Sistem distribuit Peer-to-Peer pentru suportul monedelor digitale

Mihai Baba

Rezumat

Problema studiată vizează construirea unui sistem de plată electronic bazat pe rețelele distribuite P2P(Peer-to-Peer) ce are drept scop posibilitatea plății fără ajutorul unei instituții financiare cu rolul de a coordona tranzacțiile.

Arhitectura sistemului este construită din două părți, ce sunt constituite din două servicii:

- Suportul peer-to-peer pe care se bazează întreg sistemul, fiind reprezentat de un DHT(Distributed Hash Table) ce asigură un protocol de regăsire a cheilor stocate distribuit în rețea
- Sistemul tranzacțional propriu-zis ce asigură transferul tranzacțiilor monedelor digitale (în cazul de față Bitcoin), ce este implementat deasupra rețelei peer-to-peer

Pentru construirea rețelei peer-to-peer și a protocolului de regăsire a informațiilor din rețea am ales ca model de referință sistemul distribuit CHORD. Acest sistem reprezintă un DHT ce oferă atât performanțe logaritmice în cadrul căutării și operației de cuplare a nodurilor la rețea, cât și un sistem de distribuire uniformă a cheilor de căutare (Consistent Hashing), împreună cu toleranță la defecte ale nodurilor sau decuplări ale acestora.

Prin acest sistem fiecare nod din rețea (peer) menține legături cu puține alte noduri ale rețelei, mai exact cu un număr de log(N) noduri, unde N este numărul tuturor nodurilor. Astfel, odată cu creșterea rețelei, informațiile reținute de fiecare nod crește logaritmic, făcându-l un sistem scalabil cu un cost al comunicațiilor redus. Rețeaua CHORD presupune ajustarea automată a informațiilor de legătură dintre noduri, asigurând astfel o disponibilitate crescută chiar și în cazul schimbărilor constante din rețea (cuplări ale noilor noduri sau decuplări ale nodurilor participante).

A doua parte a sistemului este reprezentată de implementarea suportului tranzacțional propriu-zis, ce este cuplat la rețeaua peer-to-peer descrisă mai sus, CHORD. Acest suport asigură transferul tranzacțiilor monedelor digitale prin intermediul rețelei într-o manieră securizată, la care fac parte toate nodurile participante din rețea, fără a fi nevoie de o instituție financiară care să coordoneze totul.

Fiecare tranzacție este unicată prin asignarea unei chei hash și a unei semnături digitale a utilizatorului care o inițiază și este verificată de întreaga rețea înainte de a fi validată și procesată. Odată procesată, tranzacția în cauză este asignată unui lanț de chei hash distribuit în rețea, astfel asigurându-i-se imunitatea și unicitatea prin intermediul unei înregistrări ce poate fi schimbată sau modificată doar prin refacerea lanțului de chei realizate până la tranzacția curentă. Această înregistrare a lanțului de chei distribuit în rețea reprezintă modalitatea principală de securizare împotriva atacatorilor (denumită „proof-of-work”), aceștia având nevoie de cel puțin 50% din puterea de procesare a întregii rețele pentru a o putea sparge.