# Discurs

Blockchain-ul este o tehnologie inventata pentru cei care vor sa faca tranzactii cu monede virtuale. Practic ce sunt niste monede virtuale? sunt niste valori pe care vrem sa le transferam dintr-un cont in altul.

In principiu fiecare user care vrea sa utilizeze chestiunea asta este indentificat printr-o adresa. Cand vor sa faca tranzactii de la unul la altul, cei care au monezi inregistreaza o tranzactie in blockchain.

Ce inseamna asta? – Despre broadcast / descentralizare

Cineva inregistreaza o tranzactie la un nod, dupa care acel nod trimite acea tranzactie si altor noduri, iar acele noduri trimit mai departe altor noduri, intr-un final toate nodurile stiind de acea tranzactie.

Sistemul asta este complet descentralizat in sensul ca nu exista o unitate central care colecteaza informatiile. Si atunci sunt anumite noduri care aleg sa construiasca blocuri care vor contine tranzactii si blocurile se construiesc intr-un process care se cheama de obicei mining.

Ce inseamna mining? –mining/validare

Imi iau cateva tranzactii, incerc sa le pun intr-o anumita ordine astfel incat sa obtin un hash cu o anumita valoare intr-un anumit bloc. Procesul ala se cheama proof of work. Si de obicei la bitcoin ca sa pot face un bloc, procesul ala imi ia in jur de 10 minute.

In momentul in care s-a construit un bloc cu tranzactii, acel bloc este trimis la toata lumea pentru a fi validat. In sensul ca ceilalti se uita acolo si vad ca hash-urile si tot ce tine de integritatea blocului este construit correct si atunci se construieste un bloc si blocul asta va fi adaugat la lantul de blocuri existente pana atunci.

O data o tranzactie adaugata in blockchain ea nu mai poate fi modificata din cauza unei smecherii cu niste hash-uri.

Ce inseamna asta?

Inseamna ca ceilalti care primesc blocul daca vad ca blocul este in regula o sa-l considere ca parte a blockchain-ul. Dupa ei o sa incerce sa construiasca si ei mai departe alte blocuri in care sa adauge alte tranzactii

Care este problema noastra? – problema cu consumul de energie si reward-ul

Una din problemele cele mai mari este ca fiecare poate sa faca mining, de ce e o problema asta? Problema este ca acest mining necesita foarte foarte multa energie. Sunt calculatoare care merg nonstop, sunt mining hubs uriase care contin o gramada de calculatoare si toate astea incearca in acelasi timp sa creeze blocuri si sa le adauge in retea. Acest consum de energia pe care il face bitcoin-ul este echivalentul a cat consuma o tara de exemplu de diminesiunile irlandei, si asta doar la bitcoin, mai sunt si alte monede, ethereum etc

Revenind la proof of work, fiecare incearca sa construiasca blocuri? De ce? Pentru ca este un reward daca blocul lui a fost acceptat si primesti 25 de bitcoin, 8000 de dolari un bitcoin sunt niste bani….

-Proof of stake

Si atunci a aparut un protocol care se cheama proof of stake. Acest protocol incearca sa limiteze numarul de personae care fac mining. Cumva incearca sa ghiceasca, sa stabileasca dinainte pe cei care vor construii blocurile pur si simplu facand un fel de consens relative la cei care vor sa construiasca.

Si cand ma refer la proof of stake? Pe cine o sa aleg sa construiasca blocurile? Pe cei care au cel mai mare interes ca sistemul asta sa functioneaza, adica cei care au cei mai multi bani. Pe masura ce ai mai multi bani iti cresc putin sansele sa faci noi blocuri

-Despre broadcast / descentralizare

-mining/validare

-problema cu consumul de energie si reward-ul

-Proof of stake

Pe langa problema prezentata mai sus, mai subliniez si faptul ca in momentul de fata nu prea exista nici o implementare a acestui protocol, fiind destul de nou. Si astfel mi-am propus sa construiesc o implementare care sa sprijine partea practica sis a testez cam cat de greu este sa construiesti acel protocol pentru ca apar o multime de problem de implementare care nu sunt specificate intr-un paper

La contributii pot spune ca principala contributie este implementarea protocolului care genereaza o lista de probleme ce apar in momentul implementarii si nu sunt specificate in paper cum ar fi.

In continuare o sa explic pe scurt unele chestii de tin de acest protocol.

In figura urmatoare putem vedea niste tranzactii. Ne uitam la prima tranzactie tx0, asa arata o traanzactie intr-un bloc, practic contine o lista cu input-uri si o lista cu output-uri care specifica de unde vin acesti bani(adica din alte output-uri) si unde se duc ei. Si practic cand calzculez suma unui user caut dupa acele output-uri care nu au mai fost folosite intr-un input inca.

Am vorbit pana ana acum despre partea in care proof of stake incearca sa prezica ce nod va construii un bloc in continuare. Pentru asta avem nevoie ne niste timpi, deoarece cand se va face o prezicere, se va spune ca nodul x va produce un bloc la data x. Si pentru asta timpul in protocol este impartit in epoci iar fiecare epoca este impartita in slot-uri, un slot fiind o perioada scurta de timp, 10 secunde de exemplu, numaratoare incepand de la data cand primul bloc a fost adaugat.

Astfel un nod va fi programat la o data, epoca 4 slotul 5, spre exemplu si va va construii un bloc in acel slot, intr-un anumit slot doar un nod fiind desemnat sa construiasca un singur bloc.

Exista 3 tipuri de blocuri, primul bloc de geneza unde este pus numarul total de monede, blocurile obisnuite unde sunt incarcate tranzactiile, iar blocurile genesis sunt blocurile care sunt construite doar cate unul pe epoca si in acele blocuri sunt trecute persoanele care pot construii blocurile intr-un anumit slot.

Cum este realizata aceasta votare?

In 2 parti. Prima parte se numeste multiparty computation si are rolul de construii un seed in retea si a doua parte follow de satoshi care foloseste acel seed si alege slot leader-ii.

In mpc fiecare nod trimite in retea un string critat cu cheia sa privata in commitment phase, in a doua parte fiecare nod trimite string-ul din semnatura si in a 3 a parte se verifica practic semnatura digitala toate mesajele care sunt validate intrand in constructia acelui seed astfel se obtine un seed comun in toata reteaua.

A doua parte numita follow the satoshi in care este construit un arbore binar ca acesta folosind o functie de random initializata cu seed-ul de la faza anterioara. Pe frunze sunt stakeholder-ii, iar pe nivelele superioare este suma celor 2 fii de pe nivelul de jos. Cand se alege un stakeholder se initializeaza un random cu seed-ul concaneta cu numarul slot-ului si se parcurge arborele de la radacina. Explic eu rapid

Fiecare nod va isi va programa folosind acest backgroudn scheduler niste funtii care vor fi activate in fiecacre slot sau la mai multe slot-uri si care vor verifica daca nodul poate construii blocul si vor avea grija ca un nod sa voteze in fiecare epoca, functiile reprogramandu- se singure din nou si din nou

Algoritmul de consen cauta practic cel mai lung blockchain valid din retea, acela fiind considerat blockahin-ul corect.

Apu-ul si initializarea unui nod. Un nod porneste sub forma unui server web ce expune un api, la pornire nodu se va inregistra la un trusted nod care ii va oferit toate informatiile necesare si va anunta si celelalte noduri din retea despre existenta acelui nou nod.