Bitcoin: Sisiṱeme ya tshelede ya eḽekṱhroniki kha munwe na munwe

nga Satoshi Nakamoto 2008/10/31

Tshihumbulelwa

Nḓila ya u rumela munwe na munwe tshelede ya elekṱhroniki i ḓo tendela mbadelo nga inthanethe uri dzi rumeliwe ubva kha muthu muthihi uya kha munwe u fhirisa uya kha zwiimiswa zwa masheleni. Ṱhaluso ya didzhithaḽa i neaho tshipiḓa tsha thandululo, fhedzi mbuelo dzone dzone dzi lozwiwa kharali mufareli mulifhelwa u kha ḓi ṱoḓea u thivhelwa thengo mbili. Ri themendela thandululo kha thaidzo ya thengo mbili hu tshi khou shumisiwa vhuṱumanyi ha munwe uya kha munwe. Zwiifhinga zwa thengiselano ya vhuṱumanyi nga u zwi shandukisela kha uya phanḓa ha thevhekano ya vhuṱanzi ha tshandukiso ya mushumo, u thomiwa ha rekhodo ine i nga si kone u shandukisiwa nga nṱhani ha u dovha hafhu u ita vhuṱanzi ha mushumo. Thevhekano ndapfu a yi nei fhedzi vhuṱanzi ha mutevhe wa zwe zwa vhonala zwi tshi itea, fhedzi vhuṱanzi ha uri ibva kha muḓagasi muhulwane. Sa musi vhunzhi ha muḓagasi wa CPU hu tshi languliwa nga zwishumiswa zwa elekṱhroniki zwine zwa khou shumisana kha ulwa na nethiweke, zwi ḓo ita mutevhe wo lapfaho na vhugevhenga nga inthanethe. Nethiweke nga yone ine i ṱoḓa kudzudzanyele kuṱuku. Milaedza is hashiwa kha nungo dzoṱhe dza mutheo na uri zwishumiswa zwa elekṱhroniki zwi nga ṱuwa na u dovha zwa dzhena kha nethiweke nga u funa, kha u tevhela vhuṱanzi a mutevhe mulapfu wa mushumo kha zwe zwa itea musi zwo ṱuwa.

Marangaphanḓa

Vhubindudzi ha inthanethe vho ḓi tika nga maanḓa kha zwiimiswa zwa masheleni hu tshi shuma sa mufareli mulifhelwa u rumela mbadelo dza elekṱhroniki. Naho sisiṱeme i tshi shuma zwavhuḓi kha thengiso nnzhi, i dovha ya tambula nga u shaya maanḓa kha modela wo ḓi sendekaho nga fulufhelo. Thengiso dzi sa humeli murahu a dzi konadzei, sa musi zwiimiswa zwa masheleni zwi nga si kone u iledza vhupfumedzi ha khuḓano. Mutengo wa vhupfumedzani u engedza ndifho dza thengiselano, ine ya fhungudza thengiselano ya fhasi nga vhuhulwane na u thivhela u konadzea ha thengiselano ṱhukhu na uri hun na ndifho khulwane kha ndozwo i sa koniho u humisela murahu mbadelo kha tshumelo dzi sa humeli murahu. Na khonadzeo dza u humisela murahu, ṱhoḓea dza u fulufhedzea ho phaḓalazwaho. Vharengisi vha tea u vhilaela nga ha vharengi vhavho, nga u vha dina kha u ṱoḓa mafhungo manzhi u fhira ane vha ṱoḓa. Phesenthe inwe ya vhukwila yo tendelwa sa ine i nga si thivhelwe. Hedzi ndifho na u sa ḓivhea ha mbadelo dzi nga nga thivhelwa nga muthu nga u shumisa tshelede nga tshanḓa, fhedzi a huna zwi shumiswa zwire hone zwa u ita mbadelo nga fhethu ha vhudavhidzani hu sina mufareli mulifhelwa.

Zwine zwa ṱoḓea ndi sisiṱeme ya mbadelo ya elekṱhroniki yo ḓi sendekaho nga vhuṱanzi cryptographic hu si vhufareli, hu tendelaho vhalifhelwa vha ṱoḓaho u rengiselana hu sina ṱhoḓea ya mufareli mulifhelwa. Thengiselano dzine dzi sa koni u humela murahu nga khomphyutha dzi ḓo tsireledza vharengisi kha vhukwila, na maitele zwishumiswa zwa mufareli mulifhelwa dzine dzi nga itiwa zwo leluwa u itela u tsireledza vharengi. Kha heli bambiri, themendela thandululo kha thaidzo ya u renga luvhili nga u shumisa tshifhinga tsha seva tsho phaḓalzwaho kha munwe na munwe kha u ita vhuṱanzi ha khomphyutha kha thengiselano dza matevhekanele. Sisiṱeme yo tsireledzea arali zwishumiswa zwa vhukuma zwa elekṱhroniki zwi shumiasnaho kha u langula muḓagasi wa CPU u fhira zwinwe zwigwada zwa zwishumiswa zwa elekṱhroniki zwi shumisanaho u ṱhasela.

Thengiselano

Ri ṱalusa tshelede ya elekṱhroniki sa mutevhe wa ṱhaluso ya didzhithaḽa. Mulangi munwe na munwe u rumela tshelede kha munwe nga u saina didzhithaḽa ya u shandukisa thengiselano dzo fhiraho na khii ya tshitshavha kha mulangi a tevhelaho na u ṱanganyisa hezwi kha mafhedziselo a khoini. Mubadeli u tea u seduzlusa tsaino u ṱoḓisisa mutevhe wa vhulangi.

Thaidzo yone ndi ya uri mubadeli ha nga koni u ṱolisisa uri munwe wa vhalangi ha ngo renga luvhili khoini. Thandululo yo ḓoweleaho ndi u ḓivhadza vhuvhusi vhu fulufhedzeaho, kana mukango une wa sedzulusa thengiselano inwe na inwe kha thengo mbili. Nga murahu ha thengiselano inwe na inwe, masheleni a tea u humiseliwa murahu kha mukango u itela khoini ntswa na uri ndi masheleni fhedzi o itiwaho ubva kha mukango a fulufheliwa kha u sa renga luvhili. Thaidzo kha heyi thandululo ndi ya uri khombo ya ndozwo kha sisiṱeme yoṱhe ya tshelede yo ḓi sendeka kha khamphani i langulaho mulango, kha thengiselano inwe na inwe i dzhenaho khayo, u fana na bannga.

Ri ṱoḓa nḓila ya uri mubadeli a ḓivhe uri vhalanguli vha murahu a vhongo saina thengiselano inwe na inwe mathomoni. Kha nḓivho yashu, thengiselano ya mathomoni ndi yone yo teaho, zwino a rina ndavha nga ndingo dzo itiwaho kha thengo mbili. Nḓila nthihi ya u khwaṱhisedza u savha hone ha thengiselano ndi u ḓivha nga thengisealano dzoṱhe. Kha modela wo ḓi sendekaho nga mukango, mukango u ḓivha nga ha thengiselano dzoṱhe kha u khetha u swika phanḓa[1], na uri ri ṱoḓa sisiṱeme kha vhadzheneleli uri vha tende kha ḓivhazwakale nthihi ya thengo kha zwe zwa ṱanganezwa. Mubadeli u ṱoḓa vhuṱanzi kha uri tshifhinga tshinwe na tshinwe tsha thengiselano, vhunzhi ha zwi shumiswa zwa elekṱhroniki zwo tenda uri ndi ya u thoma u ṱanganezwa.

TShifhinga tsha seva

Thandululo ine ra i themndela i thoma nga tshifhinga tsha seva. Tshifhinga tsha seva tshi shuma nga u dzhia tshigwada tsha hash tsha zwishumiswa kha tshifhinga na u huwelela hash yo phaḓaladziwaho, sa gurannḓa kana Usenet post[2-5]. Tshifhinga tshi sumbedza uri data itea uvha hone nga hetsho tshifhinga, zwi khagala, uri u itela ri dzhene kha hash. Tshifhinga tshinwe tshinwe

tshi katela tshifhinga tsho no fhiraho kha hash yatsho, ya u thoma mutevhe, na tshifhinga tshinwe na tshinwe hafhu kha u khwaṱhisedza zwinwe zwire phanḓa.

Vhuṱanzi ha mushumo

U ṱhaphudza tshifhnga tsha seva tsho kovhekanyiwaho kha maitele a munwe uya ha munwe, ri ḓo ṱoḓa vhuṱanzi ha sisiṱeme ya mushumo I fanaho na Hashcash ya Adam Back[6], u fhirisa gurannḓa kana milaedza ya Usenet. Vhuṱanzi ha mushumo hu katela ṱholisiso ya vhundeme kha uri musi hu tshi shukisiwa, sa SHA-256, hash i thoma nga nomboro ya dziro biti. Mushumo u angaredzaho ndi tshisumbavhuḓiandisi kha nomboro ya dziro biti i ṱoḓeaho ine i nga ṱoḓisiwa nga u ita hash nthihi.

Kha nethiweke ya tshifhinga tshashu, ro ṱhaphudza vhuṱanzi ha mushumo nga u engedza tshifhinga tshithihi kha kuvhumbele u swika kha vhundeme vhu tshi waniwa vhu nea kuvhumbele kwa hash hune ha dziro biti dzi ṱoḓeaho. Musi vhuḓidini ha CPU ho ḓi nekedzela kha u fusha ṱhoḓea ya vhuṱanzi ha mushumo, tshivhumbeo tshi nga si shandukiswe nga nṱhani ha u dovholola mushumo. Sa nga murahu ha kuvhumbele ku no tevhelana nga murahu hatsho, tshanduko ya kuvhumbele kwa mushumo hu katela u dovholola zwivhumbeo zwoṱhe nga murahu.

Vhuṱanzi ha mushumo hu tandulula thaidzo ya u sumbedza zwifanyiso zwa vhunzhi ha u itwa ha tsheo. Kharali vhunzhi ho ḓi sendeka kha -IP-aḓiresi nthihi na -khetho-nthihi, i nga shandukisiwa nga munwe na munwe ane a kona u kovha IPs nnzhi. Vhuṱanzi ha mushumo ndi ha ndeme kha CPU-nthihi-khetho-nthihi. Vhunzhi ha tsheo dzo imelelwa nga mutevhe mulapfu, ine vhuṱanzi vhunzhi vhuhulwane vha vhuḓidini ha mushumo ho itiwaho. Kharali vhunzhi ha muḓagasi wa CPU u tshi languliwa nga zwishumiswa zwa elekṱhronik zwi fhulufhedzeaho, mutevhe u fuflufhedzeaho u ḓo hula nga u ṱavhanya na u ṱavhanyesa ha mutevhe u ṱaṱisanaho. U vhuyedzedza tshivhumbeo tsho fhiraho, tshigevhenga tshi tea u dovholola vhuṱanzi ha mushumo wa tshivhumbeo na zwivhumbeo zwoṱhe nga murahu hatsho wa dovha u wana na u fhira mushumo u fulufhedzeaho wa tshishumiswa tsha elekṱhroniki. Ri ḓo sumbedza hu si kale kha uri khonadzeo dza tshigevhenga tshi ongolowaho kha u fara tshisumbavhuḓiandisi sa tshivhumbeo tshi vhuyelelaho tsho engedzea.

U lifha u engedzeha luvhilo lwa zwivhumbakhomphyutha na u fhambana dzangalelo kha zwishumiswa zwa elekṱhroniki zwi shumaho tshifhinga tshinzhi, vhuṱanzi ha mushumo u konḓaho hu wnala nga u sundulusa mbalotshikati yo livhaho nomboro ya mbalotshikati ya tshivhumbeo nga awara. Kharali dzi tshi itiwa nga luvhilo, u konḓa hu a engedzeha.

Nethiweke

Nḓila dza u shumisa nethiweke ndi dzi tevhelaho:

1. Thengiselano ntswa ndi u hasha kha noudzu dzoṱhe.
2. Noudu inwe na inwe i kuvhanganya thengiselano ntswa kha tshivhumbeo.
3. Noudu inwe na inwe i shuma kha u wana u konḓa kha vhuṱanzi ha mushumo kha tshivhumbeo tshayo.
4. Musi noudu i tshi wana vhuṱanzi ha mushumo, i hasha tshivhumbeo tsha noudzu dzoṱhe.
5. Noudu dzi tendela tshivhumbeo fhedzi kharali thengiselano dzoṱhe khadzo dzi dza vhukuma na dzi sa athu shumisiwa.
6. Noudzu dzi sumbedza thendelo kha buḽoko nga u shumela u ita buḽoko i tevhelaho kha tshaine, hu tshi khou shumisiwa hash kha tshivhumbeo tsho tendelwaho sa hash yo fhiraho.

Noudzu dzi dzulela u ṱhogomela mutevhe wo lapfaho kha nthihi ya vhukuma na u isa phanḓa kha u shumela u dzi engedza. Kharali noudzu mbili dzi tshi hasha vesheni kha tshivhumbeo tshi tevhelaho nga khathihi, dzinwe noudzu dzi nga ṱanganedza nthihi kana inwe u thoma. Kharali zwo ralo, dzi shuma kha nthihi ya thoma yp ṱanganezwaho, fhedzi u tsireledza tshipiḓa tshinwe kharali dzavha ndapfu. Vhuṱumanyi vhu ḓo vunḓea musi vhuṱanzi ha mushumo hu tshi wanala na tshipiḓa tshithihi tshi tshivha tshilapfu; dzi noudzu dze dzavha dzi tshi khou shuma kha tshipiḓa tshinwe tshi ḓo shanduka kha nthihi ndapfu.

Khasho ya thengiselano ntswa a yongo tea u swikelela noudzu dzoṱhe. Kharali dzo swikelela noudzu nnzhi, dzi tea u dzhena kha tshivhumbeo phanḓa ha vhulapfu. Khasho dza tshivhumbeo dzi a konḓelela kha milaedza yo laṱiwaho. Kharali noudzu i sa ṱanganedzi tshivhumbeo, i ḓo tshi humbela musi musi tshi tshi ṱanganedza tshivhumbeo tshi tevhelaho na u ṱhogomela tshithihi tsho hangwiwaho.

Ṱhuṱhuwedzo

Nga buthano, thengiselano ya u thoma kha buḽoko ndi thengiselano yo khetheaho ine ya thoma tshelede ntswa i languliwaho mufhaṱi wa tshivhumbeo. Hezwi zwi engedza ṱhuṱhuwedzo kha noudzu kha u tikedza nethiweke, na u nea nḓila ya u thoma u phaḓaladza khoini sa musi hu sina vhulangi ha vhukati kha u dzi ita. U engedzeha ho khwaṱhaho kha ṱhanganyelo ya u sa shanduka kha masheleni maswa ndi u vhambedza maini wa musuku kha u kovhekana. Kha vhuimo hashu, ndi tshifhinga tsha CPU na muḓagasi u phaḓalazwaho.

Ṱhuṱhuwedzo i nga badelwa nga mbadelo ya thengiselano. Vhundeme ha nnḓa kha thengiselano ndi ṱhukhu kha vhundeme ha nga ngomu, phambano ndi mbadelo ya thengiselano ine ya engezwa kha vhundeme ha ṱhuṱhuwedzo kha buḽoko ire na thengiselano. Musi hu saathu u sumbezwa nomboro ya masheleni uri o dzhena kha phaḓalazwo, ṱhuṱhuwedzo i nga shandukiswa tshoṱhe kha mbadelo ya thengiselano na u savha na mbadelothangeli.

Ṱhuṱhuwedzo i nga kona u thusa u ṱuṱuwedza noudzu uri dzi fhulufhedzehe. Kharali mudzia vhupangwa hu kona u kuvhangana muḓagasi munzhi wa CPU u fhira noudzu dzoṱhe dzi fhulufhedzeaho, utea u khetha kha u shumisa kha u fhura vhathu nga utswa murahu mbadelo

dzawe, kana u i shumisa u ita masheleni maswa. U tea u zwi wana zwi tshi vhuyedza u tevhedza milayo,sa milayo i no mufha khoini nnzhi maswa u fhira vhathu vhoṱhe vho ṱanganyisiwa, u fhira u nyadza sisiṱeme na vhungoho ha lupfumo lwawe.

U dzhiulula tshikhala tsha disiki

Musi thengiselano ya zwino kha masheleni a ḓo vhulungiwa nga fhasi buḽoko dzo eḓanaho, thengiselano yo itiwaho i sa athu u laṱiwa u vhulunga tshikala kha disiki. U thoma hezwi hu songo kwashiwa buḽoko ya hash, thengiselano dzi a shandukisiwa kha muri wa Merkle [7][2][5], na mudzi fhedzi wo katelwaho kha buḽoko ya hash. Dzi buḽoko zwa kale zwo vhekanyiwaho nga urwa madavhi a muri. Tshanduko dza nga ngomu a dzina ṱhoḓea ya uri dzi vhulungiwe.

Ṱhoho ya buḽoko i shayaho thengiselano i ḓovha 80 baithi. Kharali ri tshiri zwivhumbeo zwi itiwa tshifhinga tshoṱhe tsha mithethe ya 10, 80 baithi * 6 * 24 * 365 = 4.2MB nga nwaha. Sa musi dzisisiṱeme ya khomphyutha dzi ḓoweleaho u rengisa na RAM ya 2GB ubva 2008, na mulayo wa Moore u humbulela nyaluwo ya zwino ya 1.2GB nga nwaha, fhethu ha u vhulunga a hongo tea uvha thaidzo naho kharali ṱhoho ya buḽoko i ḓo vheiwa kha fhethu ha ekhiṱhironiki ha u vhulunga.

Ṱhanzielaṱhoḓisiso yo leluwaho ya mbadelo

Zwi a konadzea u ṱolisisa mbadelo hu songo shumisiwa nethiweke yoṱhe ya noudu. Mushumisi u ṱoḓa fhedzi u vhea khophi ya ṱhoho dza tshivhumbeo kha mutevhe mulapfu wa vhuṱanzi ha mushumo, ine a nga i wana nga u vhudzisa noudu dza nethiweke u swika a tshi fushea uri una mutevhe mulapfu, na u wana davhi ḽa Merkle ḽi no ṱangana na thengiselano kha tshifhinga tsha nga ngomu tsha tshivhumbeo. A nga si kone u sedza thengiselano nga ene mune, fhedzi nga u i ṱanganya ba fhethu ha mutevhe, u ḓo vhona uri noudu ya nethiweke yo i tenda, na buḽoko ya dzhenisiswa nga murahu ha u isa phanḓa na u khwaṱhisa uri nethiweke yo i tendela.

Naho zwo ralo ṱhanzielaṱhoḓisio ndi ya vhukuma kharali noudzu dza vhukuma dzi ḓo langula nethiweke, fhedzi zwi a konḓesa kharali nethiweke i tshi kundiwa nga ḽibvemu. Musi noudzu dza nethiweke dzi tshi ḓo kona u ṱanziela thengiselano nga vhone vhane, nḓila dzo leluwaho i nga fhuriwa nga thengiselano ya ḽibvemu lwa tshifhinga tshilapfu tshine ḽibvemu ḽi nga kona u isa phanḓa na u kunda nethiweke. Nḓila nthihi ya u tsireledza hezwi ndi u tendela tsivhudzo ubva kha noudzu dza nethiweke musi dzi tshi vhona buḽogo i savhi yone, i ita uri softhiwee ya mushumisi i dawunilode buḽoko yoṱhe na u tsivhudza dzi thengiselano kha u khwaṱhisedza u sa shuma zwavhuḓi. Mabindu ane a ṱanganedza mbadelo dza tshifhinga tshoṱhe ine I nga ḓi kona u ṱoḓa u shumisa noudzu dzadzo kha tsireledzo yo ḓi imisaho nga yoṱhe na ṱhanzielaṱhoḓisiso u ṱavhanyaho.

U ṱanganyisa na u fhambanya vhundeme

Naho zwi tshi konadzea u dzudzanya masheleni u eṱhe, zwi a konḓa u ita thengiselano dzo fhambanaho kha tshelede inwe na inwe kha yo rumeliwaho. U tendela vundeme uri vhufhandekanyiwe na u ṱanganyiso, thengiselano i na zwa nga ngomu na zwa nga nnḓa. Kanzhi huvha na nga ngomu huthihi ubva kha thengiselano khulwane ya murahu kana ha nga ngomu hunzhi hu ṱanganyisaho tshikalo tshiṱuku, na nga nnḓa huvhili: nthihi ya mbadelo na nthihi ya u huma, kharali i hone, u humela murahu kha muremeli.

Zwi tea u nwaliwa uri fan-out, hunethengiselano dzi ḓi sendeka nga thengiselano dzo vhalaho, na uri hedzo thengiselano dzo ḓi sendeka nga dzinwe nnzhi nnzhi, a si thaidzo fhano. A huna ṱhoḓea dza u dzhia khophi nthihi ya thengiselano dza murahu.

Tshidzumbe

Modela wa bannga wo ḓoweleaho u swikelela vhuimo vha tshidzumbe nga u fhungudza u wanala ha nḓovho kha vhathu vhare ngomu na mufareli mulifhelwa. Ṱhoḓea dza u anḓadza thengiselano dzoṱhe kha tshitshavha zwi thivhela heyi nḓila, fhedzi tshidzumbe tshi nga kona uvha hone nga u thutha I tshimbila ha mafhungo nga ngomu ha hunwe fhethu: nga u vhea khili kha tshitshavha lwa tshiphiri. Tshitshavha tshi nga kona u vhona munwe u khou rumela tshelede kha munwe, fhedzi vha shaya nḓivho ya u kwamana na thengiselano ya munwe. Hezwi zwifana na vhuimo ha nḓivho yo bvisiwaho nga kha zwa masheleni, hune tshifhinga na tshikalo tsha thengiso dza muthu muthihi, "theiphi", iya phaḓalazwa kha tshitshavha, fhedzi hu sa sumbedziwe vhathu.

Sa tsireledzo yo engedziwaho, phere dza khili ntswa dzi tea u shumiswa kha thengiselano inwe na inwe u itela uri dzi songo kwamana na mulangi o ḓoweleaho. Hunwe u kwamana a hu hanedzei na thengiselano dzo vhalaho dza nga ngomu, zwiine zwa sumbedza uri zwa nga ngomu zwavho zwovha zwi tshi languliwa nga mulanguli uyo. Khombo ndi ya uri mulanguli wa khili a sumbedziwe, u kwamana hu nga sumbedza dzinwe thengiselano dzine dzavha dza mulanguli uyo.

Mbalelo

Ri tea u ṱhogomela vhuimo ha mufhura ane a kho lingedza u ita nḓila ya u ṱavhanya u fhira ane a ṱoḓa u ita i no fhulufhedzea. Naho hezwi zwo bvelezwa, a zwi iti uri sisiṱeme i bvule kha tshanduko dzinwe vho, sa u u wana vhundeme muyani kana u dzhia tshelede ye yavha i si ya mufhura. Noudzu dzi nga si tendele thengiselano dzi savhi dzone sa mbadelo, na uri noudzu dzi fhulufhedzeaho dzi nga si tendele buḽoko dzire nadzo. Mufhuri a nga kona fhedzi u shandukisa thengiso dzawe u itela u dzhia murahu tshelede ye a i shumisa.

Mbambe vhukati ha tshaine ya ngoho na tshaine ya muṱhaseli dzi nga dzudzanyea sa ṱhanganyo ya tshivhangalala. U bvelela ha tshaine ya vhukuma hu engezwa nga buḽoko nthihi, i engedzeha nga +1, na uri u balelwa tshaine ya muṱhaseli i ḓo engedziwa nga buḽoko nthihi, ya fhungundza tshikhala nga -1.

Khonadzeo dza uri muṱhaseli a swikelele ubva kha u fhenyiwa zwi a vhambedziwa na u fhungudzea ha thaidzo ya mugembuli. Kha riri mugembuli are na u thoma ha khredithi i sina vhukono kha u fhenyiwa na u tamba nomboro I sa gumi kha ndingo u itela u swikelela breakeven. Ri nga kona u vhalela khonadzeo ine a swikelela breakeven, kana uri muṱhaseli u swikelela na tshaine dza vhukuma, sa zwitevhelaho[8] :

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

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

Uya nga khumbulelo yashu ya uri $p > q$, khonadzeo dzi a fhungudza tsumbavhuḓiandisi sa nomboro ya dzi buḽoko ine muṱhaseli u tea u swikelela nyengedzedzo. Sa izwi khonadzeo dzi sa imi naye, kharali a songo candela phanḓa hu kha ḓivha na tshifhinga, khondzeo dzawe dza uvha ṱhukhu sa hezwi a tshi salela murahu.

Zwino ri vho ṱhogomela uri ndi tshifhinga tshingafhani kha uri muthu wa thengiselano ntswa tshine a ṱoḓa u ima zwi saathu u ḓivhea uri murumeli a nga si shandukise thengiso. Ri humbulela uri murumeli ndi muṱhaseli ane a ṱoḓa muthu a tende uri o badelwa lwa tshifhinga, nga zwenezwo a shandukele kha u badela murahu nga murahu ha tshifhinga tsho fhiraho. muṱanganedzi u ḓo vhudziwa musi zwi tshi itea, fhedzi murumeli u fhulufhela uri hu si tshena tshifhinga.

Muṱanganedzi u ḓo ita phere ntswa dza khili na u nea khili ya tshitshavha kha murumeli a saathu u saina. Hezwi zwi thivhela murumeli kha u lugisa tshaine ya dzibuḽoko phanḓa ha tshifhinga, zwenezwo nga u ita thengiselano nga tshifhinga tshenetsho. Hezwi thengiselano yo itiwa, murumeli a sa fhulufhedzei a thoma u shuma tshiphirini kha tshaine ya pharaḽeḽe ine yavha na vesheni ya thengiselano yawe.

Muthu u ima u swikela thengiselano I tshi dzhenisiwa kha buḽoko na dzibuḽoko dza z dzo ṱanganyisiwa nga murahu hadzo. Ha ḓivhi tshifhinga tshone tsha mvelaphaḓa ye muṱhaseli a ita, fhedzi nga u humbulela uri buḽoko dza vhukuma dzo dzhia tshifhinga lavheleliwaho kha buḽoko, mvelaphanḓa ya muṱhaseli I ḓovha u kovha ha Poisson na vhundeme vho lavheleliwaho:

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

U wana khonadzeo muṱhaseli a nga kona u swikelela zwino, ri engedza tshikalo tsha Poisson

khaṱhanganyelo ya mvelaphaṋda ye avha a tshi ḓo itiwa nga khonadzeo dza uri a swikelele kha heyo phoithi:

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

U dzudzanya habe u thivhela ṱhanganyo i sa fheli kha u kovha…

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

U shandukisela kha khoudu ya 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;
}
```

U shumisa mvelelo, ri kona u vhona khonadzeo dzi tshi fhungudzea lwa tshisumbavhuḓiandisi 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
```

U tandulula P ṱhukhu kha 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
```

Magumo

Ro themendela sisiṱeme ya mbadelo nga eḽekṱhronik i songo ḓi sendeka nga fhulufhelo. Ro thoma nga mutheo wo ḓoweleaho wa dzi khoini dzo itiwaho ubva kha tsaino ya didzhithaḽa, ine ya nea ndangulo yo khwaṱhaho, fhedzi ivha i songo fhelela musi i tshi shaya nḓila ya u thivhela mbadelo mbili. U tandulula hezwi, ro themendela nethiweke ya muthu na muthu hu tshi shumisiwa ṱhanziela ya mashumo u itela u rekhoda ḓivhazwakale ya dzi mbadelo ine ya ṱavhanya uvha u sa konadzea ha khomphyutha u itela muṱhaseliwa u shandukisa kharali noudzu dza vhukuma dzi langula vhunzhi ha muḓagasi wa CPU. Nethiweke yo khwaṱha kha u sa dzudzanyea ho leluwaho. Noudzu dzi shuma dzoṱhe nga tshifhinga tshithihi na u sa shumisana zwiṱuku. A huna ṱhoḓea ya uri dzi waniwe, sa musi milaedza i songo dzula hunwe fhethu na uri i ṱpḓa u swikisiwa kha mutheo wa vhuḓidini. Noudzu dzi nga ṱuwa na u humela kha nethiweke nga u tou funa, u tenda tshaine vhuṱanzi sa ṱhanziela kha zwe zwa itea musi dzo ṱuwa. Vha khetha nga muḓagasi wa CPU, u ombedzela thendelo ya dzibuḽoko dza vhukuma nga u shumela u engedza na u hanedza dzibuḽoko dzi si dza vhukumanga u hanedza u shuma nadzo. Ṱhoḓea dza mulayo na ṱhuṱhuwedzo i nga khwaṱhisiwa nga hezwi zwishumiswa.

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.