PPCoin: Cripto-Valută cu Dovadă a Mizei (Proof-of-Stake)

Sunny King, Scott Nadal
19 August, 2012

Abstract

Un design de criptomonedă peer-to-peer derivat din Bitcoin-ul lui Satoshi Nakamoto. *Dovadă a Mizei* (Proof-of-stake) înlocuiește *Dovada Muncii* (proof-of-work) pentru a oferi o mai mare securitate a rețelei. Conform acestui design hibrid, *Dovada Muncii* asigură în principal fabricarea inițială a monedelor și este în mare parte neesențială pe termen lung. Nivelul de securitate al rețelei nu depinde de consumul de energie pe termen lung, oferind astfel o criptomonedă peer-to-peer eficientă din punct de vedere energetic și mai competitivă din punct de vedere al costurilor. *Dovada Mizei* se bazează pe vârsta monedei și este generată de fiecare nod printr-o schemă de hash care prezintă similaritate cu Bitcoin, dar în spațiu de căutare limitat. Istoricul blockchainului și decontarea tranzacțiilor sunt protejate în continuare de un mecanism central, ce difuzează puncte de control.

Introducere

De la crearea Bitcoinului (Nakamoto 2008), *Dovada Muncii* a fost designul predominant al criptomonedei peer-to-peer. Conceptul de *Dovadă a Muncii* a constituit coloana vertebrală a modelului de fabricație și securitate, al design-ului lui Nakamoto

În octombrie 2011, ne-am dat seama că, conceptul de *vârstă a monedelor* poate facilita un design alternativ cunoscut sub numele de *Dovadă a Mizei*, față de sistemul de *Dovadă a Muncii* la Bitcoin.
De atunci, am format un proiect în care *Dovada Mizei* este utilizată pentru a construi modelul de securitate al unei cripto-valute *peer-to-peer* și o parte a procesului său de fabricare, în timp ce *Dovada Muncii* facilitează în principal partea inițială a procesului de fabricare, și își reduce treptat semnificația. Acest design încearcă să demonstreze viabilitatea viitoarelor criptomonede peer-to-peer fără dependență de consumul de energie. Am denumit proiectul *ppcoin*.

Vârsta monedei

Conceptul de *vârstă a monedelor* a fost cunoscut de Nakamoto cel puțin încă din 2010 și folosit în Bitcoin, de exemplu pentru a ajuta la prioritizarea tranzacțiilor, deși nu a jucat un rol important în modelul de securitate al Bitcoin. *Vârsta monedei* este pur și simplu definită ca *suma valutară păstrată*. Într-un exemplu simplu de înțeles, dacă Bob a primit 10 monede de la Alice și le-a ținut timp de 90 de zile, spunem că Bob a acumulat 900 de monede-zile în *vârsta monedei*.
Când Bob a cheltuit cele 10 monede pe care le-a primit de la Alice, spunem că monedele-zile acumulate de Bob cu aceste 10 monede au fost consumate (*distruse*).

Pentru a facilita calculul vârstei monedelor, am introdus un câmp de marcare temporală în fiecare tranzacție. Protocoalele legate de *timestamp*-ul blocului și de tranzacționare sunt consolidate pentru a asigura calculul vârstei monedei.

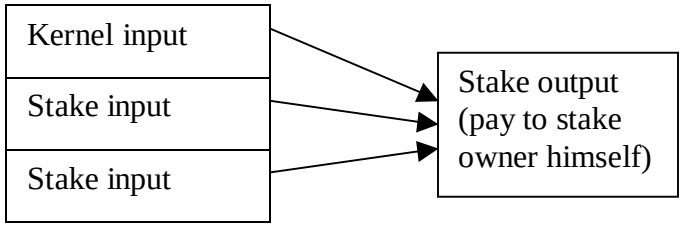
Dovada Mizei (Proof-of-Stake)

Dovada Muncii a contribuit la nașterea progresului major al lui Nakamoto, cu toate acestea *Dovada Muncii* înseamnă că cripto-moneda este dependentă de consumul de energie, introducând astfel costuri semnificative generale în funcționarea acestor rețele, care este suportat de către utilizatori printr-o combinație de inflație și comisioane de tranzacție. Pe măsură ce rata monetară încetinește în rețeaua Bitcoin, în cele din urmă ar putea exercita presiuni asupra majorării taxelor de tranzacție pentru a susține un nivel preferat de securitate. Ne întreabăm în mod natural dacă trebuie să menținem consumul de energie pentru a avea o criptomonedă descentralizată? Astfel, este o etapă importantă atât teoretic cât și tehnologic, să demonstreze că securitatea criptomonedelor de la egal la egal nu trebuie să depindă de consumul de energie.

Un concept numit ***Dovadă a Mizei*** a fost discutat în cercurile Bitcoin încă din 2011. În general, dovada mizei înseamnă o formă de dovadă a proprietății monedei. *Vârsta monedei consumate* de o tranzacție poate fi considerată o formă de *Dovadă a Mizei*. Am descoperit în mod independent conceptul de *Dovadă a Mizei* și conceptul de *Vârstă a Monedelor* în octombrie 2011, prin care ne-am dat seama că dovada mizei poate într-adevăr să înlocuiască majoritatea funcțiilor *Dovezii de Muncă* cu reproiectarea atentă a modelului Bitcoin. Acest lucru se datorează în principal faptului că, similar cu *Dovada Muncii, Dovada Mizei* nu poate fi falsificată. Desigur, aceasta este una dintre cerințele critice ale sistemelor monetare - dificultăți de contrafacere. Vorbind filosofic, banii sunt o formă de dovadă a muncii din trecut, astfel ar trebui să poată înlocui singuri dovada muncii.

Generarea blocurilor cu Dovada Mizei

În designul nostru hibrid, blocurile sunt separate în două tipuri diferite, blocuri de *Dovadă a Muncii* și blocuri *Dovadă a Mizei*.



Structura Transacției de *Dovadă a Muncii* (Coinstake)

Dovada Mizei în noul tip de blocuri este o tranzacție specială numită **coinstake** (*numită după tranzacția specială în Bitcoin coinbase*). În blocul tranzacției coinstake proprietarul primește monede consumându-și astfel vârsta tranzactiei, câștigând în același timp privilegiul de a genera un bloc pentru rețea fabricând Dovada Mizei.

Prima intrare a coinstake-ului se numește *kernel* și este necesară pentru a îndeplini anumite protocoluri de țintă hash, făcând astfel generarea de blocuri un proces stocastic similar cu blocurile de *Dovadă Muncii*. Cu toate acestea, o diferență importantă este că operația de hash se face pe un spațiu de căutare limitat (mai précis: un hash pe secundă la ieșirea portofelului neutilizat) în loc de un spațiu de căutare nelimitat ca în *Dovada Muncii*, astfel nu există un consum semnificativ de energie.

Ținta hash pe care trebuie să o ajungă miezul mizei, este o țintă pe unitatea de vârstă a monedei (monedă-zi) consumată în nucleu (*spre deosebire de ținta în Dovada Muncii la Bitcoin, care este o valoare țintă fixă aplicabilă fiecărui nod*). Astfel, cu cât este consumată mai mult vârsta monedelor în nucleu, cu atât este mai probabil să se îndeplinescă hashul.
De exemplu, dacă Bob are un portmoneu care a acumulat 100 de ani-monedă, se așteaptă ca aceasta să atingă nucleul în 2 zile, atunci Alice cu ieșirea ei de 200 de ani-monedă se poate aștepta aproximativ peste o zi.

În proiectul nostru, atât ținta hash *Dovada Muncii*, cât și ținta hash *Dovada Mizei* sunt ajustate continuu, ce e mai bine decât intervalul de ajustare de două săptămâni cum e la Bitcoin. Asta e pentru a evita saltul brusc al ratei de generare a rețelei.

Fabricarea bazată pe Dovada Mizei

S-a introdus un nou proces de fabricare pentru blocurile de *Dovadă a Mizei*, adăugător la minarea cu *Dovada Muncii* la Bitcoin. Blocul de *Dovadă a Mizei* face monede pe baza *vârstei consumate* a monedei în tranzacția *coinstake*. Se alege rata de fabricare de 1 cent pe monedă-an consumată, pentru a provoacă inflație scăzută pe viitor.

Am păstrat *Dovada Muncii* ca parte a procesului pentru a facilita fabricarea inițială. De asemenea este de conceput că într-un sistem de *pură Dovadă a Mizei*, fabricarea inițială poate fi pornită din blocul genesis (*primul bloc*) printr-un proces similar cu cel de Stock Market. Oferta Inițială Publică (IPO).

Protocolul principal

Protocolul pentru a determina ce blockchain concurent va câștiga ca blockchain principal a fost schimbat, pentru a utiliza vârsta monedei consumate. Aici fiecare tranzacție din bloc contribuie cu *vârsta monedei consumate* la scorul blocului. Blockchain-ul cu o mai mare vârstă totală a monedelor consumate, este ales ca blockchain principal.

Acest lucru este în contrast cu utilizarea Dovezii de Muncă în protocolul Bitcoin, unde *activitatea totală* este utilizată pentru a determina lanțul principal.

Noul design atenuează unele îngrijorări de 51%, ale Bitcoin-ului în care sistemul este considerat sigur doar atunci când nodurile bune controlează cel puțin 51% din puterea de exploatare a rețelei. În primul rând, costul controlului ar trebui să fie mai mare decât costul puterii de minare, crescând astfel și costul atacului pentru entitățile foarte puternice. Vârsta monedelor atacatorului este consumată în timpul atacului, ceea ce face mai dificil pentru atacator ca să continue atacul și să împiedice pătrunderea tranzacțiilor în lanțul principal

Punctele de control: Protecția Istoriei

Unul dintre dezavantajele utilizării vârstei totale a monedei consumate pentru a determina lanțul principal e că: eeste cel mai jos cost pentru atac asupra întregului lanț de blocuri, din toată istoria. Chiar dacă Bitcoin are o protecție relativ puternică, Nakamoto a introdus și puncte de control în 2010, ca mecanism de consolidare a lanțului de blocuri, prevenind orice posibilă modificare ale vreo unei părții ale lanțului, înaintea punctului de control.

O altă neliniștire este că și costul atacului cu dublă cheltuială ar fi putut fi redus, deoarece atacatorul ar putea avea nevoie doar de a acumula o anumită cantitate de vârstă a monedei și de a forța reorganizarea blockchainului. Pentru a face comerțul practic într-un astfel de sistem, am decis să introducem o formă suplimentară de puncte de control care sunt difuzate central, la intervale mult mai scurte, de câteva ori pe zi, pentru a servi la înghețarea blockchainului și finalizarea tranzacțiilor. Acest nou tip de punct de control este difuzat similar cu sistemul de alertă la Bitcoin.

Laurie (2011) susținea că Bitcoin nu a rezolvat complet problema consensului distribuit, deoarece mecanismul pentru punctele de control nu este distribuit. Am încercat să proiectăm un protocol practic de checkpoint distribuit, dar am ajuns la concluzia că e prea dificil ca să ne protejăm împotriva atacului divizat de rețea. Deși mecanismul de verificare difuzat este o formă de centralizare, îl considerăm acceptabil înainte ca o soluție distribuită să fie disponibilă.

Un alt motiv tehnic implică utilizarea punctelor de control difuzate central. Pentru a vă apăra împotriva unui tip de atac de negare a serviciului, nucleul *coinstake* trebuie verificat înainte ca un bloc *Dovadă a Mizei* să poată fi acceptat în baza de date locală (arborele blocului) a fiecărui nod. Datorită modelului de date al nodului Bitcoin (specificarea indicelui tranzacției) este necesar un termen limită de verificare pentru a asigura capacitatea tuturor nodurilor, de a verifica conexiunea fiecărui nucleu *coinstake* înainte de a accepta un bloc în arborele blocului. Datorită considerațiilor practice de mai sus, am decis să nu modificăm modelul de date al nodului, ci să folosim în schimb punctele de control centrale. Soluția noastră este să modificăm calculul vârstei monedei pentru a necesita o vârstă minimă, cum ar fi o lună, sub care vârsta monedei este calculată ca zero. Apoi, punctul de control central este utilizat pentru a se asigura că toate nodurile pot conveni asupra tranzacțiilor anterioare mai vechi de o lună, permițând astfel verificarea conexiunii kernel coinstake, deoarece un kernel necesită o vârstă de monedă diferită de zero, astfel că trebuie să utilizeze o ieșire de acum mai mult de o lună.

Semnăturile Blocurilor și Duplicatul Protocolului de Miză

Fiecare bloc trebuie să fie semnat de proprietarul său pentru a împiedica copierea și utilizarea aceleiași Dovezi de Miză de către atacatori.

Un Protocol Duplicat de Miză este conceput pentru a se apăra împotriva unui atacator folosind o singură Dovadă de Miză cu care poate genera o multitudine de blocuri ca atac de negare a serviciului. Fiecare nod colectează perechea (kernel, timestamp) a tuturor tranzacțiilor coinstake pe care le-a văzut. Dacă blocul primit conține o pereche duplicată ca blocul primit anterior, ignorăm un astfel de bloc (duplicat de miză) până când un bloc succesor este primit ca bloc orfan.

Eficienta energetică

Atunci când rata Dovezii de Muncă se apropie de zero, există din ce în ce mai puține stimulente pentru generarea blocurilor. În acest scenariu pe termen lung, consumul de energie în rețea poate scădea la niveluri foarte scăzute, deoarece minerii dezinteresați opresc exploatarea blocurilor de dovadă a muncii. Rețeaua Bitcoin se confruntă cu un astfel de risc, cu excepția cazului în care volumul / comisionul tranzacției crește la niveluri suficient de ridicate pentru a susține consumul de energie. Conform proiectării noastre, chiar dacă consumul de energie se apropie de zero, rețeaua este încă protejată de Dovada Mizei. Deci, o numim: o cripto-monedă *de termen lung, eficientă* din punct de vedere energetic, chiar când consumul de energie la Dovada Muncii se apropie de zero

Alte considerente

Am modificat rata de generare la Dovada Muncii, pentru a nu fi determinată de înălțimea blocului (timp), ci determinată de dificultate. Când crește dificultatea de exploatare, rata de generare la Dovadă Muncii este redusă. O curbă relativ netedă este aleasă spre deosebire de funcțiile pasului Bitcoin, pentru a evita șocul artificial al pieței. Mai precis, o curbă continuă este aleasă astfel încât fiecare creștere de 16 ori a dificultății să se înjumătățească cantitatea monedelor.

Pe termen mai lung, curba de generare cu Dovada Muncii nu ar fi prea diferită de cea a Bitcoin în ceea ce privește comportamentul inflaționist, având în vedere continuarea Legii lui Moore. Considerăm că este înțelept să urmăm observația tradițională conform căreia piața favorizează o monedă cu inflație scăzută față de o monedă cu inflație ridicată, în ciuda criticilor semnificative ale Bitcoin din partea unor economiști de masă din motive ideologice în opinia noastră.

Babaioff și colaborarorii (2011) au studiat efectul taxei de tranzacție și au susținut că taxa de tranzacție este un stimulent pentru a nu coopera între mineri. În sistemul nostru, acest atac este accentuat, astfel încât nu mai acordăm taxe de tranzacție pentru a bloca proprietarul. Am decis să distrugem în schimb taxele de tranzacție. Aceasta elimină stimulentul de a nu recunoaște blocurile altor mineri. De asemenea, servește ca o forță deflaționistă pentru a contracara forța inflaționistă de la fabricarea cu Dovada Mizei.

De asemenea, alegem să aplicăm taxele de tranzacționare la nivel de protocol pentru a ne apăra împotriva atacului de balonare.

În timpul cercetării noastre am descoperit și o a treia posibilitate în afară de Dovada muncii și Dovada mizei, pe care le-am numit *Dovada Excelenței*. În cadrul acestui sistem, în mod obișnuit se organizează periodic un turneu pentru a bate monede pe baza performanței participanților la turneu, mimând premiile turneelor din viața reală. Deși acest sistem tinde să consume și energie atunci când inteligența artificială excelează în jocul implicat, am găsit în continuare conceptul interesant chiar și într-o astfel de situație, deoarece oferă o formă oarecum inteligentă de consum de energie.

Conclusia

După validarea designului nostru pe piață, ne așteptăm ca modelele de Dovadă a Mizei să devină o formă potențial mai competitivă de criptomonedă peer-to-peer decât proiectele de Dovada Muncii, datorită eliminării dependenței de consumul de energie, realizând astfel inflație mai mică, taxe de tranzacție mai mici la niveluri comparabile de securitate a rețelei.

Confirmare

Multe mulțumiri lui Richard Smith, pentru că a ajutat la testare și la diverse lucrări legate de rețea și forcare.
Dorim să mulțumim dezvoltatorilor Satoshi Nakamoto și Bitcoin-ului a căror strălucită lucrare de pionierat ne-a deschis mintea și a făcut posibil un astfel de proiect.

Referințe

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): "Probabil că monede descentralizate este imposibil de făcut, dar să le facem cel puțin eficiente". (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.
(http://www.bitcoin.org/bitcoin.pdf)