Bitcoin: Rafitra vola elektronika Peer-to-Peer

by Satoshi Nakamoto 2008/10/31

saro-takarina

Ny dikan-teny elektrônika mitovy amin'ny mitovy aminy dia ahafahan'ny fandoavam-bola alefa mivantana avy amin'ny antoko iray mankany amin'ny iray hafa nefa tsy mandalo andrim-bola. Ny sonia nomerika dia manome ampahany amin'ny vahaolana, saingy very ny tombontsoa lehibe indrindra raha mbola takiana ny antoko fahatelo azo itokisana mba hisorohana ny fandaniana avo roa heny. Manolotra vahaolana amin'ny olan'ny fandaniana avo roa heny izahay amin'ny alàlan'ny tamba-jotra peer-to-peer. Ny tambajotra dia manipika ny fifampiraharahana amin'ny alàlan'ny fametahana azy ireo amin'ny rojo porofo-asa mifototra amin'ny hash, mamorona rakitra tsy azo ovaina raha tsy mamerina ny porofo-asa. Ny rojo lava indrindra dia tsy vitan'ny hoe porofon'ny filaharan'ny zava-nitranga hita maso, fa porofo koa fa avy amin'ny dobo lehibe indrindra amin'ny herin'ny CPU izany. Raha mbola fehezin'ny nodes izay tsy miara-miasa hamely ny tambajotra ny ankamaroan'ny herin'ny CPU, dia hiteraka rojo lava lava indrindra sy mahery vaika ny mpanafika. Ny tambajotra mihitsy dia mitaky rafitra kely indrindra. Ny hafatra dia alefa amin'ny ezaka tsara indrindra, ary ny nodes dia afaka miala sy miditra indray amin'ny tambajotra amin'ny sitrapony, manaiky ny rojo porofo lava indrindra amin'ny asa ho porofon'ny zava-nitranga tamin'izy ireo.

Fampidirana

Ny varotra amin'ny Internet dia nanjary niantehitra saika tamin'ny andrim-panjakana ara-bola miasa ho antoko fahatelo azo itokisana amin'ny fikarakarana ny fandoavam-bola elektronika. Na dia miasa tsara aza ny rafitra ho an'ny ankamaroan'ny fifampiraharahana, dia mbola mijaly noho ny fahalemen'ny modely mifototra amin'ny fahatokisana. Ny fifampiraharahana tsy azo averina tanteraka dia tsy azo atao, satria ny andrim-panjakana dia tsy afaka misoroka ny fifanolanana. Ny vidin'ny fanelanelanana dia mampitombo ny vidin'ny fifampiraharahana, mametra ny haben'ny fifampiraharahana azo ampiharina faran'izay kely indrindra ary manapaka ny mety hisian'ny fifampiraharahana madinidinika kely, ary misy vidiny mivelatra kokoa amin'ny fahaverezan'ny fahafahana manao fandoavam-bola tsy azo averina ho an'ny serivisy tsy azo averina. Miaraka amin'ny mety hisian'ny fiverenana dia miparitaka ny filana fitokisana. Ny mpivarotra dia tokony ho mailo amin'ny mpanjifany, manakorontana azy ireo amin'ny fampahalalana bebe kokoa noho izay ilainy. Ekena ho tsy azo ialana ny isan-jaton'ny hosoka. Ireo sarany sy tsy fahazoana antoka momba ny fandoavam-bola ireo dia azo sorohina manokana amin'ny fampiasana vola ara-batana, saingy tsy misy rafitra ahafahana mandoa vola amin'ny fantsom-pifandraisana tsy misy antoko azo itokisana.

Ny ilaina dia rafitra fandoavam-bola elektronika mifototra amin'ny porofo kriptografika fa tsy

fitokisana, mamela ny antoko roa vonona hifampiraharaha mivantana tsy mila antoko fahatelo azo itokisana. Ny fifampiraharahana izay tsy azo atao ny mamadika dia hiaro ny mpivarotra amin'ny hosoka, ary azo ampiharina mora foana ny fomba fiasan'ny escrow mba hiarovana ny mpividy. Ato amin'ity taratasy ity, manolotra vahaolana amin'ny olan'ny fandaniana avo roa heny izahay amin'ny alàlan'ny mpizara timestamp zaraina amin'ny mpiara-mianatra mba hamoronana porofon'ny kajy momba ny filaharan'ny fifampiraharahana. Ny rafitra dia azo antoka raha toa ka miray tsikombakomba amin'ny herin'ny CPU bebe kokoa noho ny vondron'olona mpanafika rehetra ny nodes marina.

varotra

Ny vola madinika elektronika dia faritanay ho rojo sonia nomerika. Ny tompony tsirairay dia mamindra ny vola madinika amin'ny manaraka amin'ny alalan'ny sonia nomerika ny tenifototra momba ny fifampiraharahana teo aloha sy ny fanalahidin'ny daholobe an'ny tompony manaraka ary manampy azy ireo amin'ny faran'ny vola madinika. Ny mpandoa vola dia afaka manamarina ny sonia mba hanamarinana ny rojo fananana.

Ny olana mazava ho azy dia tsy afaka manamarina ny mpandoa vola fa ny iray amin'ireo tompony dia tsy nandany roa ny vola madinika. Ny vahaolana mahazatra dia ny fampidirana manam-pahefana foibe azo itokisana, na mint, izay manara-maso ny varotra rehetra raha misy fandaniana avo roa heny. Aorian'ny fifampiraharahana tsirairay, ny vola madinika dia tsy maintsy averina amin'ny solila mba hamoahana vola madinika vaovao, ary ny vola madinika navoaka mivantana avy amin'ny solila ihany no azo antoka fa tsy ho lany indroa. Ny olana amin'ity vahaolana ity dia miankina amin'ny orinasa mitantana ny mint ny hiafaran'ny rafi-bola iray manontolo, izay tsy maintsy mandalo azy ireo, toy ny banky.

Mila fomba ahafantaran'ny mpandoa vola fa tsy nanao sonia ny fifampiraharahana teo aloha ireo tompona teo aloha. Ho an'ny tanjonay, ny fifampiraharahana voalohany indrindra no zava-dehibe, noho izany dia tsy miraharaha ny fikasana handany avo roa heny izahay. Ny hany fomba hanamafisana ny tsy fisian'ny fifampiraharahana dia ny fahafantarana ny fifanakalozana rehetra. Ao amin'ny modely mifototra amin'ny mint, fantatry ny mint ny fifampiraharahana rehetra ary nanapa-kevitra hoe iza no tonga voalohany. Mba hanatanterahana izany tsy misy antoko azo itokisana dia tsy maintsy ambara ampahibemaso ny fifampiraharahana[1], ary mila rafitra iray ahafahan'ny mpandray anjara manaiky ny tantara tokana momba ny lamina noraisina. Mila porofo ny mpandoa vola fa amin'ny fotoanan'ny fifampiraharahana tsirairay, ny ankamaroan'ny nodes dia nanaiky fa io no voaray voalohany.

Mpizara timestamp

Ny vahaolana atolotray dia manomboka amin'ny mpizara timestamp. Ny mpizara timestamp dia miasa amin'ny alàlan'ny fakana tenifototra amin'ny singa iray hosokajiana fotoana ary hamoahana

betsaka ny hash, toy ny amin'ny gazety na lahatsoratra Usenet[2-5]. Ny mari-pamantarana dia manaporofo fa tsy maintsy nisy ny angon-drakitra tamin'izany fotoana izany, mazava ho azy, mba hidirana amin'ny hash. Ny mari-potoana tsirairay dia ahitana ny mari-potoana teo aloha ao amin'ny hash-ny, mamorona rojo, miaraka amin'ny mari-pamantarana fanampiny tsirairay manamafy ireo eo alohany.

Porofon'ny asa

Mba hampiharana ny mpizara famantaranandro zaraina amin'ny fomba mitovy, dia mila mampiasa rafitra porofo momba ny asa mitovy amin'ny Hashcash an'i Adam Back [6] isika, fa tsy lahatsoratra an-gazety na Usenet. Ny porofon'ny asa dia misy ny fisavana sanda izay rehefa voasokajy, toy ny amin'ny SHA-256, dia manomboka amin'ny bitika aotra ny hash. Ny asa antonontonony ilaina dia mihamitombo amin'ny isan'ny bitika aotra ilaina ary azo hamarinina amin'ny fanatanterahana ny hash tokana.

Ho an'ny tambajotran'ny timestamp, dia mampihatra ny porofon'ny asa izahay amin'ny alàlan'ny fampitomboana ny nonce ao amin'ny sakana mandra-pahitana sanda iray manome ny hash an'ny sakana ny bitika aotra ilaina. Raha vantany vao lany ny ezaka CPU mba hanomezana fahafahampo ny porofo-asa, dia tsy azo ovaina ny sakana raha tsy mamerina ny asa. Satria ny blocs taty aoriana dia voafatotra aorian'izany, ny asa hanovana ny sakana dia ahitana ny famerenana ny sakana rehetra aorian'izany.

Ny porofo-asa ihany koa dia mamaha ny olan'ny famaritana ny fisoloan-tena amin'ny fanapahankevitra maro. Raha mifototra amin'ny iray-IP-address-iray-vote ny ankamaroany, dia mety havadika ho an'izay afaka mizara IP maro izany. Ny porofon'ny asa dia vato iray-CPU-iray. Ny fanapahankevitry ny maro an'isa dia asehon'ny rojo lava indrindra, izay manana ezaka porofo lehibe indrindra amin'ny asa atao amin'izany. Raha fehezin'ny nodes marina ny ankamaroan'ny herin'ny CPU, dia hitombo haingana indrindra ny rojo honest ary hihoatra ny rojo mpifaninana rehetra. Mba hanovana ny sakana teo aloha, ny mpanafika dia tsy maintsy mamerina ny porofon'ny asan'ny sakana sy ny sakana rehetra aorian'izany ary avy eo dia mahatratra sy mihoatra ny asan'ireo nodes marina. Hasehontsika any aoriana fa mihena tsikelikely ny mety hisian'ny mpanafika miadana kokoa rehefa ampiana sakana manaraka.

Mba hanonerana ny fampitomboana ny hafainganam-pandehan'ny fitaovana sy ny fahalianana miovaova amin'ny fampandehanana ny nodes rehefa mandeha ny fotoana, ny fahasarotan'ny porofo momba ny asa dia faritana amin'ny salan'isa mihetsika mikendry ny isan'ny sakana isan'ora. Raha vita haingana loatra izy ireo dia mitombo ny fahasarotana.

Tambajotra

Ny dingana amin'ny fampandehanana ny tambajotra dia toy izao manaraka izao:

1. Ny fifampiraharahana vaovao dia alefa amin'ny node rehetra.
2. Ny node tsirairay dia manangona fifanakalozana vaovao ao anaty sakana iray.
3. Ny node tsirairay dia miasa amin'ny fitadiavana porofo sarotra ho an'ny sakanany.
4. Rehefa mahita porofon'ny asa ny node iray, dia alefany any amin'ny node rehetra ilay sakana.
5. Ny nodes dia manaiky ny sakana raha tsy manan-kery ny fifampiraharahana rehetra ao anatiny ary tsy efa lany.
6. Ny nodes dia maneho ny fanekeny ny sakana amin'ny fiasana amin'ny famoronana ny sakana manaraka ao amin'ny rojo, amin'ny fampiasana ny hash an'ny sakana ekena ho toy ny hash teo aloha.

Nodes dia mihevitra foana ny rojo lava indrindra ho ny marina ary hiasa hatrany amin'ny fanitarana azy. Raha misy nodes roa mandefa dikan-teny hafa amin'ny sakana manaraka miaraka, dia mety hahazo ny iray na ny iray aloha ny node sasany. Amin'izay fotoana izay, dia miasa amin'ny voalohany azony izy ireo, fa tehirizo ny sampana hafa sao lava kokoa. Ho tapaka ny fatorana rehefa hita ny porofo momba ny asa manaraka ary mihalava ny sampana iray; ireo node izay niasa tao amin'ny sampana hafa dia hifindra any amin'ny iray lava kokoa.

Tsy voatery ho tonga any amin'ny node rehetra ny fandefasana fifampiraharahana vaovao. Raha mbola mahatratra nodes maro izy ireo dia hiditra ao anaty sakana tsy ho ela. Mandefitra amin'ny hafatra latsaka ihany koa ny fandefasana block. Raha tsy mahazo sakana ny node iray dia hangataka izany izy rehefa mahazo ny sakana manaraka ary mahatsapa fa tsy afaka iray.

Famporisihana

Araka ny fifanarahana, ny fifanakalozana voalohany amin'ny sakana iray dia fifampiraharahana manokana izay manomboka vola madinika vaovao an'ny mpamorona ny sakana. Izany dia manampy famporisihana ho an'ny nodes hanohanana ny tambajotra, ary manome fomba hizarana ny vola madinika amin'ny voalohany, satria tsy misy fahefana foibe hamoaka azy ireo. Ny fanampiana tsy tapaka amin'ny habetsaky ny vola madinika vaovao dia mitovy amin'ny mpitrandraka volamena mandany loharanon-karena hanampiana volamena amin'ny fivezivezena. Amin'ny tranga misy antsika dia fotoanan'ny CPU sy herinaratra no lany.

Ny famporisihana koa dia azo vatsiana amin'ny saram-pandraharahana. Raha ambany noho ny sandan'ny fampidiran-dresaka ny sandan'ny famoaham-bola, dia saram-pandraharahana izay ampiana amin'ny sandan'ny fandrisihana ny sakana misy ny varotra ny fahasamihafana. Raha vantany vao niditra mivezivezy ny isan'ny vola madinika, ny fandrisihana dia afaka mivadika tanteraka amin'ny saram-pandraharahana ary tsy misy vidim-piainana tanteraka.

Ny famporisihana dia mety hanampy amin'ny famporisihana ny nodes hijanona ho marina. Raha toa ny mpanafika tia vola dia afaka manangona hery CPU bebe kokoa noho ireo node marina rehetra, dia tsy maintsy misafidy izy na hampiasa izany mba hamitahana olona amin'ny

fangalarana ny karamany, na hampiasa izany hamokarana vola madinika vaovao. Tokony ho hitany fa mahasoa kokoa ny milalao amin'ny fitsipika, fitsipika toy izany izay mankasitraka azy amin'ny vola madinika vaovao kokoa noho ny hafa rehetra mitambatra, noho ny manimba ny rafitra sy ny fahamarinan'ny hareny.

Famerenana ny habaka kapila

Raha vantany vao nalevina tao ambanin'ny sakana ampy ny fifampiraharahana farany amin'ny vola madinika iray, dia ariana ny vola lany alohan'ny hanariana azy mba hitsitsiana toerana malalaka. Mba hanamorana izany tsy handrava ny hash an'ny sakana, ny fifampiraharahana dia hasiana amin'ny hazo Merkle [7][2][5], ary ny fakany ihany no tafiditra ao amin'ny hash an'ny sakana. Ny blocs taloha dia azo fehezina amin'ny fametahana ny sampan'ilay hazo. Tsy mila tehirizina ny hash anatiny.

Ny lohatenin'ny sakana tsy misy fifampiraharahana dia tokony ho 80 bytes. Raha ataontsika hoe misy sakana dia avoaka isaky ny 10 minitra, 80 bytes * 6 * 24 * 365 = 4.2MB isan-taona. Miaraka amin'ny rafitra informatika mazàna amidy miaraka amin'ny 2GB an'ny RAM amin'ny 2008, ary ny Laläàn'i Moore maminavina ny fitomboan'ny 1.2GB amin'izao fotoana izao isan-taona, dia tsy tokony ho olana ny fitahirizana na dia tsy maintsy tazonina ao anaty fitadidiana aza ny lohatenin'ny sakana.

Fanamarinana fandoavana tsotsotra

Azo atao ny manamarina ny fandoavam-bola nefa tsy mandeha amin'ny node tambajotra feno. Ny mpampiasa iray ihany no mila mitazona dika mitovy amin'ny lohatenin'ny sakana amin'ny rojo porofo lava indrindra amin'ny asa, izay azony amin'ny alalan'ny fangatahana node tambajotra mandra-pahazoany antoka fa manana rojo lava indrindra izy, ary mahazo ny sampana Merkle mampifandray ny varotra amin'ny sakana. misy fe-potoana izy io. Tsy afaka manamarina ny raharaham-barotra ho an'ny tenany izy, fa amin'ny fampifandraisana azy amin'ny toerana iray ao amin'ny rojo, dia hitany fa nisy node tambajotra iray nanaiky izany, ary nampiana sakana taorian'ny nanamarinany bebe kokoa fa nanaiky izany ny tambajotra.

Noho izany, azo ianteherana ny fanamarinana raha toa ka voafehin'ny nodes marina ny tambajotra, saingy marefo kokoa raha resin'ny mpanafika ny tambajotra. Raha afaka manamarina ny fifampiraharahana ho an'ny tenany ny nodes tambajotra, ny fomba notsotsotra dia mety ho voafitaky ny fifampiraharahana noforonin'ny mpanafika raha mbola afaka manohy mandresy ny tambajotra ny mpanafika. Ny paika iray hiarovana amin'izany dia ny fanekena fampandrenesana avy amin'ny node-tambajotra rehefa mahita sakana tsy mety izy ireo, manosika ny lozisialin'ny mpampiasa mba hisintona ny sakana feno sy ny fifampiraharahana fanairana hanamafisana ny tsy

fitovian-kevitra. Ireo orinasa izay mahazo fandoavam-bola matetika dia mety mbola te-hanodina ny node manokana ho an'ny fiarovana mahaleo tena sy fanamarinana haingana kokoa.

Mampitambatra sy mizara ny sanda

Na dia azo atao aza ny mitantana vola madinika tsirairay, dia sarotra ny manao fifampiraharahana misaraka isaky ny cent amin'ny famindrana. Mba ahafahana mizara sy mitambatra ny sanda, dia misy fidirana sy vokatra marobe ny fifanakalozana. Amin'ny ankapobeny dia hisy fampidirana tokana avy amin'ny fifampiraharahana lehibe kokoa teo aloha na fampidiran-dresaka maromaro mitambatra vola kely kokoa, ary vokatra roa raha be indrindra: ny iray ho an'ny fandoavana, ary ny iray mamerina ny fanovana, raha misy, miverina amin'ny mpandefa.

Marihina fa tsy olana eto ny fan-out, izay iankinan'ny fifampiraharahana amin'ny fifampiraharahana maromaro, ary miankina amin'ny maro hafa izany. Tsy ilaina mihitsy ny maka dika mitovy tanteraka amin'ny tantaran'ny fifampiraharahana.

ny fiainana manokana

Ny maodely banky nentim-paharazana dia mahatratra haavon'ny fiainana manokana amin'ny alàlan'ny famerana ny fidirana amin'ny fampahalalana ho an'ny antoko voakasika sy ny antoko fahatelo azo itokisana. Ny tsy maintsy manambara ampahibemaso ny fifampiraharahana rehetra dia manakana an'io fomba io, saingy mbola azo tazonina ny fiainana manokana amin'ny alàlan'ny fanitsakitsahana ny fikorianan'ny vaovao amin'ny hafa. toerana: amin'ny fitazonana ny fanalahidin'ny daholobe tsy fantatra anarana. Ny vahoaka dia mahita fa misy olona mandefa vola amin'olon-kafa, saingy tsy misy fampahalalana mampifandray ny fifampiraharahana amin'iza na iza. ny varotra tsirairay, ny "kasety", dia avoaka ho an'ny besinimaro, saingy tsy lazaina hoe iza ireo antoko.

Amin'ny maha-firewall fanampiny dia tokony hampiasaina ny mpivady fanalahidy vaovao isaky ny fifampiraharahana mba tsy hampifandray azy ireo amin'ny tompony iombonana. Ny fampifandraisana sasany dia mbola tsy azo ihodivirana amin'ny fifampiraharaham-pidirana marobe, izay tsy maintsy manambara fa tompon'ny tompony ihany ny fampidirana azy ireo. Ny loza dia ny hoe raha miseho ny tompon'ny lakile iray, ny fampifandraisana dia mety manambara fifampiraharahana hafa izay an'ny tompony ihany.

Kajy

Heverintsika ny toe-javatra misy ny mpanafika manandrana mamorona rojo hafa haingana kokoa noho ny rojo marina. Na dia tanteraka aza izany, dia tsy manilika ny rafitra misokatra amin'ny

fanovana tsy misy dikany, toy ny famoronana sanda avy amin'ny rivotra manify na fakana vola izay tsy an'ny mpanafika mihitsy. Ny Nodes dia tsy hanaiky fifampiraharahana tsy mety ho fandoavambola, ary ny nodes marina dia tsy hanaiky mihitsy ny sakana misy azy ireo. Ny mpanafika dia afaka manandrana manova ny iray amin'ireo fifampiraharahany manokana mba hamerenana ny vola laniny vao haingana.

Ny hazakazaka eo anelanelan'ny rojo honest sy ny rojo mpanafika dia azo aseho ho toy ny Binomial Random Walk. Ny hetsika fahombiazana dia ny rojom-pahamarinana izay ampitomboina amin'ny sakana iray, mampitombo ny fitarihany amin'ny +1, ary ny hetsika tsy fahombiazana dia ny rojom-piraketan'ny mpanafika izay ampitomboina amin'ny sakana iray, mampihena ny elanelana amin'ny -1.

Mitovy amin'ny olan'ny Gambler's Ruin ny mety hisian'ny mpanafika iray hahatratra ny tsy fahampiana iray. Eritrereto hoe manomboka amin'ny tsy fahampiana ny mpiloka iray manana trosa tsy voafetra ary milalao fitsapana tsy manam-petra mba hanandramana hahatratra ny fiverenana. Azontsika fikajiana ny mety ho tohiny, na hoe tratran'ny mpanafika ny rojo marina, toy izao manaraka izao[8]:

$$
\begin{aligned}
p &= \text{mety ho hitan'ny node marina ny sakana manaraka} \\
q &= \text{mety hahita ny sakana manaraka ny mpanafika} \\
q_z &= \text{mety ho tratran'ny mpanafika} z \text{misakana ao ambadika}
\end{aligned}
$$

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

Raha jerena ny vinavinay $p > q$, mihena be ny mety hitranga rehefa mitombo ny isan'ny sakana tsy maintsy harahin'ny mpanafika. Miaraka amin'ny fanoherana azy, raha tsy mitsambikina tsara aloha izy, dia ho kely ny vintana ananany rehefa lavo kokoa izy.

Heverintsika izao hoe hafiriana no tokony hiandrasan'ny mpandray ny fifampiraharahana vaovao vao tena azo antoka fa tsy afaka manova ny fifampiraharahana ny mpandefa. Heverintsika fa mpanafika ilay mpandefa izay te hampino ny mpomba azy fa nandoa vola kely izy, avy eo avadiho mba hamerenana amin'ny tenany rehefa tapitra ny fotoana. Hampandrenesina ny mpandray rehefa mitranga izany, saingy manantena ny handefa izany ho tara loatra.

Mamorona mpivady fanalahidy vaovao ny mpandray ary manome ny fanalahidin'ny daholobe ho an'ny mpandefa fotoana fohy alohan'ny hanaovana sonia. Izany dia manakana ny mpandefa tsy hanomana andiana sakana mialoha ny fotoana amin'ny alàlan'ny fampandehanana azy tsy tapaka mandra-pahatongan'ny vintana tsara ho lasa lavitra, dia manatanteraka ny fifampiraharahana amin'izay fotoana izay. Rehefa alefa ny fifampiraharahana dia manomboka miasa mangingina amin'ny rojo mirazotra misy dikan-teny hafa amin'ny fifampiraharahany ilay mpandefa tsy marina.

Ny mpandray dia miandry mandra-panampiana ny varotra amin'ny sakana sy z blocs dia nampifandraisina taorian'izany. Tsy fantany ny tena fivoaran'ny mpanafika, fa raha heverina fa ny

sakana marina dia naka ny salan'isa andrasana isaky ny sakana, ny mety ho fivoaran'ny mpanafika dia fizarana Poisson miaraka amin'ny sanda andrasana:

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

Mba hahazoana ny mety ho azon'ny mpanafika amin'izao fotoana izao, dia ampitomboinay ny hakitroky ny Poisson isaky ny fandrosoana azony atao amin'ny mety ho tratrany manomboka amin'io fotoana io:

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

Mandamina indray mba hisorohana ny famintinana ny rambony tsy manam-petra amin'ny fizarana...

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

Mivadika ho kaody C...

```
#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;
}
```

Amin'ny fampandehanana valiny sasany, dia afaka mahita ny mety hihena be amin'ny 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
```

Famahana ny P latsaky ny 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
```

Fehiny

Nanolotra rafitra ho an'ny fifanakalozana elektronika tsy miankina amin'ny fitokisana izahay. Nanomboka tamin'ny rafitra mahazatra amin'ny vola madinika vita amin'ny sonia nomerika, izay manome fanaraha-maso matanjaka ny fananana, saingy tsy feno raha tsy misy fomba hisorohana ny fandaniana avo roa heny. Mba hamahana izany, dia nanolotra tambajotram-pirahalahiana izahay amin'ny fampiasana porofo-of-asa mba hanoratana tantaram-bahoaka momba ny fifampiraharahana izay lasa tsy azo ampiharina haingana ho an'ny mpanafika mba hiova raha toa ka mifehy ny ankamaroan'ny herin'ny CPU ny nodes marina. Ny tambajotra dia matanjaka amin'ny fahatsorany tsy voarafitra. Ny nodes dia miasa miaraka amin'ny fandrindrana kely. Tsy mila fantarina izy ireo, satria ny hafatra dia tsy alefa any amin'ny toerana manokana ary mila ampitaina amin'ny ezaka tsara indrindra. Ny Nodes dia afaka miala sy miditra amin'ny tambajotra amin'ny sitrapony, manaiky ny rojo porofo momba ny asa ho porofon'ny zava-nitranga tamin'izy ireo. Mifidy

amin'ny herin'ny CPU izy ireo, maneho ny faneken'izy ireo ny sakana manan-kery amin'ny alàlan'ny fanitarana azy ireo ary ny fandavana ny sakana tsy mety amin'ny fandavana ny hiasa amin'izy ireo. Ny fitsipika sy fandrisihana ilaina rehetra dia azo ampiharina amin'ity rafitra marimaritra iraisana ity.

andinin-tsoratra masina

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.