Bitcoin: Lenaneo la tša elektroniki la tšhelete la thaka-go-thaka

ka Satoshi Nakamoto 2008/10/31

Sengwalwa

Mohuta wa tšhelete wa elektroniki wa thaka-ka-thaka o ka dumelela ditefo tša inthanete gore di romelwe go tšwa go motho yo motee go ya go yo mongwe ntle le go e romela pankeng. Mesaeno ya titšithale ke karolo ya tharollo, eupša meholagolo e lahlega ge eba go hlokega motho wa boraro gore a efoge tirišopedi. Re šišinya tharollo go bothata bja tirišopedi ka go šomiša kgokaganyo ya thaka-go-thaka. Kgokaganyo e tlogela kgatišo ya nako tša dithekišetšano ka go di fetolela tšhedimošo yeo e tsenego go ye nngwe ka go e iša go molokoloko wa mošomo woo o theilwego godimo ga bohlatse bjoo bo fetoletšwego ge e be e tsena mo khomphuthareng, gomme e tla dira kgatišo yeo e ka se kgonego go fetolwa ntle le go dira bohlatse-bja-mošomo ka lefsa. Molokoloko yo motelele ga se bohlatse bja go bontšha tatelano ya ditiragalo tšeo di bonwego fela, eupša ke bohlatse bja gore e tšwile go letamo le legolo la maatla a CPU. Ga feela bontšhi bja maatla a CPU a laolwa dinotse tšeo di sa thušego go hlasela kgokaganyo, di tlile go dira molokololo wo motelele le tšeo di ka hlaselago go tšwa ka ntle. Kgokaganyo ka bo yona e tlile go hloka sebopego se sennyane. Melaetša e tlile go phatlalatšwa ka dinako tša maleba, gomme dinotse di ka kgona go tloga ebile di a tsena go kgokaganyo, ka go amogela ketane ya mošomo wa bohlatse wo motelele bjalo ka bohlatse ka seo ba se dirilego ge di be di se gona.

Matseno

Kgwebo mo Inthaneteng e ithekgile ka go ikgetholla gannyane go dipanka tšeo di šomago bjalo ka motho wa boraro mo tshepedišong ya ditefo tša elektroniki. Ge lenaneo le šoma gabotse go dithekišetšano tše dintšhi, le sa tshwenya ke bofokodi bjoo bo lego gona bja mmotlolo wa go tshepa. Dithekišetšano tša go go se bušetšwe morago ga di kgonege, ka ge dipanka di ka se kgone go efoge go dingangišano tša dipoledišano. Theko ya dipoledišano di oketša theko ya dithekišetšano, e lekanetša minimamo ya bogolo bja dithekišetšano tšeo di tlwaelegilego le go fokotša kgonagalo ya dithekišetšano tše nnyane, ebile go na le theko ye kgolo go tahlegelo ya go dira ditefo tša go bušetšwa go ditirelo tša go se bušetšwe morago. Ka kgonagalo ya go bušetša morago, go ba le tlhokego ya tshepo. Barekiši ba swanetše go ela bareki hloko, ba ba tshwenye ka go nyaka tshedimošo ye ntšhi go feta ka moo e hlokegago. Peresente ye nngwe ya bofora e amogetšwe bjalo ka yeo e ka se kgone go efeogwa. Go se kgonthišišege ga ditheko le ditefo tše go ka efogwa ka nnete ka go šomiša kharentshi ya nnete, eupša ga gona mokgwa wo o lego gona go ka dira ditefo tše ka tšhanele ya dipoledišano ka ntle ga motho wa boraro yo a tshepegilego.

Seo se hlokegago ke lenaneo la go lefa la eletroniki leo le thekgilwego godimo ga bohlatse bja cryptographic (mabokgoni a sofotewe a go kgona go thekga mesaeno ya titšhithale le tshepedišo ya go fetolela tshedimošo yeo e itšego go iša go ye nngwe mo khomphuthareng) go na le go gore e thekgwe godimo ga tshepo, e dumelela batho bafe goba bafe ba babedi gore ba rekišetšane ntle le go hloka motho wa boraro. Dithekišetšano tšeo di sa kgonego go bušetšwa morago ka khomphuthara di tlile go šireletša barekiši go bofora, mokgwa wa setlwaedi wa tokomane ya tumelelano o ka šomišwa gore o šireletša bareki. Mo letlakaleng le, re šišinya tharollo ya bothata bja tirišopedi ya tšhelete (double-spending) go šomišwa seba ya go phatlalatša kgatišo ya nako ya thaka-ka-thaka go dira bohlatse bja khomphuthara ka tatelano ya dithekišetšano. Lenaneo le šireletšegile ge fela dinotse ka moka tša nnete di ka laola bontšhi bja maatla a CPU go feta dihlopha dife goba dife tša dinotse tšeo di hlaselago.

Transactions

Re hlaloša khoine ya elektroniki bjalo ka molokoloko wa mesaeno ya titšhithale. Beng ba bangwe le ba bangwe ba tlile go romela khoine go yo a latelago ka go saena tshepedišo ya go fetolela tshedimošo ye itšego go iša go ye nngwe ya thekišetšano ya go feta ka setitšithale gomme senotlelo sa setšhaba sa mong yo a latelago ebile le go oketša tve mafelelong a khoine. Motho yo a lefago a ka netefatša mesaeno ka go netefatša molokoloko wa mong.

Bothata ke ge motho yo a lefago a sa kgone go netefatša go yo mongwe wa bang ga se a dirišepedi khoine. Tharollo yeo e tlwaelegilego ke go tsebiša molaodikgolo yo a tshepegilego, goba mothopo, yo o lekolago ge go dirwa tirišopedi go thekišetšano ye nngwe le ye nngwe. Ka morago ga thekišetšano ye nngwe le ye nngwe, khoine e swanetšwe gore e bušetšwe go mothopo gore o ntšhe khoine ye nngwe, ebile ke dikhoine tšeo di ntšhitšego ke mothopo fela tšeo go dumelwago gore di ka se dirišwe gabedi. Bothata ka tharollo ye ke gore pheletšo ya lenaneo ka moka la tšhelete le ipotile ka kgwebo e sepediša mothopo, thekišetšano ye nngwe le ye nngwe e feta go bona, go swana le panka.

Re hloka tsela ya go dira gore motho yo a lefago a tsebe gore mong wa kgale ga se a saena dithekišetšano dife goba dife tša pejana. Ka morero wa rena, thekišetšano ya pejana ke yona yeo re e balago, bjale a re na taba ka maiteko a tirišopedi a morago. Tsela fela yeo e netefatšago tlhokego ya thekišetšano ke go kgafa šedi go dithekišetšano ka moka. Go motlolo wo o thekgilwego go mothopo, mothopo o be o tseba ka dithekišetšano ka moka ebile o tšere sephetho sa gore ke efe yeo e fihlago pele. Go fihlela se ntle le motho wa go tshepega, dithekišetšano di swanetšwe gore di phatlalatšwe mo setšhabeng[1], ebile re hloka lenaneo la bakgathatema gore ba dumelelane go histori ye tee ya tatelano yeo di tla go amogelwa ka yona. Motho yo a lefago o hloka bohlatse gore ka nako ya thekišetšano ye nngwe le ye nngwe, bontšhi bja dinotse bo dumetše gore ke yona ya matho ya go amogela.

Seba ya kgatišo ya nako

Tharollo yeo re e šišinyago e thoma ka seba ya kgatišo ya nako. Seba ya kgatišo ya nako e šoma ka go tšea tshedimošo yeo e fetoletšwego ya poloko ya dilo gore nako e kgatišwe le go phatlalatša tshedimošo yeo e fetolwetšwego go ye nngwe, bjalo ka sephatlalatšwa sa kuranteng goba Usenet [2-5]. Kgatišo ya nako e hlatsela gore tshedimošo yeo e kgobokeditšwego e swantše e le gore e be e le gona ka nako yeo, go molaleng, gore e ka tsena ka ka gare ga tshepedišo ya go fetolela tšhedimošo ye itšego go iša go ye nngwe. Kgatišo ya nako ye nngwe le ye nngwe e akaretša kgatišo ya nako yeo e fetilego ka gare ga tšhepedišo ya yona ya go fetolela tšhedimošo go ye nngwe ka go išwa go ye nngwe, e hloma molokolokolo, ka kgatišo ya nako ye nngwe le ye nngwe ya koketšo e matlafatša tšeo di tlilego pele ga yona.

Bohlatse bja Mošomo

Go diragatša seba ya kgatišo ya nako yeo e phatlaladitšwego ya maemo a thaka-go-thaka, re tlile go hloka lenaneo la bohlatse-bja-mošomo la go swana le la Adam Back's Hashcash[6], go na le diphatlhalatšwa tša kuranta goba Usenet. Bohlatse-bja-mošomo bo akaretša go lekodišiša maemo a ge tshedimošo yeo e fetoletšwego go ye nngwe, bjalo ka SHA-256, tshepedišo ya phetolelo ya tshedimošo go išwa go ye nngwe ka go thoma ka nomoro ya dibitsi tša lefela. Tekanyo ya mošomo woo o hlokegagao o lekana ka nomoro ya dibits tša lefela tšeo di hlokegago ebile di kgona go netefetšwa ka go dirwaa tshedimošo ye tee yeo e fetoletšwego go ye nngwe.

Mo kgokaganyong ya rena ya kgatišo ya nako, re dira bohlatse-bja-mošomo ka go oketša di nontshe ka gare ga poloko go fihla maemo a hwetšwa ao a fago poloko tša tshedimošo yeo e fetoletšwego go ye nngwe dibits tše lefela. Ge maiteko a CPU a oketšega gore e kgotsofatše bohlatse-bja-mošomo, poloko e ka se kgone go fetolwa ntle le gore mošomo o dirwe ka lefsa. Ka morago dipoloko di dira molokoloko ka morago ga yona, mošomo wa go fetola poloko o tla akaretša go dira dipoloko ka lefsa ka morago ga yona.

Bohlatse-bja-mošomo borarabolla bothata bja go laetša boemedi ge bontšhi bo tšea diphetho. Ge bontšhi bo be bo ithekgile godimo ga IP-aterese-ye-tee-boutu-ye-tee, e ka tlolwa ke motho wa go nyatša lenaneo goba mokgatlo yo a kgonago go aroganya di IP tše dintšhi. Bohlatse-bja-mošomo bo bohlokwa go CPU-ye-tee-boutu-ye-tee. Sephetho sa ba bantšhi se emelwa ke molokolokolo yo motelele, yo o nago le maatla a bohlatse-bja-mošomo a magolo ao a bolokilwego go wona. Ge bontšhi bja maatla a CPU a laola ke dinotse tša nnete, molokoloko wa nnete o tlile go gola ka lebelo le go feta melokoloko yefe goba yefe yeo e phadišanago nayo. Go matalafatša kago yeo e fetilego, mohlasedi o tla swanelwa ke go dira bohlatse-bja-mošomo bja poloko ka lefsa le dipoloko ka moka ka morago ga fao ebile ya fihlela le go feta mošomo wa dinotse tša nnete. Re tlile go bontšha ka morago nyana kgonagalo ya mohlasedi wa go nanya a fihlela le go senya ka go šoro

ge dipoloko tše di šetšego di lokelwa.

Go lefa koketšo ya lebelo la hatewe le kgahlego ya go fapafapapna mo go tshepedišong ya dinotse ka morago ga nako, mathata a bohlatse-bja-mošomo bo laelwa ke tekanyo yeo e sepelago yeo e nepilego nomoro ya tekanyo ya dipoloko iri ye nngwe le ye nngwe. Ge di ka dirwa ka pela, mathata a tlile go oketšega.

Kgokaganyo

Makgato a go sepediša kgokaganyo ke a a latelago:

1. Dithekišetšano tše di mpfsa di tlile go phatlalatšwa go dinotse ka moka.
2. Notse ye nngwe le ye nngwe e tšea dithekišetšano tše di mpfsa ka gare ga kago.
3. Notse ye nngwe le ye nngwe e šoma ka go hwetša bothata bja bohlatse-bja-mošomo bja kgao ya yona.
4. Ge notse e hwetša bohlatse-bja-mošomo, e phatlalatša poloko go dinotse ka moka.
5. Dinotse di amogela poloko ge fela dithekišetšano ka moka ka gare yona di šoma gabotse ebile di se štwe di šomišwa.
6. Dinotse di hlagiša kamogelo ya tšona ya poloko ka go dira kago yeo e latelago mo molokolokong, go šomišwa tshepedišo ya go fetolela tshedimošo go ye nngwe ya kago ye e amogetšwego bjalo ka tshepedišo ya tshedimošo ya go fetolela go ye nngwe yeo e fetilego.

Dinotse di phela di šetša molokoloko yo motelele go ba wona wa nnete ebile di tlile go tšwela pele ka go šoma e di oketša. Ge dinotse tše pedi di phatlalatša mehuta ya poloko ka nako ye tee, dinotse tše dingwe di ka amogela ye tee goba ye nngwe pele. Ge go le bjalo, di šoma go yeo ba e hweditšego la mathomo, eupša ba boloka dikalana tše dingwe ge e ka ba e telele. Setlemaganyi se tlile go robega ge bohlatse-bja-mošomo wo o latelago se ka hwetšwa ebile kalana e tlile go ba e telele, dinotse tveo di be di šoma go kalana ye nngwe e tlile go fetogela go ye telele.

Go phatlalatšwa ga thekišetšano ye mpfsa ga e hloke gore e fihlelela dinotse ka moka. Ge fela e ka fihlelela dinotse tše dintšhi, di tlile go tsena ka gare ga poloko ka pejana. Go phatlalatšwa ga kago go kgona go kgotlelela melaetša yeo e lahletšwego. Ge notse e ka se hwetše poloko, e tlile go e kgopela ge e amogela kago ya go latela gomme ya lemoga gore ga se ya e hwetša.

Incentive

Ka kwano, thekišetšano ya mathomo ka gare ga poloko ke thekišetšano yeo e kgethegilego yeo e thomago khoine ye mpfsa ya mohlodi wa poloko. Se se oketša ponase go dinotse gore di thekge kgokaganyo, ebile e bula tsela gore e kgone go phatlalatša dikhoine ka go dikologa, ka ge go na le taolo ya magareng ya go di ntšha. Koketšo yeo e sa fetogego ya tekanyo ya dikhoine tše di mfsa e sepedišana le baepi ba gauta ba šomiša methopo go oketša gauta gore e dikologa. Mo sebakeng sa rena, ke nako ya CPU le mohlagase wo o šomišwago.

Ponase e ka kgona go lefswa ka ditefelo tša thekišetšano. Ge boleng bja setšweletšwa sa thekišetšano bo le ka tlase ga boleng bja setsenywa, phapano ke gore ditefelo tša thekišetšano yeo e oketšwago ka gare ga boleng bja ponase bja poloko yeo e sweregо thekišetšano. Ge palo ya dikhone tšeo rulagantšwe peleng di tsena ka go dikologa, ponase e ka fetogela go ditefelo tša thekišetšano gomme e se ke ya ba le infleišene.

Ponase e ka thuša gore e hohleletše dinotse gore di dule di botegile. Ge mohlasedi wo megabaru a ka kgona go aga maatla a CPU a mantši go feta dinotse ka moka tšeo di botegilego, o tlile go hloka gore a kgethe magareng a go e šomiša ka go radia batho ka go ba utšwa tšehelete yeo a e lefilego, goba ka go e šomiša ka go dira dikhoine tše dingwe. A ka hola tšhelete ye ntšhi ka go latela molao, melao ye mebjalo e ka mo fa dikhoine tše dintšhi tše di mfswa go feta batho ba kopane, go na le go lebelela lenaneo fase le kgonthišišo ya lehumo la gagwe.

Reclaiming Disk Space

Ge thekišetšano ya morago ka gare ga khoine e bolokwa ka tlase ga poloko, dithekišetšano tšeo di dirišitšwego pele di lahlwa go boloka speyisi sa tiski. Go hlahla se ntle le go roba tshedimošo ya poloko yeo e fetolelwago go ye nngwe, dithekišetšano di fetotšwe ka gare ga Merkle Tree [7][2][5], ka medu fela yeo e akaretšago tshedimošoya poloko yeo e fetotšwego go ye nngwe. Dipoloko tva kgale di ka swarišana ka go tloša dikalana tša mohlare. Bokagare bja tshedimošo yeo e fetotšwego go išwa go ye nngwe ga bo hloke gore bo bolokwe.

Sehlogo sa poloko e se na dithekišetšano e ka ba dibytes tše 80. Mohlomongwe dipoloko di dirwa ka morago ga metsotso ye 10 ye mengwe le ye mengwe, dibyte tše * 6 * 24 * 365 = 4.2MB ngwaga ka ngwaga. Ka mananeo a khomphuthara ao a rekišago ka 2GB ya RAM go tloga ka 2008, le Moore's Law e bolelela pele ka go gola ga 1.2GB ngwaga ka ngwaga, bobolokelo ga se ba swanelwa ke go ba bothata ge sehlogo sa poloko se swanetšwe gore se beiwe ka gare ga memori.

Simplified Payment Verification

Go a kgonega gore a netefatše ditefo ntle le go sepediša kgokaganyo ya dinotse ye e tletšego. Modiriši o hloka go dira khophi ya dihlogo tša poloko ya molokoloko wo motelele wa bohlatse-bja-mošomo, yeo a ka e hwetšago ka go botšiša go dinotse tša kgokaganyo go fihla a kgotsofala gore o na le molokoloko wo moteletelele, le go hwetva kalana ya Merkle yeo e tswalantšhago thekišetšano go ya go kgatišo ya nako yeo poloko e lego ka gare ga yona. Ga a kgone go lekola thekišetšano ka bo yena, efela ka go e tšwalantšha le lefelo ka gare ga molokoloko, o kgona go bona gore node ya kgokaganyo e amogetše, ebile dipoloko di okeditše ka morago ore e netefatše gore kgokaganyo e amogetše.

Ge go le bjalo, netefatšo e a tshepega ge dinotse tše botegilego di na le taolo ya kgokaganyo, eupša e bokoa kudu ge kgokaganyo e fenywa ke mohlasedi. Ge dinotse tša kgokaganyo di kgona go netefatša dithekišetšano, tsela ye e nolofaditšwego e ka forwa ke dithekišetšano tša maitirelo tšeo di dirwelog ke mohlasedi go fihla mohlasedi a tšwela pele ka go fenya kgokaganyo. Leano le le tee la go šireletša gahlanong le se go ka ba go amogela ditsebišo go tšwa go dinotse tša kgokaganyo ge di hwetša poloko yeo e sa šomego, e dira gore sofotewe ya modiriši a tounoloute poloko yeo e tletšego ebile e tsebiše dithekišetšano go netefatša go sepele gabotse. Dikgwebo tšeo amogelago ditefo gantšhintšhi di ka nyaka go sepetša dinotse tša yona ka tšhireletšo ya go ikemela ye ntšhi le go netefatša ka pela.

Combining and Splitting Value

Le ge go swara dikhoine ka botee go kgonega, go ka ba boima gore di sepedišwe ka lebaka la bogolo bja tšona gore di kgaogantšhwe ka sente ye nngwe le ye nngwe ge e romelwa. Go dumelela gore boleng bo kgaogantšhwe le gore bo hlakantšhwe, dithekišetšano di swara ditsenywa le ditšweletšwa tše dintšhi. Mehleng go ka ba le setsenywa se se tee go tvwa go thekišetšano ya morago ye kgolo goba ditsenywa tše dintšhi tše di hlakantšhago dikelo tše nnyane, ebile ka nako ye ntšhi ditšweletšwa tše pedi: ye tee ke ya tefo, mola ye nngwe e le ya go bušetša tšhentšhi, ge e le gona, morago go yo a e rometšego.

E swanetše gore e elwe hloko gore ga se ya boela, mo thekišetšano e ithekgile go dithekišetšano tše mmalwa, ebile dithekišetšano tšeo di ithekgile godimo ga tše dingwe tše dintšhi, ga se bothata mo. Ga go na tlhokego ya go ntša khopi ya histori ya thekišetšano yeo ikemetšego ka noši ka moka.

Khupamarama

Motlolo wa panka wo o tlwaelegile o fihlelela maemo a khupamara ka go lekanetša tumelelo ya tshedimošo go batho bao ba amegago le batho ba boraro bao ba tshepegilego. Tlhokego ya go tsebiša dithekišetšano ka moka e phatlalatšwa thibelo ya tsela ye, efela khupamarama e ka kgona go šireletšwa ka go roba go thsepedišo ya tshedimošo lefelong le lengwe: ka go dira gore dinotlelo tša setšhaba di se ke di a tsebjwa. Setšhaba se go na go bona ge motho a romela tšhelete go yo mongwe, eupša ntle le tsehdimošo yeo e tswalanygo thekišetšano go motho yo mongwe. Se se swana le maemo a tshedimošo ao a ntšhitšwego go kabelano ya phahlo., moo nako le kelo ya dikgwebišano ka noši, "tape", e bewago gore e bonwe ke setšhaba, eupša ntle le go tseba gore mang ke mang.

Bjalo ka fayawolo ya koketšo, dinotlelo tše di fsa di swanetšwe gore di šomišwe mo thekišetšanong ye nngwe le ye nngwe go di kgaogantšha gore di se ke di a hlakana go beng bao ba tlwaelegilego.

Tswalanyo ye nngwe o ka se e efoge ka dithekišetvano tše dintšhi-tša-ditsenywa, tšeo di tšweletšago gore ditsenywa tša yona di be di na le beng ba ba tee. Kotsi mo ke gore mong senotlelo a ka tšweletša gore dithekišetšano tše dingwe di be e le tša mong yo motee.

Calculations

Re akanya tlhalošo ya ka moo dilo di ka ba e le gore di diregile ka gona mohlasedi a ka be a leka go dira molokoloko yo mongwe ka pela go feta molokoloko wa potego. Le ge se se ka kgonagala, ga se lahle lenaneo gore lebulele diphetogo tša sepetho seo se sa ithekgago godimo ga lenaneo, bjalo ka go iterela mohola mo moyeng goba ka go tšea tšhelete yeo e be e se ya mohlasedi. Dinotse di ka se amogele thekišetšano yeo e sa šomego bjalo ka tefo, ebile notse ya potego e ka se tsoge e amogetše poloko yeo e nago le tšona. Mohlasedi a leka go fetola fela ye nngwe ya dithekišetšano tša gagwe gore a tšee tšhelete ye a šetše a e dirišitše.

Lebelo magareng ga molokoloko wa potego le molokoloko wa mohlassedi e ka bitšwa Binomial Random Walk. Tiragalo ya katlego ke ge molokoloko wa potego o oketša ka poloko ye tee, e ikokeletša ka go etela pele ka +1, ebile tiragalo ya go se atlege ke ge molokoloko wa mohlasedi o oketša ka poloko ye tee, o fokotša sekgooba ka -1.

Phorophabilithi ya gore mohlasedi a e sware go tšwa go tefisiti yeo e filwego go sepedišana le bothata bja Gamble's Ruin. Ga re kempolara e na le sekoloto seo se se nago tekanyetšo se thoma ka go ba tefisiti ebile se raloka ka kgonagalo ya ditrayale tša palo ya go se felele go leka go fihlelela kgaola ka bogare. Re ka hlakantšha phorophabilithi ya go fihlelela kgaola ka bogare, goba ya gore mohlasedi a ka fihelela molokoloko wa potego, bjale ka se se latelago[8] :

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

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

Go ya ka kgopolo ya rena $p > q$, phorophabilithi e ka fokotšega kudu ge palo ya dipoloko yeo mohlasedi a swanetšego gore a e fihlelele e oketšega. Ge dilo ka moka di se ka lehlakoreng la gagwe, ge a ka se be le mahlatse a go ya pele ka pela, sebaka sa gagwe se ba se sennyane kudu ge a šalela morago.

Gonabjale re akanya gore ke nako ye kaakang yeo moamogedi wa thekišetšano ye mfsa a ka hloka go ema pele a ka ba le bonnete bja gore moromedi a ka se fetole thekišetšano. Re gopola gore moromedi ke mohlasedi yo a nyakago gore moamogedi a nagane gore o mo lefile sebakanyana, ge a fetša a fetolele tefo go yena ka morago ga ge nako e fetile. Moamogedi o tliel go tsebišwa ge seo se direga, eupša moromedi o holofela gore šetše e le llata.

Moamogedi o dira dinotlelo tše dingwe gomme o di fa moromedi senotlelo pele a ka e saena. Se se thibela gore moremedi a ka dira molokoloko wa dipoloko pele ga nako ka go šoma a sa fetše go yona go fihla a ba mahlaste ka moo go lekanego gore a be pele, ge a fetša a dire thekišetšano ka yona nako yeo. Ge thekivetšano e rometšwe, moromedi wa go se tshepege o tla thoma go šoma ka sephiring go molokoloko wa go lebana wo o swerego lehlakore le lengwe la thekišetvano ya gagwe.

Moamogedi o la leta go fihla thekišetšano ya gagwe e ka oketšwa go poloko le z dipoloko kgale di tswalantšhitšwe ka morago ga yona. Ga a tsebe tšwelopele ya mohlasedi gabotse, eupša go gopola gore dipoloko tva potego di tšere nako yeo e letetšwego ya tlwaelo go poloko ka poloko, tšwelopele ya mohlasedi e tlile go ba phatlalatšo ya Poisson ka boleng bjo bo letetšwego:

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

Go hwetša phorophabilithi mohlasedi a ka kgona go e fihelela le gabjale, re malthipholaya Possion ka tensithi ya tšwelopele ye nngwe le ye nngwe a ka be a e dirile ka phorophabilithi yeo a ka e fihlelela go tloga gona moo:

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

Di beakanye go efoga go hlakantša mosela woo o sa felelego wa phatlalatšo...

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

Converting to C code...

```
#include
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Re dira dipoelo, re kgona go bona gore phorophabilithi e fokotšegile ka 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
```

Go rarabolla P ge e le ka tlase ga 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
```

Thumo

Re šišintše lenaneo la dithekišetšano la elektroniki ntle le go tshepela go tshepo. Re thomi ka tlhomo ya dikhoine yeo e dirilwego go tšwa go mesaeno ya titšithale, yeo e fago taolo ye ntšhi go beng, eupša ga se ya felelal ntle le tsela ya go thibela tirišopedi. Go rarabolla se, re šišintše kgokaganyo ya thaka-go-thaka ka go šomiša bohlatse-bja-mošomo go kgatiša histori ya setšhaba

ya dithekišetšano tšeo di sa kgonego go ba tša sekhomphuthara ka pela gore mohalsedi a ka fetola dinotse tša potego di laola maatla a mantši a CPU. Kgokaganyo e na le maatla ebile e phedile ka go se agege ka moo go nolofaditšwego. Dinotse di šoma ka moka ka nako ye tee ka tshepedišo ye nnyane. Ga di hloke go tsebjwa, ka ge melaetša e sa išwa go lefelo lefe goba lefe leo le itšego ebile le išwa ka tšea matsapa a magolo fela. Dinotse di sepela ebile di kopana gape le kgokaganyo ge di nyaka, kamogelo ya molokoloko wa bohlatse-bja-mošomo ke bohlatse bjaseo se diragetšego ge di be di sepetše. Dibouta ka maatla a CPU a yona, di tšweletša kamogelo ya dipoloko tša go šoma ka go di oketša le go gana go šoma go dipoloko tšeo di sa šomego. Any needed rules and incentives can be enforced with this consensus mechanism. Melao le diponase dife goba dife tšeo di hlokegago di ka lokelwa le sedirišwa se ka tumelelo ya bohle.

Ditšhupetšo

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.