Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing

Byzcoin este un protocol de consens care se bazeaza pe semnarea colectiva pentru a valida tranzactii Bitcoin astfel incat sa fie ireversibile in cateve secunde comparativ cu modelul initial care permite doar 7 tranzactii pe secunda. Acesta reuseste sa obtina consens Byzantin reusind sa pastreze ideea de participare deschisa pe care o introduce Bitcoin, forming dinamic grupuri de consens propotionate in functie de puterea de hash pe care acestea o au intr-un anumit interval de timp. Byzcoin foloseste si arbori Merkel si Schimdt de comunicare pentru a optimiza validarea tranzactiilor si verificarea acestora sub conditii normale oferind de asemenea si siguranta si toleranta la erorile Bizantine ce pot aparea.

Byzcoin construieste pe problemele pe care modelul Bitcoin le prezinta, cautand astfel sa le rezolve si sa ofere cat mai multe tranzactii pe secunda astfel incat plata cu cryptocurrency sa devina la fel de accesibila precum plata cu cardul Visa sau Mastercard. Principala problema pe care o are modelul Bitcoin este aceea ca algorithmul de consens ofera o consistenta probabilistica. Consesnsul descentralizat si securitatea provin din ideea ca majoritatea minerilor urmeaza aceleasi reguli si mereu urmaresc sa ofere cel mai mare lant de tranzactii astfel incat sa fie rasplatiti pentru munca lor. Ideea principala ca o grupare minoritara nu va fi capabila sa creeze un lant de tranzactii fals suficient de repede incat sa depaseasca adevaratul lant creat de ceilalti participanti, acest lucru necesitant o participare mai mare de 50%.

In acest model este posibil ca mai multi mineri sa gaseasca blocuri diferite pe care mai apoi sa le inlantuiasca astfel incat sa apara forkuri sau inconsistente in blockchain. Un block bitcoin este limitat la 1MB ceea ce rezulta intr-un numar mic de tranzactii pe secunda. Datorita forkurilor temporare si a introducerea de mineri rauvoitori intregul sistem poate ajunge intr-o stare unavailable timp de 10 minute ceea ce este destul de mult.

Byzcoin urmareste sa rezolve aceste probleme si multe altele pastrand totusi ideea de open membership (adica oricine sa poate participa obtinandu-se astfel un sistem descentralizat). Acesta implementeaza algoritmul practic pentru toleranta la erori bizantine care este construit peste protocolul de semnare CoSi. Aceastea 2 in combinatie impreuna cu separarea validarii si minarii tranzactiilor idee provenita din Bitcoin NG ofera un sistem scalabil, rapid si sigur care in practica poate produce rezultate neasteptat de bune. Desigur nu reuseste sa acopere toate problemele cum ar fi double spending, insa este o imbunatatire vizibila.

Ideea de a folosi PBFT a venit din natura problemei pe care acesta o rezolva. Algoritmul ofera o solutie practica si asigura faptul ca intr-un sistem distribuit, participantii pot ajunge la o decizie comuna, facand fata la membrii corupti care pot produce erori bizantine, atata timp cat sunt 3f+1 participanti unde f este numarul de calculatoare corupte. In modelul nostru avem nevoie ca participantii sistemului sa valideze diverse tranzactii si sa cada de acord ca ordinea acestora este corecta datorita naturii ireversibile a blockchainului.

Algoritmul are 3 faze distincte:

1. In prima faza un leader(nod primar) trimite catre toti participantii un mesaje de pregatire care semnifica inceputul unei noi runde de votare
2. Fiecare nod primesate mesajul, il valideaza si pregateste la randul lui un mesaj care va fi distribuit tuturor participantilor la retea.
3. Dupa ce face broadcast acesta asteapta 2f + 1 mesaje dupa care in functie de aceasta ia decizi finala pe care o transmite iarasi celorlanti participanti.

Siguranta algoritmului vine din ideea ca leaderul este unul corect, de aceea algoritmul are un sistem ce poate face fata in caz ca leaderul este unul corupt. Daca nodurile simt ca liderul trimite mesaje false se va propune o schimbare de leader, iar toate celelalte noduri vor vota cine sa ii ia locul. Algoritmul a demostrat rezultate foarte bune, problema acestuia fiind faptul ca fiecare nod trebuie sa comunice cu fiecare. Intr-un sistem mic, acest lucru este posibil insa nu este scalabil intr-un sistem precum dorim noi sa il folosim. Alta problema ar fi ca este nevoie de un grup fix de participanti la retea ceea ce incalca ideea de open membership pe care Bitcoin o promoveaza si nu am mai obtine descentralizarea dorita.

Pentru a rezolva aceste probleme este propus protocolul de semnare Cosi care din fericire este unul scalabil. Acesta asigura validarea unui statement de catre mai multi martori participanti ai unui sistem. Protocolul contine un leader si mai multi martori si folosind arbori de comunicare se poate efectua o semnare colectiva care mai apoi sa fie comparata cu semnatura colectiva a participantilor pentru a fi validata.

Pentru ca un mesaj sa fie validat acesta trebuie sa treaca prin 4 etape:

1. Leaderul incepe runda prin emiterea unui mesaj in jos pe arborele de comunicare care initilizeaza semnarea si de asemenea poate contine si mesajul ce treubuie validat. Daca nu este dat in pasul 1 acesta va fi oferit in pasul 3.
2. Fiecare nod isi alege un secret pe care il foloseste sa produca in Schnor commitment. Fiecare nod primeste de mai sus un astfel de commitmet la care agrega commitmentul sau.
3. Leaderul produce o provocare criptografica folosind o functie has pe commitmentul Schonr produs colectiv de catre copii si o trimite acestora impreuna cu mesajul.
4. Folosind commitmentul fiecare nod produce un raspuns agregat care este mai apoi trimis la leader.

Rezultatul acestui proces este o semnatura Schnorr pe care toate lumea o poate verifica improtriva cheii publice produse initial prin agregare astfel obtinandu-se o verificare eficienta a acestei semnaturi. Pe langa aceste imbunatatiri care asigura ca putem folosi algortimul PBFT intr-un sistem mare utilizand scalabilitatea protocolului Cosi, echipa Byzcoin propune si o separare a procesului de verificare a tranzactiilor de cel al alegerii unui lider. Acest lucru creste viteza cu care tranzactiilor pot fi validate si salveaza resurse importante care altfel ar fi utilizate fara folos. Se introduc conceptele de microblocks si keyblocks de catre Bitcoin Ng, Byzcoin folosind si el aceste idei.

In continuare va fi descris procesul de validare pentru o moneda creata peste protocolul Byzcoin si realizeaza acest lucru participantii la retea.

Validarea unei tranzactii se face folosind ideea de proof of work introdusa de Bitcoin care demonstreaza ca participantul este dispus sa ofere o putere de computare hash in schimbul unei recompense. Numai cei ce ofera aceste resurse vor fi permisis sa valideze si sa devina membrii in grupul de consens. Byzcoin adopta acest mecanism imbunatatindu-l si transformandu-l intr-un proof-of-membership. Aceste mecanism pastreaza balanta de putere pe care minerii o au folosind drepturi de participare in grupul de consens alocate in functie de puterea hash oferita intr-un anumit interval de timp. In functie de cat de multe tranzactii valideaza un participant intr-un interval de timp ii vor fi oferite shareruri care mai apoi vor putea fi folosite pentru identificarea acelui membru ca fiind unul de incredere. Ideea este ca aceste shareruri expira si sunt valide numai o perioada de timp, lucru care incurajeaza rasplatirea participantilor activi. Participantii vor fi rasplatiti proportional cu puterea hash oferita in intervalul de timp.

Pentru validarea tranzactiilor protocolul CoSi este folosit prin implementarea a 2 runde initiate de leaderul curent, In prima runda liderul obtine prin PBFT atestari de la majoritatea participantilor dupa care in a doua runda liderul obtine atestaru ca semnarea a fost facuta cu success de 2/3 din participanti.

Chiar daca acest proces este scalabil, poate fi imbunatatit prin separarea responsabilitatii de alegere a leaderului si validare/semnare a trazanctiilor. Pentru a face acest lucru Byzcoin foloseste micro-blocuri care sunt practic blocuri de tranzactii stocate pregatite de commit. Micro-blocurile sunt create la fiecare cateva secunde de catre leader si foloseste protocolul CoSi pentru a le semna si valida. Dupa care blocurile-cheie sunt introduse care sunt practic minate prin proof-of-work si sunt folosite pentru alegerea liderilor.

Decuplarea verificarii tranzactiilor de alegerea liderului poate veni cu un cost. Momentan in PBFT leaderul ales este schimbat doar daca prezinta anumite probleme sau este corupt ceea ce poate oferi o putere prea mare intr-un astfel de sistem numai unei singure entitati. Pentru a rezolva aceasta problema un mecanism de alegere a leaderului este introdus impreuna cu unul de schimbare a ferestrei de alegeri. De fiecare data cand un bloc cheie este semnat Byzcoin forteaza un view-change pentru acel miner care a semnat blocul. Prin acest mod puterea de a verifica transactii in blocuri este asignata numai minerului de drept care detine o serie de micro-blocuri de cand a fost semnat pana cand va fi semnat urmatorul. Cand apare un confilct mai multe astfel de view-changes sunt necesare pentru a convinge cu success ceilalti participanti sa adopte blocul lor.

De exemplu in cazul unui fork pe blocuri cheie, una sau mai multe blocuri castiga dreptul de a fi adaugat in chain. Totusi daca minerul blocului pierzator face un broadcast la blocul sau si 33% de participanti adevarati sunt de acord atunci acela va fi pus inainte de a afla ca este unul mai mare.

Avand toate aceste imbunatatiri protocolul Byzcoin demostreaza rezultate foarte bune, concurand cu tranzactiile Visa sau mastercard reusind totusi sa acopere multe probleme care pot aparea in modelul Bitcoin.