Stocarea Descentralizată a Datelor în Blockchain

Conf. dr. Cristian KEVORCHIAN

Universitatea in București

ck@fmi.unibuc.ro

cristian.kevorchian@unibuc.ro

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 în 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.

Swarm

- Swarm este o platformă de stocare distribuită peste care operează:
  - un serviciu de distribuție a conținutului,
  - un nivel destinat stivei ethereum web3 care își propune să ofere un storage descentralizat și redundant pentru cod dapp, date utilizator, blockchain și date de stare.
- Swarm își propune să ofere diverse servicii de pentru web3, efectuarea de transacții(Sworm robotics), comunicarea pe baza de mesaje nod-la-nod, streaming media, servicii de baze de date descentralizate și infrastructură scalabila de servicii descentralizate.

Aplicații Descentralizate(DApps)

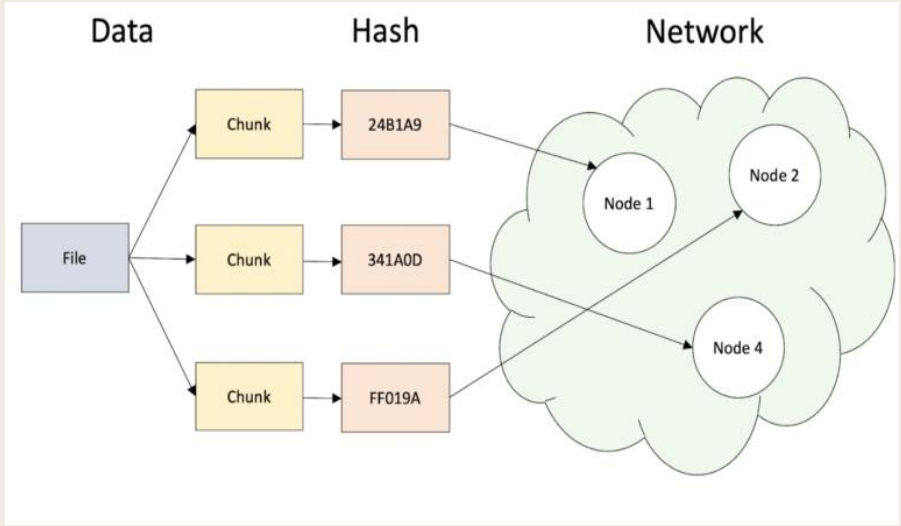
- Ethereum, permite implementarea aplicațiilor descentralizate (DApps).
- Ideea centrala a DApp-urilor constă în implementarea unei aplicații sub formă de smart contract pe un blockchain imutabil, eliminând astfel serverele de aplicații și single-point-of-failure.
- Ethereum Swarm este conceput pentru a îmbunătăți deployment-ul DApp-urilor și, prin extensie, a paradigmei Web 3.0, servind ca o soluție descentralizată de stocare a datelor.
- Dificil să de realizat Web 3.0 funcțional într-un mod pur descentralizat. Există două motive:
    1. interacțiunea cu smart contracts este complicată, motiv pentru care, majoritatea DApp-urilor oferă o interfață web, constând dintr-un front-end off-chain care este găzduit pe un server web tradițional și servit prin protocolul HTTP. (introduce o componentă centralizată)
    2. În al doilea rând, este foarte scump să stochezi cantități mari de date pe un blockchain, motiv pentru care DApp-urile necesită de obicei o modalitate de stocare a unor date în afara chain-ului. In plus, utilizarea unui sistem de gestionare a bazelor de date sau a unui sistem de fișiere tradițional este contrar modelului descentralizat.

Stocare Decentralizată

- O alternativă la soluțiile bazate pe componente centralizate poate fi varianta descentralizată, o rețea peer-to-peer (P2P) de noduri care partajează de o manieră colaborativă resursele.
- Rețeaua P2P acționează ca o soluție de stocare cloud distribuită cu redundanță build-in. În teorie, orice tip de date poate fi găzduit și servit dintr-o astfel de rețea descentralizată, inclusiv datele off-chain ale DApp și fișierele care constituie front-end-ul pentru acestea.
- Cea mai cunoscută soluție de stocare distribuită este IPFS, care utilizează o structură de date distribuită(Hashtable) pentru a stoca conținut într-o rețea de noduri. Cu toate acestea, conținutul IPFS nu este garantat a fi disponibil, cu excepția cazului în care proprietarul de date original continuă să îl difuzeze de la propria gazdă.
- Acest lucru se datorează faptului că propagarea conținutului prin rețea este prioritizată în funcție de popularitate, iar conținutul nepopular poate orientat catre GC.
- Noduril nu sunt “stimulate” pentru găzduirea conținutului fapt ce generează o problemă în arhitecturarea soluțiilor de stocare descentralizate.

Arhitectura Swarm

- Swarm este implementarea Ethereum a unei rețele descentralizate de stocare a fișierelor.
- Se bazează pe Ethereum Geth și interacțiunea cu rețeaua de stocare este strâns legată de blockchain-ul Ethereum și necesită un cont Ethereum.
- Datele sunt împărțite în blocuri numite chunk-uri, care au dimensiunea maximă de 4 KB. Nivelul rețea este agnostic la ceea ce reprezintă aceste chunk-uri, de exemplu, indiferent dacă fac parte dintr-un fișier sau orice altă bucată de date.
- Bucățile sunt distribuite peste rețea și sunt adresate printr-un hash de 32 de octeți generat de conținutul lor.
- Ethereum Name Service (ENS), permite utilizatorilor să înregistreze nume care pot fi citite în clar pentru conținutul lor. ENS este implementat ca un smart contract în rețeaua Ethereum și poate fi considerat echivalentul serviciului de nume (DNS).



Swarm vs IPFS

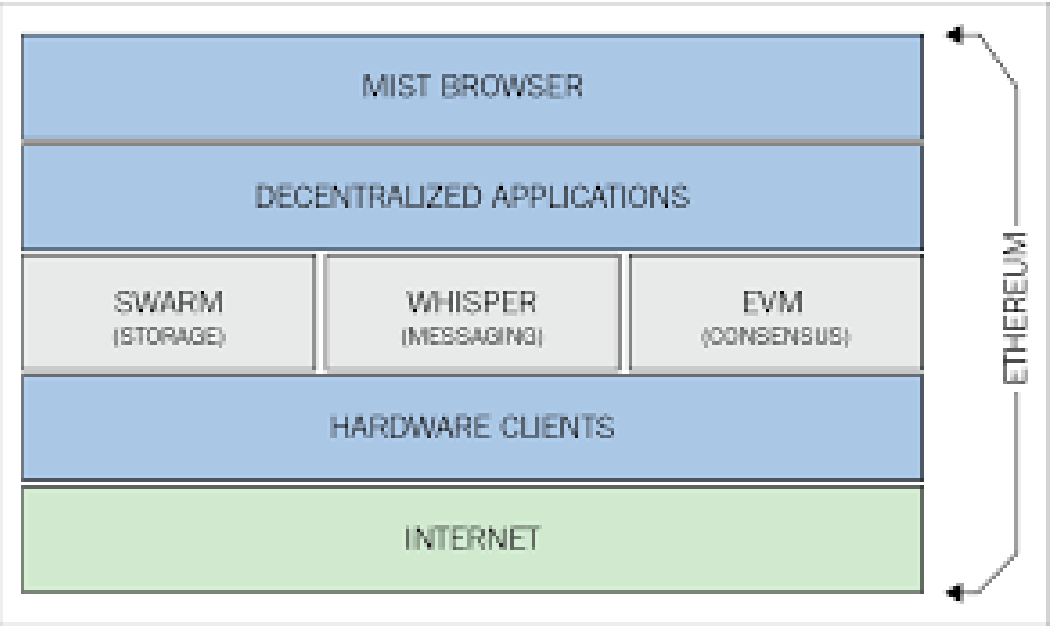
- Ethereum Swarm se diferențiază de IPFS nu doar ca mod de referentiere și a conținutului pus la dispoziție pe propriul spațiu de stocare al utilizatorului.
- Acesta constituie de fapt un serviciu cloud pe care se poate încărca conținut.
- Nu există nicio garanție că conținutul încărcat va rămâne disponibil, deoarece nodurile pot părăsi rețeaua când doresc sau chiar își pot reduce capacitatea de stocare.
- Pentru viitor este planificată dezvoltarea unui layer de stimulare, pentru a compensa proprietarii de noduri pentru oferirea de spațiu de stocare.
- Acest lucru este posibil numai printr-o integrare mai strânsă cu Ethereum.

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, 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

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.

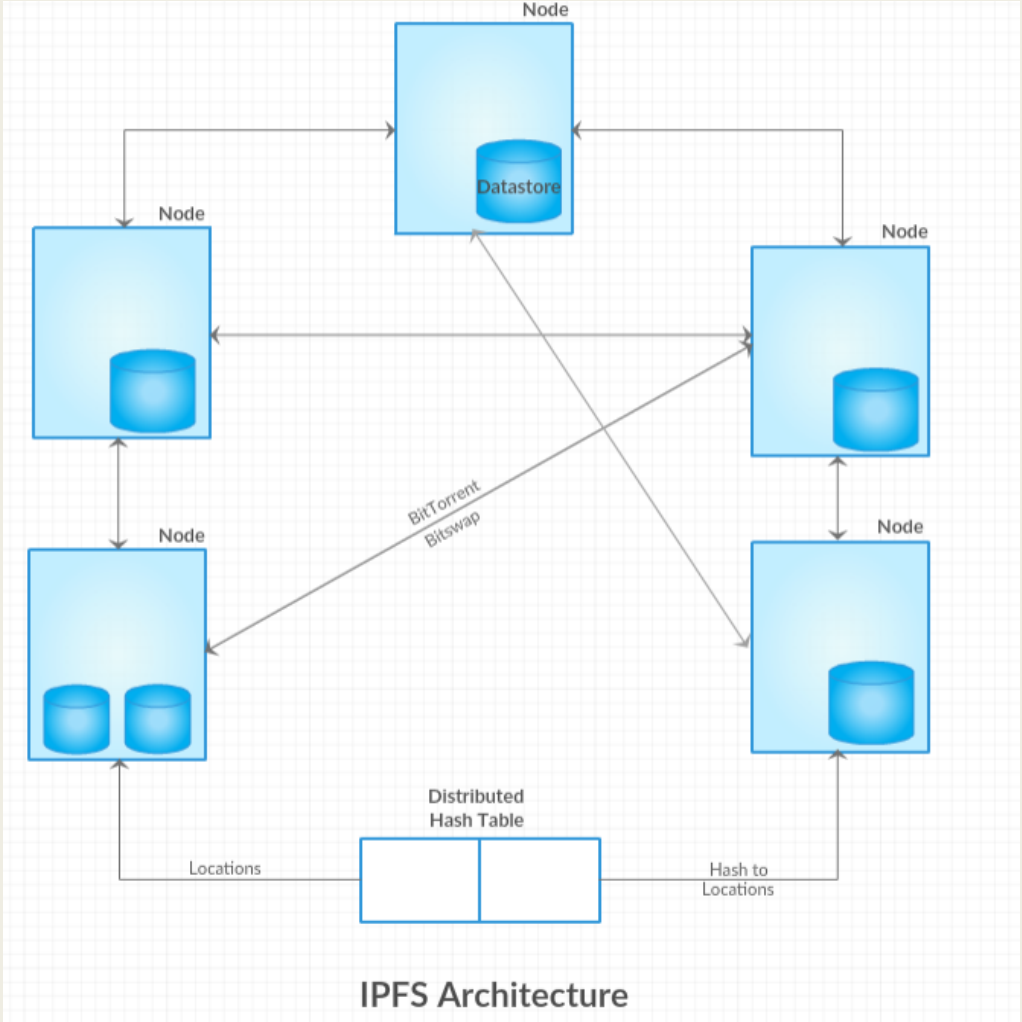


Concepte cheie

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 asociată locatiei fisierului.
Odata ce locatia a fost determiata, transferul se realizeaza peer-to-peer ca un transfer decentralizat.



Noduri Distribuite

- Nodurile sunt computerele care dețin obiectele descentralizate în speță fișierele de date care formează sistemul global de fișiere.

- 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 server-ul pe care este stocatat:

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

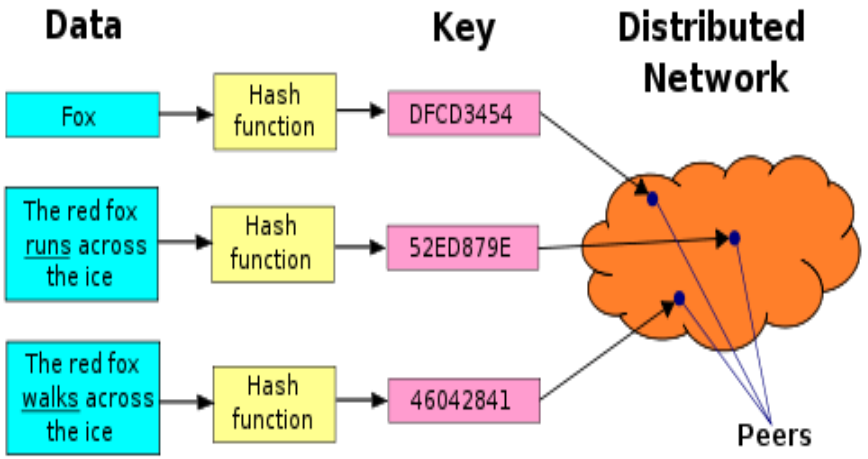
- **IPFS ofera o solutie decentralizata.**

- 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.

Conținut adresabil si localizarea obiectelor

- Segmentul de routare al protocolului IPFS gestioneaza DHT (Distributed Hash Table) pentru localizarea nodului la fel pentru fișiere.
- 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. Nodurile peer cuprind blocurile de date care sunt transferate cu ajutorul protocolului BitSwap, asemanator BitTorrent.

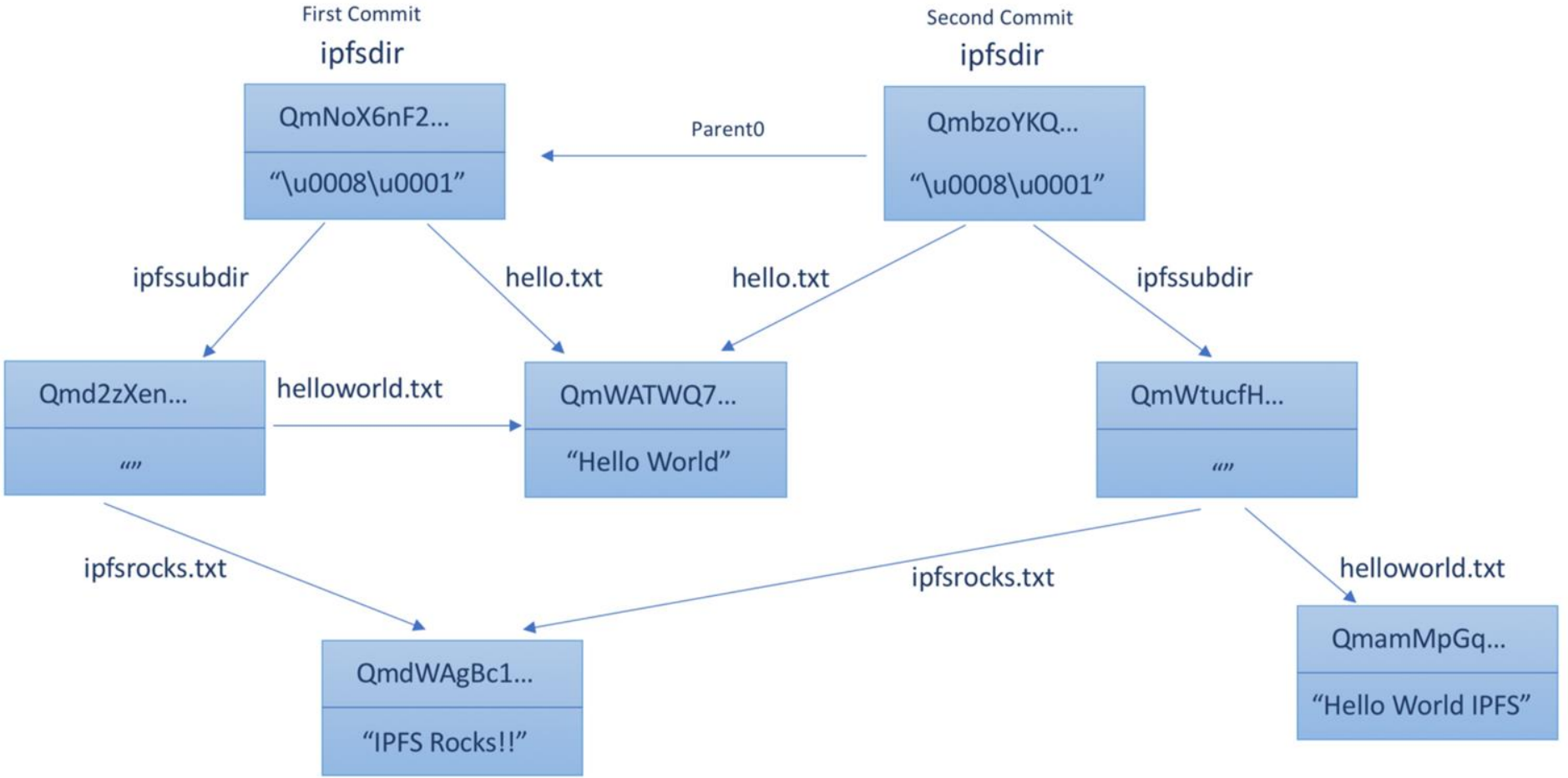
- Când se conectează P2P nodurile, schimbă blocurile pe care le au (**have_list**) și blocurile pe care le caută (**want_list**) sistemul fiind asemanator cu un **sistem barter**

- 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

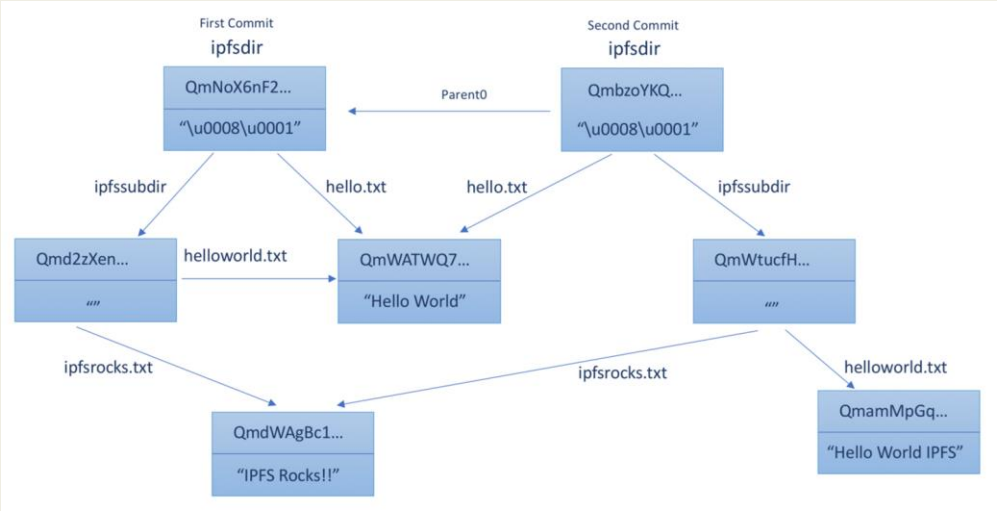
- Versiuni multiple ale unui fișier sunt menținute utilizând o structură de date de tip Merkle Directed Acyclic Graph la un nivel de abstractie superior sistemului de gestiune a fișierelor.
- Elementele de bază ale blocului(lista de blocuri, arborele blocului reprezentând o instanță și commit-ul care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

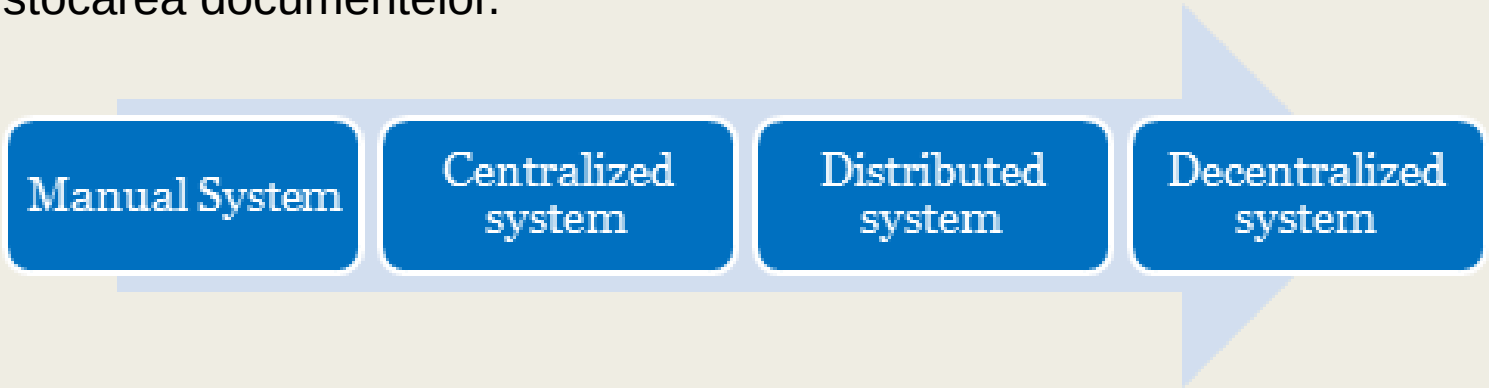


Relatia cu Blockchain

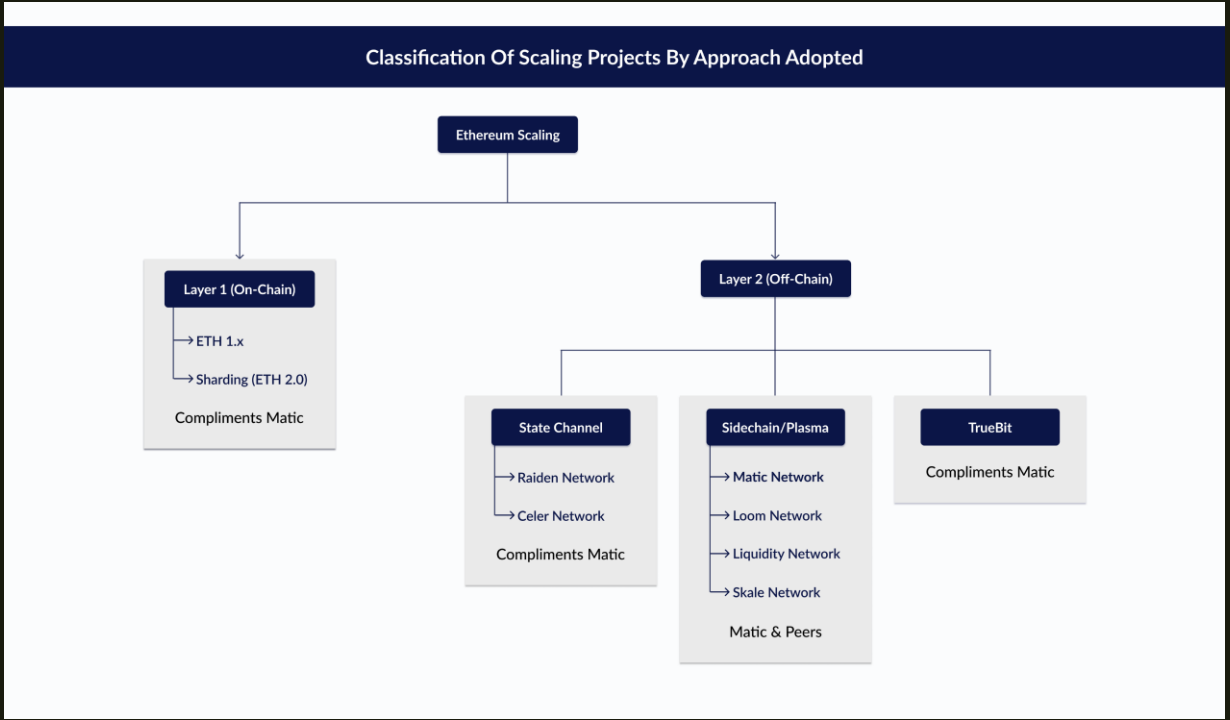
- IPFS poate fi un sistem decentralizat, independent de fișiere.
- Acesta poate fi complementar sistemului centralizat bazat pe HTTP.
- Am discutat despre aceasta în contextul sistemelor blockchain, deoarece poate avea un rol important in stocare descentralizată pentru aplicații blockchain associate 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.



SCALAREA ÎN ETHEREUM 2.0



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