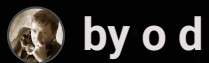


# MetaMask: Ваш Міст до Блокчейну

Локальний криптогаманець для безпечної взаємодії з блокчейном





# Основні терміни

Гаманець

Програма для зберігання  
приватного ключа

Приватний ключ

Секретний код






Публічна адреса

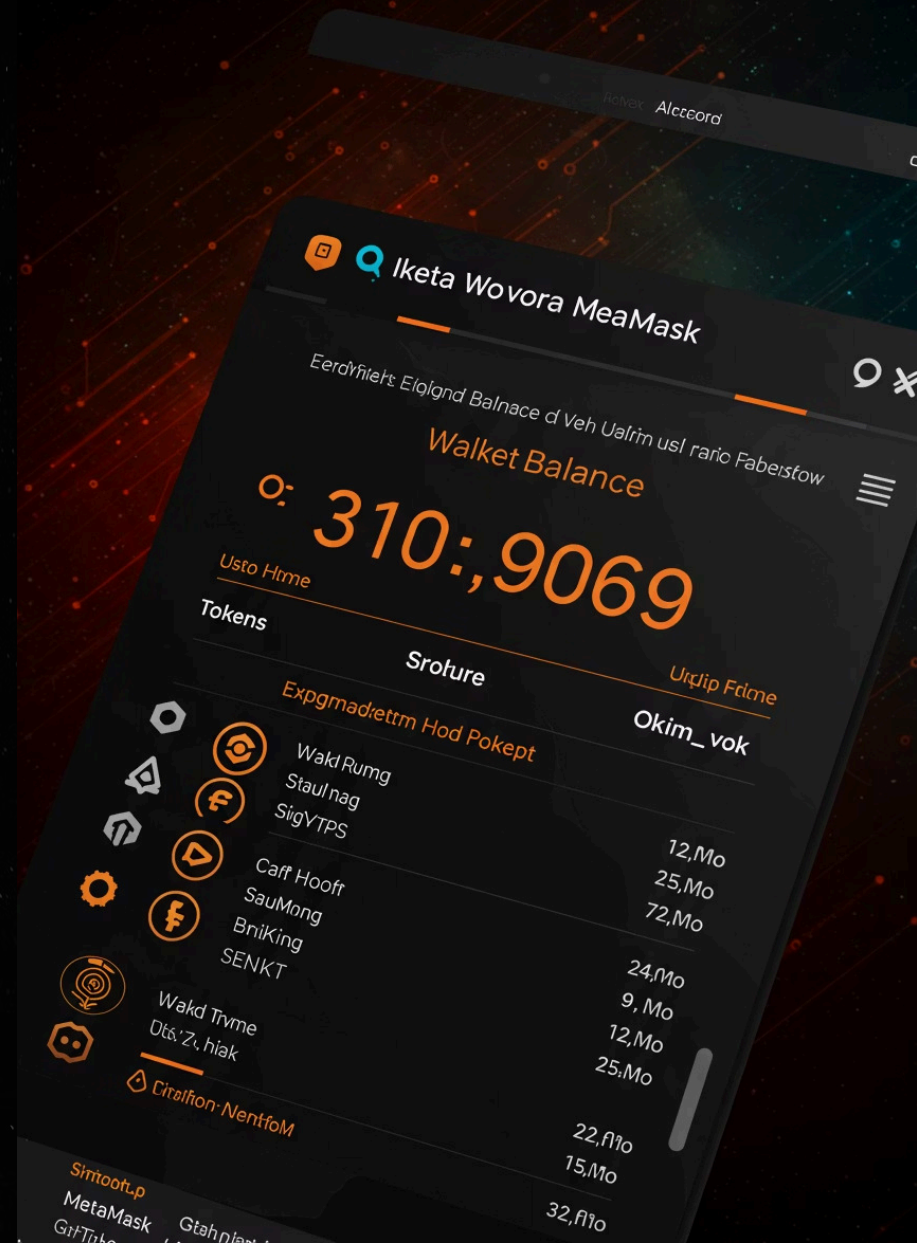
Відкрита адреса (0хABC...)

Транзакція

Повідомлення, що змінює стан  
блокчейну

# Що робить MetaMask?

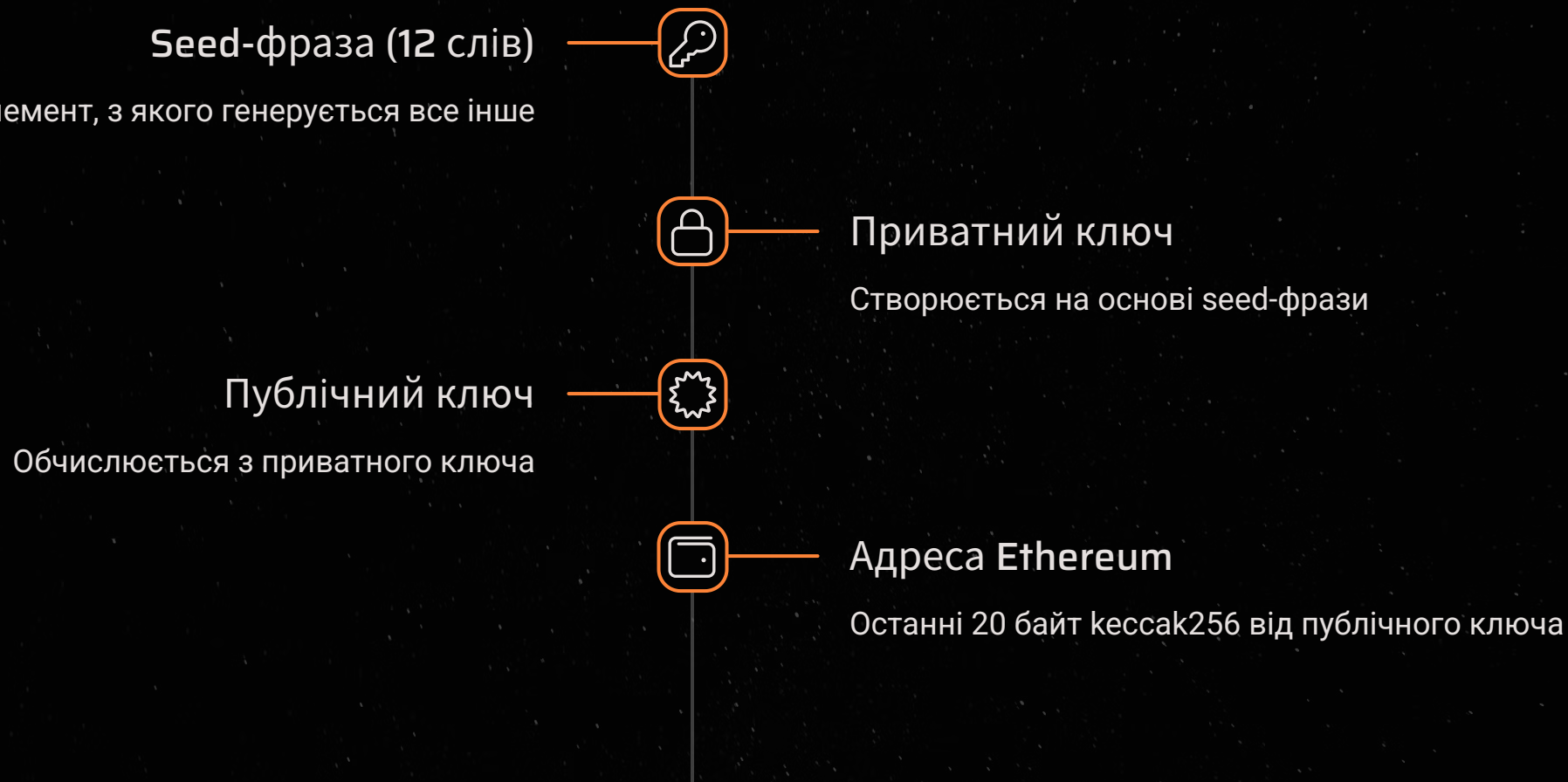
-  Зберігає ключ локально
-  Надає сайту доступ до акаунта користувача для підпису транзакцій і запитів до блокчейну
-  Показує баланс і токени (зчитує з блокчейну)
-  Підписує транзакції
-  Надсилає транзакції в мережу, яку обрав користувач





# Основний ланцюжок

Процес створення та виведення адреси Ethereum:





# Покрокова схема:

Як генерується адреса Ethereum із приватного ключа:



Генерується приватний ключ

Випадкове велике число: 0x48f1a2b3c4d5e6f7...



Обчислюється публічний ключ (ECDSA)

$0x04 + X + Y$  координати точки на кривій secp256k1

Цей ключ завжди відповідає приватному. Це математика, а не магія.



Обчислюється адреса Ethereum

$\text{keccak256}(\text{publicKey}) \rightarrow$  останні 20 байт  $\rightarrow$  адреса

`address = '0x' + keccak256(publicKey).slice(-40);`



## Висновок:

Твоя адреса генерується тільки з твого приватного ключа, і лише цей ключ може підписувати транзакції, які від імені цієї адреси приймаються блокчейном.



Чи адреса генерується з приватного?



Так, однозначно



Чи можна з адреси дізнатись ключ?



Ні, це одностороння функція (хешування + криптографія)



Чи можна довести, що це мій гаманець?



Так, тільки ти можеш підписати дані цим ключем

# Надсилання токенів

Процес надсилання криптовалюти через MetaMask складається з чотирьох послідовних етапів:



## Введення даних

Вкажіть адресу отримувача (0x...) та суму токенів. Перевірте наявність достатнього балансу та газу для оплати транзакції.



## Формування транзакції

MetaMask створює структуру транзакції з nonce, gasLimit, gasPrice, to, value та data полями. Для ERC-20 токенів використовується метод transfer() у data.



## Підпис приватним ключем

Ваш приватний ключ (що зберігається локально) криптографічно підписує транзакцію, доводячи, що саме ви її авторизували без розкриття ключа.



## Відправка в мережу

Підписана транзакція надсилається через RPC-з'єднання в mempool мережі. Майнери верифікують підпис та включають її в блок після підтвердження.

# Безпека MetaMask

Локальне зберігання

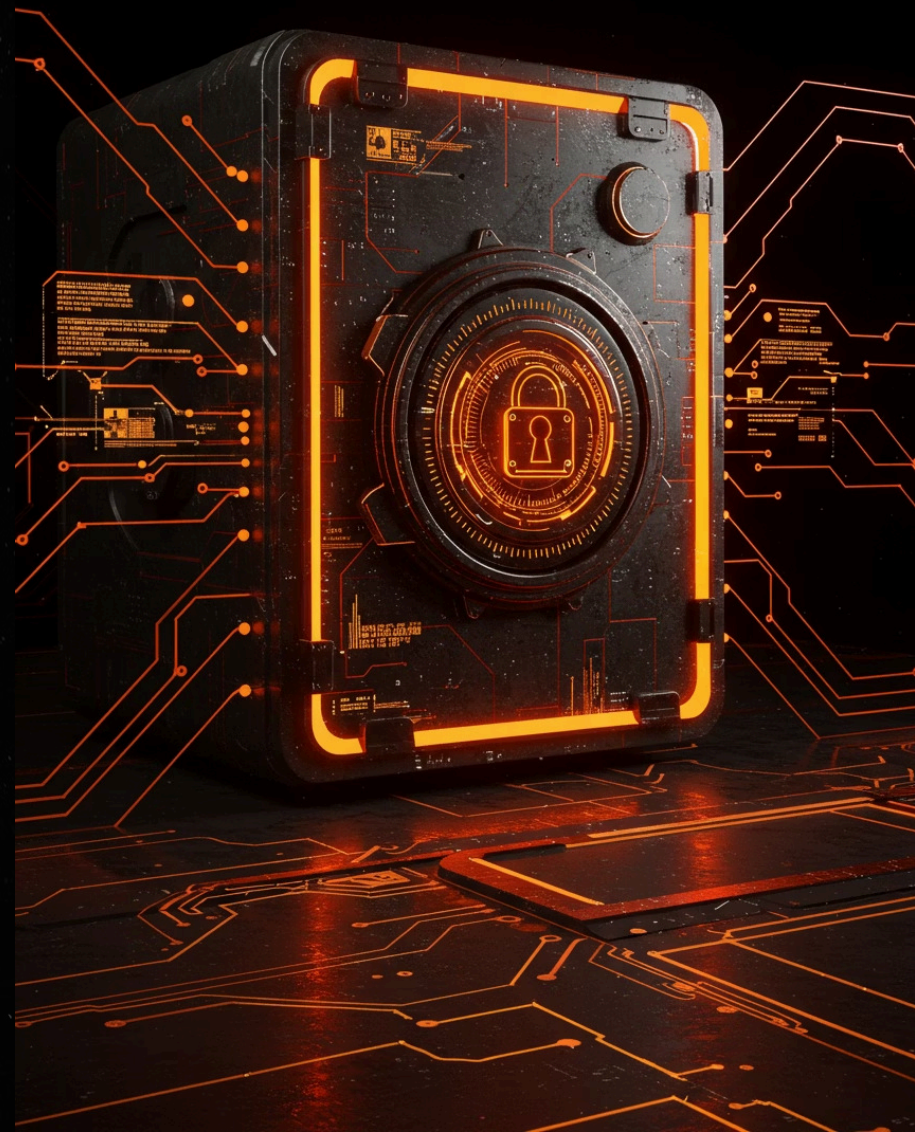
Ключ не залишає браузер

Шифрування

Пароль захищає доступ

Seed-фраза

12 слів для відновлення





# Підтримувані мережі

**Ethereum Mainnet**

Основна мережа

1

**Testnet**

Sepolia, Goerli



**Інші блокчейни**

Polygon, BSC



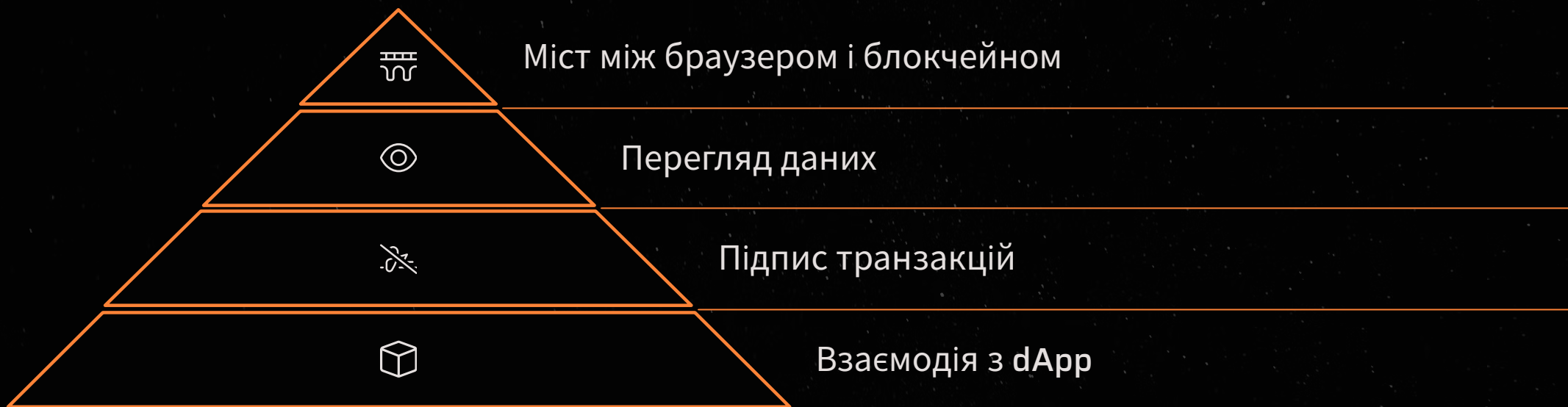
**Локальні мережі**

Ganache





# Ключова ідея MetaMask



# Генерація seed-фрази



Генерація в браузері

Створюється локально



Повна приватність

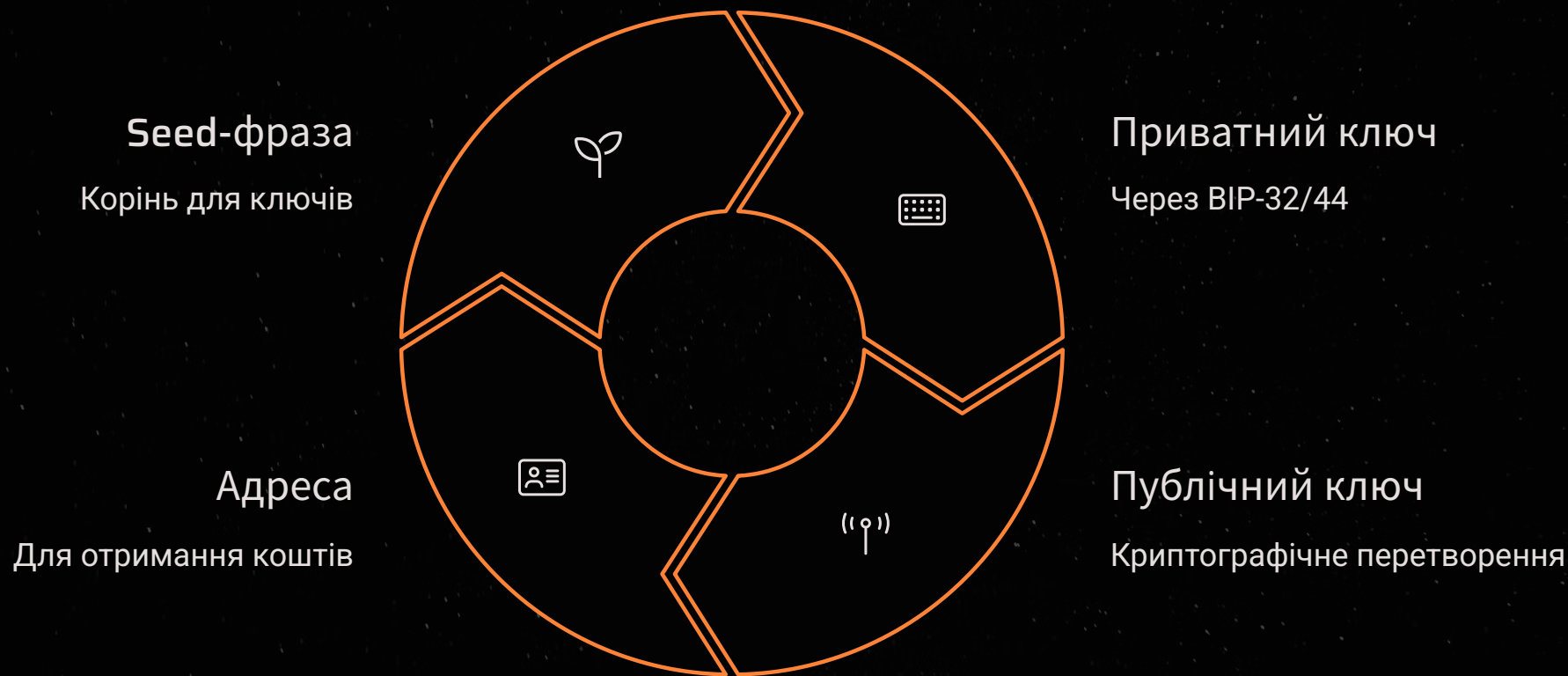
Не передається на сервери



Локальна криптографія

Всередині браузера

# Створення ключів



# Взаємодія з блокчейном



Користувач

Ініціює дію



MetaMask

Формує запит



RPC-вузол

Передає в мережу



Блокчейн

Обробляє транзакцію





# Що таке RPC-вузол?

👉 **RPC-вузол** — це **сервер**, через який MetaMask (і взагалі dApps) "бачать" блокчейн.

## Що таке RPC-вузол?

- має **повну копію блокчейну**
- приймає запити від клієнтів (твого браузера або MetaMask)
- відповідає через **JSON-RPC** інтерфейс

## Як працюють запити

📡 MetaMask надсилає запити на кшталт:

```
{
  "method": "eth_getBalance",
  "params": ["0x123..."]
}
```

І RPC-вузол повертає результат.

## Що таке RPC URL?

Це адреса до вузла, куди MetaMask надсилає запити, наприклад:

- <https://mainnet.infura.io/v3/<твій-ключ>> (Ethereum Mainnet)
- <https://rpc.sepolia.org> (Sepolia Testnet)
- <http://127.0.0.1:7545> (локальний вузол Ganache)

## 🔗 Як MetaMask знаходить або обирає RPC-вузол?

### 🌐 Стандартні мережі

Для основної мережі Ethereum і відомих тестових мереж (Sepolia, Goerli) MetaMask вже має **вбудовані RPC-адреси**, зазвичай через **Infura** (партнер MetaMask)

### ⚙️ Користувацькі мережі

Коли ти додаєш свою мережу (наприклад, Ganache), ти **вказуєш RPC вручну**:

```
Network Name: Ganache
RPC URL: http://127.0.0.1:7545
Chain ID: 1337
```

MetaMask не "знаходить" RPC автоматично — ти маєш додати його сам.

## 📡 Що робить RPC-вузол?

Функція	Приклад
📄 Отримати баланс	eth_getBalance(address)
📤 Надіслати транзакцію	eth_sendRawTransaction(signedTx)
🔍 Прочитати дані контракту	eth_call({ to, data })
📦 Отримати блок, транзакцію	eth_getBlockByNumber, eth_getTransactionByHash

🔥 **Висновок:** 🧠 **RPC-вузол** — це як "блокчейн-сервер", через який MetaMask взаємодіє з Ethereum. MetaMask обирає RPC-вузол **залежно від мережі**. Ти можеш вручну додати свій вузол. dApp завжди працює через RPC.

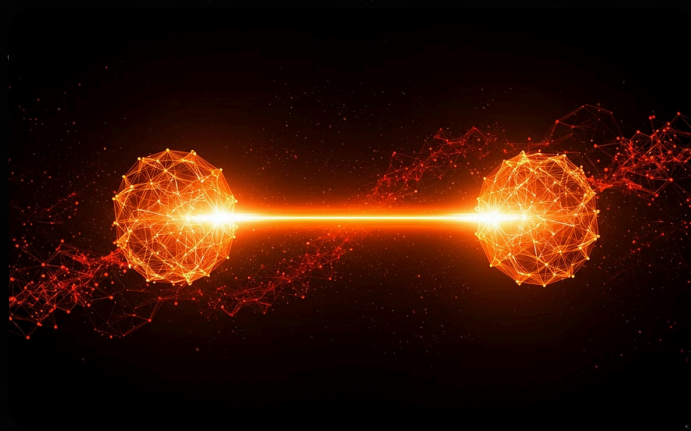


# Переваги локального гаманця



Самостійне зберігання

Повний контроль над активами



Без посередників

Пряма взаємодія з блокчейном



Приватність

Дані не передаються третім особам

# Порівняння з іншими гаманцями



## MetaMask

Локальний, у браузері



## Апаратні

Фізичні пристрої



## Мобільні

Додатки для смартфонів





# Ключові висновки

100%

Локальність

Всі операції виконуються на  
пристрої

0

Передача ключів

Приватні дані не залишають  
браузер

12

Слів у фразі

Достатньо для повного  
відновлення

