



Arhitectura Aplicațiilor Blockchain

Conf.dr. Cristian Kevorchian
Facultatea de Matematică și Informatică

Evoluția tehnologiei BLOCKCHAIN

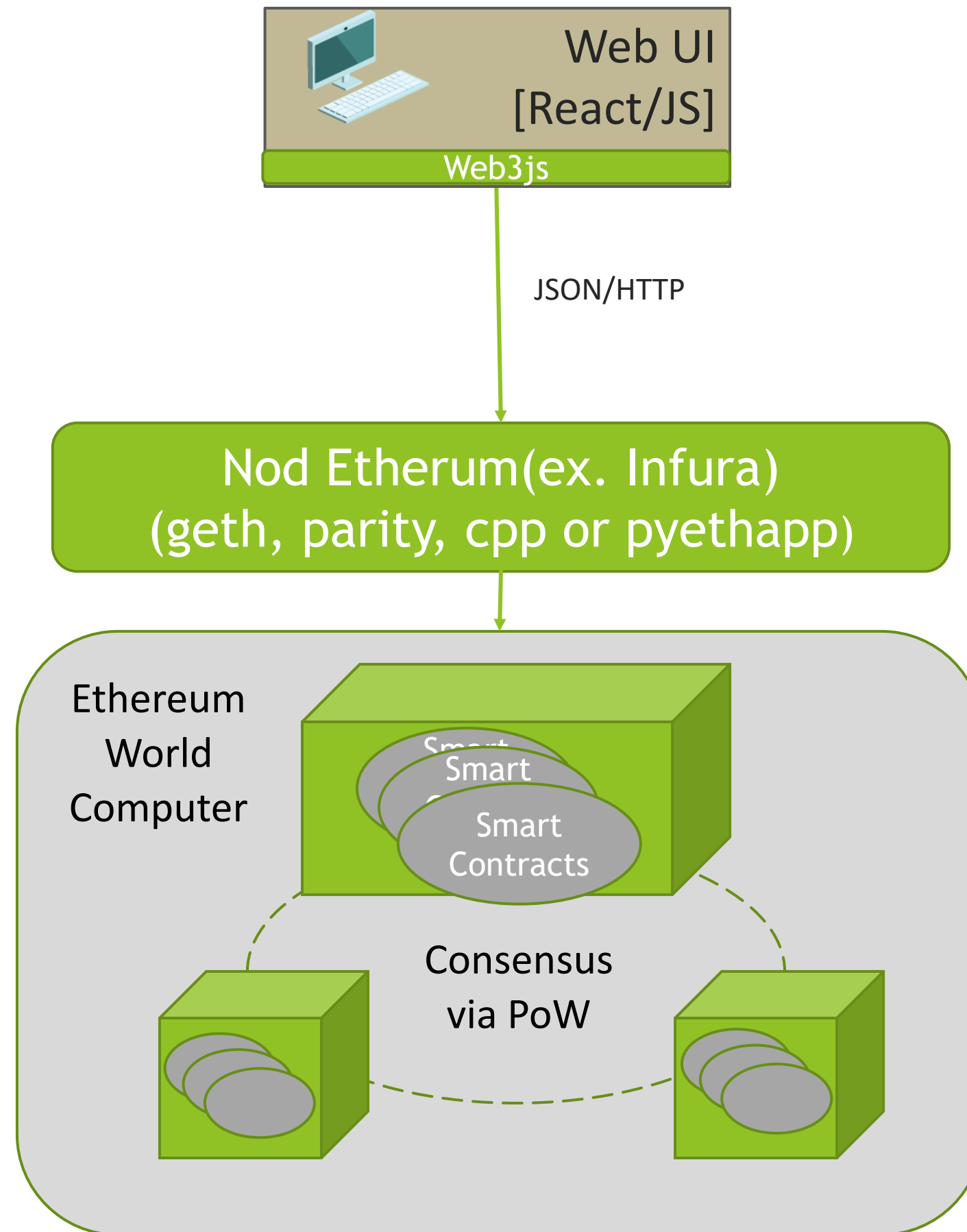
Prima Generație: Încărcarea și transferul asset-urilor digitale, cum ar fi Bitcoin.

A doua generație: Automatizarea procesului de transfer prin "smart contracts" (ex. Ethereum)

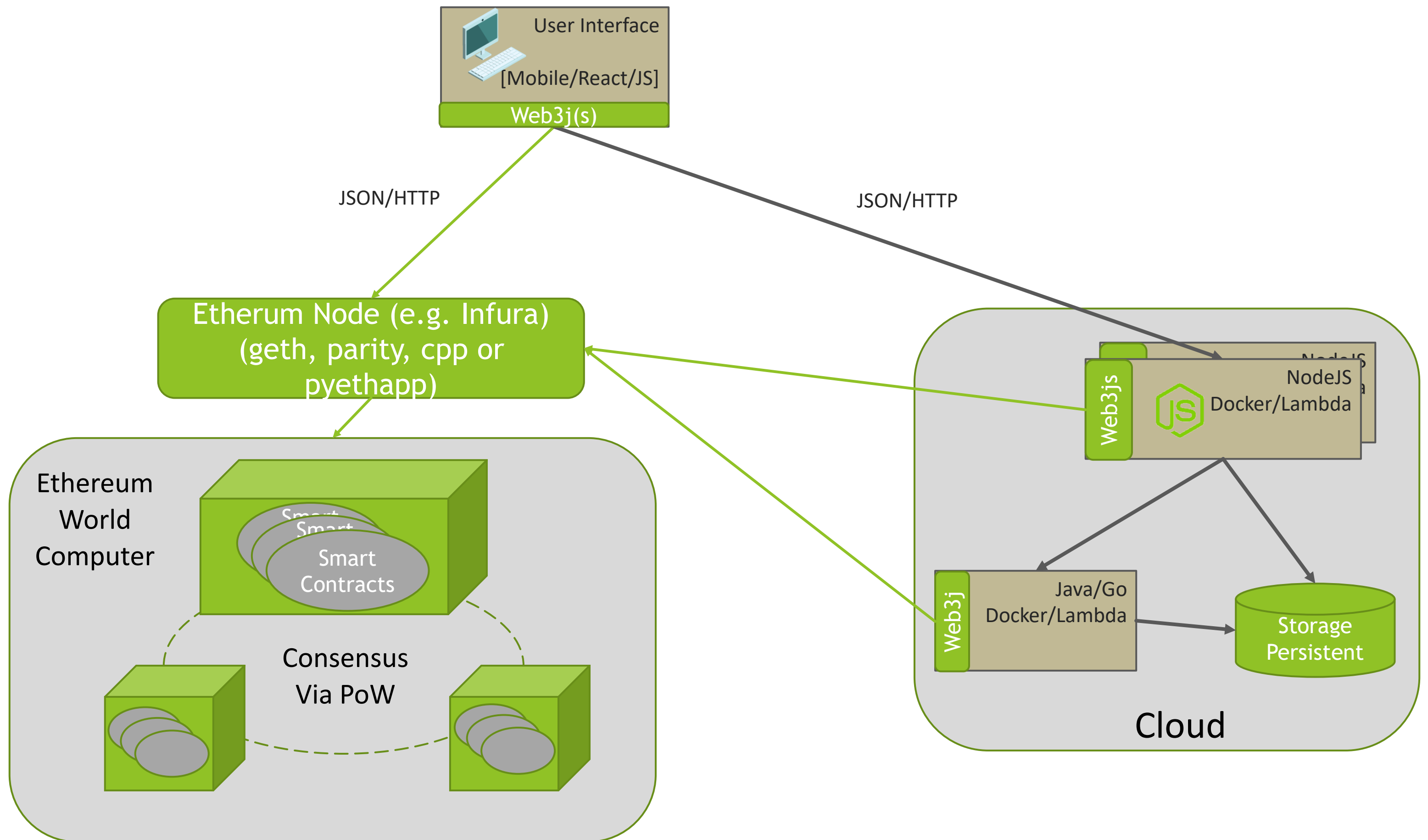
A treia generație: **Enterprise blockchain** (ex. Hyperledger, R3 Corda & Ethereum Quorum)

Generația următoare: Scalabilă, Decentralizată și Concurentă (Ex. RChain)

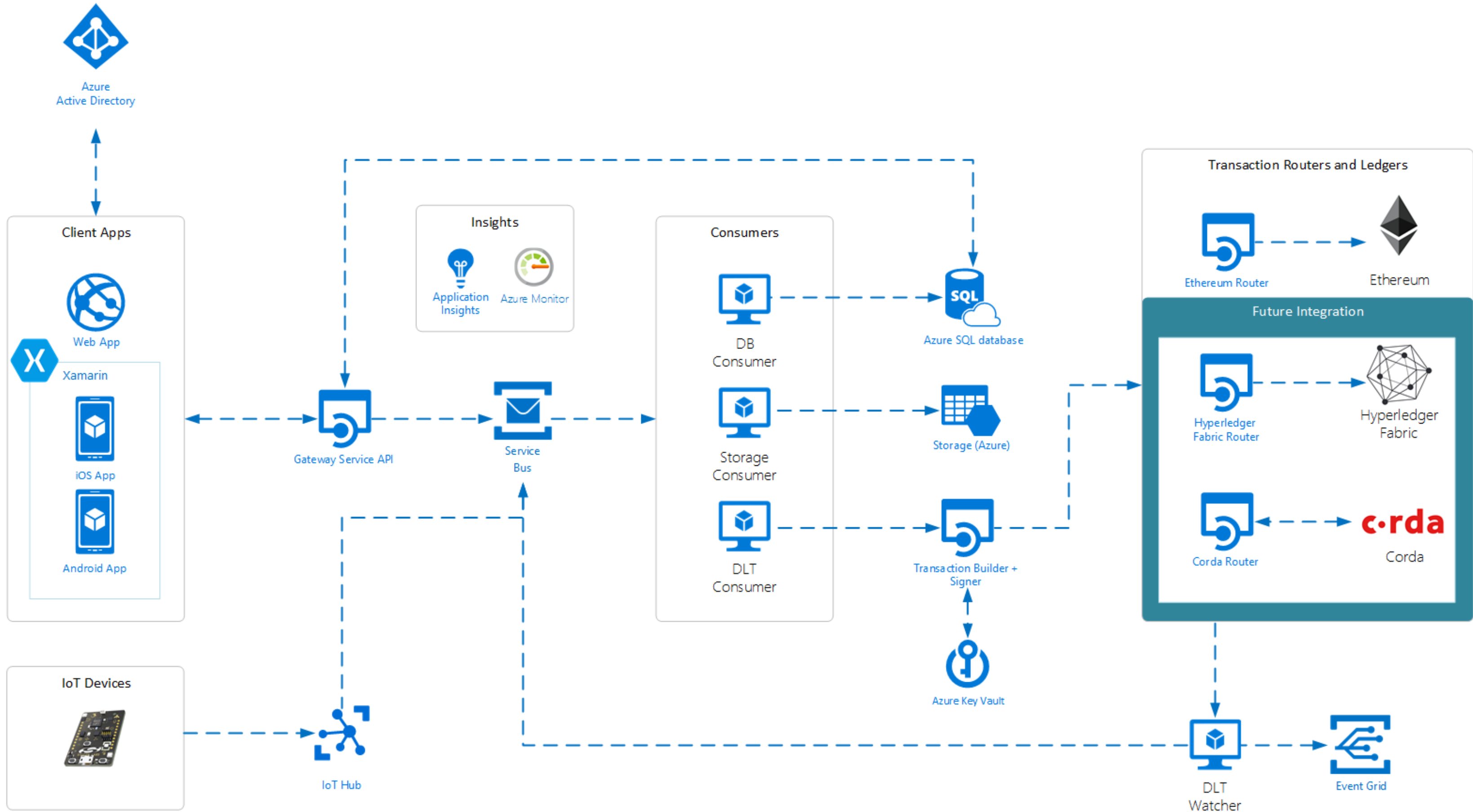
Architectura unei Dapp în ETHEREUM



Arhitecturi SaaS în Ethereum



Azure Blockchain Workbench

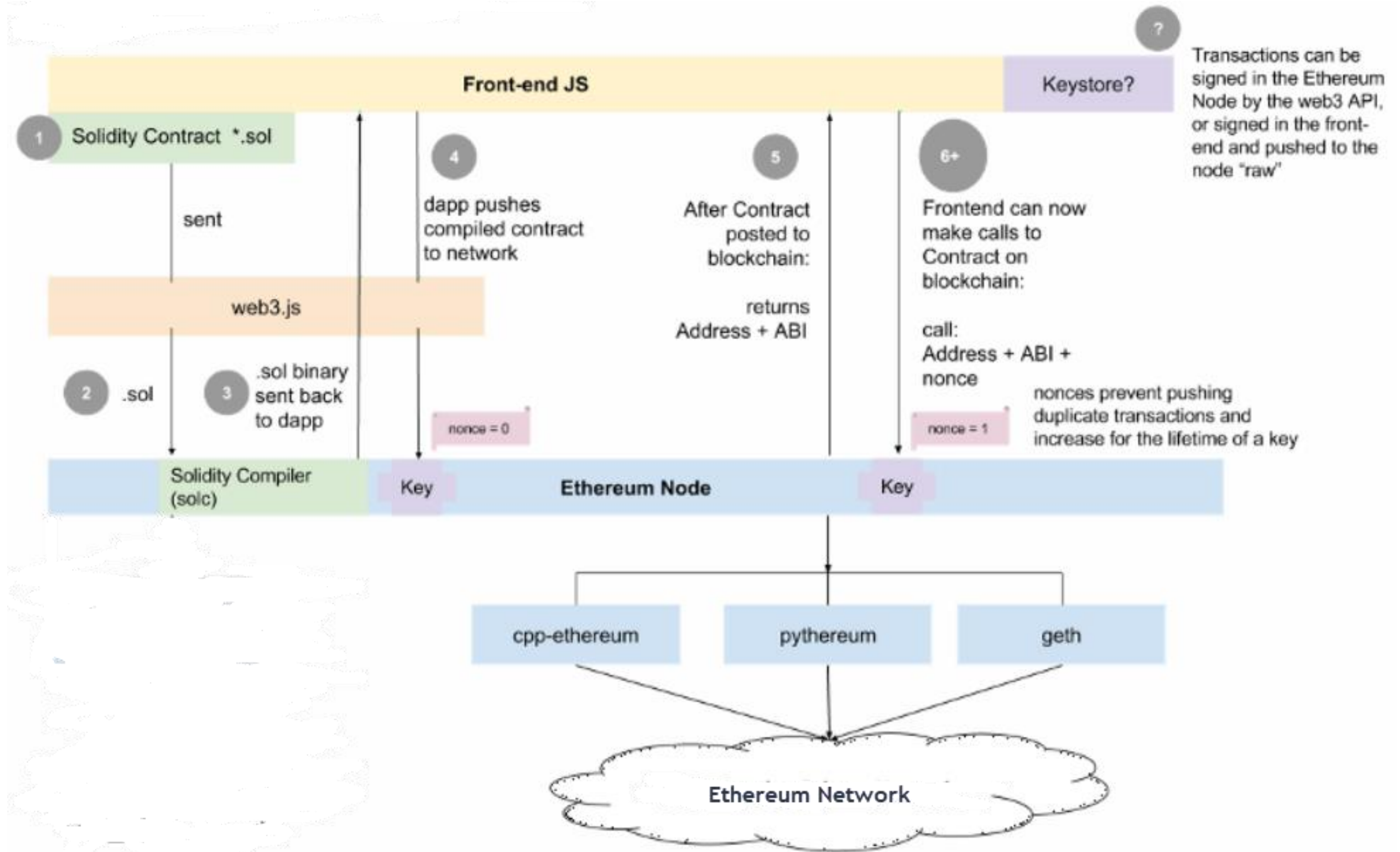


```
contract Coin {
    address minter;
    mapping (address => uint) balances;
    function Coin() {
        minter = msg.sender;
    }
    function mint(address owner, uint amount) {
        if (msg.sender != minter) return;
        balances[owner] += amount;
    }
    function send(address receiver, uint amount) {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
    function queryBalance(address addr) constant returns (uint balance) {
        return balances[addr];
    }
}
```

Contracte Inteligente(en. Smart Contracts)

- ▶ Se execută în Ethereum Virtual Machine (EVM)
- ▶ Limbaje
 - ▶ Solidity: cel mai cunoscut, complet Turing, similar cu JavaScript
 - ▶ Serpent(Buterin: "outdated tech")

Scenariu de implementare al unui "smart contract"



Probleme Deschise

- Securitate
 - Asigurarea faptului că diverse entități neautorizate să nu poată accesa sau modifica date.
 - Gestiunea cheilor private
 - Minimizarea vectorilor de atac
- Latența transacțiilor și costul- Realizarea consensului necesită timp, ceea ce ridică unele probleme pentru variantele enterprise
- Verificarea simbolică a contractelor

Medii de lucru cu ETHEREUM

- Solidity – Limbaj de programare pentru scrierea de "smart contracts" si executarea lor pe ETHEREUM.
- Remix – IDE Online(<https://remix.Ethereum.org>) pentru scrierea și debugging-ul contractelor smart în Solidity
- Truffle – Framework pentru compilarea, migrarea și testare "smart contract"
- React – Bibliotecă pentru "front end"
- IPFS – Storage descentralizat (SWARM -
- DappHub – Dezvoltarea, testarea și instalarea de contracte Ethereum.
- Web3.js & Web3j – O bibliotecă Java pentru integrarea cu un nod Ethereum
- uPort – Managementul identității, si semnarea digital a transacțiilor în ETHEREUM

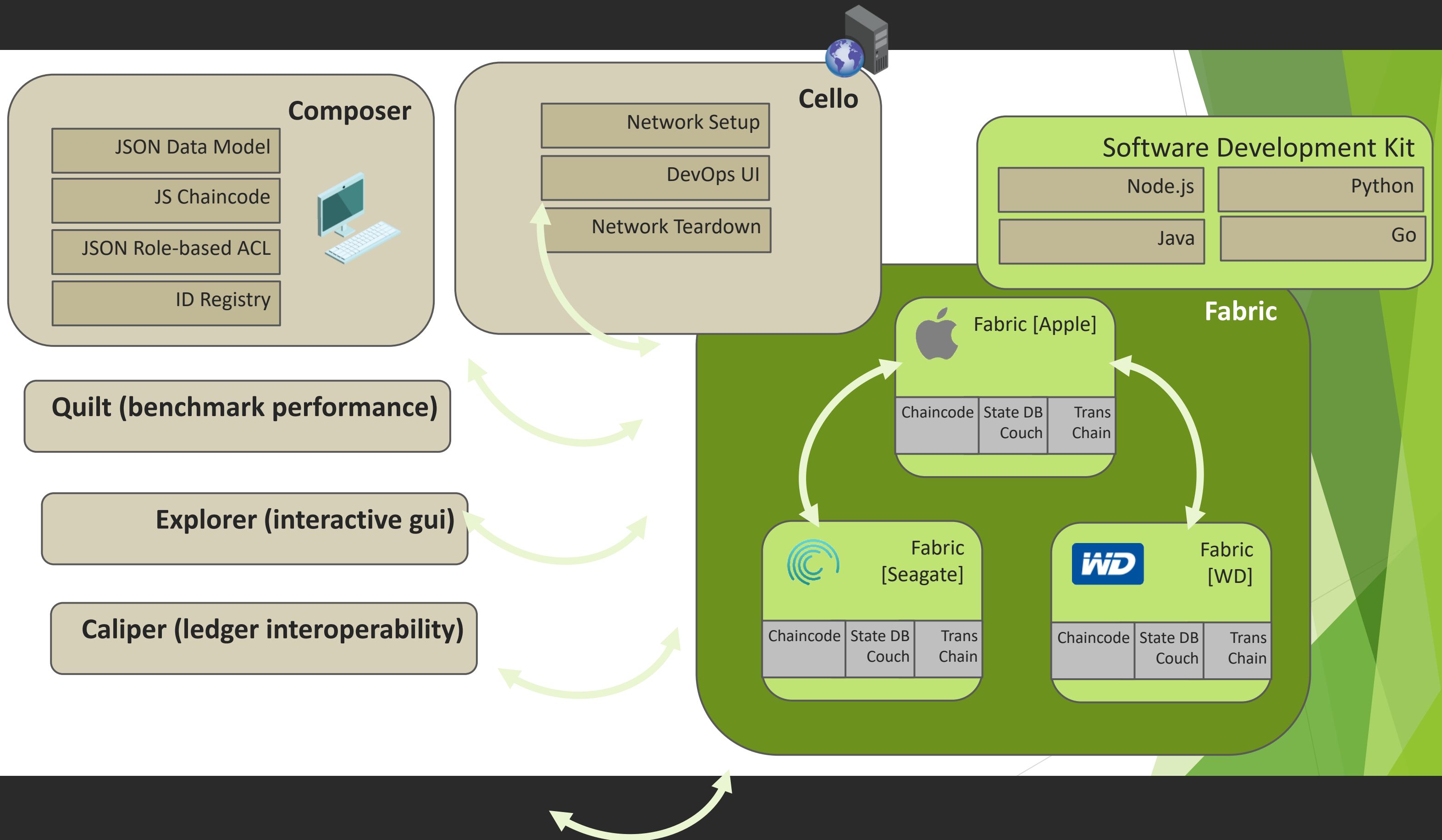
- ▶ Scalabilitate la nivel enterprise
- ▶ Tranzacții private - Contracte conf
- ▶ Menținerea securității
- ▶ Arhitectură modulară- Componente "Plug and Play"
- ▶ Componente
 - ▶ Servicii de "Membership"
 - ▶ Servicii de Coordonare
 - ▶ Baza de date a stărilor

Obiective pentru Hyperledger

Proiectarea Hyperledger

- Asset-urile
- Membrii
- Tranzacțiile
- Evenimentele

Hyperledger – Siva de instrumente pentru dezvoltare și implementare



BaaS(Blockchain as a Service)

- ▶ Blockchain as a Service (BaaS) permite utilizatorilor să folosească soluții bazate pe cloud pentru a dezvolta, găzdui și utiliza aplicații descentralizate în blockchain, cum ar fi contractele inteligente și funcții pe blocurile din blockchain, în condițiile în care furnizorul de servicii cloud gestionează toate sarcinile necesare menținerii operaționale a infrastructurii
- ▶ Este o dezvoltare de tip SaaS în ecosistemul blockchain, care contribuie indirect la adoptarea blockchain la nivel enterprise.

Avantaje în utilizarea BaaS

- ▶ Dezvoltare și validarea scenariilor de blockchain prin utilizarea conexiunilor asociate serviciilor cloud din Azure
- ▶ Securizează stocarea datelor pe o platformă cloud deschisă și disponibilă la nivel global
- ▶ Scalabilitate conform specificațiilor asociate aplicațiilor și a cerințelor de performanță aferente
- ▶ Funcționalitatea contractelor inteligente la nivel enterprise, utilizând Contractele Smart Enterprise
- ▶ Utilizează machine learning și tehnologii big data, reutilizarea codului și API-urile pentru integrarea cu funcționalități non-blockchain
- ▶ Acces la o gamă largă de rețele de blockchain pentru aplicații de construcție (Corda, Ethereum, Hyperledger Fabric)

Competente(bestjobs.ro)

- Software/Solution Architect
 - Responsible for selecting technologies and defining responsibilities for each module: User Interface/Mobile App, Server & Database (including blockchain)
 - Must have a good understanding of the objectives of using a blockchain technology and blockchain limitations
- Blockchain Data Modeler
 - Responsible for blockchain data modeling and smart contract design
 - Similar to a relational or no-SQL database modeler, must have experience developing solutions on the target blockchain