Bitcoin: Sisteme ya Khexe ya Tintangha ya Xielekitironiki

hi Satoshi Nakamoto 2008/10/31

Nkomiso

Vhexini ya tintangha ya khexe ya xielekitroniki yi ta pfumelela tihakelo ta le ka inthanete ku va ti rhumeriwa ku suka eka munhu wun'we ku ya eka wun'wana handle ko tirhisa nhlangano wa swa timali. Minsayino ya xidijitali yi lulamisela hi xiphemu xa xintshuxo, kambe mimbuyelonkulu ya lahleka loko munhu wa vunharhu a ha laveka ku siveka ku tirhisa mali hi ka mbirhi. Hi ringanyeta leswaku xintshuxo xa ku tirhisa mali hi ka mbirhi I ku tirhisa netiweke ya tintangha. Netiweke ya tithiranzekixini ta timestamps hi ku ti hexa eka nketani leyi yaka emahlweni ya vumbhoni bya ntirho, ti endla rhikhodo leyi nga ta ka yi nga cinciwi handle ka rhikhodo ya vumbhoni bya ntirho. Nketani yo leha ngopfu a yi nge tirhi ntsena tanihi vumbhoni bya ntirho bya timhangu leti nga endleka, kambe vumbhoni bya leswaku matimba lamakulu ma CPU. Ntsena loko majorothi ya matimba ya CPU ya lawuriwa hi tinodi leti tirhaka kun'we ku hlasela netiweke, ti ta vumba nketani yo leha ngopfu no rhangela vahlaseri. Netiweke hi yoxe yi lava xivumbeko xitsongo. Mahungu ma haxiwa hi ndlela yo antswa, naswona tinodi ti nga sukela kumbe ti joyina netiweke hi ku tsakela, no amukela vumbhoni bya ntirho byo leha bya nketani tanihi vumbhoni bya leswi nga humelela loko ti nga ri kona.

Masungulo

Ku sungula eka Inthanete swi ya hi minhlangano ya swa timali leyi phakelaka vukorhokeri eka munhu wa vunharhu loyi a nga tshembheka ku tirhana na tihakelo ta xielekitironiki. Hambi loko sisteme yi tirha kahle eka tithiranzekixini tin'wana, ya ha tikeriwa hi leswi yi nga swi tekelela swo vevuka ka endlelo leri landzaka vutshembhi. Tithiranzekixini leti nga thleleriki endzhaku a ti koteki, hikuva minhlangano ya swa timali a yi koti ku ahlula minkatetano. Tihakelo ta minkanetano ya tithiranzekixini yi tlakukile, yi hunguta sayizi ya thiranzekixini ya minimamu na ku tsema tithiranzekixini letintsongo, naswona ku na hakelo yikulu ya ku lahlekeriwa ka vukorhokeri bya ku thlerisela endzhaku tihakelo. Laha swi kotekaka ku thlerisela endzhaku, ku laveka ka ku tshembha ka hangalaka. Vaxaviselani va fanele ku xiya tikhasitama ta vona, ku va nyika mahungu mo tala lama a va nga ta ma tsakela ku ma kuma. Phesente yo karhi ya vuxisi ya amukeliwa tani hi leyi nga papalatekiki. Tihakelo leti na tihakelo leti nga tiyisisiwangiki ti nga papalatiwa eka munhu hi ku tirhisa mali yo khomeka, kambe a ku na endlelo leri tirhaka ra ku endla tihakelo hi tichanele ta vuhlanganisi handle ka munhu loyi a nga tshembheka.

Leswi swi lavekakak i sisteme ya tihakelo ta xielekitironiki eka vumbhoni bya cryptografiki ku nga ri

ku tshembha, ku pfumelela vanhu vambirhi lava swi tsakelaka ku hakelala hi ku kongoma ku nga laveki ku tshembha ka munhu wa vunharhu. Tithiranzekixini leti landzaka sisteme ya khomphyuta a ti koti ku thlerisela endzhaku loko muxavisi loyi a sirheleriweke a xava eka vaxisi, maendlelo ya ntolovelo ya ka simekiwa ku sirhelela vaxavi. Eka phepha leri, hi ringanyeta leswaku xintshuxo xa xiphiqo xo hakela hi ka mbirhi hi ku tirhisa netiweke ya tintangha yi hangalasiwa eka sevha ya timestamp ku endlela ku endla vumbhoni bya khomphyuta bya ndlela yo landzelelana ka tithiranzekixini. Sisteme yi hlayisekile ntsena loko tinodi ti tshembheka eka ku hlangaleta matimba yo tala ma CPU ku tlula ku tirhisana na ntlawa wa tinodi to hlasela.

Tithiranzekixini

Hi hlamusela khoyini ya xielekitironiki tanihi nketani ya minsayino ya xidijitali. N'winyi wun'wana na wun'wana u hundzisela khoyini eka munhu la landzelaka hi ku sayina xidijitali eka thiranzekixini leyi nga hundza na khiya ra mani na mani ra n'winyi la landzelaka loko leswi swi hlanganisiwa emakumu ka khoyini. Muhakeli a nga tiyisisa minsayino ku tiyisisa nketani ya vun'winyi.

Xiphiqo hi leswaku muhakeri a nge tiyisisi leswaku vinyi a va hakelanga hi ka mbirhi hi khoyini. Xintshuxo xo toloveleka I ku tivisa matimba ya lexikarhi lama nga tshembheka, kumbe minti, leyi chekaka thiranzekixini yin'wana na yin'wana eka ku hakela ka mbirhi. Endzhaku ka thiranzekixini yin'wana na yin'wana, khoyini yi faneleyi fanele ku vuyela eka minti ku humesiwa ka khoyini yintshwa, naswona I khoyini leyi humesiwaka ntsena hi ku kongoma ku suka eka minti leyi tshembhiwaka ku ka yi nga hakerisi hi ka mbirhi. Xiphiqo hi xintshuxo lexi hi leswaku xiyimo xa sisteme hinkwayo ya mali xi le mavokweni ya khamphani leyi fambisaka minti, nakona thiranzekixini yin'wana na yin'wana yi fanele ku hundza hi le ka yona, ku fana na bangi.

Hi lava ndlela ya leswaku muhakeli a tiva leswaku vin'yi va nkarhi lowu nga hundza a va sayinelanga tithiranzekixini ta le masunguleni. Hi xikongomelo xa hina, thirathzekixini ya le masunguleni hi yona leyi hlayiswaka, kutani a hi na mhaka na ku ringeta ka le ndzhaku ko hakela hi ka mbirhi. Ndlela yin'we ntsena yo tiyisisa ku nga ri kona ka thiranzekixini I ku tiva hi tithiranzekixini hinkwato. Eka muxaka lowu landzaka minti, minti a yi ti tiva tithiranzekixini hinkwato naswona yo teke xiboho xa leswaku ku fika yihi ku sungula. Ku fikelela leswi handle ka munhu loyi a nga tshembheka, tithiranzekixini ti fanele ku tivisiwa eka mani na mani[1], naswona hi lava sisteme ya vateka xiave ku pfumela matimu man'we ya odara leyi nga amukeriwa. Muhakeli u lava vumbhoni bya bya leswaku hi nkarhi wa thiranzekixini yin'wana na yin'wana, tinodi to hlaya a ti pfumelelana leswaku a yi sungule yi amukeriwa.

Sevha ya Timestamp

Xintshuxo lexi hi xi ringanyetaka xi sungula hi sevha ya timestamp. Sevha ya timestamp yi tirha hi ku teka hexe ya buloko ya minchumu leyi nga ta rhekhodiwa hi nkarhi naswona yi hangalasiwa hi hexe, ku fana na le ka phephahungu kumbe poso ya Usenet post[2-5]. Timestamp yi komba

leswaku datara a yi ri kona nkarhi lowu nga hundza eka hexe ya yona, ku endlela ku maka nketani, leyi vumbekaka endzhaku ka timestamp yin’wana na yin’wana leyi nga yi rhangela.

Vumbhoni bya Ntirho

Ku simeka sevha ya timestamp leyi hangalakeke eka ntangha - ntangha, hi ta lava ku tirhisa sisteme ya vumbhoni bya ntirho byo fana na bya Adam Back's Hashcash[6], ku nga ri phephahungu kumbe topiso ta Usenet posts. Vumbhoni bya ntirho byi katsa ku xopaxopa nkoka lowu nga hexiwa, ku fana na SHA-256, hexe yi sungula hi nomboro ya tibiti ta tandza. Ntirho wa nhlayo xikarhi wa laveka eka ku vona nomboro ya tibiti ta tandza leyi lavekaka naswona yi nga tiyisisiwa hi ku tirhisa hexe yin’we.

Eka netiweke ya hina ya timestamp, hi simeka vumbhoni bya ntirho hi ku ngetela eka buloko ku fikela nkoka wu kumeka lowu nyikaka hexe ya buloko leyi lavaka tibitsi ta tandza. Loko se ku ringetela ka CPU ku ndlandlamuxiwile ku endlela ku enerisa vumbhoni bya ntirho, buloko a yi nge cinci handle ko endla ntirho nakambe. Tanihi leswi tibuloko ta le ndzhaku ti nga hakiwa endzhaku ka yona, ntirho wo cinca buloko wu ta katsa ku endla nakambe ka tibuloko leti nga endzhaku.

Vumbhoni bya ntirho byi thlela byi lulamisa xiphiqo xo kuma vuyimeri bya majorithi yo teka swiboho. Loko majorithi a yi ya hi ku adirese yin’we ya IP I vhoti yin’we, a swi ta cinciwa hi munhu wun’wani na wun’wani loyi a phakelaka ti IP to tala. Vumbhoni bya ntirho kahhlekahle i CPU-yin’we- vhoti-yin’we. Xiboho xa majorithi xi yimeriwa hi ketani yin’we yo leha eka hinkwato, leyi nga na vumbhoni bya ntirho lebyikulu lebyi vekiseke eka yona. Majorithi ya matimba ya CPU ya lawuriwa hi tinodo to tshembheka, nketani yo tshembheka yi ta kula hi xihatla no rhangela tiketani leti phikizanaka na yona. Ku antswisa buloko leyi nga hundza, muhlaseri u ta fanela ku endla hi vuntshwa vumbhoni bya ntirho wa buloko na tibuloko hinkwato leti nga endzhaku ka yona naswona leti nga ta yi khoma na ku hundza ntirho wa tinodi to tshembheka. Hi ta komba endzhaku leswaku swi nga endleka leswaku muhlaseri wo nonoka a khoma tibuloko leti nyamalalaka tanihi tibuloko leti ngeteliwaka.

Ku riha eka ku tlakuka ka rivilo ra hardware na ntsakelo wo hambanana wa ku tsutsuma ka tinodi hi ku famba ka nkarhi, vumbhoni byo tika ka ntirho byi va kona hikwalaho ka mpfuka-xikarhi wa ku famba ka thagete ya nhlayo ya tibuloko hi awara. Loko ti makeka hi xihatla, ku va na ku tlakuka ka ku tikeriwa.

Netiweke

Magoza mo fambisa netiweke hi lama landzelaka:

1. Thiranzekixini tintshwa ti hangalasiwa eka tinodi hinkwawo.

2. Nodi yin’wana na yin’wana yi hlengeleta tithiranzekixini tintshwa ti ya eka buloko.
3. Nodi yin’wana na yin’wana yi triha hi ku vumbhoni-bya-ntirho byo tika bya buloko ya rona.
4. Loko nodi yi kuma vumbhoni-bya-ntirho, yi hangalasa buloko eka madingu hikwawo.
5. Tinodi ti amukela buloko ntsena loko tithiranzekixini hinkwato leti nga eka rona ti ri ta ntiyiso naswona ti nga se tirhisiwa.
6. Tinodi ti kombisa ku amukela ka tona ka buloko hi ku tirhana no endla buloko yintshwa eka nketani, hi ku tirhisa hexe ya buloko leyi amukeriweke ku fana na le ka hexe leyi nga hundza.

Tinodi ti tekela enhlokweni nketani leyo leha ngopfu minkarhi hinkwayo ku va yona yo lulama naswona yi ya emahlweni yi ndlandlamuxa. Loko tinodi timbirhi ti haxa tivhexini to hambanahambana eka buloko leyi landzelaka hi nkarhi wun’we, tin’wana tinodi ti nga ha kuma yin’we kumbe yin’wana ku sungula. Hi ndlela yaleyo, ti tirha eka yo sungula leyi ti yi kumaka. Kambe ti hlayisa rhavi lerin’wana loko ro tshika ri leha. Thayihe yi ta tsemeka loko vumbhoni bya ntirho lebyi landzelaka byi kumeka naswona rhavi rin’we ri sungula ku leha, tinodi leti a ti tirha eka rhavi lerin’wana ti ta cincela eka lero leha.

Vuhaxi bya tithiranzekixini tintshwa a swi bohi ku va ti fiki eka tinodi hinkwato. Ntsena loko ti fikelela tinodi to tala, ti ta nghena eka buloko ku nga ri khale. Vuhaxi bya buloko na byona bya amukela mahungu lama nga siyiwa. Loko nodi yi nga kumi buloko, yi ta yi kombela loko yi yi amukela buloko leyi landzelaka no vona leswaku yi lahle yin’we.

Xihlohloteli

Hi ntwanano, thiranzekixini yo sungula eka buloko i thiranzekixini yo hlawuleka leyi sungulaka khoyini yintshwa ya muendli wa buloko. Leswi swi tatisa xihlohloteli leswaku tinodi ti seketela netiweke, no lulamisela hi ndlela yo sungula ku hangalasa tikhoyini eka vuhangalasi, tanihi leswi ku nga riki na vulawuri bya le xikarhii byo tihumesa. Ku tatisa ka ntsengo wa tikhoyioni tintshwa i analogo ya van’watimayini va nsuku lava ndlandlamuxaka swipfuno ku tatisa eka nsuku eka vuhangalasi. Eka hina, i nkarhi wa CPU na gezi leswi ndlandlamukaka.

Xihlohloteli xi nga thlela xi kuma mali eka hakelo ya thiranzekixini. Loko nkoka wa leswi humaka swa thiranzekixini wu ri wuntsongo eka nkoka wa leswi nghenaka, ku hambana ka hakelo ya thiranzekixini loku ngeteriwaka eka nkoka wa xihlohloteli xa buloko leyi nga na thiranzekixini. Loko se nomboro leyi vekiweke ya tikhoyini yi nghenisiwa eka vuhangalasi, xihlohloteli xi nga cinca tihakelo hinkwato ta thiranzekixini naswona ti nga hakerisiwi na xibalo.

Xihlohloteli xi nga pfuna ku hlohlotela tinodi ku tshama ti tshembhekile. Loko muhlaseri loyi a nga na makwanga a kota ku vumba matimba ya CPU ku tlula tinodi hinkwato, u ta fanela ku hlawula exikarhi ko yi tirhisa ku endla vuxisi eka vanhu hi ku yiva tihakelo ta yena kumbe hi ku endla tikhoyini tin’wana tintshwa. U fanele ku kuma leswaku swa vuyerisa ku tlanga hi milawu, milawu leyi n’wi vuyerisaka hi tikhoyini tintshwa ku tlula ta lavan’wana ti hlanganile, ku tlula ku tekela ehansi sisteme na ku xiviri xa rifuwo ra yena.

Ku Koxa nakambe Xivandla xa Disk

Loko se thiranzekixini eka tikhoyini yi celeriwile ehansi ka tibuloko, tithiranzekixini ta le mahlweni ka tona ti nga lahliwa ku hlayisa xivandla xa disk. Ku pfuna eka leswi handle ko tlula hexe ya buloko, tithiranzekixini ti hexiwa eka Merkle Tree [7][2][5], rimintsu ri katsiwa ntsena eka hexe ya buloko. Tibuloko ta khale ti nga hlangananisiwa hi ku tlandlunula marhavi ya nsinya. Tihexe ta le ndzeni a ti lavi ku hlayisiwa.

Heda ya buloko leyi nga riki na tithiranzekixini yi ta va kwalomu ka 80 wa tibayiti. Loko ho buloko yi endliwa timinete tin'wana na tin'wana ta 10, 80 wa tibayiti * 6 * 24 * 365 = 4.2MB hi lembe. Tisisteme ta khomphyuta ti xavisiwa ti ri kwalomu ka 2GB ya RAM hi 2008, naswona Moore's Law ku vhumbha ku kulaka nkarhi wa sweswi ka 1.2GB hi lembe, xitoreji a xi fanelanga ku va xiphiqo hambi leswi tiheda ta buloko ti faneleke ku tsundzukiwa.

Ku Tiyisisa ka Tihakelo loku Olovisiweke

Swa koteka ku tiyisisa tihakelo handle ko fambisa nodi ya netiweke hinkwayo. Mutirhisi u lava ntsena ku hlayisa khopi ya tiheda ta buloko ya vumbhoni bya ntirho bya nketani yo leha, leyi nga khomaka tinodi ta netiweke ya nketani yo leha, no kuma rhavi ra Merkle leri hlanganisaka thiranzekixini na buloko ya timestamped ya yona. A nge koti ku cheka thiranzekixini hi yexe, kambe hi ku yi hlanganisa no yi veka eka nketani, a nga vona leswaku nodi ya netiweke yi yi amukerile, naswona tibuloko leti nga ngeteriwa endzhaku ka yona ti tiyisisa ku ya emahlweni leswaku netiweke yi yi amukerile.

Loko swi ri tano, ku tiyisisa i ndlela yo tshembheka ntsena loko tinodi to tshembheka ti lawula netiweke, kambe ti le ka nxungeto loko netiweke yi tluliwa hi matimba hi muhlaseli. Loko tinodi ta netiweke ti nga kota ku tiyisisa thiranzekixini hi toxe, ndlela yo olova yi nga yengiwa hi tithiranzekixini ta vuxisi ta muhlaseli ntsena loko muhlaseli a ya emahlweni a hlula netiweke hi matimba. Qhinga rin'we ro sirhelela ehenhla ka leswi ku ta va ku amukela swilemuxo swa tinodi loko ti kuma buloko leyi nga tirhiki, leswi endlaka leswaku software ya mutirhisi yi dawuniloda buloko yi helerile na ku lemuxa hi tithiranzekixini ku tiyisisa ku hambana. Bindzu leri amukelaka tihakelo hi xitalo ra ha lava ku tsutsumisa tinodi ta rona ku kuma vusirheleri byo tiyimela na ku tiyisisa ka xihatlka.

Ku Hlanganisa na ku Hambanisa Nkoka

Hambiloko swi nga ta ka swi nga olovi ku khoma khoyini ha yin'we, a swi nge kombi vuthlari ku hambanisa thiranzekixini ya sente yin'wana na yin'wana leyi hundzisiwaka. Ku pfumelela nkoka wa ku hambana na ku hlangana, tithiranzekixini ti na ti iniphuti na ti outphuti leti andzeke. Ku tala ku va

na inphuti yin’we eka thiranzekixini yo leha leyi nga hundza yi andzisiwa na mintsengo leyitsongo ya tiimphuti timbirhi: yin’we ya tihakelo, leyin’wana ya ku cinca loku vuyelelaka, loko ko va na ku vuyela eka murhumeri.

Swi fanele ku lemukiwa leswaku fan-out, laha thiranzekixini yi yaka hi tithiranzekixini to hambanahambana, na tithiranzekixini leti yaka hi to tala, a hi xiphiqo laha. A ku laveki ku hetisa khopi leyi nga yoxe ya matimu ya thiranzekixini.

Xihundla

Endlelo ro banga ra ntoilovelo ri fikelela levhele ya xihundla hi ku hunguta mahungu eka lava nga na xiave na munhu wa vunharhu loyi a tshembhekeke. Nkoka wa ku tivisa tithiranzekixini hinkwato erivaleni a swi katsi endlelo leri, kambe xihundla xi nga ha va kona hi ku tsema nkhuluko wa mahungu ku va wu humelela: hi ku hlayisa swikhiya swa mani na mani swi tumberile. Mani na mani a nga vona leswaku un’wana u rhumele wun’wana ntsengo wo karhi, kambe handle ka mahungu lama hlanganisaka thiranzekixini eka wun’wana na wun’wana. Leswi swi fana na levhele ya mahungu lama humesiwaka hi mixaviselano ya xitoko (stock exchanges), laha nkarhi na sayizi ya mubindzuri wun’we, "thepi", yi vekiwaka erivaleni, kambe ku nga hlayiwi leswaku ivamani lava nga na xiave.

Tanihi xisirheleri xa firewall, phere ya khiya yi fanele ku tirhisiwa eka thiranzekixini yin’wana na yin’wana ku endlela leswaku yi nga hlanganisiwi na n’winyi wa ntolovelo. Ku hlanganisa kun’wana a ku papalateki na tithiranzekixini ta andziso, leswi paluxaka leswaku inphuti ya tona i ya n’winyi wun’we. Nxungeto hi leswaku n’winyi wa khiya wa paluxiwa, ku hlanganisa ku nga paluxa tithiranzekixini letin’wana leswaku i ta n’winyi wun’we.

Mikhakhuleto

Hi languta xiyimo lexi muhlaseli a nga ringetaka ku endla nketani yin’wana leyi nga tshembheka yo hatlisa ku tlula tin’wana. Hambi loko leswi swi fikeleriwa, a swi humeseli sisteme ehandle ku cinciwa hi muhlaseli, ku fana na ku timbuluxa nkoka wa moya wo vevuka kumbe ku teka mali leyi a yi nga ri ya muhlaseli. Tinodi a ti nge amukeli thiranzekixini leyi nga riki yona tanihi hakelo, tinodi to tshembheka a ti nge amukeli buloko leyi nga na tona. Muhlaseli a nga ringeta ku cinca yin’we hi tithiranzekixini ta yena ku vuyisa mali leyi a ha ku yi tirhisaka.

Mphikizano exikarhi ka nketani yo tshembheka na nketani ya muhlaseli swi na swihlawulekisi swa Binomial Random Walk. Mhangu ya ku humelelai nketani yo tshembheka leyi ndlandlamuxiwaka hi buloko yin’we, ku engetela hi +1, na ku hluleka ma mhangu loku nga nketani ya muhlaseli loku ndlandlamuxiwaka hi buloko yin’we, ku hungutiwa ka vangwa hi -1.

Muhlaseli swa endleka a kuma leswi nga sala swa xiphiqo xa Gambler's Ruin. A hi nge mugembuli loyi a nga riki na swo xava swo tala u sungulela hansi ku tlanga hi tinomboro leti nga riki na makumu eka ku ringeteka ku fika nhlayo yo fana na ya le masunguleni. Hi nga khakhuleta ku ringanyeta leswaku a nge fikeleli nhlayo yo fana na ya le masunguleni, loko muhlaseli a hlangana na nketani yo tshembheka, hi ndlela leyi[8] :

p = vukoteki bya nodi yo tshembheka ku kuma buloko leyi landzelaka ya bloko ya
q = nga ringana na ku va muhlaseli a kuma leswaku buloko ya
q_z = swa endleka muhlaseli a nga pfuki a fikelerile eka tibuloko ta z endzhaku ka z blocks be

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

Nyika ku ringanyeta ka hina ka leswaku $p > q$ swa endleka ti ya ehansi tanihi leswi nhlayo ya tibuloko leti muhlaseli a nga ti fikelelaka yi tlakuka. Ku ri na ti odo ehenhla ka yena, loko a nga tluleli emahlweni hi nkateko ka ga ri na nkarhi, tichansi ta yena ti sungula ku va tintsongo hikuva u salela endzhaku.

Sweswi hi swi teka ku muamukeri wa thiranzekixini yintshwa u fanele ku yima loko a nga se rhumea hikuva thiranzekixini a yi nge cinci. Hi swi teka ku muhlaseli loyi a lavaka ku endla leswaku muamukeri a tshembha leswaku u n'wi hakerile nkarhi nyana, kutani swi cinca ku hakela ku vuya eka yena endzhaku ka ku va nkarhi wu hundzile. Ku amukela ku ta lemukisiwa loko ku humelela, kambe murhumeli u tshembha leswaku nkarhi wu hundzile.

Muamukeri u ta endla khiya rintshwa no nyika khiya ra mani na mani eka murhumeri endzhaku ka nkarhi nyana ku nga se sayiniwa. Leswi swi sivela leswaku murhumeli a lulamisa nketani emahlweni ka tibuloko ta nkarhi hi ku tirhana na yona ku ya emahlweni, kutani a endla thiranzekixini eka nkarhi wolowo. Loko se thiranzekixini yi rhumeriwile, ku nga tshembheki ka murhumeri ku sungula ku tirha hi xihundla eka nketani yo longoloka leyi nga na vhexini yin'wana ya thiranzekixini ya yena.

Muamukeli u rindza ku fika thiranzekixini yi ngeteliwa eka buloko naswona tibuloko ta z ti hlanganisiwile endzhaku ka yona. A nga swi tivi leswau ntsengo wo lulama i wo ya emahlweni ku va muhlaseli a wu endla, kambe swi tekiwa leswaku buloko yo tshembheka yi teke nhlayo-xikarhi ya nkarhi lowu languteliweke hi buloko, ku ya emahlweni loku nga endliwa hi muhlaseli, vuswikoti bya muhlaseli byi ta hangalasiwa tanihi Chefu leyi nga na nkoka lowu languteliweke:

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

Ku kuma ku ehleketelela ka muhlaseli loku a nga ku fikelelaka, hi fanele ku andzisa Chefu ya le makumu ka ntsengo wun'wana na wun'wana wa ku ya emahlweni loku a nga ku endlaka hi ku ehleketelela ka leswaku u ta fikelela eka poyinti yaleyo:

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

Ku lulamisa nakambe ku papalata nkomiso wa ncila lowu nga riki na makumu wa vuhangalasi…

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

Ku cinciwa ka Khodi 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;
}
```

Ku tirhaniwa na mimbuyelo yin'wana, hi vona ku ya ehansi ka xiseketelo xa 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
```

Ku tirhana na P ehansi ka 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
```

Mahetelelo

Hi ringanyetile sisteme ya tithiranzekixini ta xielekitironiki handle ka tshembho. Hi sungule hi rimba ra ntolovelo ra tikhoyini leti nga endliwa hi misayino ya xidijitali, handle ko lulamisela hi vulawuri bya vun'winyi, kambe ya hela handle ka ndlela yo hakela hi ka mbirhi. Ku lulamisa leswi, hi bumabumela ku tirhisiwa ka netiweke ya tintangha hi ku tirhisa vumbhoni bya ntirho ku rhikhoda matimu ya thirhanzekixini ya mani na mani leyi hatlaka yi endla leswaku muhlaseli a cinca loko tinodi to tshembheka ti lawula matimba ya majorothi ya CPU. Netiweke i ndlela yo olova leyi nga vumbiwangiki. Tinodi ti tirha xikan'we hi vuhlanganisi. A ti bohi ku boxiwa, hikuva mahungu a ma fambisiwi ku ya eka ndhawu yo karhi naswona ma fanele ku dilivhariwa hi ndlela yo antswa. Tinodi ti nga tshika kumbe ti joyina nakambe netiweke hi ku tsakela ka tona, ku amukela nketani ya vumbhoni bya ntirho wa leswi nga humelela loko ti ngfa ri kona. Ti vhota na matimba ya CPU, ti hlamusela ku amukela ka ton aka tibuloko ta xiviri to ti ndlandlamuxa no alela tibuloko ta xiviri hi ku alela ntirho wa tona. Milawu leyi lavekaka na tihakelo swi nga boheleriwa eka Endlelo lera ntwanano.

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.