Bitcoin: Tsarin Kuɗi na Laturoni na Tsara-da-tsara

daga Satoshi Nakamoto 2008/10/31

Tsokaci

Sigar tsara-da-tsara na tsabar kuɗi na laturoni zai ba da damar aika biyan kuɗi ta kan layi kai tsaye daga wannan ƙungiya zuwa wata ba tare da shiga cikin cibiyar kuɗi ba. Sa hannu na dijital yana bayar da wani ɓangare na mafita, amma muhimman fa'idoji sun ɓace idan har yanzu ana buƙatar wani amintaccen ɓangare na uku don hana kashe kuɗi sau biyu. Muna ba da shawarar mafita ga matsalar kashe kuɗi sau biyu ta hanyar amfani da sadarwa ta tsara-zuwa- tsara. Ƙididdiga na lokaci na hanyar sadarwa yana ɗaukar mu'amaloli ta hanyar sanya su cikin jerin abubuwan da ke ci gaba da tabbatar da aikin tsani, suna yin rikodin da ba za a iya canja shi ba tare da sake tabbatar da aikin ba. Sarƙar mafi tsayi ba wai kawai ta zama hujja na jerin abubuwan da aka shaida ba, amma tabbacin cewa ya fito ne daga mafi girman tafkin ƙarfin CPU. Matuƙar ana sarrafa yawancin ƙarfin CPU ta cibiya waɗanda ba sa haɗin kai don kai hari kan hanyar sadarwar, za su haifar da mafi tsayin sarƙa da wuce gona da iri ga mahara. Cibiyar sadarwar kanta tana buƙatar tsari kaɗan. Ana watsa saƙon akan ƙoƙari mafi kyawu, kuma cibiyar yana iya barin su su koma hanyar sadarwar yadda ake so, suna karɓar sarƙar hujjar-aiki mafi tsayi a matsayin tabbacin abun da ya faru yayin da ba sa nan.

Gabatarwa

Ciniki a kan intanet ya zo ya dogara kusan na keɓance ga cibiyoyin kuɗi waɗanda ke aiki a matsayin wata amintacciyar ƙungiya don aiwatar da biyan kuɗi na laturoni. Duk da yake tsarin yana aiki da kyau ga yawancin mu’amaloli, har yanzu yana fama da rauni na asali na ƙirar dogara. Cikakkun mu’amalar da ba za’a iya juyarwa ba ba za ta yiwu ba, tunda cibiyoyin kuɗi ba za su iya gujewa sasanta jayayya ba. Farashin sasanci yana ƙara farashin mu’amala, yana iyakance mafi ƙarancin ƙimar mu’amala mai amfani da yanke yiwuwar ƙananan mu'amaloli na yau da kullum, kuma akwai babban farashi a cikin asarar ikon yin biyan kuɗin da ba za’a iya juyarwa ba don ayyukan da ba za’a iya juyarwa ba. Tare da yiwuwar juyawa, buƙatar amana ta bazu. Dole ne 'yan kasuwa su yi hattara da abokan cinikayyar su, suna ɓata musu rai don ƙarin bayani fiye da yadda za su buƙata. An karɓi wani kaso na zamba a matsayin wanda ba za’a iya gujewa ba. Ana iya gujewa waɗannan farashin da rashin tabbas na biyan kuɗi ta hanyar amfani da kuɗin zahiri, amma babu wata hanyar biyan kuɗi ta hanyar sadarwa ba tare da amintacciyar ƙungiya ba.

Abun da ake buƙata shine tsarin biyan kuɗi na laturoni wanda ya dogara da bayanan sirri maimakon amana, wanda ke ba da damar kowane bangare biyu masu son yin mu'amala da juna

kai tsaye ba tare da buƙatar wani amintaccen ɓangare na uku ba. Juyar da mu'amalolin da ba su da inganci domin kare masu siya daga zamba, kuma ana iya aiwatar da hanyoyin ƙetare na yau da kullun don kare masu siya. A cikin wannan takarda, muna ba da shawarar mafita ga matsalar kashe kuɗi sau biyu ta amfani da sabar tambarin lokaci da aka raba tsakanin ɗan-tsari don samar da shaidar ƙididdiga na tsarin mu'amaloli na lokaci-lokaci a tsakanin tsara-da-tsara. Tsarin yana da aminci idan dai cibiyar na gaskiya suna tare kan sarrafa ƙarin ƙarfin CPU fiye da kowane rukunin haɗin gwiwar cibiyar na mahari.

Mu'amaloli

Muna bayyana kuɗin laturoni azaman sarƙar sa hannun dijital. Kowane mai shi yana canja wurin tsabar kuɗin zuwa na gaba ta hanyar sanya hannu kan tsani na cinikin da ya gabata da maɓallin jama'a na mai mallaka gaba da ƙara waɗannan zuwa ƙarshen tsabar kuɗin. Mai karɓar kuɗi zai iya tabbatar da sa hannun don tabbatar da sarƙar mallaka.

Matsalar ita ce mai karɓar kuɗi ba zai iya tabbatar da cewa ɗaya daga cikin masu mallakar kuɗi bai kashe tsabar kuɗi sau biyu ba. Magani na gama gari shine gabatar da ahukumar buga kuɗi na tsabaacciyar hukuma ta tsakiya, ko hukumar buga kuɗi na tsaba, wacce ke bincikar kowace mu'amala don kashewa sau biyu. Bayan kowace mu'amala, tsabar kuɗin dole ne a mayar da shi zuwa ga hukumar buga kuɗi na tsaba don fitar da sabon tsabar kuɗi, kuma tsabar kuɗi da aka bayar kai tsaye daga hukumar buga kuɗi na tsaba kawai aka amince cewa ba za’a kashe su sau biyu ba. Matsalar wannan mafita ita ce, makomar tsarin kuɗin gaba ɗaya ya dogara ne akan kamfanin da ke tafiyar da hukumar buga kuɗi na tsaba, tare da kowane ciniki sai yabi ta wajen su, kamar banki.

Muna buƙatar hanya don mai karɓar kuɗi ya san cewa masu mallakar da suka gabata ba su sanya hannu kan wata mu'amala ta farko ba. Domin dalilanmu, cinikin da ya gabata shine wanda yake da ƙima, don haka ba mu damu da yunƙurin kashewa sau biyu ba. Hanya guda don tabbatar da rashin ciniki shine sanin duk mu'amaloli. A cikin tsarin hukumar buga kuɗi na tsaba, ya san duk mu'amaloli kuma ya yanke shawarar wanda ya fara zuwa. Don cim ma wannan ba tare da kungiyar da aka gasgata ba, dole ne a sanar da mu'amaloli a bainar jama'a[1], kuma muna buƙatar tsarin don mahalarta su amince da tarihi guda ɗaya na tsarin da aka karɓa. Mai karɓar kuɗi yana buƙatar tabbacin cewa a lokacin kowane ciniki, yawancin cibiyoyin sun yarda cewa shine na farko da aka karɓa.

Sabar Tambarin Lokaci

Mafitar da muke ba da shawara tana farawa da sabar tambarin lokaci. Sabar tambarin lokaci tana aiki ta ɗaukar tsani na tubalin abubuwan da za’a yiwa tambarin lokaci da bayyana buga tsani, kamar a cikin jarida ko adireshin Usenet[2-5]. Tambarin lokaci yana tabbatar da cewa dole ne bayanan sun tabbata a lokacin, a fili, don shiga cikin tsani. Kowane tambarin lokaci ya haɗe da

tambarin lokaci da ya gabata a cikin tsaninsa, yana yin sarka, tare da kowane ƙarin tambarin lokaci yana ƙarfafa wanda suka gabace shi.

Tabbacin Aiki

Don aiwatar da sabar tambarin lokaci da aka rarraba akan tsarin tsara-zuwa-tsara, za mu buƙaci yin amfani da tsarin hujja-na-aiki mai kama da Adam Back's Hashcash[6], maimakon jaridu ko adireshin Usenet. Tabbacin-aiki ya ƙunshi dubawa don ƙimar da lokacin tsani, kamar tare da SHA-256, tsani yana farawa da adadi na sifili. Matsakaicin aikin da ake buƙata yana da ƙima a cikin adadin sifili da ake buƙata kuma ana iya tabbatarwa ta hanyar aiwatar da tsani ɗaya.

Don cibiyar sadarwar mu ta tambarin lokaci, muna aiwatar da hujja-na-aiki ta hanyar ƙara ƙima a cikin tubali har sai an sami ƙimar da ke bawa tsani ƙimar da ake buƙata. Da zarar an ƙaddamar da bunƙasa ƙoƙarin CPU don ya gamsar da hujja-na-aiki, ba za’a iya canja tubali ba tare da sake yin aikin ba. Kamar yadda daga baya aka ɗaure tubalan bayansa, aikin canja tubali zai haɗa da sake yin duk tubalan bayansa.

Hujja-na-aiki kuma yana magance matsalar ƙayyadaddun wakilci a cikin yanke shawara mafi yawa. Idan mafi rinjaye sun dogara ne akan ɗaya-IP-adireshi-ɗaya-zaɓi, duk wanda zai iya rarraba IPs da yawa zai iya jujjuya shi. Hujja-na-aiki shine ainihin ɗaya-CPU-ɗaya-zaɓi. Mafi yawan yanke shawara ana wakilta ta mafi tsayin sarƙa, wanda yake da mafi girman ƙoƙarin hujja-na-aiki da aka saka a ciki. Idan yawancin ƙarfin CPU ana sarrafa su ta hanyar cibiya na gaskiya, sarƙar gaskiya za ta yi girma cikin sauri kuma ta zarce kowane sarƙoƙi masu fafatawa. Don gyara tubalan da suka gabata, mai hari dole ne ya sake tabbatar da hujja-na-aiki ga tubulin da duk tubalan bayan sa sannan ya tarar har ya zarce aikin cibiya na gaskiya. Za mu nuna daga baya cewa yiwuwar mai kai hari a hankali yana tararwa yana raguwa sosai yayin da aka ƙara tubalan na gaba.

Domin daidaito da haɓaka saurin kayan masarufi da ra'ayoyi daban-daban don gudanar da cibiya akan lokaci, wahalar hujja-na-aiki yana ƙayyade matsakaita masu motsi wanda ke niyyar samun matsakaicin adadin tubalan a cikin awa ɗaya. Idan an ƙirƙire su da sauri, wahalar tana ƙaruwa.

Hanyar sadarwa

Matakan tafiyar da hanyar sadarwar sune kamar haka:

1. Sababbin mu'amaloli ana watsa su zuwa duk cibiyoyi.
2. Kowace cibiya tana karbar sababbin mu’amaloli a cikin tubali.
3. Kowace cibiya tana aiki akan nemo hujja-na-aiki mai wahala don tubalinta.
4. Lokacin da cibiya ta sami hujja-na-aiki, tana watsa tubalin zuwa duk cibiyoyi.

5. Cibiyoyi suna karɓar tubalin kawai idan duk mu’amaloli a cikinsa suna da inganci kuma ba a riga an kashe su ba.
6. Cibiyoyi suna bayyana yarda da tubalin ta hanyar yin aiki don ƙirƙirar tubali na gaba a cikin sarƙar, ta yin amfani da tsani na tubalin da aka karɓa kamar tsanin da ya gabata.

Cibiyoyi ko da yaushe suna la'akari da mafi tsayin sarƙa ta zama mafi inganci kuma za su ci gaba da yin aiki akan tsawaita ta. Idan cibiyoyi biyu suna watsa samfuri daban-daban na tubalin da zai gabata a lokaci guda, wasu cibiyoyin na iya karɓar ɗaya ko ɗayan farko. A wannan yanayin, suna aiki a kan na farko da suka karɓa, amma suna ajiye wani reshe idan ya yi tsayi. Za’a karya ƙullin lokacin da aka sami hujja-na-aiki na gaba kuma reshe ɗaya ya daɗe; cibiyoyin da ke aiki a ɗaya reshe za su canja zuwa wanda ya fi tsayi.

Sababbin watsa shirye-shiryen mu’amaloli baya buƙatar zuwa ga duk cibiyoyi. Muddin sun kai zuwa ga cibiyoyi da yawa, za su shiga cikin tubali ba da daɗewa ba. Tubalan watsa shirye- shirye kuma suna da jurewa sauke saƙonni. Idan cibiya bata karɓi tubali ba, zata buƙace shi lokacin da ta karɓi tubali na gaba kuma za ta gane ta rasa ɗaya.

Tukwuici

Ta hanyar al'ada, mu'amala ta farko a cikin tubali ita ce mu'amala ta musamman wacce ke fara sabon tsabar kuɗi mallakar wanda ya ƙirƙiri tubalin. Wannan yana ƙara ƙwarin gwiwa ga cibiyoyi don tallafawa hanyar sadarwa, kuma yana ba da hanyar da za’a fara rarraba tsabar kuɗi zuwa wurare daban-daban, tunda babu wata babbar hukuma dake bayar da su. Ci gaba da gyare-gyaren adadin sababbin tsabar kuɗi daidai yake da masu haƙar zinare da ke kashe albarkatu don ƙara yawan zinaren da yake yawo. A wajenmu, lokaci ne na CPU da wutar laturoni da ake kashewa.

Hakanan za'a iya samar da tukwuici ta hanyar kuɗin ciniki. Idan ƙimar fitarwar mu’amala tayi ƙasa da ƙimar shigarwarsa, bambancin shine kuɗin mu’amala wanda aka ƙara zuwa ga ƙimar tukwuici na tubalin mai ɗauke da mu’amala. Da zarar an ƙididdige adadin tsabar kuɗi sun shiga wurare daban-daban, abun tukwuicin zai iya canjawa gaba ɗaya zuwa kuɗin mu’amala kuma ya zama gaba ɗaya babu hauhawar farashi.

Tukwuici na iya taimakawa wajen bada ƙwarin gwiwa ga cibiyoyi don tsayawa akan gaskiya. Idan maharin mai haɗama zai iya tara ƙarin ƙarfin CPU fiye da duk cibiyoyin gaskiya, dole ne ya zaɓi tsakanin amfani da shi don damfarar mutane ta hanyar satar kuɗinsa, ko amfani da su don samar da sababbin tsabar kuɗi. Ya kamata ya ga cewa yafi riba yabi dukkan ƙa’idoji, irin waɗannan ƙa’idojin waɗanda ke fifita shi da sababbin tsabar kuɗi fiye da kowa idan aka haɗa, fiye da raunana tsarin da kuma lalata ingancin dukiyarsa.

Maido da Sararin Faifai

Da zarar an binne sabuwar mu’amalar tsabar kuɗi a ƙarƙashin isassun tubalan, mu’amalar da aka

kashe kafin wannan za’a iya jefar da ita don adana sararin faifai. Don sauƙaƙe wannan ba tare da karya tsanin tubalin ba, ana sanya tsanin mu’amala a cikin Bishiyar Merkle [7] [2] [5], tare da tushen kawai an haɗa shi a cikin tsanin tubalin. Ana iya haɗa tsofaffin tubalan ta hanyar soke rassan bishiyar. Tsanuka na ciki basa buƙatar adanawa.

Kan tubalin ba tare da ciniki ba zai zama kusan bytes 80. Idan muka ɗauka ana samar da tubalan duk bayan minti 10, 80 bytes * 6 * 24 * 365 = 4.2MB a kowace shekara. Tare da tsarin kwamfuta yawanci ana siyar da 2GB na RAM kamar a 2008, kuma Dokar Moore tana hasashen haɓaka 1.2GB a halin yanzu a kowace shekara, bai kamata ajiya ta zama matsala ba koda kuwa ya zama dole a adana kan tubalan a cikin ƙwaƙwalwar ajiya.

Sauƙaƙaken Tabbacin Biyan Kuɗi

Yana yiwuwa a tabbatar da biyan kuɗi ba tare da gudanar da cikakken ƙullin hanyar sadarwa ba. Mai amfani kawai yana buƙatar adana kwafin kan tubalin na sarƙa mafi tsayi ta hujja-na-aiki, wanda zai iya samu ta hanyar tambayar cibiyoyin sadarwa har sai ya tabbata yana da mafi tsayin sarƙar, kuma ya sami reshen Merkle da ke haɗa mu’amala zuwa tubalin da aka yiwa tambarin lokaci a ciki. Ba zai iya bincika mu’amalar da kansa ba, amma ta hanyar haɗa shi zuwa wani wuri a cikin sarƙar, zai iya ganin cewa cibiyar hanyar sadarwa ya karbe shi, kuma an ƙara tubalan bayan ya ƙara tabbatar da hanyar sadarwar ta karɓe shi.

ADon haka, tabbacin abun dogaro ne muddin cibiyoyin gaskiya suna sarrafa hanyar sadarwar, amma ya fi rauni idan maharin ya rinjayi hanyar sadarwar. Yayin da cibiyoyin sadarwa na iya tabbatar da mu’amaloli da kansu, hanyar da aka sauƙaƙa maharin zai iya yaudareta ta hanyar ƙirƙira mu’amaloli na karan kansa muddin maharin na iya ci gaba da mamaye hanyar sadarwar. Dabara ɗaya don kare wannan ita ce karɓar faɗakarwa daga cibiyoyi na cibiyar sadarwa lokacin da suka gano tubali mara inganci, wanda yasa software mai amfani zazzage cikakken tubalin da faɗakar da mu’amaloli don tabbatar da rashin daidaituwa. Kasuwancin da ke karɓar biyan kuɗi akai-akai wataƙila har yanzu suna son gudanar da nasu cibiyoyin don ƙarin tsaro mai zaman kansa da saurin tabbatarwa.

Haɗawa da Rarrabe Ƙima

Ko da yake yana yiwuwa kowane mutum ɗaya ya sarrafa tsabar kuɗi, ba zai zama da wahala a yi mu’amala daban ga kowane cent a cikin canja wuri ba. Don ba da izinin raba ƙima da haɗin kai, mu’amaloli sun ƙunshi abubuwa da yawa na shigarwa da fitarwa. A al'ada za’a sami ko dai shigarwa guda ɗaya daga cikin mu’amalar da ta gabata mafi girma ko kuma shigarwa da yawa waɗanda ke haɗa ƙananan adadi, kuma aƙalla nau'i biyu na fitarwa: ɗaya don biyan kuɗi, ɗaya kuma mai mayar da canji, idan akwai, komawa ga mai aikowa.

Ya kamata a lura cewa fanka-waje, inda ciniki ya dogara da mu’amaloli da yawa, kuma waɗannan mu’amaloli sun dogara da yawa, ba matsala a nan. Ba za’a taɓa buƙatar cire cikakken kwafin tarihin mu’amala ba.

Keɓanta Sirri

Tsarin banki na gargajiya yana samun matakin sirri ta hanyar iyakance damar samun bayanai ga ɓangarorin da abun ya shafa da amintaccen bangare na uku. Wajabcin sanar da duk mu’amaloli a bainar jama'a yana hana wannan hanyar, amma har yanzu ana iya kiyaye sirri ta hanyar karya kwararar bayanai a wani wuri: ta hanyar ɓoye maɓallan jama'a ba tare da an san su ba. Jama'a na iya ganin cewa wani yana aika adadi zuwa wani, amma ba tare da bayanin da ke haɗa ciniki da kowa ba. Wannan ya yi kama da matakin bayanan da aka fitar ta hanyar musayar hannayen jari, inda ake bayyana lokaci da girman kasuwancin mutum, "kaset" ɗin ana futo dashi bainar jama’a, amma ba tare da bayyana su wanene bangarorin ba.

A matsayin ƙarin tacewar zaɓi, ya kamata a yi amfani da sabon maɓalli guda biyu don kowace mu’amala don kiyaye su daga haɗa su da gama garin mai shi. Wasu haɗin kan har yanzu ba zai yiwu ba tare da mu’amalar shigarwa da yawa ba, wanda dole ne ya bayyana cewa shigarwar da suka samu na mai su ɗaya ne. Haɗarin shine idan an bayyana mai maɓalli, haɗawa zai iya bayyana wasu mu’amaloli waɗanda na mai shi ɗaya ne.

Lissafi

Mun yi la'akari da yanayin maharin da ke ƙoƙarin samar da wata sarƙa ta dabam cikin sauri fiye da sarƙar gaskiya. Ko da an cim ma hakan, ba zai jefa tsarin a buɗe ga sauye-sauye na son rai ba, kamar ƙirƙirar ƙima daga siririyar iska ko ɗaukar kuɗin da ba na maharin ba. Cibiyoyi ba za su karɓi mu’amala mara inganci a matsayin biyan kuɗi ba, kuma cibiyoyi na gaskiya ba za su taɓa karɓar tubalin mai ɗauke da su ba. Mai hari zai iya ƙoƙarin canja ɗaya daga cikin tasa mu'amalar don ɗaukar kuɗin da ya kashe kwanan nan.

Za a iya siffanta tseren dake tsakanin sarƙar gaskiya da sarƙar mahari a matsayin Binomial Random Walk. Lamarin nasara shine sarƙar gaskiya da aka tsawaita ta ɗaya tubalin, yana ƙara jagorancinsa da +1, kuma abun da ya faru na rashin nasara shine ƙara sarƙar maharin ta hanyar tubali ɗaya, yana rage tazarar da -1.

Yiwuwar mahari ya kama daga gibin da aka bayar yayi daidai da Matsalar Rushewar Dan caca. Tsammanin dan wasan da ke da bashi mara iyaka ya fara kuma ya yi gwaji mara iyaka don ƙoƙarin kaiwa ga karya. Za mu iya ƙididdige yiwuwar da ya taɓa kai wa ga ƙarya, ko kuma cewa maharin ya taɓa samun sarƙar gaskiya, kamar haka[8]:

p = yiwuwar cibiyar gaskiya ya sami na gaba tubali
q = yiwuwar maharin ya sami na gaba tubali
q_z = yiwuwar maharin zai iya riske shi daga tubalin z z baya

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

Idan muka yi la'akari da cewa $p > q$, yiwuwar ta ragu sosai yayin da adadin tubalan da maharin yake so ya cim ma suka ƙaru. Tare da rashin daidaituwa a kansa, idan bai yi sa'a a gaba da wuri ba, damarsa ta zama kadan yayin da ya kara faduwa a baya.

Yanzu muna la'akari da tsawon lokacin da mai karɓar sabuwar mu'amala ke buƙatan jira kafin ya ishe shi ya tabbatar mai aikawa ba zai iya canja mu'amala ba. Muna ɗauka cewa mai aikawa mahari ne wanda yake so ya sa wanda aka karɓa ya yarda cewa ya riga ya biya shi a ɗan tsawon lokaci, sannan ya canja shi don mayar wa kansa bayan wani lokaci ya wuce. Za'a faɗakar da mai karɓa lokacin da hakan ya faru, amma mai aikawa yana fatan zai yi latti.

Mai karɓa yana samar da sabon maɓalli biyu kuma yana ba da maɓallin jama'a ga mai aikawa jim kaɗan kafin sa hannu. Wannan yana hana mai aikawa shirya jerin tubalan kafin lokaci ta hanyar yin aiki akansa akai-akai har sai ya yi sa'a ya yi nisa sosai, sannan aiwatar da mu'amala a lokacin. Da zarar an aika da mu'amala, mai aikawa mara gaskiya zai fara aiki a asirce akan sarƙar layi ɗaya mai dauke da wani nau'i na mu'amalarsa.

Mai karɓa yana jira har sai an ƙara mu'amala zuwa tubalin kuma an haɗa tubalin z a bayansa. Bai san ainihin adadin ci gaban da maharin ya samu ba, amma zai ɗauka cewa tubalan masu gaskiya sun ɗauki matsakaicin lokacin da ake tsammanin kowane tubalin ya dauka akan kowane tubali ɗaya, yiwuwar ci gaban maharin zai zama rarraba Poisson tare da ƙimar da ake sa rai:

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

Don samun yiwuwar wanda maharin zai iya kamawa a yanzu, muna ninka yawan Poisson ga kowane adadin ci gaban da zai iya samu ta hanyar yiwuwar da zai iya kamawa daga wannan lokacin:

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

Sake tsarawa don guje wa taƙaita wutsiya mara iyaka na rarrabawa…

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

Juyawa zuwa C code…

```
#include
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Tafiyar da wasu sakamako, za mu iya ganin yiwuwar ta ragu sosai tare da 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
```

Sarrafa P kasa da 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
```

Kammalawa

Mun ba da shawarar tsarin mu’amalar laturoni ba tare da dogaro da amana ba. Mun fara da tsarin yau da kullum na tsabar kuɗi da aka yi daga sa hannu na dijital, wanda ke ba da iko mai ƙarfi na ikon mallaki, amma bai cika ba ba tare da hanyar hana ƙashe kuɗi biyu ba. Don magance wannan, mun ba da shawarar hanyar sadarwar tsara-da-tsara ta hanyar amfani da hujja-na-aiki don nadar bayanan tarihin mu’amala na jama'a wanda da sauri ya zama ba zai yiwu ba ga mai hari ya canja idan cibiyoyi na gaskiya suna sarrafa yawancin ƙarfin CPU. Cibiyar sadarwa tana da ƙarfi a cikin sauƙi mara tsari. Cibiyoyi suna aiki gaba ɗaya tare da daidaitawa kaɗan. Ba sa buƙatar a gano su, tunda ba a tura saƙon zuwa wani wuri na musamman kuma kawai ana buƙatar isar da su ne bisa kyakkyawan ƙoƙari. Cibiyoyi na iya tafiya kuma su sake shiga hanyar sadarwar yadda ake so, suna karɓar sarƙar hujja-na-aiki azaman hujja na abun da ya faru yayin da suka tafi. Suna zaba da ƙarfin CPU ɗin su, suna bayyana yarda da ingantattun tubalan ta hanyar yin aiki kan tsawaita su da ƙin tubalan da ba su da inganci ta hanyar ƙin yin aiki a kansu. Ana iya aiwatar da duk wasu ƙa’idoji da abubuwan ƙarfafawa tare da wannan hanyar haɗin gwiwa.

References

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.