Sistem distribuit peer to peer pentru administrarea unei monede digitale securizate

Sorin Nuțu

Rezumat

Transferul banilor în mediul online se realizează în prezent folosind un intermediar, care este reprezentat de o insituție financiară. Tranzacțiile nu pot fi făcute în orice condiții deoarece trebuie plătite diferite taxe pentru trimiterea banilor sau pentru administrarea conturilor. În plus, Băncile Centrale, prin măsurile pe care le pot întreprinde pot controla în anumite limite evoluția unei valute și astfel pot afecta valoarea efectivă a resurselor financiare pe care un client le deține. În cazul în care o bancă intră în faliment, doar o parte din banii deținuți de clienți pot fi recuperați. Fiind momentan singura soluție de tranzacționare în mediul online, aceste neajunsuri sunt implicit acceptate de către utilizatori.

Lucrarea de față propune o soluție pentru această problemă, folosind un sistem distribuit peer-to-peer descentralizat în care nu există nicio autoritate centrală, semnături digitale pentru a securiza tranzacțiile, un protocol criptografic pentru generarea și verificarea tranzacțiilor valide și o bază de date distribuită numită *blockchain*, care stochează o stare coerentă a întregii valute existente în sistem. O asfel de monedă se numește *cryptocurrency (eng.)*.

Aplicația cuprinde trei module principale:

- Modulul sistemului distribuit peer-to-peer, care formează un *overlay network (eng.)* peste nodurile conectate în rețea pentru a facilita comunicația între utilizatori. Acest modul oferă modulelor superioare o interfață prin care se pot trimite mesaje de tip unicast sau broadcast.
- Modulul care implementează protocolul monedei digitale.
- Modulul client, care oferă utilizatorilor o interfață pentru accesarea sistemului.

Deoarece nu există un server central la care să se conecteze utilizatorii, aceștia trebuie să se organizeze singuri pentru a putea comunica. Structura logică a sistemului distribuit este cea folosită în tabela de dispersie distribuită Chord. Aceasta presupune organizarea logică a nodurilor într-un inel. Pentru a evita complexitatea liniară în raport cu numărul de noduri din rețea pentru a trimite un mesaj, fiecare nod reține un tabel cu alte conexiuni iar un mesaj poate fi trimis în timp logaritmic în raport cu numărul de noduri. Modulul organizează nodurile în structura dorită, facilitează intrarea nodurilor în inel, detectează plecarea unor noduri, reface structura inelului și oferă un mecanism eficient de trimitere a mesajelor în rețea. Nodurile participante au același statut, ele având atât funcții de server cât și de client pentru alte noduri din rețea. Pentru ca un nod să poată intra în sistem trebuie să cunoască cel puțin un alt nod care face deja parte din inel.

Modulul monedei digitale rezolvă două probleme majore. Prima este cheltuirea unor bani de către un utilizator rău intenționat pe care acesta nu îi deține. A doua problemă este cheltuirea multiplă a unei sume de bani (*double spending eng.*). Prima problemă se rezolvă prin înlănțuirea tranzacțiilor din sistem și folosirea semnăturilor digitale pentru a nu permite falsificarea sau modificarea tranzacțiilor deja efectuate. Pentru a rezolva a doua problemă, fiecare nod contribuie la menținerea unei baze de date distribuite prin verificarea și înglobarea tranzacțiilor în blocuri și rezolvarea unei probleme numită *proof-of-work* pentru fiecare bloc. Doar tranzacțiile care se găsesc în blocurile pentru care problema a fost rezolvată sunt considerate valide. Blocurile sunt la rândul lor înlănțuite și modificarea unei tranzacții presupune rezolvarea problemei *proof-of-work* atât pentru blocul din care aparține cât și pentru toate blocurile care se află după el. Astfel, dacă nodurile oneste dețin cel puțin jumătate din puterea de calcul din rețea, un atacator nu poate rezolva problema la fel de repede ca acestea și nu poate comite un atac de tipul *double spending*.