Bitcoin: Habka Lacagta Kaashka Ah Ee Peer-Ka

waxaa qoray Satoshi Nakamoto 2008/10/31

Abstrees

Nooca is-af-abuurka ah ee kaashka ah ee kaashka elektiroonigga ah ayaa u oggolaanaya lacagaha internetka in si toos ah loogu diro qaybo ka mid ah dhinac kale iyada oo aan la marin hay'ad maaliyadeed. Saxiixyada Dijital ah waxay bixiyaan qayb ka mid ah xalka, laakiin faa'iidooyinka ugu weyn ayaa lumaya haddii dhinac saddexaad oo aamin ah uu wali looga baahan yahay inuu ka hortago laba-laab. Waxaan soo jeedineynaa xalka dhibaatada laba- saamayntu ku badan tahay annagoo adeegsanayna shabakad aasooga ah. Shabakadda Waqtiga Toodestamps Macaamilka ayaa ku kacaya silsilad socda oo ah silsilad socda oo ah oo ah shaqo-ku-ool-shaqo, sameynta diiwaan aan la beddeli karin iyada oo aan dib loo soo celin caddaynta-shaqa-la'aanta. Silsiladda ugu dheer ma aha oo keliya caddeyn muujineysa isku xigxiga dhacdooyinka marqaati ah, laakiin caddeeyay inay ka timid barkadda ugu weyn ee awoodda CPU. Ilaa inta badan awooda Awoodda CPU ay ka taliso noodes oo aan iskaashi laheyn in la weeraro shabakadda, waxay abuuri doonaan silsiladda ugu dheer iyo kuwa weerarada ka soo horjeeday. Shabakada lafteeda waxay u baahan tahay qaab yar. Farriimaha ayaa loo baahiyaa si ku saleysan dadaallada ugu wanaagsan, oo qanjirradu way ka baxaan oo ku farxi karaan shabakadda ee dardaaranka, aqbalaadda silsiladda ugu dheer ee caddaaladda u ah waxa dhacay markii ay dhaafeen.

Hordhac

Ganacsiga internetka ee internetka ayaa u yimid inay si gaar ah ugu tiirsan tahay hay'adaha maaliyadeed ee u adeegaya iyada oo lagu aaminay dhinac saddexaad oo lagu kalsoon yahay si ay uga baaraandegaan lacagaha elektiroonigga ah. In kasta oo nidaamku sifiican ugu shaqeeyo wax ku filan macaamil ganacsiyada, weli waxaa ku dhaca daciifnimada dhaxalka ah ee hannaanka ku saleysan aaminaadda. Gunnada aan la is-eedeyn oo aan la beddeli karin runtii suurtagal maahan, maadaama hay'adaha maaliyadeed aysan ka fogaan karin dhexdhexaadinta khilaafaadka. Qiimaha dhexdhexaadintu waxay kordhisaa qarashka macaamilku, xaddidaya cabirka macaamil ganacsi ee ugu yar oo goynta suurtagalnimada macaamil ganacsi oo yar yar, oo waxaa ku jira kharash ballaaran oo ku saabsan luminta bixinta lacagaha aan la is-waafajin karin ee adeegyada aan la beddeli karin. Suurtagalnimada dib-u-noqoshada, baahida loo qabo aaminaadda ayaa faafiya. Ganacsatada waa inay ka digtoonaadaan macaamiishooda, iyaga oo ku dhisi doona macluumaad ka badan inta ay haddii kale u baahan lahaayeen. Boqolkiiba khayaanada qaarkood ayaa loo aqbalaa inay yihiin mid aan laga maarmi karin. Kharashaadkaan iyo qiimahan aan la xakameyn waa laga fogaan karaa qof ahaan iyadoo la adeegsanayo lacag jir ahaaneed, laakiin

qaab ma jiro si lacag looga bixiyo kanaalada isgaarsiinta iyada oo aan xisbi la aaminin.

Waxa loo baahan yahay waa nidaam lacageed elektiroonig ah oo ku saleysan caddeynta conpptographic halkii ay ku kalsoon tahay, taasoo u oggolaanaysa laba dhinac oo diyaar ah inay si toos ah isula wareegaan dhinac saddexaad oo aan loo baahnayn. Macaamilada kumbuyuutarrada kumbuyuutarrada si macquul ah loo beddelo waxay ka difaaci doonaan iibiyaasha khayaanada, iyo qaababka qaab-dhismeedka caadiga ah ayaa si fudud looga hirgalin karaa si loo ilaaliyo iibsadayaasha. Waraaqdan, waxaan u soo jeedineynaa xalka mushkiladda laba-geesoodka ah iyadoo la adeegsanayo isu-qaybinta server-ka jeer ee 'Timestamp server' si loo abuuro caddeyn kombuyuutar ah oo ku saabsan nidaamka takoorka ee xawaaladaha. Nidaamku waa aamin illaa inta noodyada daacad ah ay si wada jir ah u xakameeyaan awoodda 'CPU' oo ka badan koox kasta oo iskaashi ah oo qandaraasyada weerarka ah.

Macaamil

Waxaan qeexnaa muucoin elektarooniga ah sida silsilad saxeexyo dhijitaal ah. Milkiilaha kasta oo wareejinta xeebta si ay xiga by sharaf saxiixayo hash ah ee macaamil ganacsi hore iyo furaha dadweynaha ee milkiilaha xiga iyo ku daray, kuwaas oo ay u dhamaadka xeebta. Lacag bixinta A xaqiijin karaa saxiixyada si loo xaqiijiyo silsiladda lahaanshaha.

Dhibaatada dabcan waa mushaharka ma xaqiijin karo in mid ka mid ah milkiilayaasha aysan labanlaabnay lacagta qadaadiicda. Xallaab caan ah ayaa ah in la soo bandhigo maamul udub dhexaad u leh, ama mint, taas oo hubinaysa macaamil kasta oo ku saabsan laba-laab. Dareer kasta oo ka dib, qadaadiicda waa in lagu celiyaa mint si ay u soo saarto qadaadiic cusub, oo kaliya qadaadiic toos ah ayaa laga soo saaray miraha laguma aaminin in aanu labanlaabin. Dhibaatada xalkaan ayaa ah in masiirka nidaamka lacagta oo dhami ay kuxirantahay shirkadda ku shaqeysa militariga, oo ay la socdaan macaamil kasta oo ay ku jiraan, sida bangiga oo kale.

Waxaan u baahan nahay hab mushaharka ah si aan u ogaano in milkiilayaashii hore aysan saxeexin wax lacag ah oo macaamil hore ah. Ujeeddadeena, macaamilkii ugu horreeyay waa kan tirinta, sidaa darteed dan kama lihin isku dayga dambe ee laba-qalin. Sida kaliya ee lagu xaqiijinayo maqnaanshaha macaamil ganacsi waa in laga warqabo dhammaan macaamil ganacsi. Qaabka ugu sareeya ee ku saleysan mint-ka, mint ayaa ka warqabay dhammaan macaamil ganacsi oo dhan wuxuuna go'aansaday kaas oo markii hore yimid. Si tan loo gaaro iyada oo aan laheyn koox aan la aaminayn, macaamil xawilaadda waa in si cad loogu dhawaaqo [1], waxaanan u baahanahay nidaam kaqeybgaleyaasha si ay ugu heshiiyaan hal taariikh oo ah amarkii lagu helay. Lacagta bixiyaha waxay u baahan tahay caddeyn taas oo ah waqtiga macaamil kasta oo macaamil kasta, inta badan magacyada ay ku heshiiyeen waxay ahayd kii ugu horreeyay ee la helay.

Wakhtiga serverka

Xalka aan soo jeedinay wuxuu ku bilaabaa serverka jadwal. Server Time shaqeeya by qaadashada hash of block ah alaabta la la garab iyo ballaaran daabacayo hash ah, sida wargeys ama post Usenet [2-5]. Waa in waqtigii caddeyneysaa in xogta waa in ay ka jirey waqtiga, iska cad, si aad u hesho galay hash ah. Shaabad kasta oo mar ka mid ah shaabad xilliyadii hore ee hash ay, la xirrira silsilad, oo leh kasta oo wakhti dheeraad ah ay xoojinta kuwa ka hor.

Caddeynta shaqada

Si loo hirgaliyo server-ka 'Timestamp' ee loo qaybiyey si sahlan fac-u-dhigga, waxaan u baahan nahay inaan u isticmaalno nidaam-caddeyn-shaqo oo la mid ah Adam dib-u-dhigga Lacagta 'Adam's Report's Cash [6], halkii qoraallada loo yaqaan' onenet '. Shaqo-u-shaqaynta ayaa ku lug leh iskaanka si loogu qiimeeyo markii la xareeyay, sida SHA-256, Hash wuxuu ku bilaabmayaa dhowr laab oo eber ah. Celcelis ahaan shaqada loo baahan yahay waa mid loo qurxiyo tirada tirada xeryaha eber ee loo baahan yahay waxaana la xaqiijin karaa iyadoo la fulinayo hal xashiish.

Waayo, nidaamka jadwalka shabakad, waxaan hirgelin caddaynta-of-shaqo by kordhinta hal mar ee block ah ilaa qiimaha la helo in siinayaa hash block ee meesha loo baahan yahay eber. Marka dadaal CPU ayaa la filayaa in ay u dherjiyo caddaynta-of-shaqo, block ma la beddeli karo iyada oo aan sameynaaya shaqada. Sida aagag dambe yihiin xiraa kadib, shaqada si loo beddelo block ka mid ah falnay lahaa dhammaan aagag ka dib waxa.

Waxa kale oo caddeynta-ka-shaqo la xalinayo dhibaatada go'aaminta wakiilnimo ee go'aan qaadashada intooda badan. Haddii intooda badan waxay ku salaysnaayeen mid-IP cinwaanka- ka mid ah-cod, waxaa wareejin karto by qof kasta oo awoodaan si loo qoondeeyo badan IPs. Caddaynta-of-shaqo muhiimad ahaan waa mid-CPU-mid cod. Go'aan intooda badan waa wakiil by silsiladda ugu dheer, taas oo uu leeyahay dadaalka ugu weyn ee caddaynta-of-shaqo ku maalgelisay it in. Haddii aqlabiyadda ah ee awood CPU waxaa gacanta ku tolayaa daacad ah, silsiladda daacad ah kori doono ugu dhaqsaha badan iyo Xawliga wax kasta oo silsiladaha ku tartamaya. Si aad u habeeyo block a ee la soo dhaafay, weeraryahanka ah lahaa Shaqadu ay u hesho caddeynta-of shaqada ee block ah iyo dhammaan baloog ka dib markii ay qaadi ilaa leh iyo ka dul mari shaqada of odayada daacad ah. Waxaan mar dambe ku tusi doonaa in itimaalka ah oo weeraryahanka ah gaabta kor ku dhacdo in ay hoos u siyaadin sida aagag xiga waxaa lagu daray.

Si aad magdhowga xawaaraha qalabka kuwa iyo danta kala duwan ee orodka ka badan waqti, dhibaato caddaynta-of-shaqo la go'aamiyo celcelis ahaan u dhaqaaqaya oo lagu beegsanayo tiro celcelis ahaan aagag halkii saac. Haddii ay aad u dhakhso dhab ah, dhibaatada ay kordhisaa.

Shabakadda

Tallaabooyinka lagu maamulayo shabakadda waa sida soo socota:

1. Hawshan waxa New waxaa la warbaahin dhammaan dhinacyada.
2. Mid kasta oo ka mid ah soo ururiya macaamil cusub galay block ah.
3. Mid kasta oo ka shaqeeya on raadinta caddaynta-of-shaqo adag ay block ah.
4. Marka Node a helaa caddayn-of-shaqo, waxaa ku baahisaa block ah in ay sanka oo dhan.
5. Qofna aqbalaan block ah oo kaliya haddii dhammaan macaamil ganacsi waxaa aan dhicin iyo hore u bixisay.
6. November muujiyaan aqbalaada ee block ah by la shaqeeya on abuuraya block xiga ee silsiladda, iyadoo la isticmaalayo hash ee ku block ah kuwa la aqbalay sida hash hore.

Qofna mar walba tixgeliyaan silsiladda ugu dheer in uu noqdo mid sax ah iyo hayn doonaa shaqada on dheeraynaysa. Haddii laba oday warbaahin qoraalkii ka kala duwan ee block soo socda isku mar, qaar ka mid ah waxaad heli kartaa mid ama kii kale ee ugu horeeyay. Sidaas daraaddeed waxay ku shaqeeyaan tii koowaad ee la helay, laakiin laanta kale ee kiiskan ha sii ahaato. Wakhtiga shaqada la qabanayo waa la jabi doonaa oo laan walba mar dambe dib ayuu u furnaan doonaa; dirir ah in shaqeeya on laanta kale ka dibna is beddel doonaa mid ka dheer.

Broadcasts turjumaan New uma baahna in ay gaaraan dhammaan sanka. Intay gaaraan sanka badan, ayaa si fiican u qabsan doonaa. Baahiyeyaasha Block sidoo kale dulqaad of farriimaha hoos u. Haddaan qof isku barbaarin ah la helin wuxuu u codsan doonaa markuu qaabilo dhagaha xigta oo uu ogaado in ay geshay.

Dhiirigelin

By shir, macaamil ganacsi ee ugu horeeyay ee block ah waa macaamil ganacsi gaar ah in uu bilaabo coin cusub leeyahay abuuraha block ah. Tani waxay ku darayaa niyad ah ee maskaxda si ay u taageeraan shabakadda, waxayna bixisaa hab si marka hore u qeybinaya Shilimaad galay wareegga, tan iyo ma jirto maamulka dhexe si ay u soo saari. Intaa waxaa dheer joogta ah ee qadar joogto ah iyo Shilimaad cusub oo ah tarjumaysaa dahabka macdan qodayaasha ballaarinta khayraadka si ay dar dahab ah si ay wareegga. Xaaladdeenna, waa waqti un iyo korontada la filayo.

Niyad waxaa sidoo kale lagu maalgelin karaa lacag macaamil ganacsi. Haddii qiimaha wax soo saarka ee macaamil ganacsi uu ka yar yahay qiimaha ay aqbasho, farqiga waa lacag macaamil ganacsi in lagu daray qiimaha niyad of block ka kooban macaamil ganacsi ah. Marka tiro aan cayimin oo Shilimaad u galay wareegga, niyad-guurka gebi ahaan ku gudbi kartaa oo gebi ahaanba kharashka macaamil ganacsi iyo in si buuxda sicir-bararka lacag la'aan ah.

Niyad wuxuu kaa caawin karaa dhiiri-galinta ka waddo in ay ka sii daacad ah. Haddii weeraryahanka damaaci awoodaan in ay soo shiriso awood badan CPU ka badan dhammaan midihii daacad ah, wuxuu lahaa inuu doorto inta u dhaxaysa isticmaalaya waa in ay dib u caayo dadka by lacagaha uu, ama u isticmaalaya in ay dhalin Shilimaad cusub. Waa inuu helaa faa'iido

dheeraad ah si ay u ciyaaraan by xeerarka, sida in isaga raalli shilimaad ka badan qof kasta oo kale oo la isku daray, ka badan in ay wiiqdo nidaamka iyo ansax ah ee maalkiisa u gaar ah.

Dib U Helidda Cuntada

Marka macaamil ganacsi ugu dambeeyay ee sariir waxaa lagu aasay meel ka yar geeridi ku filan, macaamil wax la kharash gareeyey ka hor waxaa lagu tuuri karaa si ay u badbaadiyaan meel bannaan oo. Si loo fududeeyo this iyada oo aan jebinta hash block ee, xawaalad waxaa lagu daadshay in Geed Merkle [7] [2]], oo leh kaliya xididka ay ka mid yihiin hash block ah ee. Cimaarado duugoobay ayaa ka dibna waxaa lagu lammaaniyaa karaa bal adeygii iyo laamaha geedka. Arrimaha gudaha waxay ku degdegina uma baahna in la keydiyo.

Header block A with macaamil xawaalad jirin noqon lahaa oo ku saabsan 80 bytes. Haddii aan u malaynayaa in dhul yihiin guud ahaan 10 daqiiqo kasta, 80 bytes * 6 * 24 * 365 = 4.2MB sanadkiiba. Iyada oo nidaamyada kombiyuutarka caadi ahaan iibinta 2GB ee RAM sida of 2008, iyo Moore ee Sharciga saadaalinta koritaanka ee hadda 1.2GB sanadkiiba, kaydinta waa in aan noqon dhibaato xitaa haddii madaxda block waa in la hayaa xasuusta.

Caddeymo Lacag Bixinta

Waxaa suurtagal ah in lagu xaqiijiyo lacagaha iyadoon la sameyn shabakad buuxda. Kaliya qof isticmaala waa inuu nuqul ka mid ah madax-bannaanida block ee silsiladda ugu dheer ee cadeynta dadka, oo uu ka heli karo shabakadda lagu xiranayo ilaa uu ka dhaadhiciyay silsiladda ugu dheer, iyo helitaanka laanta Merkle ee ku xira bullaacadaha si ay u gudubto. Wuxuu kuma hubin karo macaamil ganacsi isaga nafsaddiisa, laakiin by it to meel ka soo silsilad, waxa uu arki karaa in shabakad halkii ayaa u aqbalay, iyo baloog ku daray ka dib waxa dheeraad ah xaqiijiyo shabakadda ayaa u aqbalay.

Sida sida, xaqiijinta waa lagu kalsoonaan karo ilaa inta daacad Galoble xakameeyo shabakadda, laakiin waa nugul haddii shabakad way xoog batay by weeraryahanka ah. Iyadoo shabakad ma xaqiijin karaa macaamil ganacsi isu for, habka ugu fududeeyey in lagu dhayax kara by macaamil ganacsi ah weeraryahanka ah ee Been abuurto ilaa inta weerarka sii wadi karaan inay awood shabakadda. Mid ka mid ah istiraatiijiyad si loo ilaaliyo this noqon lahayd in ay aqbalaan hel ka yimid shabakadda sanka marka ay ogaan block aan eryin, isla markiiba software user ee si dejisan block buuxa iyo shafeedhay si loo xaqiijiyo is cajabin ay. Ganacsiyada in ay helaan lacagaha soo noqnoqda laga yaabo in weli doonayaan in ay maamulaan sanka ah ee ammaanka madax-bannaan dheeraad ah iyo xaqiijinta dhakhso badan.

Isku-darka Iyo Qiimaha Neefsashada

Inkasta oo ay noqon lahayd suurto gal ah in siddo shilimaad shaqsi, waxay noqon lahayd unwieldy si ay u sameeyaan macaamil ganacsi oo gaar ah ee boqolkiiba kasta ee kala iibsiga ah. Si loo suurtogeliyo in qiimaha loo kala go'ay oo la isku daray, macaamil ganacsi waxaa ku jira dhawr iyo qawl. Sida caadiga ah waxaa jiri doona labada aqbasho hal ka soo macaamil ganacsi hore ka weyn ama kala duwan oo la isku daraa xaddi yar yar, iyo ugu labada qaybood: mid ka mid ah lacag-bixinta, iyo mid ka soo laabanaya isbedelka, haddii ay wax kasta oo, dib u soo dirtay diraha.

Waa in la ogaadaa in taageere-out, halkaas oo macaamil ganacsi ku xiran tahay macaamil ganacsi dhowr ah, iyo macaamil-kuwa ku xiran badan oo dheeraad ah, ma aha dhibaato halkan. Marna waxaa jira baahida loo qabo in laga saaro nuqul ka mid ah oo dhamaystiran oo taariikhda macaamil-ee.

Asturaad

Habkaa soo jireenka ah hanata heer of asturnaanta by xadidaysa helitaanka macluumaadka si labada dhinac ku lug iyo xisbiga ku kalsoon tahay saddexaad. Baahida loo qabo in ay ku dhawaaqaan dhamaan macaamil furan meel fagaare ah ka dhigi habka this, laakiin asturnaanta weli waxaa lagu maamuli karaa by jebinta socodka macluumaadka meel kale: by haysashada furaha dadweynaha si qarsoodi ah. Waxaad dadweynaha u arkeysaa in qof kale lacag u dirsanayo, laakiin aanu jirin war qofkaasi ku xiriirinayo wuxuu khaas u yahay. Tani waxay la mid tahay heerka macluumaadka la sii daayay by is-weydaarsiga stock, halkaas oo waqtiga iyo size ee caado shaqsi, "cajalad", waxaa lagu sameeyey dadweynaha, laakiin aan sheegaya kuwa ay labada dhinac ay ahaayeen.

Sida dab damiye oo dheeraad ah, labo muhiim ah oo cusub waa in la isticmaalaa macaamil ganacsi kasta si ay iyaga ka ilaaliso lala milkiilaha caadi ah. Qaar isku xira weli waa laga hortegi karin macaamil maalyo kala duwan-aqbasho, kuwaas oo daruuri u muujiyo in sir ah ayaa laga leeyahay mulkiilaha isku. Khatarta meesha ay leedahay haddii milkiilaha furaha lagu shaaciyo, waxaa la muujin karaa lacag kale oo taas ka tirsanaa mulkiilaha isku.

Xisaabinta

Waxaan ka fiirsan abuurey oo ah weeraryahanka isku dayaya in ay dhalin silsilad ah beddelid ka dhaqso badan silsiladda daacad ah. Xitaa haddii uu jidkan dhaco, ma tuurin nidaamka u furan isbedel aan loo aabo yeelin, sida inuu qiimeyn ka bixiyo hawada khafiif ah ama lacag madax u ah oo aan waligeed horay u jirin ayaa loo yiri: Qofna ma inay aqbalaan macaamil ganacsi aan sax ahayn sida lacag bixinta, iyo madax daacad ah marnaba aqbali doono block ah iyaga oo ka

kooban. Weeraryahanka isku dayi kartaa oo kaliya in la beddelo mid ka mid ah isaga u gaar ah macaamil ganacsi si lacag dib uu dhawaan ku bixisay qaadan.

Jinsiyad The u dhexeeya silsiladda oo daacad ah iyo silsilad weeraryahanka ah waxaa lagu gartaa sida Nagula Soco Binomial. Dhacdada guusha waa silsiladda daacad ah lagu kordhin by hal block, sii kordhaya ay hogaanka by +1, iyo dhacdo guuldarada yahay silsiladda weeraryahanka ee lagu kordhin by hal block, yaraynta farqiga by -1.

Itimaalka weeraryahanka ah ilaa qaadaan ka soo hoos u dhaca ah a la siiyey, waxa ay ka tarjumaysaa dhibaatada baabba'a Gambler ee. Ka soo qaad khamaarkii leh deyn aan xad lahayn ay bilaabataa at hoos u dhaca ah iyo ciyaartaa Tanoo tiro aan koobi karayn of jirrabaaddaha inay isku dayaan in ay gaaraan horumar ah. Waxaan xisaabo kartaa siday suurtogal ku uu abid gaaro horumar degdeg ah, ama in weeraryahanka ah abid ku wajahan leh silsiladda daacad ah, sida soo socota [8]:

$$
\begin{aligned}
p &= \text{probability an honest node finds the next block} \\
q &= \text{probability the attacker finds the next block} \\
q_z &= \text{probability the attacker will ever catch up from } z \text{ blocks behind}
\end{aligned}
$$

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

Marka la eego our sifoobo in $p > q$, itimaalka aan faqiirsan sida tirada baloog weerarka uu leeyahay in ay ku qabsadaan leh korodhka. Iyada oo xumaatee ku isaga ka gees ah, haddii uusan sameeyo sambabada a nasiib hore on, fursadaha uu noqdo kuwo baabi'i yar yar sidii uu u sii daba dhaco.

Hadda waxaan ka fiirsan inta qaataha ah ee macaamil ganacsi oo cusub oo u baahan yahay in ay sugaan ka hor inta ku filan oo soo dirtay oo aan ka beddeli karo turjumidda. Waxaan u qaadan diraha waa weeraryahanka ah oo doonaya inuu sameeyo qaataha ah aaminsan wuxuu isaga bixisay in muddo ah, ka dibna waxa u beddelato inaad dib u bixiso si naftiisa muddo ka dib ayaa ka gudbay. Qaateyaasha wuxuu la socoto digniinaha doonaa marka ay taasi dhacdo, laakiin amaahiya waxay rajaynaysaa inay goor dambe noqon doono.

Qaateyaasha Guud labo muhiim ah oo cusub oo ku siinayaa furaha dadweynaha in ay soo dirtay wax yar ka hor saxiixa. Tani waxay ka hortagtaa amaahiya ka soo diyaarinta silsilad ah aagag ka hor waqtiga by shaqeeya waxa on joogto ah ilaa uu waa nasiib ku filan si aad u hesho meel fog ka hor, ka dibna toogashadiisa macaamilka ganacsi ee xilligan in. Marka macaamil ganacsi waxaa loo diraa, diraha aan daacad ahayn bilaabo ka shaqeeya qarsoodi ah on silsilad isku midka ah ka kooban version beddelid of uu macaamil ganacsi.

Qaataha waxa uu sugaa ilaa macaamil ganacsi ayaa lagu daray in ay block ah iyo baloog waxay leeyihiin lala it ka dib. Ma garanayo tirada saxda ah ee horumarka weerarka uu sameeyay, laakiin heerna isa ku dekedda daacad qaatay waqti celcelis ahaan la filayaa block, horumarka iman kara

weeraryahanka ayaa noqon doona Sun qaybinta kula qiimaha filayaa:

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

Si loo helo itimaalka weerarka weli ku qaadi kara ilaa hadda, waxaan u tarmin, Sun cufnaanta for qadar kasta oo horumar ah uu u samayn karay by itimaalka uu ku qaadi kara ilaa dhibic in:

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

Reqabanqaabinaya in ay iska ilaaliyaan lagaala badhidii aan la koobi karayn of qaybinta ...

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

Badalashada 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;
}
```

Running natiijada qaar ka mid ah, waxaan ka arki kartaa dhibic dhici kara ee ku filin ay la 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
```

Xalinta for P ka yar 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
```

Natiijooyinka

Waxaan soo jeediyey nidaam for macaamil xawaalad elektaroonik ah oo aan ku tiirsan trust. Waxaan ku bilaabay qaabka caadiga ah ee shilimaad laga sameeyey saxiixyada dhijitaalka, kaas oo bixiya ay gacanta xoog leh lahaanshaha, laakiin waxa aan dhamaystirnayn si looga hortago qarashyada laba-dhaca. Si taa loo xaliyo, waxaan soo jeedinay shabakad dad wadal-ka kooban oo isticmaalaya cadeyn-of-shaqo si loo qoro taariikh ganacsi oo sida ugu dhaqsiyaha badan kombiyuutarka u hirgali karo oo ah qofka soo weeraray si loo badalo hadii daacad ah nodes xukunka awooda CPU ay badanyihiin. Shabakaddu waa mid xoogan ee ay xog la'aan u habaysan. Qofna shaqeeyaan oo dhan hal mar la isuduwidda yar. Waxay uma baahna in la aqoonsaday, tan iyo farriimaha aan loo adkeeyaa meel kasta oo gaar ah oo kaliya u baahan in la gacangeliyey ku saleysan dadaal ugu wanaagsan. Qofna ka bixi kartaa oo naqdi doontaan shabakadda at doono, aqbalayaan silsiladda caddayn-of-shaqo sida caddaynta wixii dhacay halka ay ka baxeen. Waxay u codeeyaan ay awood CPU, oo loo muujiyo aqbalaada ee ansax ah by shaqeeya on iyaga u kordhin iyo diidayeen aagag aan sax ahayn by diiday in ay iyaga ka shaqeeyaan on. Sharciyo kasta oo loo baahan yahay iyo dhiirrigelin lagu dhaqangelin karaa farsamo la isla oggolaansho this.

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.