I-Bitcoin: Imali ye-intanethi yabarhwebi

nguSatoshi Nakamoto 2008/10/31

Ingabula-zigcawu

Imali eluhlobo olungangxengwanga lweletronikhi yabarhwebi iyabavumela abantu ukuba babhatalane besebenzisa i-intanethi bengakhangange baye ebhankini okanye kwiziko leenkonzo zezimali. Umzila ebihamba kuwo kwi-intanethi uluncedo, kodwa eyona nzuzo yokusebenzisa olu hlobo lorhwebo iye ilahleke ukuba kusafuneka umntu ongomnye othembekileyo ukuba ibe nguye ekufuneka athintele inkqatho yokusetyenziswa kwemali ye-bitcoin izihlandlo ezibini. Sicebisa ukuba ukusombulula le ngxaki yokusetyenziswa kabini sisebenzisa ubuchwepheshe bonxibelelwano babarhwebi abasebenzisanayo. Obu buchwepheshe buza kubhala iinkcukacha zonke zonaniselwano kwisixokelelwano esinamakhonkco-lwazi buze buziphawule ngophawu oluthile oluyimfihho, uphawu olo luza kuba bubungqina bomsebenzi owenziweyo obungenakutshintshwa nangubani na ngaphandle kokuba lo msebenzi wenziwe kwakhona. Esi sixokelelwano samakhonkco olwazi asisebenzi njengobungqina omsebenzi owenziweyo kunye nobulandelelana ngawo kuphela koko nobokuba olu lwazi luphuma emathunjini ekhompyutha engenakuqhekezwa yonakaliswe. Ukuba nje iikhompyutha ezinolu lwazi zilawula kwizitishi ezincinci ezingasebenzi kunye zizama ukuyonakalisa, ziza kuvelisa isixokolelwano solwazi eside kangangokuba sinokwahlula nabo bafuna ukusonakalisa. Esi sixokelelwano solwazi sona nje sisodwa asifuni bubuxhaka-xhaka bungako bobuchwepheshe. Imiyalezo ipapashwa phantsi kononophelo oluphezulu, futhi nezi zitishi zincinci (ii-nodes) zisetyenziselwa ukusilawula zingamana ziphuma ziphinde zibuye ngokuthanda kwazo, futhi naxa zibuya ziza kufika umsebenzi owenziweyo ngoku bezingekho ukho qha ke ngoko umthamo wawo umkhulu kakhulu ngoku.

Intshayelelo

Urhwebo oluqhutywa nge-intanethi sele luxhomekeke kumaziko ezezimali odwa ngoku wona asebenza njengequmrhu lesithathu elithembakeleyo lokwamkela nokukhupa iintlawulo ezenziwa nge-intanethi. Nangona le nkqubo isebenza kakuhle kwiimeko ezininzi, kodwa isasekelwe kwinto enye ekukuthembeka. Awukwazi ukwenza intlawulo engenakuphinda ijikwe, kuba amaziko ezimali ayayazi into yokuba kuza kufuneka engenelele rhoqo xa kukho uxambuliswano. Indleko zokuhlalela iindibano zokusombulula iimbambano zinyusa umrhumo ohlawulwayo ngokuphatha izimali, into leyo eyenza kubenzima ukuthumela imali encinci, oko ke kubangela ukuba kungabikho lula ukuthumela nje imalana encinci engabalulekanga nganto, futhi baninzi abalahlekelwayo yile ngxaki yokungakwazi ukuthumela imali engenakuphinda ijikwe yeenkonzo nazo ezingajikwayo xa sele zenziwe. Xa kukho amathuba okuba into eyenziweyo ingaphinda ijikwe, loo nto inyanzelisa ukuba kukhokeliswe phambili ukuthembana. Abarhwebi kufuneka babalumkele abathengi, babacele ukuba banike ubucukubhede obuninzi ngaphezu kobu bebenokufunwa ukuba

bekungenje. Buyaziwa bona ubuqhetseba ukuba bakuhlala bukho futhi wamkelwe umyinge othile wabo. Ezi ndleko kunye neentlawulo ezinokuphindwa zijikwe zingathintelwa ngokuthi kusetyenziswa imali ebambekayo, kodwa ayikho indlela yokwenza oku kungekho qela lithenjiweyo kula ananiselanayo.

Into efunekayo yindlela yokuhlawula imali esebenzisa i-intanethi kuze kuthunyelwe ubungqina ngendlela efihlakeleyo endaweni yokuxhomekeka kumba wokuthembana kuphela, into leyo eza kuvumela ukuba bantu ababini bakwazi ukuhlawulana ngqo bodwa kungekho mfuneko yomnye umntu wesithathu othembekileyo. Izimali ezibhatalweyo ekungelulanga ukuzijika nge-intanethi zikhusela abarhwebi abathengisayo ekubeni ngamaxhobo obuqhetseba, futhi iinkqubo zokumana kuphicothwa ii-akhawunti zikhusela abarhwebi abathengayo. Kule ngxelo yophando siza nesisombululo kule ngxaki yokusetyenziswa kwe-bitcoin izihlandlo ezibini kusetyenziswa ubuchwepheshe bekhompyutha bokuphawula iinkcukacha zeentlawulo ngendlela ezilandelelene ngayo iintlawulo obuthi bukhuphe nobungqina ngekhompyutha obuchaza kanye indlela iintlawulo ezilandelelene ngayo. Le nkqubo ikhuseleke kuphela ukuba izitishi ezincinci zogcino-lwazi (ii-nodes) ezilawula amathumbu ekhompyutha zilawula ubuninzi boqobo nolwazi olukwikhompyutha zibambisene ngendlela engaphezulu kwale inokusetyenziswa ngamanye amaziko amancinci wona ahlasela aze onakalise ulwazi olukwiikhompyutha.

Iintlawulo

Ingqekembe e-elektronikhi siyichaza njengomzia ohanjwe lunaniselwano kwi-intanethi. Umntu ngamnye uthumela i-bitcoin komnye nge-intanethi ngokuthi atyikitye umzila wale ntlawulo yangaphambili kunye neqhosha likawonke-wonke lalo mntu ulandelayo ize yonke le nto idityaniswe. Lo ubhatalayo uye aqinisekise wonke umzila we-intanethi ohanjwe yile ntlawulo ngokuthi ajonge ukuba ngoobani na abebethatha inxaxheba kolu naniselwano, ngamanye amazwi iinkcukacha zabo bonke abanikazi bangaphambili bale bitcoin.

Ingxaki ke inye yeyokuba lo ubhatalwayo akakwazi ukuzifumana iinkcukacha zokuba omnye wabo bebekhe bangabanikazi bale ngqekembe inye khange ayisebenzise na ngaphambili. Isisombululo esilula kule ngxaki kukuba kubekho elinye iqumrhu elithembekileyo, okanye iziko lokwenza imali, eliza kuphica zonke iintlawulo ezenziweyo ukujonga ukuba khange isetyenziswe kwenye into ngaphambili le bitcoin. Emva kwentlawulo nganye, i-bitcoin kufuneka ibuyiselwe kumzi wokwenza imali ukuze wona ukhuphe imali entsha, ngolo hlobo ke iza kuba yimali evela kwiziko lokwenza imali kuphela eza kuthathwa ngokuba ithembakele kwaye khange isetyenziselwe enye into ngaphambili. Ingxaki ngesi sisombululo kukuba lonke olu hlobo lorhwebo luza kuxhomekeka kule nkampani yenza imali, yonke intlawulo yenziwe yiyo, kanye ngolu hlobo iibhanki zenza ngalo.

Sifuna indlela eza kwenza lo mntu uhlawulayo azi ukuba lo mntu ebengumnikazi wale mali ngaphambili khange ahlawule ngayo kwenye into. Kolu phando lwethu, sijonga la ntlawulo yokuqala ngqa, asizihluphi ngamalinge ebesandula ukwenziwa okusebenzisa le mali inye kabini.

Inye indlela yokwazi ukuba khange kwenziwe linge lamgunyathi, kukuphanda ngazo zonke iintlawulo ebezenziwe. Kule nkqubo yokusetyenziswa kweziko lokwenza imali, eli ziko belizazi zonke iintlawulo ezenziweyo yaze yalilo nelikwaziyo ukubona ukuba yeyiphi eyokuqala intlawulo. Ukuze sikwazi ukwenza oku kungekho qumrhu lesithathu lithembakeleyo, zonke iintlawulo zonaniselwano kufuneka zibhengezwe esidlangalaleni [1], kufuneka kukho inkqubo apho abantu abachaphazelekayo bezakuvumelana ngendlela ezilandelelene ngayo iintlawulo zonaniselwano ukususela kweyokuqala ukuza kutsho kweyokugqibela. Lo mntu uhlawulwayo ufuna ubungqina bokuba ngethuba kusenziwa intlawulo, uninzi lwamaziko alawulo ikhompyutha ayavumelana ukuba iyaqala ukwenziwa.

Ubuxhaka-xhaka bokugxim fiza ixesha

Isisombululo esiza naso siqala ngobuxhaka-xhaka bekhompyutha obugxim fiza ixesha. Obu buxhaka-xhaka busebenza ngokuthi kuthathwe isixa samasuntswana olwazi aza kugxim fizwa luze olu phawu lusetyenziselwe ukugxim fiza amasuntswana lupapashwe kwiqonga lokusasaza ulwazi kuwonke-wonke elifana nephephandaba okanye ulwazi olupapashwa kwi-intanethi [2-5]. Esi sixhobo sokugxim fiza ulwazi siluphawula njengobungqina bokuba olu lwazi luyaziwa. Isigxim fizo ngasinye siba nesigxim fizo sangaphambili kwi-hash yaso, into leyo ethi yenze isixokelelwano, apho isigxim fizo sangaphambili kufuneka sihambelana nesi sitsha silandelayo.

Ubungqina bomsebenzi owenziweyo

Ukuze kuqaliswe inkqubo yobuxhaka-xhaka bokugxim fiza ngabantu abasebenza kunye, kuza kufuneka kusetyenziswe inkqubo ekhokelisa ukubaluleka kobungqina efanayo ne-Hashcash ka-Adam Back [6], endaweni yephephandaba okanye ulwazi olupapashwe kwi-intanethi. Ubungqina bomsebenzi owenziweyo buquka ukukhuphela ixabiso lolwazi obeselenziwe i-hash, ngokusebenzisa into efana ne-SHA-256, ize i-hash iqale ngesuntswana lolwazi elingu-0. Mninzi kakhulu umsebenzi onokwenziwa ngesuntswana lolwazi elingu-0 oku kungaqinisekiswa ngokuthi kusetyenziswe i-hash enye.

Kwinkqubo yethu yokugxim fiza siye sisebenzise inkqubo yobungqina bomsebenzi owenziwiyo ngokwandisa inani elisetyenziswa kanye lalo msebenzi (i-nonce) kwibloko kude kufumaneke inani eliza kunika uphawu olufihlakeleyo lwebloko kude kufumaneke ulwazi olwaneleyo olungu-0 lwamasuntswana olwazi . Yakuba i-CPU isetyenziwe ukuze ikwazi ukubonisa ubungqina bomsebenzi owenziweyo, ibloko ayinakutshintshwa kungakhange kuphindwe kuqalelwe phantsi. Ngenxa yokuba iibloko ethubeni ziye zidityaniswe zibe sisixokolelelwano, ukutshintsha ibloko nganye kuza kufuna ukuba kuqaliswe phantsi umsebenzi ngokutsha kwenziwe iibloko ngokutsha.

Ubungqina bomsebenzi owenziweyo busombulula nengxaki yokubona izimvo zabantu xa iinkqubo

yokuthatha isigqibo ixhomekeka kwisininzi. Ukuba isininzi besibalwa ngokuba kuthiwe idilesi ye-IP nganye mayivote kube kanye, le ndlela yokubala isininzi ingaqhatheka lula ngokuba umntu abe nee-IP ezininzi. Inkqubo ekhokelisa ubungqina bomsebenzi owenziweyo yona ithi kuvotwa ngokwe-CPU. Isigqibo sesininzi siza kubonwa ngezona bloko zininzi, ezinobungqina bomsebenzi omninzi owenziweyo. Ukuba ubuninzi be-CPU bulawulwa kwizitishi ezincinci (ii-nodes) ezithembekileyo, kuza kukhula isixokolelwano esingenazikroba esikhawulezileyo ngesantya esiza kubangaphezulu kwesezinye izixokelelwano esikhuphisana nazo. Ukuze akwazi ukwenza ubuqhetseba kwibloko engaphambili, lo nqalintloko wenza umonakalo kuza kufuneka aqale abe nobungqina bomsebenzi ubuwenziwe kule bloko kunye nezinye iibloko ezilandela yona aze akhawuleze ngesantya esiphezulu esiza kumenza ade agqithe kwesi asebenza ngaso amazikwana amancinci alawula olu rhwebo. Siza kubonisa kwalapha ethubeni ukuba mancinci kakhulu amathuba okuba isela elingenileyo kuba lifuna ukwenza umonakalo lihambe ngesantya esiza kwenza ukuba likwazi ukude liyokufika entloko, kule ndawo sele kukuyo ngoku.

Ukuzama ukuthintela umonakalo onokwenziwa zezi khompyutha zintsha zihamba ngesanya esiphezulu kakhulu kunye nokuphelelwa ngumdla nokuzinikela kwabo basebenza kwezi zitishana zincinci zilawulwayo, umthamo olindelekileyo nofunekayo wubungqina bomsebenzi owenziweyo uza kutshintshwa. Ukuba isantya sinyuswe kakhulu, kuza kuba nzima nokuba kwenziwe umonakalo ngonqali-ntloko.

Isixokelelwano seekhompyutha

Amanqanaba okuphatha isixokelelwnao seekhompyutha ngala alandelayo:

1. Iintlawulo zonaniselwano ezintsha zipapashwa kuzo zonke izitishi ezincinci zolwazi.
2. Isitishi esincinci ngasinye siqokelela iinkcukacha zentlawulo entsha siyifake kwibloko.
3. Isitishi esincinci ngasinye sizama ukukhangela ubungqina bomsebenzi owenziweyo obusitheleyo kwibloko nganye.
4. Xa isitishi esincinci sifumana ubungqina bomsebenzi owenziweyo, siyabupapasha kuzo zonke izitishi ezincinci zolwazi.
5. Isitishi siyamkela ibloko kuphela xa zonke iintlawulo zisemthethweni futhi ingezizo ezemali esele isetyenzisiwe ngaphambili.
6. Izitishi ezincinci zolawulo-lwazi zicaca ukuba ziyamkele ubloko ngokuthi ziqalise ukwakha ibloko elandelayo, zisebenzisa i-hash yebloko esele yamkelwe njenge-hash yangaphambili.

Izitishi ezincinci zolawulo-lwazi zizithatha ngokuba azinazimpazamo izixokelelwano zeebloko ezizezona zide kwaye ziyaqhuba zizama ukuzandisa. Ukuba izitishi ezibini zipapasha iibloko ezimbini ezingafaniyo ngexesha elinye, izitishi zingafumanisa nokuba yeyiphi ibloko kuqala. Xa kunjalo, ziza kusebenzisa le ifunyenwe kuqala, zize ziyibeke elugcinweni enye ukulungiselela xa kunokwenzeka ikhule, nayo ibe sisixokelelwano eside. Le ngxaki iza kusonjululwa xa kufunyanwa ubungqina obulandelayo bomsebenzi owenziweyo size esinye isixokelelwano sibe side ngaphezu kwesinye, izitishi ebezisebenza kwesinye isixokelelwano besilisetyana ziza kutshintshela kwesi

sixokelelwano side.

Upapasho lweentlawulo zonaniselwano ezintsha akunyanzelekanga ukuba lufike kuzo zonke izitishi ezincinci. Ukuba nje lufike kwizitishi ezincinci ezininzi, luza kufika kwibloko kungekudala. Inkqubo yokupapasha yeebloko iyakwazi ukuyibona imiyalezo ethunyelwe ngempazamo. Ukuba isitishi esincinci asifumani bloko, siza kuyicela xa sifumana ibloko elandelayo size sibone ukuba kukho ibloko esingayifumenanga.

Umvuzo

Ngokomthetho, intlawulo yokuqala kwibloko yintlawulo yonaniselwano eyodwa ethi izale i-bitcoin entsha yengcali leyo iqale ibloko. Oku kungumvuzo okhuthaza izitishi ukuba zincedise abarhwebi, kwaye yindlela yokuqalisa ukukhupha ii-bitcoin ziye ebantwini abafuna ukurhweba ngazo, njengoko kungekho qumrhu lingundlunkulu olawula olu hlobo lorhwebo. Ukuthi gqolo kusongezwa i-bitcoin ezintsha kufana nabasebenzi-mgodini abomba igolide ngenjongo zokuba iye ebantwini abarhweba ngayo. Kolu uhlobo lorhwebo, yikhompyutha nombane izinto ezisebenzayo.

Umvuzo ungafumaneka nakwimirhumo yokwenza iintlawulo zonaniselwano. Ukuba ixabiso lomsebenzi wokuyila i-bitcoin lingaphantsi kwixabiso elifunyanwayo ngokurhweba ngayo, le mali itsaliweyo yile yokwenza intlawulo yonaniselwano. Zakuba ziyiliwe zaze zakhutshelwa abantu abarhwebayo ii-bitcoin ezilinani elithile elicetywe kwangaphambili, umvuzo ungayimirhumo yokwenza iintlawulo zonaniselwano ungadibani nokudibana nomrhumo oxhomekeka kumaxabiso ezinto ngelo xesha.

Lo mvuzo ungenza nezitishi ezincinci zithembakale. Ukuba unqali-ntloko ofuna ukwenza umonakalo uyakwazi ukuba ne-CPU enesantya esingaphezulu kuzo ezi zezitishi ezincinci zolawulo-lwazi, kuza kunyanzeleka ukuba akhethe ukuba enze ubuqhetseba bokuthi ebe ebantwini la ntlawulo ebesele eyenzile okanye enze i-bitcoin ezintsha. Angakhetha ukuba angaphuli mthetho kuba le mithetho inceda kwayena ngenxa yokuba uza kufumana ii-bitcoin ezininzi ngaphezu komntu wonke, kunokuba aphazamise ubuxhaka-xhaka bokuqhuba olu rhwebo kunye nemeko apho ubutyebi bakhe nabo ebubeka emngciphekweni.

Ukusebenzisa isithuba esincinci kwikhompyutha

Yakuba intlawulo yokugqibela yenziwe, yaza yafakwa ezincwadini, iintlawulo ebezenziwe phambi kwayo zingacinywa ukwenzela ukuba zingatyi indawo. Oku kwenziwa ngokuthi kusetyenziswa i-Merkle Tree [7][2][5] ngolu hlobo luboniswe ngezantsi apho kushiywa ingcambu yodwa ye-hash yebloko. Iibloko ezindala ziye zisongwe ngokuba kuqhawule amasebe alo mthi. Ii-hash ezingaphakathi akunyanzelekanga ukuba zigcinwe. s

Ibloko eyintloko ekungakhange kwenziwe ntlawulo kuyo ingazi-bytes ezingama-80. Ukuba

siyavumelana ukuba ibloko yenziwe rhoqo emva kwemizuzu eli-10, i-80 bytes * 6 * 24 * 365 = 4.2MB ngonyaka. Njengokuba, ukususela ngo-2008, sekuthengiswa iikhompyutha ezine-RAM eyi-2GB futhi xa sijonga kwinkqubo kaMoore yoqikelelo, i-RAM yeekhompyutha iza kukhula nge-1.2GB ngonyaka, ke ngoko iikhompyutha azizikuba nangxaki ngendawo yokugcina iifayile ezinkulu nokuba ibloko eziyintloko zingagcinwa. s

Indlela eLula yokuChaza iNtlawulo

Ungakwazi ukuziqinisekisa iintlawulo ungakhange ude ungene kuzo zonke izitishi ezincinci zogcino-lwazi (ii-nodes). Umntu kufuneka nje agcine ikopi yeebloko ezizintloko zesona sixokelelwano side sobungqina bomsebenzi owenziweyo, anokuzifumana ngokujonga kwizitishi zonke zogcino-lwazi ade naye aqiniseke ukuba ngenene eso sesona sixokelelwano side sobungqina bomsebenzi owenziweyo, aze ajonge kula Merkle isebe elihambelana nentlawulo ekwibloko egximfizwe iinkcukacha. Nangona engazikukwazi ukuzijongela ngokwakhe intlawulo eyenziweyo, kodwa ngokuyijonga ukuba ibisuka kweyiphi indawo kwesi sixokelelwano angasibona isitishi esincinci ibingene ngaso, kunye nebloko ezongezelelweyo emva kwaso emva kokuba ivumile ukuba yamkelwe yikhompyutha.

Ngamanye amazwi, inkqubo yokuqinisekisa intlawulo ungayithemba ukuba nje izitishi ezincinci zogcino-lwazi izizo ezilawula ubuxhaka-xhaka obusetyenziselwa urhwebo, kodwa iye ithande ukugungqa xa kuvele oonqali-ntloko abafuna ukwenza umonakalo kuyo. Nangona izitishi zogcinolwazi zikwazi ukuqinisekisa ngokwazi ukuba iintlawulo zezokwenyani ngenene, le ndlela ilawulwayo yokuhlawula ingaphazanyiswa zintlawulo zomgunyathi ezenziwe ngoonqalintloko abafuna ukwenza umonakalo ukuba nje bangakwazi ukuyoyisa baze bayilawule. Enye indlela yokuthintela oku kukuyithathela ingqalelo imiyalezo engxamisekileyo emifutshane ethunyelwa zizitishi zogcino-lwazi xa zibona ibloko yomgunyathi, zize ngolo hlobo ziyalele umntu ukuba akhuphele yonke ibloko kunye neentlawula azikhonjiswayo ukuchaza ukuba ikhona ngenene into engahambi kakuhle. Amashishini afumana iintlawulo angafuna ukuba asebenzise ezawo iinkqubo ezizimeleyo nezikwaziyo ukuqinisekisa ngokukhawuleza.

Ukudibanisa nokwahlula ixabiso

Nangona unokwazi ukusebenza nge-bitcoin uwedwa, akunakubalula ukwenza intlawulo yesenti nganye xa ubhatala. Ukuze imali yahlulwe okanye idityaniswe, iintlawulo ziyaphuma ezinye ziyangena. Kuqhele ukuba kubekho intlawulo enye engenayo esisixa esikhulu esivela kwintlawulo enkulu yangaphambili okanye iintlawulo ezininzi ezingenayo zemali encinci, kuze kubekho ezimbini eziphumayo: enye iyintlawulo eqhelekileyo, ize enye ibe yintsalela ebuyiswayo, ukuba ikhona kulowo ebeyithumele.

Kufuneka wazi ukuba ukuzisasaza iintlawulo, apho intlawulo ixhomekeke kwiintlawulo ezahlukeneyo, zize zona ezo ntlawulo zixhomekeke kwezinye ezininzi, akuyongxaki. Akukho mfuneko yokuba ube nekopi ezimeleyo yazo zonke iintlawulo ezazenziwe.

Imfihlo

Iibhanki zesiqhelo zenza iintlawulo zonaniselwano zibe yimfihlo ngokuthi zenze ukuba ulwazi ngazo lungasasazwa, luphelele nje kwabo bantu bachaphazelekayo kunye nequmrhu elingelinye lesithathu elithembakeleyo. Iimeko apho kufuneka ezi ntlawulo zibhengezwe esidlangalaleni zona azibalwa kolu hlobo lonaniselwano kodwa iinkcukacha zingagcinwa ziyimfihlo ngenye indlela: ngokugcina iinkcukacha eziyimfihlo zingaziwa. Uluntu lungabona ukuba kukho umntu othumela isixa semali esithile komnye umntu, kodwa lungayazi ukuba le mali ihlawulwa kubani na. Oku kufana nqwa nendlela olupapashwa ngayo ulwazi ngamaziko orhwebo ngezabelo, apho ixesha kunye nomthamo worhwebo ubhengezwayo, kodwa kungachazwa ukuba ngoobani abebeqhuba urhwebo.

Njengesinye sezixhobo zokhuselo, kufuneka kusetyenziswe iikhowudi eziyimfihlo kwintlawulo nganye ukwenzela ukuba bangaziwa aba bananiselanayo. Lubakhona unxulumano phakathi kweentlawulo ezivela kwiindawo ezahlukeneyo, ezithi zivele ukuba zenziwe ngumntu omnye. Ingxaki yenzeka xa isitshixo-mfihlo sithe sachazwa, lo nto ingabangela ukuba kuvele ukuba nezinye iintlawulo zezomntu omnye.

Ukubala

Sicinga ngemeko apho unqalintloko ofuna ukwenza umonakalo ezakufuna ukudala esinye isixokolelwano somgunyathi phambi kokuba esi sokwenyani siyilwe. Nokuba ingenzeka le nto, ayibangeli ukuba kwenzeke umonakalo apho abantu bazenzela utshintsho bengagqithanga mntwini, umzekelo bazenzele imali engasuki ndawo okanye bathathe imali engeyoyabo. Izitishi zogcino-lwazi azizikuyamkela intlawulo engumgunyathi, kwaye azinakuthatha kwankcukacha zinento yokwenza nayo. Loo nqalintloko uzama ukwenza umonakalo angenza utshintsho kwiintlawulo ebezenziwe nguye kuphela azibuyisele imali ebesanda kuyihlawula.

Olu kruthakruthwano phakathi kwesixokelelwano sokwenyani kunye nesomgunyathi lungafaniswa ne-Binomial Random Walk. Zithi zeziphumelele ezi zixokolelwano zokwenyani ziqale zande ngebloko enye, loo nto izenze zibe phambili ngo: +1, size esi somgunyathi sibesemva ngebloko enye, lonto yenze ukuba kuthiwe umgama phakathi kwazo ngu: -1. s

Amathuba okuba lo nqalintloko ade aleqe angabi semva angafaniswa nala nto kuthiwa yi-Gambler’s Ruin Problem. Masithi umntu ongcakazayo onemali eyaneleyo ayibolekileyo uqala ukungcakaza sele esetyaleni aze adlale izihlandlo ezininzi ezama ukuba aphume etyaleni abanemali ekhoyo. Singabala amathuba okuba ade afikelele kwiqondo lokuba angabinatyala,

okanye unqalintloko ozama ukwenza umonakalo uza kuthatha ixesha elingakanani ukuze afikelele kule ndawo sikuyo isixokelelwano sokwenyani, ngolu hlobo lulandelayo[8]:

p = ngamathuba aza kuthathwa sisitishi sogcino-lwazi phambi kokuba sifumane enye i-block
q = amathuba okuba unqalintloko afumane i-block
q_z = amathuba okuba unqalintloko afikelele kwibloko eziku- z blocks behind

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

Ngenxa yokuba besiqikelele ukuba u $p > q$, la mathuba ehla kakhulu njengokuba inani leebloko unqalintloko ekufuneka efike kuzo lisanda. Kuba ke ngoku amathuba embalwa kakhulu, ukuba akazikufumana ntlahla enze umtsi omkhulu, amathuba akhe aye encipha kakhulu kwaye uye eshiyekela kakhulu.

Ngoku masikhe siqwalasele ixesha ekufuneka lo ufakelwe imali alilinde phambi kokuba aqiniseke ukuba umntu ebethumele imali akazikuphinda ayijike. Sithatha ngokuba lo uthumele imali ngunqalintloko ofuna ukuqhatha lo uza kuyifumana acinge ukuba ubhatelwe, aze asuke ayijike ayibuyisele kuye ukuhamba kwexsha. Lo ufumene imali uza kuxelelwa ngoko nangoko xa le nto isenzeka, kodwa yena la nqalintloko uza kucinga ukuba lo ebemthumele imali uza kothuka sekophulwe.

Lo ufumana imali uza kuyila isitshixo-mfihlo esitsha aze anike isitshixo-mfihlo sikawonke-wonke kulo ebeyithumele phambi kokuba atyikitye. Oku kuthintela lo ebethumele ukuba enze isixokolelewano seebloko phambi kwexesha ngokuthi ahlale kuyo angayeki ade abe nentlahla yokuba agqithe ibe nguye ophambili, aze enze intlawulo ngalo mzuzu. Yakuba yenziwe intlawulo, unqalintloko uqalisa ukusebenza ngondlela-mnyama kwesinye isixokelelwano esingesinye esinezinye iinkcukacha zale ntlawulo.

Lo uhlawulwayo yena uza kulinda ide intlawulo ibe kanti yenzekile kwibloko futhi nebloko ezingu: z zidityanisiwe emva koko. Akayazi indima esele ihanjwe ngunqalintloko, kodwa sisithi ke le bloko inyanisekileyo ithathe eli xesha liqhelekileyo ukusebenza kwibloko enye, umgama osele uhanjwe ngunqalintloko ungachazwa ngokwethiyori ye-Poisson Distribution kwaye iziphumo zingakhangeleka ngolu hlobo:

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

Ukuze sikwazi ukubala amathuba anawo unqalintloko phambi kokuba afike kule ndawo sikuyo, siphinda-phinda eli nani lixhaphakileyo libalwe ngokwe-Poisson ngesixa somgama ngamnye osele ewuhambile unqalintloko ngamathuba anawo okufika kule ndawo zikuyo ezi bloko zokwenyani:

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

Ukuwalandelelanisa ngokutsha ukuthintela ukuba amathuba abe linani elingenasiphelo…

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

Xa kuthe kwatshintshelwa kwikhowudi engu-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;
}
```

Xa sithe sahlalutya iziphumo, siyabona ukuba amathuba ehla kakhulu ngo: 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
```

Ukusombulula isibalo si-P esingaphantsi ko: 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
```

Isiqukumbelo

Siphakamise ukuba kusetyenziswe inkqubo ye-intanethi kungaxhomekekwa kumba wokuthembana. Siqale ngokucacisa esi sicwangciso siqheliweyo sendlela etyhutyha ngayo i-bitcoin ku-intanethi, into leyo yenza ukuba xa ungumnikazi we-bitcoin akekho omnye oza kuba nebango kuyo, kodwa lonto ayincedi ukuba akhona amathuba okuba ubanjiswe umgunyathi kuthi kanti le mali ucinga ukuba unayo sele isetyenzisiweyo, qha wena loo nto awuyazi. Ukusombulula le ngxaki, siye sacebisa ukuba kusetyenziswe ubuxhaka-xhaka obuza kulawulwa ngabarhwebi bonke apho kuza kusetyenziswa ubungqina bomsebenzi owenziweyo ukuze kubhalwe zonke iinkcukacha zeentlawulo ezenziweyo esidlangalaleni into leyo eza kubangela ukuba kungabi lula kwaphela ukuba unqalintloko enze utshintsho engagunyaziswanga ukuba izitishi zogcino-lwazi ezinyanisekileyo ziza kulawula umthamo omkhulu we-CPU. Obu buxhaka-xhaka bukhangeleka bulula kakhulu kodwa kunzima ukuba bube lixhoba lokuxhatshazwa. Izitishi zogcino-lwazi ziyasebenzisana kungekho bani uzimele ngasemva. Akunyanzelekanga ukuba zaziwe njengoko imiyalezo ingathunyelwa kwindawo ethile enye qha xa ithunyelwa kufuneka kuqinisekiswe ukuba akukho ndlela yakwenza utshintsho olungaziwayo. Izitishi zingamane ziphuncuka kodwa ziphinde zibuye, zixhomekeka nje kubungqina bomsebenzi owenziweyo njengelona xhadi lilithemba xa zifuna ulwazi xa ziphinda zibuya emva kokuba bezikhe zaqhawuka. Zixhomekeke kulwazi olukwi-CPU, apho zithi zizamkele iibloko njengokuba zisisixhobo sorhwebo esithambekeleyo zize zisebenzele ukuzandisa zize zizikhabe iibloko zomgunyathi ngokwala ukusebenza ngazo. Nayiphina imithetho nemigaqo efunekayo kunye nemivuzo efumanekayo ingalula xa kusetyenziswa le ndlela yokusebenzisana.

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.