PPCoin: Peer-to-Peer Crypto-Valuta met Proof-of-Stake

Sunny King, Scott Nadal
Sunnyking9999@Gmail.com , Scott.Nadal@gmail.com)

19 Augustus 2012

Abstract

Een peer-to-peer crypto-valuta ontwerp afgeleid van Satoshi Nakamoto's Bitcoin.
Proof-of-stake vervangt proof-of-work om de meerderheid van de netwerkbeveiliging te leveren.
Onder dit Hybride-Design levert proof-of-work voornamelijk het initiële creëren van de munt oftewel het 'slaan van de munt' genaamd 'minting' en is grotendeels niet-essentieel op de lange termijn.
Het beveiligingsniveau van het netwerk is niet afhankelijk van het energieverbruik op de lange termijn waardoor een energie-efficiënte en kosten-concurrerender peer-to-peer crypto-valuta wordt geleverd. Proof-of-stake is gebaseerd op de leeftijd van de munt (coin age) en wordt gegenereerd door elke node via een hashing scheme met een gelijkenis van de Bitcoin, maar binnen een beperkte zoekruimte. Block chain geschiedenis en het overeenkomen van transacties zijn verder beschermd door een centraal uitgezonden controlepunt mechanisme.

Inleiding

Sinds de oprichting van Bitcoin (Nakamoto 2008), is proof-of-work het overheersende ontwerp van peer-to-peer crypto-valuta geweest. Het concept van proof-of-work is de ruggengraat van het 'munten-slaan' en het veiligheidsmodel van Nakamoto's ontwerp.

In oktober 2011, hebben we ons gerealiseerd dat het concept van muntleeftijd *(coin age)* kan voorzien in een alternatief ontwerp, bekend als *proof-of-stake* , aan Bitcoin's proof-of-work systeem. We hebben sindsdien een ontwerp geformaliseerd waar proof-of-stake wordt gebruikt om het beveiligingsmodel van een peer-to-peer crypto valuta te bouwen en een deel van het 'munten-slaan' proces, daar waar proof-of-work overwegend het initiële deel van het munten slaan faciliteert en waarvan de belangrijkheid gaandeweg vermindert. Dit ontwerp probeert de levensvatbaarheid van toekomstige peer-to-peer crypto-valuta aan te tonen zonder afhankelijkheid van energieverbruik. Wij hebben dit project *ppcoin* genoemd.

Muntleeftijd

Het concept van muntleeftijd was al minstens zo vroeg als in 2010 bekend bij Nakamoto en wordt bijvoorbeeld gebruikt in Bitcoin om te helpen bij het prioriteren van transacties, hoewel het geen cruciale rol speelde in de Bitcoin's veiligheidsmodel. Muntleeftijd wordt simpelweg gedefinieerd als 'valutabedrag' maal 'vasthoudt periode'. In een eenvoudig te begrijpen voorbeeld: als Bob 10 munten ontvangt van Alice en houd deze vast gedurende 90 dagen, dan zeggen we dat Bob 900 munt-dagen van muntleeftijd heeft verzameld.

Bijkomend, als Bob de 10 munten uitgeeft die hij ontving van Alice, zeggen we dat de muntleeftijd die Bob had opgebouwd met deze 10 munten is *verbruikt* (of *vernietigd*).

Om de berekening van de muntleeftijd te faciliteren hebben we een ‘timestamp’ veld in elke transactie geïntroduceerd. Blok timestamp en transactie timestamp gerelateerde protocollen worden gesterkt om de berekening van de muntleeftijd te beveiligen.

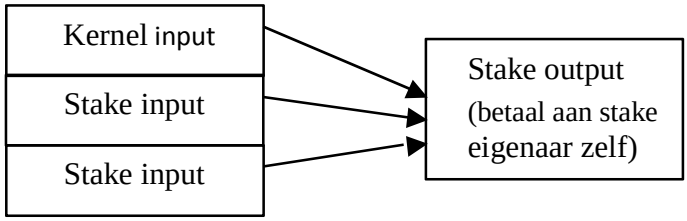
Proof-of-stake

Proof-of-work heeft geholpen met Nakamoto’s grote doorbraak, maar de aard van het proof-of-work betekent dat de crypto-valuta afhankelijk is van energie consumptie, waardoor een aanzienlijke kosten overhead wordt geïntroduceerd bij het operationeel houden van een dergelijk netwerk, waarbij de kosten worden gedragen door de gebruikers via een combinatie van inflatie en transactie kosten. Omdat de snelheid waarmee de munten gegenereerd worden vertraagt in het Bitcoin netwerk, kan dit uiteindelijk druk uitoefenen op het verhogen van transactiekosten om een gewenst niveau van beveiliging te behouden. Een logische vraag is of wij energieverbruik moeten handhaven om een gedecentraliseerde crypto-valuta te behouden. Het is dus een belangrijke mijlpaal, zowel theoretisch en technologisch, om aan te tonen dat de veiligheid van peer-to-peer crypto-valuta's niet afhankelijk hoeft te zijn van energieverbruik.

Een concept genoemd als proof-of-stake werd besproken in de Bitcoin cirkels al zo vroeg als 2011. Ruwweg gesproken, proof-of-stake is een vorm van bewijs van eigendom van de munt. Verbruikte muntleeftijd door een transactie kan worden beschouwd als een vorm van proof-of-stake. Wij hebben het concept van proof-of-stake en het concept van muntleeftijd onafhankelijk ontdekt in oktober 2011, waarbij we ons realiseerden dat proof-of-stake inderdaad de meeste functies van proof-of-work kan vervangen a.d.h.v. een zorgvuldig herontwerp van Bitcoin’s ‘munten-slaan’ en veiligheidsmodel. Dit is vooral omdat, gelijkaardig aan proof-of-work, proof-of-stake niet gemakkelijk kan worden vervalst. Uiteraard is dit één van de essentiële eisen van monetaire systemen - moeilijkheid om te vervalsen. Filosofisch gesproken, is geld een vorm van 'proof-of-work' in het verleden dus dit zou op zichzelf proof-of-work moeten kunnen vervangen.

Blok generatie onder proof-of-stake

In onze hybride ontwerp, zijn blokken verdeeld in twee verschillende typen, proof-of-work blokken en proof-of-stake blokken.



Figuur: Structuur van de Proof-of-Stake (Coinstake) transactie.

De proof-of-stake in het nieuwe block-type is een speciale transactie genoemd *coinstake* (vernoemd naar Bitcoin’s speciale transactie *coinbase*). In het coinstake transactie blok betaalt de eigenaar zichzelf, waarbij zijn muntleeftijd wordt geconsumeerd en onderwijl het recht verkrijgt voor het genereren van een block voor het netwerk en het “munten-slaan’ voor proof-of-stake.

De eerste input van coinstake heet *kernel* en is nodig om te voldoen aan bepaalde hash-target protocol, waardoor het genereren van proof-of-stake blocks een stochastisch proces wordt, vergelijkbaar met proof-of-work blocks. Echter een belangrijk verschil is dat de hash-bewerking wordt gedaan in een beperkte zoekruimte (meer in het bijzonder één hash per niet-bestede portefeuille-output (wallet-output) per seconde) in plaats van een onbeperkte zoekruimte zoals proof-of-work, dus is er geen significante energie consumptie bij betrokken.

De hash-target waaraan de stake kernel moet voldoen is een streefwaarde per eenheid muntleeftijd ('coin-day' / munt-dag) verbruikt in de kernel (in tegenstelling tot Bitcoin's proof-of-work doelstelling die een vaste streefwaarde toepast op elk node). Dus hoe meer muntleeftijd verbruikt word in de kernel, des te gemakkelijker is het om te voldoen aan het protocol van de hash-target. Bijvoorbeeld, als Bob een portefeuille-output heeft die opgeteld 100 munt-jaar bevat en verwacht dat het voor het genereren van een kernel 2 dagen nodig is, dan kan Alice ongeveer verwachten dat haar 200 munt-jaar portefeuille-output 1 dag nodig heeft voor het genereren van een kernel.

In ons ontwerp worden zowel proof-of-work hash-target en proof-of-stake hash-target voortdurend aangepast, in plaats van Bitcoin's de twee wekelijkse aanpassingsinterval, om plotselinge sprongen te voorkomen in de netwerk generatie snelheid.

'Munten-Slaan' op basis van proof-of-stake

Een nieuw 'munten-slaan' proces is ingevoerd voor proof-of-stake blokken als toevoeging op Bitcoin's proof-of-work 'munten-slaan'. Proof-of-stake blokken slaan munten op basis van de verbruikte muntleeftijd in de coinstake transactie. Een 'munt-slaan' tarief van 1 cent per verbruikte munt-jaar is gekozen om aanleiding te geven tot een lage toekomstige inflatie.

Ondanks dat we proof-of-work hebben gehouden als onderdeel van het 'munten-slaan' proces om het initiële 'munten-slaan' te faciliteren, is het denkbaar dat in een zuiver proof-of-stake systeem het eerste 'munten-slaan' volledig in genesis block kan worden gevoed via een proces vergelijkbaar met het eerste openbare aanbod (IPO – Initial Public Offer) van de aandelen beurs.

Main Chain Protocol

Het protocol voor het bepalen welk concurrerende blokketen wint als main chain (belangrijkste keten) is aangepast om de verbruikte muntleeftijd te gebruiken. Hier draagt elke transactie in een blok haar verbruikte muntleeftijd bij aan de score van het block. Het keten blok met het hoogst totaal verbruikte muntleeftijd is gekozen als belangrijkste keten.

Dit is in tegenstelling tot het gebruik van proof-of-work in Bitcoin's main chain protocol, waarbij de totale hoeveelheid werk van het blokketen wordt gebruikt om de belangrijkste keten te bepalen.

Het ontwerp vermindert een aantal bezorgdheden omtrent Bitcoin's 51% aanname, waarbij het systeem alleen als veilig wordt beschouwd wanneer goede nodes ten minste 51% van de netwerk mining kracht beheren. Als eerste zouden de kosten voor het beheren van de meerderheid hoger kunnen zijn dan de kosten van het verwerven van een aanzienlijke hoeveelheid mining kracht, met als gevolg een verhoging van de kosten voor een aanval van dergelijke krachtige entiteiten.

Ook wordt de muntleeftijd van de aanvaller verbruikt tijdens de aanval, waardoor het voor de aanvaller moeilijker wordt om te blijven voorkomen dat transacties in de belangrijkste keten wordt geplaatst.

Checkpoint: Bescherming van de geschiedenis

Een van de nadelen van het gebruiken van totale verbruikte muntleeftijd om de belangrijkste keten te bepalen is dat het de kosten van een aanval op de gehele blokketen van geschiedenis verlaagt. Hoewel Bitcoin een relatief sterke bescherming heeft over de geschiedenis, introduceerde Nakamoto in 2010 toch controlepunten als een mechanisme om de blokketen geschiedenis te versterken ter voorkoming van eventuele wijzigingen van het deel van het blokketen dat ouder is dan het controlepunt.

Een andere zorg is dat de kosten van een double-spending aanval (dubbel-uitgeven) ook kan zijn verlaagd, sinds een aanvaller alleen maar een bepaalde hoeveelheid muntleeftijd hoeft te verzamelen en een reorganisatie van de blokketen zou hoeven te forceren. Om handel praktisch te maken in een dergelijk systeem hebben wij besloten om een aanvullende vorm van controlepunten te introduceren die centraal worden uitgezonden met veel kortere tussenpozen, zoals een paar keer dagelijks, om te serveren aan freeze block chain en om transacties af te ronden. Dit nieuwe type van een checkpoint is vergelijkbaar met de Bitcoin's waarschuwing systeem.

Laurie (2011) heeft gepleit dat Bitcoin niet volledig het gedistribueerde consensusselectie probleem heeft opgelost omdat het mechanisme voor controlepuntbeheer niet gedistribueerd is. We hebben geprobeerd een praktisch gedistribueerde controlepuntbeheer protocol te ontwerpen, maar vonden het moeilijk om dit te beveiligen tegen een netwerk split aanval. Hoewel het broadcasted controlepuntbeheer mechanisme een vorm van centralisatie is, vinden wij het aanvaardbaar voordat een gedistribueerde oplossing beschikbaar is.

Een andere technische reden betreft het gebruik van centraal uitgezonden controlepuntbeheer. Om te kunnen verdedigen tegen een soort denial-of-service aanval moet de coinstake kernel worden gecontroleerd voordat een proof-of-stake blok kan worden aanvaard in de lokale database (block tree) van elke node. Als gevolg van Bitcoin's node gegevensmodel (en dan specifiek de transactie index) is een deadline van het controlepuntbeheer nodig om zeker te zijn van de mogelijkheid van elke node, om de verbinding van elke coinstake kernel te verifiëren, nog voordat een blok in de block tree wordt geaccepteerd. Vanwege de hierboven beschreven praktische overwegingen hebben we besloten om het node gegevens model niet te wijzigen, maar gebruik te maken van centrale controlepuntbeheer. Onze oplossing is een wijziging in de berekening van de muntleeftijd, welke een verplichting vereist voor een minimum leeftijd, zoals bijvoorbeeld één maand, waarbij alles ónder deze waarde wordt berekend als een muntleeftijd van nul. Vervolgens kan het centrale controlepuntbeheer worden gebruikt om ervoor te zorgen dat alle nodes overeenstemming hebben over afgelopen transacties ouder dan een maand. Hiermee wordt de verificatie van de coinstake kernel verbinding toegestaan, omdat een kernel een niet-nul muntleeftijd vereist en dus een output van meer dan een maand geleden moet gebruiken.

Block Signatures en Duplicate Stake Protocol

Elk blok moet worden ondertekend door de eigenaar om te voorkomen dat dezelfde proof-of-stake wordt gekopieerd en gebruikt wordt door aanvallers.

Een duplicate-stake protocol is ontworpen om te verdedigen tegen een aanvaller die d.m.v. het een enkele proof-of-stake een veelheid van blokken genereerd als een denial-of-service-aanval. Elke node verzamelt het (kernel, timestamp) paar van alle coinstake transacties die het heeft gezien.

Als een ontvangen blok een dubbel paar bevat identiek aan dat van een ander eerder ontvangen blok, negeren we dit dergelijke duplicate-stake blok totdat een opvolger blok (successor block) wordt ontvangen als een gekoppelde blok (orphan block).

Energie-efficiëntie

Wanneer de proof-of-work 'munt-slaan' snelheid nul benadert, is er minder en minder motivatie om proof-of-work blokken 'te slaan'. Onder dit lange termijn scenario kan het energieverbruik in het netwerk tot zeer lage niveaus dalen wanneer gedesinteresseerde gebruikers stoppen met het verzamelen van proof-of-work blokken. Het Bitcoin-netwerk wordt geconfronteerd met een dergelijke risico tenzij het transactie volume/kosten tot hoog genoeg niveaus stijgen om het energieverbruik op peil te houden. Zelfs als de energie consumptie nul benadert zal in ons ontwerp het netwerk nog steeds beschermd worden door proof-of-stake. We noemen een crypto-valuta *lang- termijn energie-efficiënt* als energieverbruik op proof-of-work is toegestaan om de nul te benaderen.

Andere overwegingen

We hebben de proof-of-work 'munt-slaan' snelheid aangepast zodat deze niet wordt bepaald door de blok hoogte (tijd), maar in plaats daarvan wordt dit bepaald door de moeilijkheidsgraad. Wanneer de moeilijkheid van het delven (mining) omhoog gaat, wordt de 'munt-slaan' snelheid verlaagd. Een relatief gladde curve is gekozen in tegenstelling tot Bitcoin's stap functies om te voorkomen dat de markt een kunstmatige shock wordt toegebracht. Meer specifiek is dat een doorlopende curve is gekozen zodanig dat, elke 16^{de} keer dat de delf moeilijkheid wordt verhoogd, de 'munt-slaan' snelheid wordt gehalveerd.

Op langere termijn zou de proof-of-work 'munt-slaan' curve niet veel verschillen aan die van Bitcoin in termen van het inflatoire gedrag, gekeken naar de voortzetting van de wet van Moore. Wij achten het verstandig om de traditionele observatie te volgen dat de markt een lage inflatie valuta verkiest boven een valuta met hoge-inflatie, ondanks significante kritiek over Bitcoin van sommige mainstream economen als gevolg van, naar onze mening, ideologische redenen.

Babaioff et al. (2011) bestudeerde het effect van transactiekosten en voerde aan dat de transactiekosten een stimulans is om bij het delven niet onderling samen te werken. Onder ons systeem is deze aanval verergerd dus geven wij geen transactiekosten meer aan de eigenaar van het blok. We besloten in plaats daarvan om de transactiekosten te vernietigen. Hiermee wordt de stimulans verwijderd van het niet erkennen van blokken van de andere gebruikers. Het dient ook als een deflatoire kracht tegen de inflatoire kracht van het proof-of-stake 'munten-slaan'.

We kiezen er ook voor om transactiekosten op protocolniveau af te dwingen om te verdedigen tegen een block bloating aanval. (het vergroten van de block chain)

Tijdens ons onderzoek hebben we ook een derde mogelijkheid naast proof-of-work en proof-of-stake ontdekt, die we *proof-of-excellence* noemen. Onder dit systeem wordt doorgaans periodiek een toernooi gehouden om munten te slaan op basis van de prestaties van de toernooi deelnemers, waarbij

de prijzen van levensechte toernooien nagebootst worden. Hoewel dit systeem de neiging heeft ook energie te verbruiken wanneer kunstmatige intelligentie uitblinkt in het betrokken spel, vonden we het concept nog steeds interessant, zelfs in een dergelijke situatie, aangezien het voorziet in een enigszins intelligente vorm van energieverbruik.

Conclusie

Na validatie van ons ontwerp in de markt verwachten wij dat proof-of-stake ontwerpen een potentieel meer concurrerende vorm zal worden van een peer-to-peer crypto-valuta proof-of-work ontwerp als gevolg van de verwijdering van de afhankelijkheid op het energieverbruik, hetgeen lagere inflatie / transactiekosten met vergelijkbare netwerk beveiligingsniveaus oplevert.

Met dank aan

Veel dank aan Richard Smith voor het helpen met testen en diverse netwerk/fork gerelateerd werk.

Wij zouden graag Satoshi Nakamoto en de Bitcoin ontwikkelaars willen bedanken wiens briljante pionierswerk onze geest heeft geopend en een project zoals dit mogelijk maakt.

Verwijzingen

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

Laurie B. (2011): Decentralised currencies are probably impossible (but let’s at least make them efficient). (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)