Arhitectura Aplicațiilor Blockchain

Conf.dr. Cristian Kevorchian
Facultatea de Matematică și Informatică

Evoluția tehnologiei BLOCKCHAIN

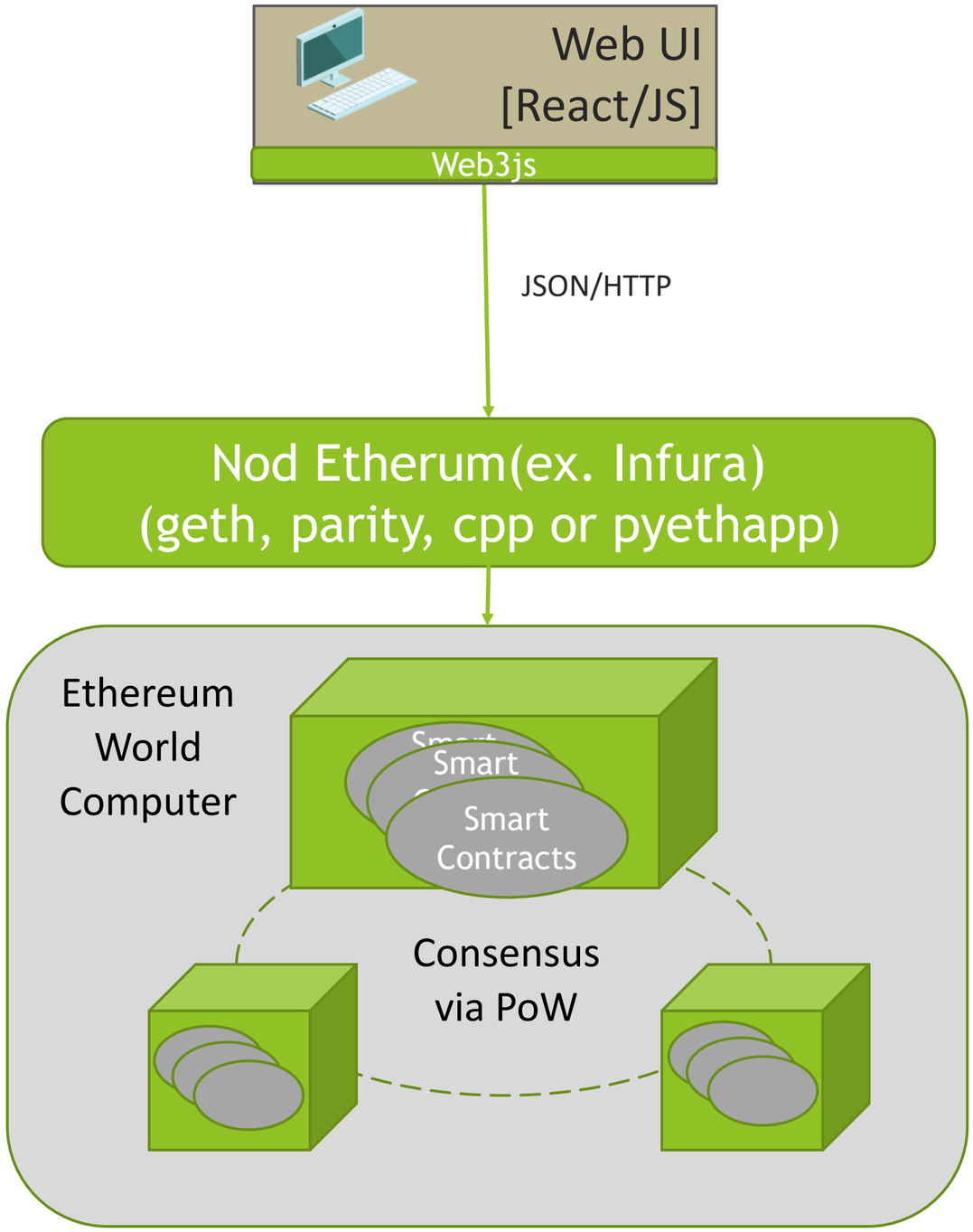
Prima Generație: Încărcarea și transferul asset-urilor digitale, cum ar fi Bitcoin.

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

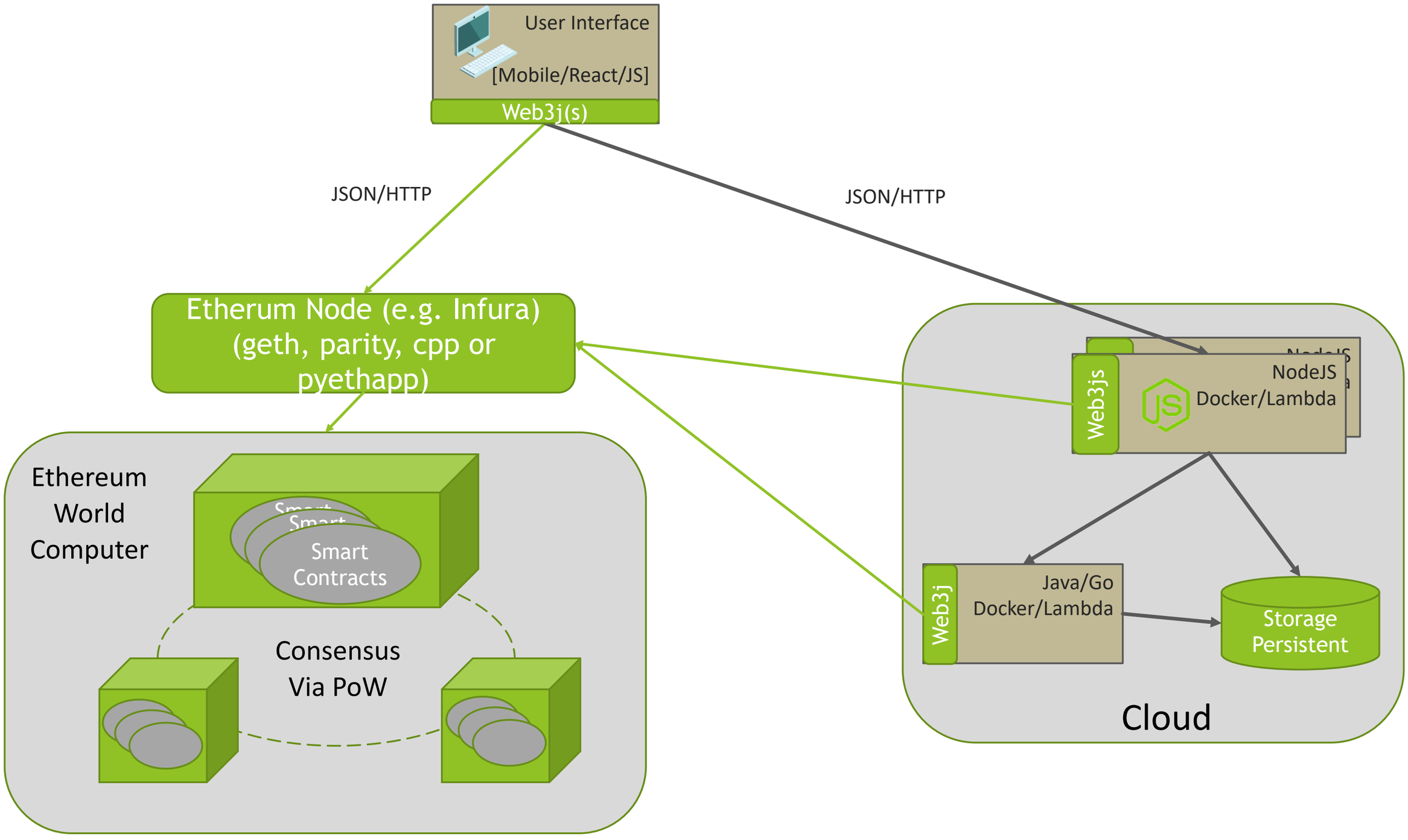
A treia generație: **Enterprise blockchain** (ex. Hyperledger, R3 Corda & Ethereum Quorum)

Generația următoare: Scalabilă, Decentralizata și Concurenta (Ex. RChain)

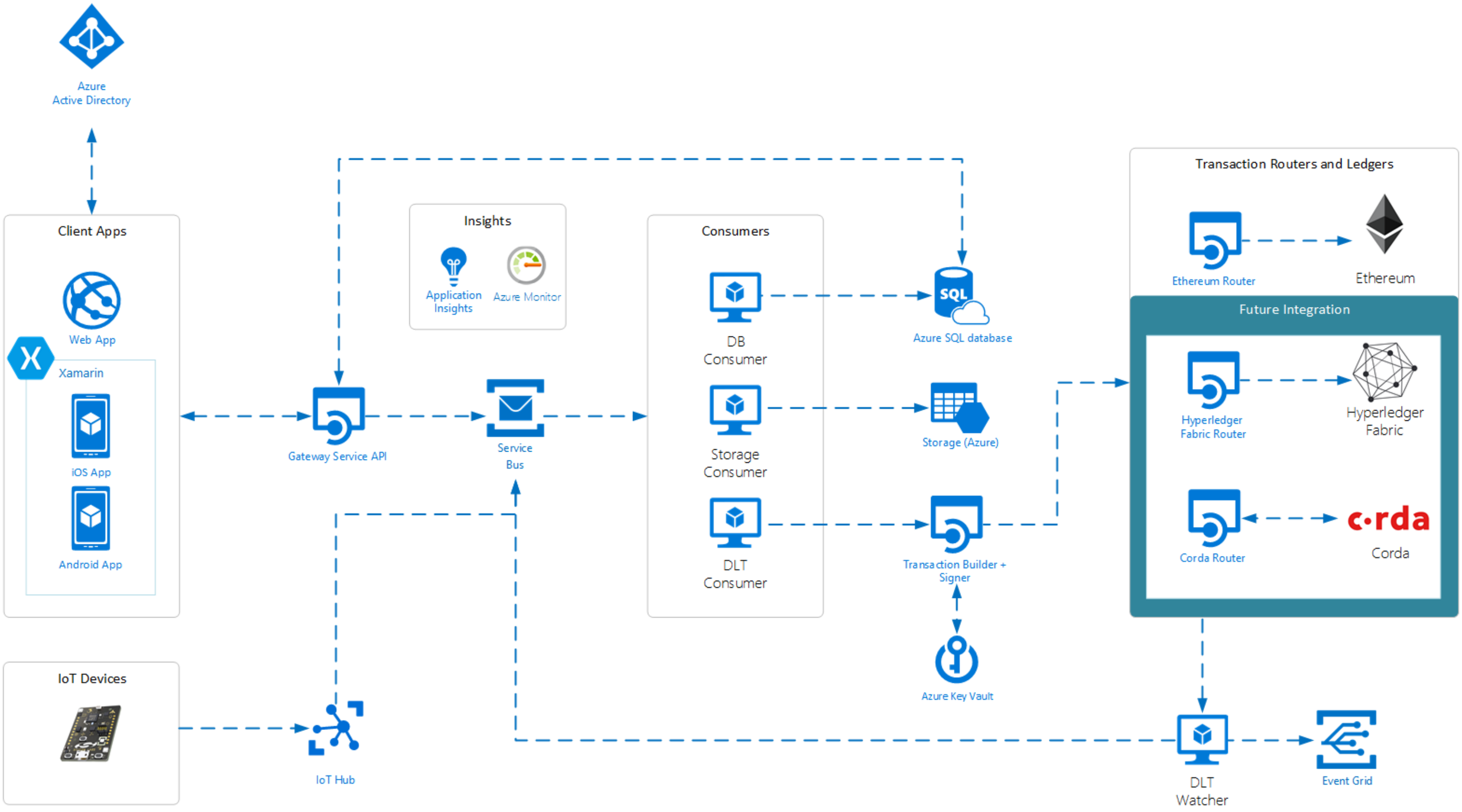
Architectura unei Dapp în ETHEREUM



Arhitecturi SaaS în Ethereum



Azure Blockchain Workbench

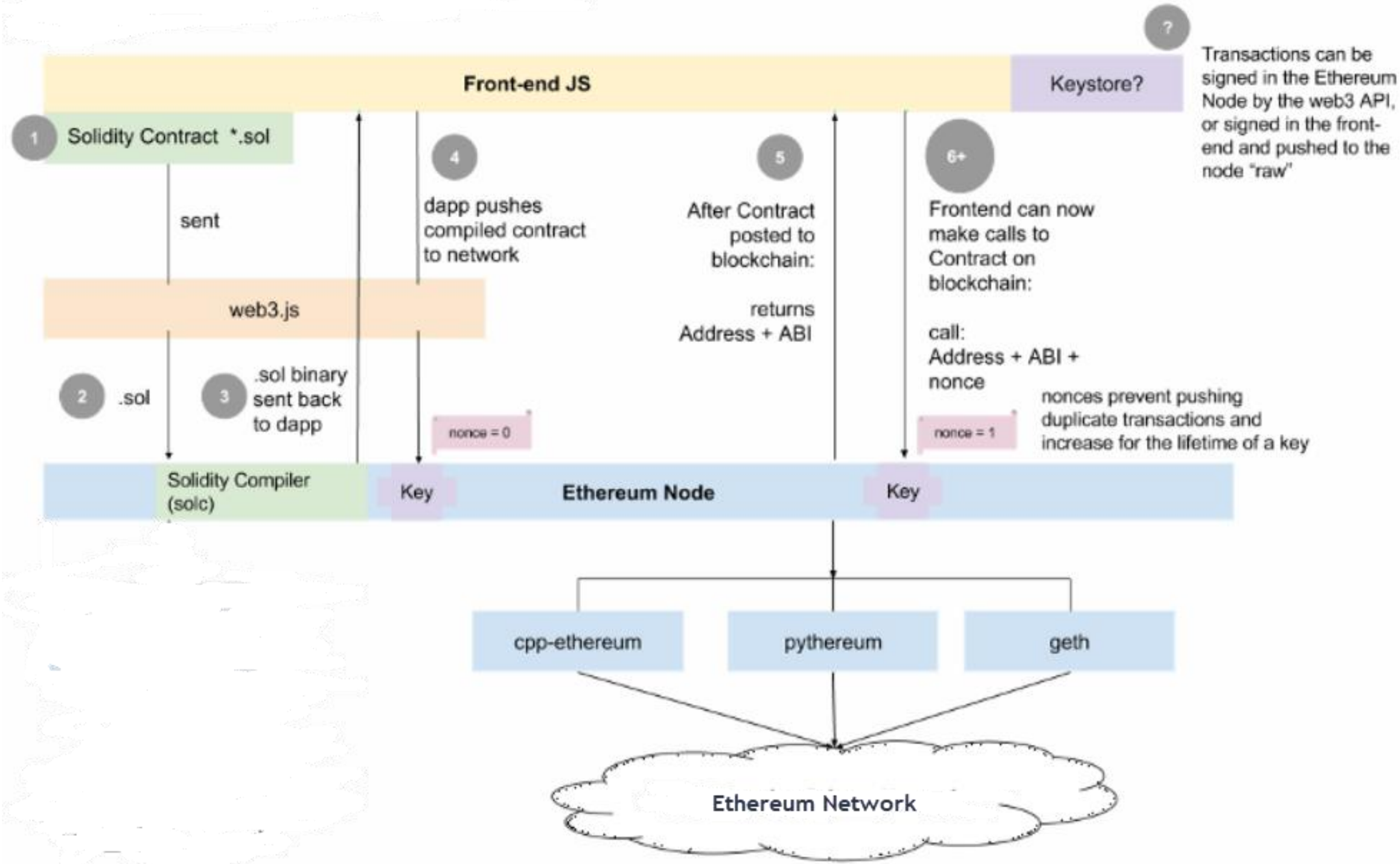


Contracte Inteligente(en. Smart Contracts)

```
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];
    }
}
```

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  - Serpent(Buterin: ”outdated tech”

Scenariu de implemntare 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

Obiective pentru Hyperledger

- 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

Proiectarea Hyperledger

- Asset-urile
- Membrii
- Tranzacțiile
- Evenimentele

Hyperledger – Siva de instrumente pentru dezvoltare și implementare

Composer

- JSON Data Model
- JS Chaincode
- JSON Role-based ACL
- ID Registry

Cello

- Network Setup
- DevOps UI
- Network Teardown

Quilt (benchmark performance)

Explorer (interactive gui)

Caliper (ledger interoperability)

Software Development Kit

- Node.js
- Python
- Java
- Go

Fabric

Fabric [Apple]

Chaincode	State DB Couch	Trans Chain

Fabric [Seagate]

Chaincode	State DB Couch	Trans Chain

Fabric [WD]

Chaincode	State DB Couch	Trans Chain

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 associate 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)

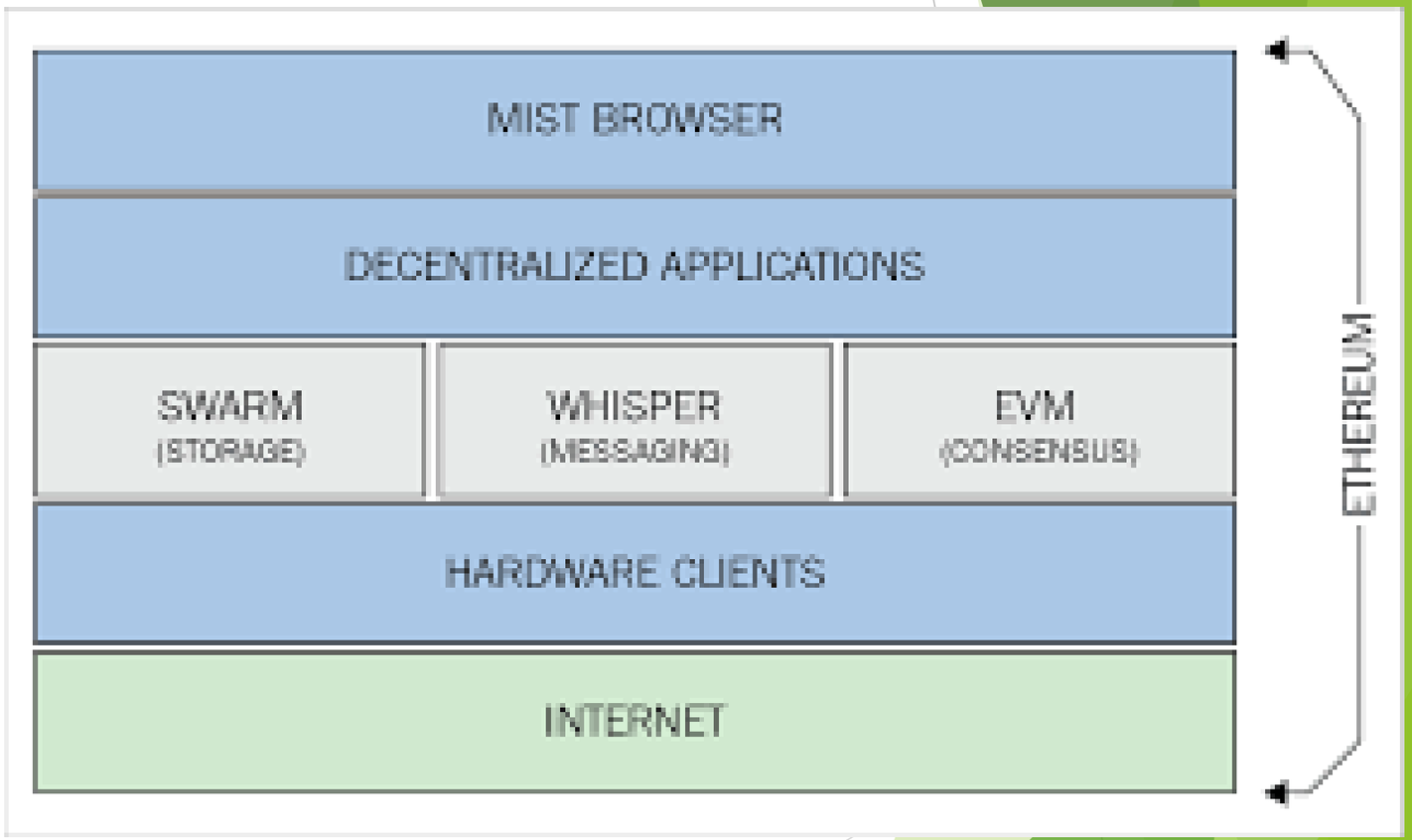
- Software/Solution Architect
  - Responsible for selecting technologies and defining responsibilities for each module: User Interface/Mobile App, Server & Database (including blockchain)
  - Must have a good understanding of the objectives of using a blockchain technology and blockchain limitations
- 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

STOCAREA DESCENTRALIZATA-Preliminarii

- Cele mai multe aplicații descentralizate care rulează pe platforma Ethereum necesită stocarea/ consultarea datelor similar aplicațiilor convenționale(centralizate) folosind PostgreSQL, MongoDB, Redis etc. EVM (Ethereum Virtual Machine) permite stocarea variabilelor și stărilor.
- La un curs de 328.79 USD/ETH in oct. 2017 1Gb de date în Ethereum însemna 5m USD
- Dacă salvarea câtorva octeți în EVM este acceptabilă din punct de vedere economic, în schimb pentru volume mari de date costurile sunt prohibitive.
- O soluție este modificarea strategiei de stocare a datelor în sensul salvării acestora în regim off-chain(spre deosebire de abordarea on-chain adoptată anterior).
- Există mai multe opțiuni de stocare în regim off-chain cum ar fi IPFS și Swarm.

Ecosistemul Ethereum

- Whisper este o componenta a protocolului Ethereum P2P, care permite transmiterea de mesaje între utilizatori prin intermediul aceleiași rețele pe care rulează blocul.
- Protocolul este separat de blockchain, astfel încât contractele inteligente nu pot fi afectate.



InterPlanetary File System(IPFS)

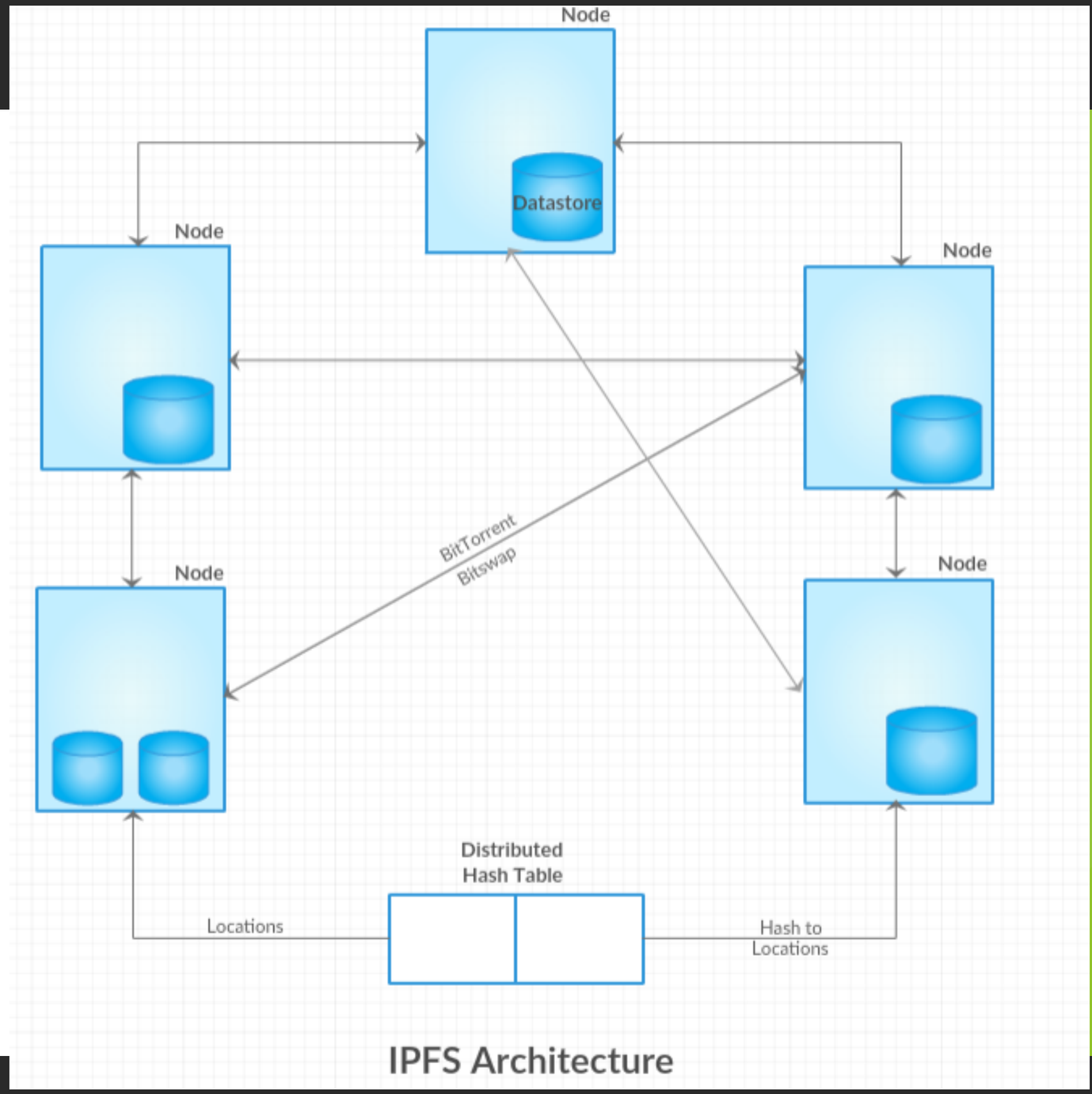
- IPFS este un sistem de fisiere distribuit peer-to-peer care poate conecta oricare două echipamente de calcul cu același system de fișiere.(Juan BENET)
- IPFS generalizează Merkle DAG(DIRECT ACYCLIC GRAPH), o structură de date care poate gestiona sisteme de fișiere versionate, blockchain-uri și chiar un ”Permanent Web”
- IPFS combină un DHT(Distributed Hash Table), un schimb intens de blocuri și un spațiu de nume auto-certificat.
- IPFS nu are niciun punct de eșec, iar existența nodurilor nu implică relații de încredere

Concepte cheie

Similar modului în care Bitcoin lucrează, IPFS combină o serie de bune practici care au contribuit la succesul ideii de system P2P, dar în același timp încearcă să limiteze problemele care au făcut ca multe dintre ele să eșueze(Tapestry).

1. Identificarea bazată pe conținut cu conținutul securizat; Rezolvarea locațiilor utilizând Distributed Hash Table (DHT)
2. Traficul de Block-uri bazat pe Bittorrent un peer-to-peer FDP(File Distribution Protocol)
3. Optimizarea traficului de block-uri utilizand protocolul Bitswap
4. Merkle DAG (Directed Acyclic Graph) versionat-bazat pe orgaizarea fisierelor, similar sistemului de control al versiunilor Git.
5. Secuitate asigurata cu Self-Certification servere pentru nodurile de stocare.

Arhitectura IPFS.
Fisierele sunt stocate distribuit, iar DHT(Distributed Hash Table), utilizeaza hash-ul fisierului drept o cheie asociata locatiei fisierului. Odata ce locatia a fost determiata, transferul se realizeaza peer-to-peer ca un transfer decentralizat.



IPFS Architecture

Noduri Distribuite

- The nodes are the computers that holds the decentralized data file objects that form the global file system.

- Nodurile sunt identificate prin hash-uri criptografice ale cheilor publice. (Similar cu nodurile noastre de blocuri).

- Ele dețin obiectele care formează fișierele care urmează să fie transferate. Obiectele sunt identificate printr-un hash iar fiecare obiect poate conține sub-obiecte, fiecare cu hash-ul propriu care este folosit la crearea hash-ului rădăcinia al obiectului. (arborele Merkle)

Continut adresabil

- In actualul protocol web global, o resursă web se identifica prin serverul pe care este stocata:

De exemplu, http://fmi.unibuc.ro/ se refera la serverul unde este gazduita pagina faculatii precu si la o anumita cale definita prin sistemul de isiere al acelui server. Aceasta este o abordare centralizata. Ce se intampla daca resursa este disponibila in mai multe locatii.

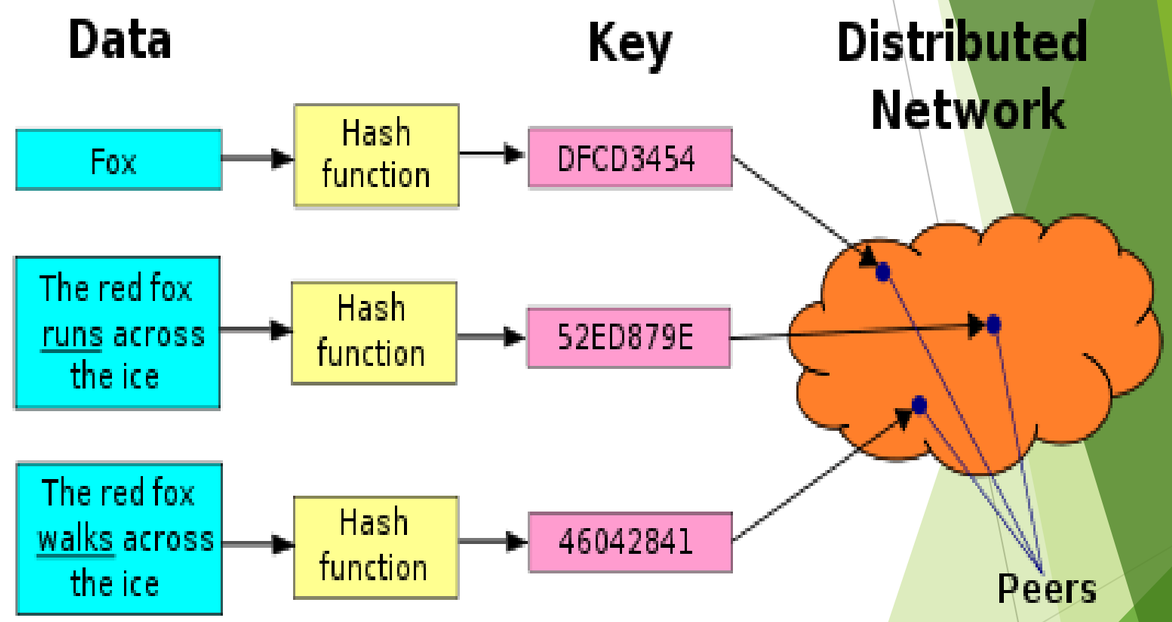
- **IPFS ofera o solutie decentralizata.**

- IPFS identifică resursele printr-un hash. În loc să identifice resursa după locație ca în HTTP, IPFS o identifică prin conținutul său sau prin hash-ul conținutului său. În acest caz, fișierul este adresat printr-un identificator universal unic, în loc de locație.

- Rezolvarea problemei locaiei. La fel unei adrese URL sau a unui link al unui site web, încep cu identificatorul hash al resursei. Este trimia o solicitare pentru oricine care are o resursă cu acest identificator; iar pe un răspuns pozitiv, accesul va fi peer-to-peer.

Continut adresabil si localizarea obiectelor

- Segmentul de routare a protocolului IPFS gestioneaza DHT (Distributed Hash Table) pentru locatia nodului la fel pentru obiectele fisierelor.
- O DHT cuprinde hash-ul drept cheie si loactia drept valoare



Localizarea si transferul blocurilor

- In cazul sistemelor tipice IPFS, DHT asociaza celei mai apropiate locatii valoarea cheii. The Noduril peer cuprind blocurile de date care sunt transferate cu ajutorul protocolului BitSwap, asemanator BitTorrent.

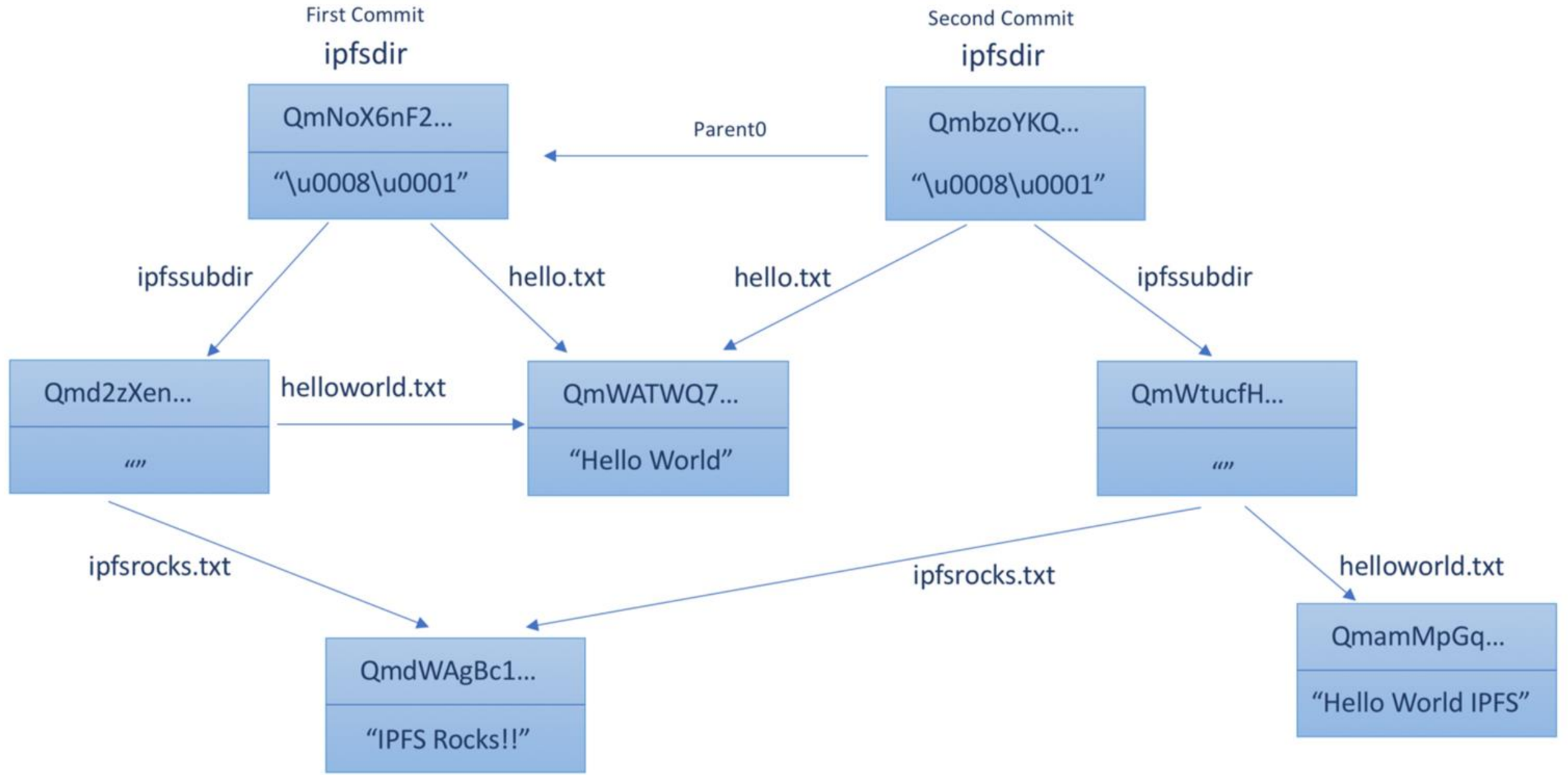
- Când se conectează P2P nodurile, schimbă blocurile pe care le au (**have_list**) și blocurile pe care le caută (**want_list**) sistemul fiind asemanator cu un **sistem barter**

- Orice dezechilibru este marcat sub forma unei balante credit/debit **BitSwap**; Protocolul **Bitswap** gestionează schimburile de blocuri care implică nodurile asociate. Astfel, nodurile din rețea trebuie să furnizeze valoare sub formă de blocuri. (Aceasta ar putea fi o aplicație ideală pentru un "token digital"; Dacă este trimis un bloc este primit un token IPFS care poate fi folosit atunci când aveți nevoie de un bloc.)

Multiple versiuni de fisiere

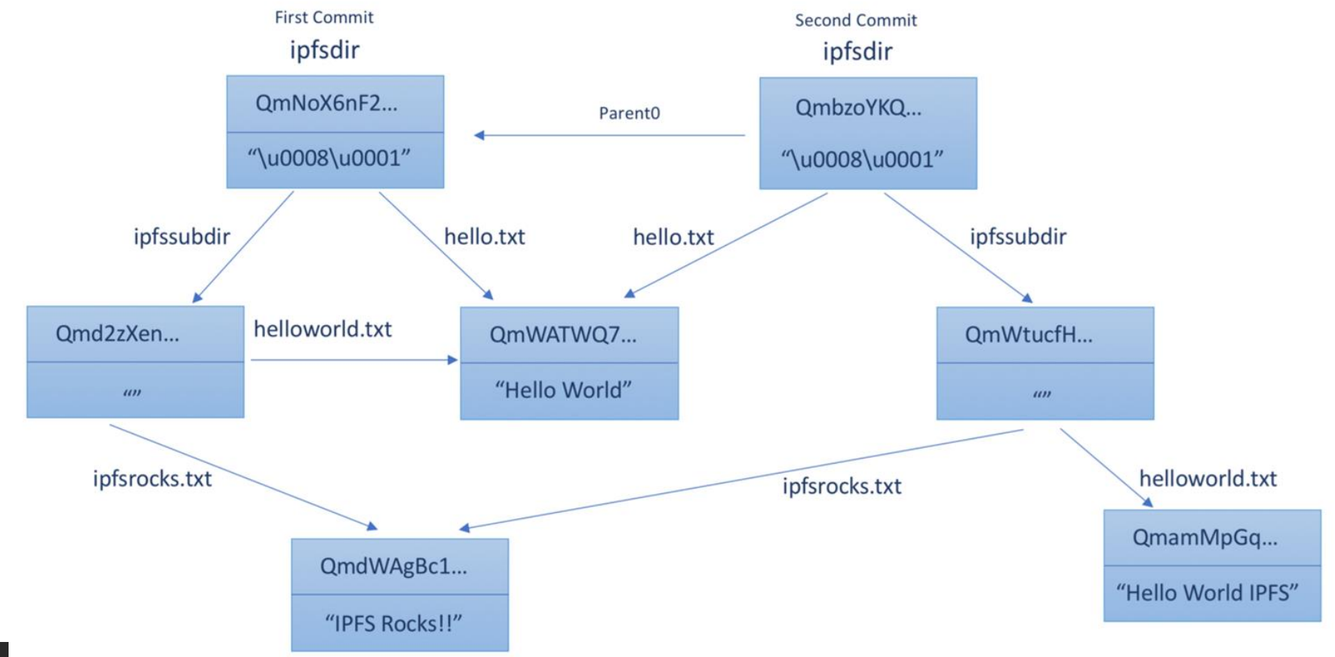
- Versiuni multiple ale unui fișier sunt menținute utilizând o structură de date de tip Merkle Directed Acyclic Graph la un nivel de abstractie superior sistemului de gestiune a fișierelor.
- Elementele de bază ale blocului(lista de blocuri, arborele blocului reprezentând o instanță și commit-ul care reprezintă snapshot-ul arborelui.

Acest Merkle DAG vă ajută de asemenea la verificarea oricărei operatiuni malitioase și, de asemenea, a deduplicării.


First Commit
ipfsdir
QmNoX6nF2...
"\u0008\u0001"
Second Commit
ipfsdir
QmbzoYKQ...
"\u0008\u0001"
Parent0
ipfssubdir
hello.txt
hello.txt
ipfssubdir
Qmd2zXen...
""
helloworld.txt
QmWATWQ7...
"Hello World"
QmWtucfH...
""
ipfsrocks.txt
ipfsrocks.txt
helloworld.txt
QmdWAgBc1...
"IPFS Rocks!!"
QmamMpGq...
"Hello World IPFS"

IPFS-partajarea fisierelor

Putem observa în această imagine două commit-uri ale cursului3Dir, cele patru noduri din stânga formează primul commit și cele trei noduri din dreapta al doilea commit.
Este un DAG în locul unui arbore Merkle pe care l-am văzut în rădăcina de stare Ethereum. Puteți observa deduplicarea, adică aceleași fișiere sunt partajate. Există două fișiere partajate

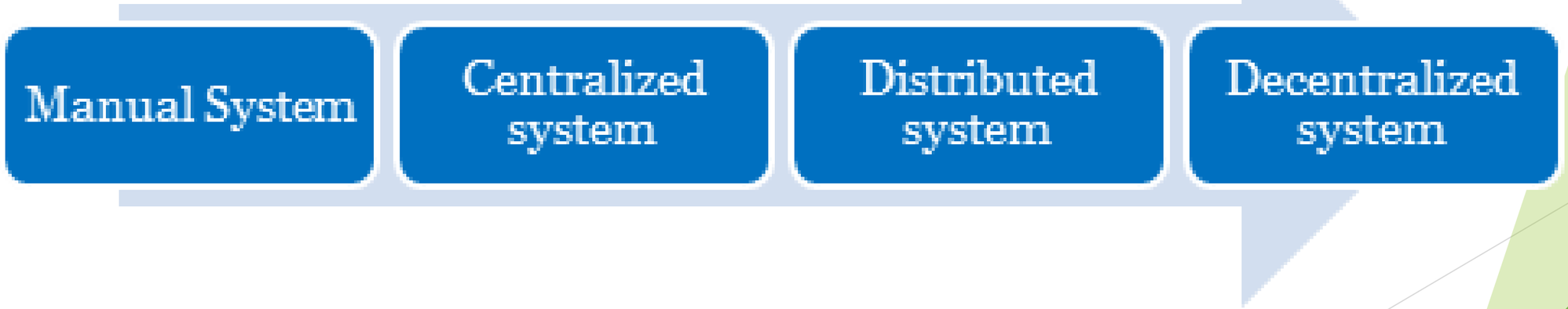


Relatia cu Blockchain

- IPFS poate fi un sistem decentralizat, independent de fișiere.
- Acesta poate fi complementar sistemului centralizat bazat pe HTTP.
- Am discutat despre aceasta în contextul sistemelor blockchain, deoarece poate avea un rol important in stocare descentralizată pentru aplicații blockchain associate cu volume mari de date pentru care va stoca numai hash-ul pe blockchain.
- In this case instead of a centralized store, IPFS can be the decentralized store that work in tandem with the decentralized ledger technology of the blockchain to create a powerful solution for many storage-rich business usecases.
- In locul unei stocari centralizate, IPFS poate stoca descentralizat în tandem cu tehnologia descentralizată blockchain pentru a crea o soluție economic acceptabila.

Concluzii,

Am discutat unele aspect legate de sisteme decentralizate de stocare care pot fi utilizate pentru stocarea off-chain a datelor pentru o aplicație blockchain. Acesta este folosit în multe aplicații de date genomice pentru stocarea datelor genomice mari și în dapps, cum ar fi Openlaw pentru stocarea documentelor.



Referinte

- Juan Bennet’s IPFS whitepaper: https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf
- https://hackernoon.com/understanding-the-ipfs-white-paper-part-2-df40511addbd
- https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0