

# Bitcoin: Enkola munnokumunno ey'ensimbi z'omutimbagano

bya Satoshi Nakamoto [2008/10/31](#)

## Abstrakiti

Enkola munnokumunno ey'ensimbi z'omutimbagano yandisobozesa ensasulagana ku kitimba okusindikibwa okuva ku omu okudda ku mulala ewatali kuyita mu kitongole kya nsimbi. Emikono gya digito gituwamu ku kyokuddamu, naye okuganyulwa okusinga kubula singa omutabaganya ow'okusatu aba akyetaagisa okuziyiza ensaasaanya ya nnabansasaana. Twanja empenda okuziyiza ekizibu ky'ensaasanya ya nnabansasaana nga tukozesa omuyungagano munnokumunno. Omuyungagano gusimba obudde ku mpanyisiganya nga guzitugga mu lujegere lw'entuttwa olw'olubeerera olukakasa obukozi, okukola obuwandiike obutasobola kukyusibwa ewatali kuddamu kukakasa bukozi. Olujegere olusinga obuwanvu terukoma kutuyamba kukakasa biki ebibaddewo, naye n'okukakasa nti bivudde mu manyi ga CPU agasinga. Kasita kiba nti amanyi ga CPU agasinga gali mu mikono gitakolagana kulumba muyungagano, emikono gino gyijja kukola olujegere olusinga obuwanvu era olumegga abalumbaganyi. Omuyungagano gwo nga gwo tegwetaaga misoso mingi. Obubaka bulangirirwa okusinzira ku ani asinze okussaamu amanyi, era ennyingo zisobola okuwanduka n'okwegatta ku muyungagano wezaagalidde, nga zikkiriza olujegere olukakasa obukozi olusinga obuwanvu ng'obukakafu ku byabaddewo nga ziwanduse.

## Ennyanjula

Okusuubulagana ku mutimbagano kuzze kweyambisa nnyo ebitongole by'ensimbi okutabaganya mu nsonga z'ensansulagana. Yadde enkola eno ekola ku mpanyisiganya ezisinga obunji, wakyaliwo emiwatwa mingi. Empanyisiganya ezitazzika mabega tezinnasoboka, anti ebitongole by'ensimbi tebisobola kwewala kutabaganya bukuubagano. Okutabaganya kuno kuwanika ebbeeyi y'okuwanyisiganya, nekissa ekkomo ku bunene bwempanyisiganya ezisobola okukolebwa, era obuwanyisiganya obutonotono nebuba nga tebusoboka. Mu ngeri y'emu waliwo okukaliga ebbeyi okuva mu butasobola kukola nsasulagana zitazzika mabega. Okuzza emabega bwekuba kusobose, obwesigwa obusingako buba bwetagisa. Abatunda baba b'ekengera ababagulako, ekivaamu okubasaba ebiboogerako ebisinga nekubyeetaagisa. Akatundu ku kikumi akoobukumpanya kakkirizibwa nga akateewalika. Okukaliga kuno n'ebigwabitalaze mu nsasulagana bisobola okuziyizibwa mu buntu singa ensimbi ezikwatikako ziba zikozeseddwa, wabula nga mpaawo ngeri yakusasulagana ku mukutu gwa mpuliziganya awatali mutabaganya.

Ekyetagisa y'engeri y'okusasulagana ku mutimbagano esinziira ku bukakafu bwa kriptografe mu kifo ky'okwesigan'gana okwabulijjo, okusobozesa abawanyisiganya okukikola awatali

mutabaganya. Empanyisiganya ezitasoboka kuzzika mabega zikugira obufere obwandikosezza abatunzi n'abaguzi. Mu lupapula luno, twanja engonjoola y'ekizibu ky'ensaasanya ya nnabansasaana nga tukozesa engabirizi eyeyanjadde kisimbabudde munnokumunno okugunjaawo obukakafu bw'olulyo lw'empanyisiganya. Sistimu eba nzigumivu kasita kiba nti ennyingo ennesimbu mu bugatte zeezilina amanyi aga CPU agasinga ekibinja kyonna eky'ennyingo ezilumba omuyungagano.

## Empanyisiganya

---

Tulambika ekinusu nga olujegere lw'emikono gya digito. Buli nnannyini kyo akiwa addako nga assa omukono ku ntutwa y'empanyisiganya eyakasembayo n'ekisumuluzo eky'olukale eky'a nannyini kinusu addako, olumala bino byonna nebigattibwa ku nkomelero y'ekinusu. اساسulwa asobola okukakasa emikono okukasa olujegere lwobwannannyini.

Obuzibu mu kino buli nti اساسulwa tasobola kukakasa nti omu kuba nnannyini kinusu abaasoose teyakisaassannyiza mirundi gisoba mu gumu. Engonjoola y'ekizibu kino eriwo ensanji zino yakukozesa mutabaganya, akebera buli mpanyisiganya okukakasa nti yasaasanyiziddwa mulundi gumu gwokka. Obuzibu bw'engonjoola eno buli nti entuuko ya sistimu y'ensimbi zonna ezikozesebwa eri mu mikono gya mutabaganya, anti buli mpanyisiganya erina kuyita mu yye, nga bwekiba mu bbanka.

Twetaaga engeri اساسulwa okumanya nti bannannyini kinusu abaasoose tebaatadde mikono ku mpanyisiganya zaakyo ndala zonna. Wano empanyisiganya embereberye yesinga obukulu, nabwekityo tetufaayo ku kugezaako kusaasanya mirundi ebiri mu mpanyisiganya zonna eziddirira embereberye mu lujegere. Enger yokka ey'okukakasa obufu bwempanyisiganya kwekumanya empanyisiganya zonna ezaali zibaddewo. Bwetuba tweyambisizza omutabaganya, aba amanyi empanyisiganya zonna era nga amanyi eriwa eyasoose okubaawo. Bwetuba tetwagalawo mutabaganya, olwo empanyisiganya zonna zirina okulangirirwa mu lukale[1], era twetaga sistimu nga abagyenigiramu bassa kimu ku lukalala lwonna olwempanyisiganya ezaali zikoledwa. اساسulwa yeetaaga obukakafu nti ku kaseera buli mpanyisiganya bwekolebwa, ennyingo ezisinga zikkaanya nti ye yasoose okufunibwa.

## Engabirizi kisimbabudde

---

Engonjoola gyetussa mu ddiro etandika n'engabirizi kisimbabudde. Engabirizi eno ekwata entutwa y'emiteeko ejilina okusimbibwako obudde ,era n'erangirira entutwa eno, nga bwekyandibadde mu lupapula lw'amawulire oba ku Usenet[2-5]. Ekisimbabudde kikakasa nti bwino ono yabeerawo mu kaseera ako, okusobola okuyingira entutwa. Mu buli ntutwa ya kisimbabudde mubaamu ekisimbabudde ekyasooseewo, era olujegere nelukolebwa, nga buli kisimbabudde ekkiddirira kikkaatiriza ebiba bisoosewo.

# Okukakasa obukozi

---

Okussa engabirizi eno mu nkola ,tujja kwetaaga sistimu ekakasa obukozi efaananako ne Hashcash ya Adam Back[6], mu kifo ky'olupapula lwamawulire oba Usenet. Okukakasa obukozi kuno kuba kwekenneenya muwendo nga bweguba gutuggiddwa,nga bwekiri mu SHA256, entutwa etandika n'ennamba ya biiti za zeero engereke. Obukozi obwetagisa bunji ekiyitiridde okusinziira ku bunji bwa biiti za zeero ezigerekeddwa era busobola okukakasibwa nga tukozesa entutwa emu.

Ku lw'omuyungagano gwaffe kisimbabudde, okukakasa obukozi tukussa mu nkola nga twongereza ku nonsi mu muteeko paka nga omuwendo guzuuliddwa oguwa entutwa y'omuteeko biiti za zeero ezeetaagisa. Kasita kiba nti amanyi ga CPU gakozezeddwa okukakasa obukozi, omuteeko tegusobola kukyusibwa okujjako nga omulimu ogukoleddwa guddiddwamu buto. Emiteeko ejiddira gyejikoma okuwera,omulimu ogwetaagisa okukyusa omuteeko guno guba gwesigama ku kuddamu kukola mirimu ku miteeko gyonna ejiguddirira.

Okukakasa obukozi mu ngeri y'emu kugonjoola ekizibu ky'okupima obukiise mu kusalawo. Okusalawo kw'abanji singa kwali kusinzira ku ndagiriro-ya-IP-emu-kalulu-kamu, oli yandisobodde okwegabira endagiriro za IP ezisoba mu emu. Okukakasa obukozi eba CPU-emu-kalulu-kamu. Okusalawo okw'abangi kusinziira ku lujegere lusinga buwanvu, anti lweluba lutaddemu amanyi agasinga endala zonna okukakasa obukozi. Bwekiba nga amanyi ga CPU agasinga gali mu mikono gya nnyingo ntuufu, olujegere olutuufu lwelujja okusinga okukula amangu era lujja kuyisa endala zonna ezivuganya. Okukyusa omuteeko oguyise kiba kyetaaga alumba okuddamu okukakasa obukozi bwomuteeko ogwo n'emiteeko gyonna ejiguli wansi, olwo naalwana naasinga obukozi bwennyingo entuufu. Mu maaso awo tugenda kulaga nti emikisa gy'alumba n'olulembwe okukwata n'okusinga amanyi g'ennyingo entuufu gyikendeerera ddala emiteeko emirala gyejikoma okweyunga ku lujegere.

Okugattawo ku bwangu bw'ebyuma bya kompyuta obweyongera, n'obuganzi bw'okuddukanya ennyingo obukyukakyuka, obukalubu bwokukakasa obukozi bugerekebwa average etambula eyesigama ku average y'omuwendo gw'emiteeko buli ssawa. Emiteeko bwejibangibwawo amangu ennyo,obukalubu nga bweyongera

## Omuyungagano

---

Emitendera gy'okuddukanya omuyungagano gy'egyino wammanga:

1. Empanyisiganya empya zirangirirwa eri ennyingo zonna.
2. Buli nnyingo ekung'anya empanyisiganya empya mu muteeko gumu.
3. Buli nnyingo enoonya enkakasabukozi ekaluba ey'omuteeko gwayo.

4. Ennyingo bwezuula enkakasabukozi, nga erangirira omuteeko eri ennyingo endala zonna.
5. Ennyingo zikikiriza omuteeko kasita kiba nti empanyisiganya zonna ezigulimu ntuufu era tezinnaasanyizibwa.
6. Ennyingo ziraga okukikiriza kw'omuteeko nga ziyita mu kutandikirawo okukung'anya omuteeko oguddako mu lujegere, nga zikozesa entuttwa y'omuteeko ogukkiriziddwa nga entuttwa eyakasembayo.

Ennyingo zitwala olujegere olusinga obuwanvu okuba olutuufu era lwezijja okwongerako. Ennyingo ebiri singa zirangirira omuteeko oguddako mu ngeri bbiri ez'enjawulo omulundi gumu, waliwo ezijja okufuna omuteeko ogwo mu ngeri ey'enjawulo ku ndala mu kusooka. Mu buufu obwo, ennyingo zikola ku muteeko gwezisoose okufuna, naye zitereka ettabi eddala kuba tezimanyirawo oba lyelinasinga obuwanvu. Okusibagana kuno kujja kumenyebwa nga enkakasabukozi eddako ezuuliddwa era nga ettabi erimu ku abiri lyeyongedde obuwanvu; ennyingo ezibadde ku ttabi erikwebedde olwo zijja kudde ku likulembedde.

Okulangirira empanyisiganya empya tekutuukirawo ku buli nnyingo. Kasita kiba nti ekirango kituuse ku nnyingo ennyinji, empanyisiganya zijja kuteekwa mu muteeko mu kaseera katono. Okulangirira emiteeko mpozzi kugumiikiriza n'obubaka obusuule. Ennyingo bwetafuna muteeko, ejja kugusaba bwenaafuna omuteeko oguddako kabi ekizuula nti waliwo gwetalina.

## Ekisikiriza

---

Mu ngeri yonna, empanyisiganya esooka mu muteeko y'empanyisiganya enkulu ebangawo ekinusu nga nnanyini kyo ye mukung'anya w'omuteeko. Kino kisikiriza ennyingo okuwagira omuyungagano, era kiwa engeri y'okubunya ebinusu mu ntandikwa, anti tewabawo mutabaganya mukulu kubitambuza. Okwongerangamu ebinusu ebipya kufananganako nga abalombi ba zzaabu bwebakozesa ebikozesebwa okubunya zzabu buli wamu. Mu sistimu eno gyetwanja, ebikozesebwa buba budde bwa CPU na masannyalaze.

Ekisikiriza kino era kisobola okuwanirirwa ebisale by'empanyisiganya. Singa omuwendo gwa output y'empanyisiganya mutono ku gwa input yaayo, enjawulo byebiba ebisale by'empanyisiganya ebigattibwa ku muwendo gw'ekisikiriza ky'omuteeko ogulimu empanyisiganya eyogerwako.

Ekisikiriza kyandiyambako okukuumira ennyingo mu bwesimbu. Singa omulumbaganyi ow'omululu asobola okukunganya amanyi ga CPU agasinga ku nnyingo entuufu, aba alina okulondawo wakati w'okufera abantu nga abba ebinusu byasasudde abalala,oba okukozesa amanyi ago okubangawo ebinusu ebipya. Mu ngeri yonna kiba kimukolera amakulu okutambulira ku mateeka, agamuwa enkizo bwaba n'ebinusu ebisinga ku mulala yenna, mu kifo ky'okuyisa amaaso mu mateeka ga sistimu ekiyinza okusaanyawo obugagga bwe.

## Oukekkereza ekifo ku diski

---

Kasita kiba nti empanyisiganya eyakasembayo mu kinusu eziikiddwa mu miteeko ejimala,

empanyisiganya ezisaasanyiziddwa emabega waayo zisobola okukasukibwa ettale okukekkereza ekifo ku diski. Okutuukiriza kino ewatali kumenya ntutwa ya muteeko, empanyisiganya zisibwa mu muti gwa Merkle [7][2][5], nga mulandira gwokka gwegussibwa mu ntutwa y'omuteeko. Olwo emiteeko emikadde gyonna gyifunzibwafunzibwa anti amatabi g'omuti gaba gatemebwako. Entutwa z'omunda ziba tezeetaaga kuterekebwa.

Akasolya k'omuteeko ogutaliimu mpanyisiganya kandibaamu baiti nga 80. Singa tugamba nti emiteeko jikung'anyizibwa buli ddakiika 10, baiti  $80 * 6 * 24 * 365 = 4.2\text{MB}$  buli mwaka. Kompyuta wetwogerera mu 2008 bweziba nga zitundibwa ne RAM wa 2GB, nga kwotadde n'etteeka lya Moore eriteebereza okukula kwa 1.2GB buli mwaka, obugazi bwa diski za kompyuta tebulina kutwerariikiriza ne bwekiba nga obusolya bw'emiteeko bulina okukuumibwa mu memory.

## Okukakasa Ensasulagana Okwangu

---

Kisoboka okukakasa obukozi awatali kuddukanya nnyingo ya muyungagano nnamba. Oli alina kukuuma kkopi ya busolya bwa miteeko obw'olujegere lw'enkakasabukozi olusinga obuwanvu, lwayinza okufuna nga yeekennenyezza ennyingo z'omuyungagano ppaka nga akakasizza nti alina olujegere olusinga obuwanvu, olwo naafuna ettabi lya Merkle erigatta empanyisiganya ku muteeko mwesimbiddwa mu budde. Tasobola kwekeberera mpanyisiganya ,naye bwajigatta ku kifo mu lujegere, asobola okulaba nti ennyingo ku muyungagano ejikkirizza, era emiteeko egyongerwako gyongera kukkaatiriza nti empanyisiganya ekkiriziddwa.

Na bwekityo, obukakafu buno bwesigamibwako kasita kiba nti ennyingo entuufu zeeziddukanya omuyungagano, naye bubeera mu katyabaga singa omulumbaganyi azisinza amanyi. Yadde nga ennyingo zisobola okwekakasiza empanyisiganya ku lwazo, engeri eno ennyangu esobola okubuzaabuzibwa empanyisiganya z'omulumbaganyi empangirire ebbanga lyamala nga awambye omuyungagano. Akamu ku bukodyo byokwewala kino kwandibadde kutemezebwako kuva ku nnyingo mu muyungagano bwezizuula omuteeko omukyamu, ekireetera softweya w'oyo akozesa omuyungagano okuwanulayo omuteeko omulamba n'empanyisiganya eziriko akabuuza okwawula entuufu ku nkyamu. Bizineesi ezifuna ensasulagana ennyinji zandyagala okuddukanya ennyingo ezaazo ku bwazo kulw'okwerinda n'okukakasa amangu.

## Okugattagatta n'okutemaatemamu omuwendo

---

Yadde kyandisobose okutambuza ebinusu ku bwannamunigina, tekyandibaddemu nsa kukola mpanyisiganya emu ku buli ssente etambuzibwa. Okusobozesa omuwendo ogutambuzibwa okugattibwagattibwa oba okutemwatemwamu, empanyisiganya zibaamu input ne output ez'enjawulo. Mu mbeera eyabulijjo, wajja kubaawo input emu okuva mu mpanyisiganya eyaakayita oba input ennyingi ezigattagatta empanyisiganya entonotono, ne output ekinene ennyo bbiri: emu

nga ya nsasulagana, endala nga ya change, yenna asigalawo adda eri asasula.

Kirina okukkaatirizibwa nti fan-out, empanyisiganya emu weyesigamira ku ndala, era n'ezo wezeesigamira ku zinnaazo endala nnyingi, ssi kizibu wano. Tewabaawo bwetaavu mu ngeri yonna kufuna kopi yeteengeredde ey'ebyafaayo by'empanyisiganya.

## Obuteeyanika

---

Enkola ya bbanka eliwo ekuuma ebyama bya ba kasitoma baayo nga eyita mu kukomako ku bwino amanyibwa abawanyisiganya ku bikwata ku bannabwe n'omutabaganya. Obuwaze bw'okulangirira empanyisiganya zonna mu lujjudde kiziyiza engeri eno, naye era obuteeyanika busobola okukuumibwa nga tuyita mu kumenyamu entambula ya bwino mu kifo ekirala: ebisumuluzo by'olukale tebilina kumanyibwako mayitire. Buli omu asobola okulaba nti gundi asindikira gundi omuwendo gundi, naye nga tewali kiyunga mpanyisiganya n'emu ku muntu yenna. Kino kifanaganako ne bwino afulumizibwa ebifo ewawaanyisiganyibwa emigabo, ewaba nti obudde ne sayizi y'emigabo ejiwanyisibwa, oba "tape", bikolebwa mu lujjudde, naye nga abawanyisiganya tebaasanguddwa.

Mu ngeri y'okunyweza eby'okwerinda, ppeya empya ey'ebisumuluzo elina okukozesebwa ku buli mpanyisiganya empya okuziyiza okubiyunga kwooyo abikozesa. Weewawo waliwo okuyunga okuteewalika bwekituuka ku mpanyisiganya eza input esoba mu emu, anti waba walina okubaawo obukakafu nti input zonna ezikozesebwa zilina nannyini yoomu. Akabi akaliwo nti singa nannyini kisumuluzo ayanikibwa, okuyunga kuno kwa ndilaga empanyisiganya endala ezooyo yenna ayanikiddwa.

## Ebibalo

---

Tuteebereza embeera nga omulumbaganyi agezaako okuluka olujegere mu bwangu obusinga ku nnyingo eziluka olutuufu. Nebwaba kino akituukirizza, sistimu tekigissa ku ntoli ze kujikyusakyusa, okugeza nga okubangawo ebinusu by'empewo oba okutwala ensimbi ezitali zize. Ennyingo tezigenda kukkiriza mpanyisiganya zitali ntuufu mu kusasulagana, era ennyingo entuufu tezilikkiriza muteeko gulimu mpanyisiganya ezo. Omulumbaganyi asobola kugezaako bugeza kukyusa emu ku mpanyisiganya ze kweddiza nsimbi zaamaze kukozesa.

Olwokaano wakati w'olujegere olutuufu n'olujegere lw'omulumbaganyi tuyinza okulwekebejja nga Binomial Random Walk. Ekiraga obuwanguzi lw'elujegere olutuufu okwongerwako omuteeko gumu, ekiyongera ku bu kulembeze bwagwo  $+1$ , ate ekiraga okumeggebwa lw'elujegere lw'omulumbaganyi okwongerako omuteeko gumu, ekikendeeza omuwatwa wakati w'enjegere zombi ne  $-1$ .



Omukisa gw'omulumbaganyi okukwata olujegere olutuufu singa aba akwebedde tuyinza okugugereza ku ekizibu ekiyitibwa Gambler's Ruin. Katugeze omuzannyi wa zzaala alina empiki ezitaliiko kkomo atandika omuzannyo ku bbanja n'azannya emirundi ejitabalika okugezaako okusasula ebbanja. Tusobola okubala omukisa gwe okusasula ebbanja, oba nti omulumbaganyi alwa ddaaki nakwata olujegere olutuufu, bwetuti[8]:

$p$  = omukisa nti ennyingo entuufu efuna omuteeko oguddako

$q$  = omukisa nti omulumbaganyi afuna omuteeko oguddako

$q_z$  = omukisa nti omulumbaganyi alikwata olujegere olutuufu okuva ku miteeko  $z$  emabega

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

Bwetuba tuteeberezza nti  $p > q$ , omukisa gugwiira ddala ennamba y'emiteeko omulumbaganyi gyalina okukwata gyejikoma okweyongera. Engeri gyekiri nti emikisa gye egyokuwangula olwokaano mitono nnyo, bwatakulembererawo nga bukyali, obuwanguzi bwe bwongerera ddala okuba mu lusuubo gyakoma okukwebera."

Kati twekebejja ebbanga asuubira empanyisiganya empya lyalina okulinda okukakasizza ddala nti omusindisi tasobola kukyusa mpanyisiganya esindikiddwa. Katugambe nti omusindisi mulumbaganyi ayagala okulowoozesa gwasindikira nti amusasudde okumala akabanga, olwo akyukire mu kiti ng'embazzi y'esasule nga akaseera kayiseewo. Gwebasindikira ajja kutemezebawo obufere buno bwebunaabawo, naye asindika asuubira nti obudde bujja kuba buyise nnyo okukwatibwa.

Asindikirwa abangawo ppeya y'ebisumuluzo empya olwo naawa ekisumuluzo ky'olukale oyo yenna asindika nga okussaako emikono tekunnabaawo. Kino kiziyiza asindika okutegeka olujegere lw'emiteeko mu nkukutu ngayita mu kugezaako okukakasa obukozi paka nga afunye omukisa naakulembera olujegere olutuufu, olwo naasindika empanyisiganya ku dakiika eyo. Empanyisiganya kasita esindikibwa, omusindisi omukumpanya atandika okukola mu nkukutu ku lujegere olulala olulimu empanyisiganya ye enkyamu.

Asindikirwa alinda paka nga empanyisiganya egattiddwa ku miteeko era emiteeko  $z$  gyiguyungiddwako oluvannyuma. Tamanya mulumbaganyi weyaatuuse, naye katugambe emiteeko emituufu gyatutte akaseera akasuubirwa okutwalibwa buli miteeko, okusenvula kw'omulumbaganyi ejja kuba Poisson distribution n'omuwendo ogusuubirwa bweguti :

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

Okufuna omukisa gw'omulumbaganyi okuwangula, tukwaata Poisson density ku buli lusenvula lweyandikoze netukubisaamu n'omukisa gwe ogwokukwata olujegere olutuufu mu kaseera ako:

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

Tuddamu okupanga okuziyiza okugatta infinite tail ya distribution

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

Bwetukissa mu 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;
}
```

Bwetutunuulira ebivudde mu bibalo, tulaba nti omukisa gukenderera ddala ne 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

Okugonjoolera P wansi wa 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

## Okuwunzika

Twanjizza sistimu y'empanyisiganya ez'omutimbagano eziteesigama ku mutabaganya wa nkomeredde. Twatandise n'okulambulula engeri ebinusu gyebibangibwawo okuva mu mikono gya digito, ekiwa obwannannyini, naye ekitalimu nsa nga tetuziyizza kusasanya kwa nnabansasaana. Okugonjoola kino, tulambuludde omuyungagano munno-ku-munno ogukozesa "okukakasa obukozi" okutereka mu lukale olukalala lw'ebyafaayo by'empanyisiganya oluzibuwalila ddala okulumbibwa n'okukyusibwakyusibwa omulumbaganyi, singa ennyingo entuufu ziba n'amanyi ga CPU agasinga. Omuyungagano guba mutebenkevu nnyo mu bwangu bwagwo. Ennyingo zonna zikola omulundi gumu awatali mutabaganya. Tezeetaaga kweyogerako, anti obubaka tebulina kifo kigere webutwalibwa era bwetaaga kutambuzibwa kusinziira ku nnyingo ki esinze okussaamu amanyi. Ennyingo zisobola okuwanduka oba okwegatta ku muyungagano wezaagalidde, era zikkiriza olujegere olukakasizza obukozi nga olulaga ekyabaddewo ebbanga lyezimala nga ziwanduse ku muyungagano. Zilonda n'amanyi ga CPU zaazo, neziraga okukkanya ku miteeko emituufu nga zigyongerayo ,n'obutakkanya ku miteeko mifu nga zigaana okujikolako. Amateeka gonna n'ebiwooyawooya ebyetaagisa bisobola okussibwa mu nkola mu ntabagana eno.

## Ensonda

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.