Bitcoin: Jafningja-rekið rafrænt peningakerfi

Satoshi Nakamoto

satoshin@gmx.com

www.bitcoin.org

Útdráttur. Eingöngu jafningjaútgáfa af rafrænum peningum myndi leyfa greiðslur á netinu til að senda beint frá einum aðila til annars án þess að fara í gegnum a fjármálastofnun. Stafrænar undirskriftir veita hluta af lausninni, en aðal bætur tapast ef traustur þriðji aðili þarf enn að koma í veg fyrir tvöfalda eyðslu. Við leggjum til lausn á tvíeyðsluvandanum með því að nota jafningjanet. Netið tímastimplar viðskipti með því að tæta þau inn í áframhaldandi keðju af tætisbundinni vinnusönnun, og myndar skrá sem ekki er hægt að breyta án þess að endurtaka vinnusönnunin. Lengsta keðjan þjónar ekki aðeins sem sönnun fyrir röðun atburða, heldur sönnun þess að það kom frá stærstu laug CPU afla. Sem lengi sem meirihluti örgjörvaaflsins er stjórnað af hnútum sem eru ekki í samstarfi við að ráðast á netið, búa þeir til lengstu keðjuna og fara fram úr árásarmönnum. Netið sjálft krefst lágmarks uppbyggingu. Skilaboð eru send út eftir bestu getu, og hnútar geta yfirgefið og gengið aftur í netið að vild og samþykkja lengstu vinnusönnunarkeðjuna sem sönnun fyrir því sem gerðist á meðan þeir voru í burtu.

1. Inngangur

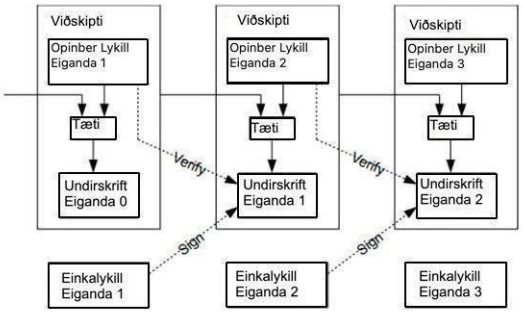
Viðskipti á netinu eru farin að treysta nær eingöngu á fjármálastofnanir sem þjóna sem traustir þriðju aðilar til að vinna rafrænar greiðslur. Þó að kerfið virki nógu vel fyrir flest viðskipti, þjáist það enn af eðlislægum veikleikum traustslíkansins. Algerlega óafturkræf viðskipti eru í raun ekki möguleg þar sem fjármálastofnanir geta ekki forðast að miðla deilum. Kostnaður við miðlun eykur viðskiptakostnað og takmarkar lágmarks hagnýt viðskiptastærð og skera úr möguleikanum fyrir lítil tilfallandi viðskipti, og það er víðtækari kostnaður í því að missa getu til að inna af hendi óafturkræfar greiðslur fyrir óafturkræfa þjónustu. Með möguleika á viðsnúningi dreifist þörfin fyrir traust. Kaupmenn verða að vera á varðbergi gagnvart viðskiptavinum sínum, þræta við þá til að fá meiri upplýsingar en þeir þyrftu annars. Ákveðið hlutfall svika er viðurkennt sem óhjákvæmilegt. Þennan kostnað og greiðsluóvissu er hægt að forðast í eigin persónu með því að nota áþreifanlegan gjaldmiðil, en ekkert kerfi er til til að framkvæma greiðslur yfir samskiptarás án trausts aðila.

Það sem þarf er rafrænt greiðslukerfi byggt á dulmálssönnun í stað trausts, sem leyfir hverjum tveimur viljugum aðilum að eiga bein viðskipti sín á milli án þess að þörf sé á traustum þriðja aðila. Viðskipti sem reikningslega eru óframkvæmanleg að snúa við myndu vernda seljendur frá svikum og auðvelt væri að innleiða venjubundið vörslukerfi til að vernda kaupendur. Í þessari grein leggjum við til lausn á tvíeyðsluvandanum með því að nota jafningja-dreifðum tímastimplaþjón til að búa til útreikningssönnun á tímaröð viðskipta. Kerfið er öruggt svo framarlega sem heiðarlegir hnútar stjórna sameiginlega meira örgjörvaafli en nokkur annar samstarfshópur árásarhnúta.

2. Viðskipti

Við skilgreinum rafkrónu sem keðju stafrænna undirskrifta. Hver eigandi flytur krónuna til þanns næsta með því að undirrita tæti af fyrri færslu og opinbera lykil næsta eiganda stafrænt og bæta þessum við endann á krónunni.

Viðtakandi greiðslu getur staðfest undirskriftir til að staðfesta keðjuna af eignarhaldi.

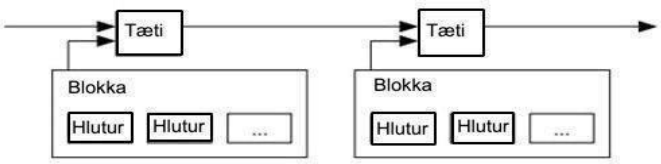


Vandamálið er auðvitað að viðtakandi greiðslu getur ekki sannreynt að einn af eigendunum hafi ekki tvöfalt eytt krónunni. Algeng lausn er að kynna til leiks traust yfirvald, eða mynt, sem athugar hver viðskipti fyrir tvöfalda eyðslu. Eftir hverja færslu verður að skila krónunni í myntina til gefa út nýja krónu, og aðeins krónur sem gefnar eru út beint úr myntinni er treyst fyrir að vera ekki tvíeytt. Vandamálið við þessa lausn er að örlög alls peningakerfisins ráðast af fyrirtæki sem rekur myntið, þar sem öll viðskipti þurfa að fara í gegnum þau, rétt eins og banki.

Við þurfum leið fyrir viðtakendur greiðslu til að vita að fyrri eigendur hafi ekki skrifað undir fyrri viðskipti. Í okkar tilgangi eru fyrstu viðskiptin sú sem gilda, svo okkur er alveg sama um síðari tilraunir til að tvíeyða. Eina leiðin til að staðfesta fjarveru viðskipta er að vera meðvitaður um öll viðskipti. Í myntbundna líkaninu var myntin meðvituð um öll viðskipti og ákvað hver kom fyrst. Til að ná þessu án trausts aðila verða viðskipti að vera opinberlega tilkynnt [1], og við þurfum kerfi fyrir þátttakendur til að koma sér saman um eina sögu um röð sem þau bárust. Viðtakandi greiðslu þarf sönnun þess að við hverja færslu hafi meirihluti hnúta samþykkt að það væri sú fyrsta móttekin.

3. Tímastimplaþjónn

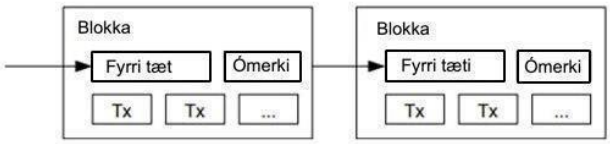
Lausnin sem við leggjum til byrjar á tímastimplaþjóni. Tímastimplaþjónn virkar með því að taka tæti af blokk af hlutum sem á að tímastimpla og birta tæti víða, eins og í dagblaði eða Usenet færslu [2-5]. Tímastimpillinn sannar að gögnin hljóti að hafa verið til á tíma, augljóslega, til að komast inn í tætið. Hver tímastimpill inniheldur fyrri tímastimpil í tæti þess, myndar keðju, þar sem hver viðbótartímastimpill styrkir þá sem á undan eru.



4. Sönnun um vinnu

Til að útfæra dreifðan tímastimpilsþjón á jafningjagrundvelli, þurfum við að nota sönnunarkerfi svipað og Adam Back's Hashcash [6], frekar en dagblaða- eða Usenet-færslur. Sönnunin á vinnu felur í sér að skanna þau gildi sem þegar tætt eru, eins og með SHA-256, byrjar tæti með fjölda núllbita. Meðalvinna sem krafist er er veldisvísis í fjölda af núllbitum sem krafist er og hægt er að sannreyna það með því að keyra eitt tæti.

Fyrir tímastimplakerfið okkar innleiðum við vinnusönnunina með því að hækka ómerkið í blokk þar til gildi finnst sem gefur tæti blokkarinnar nauðsynlega núllbita. Um leið og CPU hefur verið reynt til að láta það fullnægja vinnusönnuninni, er ekki hægt að breyta blokkinni án þess að endurtaka verkið. Af því að síðari blokkir eru hlekkjaðar eftir það, myndi vinna við að breyta blokkinni fela í sér að endurtaka allar blokkir eftir það.



Sönnunin leysir einnig vandamálið við að ákvarða fulltrúa í meirihlutaákvörðun. Ef meirihlutinn væri byggður á einni-IP-tölu-eitt-atkvæði, gæti það verið hnekkt af hverjum sem er fær um að úthluta mörgum IP-tölum. Sönnun á vinnu er í rauninni eitt-CPU-eitt atkvæði. Meirihlutiaákvörðunin er táknuð með lengstu keðjunni, sem hefur mesta vinnusönnunarátakið í því. Ef meirihluta örgjörvaaflsins er stjórnað af heiðarlegum hnútum mun heiðarlega keðjan stækka hraðast og fara fram úr öllum keðjum sem keppa. Til að breyta fyrri blokk þyrfti árásarmaður að endurtaka vinnusönnun á blokkum og öllum blokkum eftir hana og ná síðan upp og fara yfir vinnu heiðarlegra hnúta. Við munum sýna seinna að líkurnar á því að hægari árásarmaður nái sér minnkar gríðarlega þegar síðari blokkum er bætt við.

Til að vega upp á móti auknum vélbúnaðarhraða og mismunandi áhuga á að keyra hnúta með tímanum, ræðst vinnusönnunarerfiðleikinn af hlaupandi meðaltali sem miðar að meðalfjölda blokka á klukkustund. Ef þeir myndast of hratt aukast erfiðleikarnir.

5. Netkerfi

Skrefin til að reka netkerfið eru eftirfarandi:

1) Ný viðskipti eru send til allra hnúta.
2) Hver hnútur safnar nýjum viðskiptum í blokk.
3) Hver hnútur vinnur að því að finna erfiða vinnusönnun fyrir blokkina sína.
4) Þegar hnútur finnur vinnusönnun sendir hann blokkina til allra hnúta.

5) Hnútar samþykkja blokkina aðeins ef öll viðskipti í honum eru gild og ekki þegar eytt.
6) Hnútar tjá samþykki sitt fyrir blokkinni með því að vinna að því að búa til næstu blokk í keðju, með því að nota tæti samþykktu blokkarinnar sem fyrra tæti

Hnútar telja lengstu keðjuna alltaf vera rétta og munu halda áfram að vinna við að framlengja hana. Ef tveir hnútar senda út mismunandi útgáfur af næstu blokk samtímis, geta sumir hnútar fengið einn eða annan fyrst. Í því tilviki vinna þeir á þeim fyrsta sem þeir fengu, en vista hina greinina ef hún verður lengri. Jafntefli verður slitið þegar næsta sönnunarverk finnst og ein greinin lengist; hnútarnir sem voru að vinna á hinni greininni mun þá skipta yfir í lengri.

Nýjar viðskiptaútsendingar þurfa ekki endilega að ná til allra hnúta. Svo lengi sem þeir ná mörgum hnútum, munu þeir komast inn í blokk áður en langt um líður.
Blokkútsendingar þola líka slepptum skilaboðum. Ef hnútur fær ekki blokk mun hann biðja um hana þegar hann fær næstu blokk og áttar sig á því að hann missti af einni.

6. Hvatning

Samkvæmt venju eru fyrstu viðskiptin í blokk sérstök viðskipti sem hefja nýja krónu í eigu af skapara blokkarinnar. Þetta bætir hvata fyrir hnúta til að styðja við netið og veitir leið til að dreifa krónum upphaflega í umferð, þar sem engin miðlæg heimild er til að gefa þær út. Stöðug viðbót við stöðugt magn nýrra króna er hliðstætt því að gullnámumenn eyða auðlindum til að bæta gulli í umferð. Í okkar tilviki er það CPU tíma og rafmagni sem er eytt.

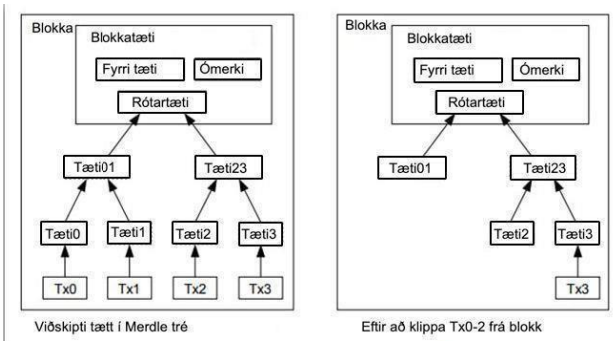
Einnig er hægt að fjármagna hvatann með viðskiptagjöldum. Ef úttaksgildi viðskipta eru minnai en inntaksviði þeirra er mismunurinn viðskiptagjald sem leggst ofan á hvataverðmæti af blokkinni sem inniheldur viðskiptin. Þegar fyrirfram ákveðinn fjöldi króna hefur farið í umferð getur hvatinn færst alfarið yfir í viðskiptagjöld og verið algjörlega verðbólgulaus.

Hvatinn getur hjálpað til við að hvetja hnúta til að vera heiðarlegir. Ef gráðugur árásarmaður getur sett saman meira CPU afl en allir heiðarlegu hnúðarnir, þyrfti hann að velja á milli þess að svíkja fólk með því að stela til baka greiðslu þeirra, eða nota þær til að búa til nýjar krónur. Honum ætti að finnast hagkvæmara að spila eftir reglunum, slíkar reglur sem hygla honum með fleiri nýjum krónum en allir aðrir saman, en að grafa undan kerfinu og gildi eigin auðs.

7. Að endurheimta diskpláss

Þegar nýjasta færslan í krónu er grafin undir nógu mörgum blokkum, máttu eyða viðskiptum áður það er hægt að fleygja þeim til að spara diskpláss. Til að auðvelda þetta án þess að brjóta tæti blokkarinnar, eru færslur tættar í

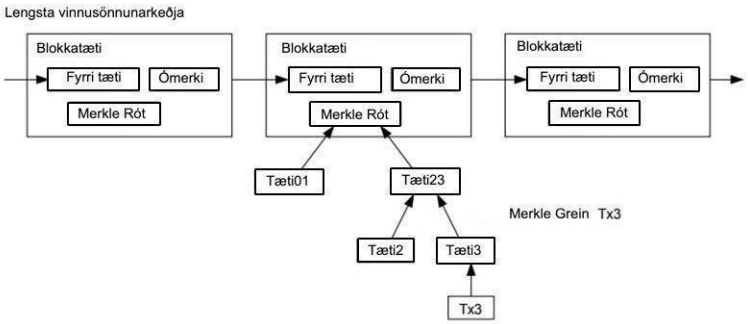
Merkle Tree [7][2][5], þar sem aðeins rótin er innifalin í tæti blokkarinnar. Þá er hægt að þjappa gömlum blokkunum með því að stinga af greinum trésins. Innri tæti þarf ekki að geyma.



Blokkhaus án viðskipta væri um 80 bæti. Ef við gerum ráð fyrir að blokkir séu að myndast á 10 mínútna fresti, 80 bæti * 6 * 24 * 365 = 4,2MB á ári. Með tölvukerfum sem seljast venjulega með 2GB af vinnsluminni frá og með 2008, og lögmál Moore spáir núverandi vexti um 1,2GB á ári, ætti geymsla ekki að vera vandamál jafnvel þó að geyma þurfi blokkhausana inni minni.

8. Einföld greiðslustaðfesting

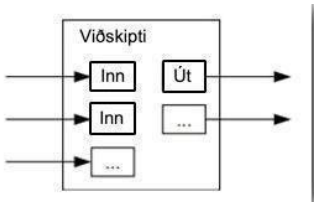
Það er hægt að staðfesta greiðslur án þess að keyra fullan nethnút. Notandi þarf aðeins að halda afriti af blokkhausum lengstu vinnusönnunarkeðjunnar, sem hann getur fengið með því að spyrjast fyrir um nethnúta þar til hann er sannfærður um að hann sé með lengstu keðjuna og fengið Merkle útibúið til að tengja færsluna við blokkina sem hún er tímastimpluð í. Hann getur ekki athugað færsluna sjálfur, en með því að tengja hana við stað í keðjunni getur hann séð að nethnútur hefur samþykkt hana, og blokkum bætt við eftir að það staðfestir enn frekar að netið hafi samþykkt það.



Sem slík er sannprófunin áreiðanleg svo lengi sem heiðarlegir hnútar stjórna netinu, en er meira viðkvæmt ef netið er yfirbugað af árásarmanni. Þó nethnútar geti staðfest viðskipti fyrir sig, getur einfaldaða aðferðin látið blekkjast af fölsuðum viðskiptum árásarmanns eins lengi og árásarmaðurinn getur haldið áfram að yfirbuga netið. Ein stefna til að verndast gegn þessu væri að samþykkja viðvaranir frá nethnútum þegar þeir uppgötva ógilda blokk, sem hvetur hugbúnað notandans til að hlaða niður fullri blokk og viðvörun um viðskipti til staðfesta ósamræmið. Fyrirtæki sem fá tíðar greiðslur munu líklega enn vilja keyra sína eigin hnúta fyrir sjálfstæðara öryggi og skjótari sannprófun.

9. Sameina og skipta virði

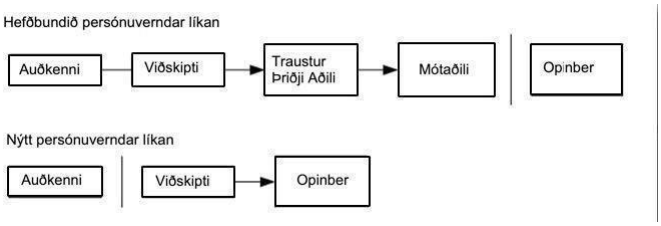
Þótt hægt væri að meðhöndla krónur hverja fyrir sig, væri ómeðfærilegt að gera sér viðskipti fyrir hvert sent í millifærslu. Til að leyfa verðmætum að vera skipt og sameinuð, innihalda viðskipti mörg inntök og úttök. Venjulega verður annað hvort eitt inntak frá stærri fyrri færslu eða mörgum aðföngum sem sameina smærri upphæðir, og í mesta lagi tvö úttök: eitt fyrir greiðsluna og eitt sem skilar breytingunni, ef einhver er, aftur til sendanda.



Það skal tekið fram að fan-out, þar sem viðskipti eru háð nokkrum viðskiptum, og þau viðskipti eru háð miklu fleirum, er ekki vandamál hér. Það er aldrei þörf á að draga út fullkomið sjálfstætt afrit af viðskiptasögu.

10. Friðhelgi

Hefðbundið bankalíkan nær friðhelgi einkalífs með því að takmarka aðgang að upplýsingum til hlutaðeigandi aðilum og traustum þriðja aðila. Nauðsyn þess að tilkynna öll viðskipti opinberlega útilokar þessa aðferð, en samt er hægt að viðhalda friðhelgi einkalífsins með því að brjóta inn flæði upplýsinga annar staðar: með því að halda opinberum lyklum nafnlausum. Almenningur getur séð að einhver er að senda upphæð til einhvers annars, en án þess að upplýsingar tengi viðskiptin við nokkurn mann. Þetta er svipað magn upplýsinga sem birtar eru af kauphöllum, þar sem tími og stærð einstaka viðskipta, "bandið", er gert opinbert, en án þess að upplýst sé hverjir aðilarnir voru.



Sem viðbótareldveggur ætti að nota nýtt lyklapar fyrir hverja færslu til að halda þeim frá því að vera tengdar sameiginlegum eiganda. Sum tenging er enn óhjákvæmileg með fjölinntak viðskipti, sem leiða endilega í ljós að aðföng þeirra voru í eigu sama eiganda. Áhættan er að ef eigandi lykils kemur í ljós gæti tenging leitt í ljós önnur viðskipti sem tilheyra sama eiganda.

11. Reikningar

Við lítum á atburðarásina þar sem árásarmaður reynir að búa til varakeðju hraðar en heiðarleg keðja. Jafnvel þó að þessu sé náð, opnar það kerfið ekki fyrir handahófskenndar breytingar, svo sem eins og að skapa verðmæti

upp úr þurru eða taka peninga sem aldrei tilheyrðu árásarmanninum. Hnútar samþykkja ekki ógilda færslu sem greiðslu og heiðarlegir hnútar munu aldrei samþykkja blokk sem inniheldur þær. Árásarmaður getur aðeins reynt að breyta einum af sínum eigin viðskiptum til að taka til baka fé sem hann eyddi nýlega.

Hægt er að lýsa kapphlaupinu milli heiðarlegrar keðju og árásarkeðju sem tvímælis Random Walk. Árangursviðburðurinn er heiðarleg keðja sem er stækkuð um eina blokk og eykur forystu hennar um +1, og bilunartilvikið er að keðja árásarmannsins er framlengd um eina blokk, sem dregur bilið úr um -1.

Líkurnar á því að árásarmaður nái sér upp úr tilteknum halla eru hliðstæðar fjárhættuspilara. Segjum sem svo að fjárhættuspilari með ótakmarkaða inneign byrji með halla og spili hugsanlega óendanlega margar tilraunir til að reyna að ná jafnvægi. Við getum reiknað út líkurnar á að hann nær jöfnunarmarki, eða að árásarmaður nái alltaf heiðarlegu keðjunni, sem hér segir [8]:

p = líkur á að heiðarlegur hnútur finni næstu blokk

q = líkur á að árásarmaðurinn finni næstu blokk

qz = líkur á að árásarmaðurinn nái nokkurn tíma upp úr z blokkum á eftir

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Miðað við forsendur okkar að p > q, lækka líkur veldisvísis eftir því sem fjöldi blokka sem árásarmaður þarf að ná hækkar. Með líkurnar á móti sér, ef hann er ekki heppinn, verða möguleikar hans hverfandi litlir eftir því sem hann fellur lengra.

Við skoðum nú hversu lengi viðtakandi nýrrar færslu þarf að bíða áður en hann verður nægilega viss um að sendandinn geti ekki breytt viðskiptunum. Við gerum ráð fyrir að sendandinn sé árásarmaður sem vill láta viðtakandann trúa því að hann hafi greitt honum fyrir nokkurri stund, skipta síðan yfir í að borga til baka sjálfur eftir að nokkur tími er liðinn. Viðtakandinn verður látinn vita þegar það gerist, en sendandi vonar að það verði of seint.

Viðtakandinn býr til nýtt lyklapar og gefur sendanda almenningslykilinn skömmu fyrir undirskrift. Þetta kemur í veg fyrir að sendandinn geti útbúið keðju af blokkum fyrirfram með því að vinna í því stöðugt þar til hann er svo heppinn að komast nógu langt á undan, og þá framkvæma viðskiptin á því augnabliki. Þegar viðskiptin hafa verið send byrjar óheiðarlegur sendandi að vinna í laumi á samhliða keðju sem inniheldur aðra útgáfu af viðskiptum hans.

Viðtakandinn bíður þar til færslunni hefur verið bætt við blokk og z blokkir hafa verið tengdar á eftir henni. Hann veit ekki nákvæmlega hversu miklum framförum árásarmaðurinn hefur náð, en að því gefnu að heiðarlegar blokkir tækju meðaltalstíma á hverja blokk, verða möguleikar framfarir árásarmannsins Poisson dreifing með væntanlegu gildi:

$$\lambda = z\frac{q}{p}$$

Til að fá líkurnar á að árásarmaðurinn gæti enn náð upp núna, margföldum við Poisson þéttleikann fyrir hvert magn af framförum sem hann hefði getað náð með líkunum sem hann gæti náð frá þeim tímapunkti:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Endurraða til að forðast að leggja saman óendanlega hala dreifingarinnar...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Umbreytir í C kóða...

```
# Innihalda   <math.h>
              Tvöfaldar líkur á velgengni árása   (Tvöfalda q, int z)
{
    Tvöfalda p    = 1.0 - q;
    Tvöfalda lamda      = z * (q / p);
    Tvöfalda summu = 1.0;
     int i, k ;
    Fyrir  (k = 0; k <= z; k++)
    {
         Tvöfalda Poisson      = exp(-lambda);
         Fyrir (i = 1; i <= k; i++)
             poisson *= lambda / i;
         sum -= poisson * (1 - pow(q / p, z - k));
    }
      Skila summu ;
}
```

Með því að keyra nokkrar niðurstöður getum við séð líkurnar lækka veldisvísis með z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Að leysa fyrir P minna en 0,1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Lokaorð

Við höfum lagt til kerfi fyrir rafræn viðskipti án þess að treysta á traust. Við byrjuðum með venjulegum ramma króna gerðar úr stafrænum undirskriftum, sem veitir sterka stjórn á eignarhald, en er ófullkomið án þess að hægt sé að koma í veg fyrir tvöfalda eyðslu. Til að leysa þetta, stungum við upp á jafningjaneti með því að nota vinnusönnun til að skrá opinbera sögu viðskipta sem verða fljótt reikningslega óframkvæmanlegt fyrir árásarmann að breyta ef heiðarlegir hnútar stjórna meirihluta CPU orku. Netið er öflugt í óskipulögðum einfaldleika sínum. Hnútar vinna allt í einu með lítilli samhæfingu. Þeir þurfa ekki að vera auðkenndir, þar sem skilaboð fara ekki beint á neinn sérstakan stað og þarf aðeins að afhenda þau eftir bestu getu. Hnútar geta yfirgefið og gengið aftur í netið að vild og samþykkja vinnusönnunarkeðjuna sem sönnun um hvað gerðist á meðan þeir voru í burtu. Þeir greiða atkvæði með örgjörvaafli sínu og lýsa samþykki sínu við gildar blokkir með því að vinna að framlengingu þeirra og hafna ógildum blokkum með því að neita að vinna á þeim. Hægt er að framfylgja öllum nauðsynlegum reglum og ívilnunum með þessu samstöðukerfi.

Heimildir

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.