Proiect Blockchain

~Implementarea unui blockchain folosind diferite tehnologii~

Un blockhain este un lant de blocuri care contin informatie. Idea a aparut in anul 1991 ca solutie pentru a asigura validitatea documentelor digitale, dar a fost folosita abia incepand cu anul 2009, odata cu crearea criptomonedei Bitcoin.

Desi tehnologia blockchain este disponibila pentru oricine, aceasta are niste proprietati care o fac sigura. Odata introdusa informatia, aceasta este modificata foarte greu. Fiecare block contine informatia proprie, hash-ul sau (un fel de id prin care este identificat) si hash-ul blocului anterior. Datele continute depind de scopul pe care il are blocul. Hash ul reprezinta semnatura blocului, iar acesta este calculate odata cu crearea blocului. (In cazul nostrum, este calculate adunand indexul blocului, timestamp-ul lui, datele continute dar si hash-ul blocului anterior). Astfel, daca orice este modificat in interiorul unui bloc, hash-ul care face referinta la el devine invalid, la fel ca tot blochain-ul.

Dar cum calculatoarele sunt foarte rapide si pot recalcula toate hash-urile odata ce se produce o schimbare, a aparut nevoia unui al mijloc de Securitate, anume Proof-of-work. Acest mechanism incetineste recalcularea, facand modificarea unui bloc mult mai durabila. Astfel, schimbarea tuturor hash-urilor ar dura mult prea mult.

O alta propretate care asigura securitatea este distribuirea blockchainului intr-o retea peer-to-peer. Astfel, fiecare persoana din retea primeste o copie intreaga a blockchain-ului.

Atunci cand un nou nod este adaugat, fiecare persoana primeste o copie prin care se verifica integritatea lantutui, inainte de a fi adaugat. In acest fel, blocurile care sunt modificate sunt respinde din retea.

Deci, pentru a putea modifica ceva intr-un blockchain, utilizator ar trebui sa modifice toate blocurile din lant, sa refaca proof-of-work pentru fiecare bloc si sa controleze maim ult de jumatate din reteaua peer-to-peer, cee ace este aproape imposibil.

Am ales implementarea unui blockchain folosind python. Proiectul contine o clasa numita Block care se refera la un element al unui blockchain. Fiecare bloc contine hash-ul blocului precedent, propriul sau index, timestampul la care a fost creat, informatia pe care o detine si se identifica printr-un hash propriu, calculate la fiecare initializare a unui nou obiect. Hash ul este calculat adunand toate elementele enumerate mai sus si aplicand asupra lor functia sha256 din libraria hashlib.

Functia genesisblock este folosita pentru crearea primului element din blockchain, deoarece acesta nu se incadreaza in tipar, neavand element precedent.

Functia newblock este folosita pentru a crea un nou bloc, bazat pe blocul anterior pe care il primeste drept parametru.

De asemenea, am definit o functie sameblock care compara 2 blocuri, pentru a verifica daca sunt identice. Am folosit aceasta functie in functia verifynotchanged care verifica daca s-au produs schimbari intre 2 blockchain-uri. (pentru a verifica daca mai sunt valide sau nu).