Layer 2 Scaling Solutions Bitcoin - State Channels

Carutasu Stefania, grupa 343

Ce sunt Layer-2 solutions?

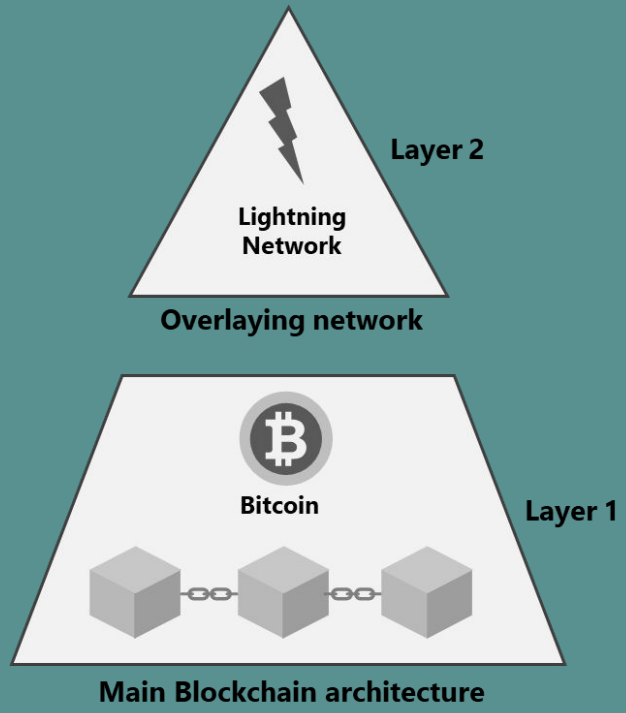
Soluțiile de tip Layer-2 este un termen creat pentru a ajuta la scalarea unei aplicații prin procesarea tranzacțiilor din rețeaua principală Ethereum Mainnet (layer 1) și menținând în același timp aceleași măsuri de securitate și descentralizare ca și rețeaua principală.

Layer-2 este o rețea suprapusă care se află deasupra stratului principal Blockchain subiacent 1. Aceste soluții sunt numite Layer-2 deoarece nu sunt scrise într-un cod care afectează stratul 1. Acestea pot fi construite peste stratul 1 folosind elemente existente deja, precum contractele inteligente.

Layer-2 în cadrul Bitcoin

Considerăm Bitcoin și Rețeaua Lightning. În acest caz, Bitcoin este primul strat (Layer-1) și Rețeaua Lightning este al doilea strat (Layer-2).

Alte exemple sunt Plasma de la Ethereum sau Polygon.



La ce sunt utile soluțiile Layer-2?

Soluțiile de scalare pentru nivelul 2 ajută la creșterea capacităților stratului 1 prin gestionarea tranzacțiilor în afara lanțului. Cele două capacități principale care pot fi îmbunătățite sunt viteza tranzacțiilor și debitul tranzacțiilor.

În plus, soluțiile de nivel 2 pot reduce foarte mult taxele de tranzacție.

Tipuri de soluții de nivel 2

Există 4 categorii de soluții de nivel 2:

- Channels
- Roll-ups
- Plasma
- Sidechains

Spre deosebire de sidechains care au propriile lor proprietăți de securitate, restul se bazează, în general, pe securitatea nivelului 1.

Channels

Canalele sunt un tip de soluții de scalare care permit crearea unui canal de tip peer-to-peer între două părți. Cele două părți pot schimba între ele un număr nelimitat de tranzacții în afara lanțului principat (adică pe nivelul 2), dar pot transmite doar două tranzacții către nivelul 1. Acestea sunt:

- Una este prima tranzacție care deschide conexiunea între stratul principal 1 și stratul canal 2.
- O altă tranzacție stocată pe stratul 1 este tranzacția care închide legătura dintre stratul 1 și stratul 2.

Prin îndepărtarea majorității tranzacțiilor de la nivelul 1, canalele de nivel 2 îmbunătățesc viteza tranzacțiilor și reduc congestionarea rețelei, taxele de tranzacție și întârzierile tranzacțiilor.

Tipuri de canale

Cele mai populare tipuri de canale sunt canalele de stare și canalele de plăți. Canalele de plăți se ocupă cu efectuarea plăților, iar canalele de stare se ocupă cu schimbările de stare generale.

a. Canale de stare
    i. Canalele de stare se ocupă cu actualizările de stare într-o rețea Blockchain
b. Canalele de plăți
    i. Canalele de plăți sunt similare cu cele de stare, dar se ocupă exclusiv cu procesarea plăților. Spre exemplu, canalul de plăți folosit de blockchain-ul Bitcoin este rețeaua Lightning. Canalele facilitează crearea de canale de plăți de tip peer-to-peer între două părți. Cele două părți pot transfera fonduri între ele pe termen nelimitat fără implicarea stratului 1. În cele din urmă, când cele două părți decid să încheie tranzacția, pot închide canalul. Starea finală a tranzacției este apoi înregistrată pe stratul Blockchain 1.

Canalele de stare

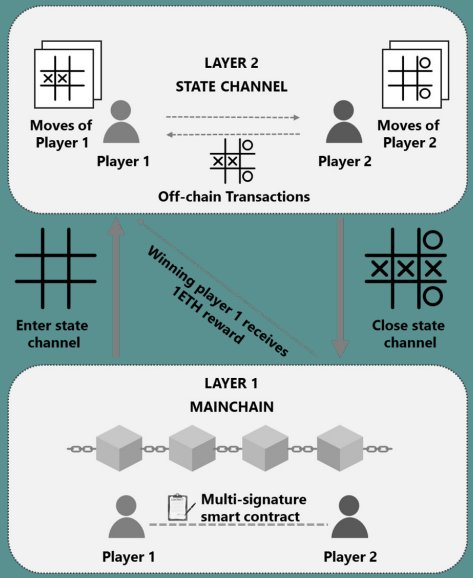
Canalele de stare sunt o formă generală a canalelor de plăți, aplicând aceeași idee în cazul oricărei operații ce produce o schimbare de stare pe un blockchain. Mutarea acestor interacțiuni din lanț fără a necesita încredere suplimentară poate duce la îmbunătățiri semnificative ale costurilor și vitezei. Canalele de stare sunt o parte critică a scalarii tehnologiilor blockchain pentru a sprijini niveluri mai ridicate de utilizare.

Componentele de bază ale unui canal de stare

1. O parte din stare blockchain-ului este blocată printr-o multisignatură a unui contract inteligent astfel încât un set specific de participanți trebuie să se pună de acord unii cu alții pentru ca starea să se actualizeze.
2. Participanții actualizează starea între ei prin construirea și semnarea tranzacțiilor care ar putea fi trimise la blockchain, dar în schimb sunt doar păstrate pentru moment. Fiecare nouă actualizare „depășește” actualizările anterioare.
3. În cele din urmă, participanții trimit starea înapoi la blockchain, care închide canalul de stare și deblochează din nou starea (de obicei într-o configurație diferită de cea cu care a început).

Canalele de stare - exemplificare folosind un joc de X și 0 în blockchain-ul Ethereum

1. Este creat un contract inteligent “Judecător” pe lanțul principal Ethereum care înțelege regulile X și 0 și îi poate identifica pe Alice și Bob drept cei doi jucători din joc. Acest contract deține premiul de 1ETH.
2. Când Alice și Bob încep jocul, canalul este deschis. Fiecare mutare creează o tranzacție în afara lanțului care conține și nonce, adică, ulterior, putem spune în ce ordine s-au efectuat mutările.
3. Când există un câștigător, canalul este închis prin trimiterea stării finale (o succesiune de tranzacții) către contractul “Judecător”, plătind o singură taxă de tranzacție. “Judecătorul” așteaptă o perioadă de timp pentru a se asigura că nimeni nu contestă rezultatul și plătește premiul (1ETH) câștigătorului.



Condiții de funcționare

Pentru funcționarea canalelor de stare, participanții trebuie să poată publica în orice moment starea curentă a canalului în blockchain. Acest lucru are ca rezultat unele limitări importante precum faptul că cineva trebuie să rămână online pentru a proteja interesele tuturor părților implicate până la închiderea canalului.

Dacă în timpul unei tranzacții una dintre părți pierde conexiunea la internet în mod neașteptat, există șanse ca această parte să aibă pierderi. Pentru a evita acest lucru se poate trimite o copie a tranzacției către mai multe servere care, printr-un contract inteligent, se angajează să publice tranzacția (pentru o taxă) în cazul în care această acțiune este necesară.

Condiții de funcționare - continuare

Fiecare actualizare nouă va depăși toate actualizările ce o preced.

Pentru a face această parte a canalului de stare să funcționeze, mecanismele de blocare și deblocare trebuie să fie proiectate cum trebuie, astfel încât vechile actualizări de stare trimise către blockchain au șansa de a fi corectate de actualizările noi de stare care le înlocuiesc.

Cea mai simplă metodă ar fi ca fiecare încercare de deblocare să pornească un timer, în timpul căruia orice actualizare nouă poate înlocui vechea actualizare (și repornește timer-ul). Când timer-ul este încheiat, starea este ajustată să reflecte ultima actualizare primită și canalul este închis.

Referințe

- https://medium.com/techskill-brew/layer-2-blockchain-scaling-solutions-channels-sidechains-rollups-and-plasma-part-16-79819e058ef6
- https://www.one37pm.com/nft/what-are-layer-2-solutions-and-why-are-they-important#:~:text=Layer%202%20is%20a%20term,speed)%20and%20reduce%20gas%20fees.
- https://ethereum.org/en/developers/docs/scaling/state-channels/#:~:text=State%20channels%20allow%20participants%20to,for%20extremely%20high%20transaction%20throughput.
- https://www.jeffcoleman.ca/state-channels/