Web3

May, 2023

Các từ khóa quan trọng

1. Chuỗi khối (blockchain)
   - Mạng lưới các máy tính cùng lưu trữ dữ liệu giống nhau
   - Ví dụ: Bitcoin, Ethereum

2. Tiền kỹ thuật số (crypto-currency)
   - Được phát hành trên chuỗi khối và quản lý bằng ví
   - Ví dụ: BTC, ETH

3. Web3
   - Ứng dụng web dùng chuỗi khối để lưu trữ và thể hiện logic
   - Ví dụ: DeFi, chợ NFT

Bitcoin và Ethereum

Chuỗi khối	Lịch sử	Công nghệ	Điểm nổi bật
Bitcoin	2008 bởi Satoshi Nakamoto	Giao dịch toàn cầu không biên giới Lưu trữ tài sản (store-of-value)	Phi tập trung, thanh toán và chuyển tiền không qua ngân hàng Giải quyết bài toán chi tiêu 2 lần (double spending)
Ethereum	2015 bởi Vitalik Buterin	Hợp đồng thông minh (smart contract) Phát hành tiền kỹ thuật số khác (token)	Định nghĩa logic, mối liên hệ trong các giao dịch tài chính

Source: The Great Unwind - TOKEN2049 Singapore 2022

8
9
ПРЦ-2.50

- Ví dụ: tìm số Nonce thỏa mãn

SHA256("blockchain" + Nonce) bắt đầu với "**000000**"

- Quá trình đào (mining)
  - SHA256("blockchain**0**") = 0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
  - SHA256("blockchain**1**") = 0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10
  - ….
  - SHA256("blockchain**10730895**") = 0x**000000**ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587

Web 1.0

"Read Only",
Decentralized

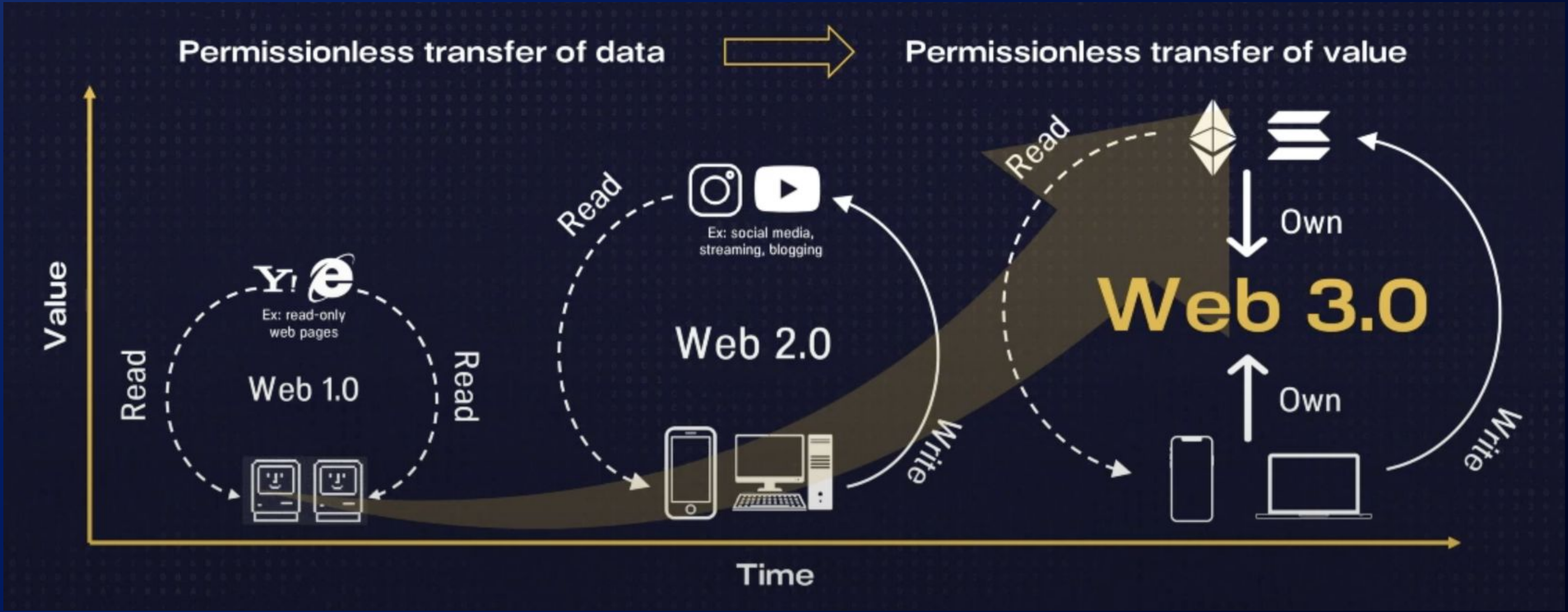
Web 2.0

Participatory,
Centralized

Web 3

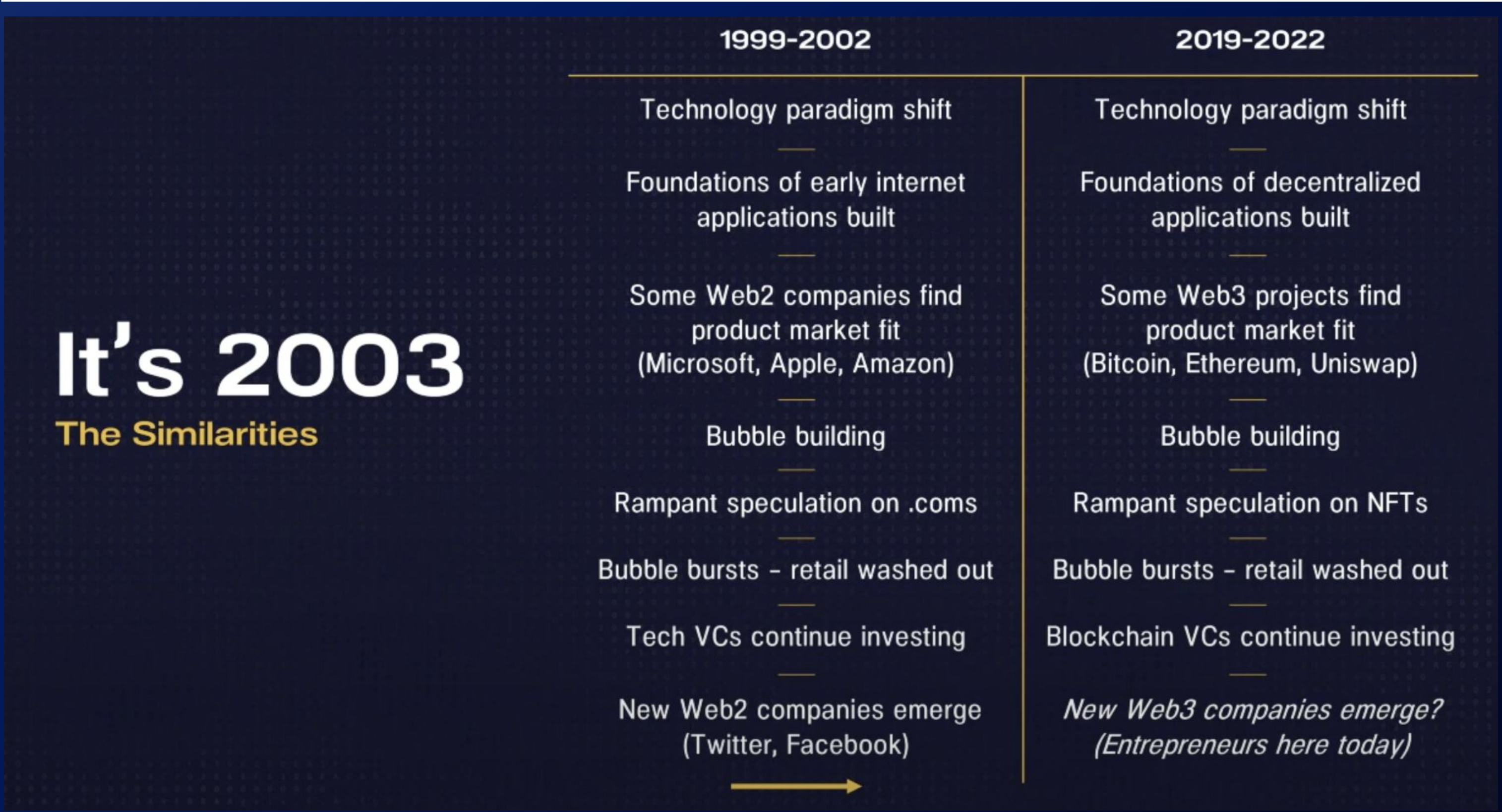
No Intermediaries,
Decentralized

Sự dịch chuyển


Permissionless transfer of data
Permissionless transfer of value
Value
Time
Read
Read
Ex: read-only web pages
Web 1.0
Read
Ex: social media, streaming, blogging
Web 2.0
Write
Read
Own
Web 3.0
Own
Write

Source: The Great Unwind - TOKEN2049 Singapore 2022

Bubble công nghệ



It’s 2003

The Similarities

1999-2002	2019-2022
Technology paradigm shift	Technology paradigm shift
Foundations of early internet applications built	Foundations of decentralized applications built
Some Web2 companies find product market fit (Microsoft, Apple, Amazon)	Some Web3 projects find product market fit (Bitcoin, Ethereum, Uniswap)
Bubble building	Bubble building
Rampant speculation on .coms	Rampant speculation on NFTs
Bubble bursts - retail washed out	Bubble bursts - retail washed out
Tech VCs continue investing	Blockchain VCs continue investing
New Web2 companies emerge (Twitter, Facebook)	*New Web3 companies emerge? (Entrepreneurs here today)*

Source: The Great Unwind - TOKEN2049 Singapore 2022

WEB3 LIMITATIONS

- Accessibility
- User experience
- Education
- Centralized infrastructure

A CLOSER LOOK

BLOCKCHAIN

Data can only be written to the Ethereum blockchain

EVM

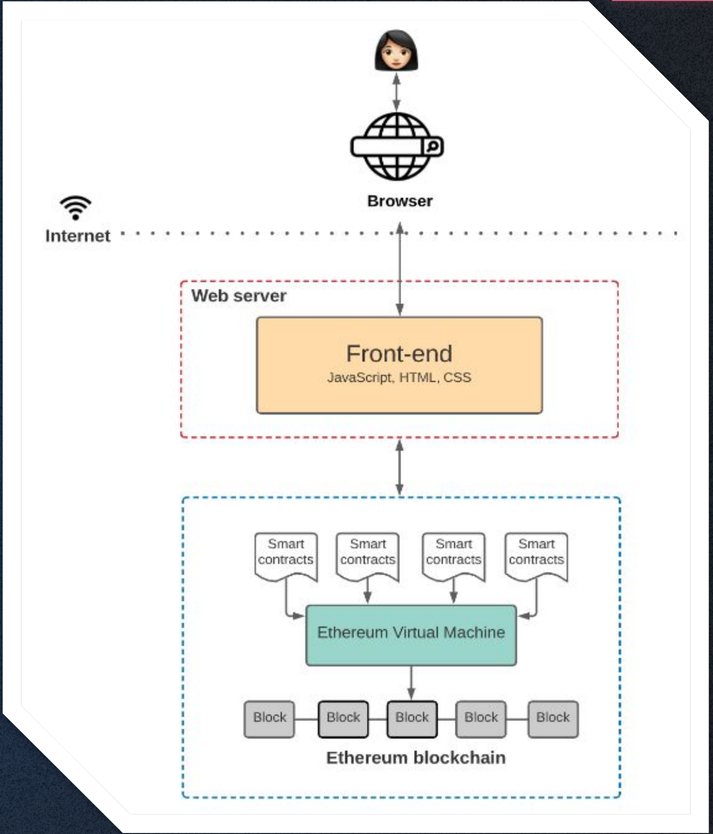
Executes the logic defined in the smart contracts and processes the state changes

SMART CONTRACTS

Defines the logic behind the state changes happening on the blockchain

FRONT-END

Defines the UI logic and communicates with the application logic defined in smart contracts

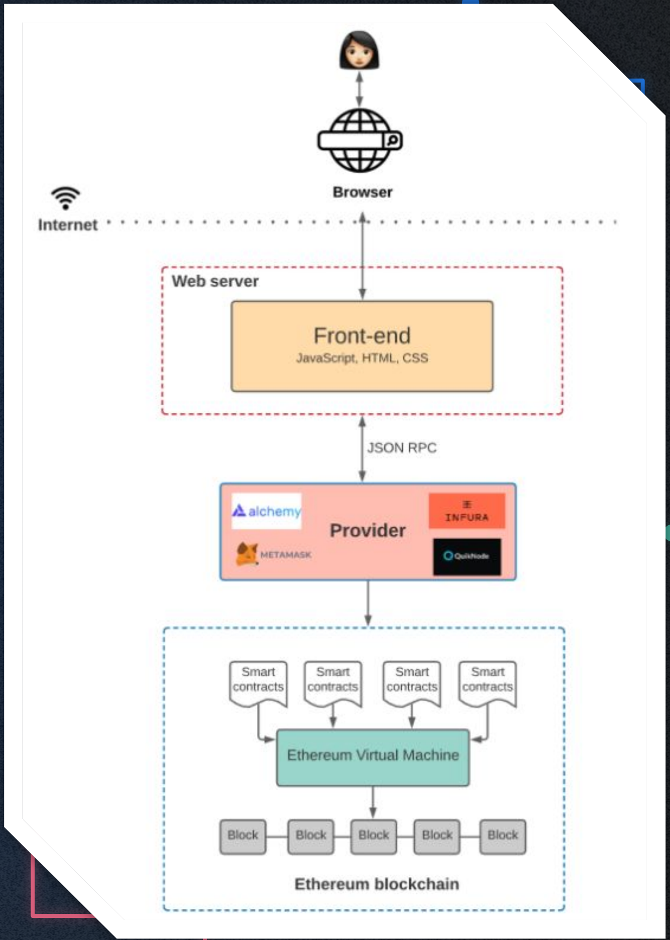


HOW DOES FRONTEND CODE COMMUNICATE WITH SMART CONTRACTS?

There are two ways to broadcast a new transaction:

- Set up your own node which runs the Ethereum blockchain software
- Use nodes provided by third-party services like Infura, Alchemy, and Quicknode

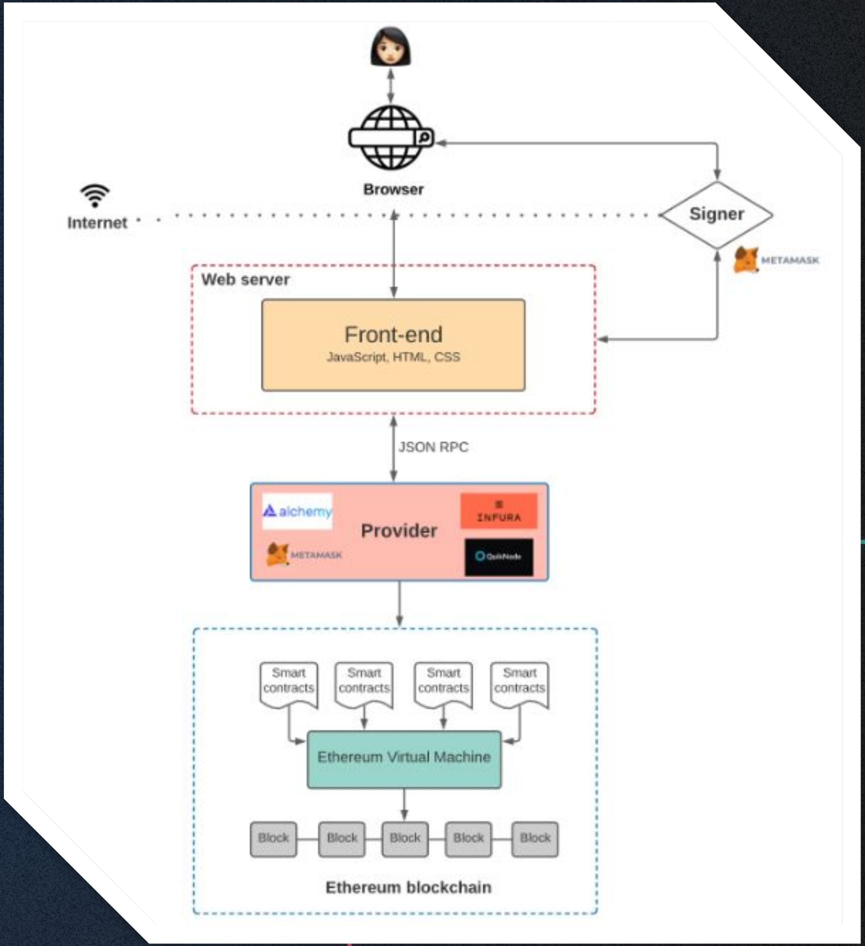
Every Ethereum client (i.e. provider) implements a JSON-RPC specification. This ensures that there's a uniform set of methods when frontend applications want to interact with the blockchain.



TO WRITE TO THE STATE

- When a user wants to publish a new post onto the chain, our DApp would ask the user to “sign” the transaction using their private key – only then would the DApp relay the transaction to the blockchain. Otherwise, the nodes wouldn’t accept the transaction.

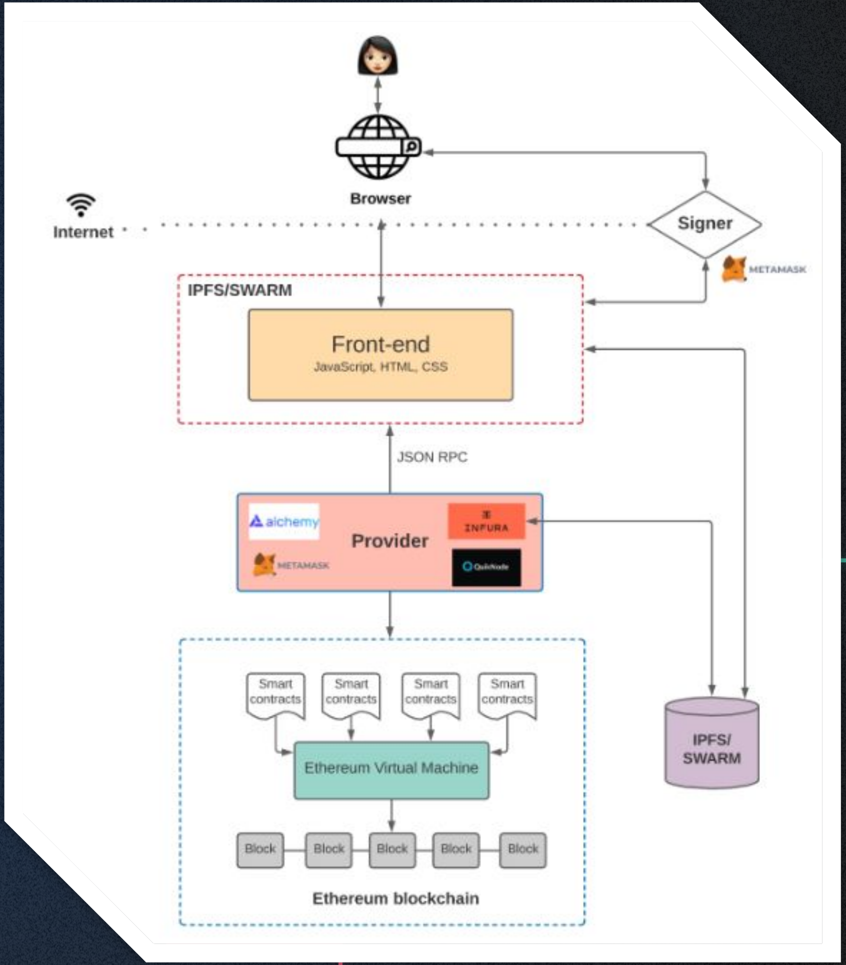
- This “signing” of transactions is where Metamask typically comes in.



STORAGE ON THE BLOCKCHAIN

- IPFS is a distributed file system for storing and accessing data. The IPFS system distributes and stores the data in a peer-to-peer network. This makes it easy for you to retrieve it when you need to.

- Swarm's incentive system is built-in and enforced through smart contracts on the Ethereum blockchain for storing and retrieving data.

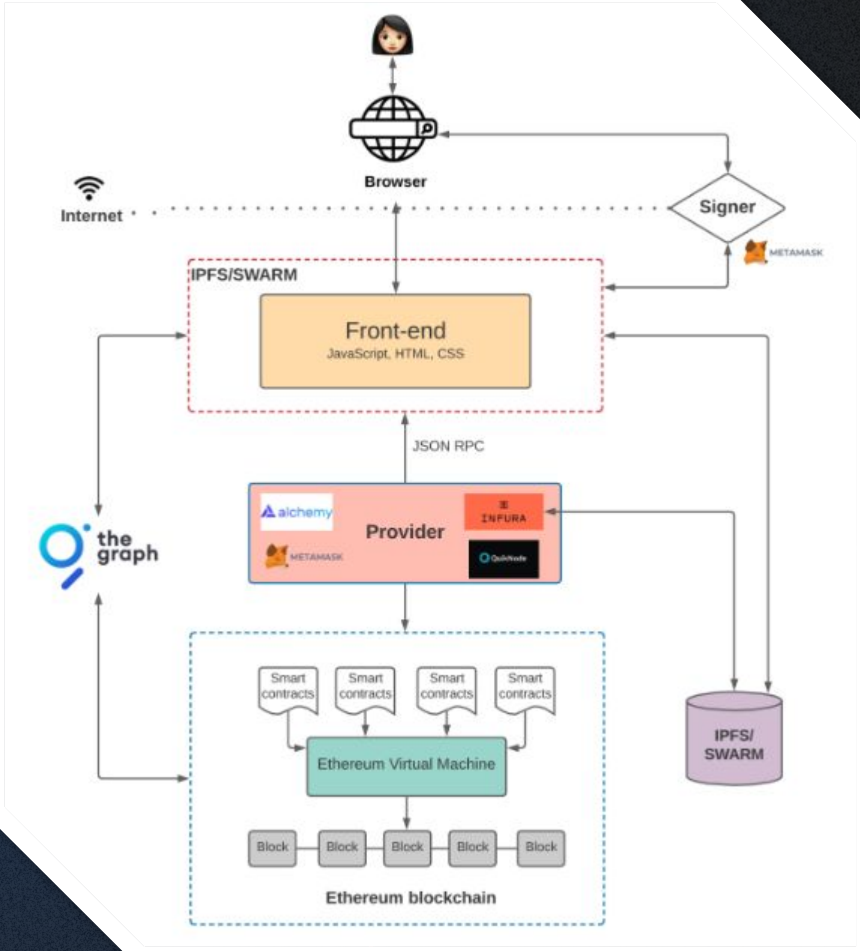


QUERYING THE BLOCKCHAIN

There are two primary ways to do this:

- Smart Contract Events**:** You can use the Web3.js library to query and listen for smart contract events. You can listen to specific events and specify a callback every time the event is fired.

- The Graph**:** The Graph is an off-chain indexing solution that makes it easier to query data on the Ethereum blockchain. It uses GraphQL as a query language, which many frontend engineers love because of how expressive it is compared to traditional REST APIs.


Browser
Internet
Signer
METAMASK
IPFS/SWARM
Front-end
JavaScript, HTML, CSS
JSON RPC
the graph
alchemy
Provider
INFURA
METAMASK
QuickNode
Smart contracts
Smart contracts
Smart contracts
Smart contracts
Ethereum Virtual Machine
Block
Block
Block
Block
Block
Ethereum blockchain
IPFS/ SWARM