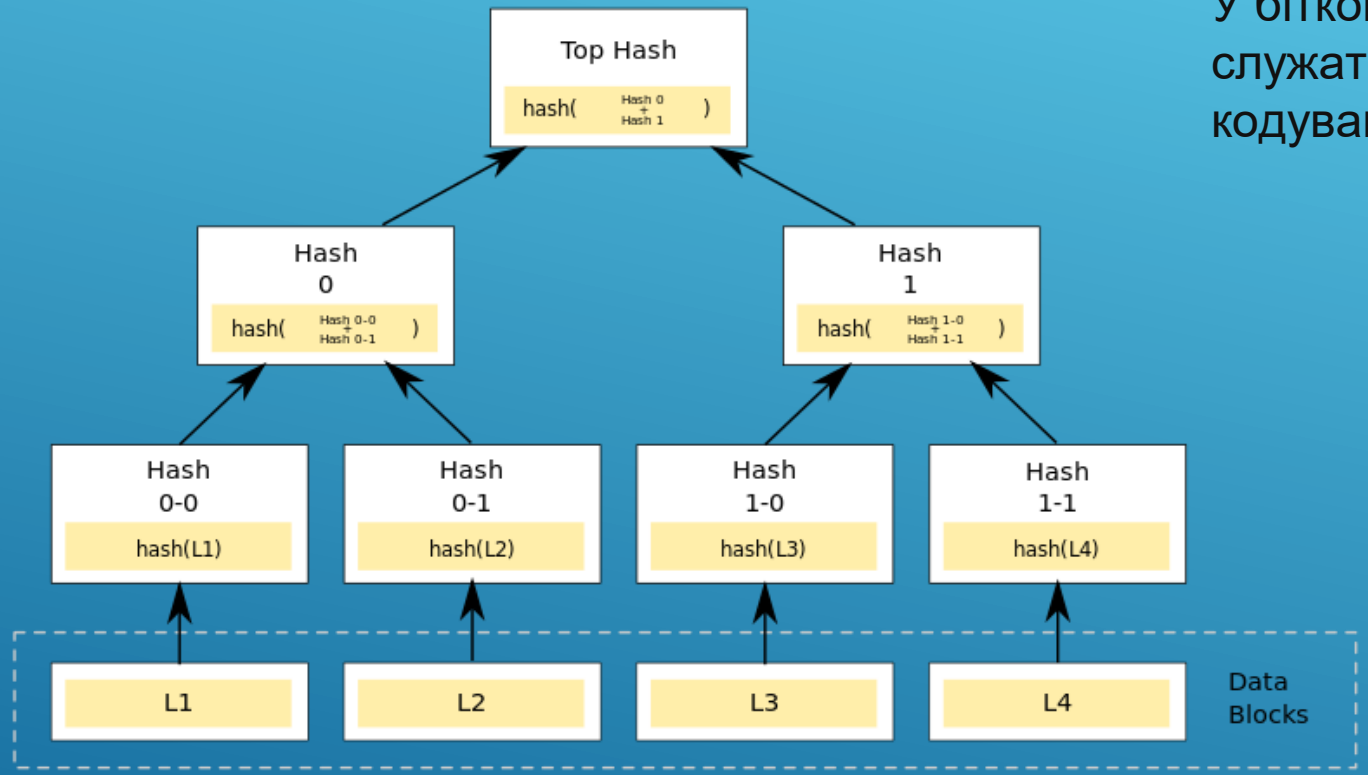
2 ДЕРЕВО МЕРКЛА (MERKLE TREE) - БІНАРНІ ДЕРЕВА

Дерево Меркла – це структура даних, яка використовується у додатках.

Хеш-деревом, **деревом Меркла** (англ. *Merkle tree*) називають повне двійкове дерево , у листові вершини якого вміщені хеші від блоків даних, а внутрішні вершини містять хеші від складання значень у дочірніх вершинах. Кореневий вузол дерева містить хеш від усього набору даних, тобто хеш -дерево є односпрямованою хеш-функцією.

У блокчейні біткойна блок транзакцій обробляється алгоритмом для генерації хеша , який є рядок цифр і літер, яка може використовуватися для перевірки того, що даний набір даних збігається з вихідним набором транзакцій, але не отримати вихідний набір транзакцій. Однак, програмне забезпечення Біткойна не обробляє весь блок даних транзакції, що представляє в середньому 10 хвилин на транзакцію, за допомогою хеш-функції за один раз. Швидше кожна транзакція хешується, потім кожна пара транзакцій об'єднується і хешується разом, і так далі, поки не буде один хеш для всього блоку. (Якщо кількість транзакцій непарна, одна транзакція подвоюється, а її хеш об'єднується із самим собою.)
Візуально ця структура нагадує дерево. На діаграмі нижче "T" означає транзакцію, "H" - хеш. Зверніть увагу, що зображення дуже спрощене; середній блок містить понад 500 транзакцій, а не вісім.

2 ДЕРЕВО МЕРКЛА (MERKLE TREE) - БІНАРНІ ДЕРЕВА

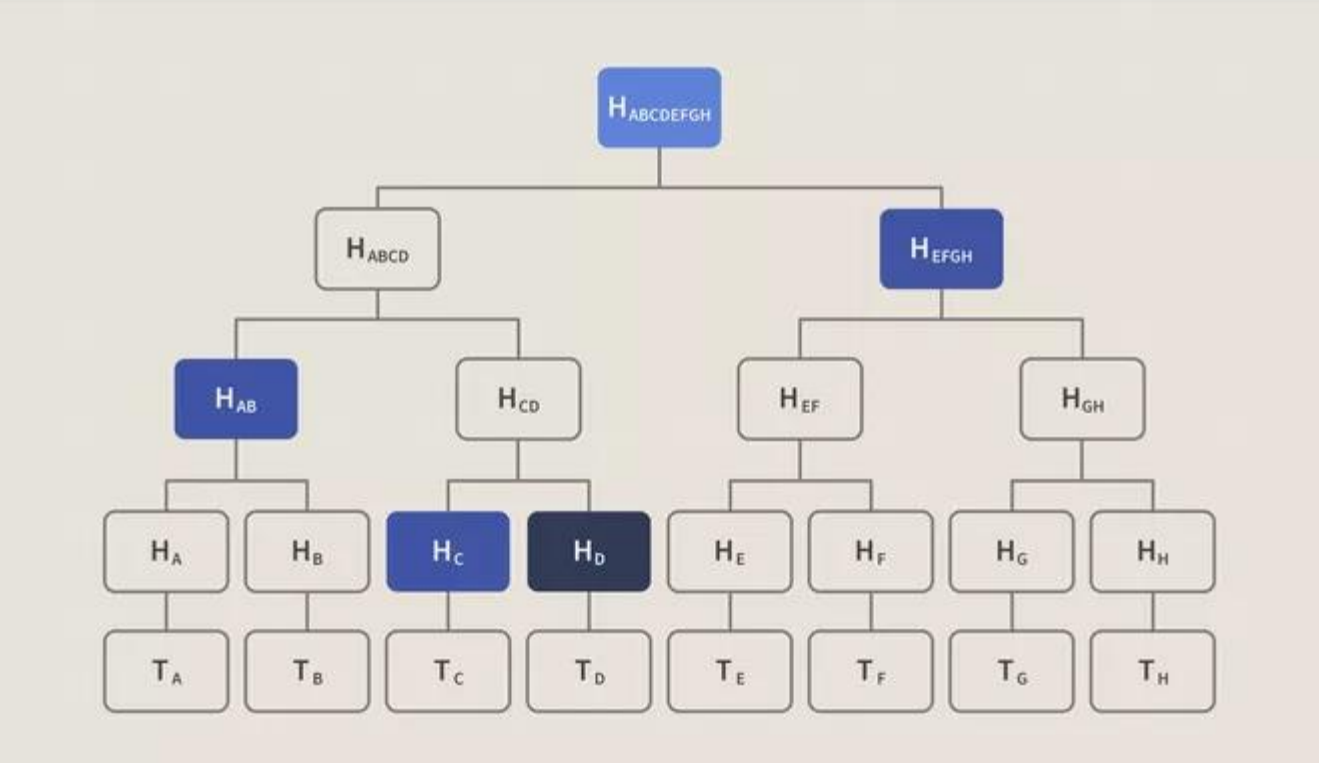


У біткойнах та інших криптовалютах дерева Меркла служать для більш ефективного та безпечного кодування даних блокчейну.

Хеші в нижньому рядку називаються «листями», проміжні хеші – «гілками», а хеш -значення вгорі – «коренем». Корінь Меркла цього блоку зберігається в заголовку: наприклад, корінь Меркла блоку # 482819 - це e045b18e7a3d708d686717b4f44db2099aabcad9bebf968de5f7271b458f71c8.

Корінь об'єднується з іншою інформацією (версія програмного забезпечення, хеш попереднього блоку, мітка часу, мета складності та одноразовий номер), а потім проходить через хеш-функцію для отримання унікального хеш -коду блоку: 00000000000000000bfc767ef8bf28c42cbd4bdbafd9aa1b5c3c33c2b089594 # 481928. Фактично, цей хеш включається не у відповідний блок, а наступний; він відрізняється від кореня Меркла.

2 ДЕРЕВО МЕРКЛА (MERKLE TREE) - БІНАРНІ ДЕРЕВА



Дерево Меркла корисне, тому що воно дозволяє користувачам перевіряти конкретну транзакцію без завантаження всього ланцюжка блоків (понад 350 гігабайт на кінець червня 2021). Наприклад, припустимо, що ви хочете переконатися, що транзакція T_D включена до блоку на діаграмі вище. Якщо у вас є кореневий хеш ($H_{ABCDEFGH}$), процес схожий на гру в судоку : ви запитуєте мережу про H_D, і вона повертає H_C, H_{AB} і H_{EFGH}. Дерево Меркла дозволяє перевірити, що все враховано за допомогою трьох хешів : заданих H_{AB}, H_C, H_{EFGH} та кореня

$H_{ABCDEFGH}$ (наш H_D (єдиний відсутній хеш) повинен бути присутнім у даних).

Наприклад, розглянемо блок із семи транзакцій. На найнижчому рівні (називається кінцевим) буде чотири хеші транзакцій. На рівні один вище кінцевого буде два хеш транзакції, кожен з яких буде з'єднуватися з двома хеш, що знаходяться нижче їх на кінцевому рівні. Нагорі (рівень два) буде останній хеш транзакції, званий коренем, і він з'єднуватиметься з двома хешами нижче за нього (на рівні один).

Фактично ви отримуєте перевернене двійкове дерево, в якому кожен вузол дерева з'єднується тільки з двома вузлами під ним (звідси і назва «бінарне дерево»). Він має один кореневий хеш нагорі, який з'єднується з двома хешами на рівні один, кожен з яких знову з'єднується з двома хешами на рівні три (кінцевий рівень), і структура продовжується залежно від кількості хеш транзакцій.

2 **ДЕРЕВО МЕРКЛА (MERKLE TREE)** - БІНАРНІ ДЕРЕВА

Корінь Меркла - це хеш усіх хешів усіх транзакцій, які є частиною блоку мережі ланцюжка блоків.

- Корінь Меркла – це простий математичний спосіб перевірки даних на дереві Меркла.
- Коріння Меркла використовується в криптовалюті, щоб гарантувати, що блоки даних, що передаються між одноранговими вузли в одноранговій мережі, є цілими, непошкодженими і незмінними.
- Коріння Меркла відіграють центральну роль у обчисленнях, необхідних для підтримки криптовалют, таких як біткойн та ефір.

Відео для перегляду:
Російська за бажанням:
https://www.youtube.com/watch?v=yTon4GUqth0
Англійською: http://surl.li/etwur

КОРІНЬ МЕРКЛА

Блокчейн складається з різних блоків, пов'язаних один з одним (звідси назва блокчейн). Хеш-дерево, або дерево Меркла , ефективно та безпечно кодує дані блокчейну. Він забезпечує швидку перевірку даних блокчейна, а також швидке переміщення великих обсягів даних з одного комп'ютерного вузла на інший в одноранговій мережі блокчейнів.

Кожна транзакція, що відбувається у мережі блокчейн, має пов'язаний із нею хеш. Однак ці хеші не зберігаються в блоці в послідовному порядку, а скоріше у формі деревоподібної структури, так що кожен хеш пов'язаний зі своїм батьком відповідно до деревоподібного ставлення батько-нащадок.

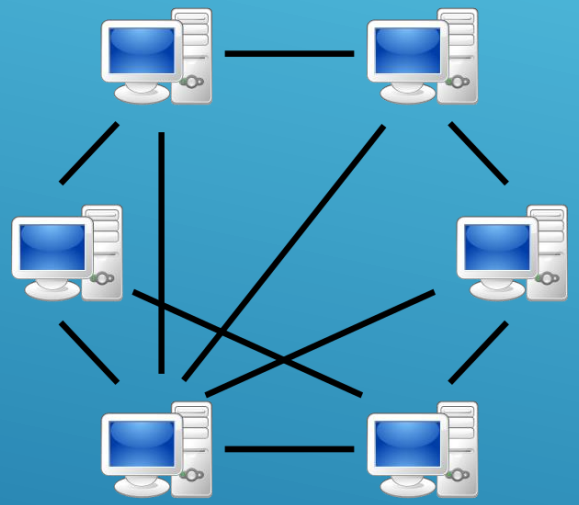
Оскільки в конкретному блоці зберігається безліч транзакцій, всі хеш транзакцій в блоці також хешуються , що призводить до кореня Меркла.

При значній кількості транзакцій у блоці складності обчислень не зростає

Кількість транзакцій	Приблизний розмір блоку	Розмір шляху (в хешах)	Розмр шляху в байтах
16 транзакцій	4 кілобайти	4 хеша	128 байт
512 транзакцій	128 кілобайт	9 хешів	288 байт
2048 транзакцій	512 кілобайт	11 хешів	352 байт
65535 транзакцій	16 мегабайт	16 хешів	512 байт

ОДНОРАНГОВІ МЕРЕЖІ

Peer-to-peer, **P2P** (з англ. — *рівний до рівного*) — варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів.



Комп'ютерні мережі типу peer-to-peer (або P2P) засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи можуть зв'язуватися між собою, на відміну від традиційної архітектури, коли лише окрема категорія учасників, яка називається серверами, може надавати певні сервіси іншим.

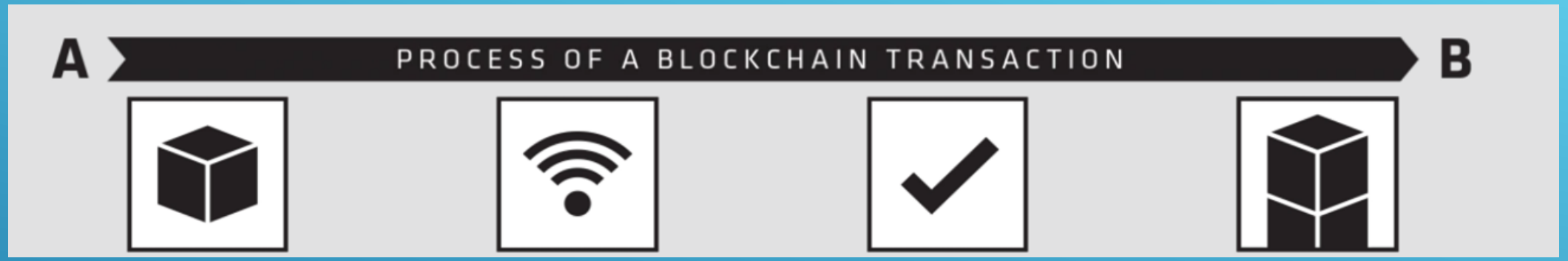
Фраза «peer-to-peer» була вперше використана у 1984 році Парбауелом Йонугуйтсманом (Parbawell Yohnuhuitsman) при розробці архітектури Advanced Peer to Peer Networking фірми IBM.

В чистій мережі «peer-to-peer» не існує поняття клієнтів або серверів, лише рівні вузли, які одночасно функціонують як клієнти та сервери по відношенню до інших вузлів мережі. Ця модель мережевої взаємодії відрізняється від клієнт-серверної архітектури, в якій зв'язок відбувається лише між клієнтами та центральним сервером. Така організація дозволяє зберігати працездатність мережі при будь-якій конфігурації доступних її учасників. Проте практикується використання P2P-мереж, які все ж таки мають сервери, але їх роль полягає вже не у наданні сервісів, а у підтримці інформації з приводу сервісів, що надаються клієнтами мережі.

В системі P2P автономні вузли взаємодіють з іншими автономними вузлами. Вузли є автономними в тому сенсі, що не існує загальної влади, яка може контролювати їх. В результаті автономії вузлів вони не можуть довіряти один одному та покладатися на поведінку інших вузлів, тому проблеми масштабування та надмірності стають важливішими ніж у випадку традиційної архітектури.

Сучасні P2P-мережі набули розвитку завдяки ідеям, пов'язаними з обміном інформацією, які формувалися у руслі того, що кожен вузол може надавати й отримувати ресурси, які надаються будь-якими іншими учасниками. У випадку мережі Napster це був обмін музикою, в інших випадках це може бути надання процесорного часу для пошуку інопланетних цивілізацій (SETI@home) або ліків проти раку (Folding@home).

3. СПЕЦІАЛЬНІ ТРАНЗАКЦІЇ.



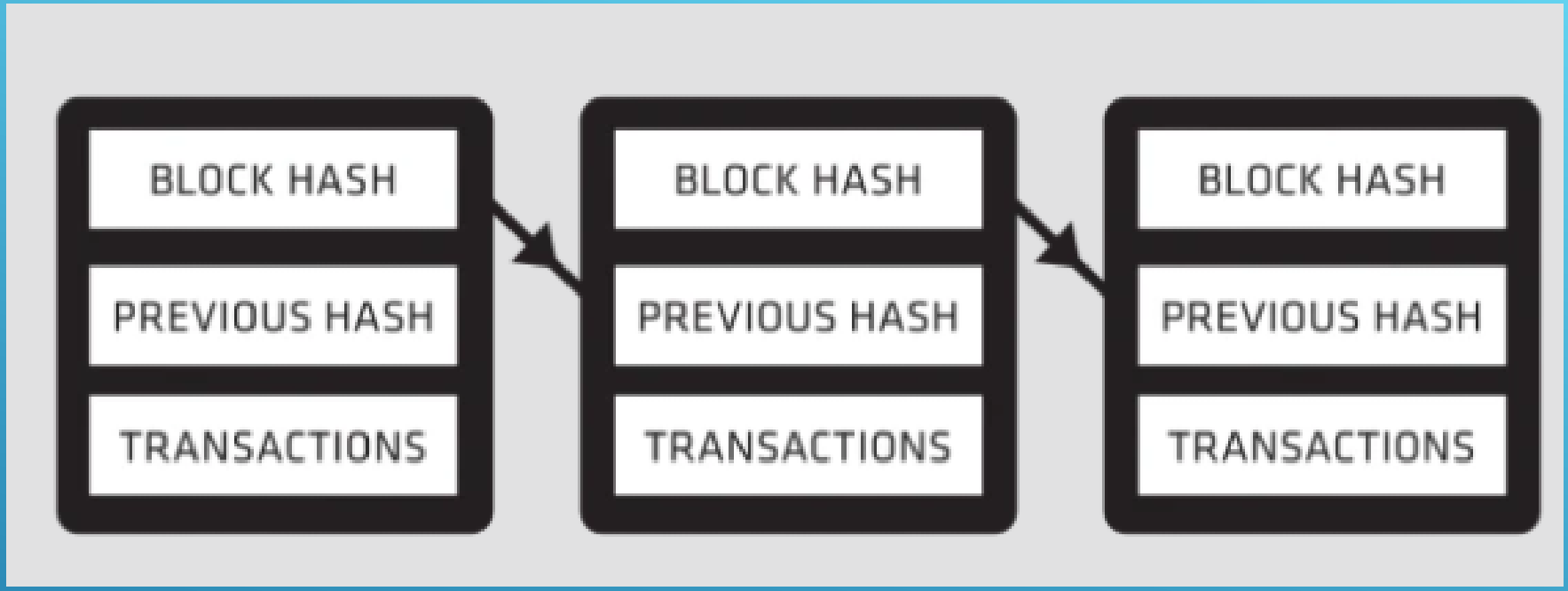
Користувач А відправляє транзакцію, щоби заплатити Користувачу В. Ця транзакція називається блоком

Цей блок транслюється кожному учаснику одноранговоі мережі для перевірки

Блок звіряється з кожним екземпляром реєстру. Якщо всі екземпляри реєстру співпадають, то транзакція затверджується

Виконання транзакції завершується, і блок додається як остання частина ланцюга блокчейну

Блокчейн - це система зберігання записів, в якій безліч незалежних джерел підтверджують достовірність запису, перш ніж вона буде додана в ланцюжок даних. Після того, як дані додані, вони не можуть бути змінені, і запис поширюється різними вузлами мережі. Додавання нового запису (називається блоком) у послідовність блокчейна вимагає встановлення її справжності безліччю учасників, підключених до мережі блокчейн. Ці блоки даних зв'язуються один з одним, утворюючи ланцюжок. Всі учасники блокчейну можуть бачити всі транзакції, що здійснюються, але особи всіх учасників приховані.



- **Хеш-код блоку**

Зашифрований рядок букв і цифр, який є постійним і унікальним для кожного блоку послідовного ланцюжка.

- **Хеш попереднього блоку Хеш**

-код, що використовується для ідентифікації з попереднього блоку, не дозволяє додавати блоки в середину ланцюжка.

- **Набір транзакцій**

Записи даних, які є підтвердженими учасниками доказом справжності бізнес-операцій.

1. Транзакції
Дві сторони обмінюються даними транзакціями; даними можуть бути гроші, контракти, медичні записи, документи, дані покупця або будь-які інші активи, які можуть бути описані в цифровій формі.

2. Підтвердження
Залежно від параметрів мережі транзакція підтверджується миттєво, або шифрується і поміщається в чергу транзакцій, що очікують підтвердження. У цьому випадку, ноди - комп'ютери та сервери в мережі - збирають транзакції в блоки і здійснюють валідацію - процедуру підтвердження (перевірки) відсутності спірних транзакцій у минулому, згідно з прийнятими правилами в мережі.

3. Структура
Кожен блок ідентифікується хеш, 256-бітним номером, створений з використанням алгоритму, узгодженого мережею. Блок містить заголовок, посилання на попередній блок хеш та групи транзакцій. Послідовність пов'язаних хешей створюють безпечний, взаємозалежний ланцюжок.

https://coinpost.finance/f/transactions-blockchain/

4. Перевірка

Блоки повинні бути перевірені на незмінність даних перед додаванням у блок-ланцюжок. Правила, якими здійснюється перевірка, називається **консенсусом.** Існує безліч механізмів консенсусу, застосування кожного залежить від потреб проекту.

5. Блокчейн майнінг

Майнери намагаються «вирішити» блок, методом підбору однієї змінної до рівняння доти, доки рішення не задовольнить цілі мережі. Такий алгоритм називається «Доказ виконання роботи» тому що правильні відповіді не можуть бути сфальсифіковані через особливість застосовуваних обчислень, що укладаються в асиметрії витрат часу. Вони значні на знаходження рішення і малі для перевірки.

http://radka.in.ua/poradi/sho-take-blokchein-iak-pracuye-lancuj.html

6. Вбудований захист

Якщо зловмисник намагається відправити змінений блок у ланцюжок, зміниться хеш-функція цього блоку та всі наступні блоки в ланцюжку. Інші вузли виявлять ці зміни та відхилять блок від основного ланцюга, запобігаючи корупції.

7. Ланцюжок

Коли блок проходить перевірку, майнери , які вирішили рівняння, отримують винагороду, а блок розподіляється по мережі та додається до основного ланцюга.

https://www.blockchain.com/explorer/prices, https://www.coursera.org/learn/cryptocurrency

4. HARD & SOFT FORK

Форк — це зміна основного протоколу блокчейну. Розгалуження блокчейну — це важливе оновлення мережі, яке може являти собою радикальні або незначні зміни та може бути ініційоване розробниками або членами спільноти.
Він вимагає від операторів вузлів — машин, підключених до блокчейну, які допомагають перевіряти транзакції в ньому — оновити протокол до останньої версії. Кожен вузол має копію блокчейну і гарантує, що нові транзакції не суперечать його історії.
Хардфорк — це радикальне оновлення, яке може зробити попередні транзакції та блокування дійсними або недійсними та вимагає від усіх валідаторів у мережі оновлення до новішої версії. Він не сумісний із попередніми версіями. Софтфорк — це оновлення програмного забезпечення, яке має зворотну сумісність і має валідатори в старішій версії ланцюжка, які бачать нову версію як дійсну.
По суті, хардфорк частіше за все призводить до постійного роз'єднання ланцюга, оскільки стара версія більше не сумісна з новою версією. Ті, хто тримає жетони на старому ланцюжку, також отримують жетони на новому, оскільки вони мають ту саму історію. Хардфорки можуть відбуватися з кількох причин.

http://surl.li/etwzc

https://tehnoobzor.com/cryptolife/o-kriptovaljutah/2748-chto-takoe-softfork-kriptovalyuty-i-dlya-chego-on-nuzhen.html

5. ОБМЕЖЕННЯ БЛОКЧЕЙНУ

Переваги та недоліки технології блокчейн у фінансовій сфері

Показники	Блокчейн	Інші IT технології
	переваги	**недоліки**
Децентралізація	Транзакція здійснюється через всю мережу, яка є гарантом здійснення операції	Транзакція здійснюється через певний центральний вузол
Смарт-контракт	Завчасно зарезервована сума на певний товар / послугу, автоматично відкладається і списується в момент його доставки	Відсутній. Необхідно самостійно контролювати наявність коштів на момент здійснення транзакції
Системи зберігання і захисту	Блокова система, що дозволяє тільки додавати інформацію	Бази даних, які схильні до зломів і нанесення шкоди / спотворення історичної інформації
Швидкість	Дев'ять транзакцій в секунду	Тисячі транзакцій в секунду
Інтеграція	Питання інтероперабельності технології в різних країнах і підтвердження правоздатностей контрагентів	Транскордонний сервіс миттєвих грошових переказів

TPS, або Transactions Per Second, вказує кількість транзакцій, які мережа блокчейну може обробляти за одну секунду. По суті, це показник швидкості та пропускної здатності мережі, який ілюструє її здатність обробляти велику

https://academy.binance.com/uk/articles/positives-and-negatives-of-blockchain

TRANSACTIONS PER SECOND, 2024 РІК

Кардано (ADA)

Хвилі

EHO

Stellar (XLM)

Трон (TRX)

Ripple (XRP)

Пульсація, відомий своєю високою швидкістю транзакцій, може обробляти до 1500 транзакцій на секунду з часом розрахунку лише 3-5 секунд. XRP пропонує значне вдосконалення порівняно зі своїми аналогами, такими як Ethereum, яким

Солана (SOL)

Ethereum (ETH)

Ethereum нещодавно завершив злиття та перейшов на Ethereum 2.0 Today, коли мережа виконує до 100 000 транзакцій на секунду. Хоча його швидкість перевірки все ще становить близько 13 [illegible] збільшення TPS [illegible] своєю [illegible] і [illegible] кандидатом для [illegible], досягнувши до 10 [illegible] транзакцій за секунду (TPS) через алгоритм консенсусу Tendermint. Однак фактична швидкість транзакцій може відрізнятися [illegible] перевантаженості мережі та

EOS

[illegible]

6. ПРИВАТНИЙ ТА ПУБЛІЧНИЙ БЛОКЧЕЙН.

Ще в 2015 році Віталій Бутерін , один із засновників шифрування Ethereum , визначив три різні типи блокчейна, це:

1.Публічний блокчейн ;

2.Блокчейн консорціуму : гросбух, що належить консорціуму. Усі транзакції там координуються вузлами, вибраними консорціумом;

3.Повністю закритий блокчейн : облік транзакцій, що координується центральним органом.

6. ПРИВАТНИЙ ТА ПУБЛІЧНИЙ БЛОКЧЕЙН.

У той же час сер Марк Уолпорт , головний науковий радник уряду Великобританії, пропонує інший набір блокчейнів :
1.Неопубліковані (відкриті) публічні гросбухи;
2.Дозволені (закриті) публічні гросбухи;
3.Дозволені (закриті) приватні гросбухи.

6. ПРИВАТНИЙ ТА ПУБЛІЧНИЙ БЛОКЧЕЙН.

Публічний (відкритий) та приватний (закритий) .
Перший тип включає спочатку незапущені (закриті) списки записів у регістрі.
Другий повністю відкритий і не потребує наглядового органу.

Загальні точки

1.Обидві децентралізовані мережі **P2P** використовують загальні регістри транзакцій. Як правило, такі системи використовуються для створення надійних платформ для обміну криптовалютами .
2.Обидва використовують спеціальні правила (механізми консенсусу) для вирівнювання вмісту регістру.
3.Обидва гарантують цілісність реєстру у разі зіткнення із шахраями або хакерами. Ви можете перевірити список, який забезпечить високий рівень безпеки .

ПЕРЕВАГИ ПУБЛІЧНОГО БЛОКЧЕЙНУ:

відсутність наглядового органу дозволяє розробляти децентралізовані програми

Немає жодної цензури . У відкритій системі досить складно змінити життєво важливі елементи, не переймаючись іншими частинами. У результаті відкриті регістри забезпечують вищий рівень довіри. Насправді слабкість – це сила!

Захист даних за розумною ціною . Крім того, щоб атакувати відкритий регістр, хакерам знадобиться набір справді потужних рішень. Іншими словами, злом загальнодоступної мережі не є економічно ефективним навіть для найрішучіших зловмисників.

Сильний мережевий ефект . У відкритій системі у розробника більше шансів зібрати користувачів навколо нової програми. Справа в тому, що всі частини відкритої книги можуть зв'язуватися один з одним безпосередньо з будь-якої частини земної кулі. Таким чином, інформація поширюється в одну мить. Зазвичай цього достатньо, щоб ваші інтернет-гаманець підтримували доступні програми, щоб залишатися в курсі подій.

ПЕРЕВАГИ ПРИВАТНОГО БЛОКЧЕЙНУ:

приватні блокчейни обмежують доступ до транзакцій між частинами . Всі важливі функції, включаючи перевірку транзакцій, аудит та координацію бази даних, доступні обмеженій кількості осіб . Іншими словами, приватний блокчейн є централізованою системою з її власним набором правил.

1.Дешевші транзакції . На відміну від публічного блокчейну є закритою мережею, всі транзакції між частинами перевіряються кількома уповноваженими особами.

2. Приватний блокчейн може похвалитися **вищим параметром транзакцій за секунду** (TPS), обмеженим пропускною здатністю найслабшого мережного вузла.

3. Оперативна перевірка транзакції .

4. Відкат транзакції . У разі потреби компанія, що володіє гросбухом, може скасувати транзакції та змінити баланс. Іноді цей підхід окупається і дозволяє запобігти передачі цінних активів шахраям.