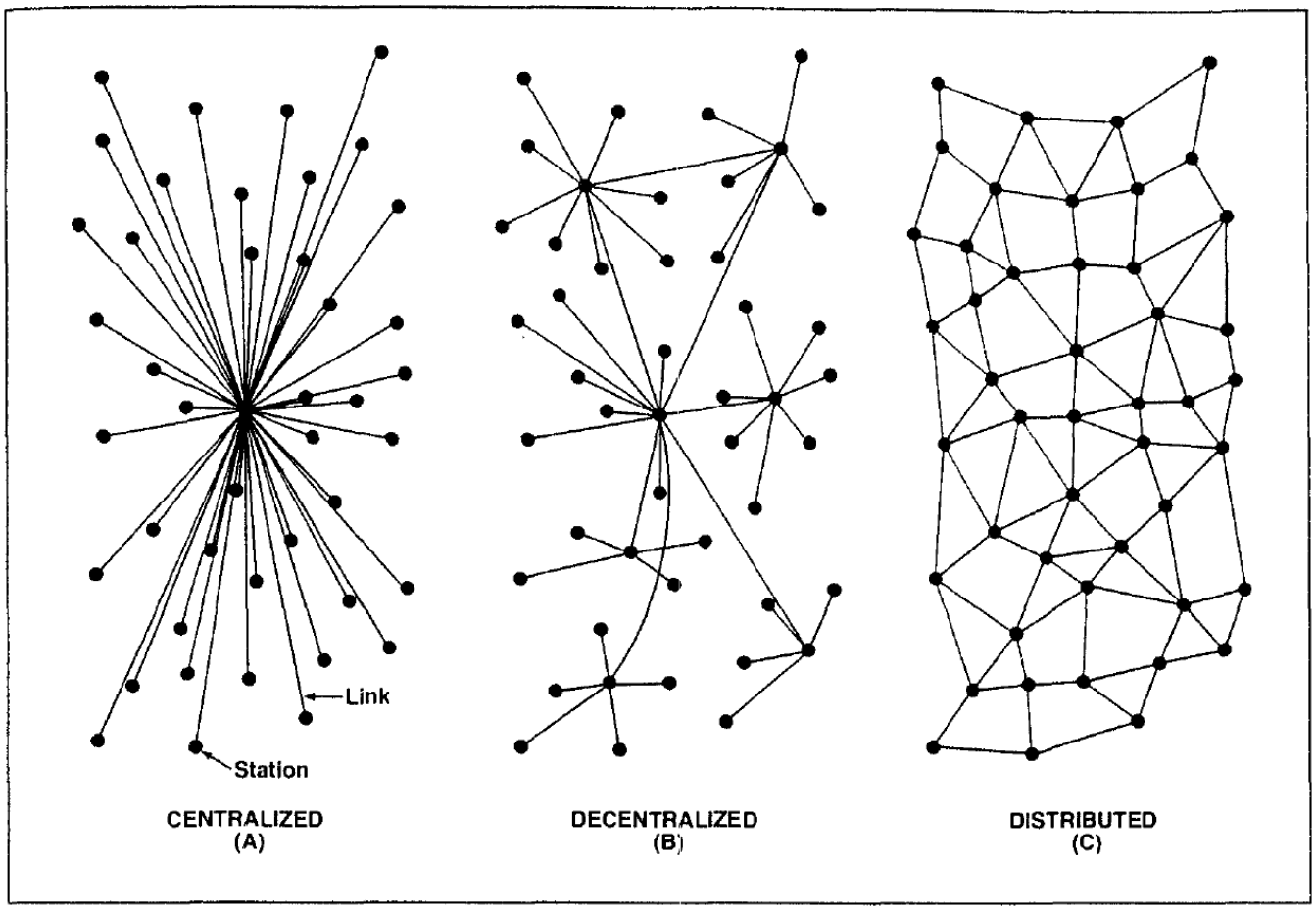
Біткоїн та криптовалютні технології
Лекція 6: Біткоїн-мережа

Юрій Жикін

17 березня, 2025

Однорангові мережі 1/2

- **Однорангова мережа** (**P2P-мережа**) - це система, яка розподіляє завдання або навантаження між *рівноправними*, *рівноцінними* вузлами, що називаються *пірами* або просто *вузлами*.



Однорангові мережі 2/2

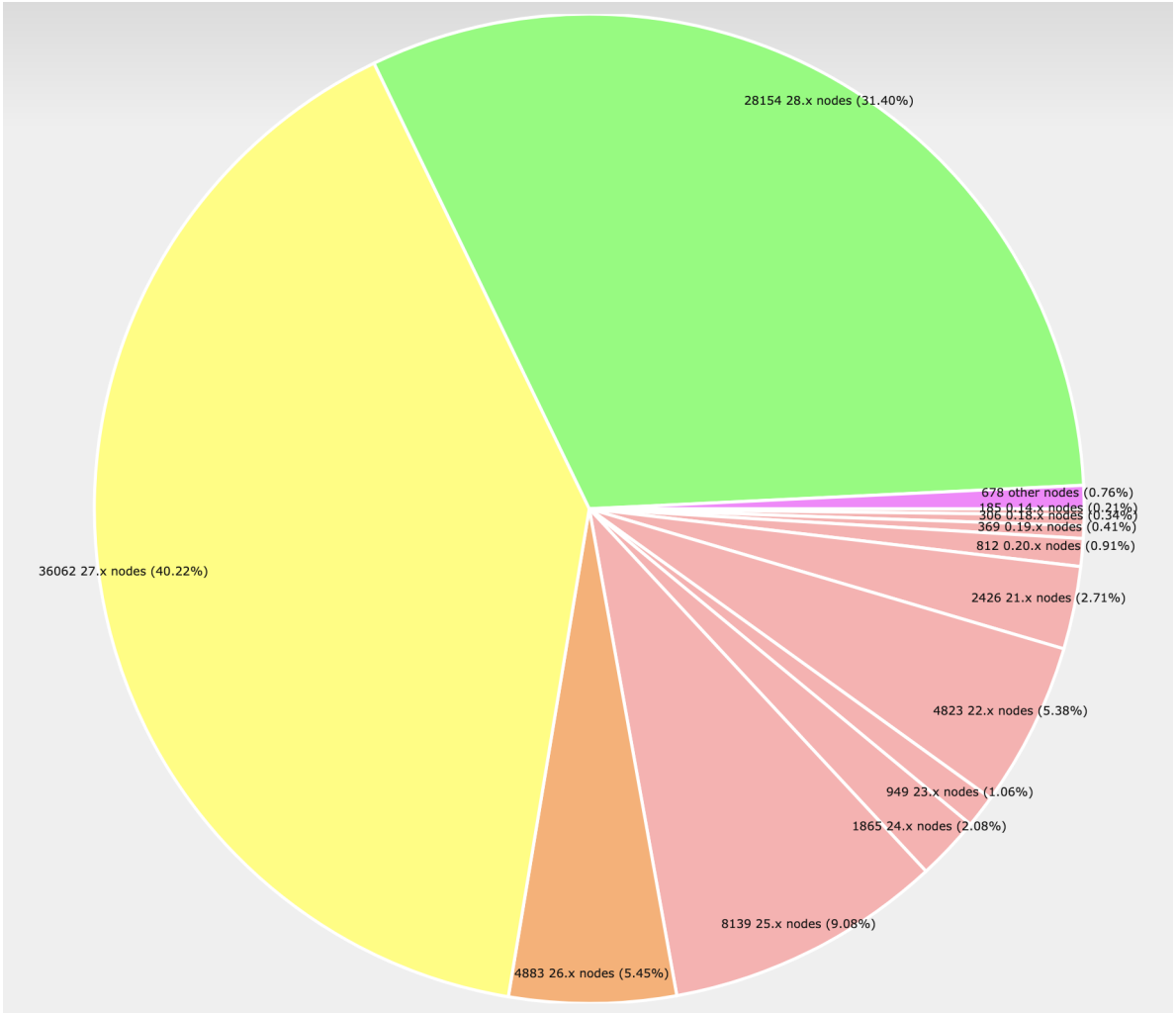
- У **централізованих** системах успішна атака на **сервер** виводить з ладу всю систему.
- У **децентралізованих** системах успішна атака на **вузол** призводить до тимчасового поділу мережі, але система продовжує функціонувати.
- У **однорангових** системах успішна атака на **вузол** не впливає на мережу, *якщо мережа достатньо велика*.
- Приклади: **Napster** та **BitTorrent**.

Біткоїн-мережа 1/2

- **Біткоїн-мережа** - це **однорангова** мережа, що складається з **Біткоїн-вузлів**, які поширюють блоки та транзакції за допомогою **протоколу пліток** і перевіряють їх відповідно до **правил консенсусу**.
- Згідно з bitnodes.io, Біткоїн-мережа має приблизно **21,000** *досяжних* вузлів, порівняно з 16,000 у 2022 році та 10,000 у 2021 році.
- Згідно з luke.dashjr.org, загальна кількість **повних** вузлів (тобто вузлів, що здійснюють перевірку даних ланцюга блоків) оцінюється приблизно у **100,000** вузлів.

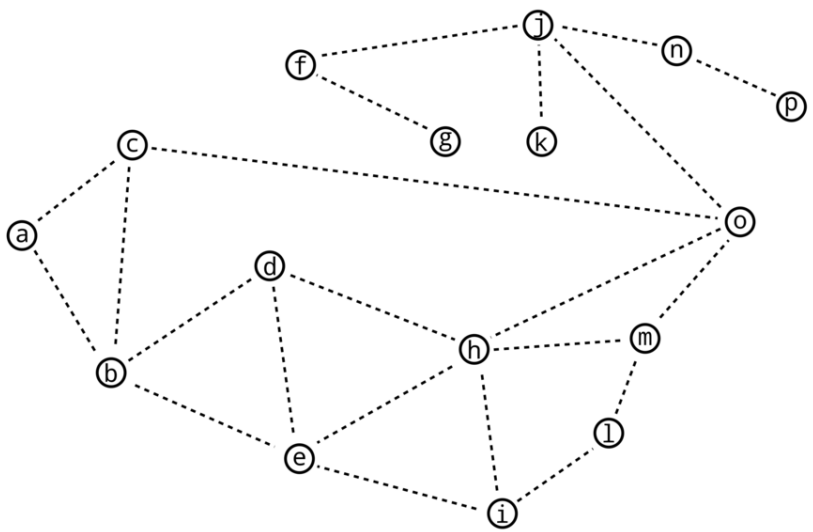
Біткоїн-мережа 2/2

- Згідно з luke.dashjr.org, 71.62% усіх вузлів працюють на найновішому програмному забезпеченні (Bitcoin Core 28.x, 27.x).



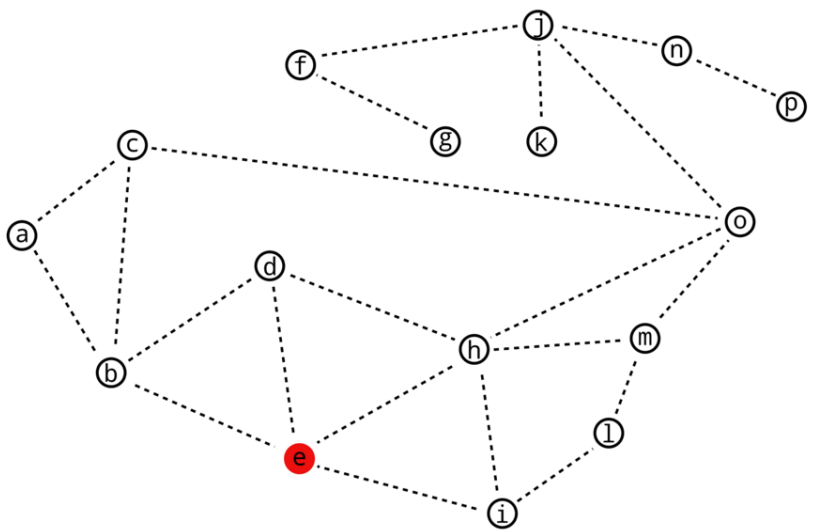
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоï комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



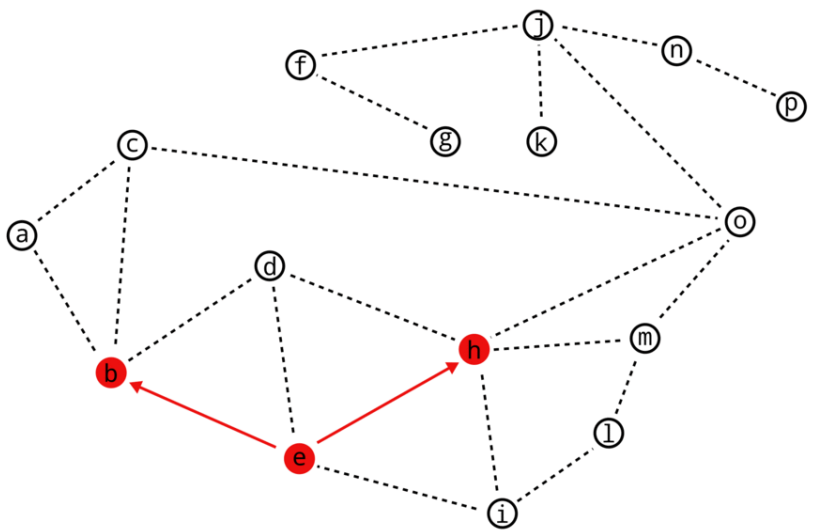
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоï комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



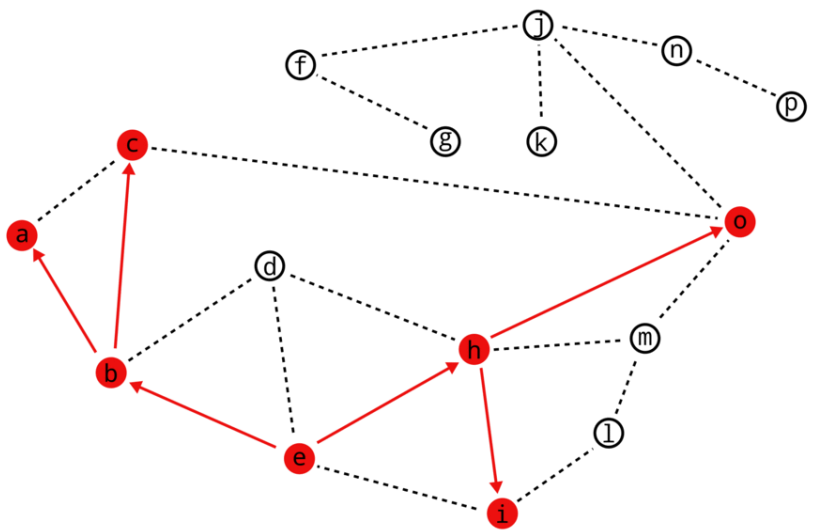
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоі комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



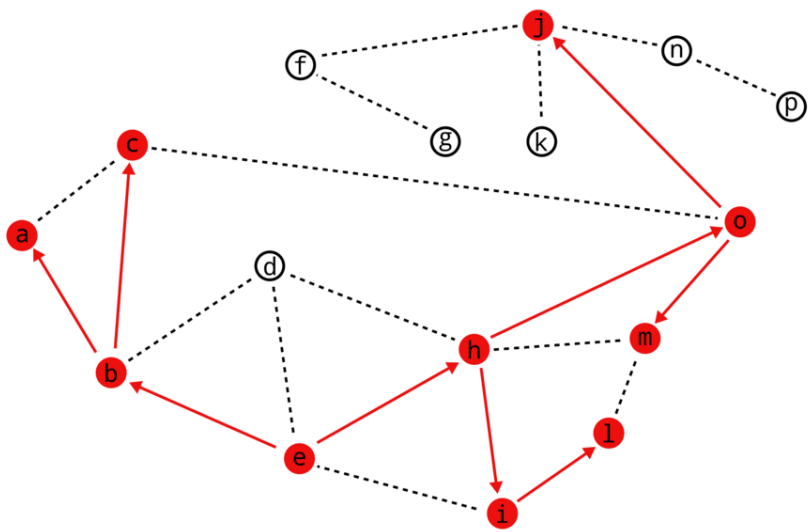
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоі комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



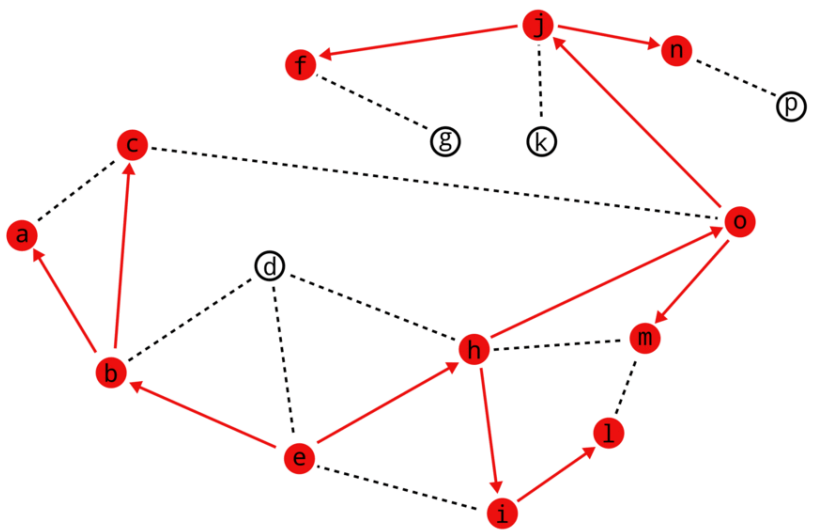
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоі комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



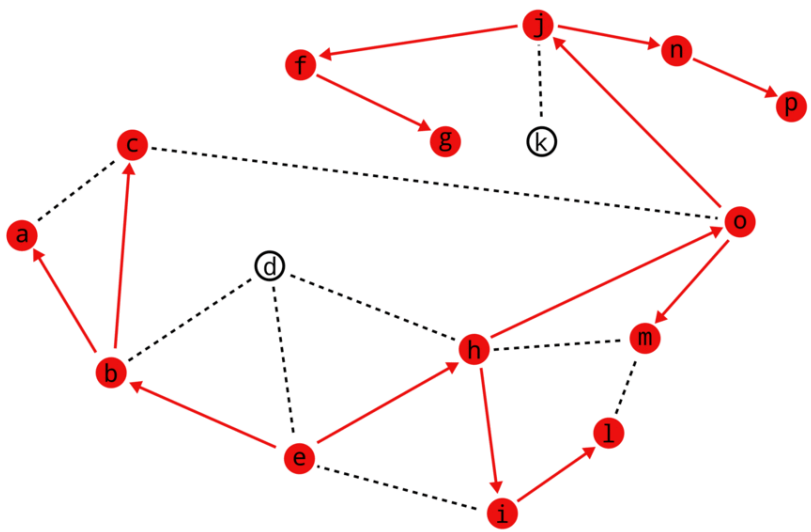
Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоі комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.



Протокол пліток

- **Протокол пліток (епідемічний протокол)** - це процес одноранговоі комунікації, заснований на принципі поширення пліток (або епідемій).
- **Отримання інформації від одного з сусідів і передача її якомога більшій кількості інших сусідів.**
- **Протокол пліток Біткоїн-системи** - це протокол поширення нових блоків і транзакцій у Біткоїн-мережі, який також забезпечує надання старих блоків з сховища новим вузлам.

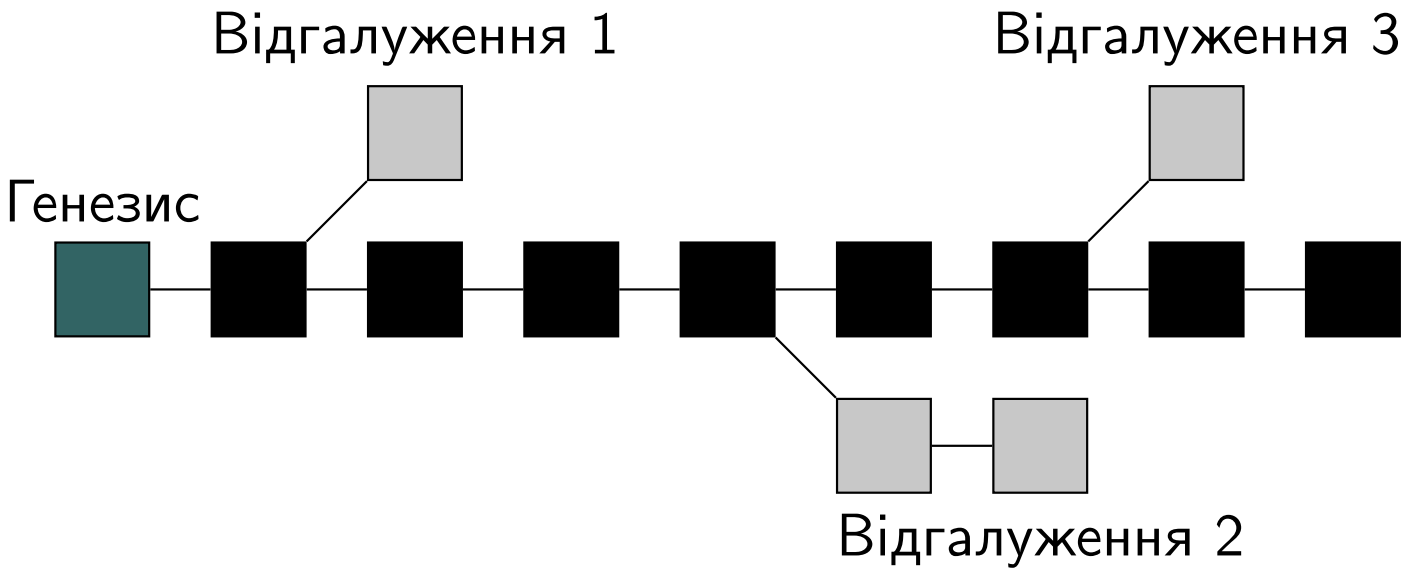


Вузол Біткоїн-мережі

- **Біткоїн-вузол** - це учасник мережі Bitcoin, програмне забезпечення, яке перевіряє блоки та транзакції і “пліткує” з іншими учасниками.
- Новий Біткоїн-вузол:
  - ініціалізує з’єднання з кількома вузлами через DNS-сервери,
  - виконує **початкове завантаження блоків** (**IBD**),
  - створює необхідні індекси (множина UTXO),
  - починає прослуховування пліток про нові блоки і транзакцій,
  - відхиляє недійсні блоки та транзакції,
  - приймає та ретранслює дійсні блоки і транзакції.

Реорганізація ланцюга 1/2

- Коли вузол отримує новий блок, який не належить до поточного ланцюга, він намагається під'єднати його до ланцюга, знайшовши **точку розгалуження**.
- Після під'єднання блоку, **ланцюг, на створення якого було витрачено більше енергії** (ланцюг з найбільшою **сукупною роботою**), обирається як дійсний ланцюг.



Реорганізація ланцюга 2/2

- **Робота ланцюга** (англ. **chainwork**) - це загальна кількість операцій хешування, яку було необхідно здійснити для створення поточного ланцюга (за оцінкою).
- **Початкове завантаження заголовків блоків** (англ. **headers-first IBD mode**) робить початкове завантаження блоків (IBD) ефективнішим, завантажуючи спочатку весь ланцюг у вигляді заголовків, а вже потім завантажуючи повні блоки для сконструйованого ланцюга.

Мемпул

- **Мемпул** (англ. **mempool**) - це структура даних у пам'яті, яка містить усі відомі дійсні транзакції, що ще не були включені до жодного блоку.
- Вузли підтримують **комбінована множина UTXO**, який складається з усіх UTXO у ланцюзі та всіх UTXO у мемпулі.
- Коли вузол отримує нову дійсну транзакцію, він додає її до мемпула.
- Коли вузол отримує новий дійсний блок, він видаляє з мемпула усі транзакції, що містяться в цьому блоці.
- Коли вузол отримує нову транзакцію, яка конфліктує з транзакцією у мемпулі, він відхиляє нову транзакцію, якщо вона не відповідає правилам **заміни за комісією** (англ. **RBF - Replace By Fee**).

Майнінг

- **Майнінгові вузли** - це звичайні вузли, які створюють нові блоки з транзакцій у mempool.
- Майнер вибирає певну кількість транзакцій (2000-4000, зазвичай у порядку зменшення комісії) для створення **шаблону блоку** відповідно до **обмеження розміру**.
- Майнінгове обладнання виконує обчислення методом грубої сили **доказу виконаної роботи** (**Proof of Work**) : $HASH256(Block) < Target$.
- Коли (якщо) блок "добуто" (тобто знайдено рішення PoW), майнер надсилає його в мережу через протокол пліток.
- Якщо інший майнер одночасно "добуває" інший блок, мережа вирішує конфлікт через реорганізацію ланцюга.

Життєвий цикл транзакції 1/2

- Транзакція **знищує** певну частину UTXO у ланцюзі та мемпулі і **створює** нову множину UTXO у мемпулі.
- **Фіналізована** дійсна транзакція поширюється через протокол пліток по всій мережі.
- Транзакція зазвичай залишається в мемпулі, доки її комісія не перевищить поріг включення у наступний блок.
- Поки транзакція знаходиться в мемпулі, її можна "підняти" в черзі за допомогою:
  - **заміни за комісією** (**Replace By Fee**, **RBF**), або
  - **"нащадок платить за предка"** (**Child Pays For Parent**, **CPFP**).

Життєвий цикл транзакції 2/2

- Рано чи пізно транзакція потрапляє в один із блоків.
- Після того як цей блок “здобуто” та поширено мережею, кожен вузол у мережі:
  - видаляє транзакцію з свого мемпулу,
  - застосовує транзакцію до множини UTXO (видаляє знищені UTXO та додає створені).
- На цьому етапі транзакція вважається **підтвердженою**.

Кінець

Дякую за увагу!